

eScan Corporate for Windows - Cloud User Guide

Product Version: 22.0.0000.xxxx Document Version: 22.0.0000.xxxx

24x7 FREE Online Technical Support

support@escanav.com https://forums.escanav.com

An ISO 27001 Certified Company

ilill

D

www.escanav.com





Copyright © 2021 by MicroWorld Software Services Private Limited. All rights reserved.

Any technical documentation provided by MicroWorld is copyrighted and owned by MicroWorld. 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. This user guide may include typographical errors, technical or other inaccuracies.

MicroWorld does not offer any warranty to this user guide's accuracy or use. Any use of the user guide or the information contained therein is at the risk of the user. MicroWorld reserves the right to make changes without any prior notice. No part of this user guide 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 Private Limited.

The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, and MailScan are trademarks of MicroWorld. Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All other product names referenced in this user guide are trademarks or registered trademarks of their respective companies and are hereby acknowledged. MicroWorld disclaims proprietary interest in the marks and names of others.

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

Document Number: Current Software Version: Technical Support: Sales: Forums: eScan Wiki: Live Chat: Published by: Date: 5BUG/04.08.2024/22.x 22.0.xxxx.xxx support@escanav.com sales@escanav.com https://forums.escanav.com https://wiki.escanav.com/wiki/index.php/ https://www.escanav.com/english/livechat.asp MicroWorld Software Services Private Limited August, 2024





Content

Introduction
Web Console Login9
Main Interface
Navigation Panel11
Dashboard14
Deployment Status
eScan Status15
License
eScan version16
Protection Status
Update Status
Scan Status19
File Anti-Virus
Proactive
Mail Anti-Virus
Anti-Spam21
Firewall
Endpoint Security
Anti – Ransomware
Protection Statistics
File Anti-Virus
Anti-Spam
Web Protection
Endpoint Security-USB
Endpoint Security-Application27





Summary Top 10	
Asset Changes	29
Configure the Dashboard Display	
Managed Computers	
Search	
Update Agent	
Adding an Update Agent	
Delete an Update Agent	
Action List	
New Subgroup	
Removing a Group	
Create Client Setup	
Properties of a group	40
Assigning a Policy to the group	41
Client Action List	43
Move to Group	44
Remove from Group	44
Refresh Client	44
Show Critical Events	44
Export	44
Show Installed Softwares	46
Create OTP	47
Properties of Selected Computer	
Understanding the eScan Client Protection Status	
Anti-Theft	51
Anti-Theft Options	51
Disable Anti-Theft	54
Select Columns	55





Policy Template	56
Managing Policies	56
Creating Policy Template for a group/specific computer	59
Configuring eScan Policies for Windows Computers	60
Configuring eScan Policies for Linux and Mac Computers	
Assigning Policy Template to a group	163
Assigning Policy Template to Computer(s)	164
Copying a Policy Template	165
Report Templates	166
Creating a Report Template	167
Creating Schedule for a Report Template	167
Viewing Properties of a Report Template	167
Deleting a Report Template	168
Report Scheduler	169
Creating a Schedule	169
Viewing Reports on Demand	171
Managing Existing Schedules	171
Generating Task Report of a Schedule	172
Viewing Results of a Schedule	172
Viewing Properties of a Schedule	173
Deleting a Schedule	173
Events and Computers	174
Events Status	174
Computer Selection	175
Edit Selection	176
Software/Hardware Changes	
Violations	179
Settings	





Event Status Setting	
Computer Selection	
Software/ Hardware Changes Setting	
Performing an action for computer	
Asset Management	
Hardware Report	
Filtering Hardware Report	
Exporting Hardware Report	
Software Report	
Filtering Software Report	
Exporting Software Report	
Software License	
Filtering Software License Report	
Exporting Software License Report	
Software Report (Microsoft)	
Filtering Software Report (Microsoft)	
Exporting Software Report (Microsoft)	
Filtering Microsoft OS Report	
Exporting Microsoft OS Report	
User Activity	
Print Activity	
Viewing Print Activity Log	
Exporting Print Activity Log	
Filtering Print Activity Log	
Exporting Print Activity Report	
Session Activity Report	
Viewing Session Activity Log	
Filtering Session Activity Log	





Exporting Session Activity Report
File Activity Report
Viewing File Activity Log
Filtering File Activity Log198
Exporting File activity Report199
Application Access Report
Viewing Application Access Report
Filtering Application Access Report
Exporting Application Access Report
Notifications
Event Alert
Unlicensed Move Alert
Settings
Web Console Settings
Excluded Clients
Two-Factor Authentication (2FA)
Enabling 2FA login
Disabling 2FA login
Users For 2FA
Administration
User Accounts
Create New Account
Delete a User Account
User Roles
New Role
View Role Properties
Delete a User Role
License





Adding and Activating a License	
Moving Licensed Computers to Non-Licensed Computers	
Moving Non-Licensed Computers to Licensed Computers	
Contact Us	
Forums	224
Chat Support	
Email Support	





Introduction

eScan Corporate for Windows – Cloud is a corporate line security solution based on SaaS platform. With this, company's network administrator can deploy robust and layered security to the connected endpoints within the organization's network system via Cloud environment.

This new cloud solution strengthens the cyber-security capabilities of the businesses by providing multi-layered protection to the IT infrastructure from complex threats and secures critical business information effectively without constraining business growth. It is an excellent combination of advanced and futuristic technologies that provides protection to Windows, Mac and Linux-based endpoints in the network.

Web Console Login

The web console login page can be accessed via this method:

- 1. Launch a web browser.
- 2. Enter the following URL: cl.escanav.com.
- 3. Web console login page appears.

Corporate for Windows - Management Console						
WEB CONSOLE	LOGIN					
Please type the Compa the Web console.	ny ID/Partner ID/Email ID, username and password to access					
Company ID/Partner ID/Email ID*						
Username:*						
Password:*	Login					
	Forgot password? Register here					

- 4. Enter the login credentials defined during installation.
- 5. Click Login.





Main Interface

About eScan 🔡

Clicking About eScan opens MircoWorld's homepage in a new tab.

Username 🤷

Clicking **Username** allows you to edit User Login details like Full name, Password and email address that you use to Login in the eScan Management Console.

Edit User			👔 Help
Enable this	account		
Account Type	e and Information		
Custom Acco	ount		
Username:	root		
Full Name*:	1011100-10140-10140		
New Password:	•••••		
Confirm Password:	•••••		
Email Address:			
	For Example: user@yourcompany.com		
Account Role			
Role*:	Administrator	~	
Save	Close		(*) Mandatory Fields

Log off

Clicking Log off logs you out of the eScan Management Console.

Company Name

This option displays user and company information.





Navigation Panel

DashBoard	
Managed Computers	Ð
Report Templates	
Report Scheduler	
Events & Computers	
Asset Management	
🗄 User Activity	
Notifications	
🗄 Settings	
Administration	
License	





Dashboard

The Dashboard module displays charts showing Deployment status, Protection status, Protection Statistics, Summary Top 10 and Asset Changes. The monitoring is done by Management Console of the computers for virus infections and security violations. To learn more, <u>click here</u>.

Managed Computers

The Managed Computers module lets you define/configure Policies for computers. It provides you various options for creating groups, adding tasks, moving computers from one group to another and vice versa. To learn more, <u>click here</u>.

Report Templates

The Report Templates module lets you create and view customized reports based on a given template, for a given period; sorted by date, computer, or action taken; and for a selected condition or target group. It also provides options for configuring or scheduling reports, viewing report properties, and refreshing or deleting existing reports. To learn more, <u>click here</u>.

Report Scheduler

The Report Scheduler module lets you schedule a new reporting task, run an already created reporting schedule, or view its properties. To learn more, <u>click here</u>.

Events and Computers

The Events and Computers module lets you monitor various activities performed on client's computer. You can view log of all events based on Event Status, Computer Selection or Software/ Hardware Changes on that client computer. Using the Settings option on the screen you can define settings as desired. To learn more, <u>click here</u>.

Asset Management

The Asset Management module provides you the entire Hardware configuration and list of software installed on computers. Using this module, you can easily keep a track of all the Hardware as well as Software resources installed on all the Computers connected to the Network. Based on different search criteria you can easily filter the information as per your requirement. It also lets you export the entire system information available through this module in PDF, Microsoft Excel or HTML formats. To learn more, <u>click here</u>.

User Activity

The User Activity module lets you monitor different tasks/activities like printing, session login time or actions on files in the client computers. To learn more, <u>click here</u>.

Notifications

The Notifications module provides you the options to enable different notifications for different actions/incidents on the endpoints. You may choose to be notified or not to be notified based on the significance of these actions in your business. To learn more, <u>click here</u>.

Settings

The Settings module lets you configure eScan Console timeout settings, dashboard setting, exclude client settings for eScan. To learn more, <u>click here</u>.





Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. By using this module, you can allocate rights to the other employees which will allow them to install eScan Client and implement Policies and tasks on other computers. To learn more, <u>click here</u>.

License

The License module lets you manage licenses of users. You can add, activate, and view the total number of licenses available for deployment, number of licenses deployed, and number of licenses remaining with their corresponding values. You can also move the licensed computers to non-licensed computers and vice-versa. To learn more, <u>click here</u>.

Icons on every status Label denotes that the status is displayed for the computers having operating system as Windows, MAC OS X or Linux.





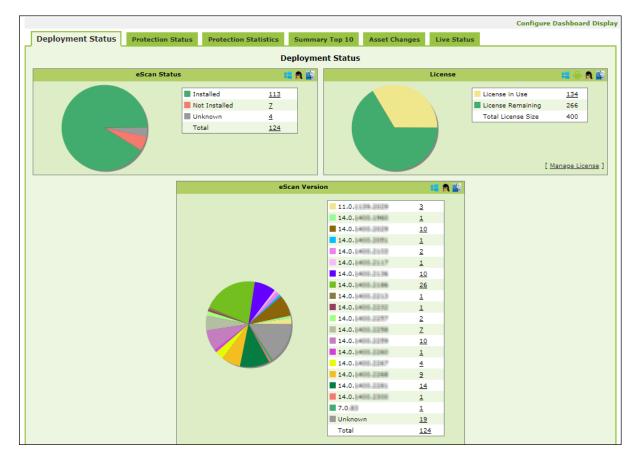
Dashboard

The Dashboard module displays statistics and status of eScan Client installed on computers in pie chart format. It consists of following tabs:

- Deployment Status
- Protection Status
- Protection Statistics
- Summary Top 10
- Asset Changes

Deployment Status

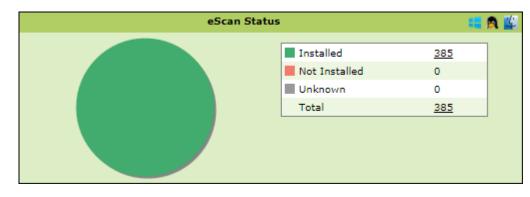
This tab displays information about eScan Client installed on computers, active licenses, and current eScan version number in use.





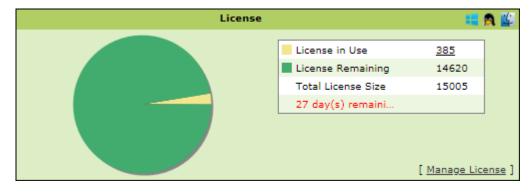


eScan Status



Installed – It displays the number of computers on which eScan Client is installed.
Not Installed - It displays the number of computers on which eScan Client is not installed.
Unknown - It displays the number of computers on which Client installation status is unknown.
(eScan Cloud is unable to receive information from the computers for a long time)

License



License in Use - It displays the number of licenses that are active. **Licenses Remaining** - It displays the number of remaining licenses.





eScan version

The eScan Version chart shows the total number of eScan versions installed on the computers on the network.

eScan	Version	🖷 🕅 🕍
		3
		1
	·	10
	Carlos Carlos Participation	2
	· · · · · · · · · · · · · · · · · · ·	1
	101000-000-000	10
		25
	Canada Canada a Su	1
		1
	· · · · · · · · · · · · · · · · · · ·	2
	- 410-10-000-000	Z
	- 2101-220-240	10
	· # 10 · # 20 · · · · · · · · · · · · · · · · · ·	1
		3
	41111200-1001	2
		15
		1
		1
		20
	Total	123

Click on the numbers on the right-side of the each version, you can view the details of the computers.

Deployment Status >> eScan Version			👧 🗳
Client OS Type All 🗸			<u>Print</u>
Machine Name	Version	Group	
#16#603#	14.0.1400.	Managed Computers\+	
SARLENADEVISI.	14.0.1400.	Managed Computers\	
\$10-7304	14.0.1400	Managed Computers\ 54444	
84-7358	14.0.1400.	Managed Computers	
#JF7208	14.0.1400.	Managed Computers\ 54444	
#4-7255	14.0.1400.	Managed Computers\	
#41-7238 	14.0.1400.	Managed Computers\ 5000000000000000000000000000000000000	
48-7982	14.0.1400.	Managed Computers	
US-7088	14.0.1400.	Managed Computers\	

ONOTE

Clicking underlined numerical displays detailed information for computers.

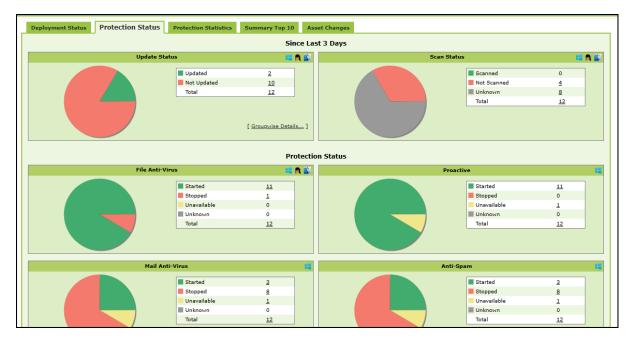
The Windows, Mac, Linux Icons at the top of every chart denote that the information is displayed for the respective Operating Systems (OS).





Protection Status

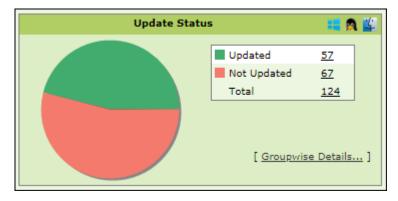
This tab displays the status of eScan Client's modules along with the Update and Scan status since last 7 days.







Update Status



Updated – It displays the number of computers on which virus signature database is updated. **Not Updated** - It displays the number of computers on which virus signature database is not updated.

Clicking Groupwise Details displays Groupwise Update Status window.

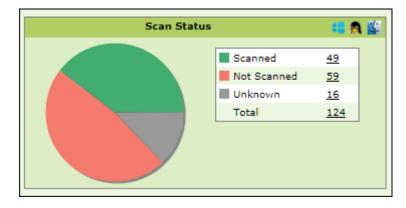
e Scan					eSca	n Ma	nage	emen	t Co	onsole
Groupwise Update Status						We	ednese	day, O	ctobe	er 23, 2019
🗄 🗐 Managed Computers	Include Sub Groups Groupwise Details Group: Managed Computers (Include Sub Groups)							<u>Print</u>		
	Group Name	<u>Updated</u>	Not Updated	License in Use	EP	<u>E0</u>	<u>CP</u>	<u>CO</u>	IL	NA
	Managed Computers	0	382	382	0	0	1	0	0	<u>381</u>
	Sample Group	0	3	3	1	0	1	0	0	1
	Test	3	0	<u>3</u>	2	0	1	0	0	0

It displays the number of computers on which virus database is Updated, Not Updated and Licenses in Use as per the group. Selecting **Include Sub Groups** checkbox will display the subgroups containing computers.





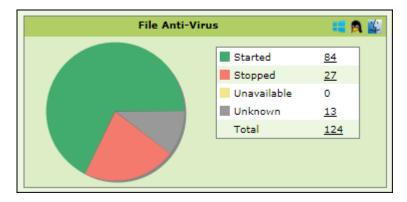
Scan Status



Scanned - It displays the number of computers that have been scanned in last 30 days for viruses and malware infections.

Not Scanned - It displays the number of computers that have not been scanned in last 30 days for viruses and malware infections.

File Anti-Virus



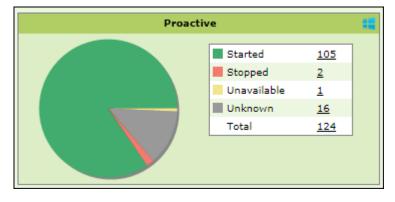
Started – It displays the number of computers on which the File Anti-Virus module is in Started state. **Stopped** – It displays the number of computers on which the File Anti-Virus module is in Stopped state.

Unavailable – It displays the number of computers where the File Anti-Virus module is unavailable. **Unknown** – It displays the number of computers where the File Anti-Virus module status is unknown.





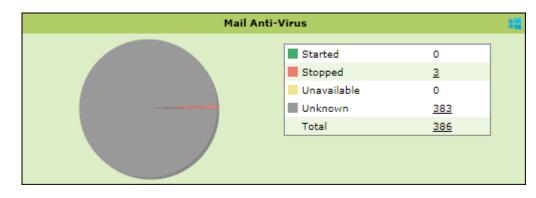
Proactive



Started - It displays the number of computers on which Proactive scanning service is running. **Stopped** - It displays the number of computers on which Proactive scanning service is stopped. **Unavailable** – It displays the number of computers where Proactive scanning service is unavailable. This module is available only in computers with Windows OS.

Unknown - It displays the number of computers on which the Proactive scanning service status is unknown.

Mail Anti-Virus



Started – It displays the number of computers on which the Mail Anti-Virus module is in Started state.

Stopped – It displays the number of computers on which the Mail Anti-Virus module is in Stopped state.

Unavailable – It displays the number of computers on which the Mail Anti-Virus module is unavailable.

Unknown – It displays the number of computers on which the Mail Anti-Virus module status is unknown.



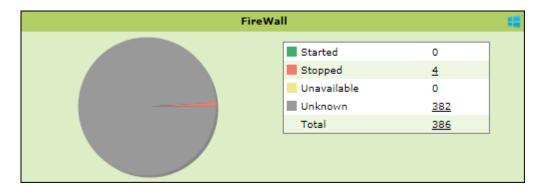


Anti-Spam

Anti-Spam						
	Started	0]			
	Stopped	3				
	Unavailable	0				
	Unknown	383				
	Total	386				

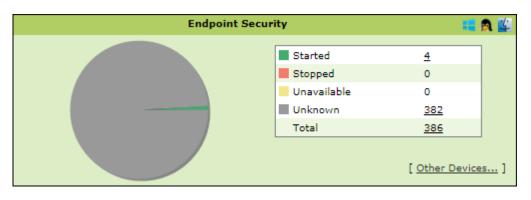
Started – It displays the number of computers on which the Anti-Spam module is in Started state. **Stopped** – It displays the number of computers on which the Anti-Spam module is in Stopped state. **Unknown** – It displays the number of computers on which the Anti-Spam module status is Unknown. **Unavailable** – It displays the number of computers on which the Anti-Spam module is Unavailable.

Firewall



Started - It displays the number of computers on which the Firewall module is in Started state.
Stopped - It displays the number of computers on which the Firewall module is in Stopped state.
Unavailable - It displays the number of computers on which the Firewall module is unavailable.
Unknown - It displays the number of computers on which the Firewall module status is unknown.

Endpoint Security







Started - It displays the number of computers on which the Endpoint Security module is in Started state.

Stopped - It displays the number of computers on which the Endpoint Security module is in Stopped state.

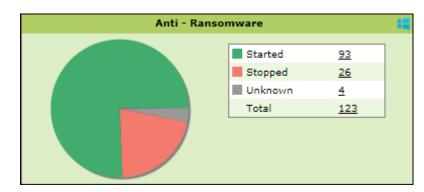
Unavailable – It displays the number of computers on which the Endpoint Security module is unavailable.

Unknown - It displays the number of computers on which the Endpoint Security module status is unknown.

Clicking Other Devices displays details about other devices.

-					
her Devices Status					
Other Devices	Allowed	Blocked	<u>Unavailable</u>	<u>Unknown</u>	Tota
SD Card	<u>6</u>	<u>0</u>	<u>0</u>	<u>382</u>	<u>388</u>
Web Cam	6	0	<u>0</u>	382	388
Bluetooth	6	<u>0</u>	<u>0</u>	382	388
USB Modem	6	<u>0</u>	<u>0</u>	382	388
Composite Devices	6	0	<u>0</u>	<u>382</u>	388
CD/DVD	6	0	<u>0</u>	382	388
Imaging Devices	6	<u>0</u>	<u>0</u>	382	388
WI-FI	6	<u>0</u>	<u>0</u>	382	388
Printer	6	<u>0</u>	<u>0</u>	382	388
	•				
	Close				

Anti – Ransomware



Started - It displays the number of computers on which the Anti – Ransomware module is in Started state.

Stopped - It displays the number of computers on which the Anti – Ransomware module is in Stopped state.

Unavailable – It display the number of computers on which the Anti – Ransomware module unavailable to system.

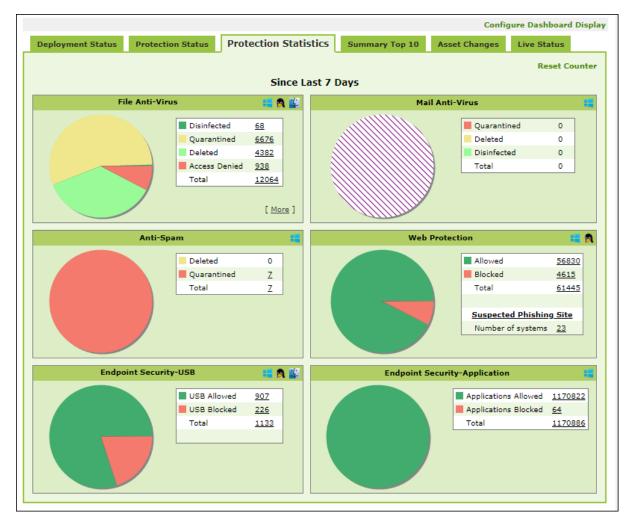
Unknown - It displays the number of computers on which the Anti – Ransomware module status is unknown.





Protection Statistics

This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



Reset Counter

Clicking **Reset Counter** resets all the statistics to zero. This option proves useful after you have taken an action on infected files and want to scan for residual infection presence.





File Anti-Virus

File Anti-Viru	- 💶 👧 🖺		
	Disinfected	<u>68</u>	
	Quarantined	<u>6676</u>	
	Deleted	<u>4382</u>	
	Access Denied	<u>938</u>	
	Total	12064	
		[<u>Mo</u>	<u>re</u>]

Disinfected – It displays the number of files disinfected by File Anti-Virus module.
Quarantined – It displays the number of files quarantined by File Anti-Virus module.
Deleted - It displays the number of files deleted by File Anti-Virus module.
Access Denied - It displays the number of files to which access was denied by File Anti-Virus module.

Clicking underlined numerical displays action taken on infected files amongst different computers and the group that computer belongs to.

Bie Scan		eScan Managei	nent Console
			06 August 2020
Protection Statistics >> File Anti-Viru	s >> Quarantined		🗮 🔛
Client OS Type All			<u>Print</u>
Machine Name	Status	<u>Group</u>	
1858-001-001-001-001-001	Quarantined (1)	Managed Computers\Escan	
	Close	-	





Clicking the **Status** link further displays the detection date and time, file path, infection description and computer's username.

	Console - Google Chrome		
D Not secure			
4.5	ican	eScan Man	nagement Console
		Tuesda	ay, September 10, 2019
Protection Statistics	s >> File Anti-Virus >> Quarantined (/)		
			Print
Date/Time	File Name	Description	Print User name
	File Name C:\Users\	Description Infected by Virus: EICAR-Test-File (DB)	
06/09/19 13:22:28			<u>User name</u>
06/09/19 13:22:28 06/09/19 13:22:30	C:\Users\	Infected by Virus: EICAR-Test-File (DB)	User name
06/09/19 13:22:28 06/09/19 13:22:30 06/09/19 13:22:31	C:\Users\ C:\Users\	Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	User name
06/09/19 13:22:28 06/09/19 13:22:30 06/09/19 13:22:31 06/09/19 13:22:33	C:/Users/ C:/Users/ C:/Users/	Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	User name
06/09/19 13:22:28 06/09/19 13:22:30 06/09/19 13:22:31 06/09/19 13:22:33 06/09/19 13:22:33	C/Users\ C/Users\ C/Users\ C/Users\	Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	
06/09/19 13:22:28 06/09/19 13:22:30 06/09/19 13:22:31 06/09/19 13:22:33 06/09/19 13:22:33 06/09/19 13:22:33	C/Users/ C/Users/ C/Users/ C/Users/ C/Users/	Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	User name
06/09/19 13:22:28 06/09/19 13:22:30 06/09/19 13:22:31 06/09/19 13:22:33 06/09/19 13:22:33 06/09/19 13:22:34 06/09/19 13:22:38	C:\Users\ C:\Users\ C:\Users\ C:\Users\ C:\Users\ C:\Users\	Infected by Virus: ELCAR-Test-File (DB) Infected by Virus: ELCAR-Test-File (DB)	User name
Date/Time 06/09/19 13:22:28 06/09/19 13:22:30 06/09/19 13:22:31 06/09/19 13:22:33 06/09/19 13:22:33 06/09/19 13:22:34 06/09/19 13:22:38 06/09/19 13:22:39	C/Users/ C/Users/ C/Users/ C/Users/ C/Users/ C/Users/ C/Users/ C/Users/	Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	

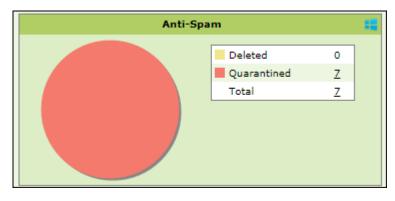
Clicking [More] displays additional protection statistics.

Malware URL Block	<u>12665</u>
Autorun Block	<u>0</u>
Executable Block USB	27548
Executable Block Network	37427
Executable Block User based	380
Proactive Statistics: Allow	<u>0</u>
Proactive Statistics: Block	<u>137</u>
Exploit Statistics Block	<u>6</u>
Ransomware Statistics Block	<u>86</u>
Total	78249



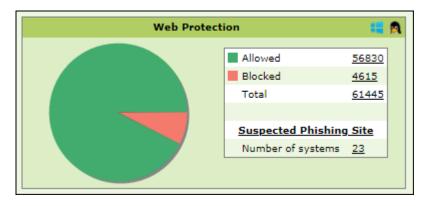


Anti-Spam



Deleted – It displays the number of files deleted by Anti-Spam module. **Quarantined** – It displays the number of files quarantined by Anti-Spam module.

Web Protection



Allowed – It displays the number of websites to which access was allowed by Web Protection module.

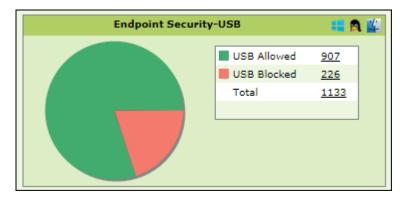
Blocked – It displays the number of websites to which access was blocked by Web Protection module.

Suspected Phishing Site – It displays the number of systems on which suspected phishing sites were blocked. After clicking the numerical, Suspected Phishing Site window appears displaying System Name, Site Status, and Computer Group. Clicking Site Status further displays Date, Time, Website name and action taken.





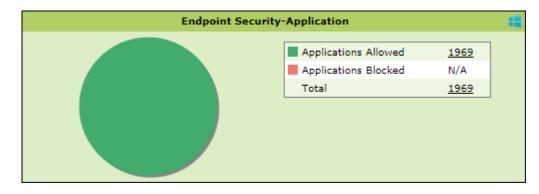
Endpoint Security-USB



USB Allowed – It displays the number of USB access allowed along with the details for the same by Endpoint Security-USB module.

USB Blocked – It displays the number of USB access blocked along with the details for the same by Endpoint Security-USB module.

Endpoint Security-Application



Applications Allowed – It displays the number of applications allowed by Endpoint Security-Application module.

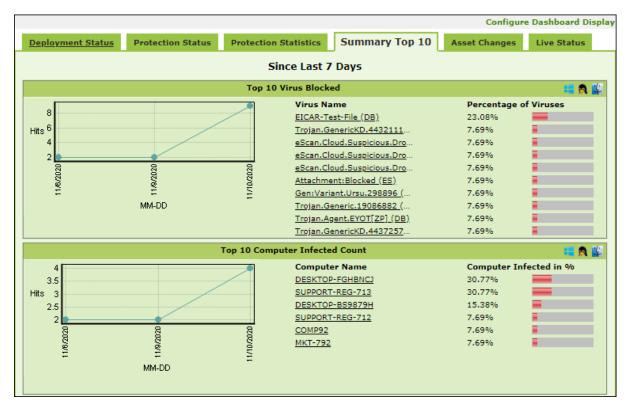
Applications Blocked – It displays the number of applications blocked by Endpoint Security-Application module.





Summary Top 10

This Tab displays top 10 Summary of various actions taken by eScan on all computers since last seven days along with bar chart and graph. This tab can be configured by clicking **Configure Dashboard Display**.



The tab displays the summary for following parameters:

- Top 10 Virus Blocked
- Top 10 Computer Infected Count
- Top 10 USB Blocked Count
- Top 10 Application Blocked Count by Computer Name
- Top 10 Application Allowed Count by Computer Name
- Top 10 Websites Blocked Count by Computer Name
- Top 10 Websites Allowed Count by Computer Name
- Top 10 Infected Emails(Mail AV)
- Top 10 Websites Blocked Count by Username
- Top 10 Websites Allowed Count by Username
- Top 10 Exploit Blocked Count





Asset Changes

This tab displays all hardware and software changes carried out on the endpoints since last seven days.

					Con	figure Dashboard Disp
Deployment Status	Protection Status	Protection Statistics	Summary 7	Тор 10 А	sset Changes	Live Status
		Since Last	7 Days			
		Hardware (Changes			
		Description	Machii	ne Count		
	RAM			0		
	CPU			0		
		ERBOARD		0	_	
	HARD	DISK		1		
		Software 0	hanges			
		Solutione	linges			
		Machine Name	New Installed Softwares	Uninstalled Softwares		
	188.0		2	0		
	18419	11 I	1	2		
	10.1	18	1	2		
			1	0		
		18.	1	1		
		Torrestanter	1	1		
	-8455		2	0	-	
			1			

Clicking the underlined machine names displays softwares installed on the computers since last seven days. Clicking the underlined numerical displays installed / uninstalled softwares on computers since last seven days.





Configure the Dashboard Display

To configure the Dashboard display

1. In the Dashboard screen, at the upper right corner, click **Configure Dashboard Display**. Configure Dashboard Display window appears displaying tabs and their parameters.

	(
Configure Dashboard Display	
Deployment Status	
eScan Status	eScan Version
License Summary	
Protection Status	
Update Status	Scan Status
File Anti-Virus	Proactive
Mail Anti-Virus	🗹 Anti-Spam
FireWall	Mail Anti-Phishing
Web Protection	Web Anti-Phishing
Endpoint Security	Privacy
Anti-Ransomware	
Protection Statistics	
File Anti-Virus	Mail Anti-Virus
🗹 Anti-Spam	Web Protection
Endpoint Security-USB	Endpoint Security-Application
Summary Top 10	
Machine Infected(Real-Time Scan)	USB Blocked
Application Allowed by Computer	Application Blocked by Computer
Website Blocked by Computer	Website Allowed by Computer
Application Blocked by App Name	Application Allowed by App Name
Website Blocked by Sites	Website Allowed by Sites
Website Blocked by Username	Website Allowed by Username
Infected Emails	Spam Emails
Virus Blocked	Exploit Blocked
VITUS BIOCKED	

- 2. Select the parameters' checkboxes to be displayed in the respective tabs.
- 3. Click OK.

The tabs will be updated according to the changes.





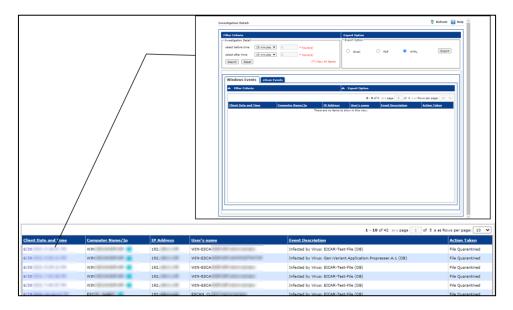




 Filter Criteria 			🔺 Exp	ort Option	
- Filter Criteria					
	VIRUS V	_			
ricei (ide 🗸			
	• v Inclu	ide 💙			
	05/01/2021				
	07/01/2021				
Search Reset					(*) View All Items
	Trojan.G	enericKD.46159122 (E	DB): 7.3%		
	Trojan.G	enericKD.46156042 (D	DB): 4.9%		
	Trojan.Ger	nericKD.46097815 (DE	8): 17.1%	EICAR-Test-File (DB): 43.9%	
	Trojan.Ger	nericKD.46097815 (DE	8): 17.1%	- EICAR-Test-File (DB): 43.9%	
	Trojan.Ger	nericKD.46097815 (DB	8): 17.1%	- EICAR-Test-File (DB): 43.9%	
	Trojan.Ge	nericKD.46097815 (DE	8): 17.1%	EICAR-Test-File (DB): 43.9%	
				C EICAR-Test-File (DB): 43.9%	
		nericKD.46097815 (DE enericKD.46033768 (D		└ EICAR-Test-File (08): 43.9%	
	Trojan.G		28.e 1(90	EICAR-Test-File (DB): 43.9%	
	Trojan.G. Trojan.G.	enericKD.46033768 (D	DB): 9.8%	EICAR-Test-File (DB): 43.9% Gen:Variant.Application.Propresser.A.1 (DB): 2.4%	
	Trojan.G. Trojan.G.	enericKD.46033768 (C enericKD.36774438 (C	DB): 9.8%		5) M Rows per pager 10 V
Client Date and Time	Trojan.G. Trojan.G.	enericKD.46033768 (C enericKD.36774438 (C	DB): 9.8%	Gen:Variant.Application.Propresser.A.1 (DB): 2.4%	S) M Rows per page: 10 V
	Trojan.Gr Trojan.Gr Trojan.Autoruns.Ge	enericKD.46033768 (C enericKD.36774438 (C nericKDS.46106404 (C	5(2); 9,6% 5(2); 9,6% 5(3); 9,6%	Gen:Variant.Application.Propresser.A.1 (DB): 2.4%	
5/3	Trojan.G Trojan.Autoruns.Ger <u>Computer Name/Jo</u>	enericKD.46033768 (C enericKD.36774438 (C nericKD.36106404 (C <u>IP.Address</u>	08); 9.6% (08); 4.9% (08); 9.6%	Gen:Variant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 (+(page 1 of Event.Description	Action Taken
5/3 5/3	Trojan.Gr Trojan.Gr Trojan.Autorum.Ger Computer, Name/Jp WIN WIN WIN WIN	enericKD.46033768 (C enericKD.36774438 (C enericKD.46106404 (C 192, 192, 192, 192, 192, 192, 192, 192,	58): 9.8% 58): 9.8% 98): 9.8% WIN- WIN- WIN-	GeniVariant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 (+ (page 1 of <u>Event Description</u> Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	Action Taken File Quarantined File Quarantined File Quarantined
5/3 5/3 5/3	Trojan.Gr Trojan.Gr Trojan.Autarum.Ger WIN WIN WIN WIN WIN	enericKD.46033768 (C enericKD.36774438 (C IP.Address 192. 192. 192.	08): 9.8% 08): 9.8% User's name WIN- WIN- WIN- WIN- WIN-	GeniVariant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 /+ (page 1 of <u>Event Description</u> Infected by Virus: GeniVariant.Application.Propresser.A.1 (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	Action Taken File Quarantined File Quarantined File Quarantined File Quarantined
5/3 5/3 5/3 5/3	Trojan.G Trojan.G Trojan.Autorum.Ger WIN WIN WIN WIN WIN WIN	enerickD.46033768 (C enerickD.36774438 (C lenerickD5.46106404 (C lp2. 192. 192. 192. 192. 192.	DB): 9.8% DB): 9.8% DB): 9.8% DB): 9.8% VIN- WIN- WIN- WIN- WIN- WIN-	Gen:Variant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 int (page 1 of Exem.Description Infected by Virus: EICAR-Test-File (DB)	Action Taken File Quarantined File Quarantined File Quarantined File Quarantined File Quarantined
/3 /3 /3 /3 /3 /2	Trejan.G Trejan.Autoruna.Ger Computer Name/In WIN WIN WIN WIN WIN WIN WIN WIN WIN WIN	enericKD.46033769 (C enericKD.36774438 (C 12.46106404 (C 192. 192. 192. 192. 192. 192. 192. 192.	58): 9.8% 58): 9.8% 58): 9.8% 580: 5.8% 580: 5.8% 580: 580: 580: 580: 580: 580: 580: 580:	Gen:Variant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 H (page 1 of <u>Svent Description</u> Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	Action Taken File Quarantined File Quarantined File Quarantined File Quarantined File Quarantined File Quarantined
V3 V3 V3 V3 V3 V2 V2 V2	Trejan.Gr Trejan.Autorum.der Computer, Name/Ip WIN WIN WIN WIN WIN WIN WIN WIN	enericKD.46033768 (C enericKD.36774438 (C terricKD5.46106404 (C 192. 192. 192. 192. 192. 192. 192. 192.	bb): 9.8% Jb): 5.8% VIN- WIN-	GeniVariant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 H (page 1 of Exent Description Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	Action Taken File Quarantined File Quarantined File Quarantined File Quarantined File Quarantined Access Denied
93 93 93 93 93 94 94 94 94 94 94 94 94 94 94 94 94 94	Trejan.Gr Trejan.Ar Trejan.Autoruns.Ger WIN WIN WIN WIN WIN ESC ESC ESC	enericKD.46033768 (C enericKD.36774438 (C enericKD.36774438 (C 192. 192. 192. 192. 192. 192. 192. 192.	bb): 9.8% Vset's name WIN- WI	GeniVariant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 /+(/ page 1 of Keent.Description Infected by Virus: ECDA.Test-File (DB) Infected by Virus: Teipan.Autoruns.GenericKDS.46106404 (DB) Infected by Virus: Trojan.Autoruns.GenericKDS.46106404 (DB)	Action Taken File Quarantined File Quarantined File Quarantined File Quarantined File Quarantined Access Danied File Deleted
Client Date and Time 5/2 5/2 5/2 5/2 5/2 5/2 5/2 5/2 5/2 5/2	Trejan.Gr Trejan.Autorum.der Computer, Name/Ip WIN WIN WIN WIN WIN WIN WIN WIN	enericKD.46033768 (C enericKD.36774438 (C terricKD5.46106404 (C 192. 192. 192. 192. 192. 192. 192. 192.	bb): 9.8% Jb): 5.8% VIN- WIN-	GeniVariant.Application.Propresser.A.1 (DB): 2.4% 1 - 10 of 41 H (page 1 of Exent Description Infected by Virus: EICAR-Test-File (DB) Infected by Virus: EICAR-Test-File (DB)	Action Taken File Quarantined File Quarantined File Quarantined File Quarantined File Quarantined Access Denied

For example, the following figure gives the summary of the virus report:

To get the detailed investigation report for a specific incident, click the hyperlink under **Client Date and Time**, as shown below:



The detailed report will be generated.





Windows Events	eScan Events Netwo	rk Incidents			
▲ Filter Criteria			🔺 Export Opt	ion	
				1 - 2 of 2 () page 1 of 1) Rows per	r page: 100 🗸
Client Date and Time	Computer Name/Ip	IP Address	<u>User's name</u>	Event Description	Action Taken
07/05/2021 10:34:17	WIN EDEMNISTING R	192.000.000	W1 R\Administrator	A logon was attempted using explicit credentials	Logged
07/05/2021 10:34:15	WIN COLONNOLT I R	192.000.000	WI R\Administrator	A logon was attempted using explicit credentials	Logged
				·	,

Windows Events: It displays the Windows event for the filtered time frame.

eScan Events: It displays the eScan events for the filtered time frame.

Network Incident: It displays the Network Incident events for the filtered time frame.





Managed Computers

To secure, manage, and monitor computers, it is necessary to add them in a group. The **Managed Computers** module lets you create computer groups, add computers to a group, define policy templates for the created groups and computers.

Based on the departments, user roles and designations, you can create multiple groups and assign them different policies. This lets you secure and manage computers in a better way.

In the navigation panel, click **Managed Computers**. The Managed Computers screen appears on the right pane.

Search Dydate Agent	
Ne gearch Till obgare utdent	
The Astron Market Bit of the Astron Market The Parket Translation	
Action List Client Action List Policy Templates	
Name Send Client Setup Link	
Policy	
Client Computers	
Group Information	
Total Subgroups	
Total Computers	
1 4 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
a second and a second	
E LA RECENT	
and the second sec	
The second	

The screen consists of following buttons:

- Search
- Update Agent
- Action List
- Client Action List
- Policy Templates





_

Search

The Search feature lets you find any computer added in Managed Computers. After clicking **Search**, Search for Computers window appears.

5	Search for Computers								[👔 Help
[- Filter									
	Computer Name / IP:									
	User's name:									
		Find Now								
Γ	Client Action List 🗸									
	Chent Action List +		1							
	Computer Name Groups	<u>IP Address</u>	User name	eScan Status	Version	Last Connection	Installed Directory			
								inere are no	items to show	in this v

The Filter section displays following fields:

Computer Name/IP

Enter a computer name or IP address.

Username

Enter a username.

Click **Find Now**. The console will display the result.





Update Agent

eScan lets you use a client computer as an update agent to deploy updates on groups of computers. By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, if you want to reduce server's workload, you can create an Update Agent for the respective group(s). The Update Agent will receive virus definitions and policies from server and distribute it to the assigned group(s). For more details, please see <u>eScan Update Agents</u>. In Managed Computers screen, clicking **Update Agent** displays a list of computers that are acting as

Update Agents for other computers in the group. The window also lets you Add or Remove Update Agents from this list. You can set an Update Agent for multiple groups.

Adding an Update Agent

To add an Update Agent, follow the steps given below:

1. In Managed computers screen, click Update Agent. Update Agent window appears.

Update Agent		ے Help
-Select Group Name and Update Age		
Update Agent:		
Group Name:		
		Add
Update Agent	IP Address Assigned to Group(s)	

2. Click icon next to Update Agent field, to select the computer. Select Computer window appears.

		×		
Select Computer	*	🝸 Help		
e- Gamaged Computers	S			
	Ok	Cancel		
* Note: Update Agent cannot be set if Hostname exceed 15 characters.				





- 3. Select a computer and click **OK.**
- 4. Click mext to Group Name field, to select the Group Name. This is the group to which the selected computer will act as an Update Agent and provide updates.
- 5. Select the Group and click **OK.**
- Click Add. The Update Agent will be set for the selected group.

Delete an Update Agent

To delete an Update Agent, follow the steps given below:

1. In Managed computers screen, click **Update Agent**. Update Agent window appears.

Select Group Name and Upda	ate Agent		
Update Agent:			
Group Name:			
		ſ	Add
Update Agent	IP Address	Assigned to Group(s)	
		Managed Community Structure 🖨	
	120120-000	Managed Computers\Laptop 💼	

- In the Assigned to Group(s) column, click .
 A confirmation prompt appears.
- 3. Click **OK**. The Update Agent will be deleted.





Action List

The Action List takes you action for a group. The drop-down contains following options:

- New Subgroup
- Remove a Group
- Create Client Setup 🥌
- Properties

New Subgroup

To create a group, follow the steps given below:

1. Click **Action List** > **New Subgroup**.

Creating New Group window appears.

			×
c	creating New Group		🝸 Help
	Create New Group		
	New Group Name :		
	Group Type :	Normal User	•
	Policy Templates :	Group Default Policy	•
[Ok Cance	I	

- 2. Enter a name for the group.
- 3. Click the Policy Templates drop-down and select a policy for the group.

4. Click OK.

A new group will be created under the Managed Computers.





Removing a Group

To remove a group, follow the steps given below:

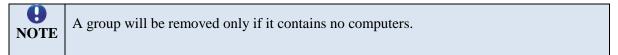
- 1. Select a group.
- 2. Click Action List > Remove Group.

A confirmation prompt appears.

×
Remove Group
Do you really want to remove the group "Sample Group" ?
Ok Cancel

3. Click **OK**.

The group will be removed.



Create Client Setup

To create a Client setup, follow the steps given below:

- 1. In the Managed Computers folder tree, select a group.
- 2. Click Action List > Create Client Setup.

Create Client Setup window appears.

	×
Create Client Setup	🝸 Help
Setup for	
Vindows	Linux/MAC
Setup Settings	
Add Policy	
Auto add to group	
Create Setup Cancel	

- 2. Select the necessary settings.
- 3. Click **Create Setup**. The Client setup will be created and a download link will be displayed in right pane.





Name	Download Client Setup 前	
Policy		
🔯 Group Tasks		
🗊 Client Computers		
Group Information		
		Not Configured
Total Subgroups		1
Total Computers		3

Properties of a group

To view the properties of a group, follow the steps given below:

- 1. Select a group.
- 2. Click Action List > Properties.

Properties window appears.

Properties (Managed Computers)	👔 Hel	P
General		
Name :	Managed Computers	1
Parent Group :		I
Group Type :	Normal User 🗸	I
Contains :	54 Groups , 124 Computers	I
Created :	03/23/2015 10:37:25 PM	I
		I
		I

In Properties, General tab displays following details:

- Group Name
- Parent Group
- Contains Sub Groups or Number of Computers in that Group
- Creation date of the Group





Assigning a Policy to the group

To assign a Policy to the group, follow the steps given below:

- 1. In the Managed Computers folder tree, select a group.
 - 2. Under the group name, click **Policy**. Policy pane appears on the right side.

Managed Computers					
Search Opdate Agent					
Action List V Client Action List V Policy Te	mplates				
🗄 🔚 Managed Computers					
	Policy				
🗄 🔚 Linux / Mac	Select Template				
🗄 💼 Sup Laptop					
⊞ 🛅 Account	Assigned Template				
	pune				
🗄 💼 Cloud Server eScan					
🗄 · 🧰 VM Lab					
HR Dept					





3. To assign a Policy Template to group, click Select Template. New policy window appears.

w Policy	👔 н
Policy Template Selection	
Group Default Policy QA SAMPLES	^
	*
Select Cancel	

- 4. Select a policy template and then click **Select**.
- 5. To assign criteria to group, click **Select Criteria**. Select Policy Criteria window appears.

Select Policy Criteria	김 Help
Set this criteria as a default criteria in case of conflict	
Policy Template Selection	
Group Default Policy	
Criteria Template Selection	
deme	
·	
Select Cancel	

- If a computer falls under both conditions created by you, it will create a conflict. To avoid such conflict, select the checkbox Set this criteria as a default criteria in case of conflict. Then select the Policy Template and Criteria Template to be used in case of conflict.
- 7. Click **Select**. The default Policy Template and Criteria Template for group will be saved and updated.





Client Action List

Client Action List lets you take action for specific computer(s) in a group. To enable this button, select computer(s) and then click **Client Action List**. The drop-down consists of following options:

- Move to Group
- Remove from Group
- Refresh Client
- Show Critical Events
- Export
- Show Installed Softwares
- Forensic/Port Communication
- Create OTP
- Properties

The Client Action List contains few options similar to Action List. These options perform same, except they perform the action only for selected computer(s).





Move to Group

To move computers from one group to other, follow the steps given below:

- 1. Go to **Managed Computers**.
- 2. Select the desired computers present in a group.
- 3. Click **Client Action List** > **Move to Group.**
- 4. Select the group in the tree to which you wish to move the selected computers and click **OK**. The computers will be moved to the selected group.

Remove from Group

To remove computers from a group, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the desired computers for removal.
- 3. Click Client Action List > Remove from Group. A confirmation prompt appears.
- 4. Click **OK**. The computers will be removed from the group.

Refresh Client

To refresh status of any client computer, follow the steps given below:

- 1. Under any group, click Client Computers. A list of computers appears on the right pane.
- 2. Select a computer.
- 3. Click Refresh Client. The Client will be refreshed.

Show Critical Events

To show critical events of specific computer, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the client computer which you want to assign policy template.
- 3. Click Client Action List > Show Critical Events.

This will display the list of all the critical events of the computer that can also be exported as a report.

Export

To export a client computer's data, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**. The right pane displays the list of computers in the group and their detailed information.





Managed Computers						
P Search						
Action List 🔻 📋 Client Action List 🔻 💕 Policy	/ Te	emplates				
The second	•	Name		Send Client Setup Link		
A Party .		Policy				
A STATUTE CONTRACTOR OF A STATUTE OF A STATU		Client	Computers			
10 (and) (1000 / 7800)						
TE Last Test Laster		Group Infe				
iti 💶 (deserti)		Total Subg	groups			
III - III IIIIIIII		Total Com	puters			
12						
10 1 4 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1						
10						
HE LOUD FRANKL						
H and a sec other to						
ill all hadden						
HE LOUIS FRANKLIK (1991						
10						
10 and 10 million						
10 (
101 and 100 million						
HE LAND PROVIDENCE	•					

 Select a client computer and the click Client Action List > Export. Export Selected Columns window appears displaying export options and a variety of columns to be exported.

Export Selected Columns				🕜 Help
Export Option				
Excel		O PDF		
Select All Columns				
Computer Name	IP Address	✓ IP Address of the connection	✓ Mac Address	
🗹 User name	Local Administrator User(s)	eScan Status	Version	
Last Connection	Installed Directory	Monitor Status	🗹 Anti-Spam	
Mail Anti-Virus	Web Protection	Endpoint Security	Firewall	
🗹 Last Update	Update Server	Client OS	Status	
Last Policy Applied	Last Policy Applied Time	Last eBackup Status		
Export Cancel				

- 3. Select the preferred export option.
- 4. Select the preferred report columns.
- 5. Click Export.

The report will be exported as per your preferences.

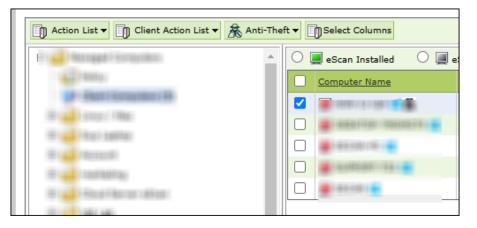




Show Installed Softwares

This feature displays a list of installed softwares on a computer. To view the list of installed softwares, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**. The right pane displays the list of computers in the group and their detailed information.



2. Select a client computer and then click **Client Action List** > **Show Installed Softwares**. Installed Softwares window appears displaying list of installed softwares and in the top right corner displays total number of installed softwares.

I	stalled Softwares	🝸 Help
C	Computer Name:	Total No.Of Installed Programs: 65
	Currently Installed Programs	
	Active Directory Authentication Library for SQL Server	
	Adobe Reader XI (11.0.10)	
	Advanced IP Scanner 2.5	
	AnyDesk	
	Apple Application Support (32-bit)	
	Apple Application Support (64-bit)	
	Apple Mobile Device Support	
	Apple Software Update	
	Bonjour	
	Canon CAPT Print Monitor 1.51	





Create OTP

The password protection restricts user access from violating a security policy deployed in a network. For example, the administrator has deployed a security policy to block all USB devices, but a user needs USB access for a genuine reason. In such situation, One Time Password (OTP) can be generated for that disables USB block policy on specific computer. The administrator can define policy disable duration ranging from 10 minutes to an hour without violating existing policy.

Generating an OTP

To generate an OTP, follow the steps given below:

- 1. In the **Managed Computers** screen, select the client computer for which you want to generate the OTP.
- 2. Click Client Action List > Create OTP. Password Generator window appears.

Computer Name:*	WIN-11-QA	
Valid for:*	10 mins 🗸	
Select Option		
🗌 File Anti-Virus 📒 👰 🎉	Allow to Change Ip	
🗌 Web Protection 📒 👰	🗌 Firewall	
EPS App Control	🗆 EPS USB 💶 👧 🎬	
🗌 Mail Anti-Virus & Anti-Spam 👯		
New Password		
Password :	B	

- 3. In the Valid for drop-down, select the preferred duration to bypass the protection module.
- 4. In Select Option section, select the module you want to disable.



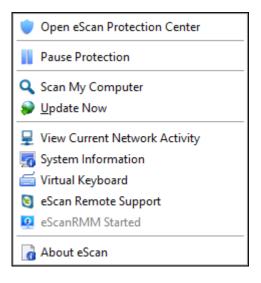


5. Click Generate Password. An OTP will be generated and displayed in Password field.

Entering an OTP

To enter an OTP, follow the steps given below:

1. In the Taskbar, right-click the eScan icon \clubsuit . An option list appears.



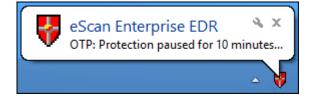
2. Click Pause Protection. eScan Protection Center window appears.

	×
K	eScan Protection Center
Enter eScan Administrator Password	
•••••	
Duration	
15 minutes 🗸 🗸	
	OK Cancel

3. Enter the OTP in the field.

4. Click OK.

The selected module will be disabled for set duration.







Properties of Selected Computer

To view the properties of a selected computer, follow the steps given below:

- 1. Select a computer.
- 2. Click Client Action List > Properties. Properties window appears displaying details.

	×
Properties	👔 Help
AND DO TO THE	
General	
Computer Name	
IP Address	
User name	
Operating System	Minister 1 Minister
AV-Status	
Anti-Virus Installed	eScan installation aborted
Version	14.0.1400.
Installed Directory	C:\Program Files (x86)\eScan\
Update Server	
Last Update	2019/09/18 09:31
Protection	
File Anti-Virus	Enabled
Mail Anti-Virus	Disabled
Anti-Spam	Disabled
Web Protection	Disabled
Firewall	Disabled (Allow All)
Endpoint Security	Enabled



If multiple computers are selected, the Properties option will be disabled.





Understanding the eScan Client Protection Status

Protected	This status is displayed when the File anti-virus module of eScan Client is enabled and eScan was updated in last 2 days.
Not Installed / Critical	This status is displayed when either eScan is not installed on any computer or File AV/Real Time Protection is disabled.
Unknown status	This status is displayed when communication is broken between Server and Client due to unknown reason.
🔅 Update Agent	This status is displayed when a computer is defined as an Update Agent for the group.
Two-FA	This status is displayed when a computer is added to 2FA license.
🖀 DLP	This status is displayed when a computer is added to DLP license.
Ebackup	This status is displayed when a computer is added to eBackup license.
C Anti-Theft	This status is displayed when a computer is added to Anti-Theft Portal.





Anti-Theft

The Anti-Theft module lets you remotely locate and lock a device. This module also lets you wipe data available on a device.

🛚 Action List 🔻 🛐 Client Action List 🔻 🏂 Anti-The			Select Columns	
i 🖬 Haragad i Kerapikan		0 [💻 eScan Installed	0 🔳 e
And Patrice			Computer Name	
AP- SHOT I REPAIRING THE				
HE LAND & HEARING & FRANK			-	
The second second				
A Long Procession				
and a second second				
History Had Florest Affect			100001	
and the second second			_	

Anti-Theft Options

To add computers in an Anti-theft, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the desired computers to add in Anti-theft Portal.
- 3. Click Anti-Theft > Anti-Theft Options.
- 4. Enter the **Email ID** then Click **OK**.

The computer will add in Anti-Theft Portal.

Anti-Theft	
Following is Email Id which will be use to Enable Anti-Theft on client Computer, If you want you can change Email Id. Email ID :	
Ok Cancel	

5. A confirmation prompt appears.



6. Click **OK**. This will redirect to Anti-Theft options.





VALUENTELLISENTE	Device Lost I	Reset Configure Data wipe			
My eScan					-
Locate Locate View Details O					
Action Features					-
Lock	Scream	A	Alert	Data wipe	
Lock View Details Э		Scream View Details �	Alert View Details ≎		a wipe Details ⊖

Anti-Theft Portal

1. It will display the anti-theft features that you can activate in case your system is lost or stolen.

WALTERNALT-THERE WE		Device Lost R	teset Configure Data wipe				
My eScan							-
Locate	9						
Locate View Detail	s O						
Action Features							-
Lock		Scream	A	Alert	A	Data wipe	
Lock View Detail	s⊖		Scream View Details 🕄		Alert View Details ⊙	Data View De	

2. In case of loss or theft, click on the system name that has been lost or stolen, the status bar under it will display the system name again and when it was last seen.





3. Click **Device Lost** and this will allow you to enable the features locate, screenshot and take photo by selecting the desired options.

NUDHALU JOHA	•	Device Lost	Reset	Configure Data wipe	
ly eScan					-
Locate	0				

4. Click **Confirm** to confirm that your system has been lost and to execute the commands Locate, Screenshot, and Camera.

Set Device as lost	×
If you set your device as stolen, below command will be sent to the device.	
	lose

- Locate: This option will allow you to locate the system in case of loss/theft. Click on the Locate option on the anti-theft portal and the last known location of the system will be displayed on the map. Procedure to Locate the system:
 - A. Click **Locate**, the status will change to **Request Pending**; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to locate the system is in progress.
 - B. View Details displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.
- Screenshot: This option will take a screen shot of the system whenever it is synced to the server.
 - A. Click **Screenshot**, the status will change to **Request Pending**; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a screenshot is in progress.





- B. **View Details** displays the last two screenshots from the successful execution of the screenshot command.
- **Take Photo**: This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the camera option on the anti-theft portal.
 - A. Click **Camera**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a snapshot is in progress.
 - B. View Details displays the last two snapshots taken from your system. Click Reset to reset the Action Features on the system; these actions can be performed on the system when it has been lost or stolen.



There are following action features:

- Lock: The Lock feature will block the system from any further access. You will have to unblock the system by entering the pin provided on the anti-theft portal. On the anti-theft portal, select your System Alias name and then click Lock to remotely block your system, to unblock your system you will have to enter the Secret Code provided at the time of executing the lock command.
- Scream: Scream will allow you to raise a loud alarm on the system; this will allow you to trace the system if it is in the vicinity. Click Scream option to remotely raise a loud alarm on your system.
- Alert: This option will allow you to send an alert message (up to 200 characters) to the lost system. This alert message will be displayed on the screen; you can write and send any message for example: Request a call back or send your address or any kind of message to the current holder of your system. With this option there will be higher chance of your lost system being returned. Click **Alert** option to remotely send a message to your lost system. Type in your message in the send message section and click confirm.
- **Data wipe**: The Data wipe feature will delete all the selected files and folders that have been added to the list to be deleted from the portal. Click data wipe option to remotely wipe all the selected files and folders or only delete the cookies and click confirm. Select the **Delete Cookies** checkbox to delete cookies or select the **Datawipe** checkbox to wipe the data and click on **Confirm**.

Disable Anti-Theft

To Disable Anti-Theft, follow the steps given below:

1. Go to Managed Computers.

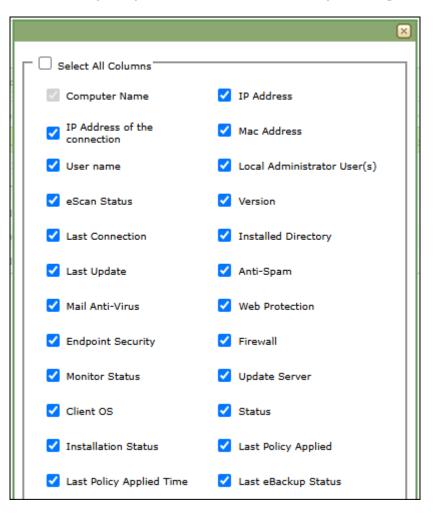




- 2. Select the desired computers in Anti-theft Portal.
- 3. Click **Anti-Theft** > **Disable Anti-Theft**.

Select Columns

You can customize the view regarding the details of devices, according to the requirement.



To configure this, select the computer and click **Select/Add Columns** option. You can select and configure the required columns accordingly.





Policy Template

This button allows you to add different security baseline policies for specific computer or group.

Managing Policies

With the policies you can define rule sets for all modules of eScan client to be implemented on the **Managed Computer** groups. The security policies can be implemented for Windows, Mac, and Linux computers connected to the network.

Defining Policies for Windows Computers

On Windows OS policies can be defined for following eScan Client modules:

File Anti-virus

The File Anti-Virus module scans all the existing files and folders for any infection. It also lets you report/disinfect/quarantine/delete infected objects. Moreover, it saves a copy of the report file for future reference, and displays attention messages. To learn more, <u>click here</u>.

Mail Anti-Virus

The Mail Anti-Virus module scans all the incoming emails. It scans the emails by breaking them into three sections the header, the subject and the body. After scanning, the module combines the sections and sends it to your mailbox. To learn more, <u>click here</u>.

Anti-Spam

The Anti-Spam module blocks spam emails by checking the content of outgoing and incoming mails and quarantines advertisement emails. To learn more, <u>click here</u>.

Web Protection

The Web Protection module lets you block websites. You can allow/block websites with time-based access restrictions. To learn more, <u>click here</u>.

Firewall

The Firewall module lets you put up a restriction on incoming and outgoing traffic and hacking. You can define the firewall settings here. You can define the IP range, permitted applications, trusted MAC addresses, and local IP addresses. To learn more, <u>click here</u>.

Endpoint Security

The Endpoint Security module monitors the application on client computers. It allows/ restricts USB, Block lists, White lists, and defines time restrictions for applications. To learn more, <u>click here</u>.

Privacy Control

The Privacy Control module lets you schedule an auto-erase of your cache, ActiveX, cookies, plugins, and history. You can also securely delete your files and folders, where the files will be deleted directly without any traces. To learn more, <u>click here</u>.

Administrator Password

Administrator Password lets you create and change a password for administrative login to the eScan protection center and Two-Factor Authentication. To learn more, <u>click here</u>.

ODS/Schedule Scan

ODS/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. To learn more, <u>click here</u>.

MWL Inclusion List

The inclusion list contains the names of all executable files which will bind itself to MWTSP.DLL. All other files are excluded. To learn more, <u>click here</u>.

MWL Exclusion List





MWL Exclusion List contains the name of all executable files which will not bind itself to MWTSP.DLL. To learn more, <u>click here</u>.

Notifications & Events

Notifications & Events allows to allow/restrict the alerts that are send to admin in case of any suspicious activity or events. To learn more, <u>click here</u>.

Schedule Update

Schedule Update policy lets you schedule eScan database updates. To learn more, click here.

Tools

Tools policy let you configure eBackup setting. To learn more, click here.

Defining Policies Mac or Linux computers

You can define policies for the following modules of eScan Client on Mac or Linux OS:

File Anti-Virus 🍛

The File Anti-virus module scans all the existing files and folders for any infection. It also lets you report/disinfect/quarantine/delete infected objects. Moreover, it saves a copy of report file for future reference, and displays attention messages. This option is available for both Linux and Mac computers. To learn more, <u>click here</u>.

Endpoint Security



The Endpoint Security module monitors the application on client computers. It allows/restricts USB, block listing, white listing, and defines time restrictions. This option is available for both Linux and Mac computers. To learn more, <u>click here</u>.

On Demand Scanning



The On Demand Scanning module lets you define the categories to be scanned. For example, you can scan only the mails or archives as per your requirement. This option is available for both Linux and Mac computers. To learn more, <u>click here</u>.

Schedule Scan



The Schedule Scan module lets you schedule the scan on the basis of time, what you want to scan and what action to be taken in case of a virus and what you want to be excluded while scanning. For example, you can create a schedule to scan the mails, sub directories and archives on a daily basis and also define the action that needs to be taken in case a virus is found; you can also exclude the scan by mask or files or folders. This option is available for both Linux and Mac computers. To learn more, **click here**.



The Schedule Update module lets you schedule updates for Linux Agents. To learn more, click here.

Administrator Password

The Administrator Password module for Linux lets you create and change password for administrative login of eScan protection center. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password.

It lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password. To learn more, <u>click here</u>.





Web Protection

The Web Protection module for Linux feature is extremely beneficial to parents as it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours. To learn more, <u>click here</u>.

Network Security

Network Security module helps to set Firewall to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. Enabling this features will prevents Zero-day attacks and all other cyber threats. To learn more, <u>click here</u>.



Priority will be given to Policy assigned through **Policy Criteria** first, then the policy given to a specific computer and lastly given to policy assigned to the group to which the computer belongs.





Creating Policy Template for a group/specific computer

To create a Policy template for a group, follow the steps given below:

- 1. Click Managed Computers.
- 2. Select the desired group and then click **Policy Template**. Policy Template window appears.

olicy Templates				💲 Refrest	n 🔋 Help
New Template	Properties 📄 Delete 📑 Assign	to Group(s) Assign to Comput	er(s) Copy Template		
Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)	^
	Mar 22 2023 05:23:03 PM	Jun 18 2024 02:30:28 PM			
	Jul 30 2024 01:31:47 PM	Jul 30 2024 02:04:09 PM	Trail		
	Aug 08 2023 04:45:49 PM	Jan 04 2024 03:53:59 PM			
	Jan 25 2022 12:50:52 PM	Mar 02 2023 11:22:28 AM	poc demo		
	Jan 23 2024 12:58:05 PM	Jan 23 2024 12:58:05 PM		ALTERNATION AND	
	Jan 24 2024 12:54:29 PM	Jan 31 2024 07:58:38 PM			

3. Click New Template. New Templates screen appears displaying modules for Windows, Linux, and Mac computers.

Sets			
nter Template Name:*			
File Anti-Virus	Ŧ	Edit	Mail Anti-Virus Edit Assign From Select Policy
Anti-Spam	Ŧ	Edit	Web Protection Edit Assign From Select Policy
FireWall Assign From Select Policy	¥	Edit	EndPoint Security Assign From Select Policy
Privacy Control Assign From Select Policy	Ŧ	Edit	

- 4. Enter a name for Template.
- 5. To edit a module, select it and then click Edit.
- 6. Click Save. The Policy Template will be saved.





Configuring eScan Policies for Windows Computers

Each module of a policy template can be further edited to meet your requirements.

File Anti-Virus

The File Anti-Virus module displays following tabs to configure:

- Objects
- Options
- Blocked Files
- Folder Protection
- File Rights
- TSPM

Objects

The Objects tab lets you configure following options:

Anti-Virus				1
Objects Options	Block Files	Folder Protection	File Rights	TSPM
Actions in case of virus	detection			
Report only				
Disinfect				
Quarantine obje	<u>ct</u>			
Delete object				
Scan local remo	vable disk drives			
Scan local hard	<u>disk drives</u>			
Scan network dr				
E. Scan files of following	<u>g types</u>			
Exclude by mask				
🖭 🗹 Not a Virus List				
Exclude Files / F	olders			
E. Scan compound				
Enable code ana				
Default Advanced	Setting	OK	Cancel	

Actions in case of virus detection

This section lists the different actions that File Anti-Virus can perform when it detects virus infection.

Report only

Upon virus detection, eScan will only report the virus and won't take any action.

Disinfect [Default]

Upon virus detection, eScan will disinfect the object. This action has 3 additional options as below:





- Make backup file before disinfection: It allows you to create a backup of an object before its disinfection.
- **Report only:** If disinfection is not possible, eScan will only report the virus infection.
- Quarantine object: If disinfection is not possible, eScan will quarantine the object.
- **Delete object:** If disinfection is impossible, eScan will remove the object from the computer.

Quarantine object

If disinfection is impossible eScan will quarantine the object. By default, the quarantined files are saved in C:\Program Files\eScan\Infected folder. You can select the Make backup file before disinfection option if you would like to make a backup of the files before they are disinfected.

Delete object

If disinfection is impossible, eScan will remove the object from the computer.

Scan local removable disk drives [Default]

Select this option if you want eScan to scan all the local removable drives attached to the computer.

Scan local hard disk drives [Default]

Select this option if you want eScan to scan all the local hard drives installed on the computer.

Scan network drives [Default]

Select this option if you want eScan to scan all the network drives, including mapped folders and drives connected to the computer.

Scan files of following types

Select this option if you want eScan to scan all files, only infectable files, and files by extension (Scan by mask). eScan provides you a list of default files and file types that it scans by extension. You can add more items to this list or remove items as per your requirements by clicking **Add/Delete**.

Exclude by mask [Default]

Select this checkbox if you want File Anti-Virus monitor to exclude all the objects in the Exclude by mask list during real-time monitoring or scanning. You can add/delete a file or a particular file extension by clicking **Add/Delete**.

Not a virus list [Default]

File Anti-Virus is capable of detecting riskware. Riskware refers to software originally not intended to be malicious but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote admin software, to the riskware list in the **Not a virus list** dialog box by clicking **Add/Delete** if you are certain that they are not malicious. The riskware list is empty by default.

Exclude Files/Folders [Default]

Select this checkbox if you want File Anti-Virus to exclude all the listed files, folders, and sub folders while it is monitoring or scanning folders. The files/folders added to this list will be excluded from only real-time scan as well as on demand scan. You can add or delete files/folders from the list of by clicking **Add/Delete**.

Scan compound objects [Default]

Select this checkbox if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected. All the procedures will be followed.

Enable Code Analyzer





Select this checkbox if you want eScan to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. After selection, File Anti-Virus not only scans and detects infected objects, but also checks for suspicious files stored on computer.

Options

The Options tab lets you configure following options:

File Anti-Virus	elp
File Anti-Virus Objects Options Block Files Folder Protection File Rights TSPM Save report file Show pack info in the report Show clean object info in the report Limit size to (KB) (avpM.rpt). Enable Auto backup / Restore Limit file size to (KB) Proactive Behaviour Monitor Display attention messages Enable Malware URL Filter Enable Ransomware Protection 	
Default Advanced Setting OK Cancel]

Save report file [Default]

Select this checkbox if you want eScan to save the reports generated by the File Anti-Virus module. The report file logs information about the scanned files and the action taken by File Anti-Virus when an infected file was found during the scan.

Show pack info in the report [Default]

Select this checkbox if you want File Anti-Virus to add information regarding scanned compressed files, such as .zip and .rar files to the Monvir.log file.

Show clean object info in the report

Select this checkbox if you want File Anti-Virus to add information regarding uninfected files found during a scan operation to the **Monvir.log** file. You can select this option to find out which files are not infected.

Limit size to (Kb) (avpM.rpt)

Select this checkbox if you want File Anti-Virus to limit the size of the **Monvir.log** file and **avpM.rpt** file. To modify the limit, enter the log file size in field.





Enable Auto backup/Restore [Default]

Selecting this checkbox lets you back up the critical files of the Windows® operating system and then automatically restores the clean files when eScan finds an infection in any of the system files that cannot be disinfected. You can configure the following settings:

- **Do not backup files above size (KB) [Default]:** This option lets you prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified.
- **Minimum disk space (MB) [Default]:** The Auto-backup feature will first check for the minimum available space limit defined for a hard disk drive. If the minimum defined space is available then only the Auto-backup feature will work, if not it will stop without notifying. You can allot the Minimum disk space to be checked from this option. By default, the minimum disk space is 500 MB.

Limit file size to (KB) [Default]

This checkbox lets you set a limit size for the objects or files to be scanned. The default value is set to **20480 Kb**.

Proactive Behavior Monitor [Default]

Selecting this checkbox enables File Anti-Virus to monitor the computer for suspicious applications/programs and block them on a real-time basis when they try to execute. Selecting this checkbox enables below options to configure:

• Ask user for action

This option allows user to receive the confirmation prompt before Proactive Behavior Monitor blocks the suspicious application/program. Select **Yes**, to proceed with the blocking of application and **No** to cancel the blocking.

• White List

Whitelisting allows you to select the files from the database that you want to exclude from being blocked. To whitelist a file/folder, click **Whitelist** and then click **Add from DB**.

Display attention messages [Default]

When this option is selected, eScan displays an alert consisting the path and name of the infected object and the action taken by the File Anti-Virus module.

Enable Malware URL Filter

This option lets you enable a Malware URL filter where eScan blocks all URLs that are suspected to be malwares. You can exclude specific websites by whitelisting them from the eScan pop up displayed when you try to access the site.

Enable Ransomware Protection[Default]

This option lets you enable Ransomware Protection on the system where eScan blocks any suspected ransomware activities performed on system. With the technology called PBAE (Proactive Behavior Analysis Engine) eScan monitors the activity of all processes on the local computer and when it encounters any activity or behavior that matches a ransomware, it raises a red flag and blocks the process.





Block Files

The Block Files tab lets you configure settings for preventing executables and files, such as autorun.inf, on network drives, USB drives, and fixed drives from accessing your computer.

	Folder Protection File Rights TSPM
Disable Autoplay on USB and Fix	xed Drives
Deny access of executables o	on USB Drives
User defined whitelist	bbA
<u>File Name</u>	Delete
	RemoveAll
Deny access of executables fr	inen Network
User defined whitelist	I I I I I I I I I I I I I I I I I I I
Folder Name	Include Subfolder Add
	Delete
	RemoveAll
	RemoveAll
	RemoveAll
Deny Access of following files	
 Deny Access of following files Quarantine Access-denied file 	s
_	s es Add
Quarantine Access-denied file	s es Add Delete
Quarantine Access-denied file	s es Add

You can configure the following settings:

Disable AutoPlay on USB and Fixed Drives

Selecting this option will disable AutoPlay when a USB/Fixed Drive is connected.

Deny access of executables on USB Drives

Select this checkbox if you want eScan to prevent executables stored on USB drives from being accessed.

Deny access of executable from Network

Select this checkbox if you want eScan to prevent executables on the client computer from being accessed from the network.

User defined whitelist

This option is enabled after selecting the **Deny access of executable from Network** checkbox. You can use this option to enter the folders that need to be whitelisted so that executables can be accessed in the network from the folders mentioned under this list. To add files, click **Add**.





Add Folder	
C:\Documents and Settings\Remya\My Documents	
🗹 Include Subfolder	
Add Cancel	

Enter the complete path of the folder to be whitelisted on the client systems. You can either whitelist the parent folder only or select the **Include subfolder** option to whitelist the subfolders as well.

Deny Access of following files [Default]

Select this checkbox if you want eScan to prevent the files in the list from running on the computers.

Quarantine Access-denied files

Select this checkbox if you want eScan to quarantine files to which access is denied.

- 1. You can prevent specific files from running on the eScan client computer by adding them to the Block Files list. By default, this list contains the value %sysdir%*.EXE@. Click Add.
- 2. Enter the full name of the file to be blocked from execution on the client systems.





Folder Protection

The Folder Protection tab lets you protect specific folders from being modified or deleted by adding them to the Folder Protection list. It lets you configure the following setting:

le Anti-Virus		👔 Hel		
Objects Options Block File	Folder Protection File Rights TSPM			
Protect files in following folders from modification and deletion				
Folder Name	Include Subfolder	Add Delete RemoveAll		
Default Advanced Setting	OK Cancel			

Protect files in following folders from modification and deletion [Default]

Selecting this checkbox enables File Anti-Virus module to protect files in specific folders from being modified or deleted on the client systems. Click **Add**. Enter the complete path of the folder to be protected on the client systems. You can either protect the parent folder only or select the **Include subfolder** option to protect the subfolders as well.





File Rights

The File Rights tab restricts or allows for remote or local users from modifying folders, subfolders, files or files with certain extensions.

jects	Options	Block Files	Folder Prote	ction Fil	e Rights	TSPM		
	*.EXE							RemoveAll
	*.COM							
Allo	w Modification	for following Fi	es					
	<u>File / Folde</u>	r Name		Inclu	ude Subfolder			Add
	%TEMP%\			V				Delete RemoveAll
	%WINDIR	%\TEMP\		V				
	Enable eScan	Local File Rights					· ·	
		_	the following files					
		users to modify			Include Subfo	<u>der</u>		Add
	not allow local <u>File / Folde</u>	users to modify			Include Subfol	der		Add Delete RemoveAll
Do	not allow local File / Folde	users to modify			Include Subfol	der		Delete
Do	not allow local File / Folde smss.exe csrss.exe	users to modify <u>r Name</u>			Include Subfol	der		Delete
	File / Folde smss.exe csrss.exe winlogon.ex	users to modify <u>r Name</u>	the following files		Include Subfol	<u>der</u>		Delete

Enable eScan Remote File Rights

Select this checkbox to allow/restrict the remote users to make any modifications to the files and folders.

Do not allow remote users to modify the following local files

The files/folders added to this list cannot be modified by the remote users.

Allow modification for following files

The files added to this list can be modified by the remote user.

Enable eScan local file rights

Select this checkbox to allow/restrict the local users to make any modifications to the files/folders.

Do not allow local users to modify the following files

The files/folders added to this list cannot be modified by the local users.

Allow modification for files

The files/folders added to this list can be modified by the local users.





TSPM

eScan's TSPM (Terminal Service Protection Module) detects brute force attacks, identifies suspicious IP addresses/hosts and blocks the access attempts from them to prevent future attacks. The IP addresses and hosts from the attacks are banned from initiating any further connections to the system. It also detects and stops attempts of attackers who try to uninstall security applications from systems and alerts administrators about the preventive measures initiated by TSPM.

File Anti-Virus	褶 Help
Objects Options Block Files Folder Protection File Rights TSPM Enable Terminal Service Protection Module Image: Terminal Service Protection Module Image: Terminal Service Protection Module Image: Terminal Service Protection Module	
WhiteListed IPs	Add Delete
Default Advanced Setting OK Cancel	

Enable Terminal Service Protection Module

Select this checkbox to activate TSPM module.

• Allow only whitelisted IPs: Select this option to allow only whitelisted IPs to connect to the endpoints.

To add a list of IP addresses to be excluded from being blocked by TSPM, click **Add**. Add IP window appears.

	×
Add IP	
IP Address*:	
Ok Cancel	(*) Mandatory Fields





Advanced Settings

Clicking Advanced Settings lets you configure advanced settings for console.

Di	isable Reload Password (2=Disable/1=Enable)	
	sable Keloau Fassword (Z=DISADIE/I=EllADIE)	1 .
Di	isplay Print Job events	1 .
🗌 IP	Address Change Allowed (2=Disable/1=Enable)	1 .
Er	nable Time Syncronization	1 .
🔲 d	lear Quarantine folder after Days specified	28
🔲 d	lear Quarantine Folder after Size Limit specified in MB	0
E>	xclude System PID from Scanning	0 •
Di	isable Virtual Key Board Shortcut key	0 •
Sł	how eScan Tray Menu	1 .
🗌 sł	how eScan Tray Icon	1 .
🗌 sł	how eScan Desktop Protection Icon	1 .
Er	nable eScan Remote Support in Non-Administrator mode	0 •
De	efine Virus Alert Time (in seconds)	20
SI SI	how Malware URL Warning	1 *

Disable Reload Password (2=Disable/1=Enable)

This option lets you enable or disable password for reloading eScan. After enabling, the user will be asked to enter reload password if user attempts to reload eScan. This is the administrator password for eScan Protection Center.

Display Print Job events (1 = Enable/0 = Disable)

This option lets you capture events for the Print Jobs from Managed Computers.

IP Address Change Allowed (2 = Disable/1 = Enable)

This option lets you enable/disable IP Address Change by the user on their computer.

Enable Time Synchronization (1 = Enable/0 = Disable)

This option lets you enable/disable time synchronization with internet. Active internet connection is mandatory for this feature.

Clear Quarantine folder after Days specified

This option lets you specify number of days after which the Quarantine folder should be cleared on Managed Computers.

Clear Quarantine Folder after Size Limit specified in MB

This option lets you specify size limit for the Quarantine folder. If the defined size limit exceeds, the Quarantine folder will be cleared on Managed Computers.

Exclude System PID from Scanning (1 = Enable/0 = Disable)

This option lets you exclude system process ID (Microsoft assigned System PIDs) from scanning on Managed Computers.

Disable Virtual Key Board Shortcut key (1 = Enable/0 = Disable)





This option lets you disable shortcut for using Virtual Keyboard on Managed Computers.

Show eScan Tray Menu (1 = Show/0 = Hide) This option lets you Hide or Show eScan Tray menu on Managed Computers.

Show eScan Tray Icon (1 = Show/0 = Hide) This option lets you hide or show eScan Tray Icon on Managed Computers.

Show eScan Desktop Protection Icon (1 = Show/0 = Hide) This option lets you hide or show eScan Protection icon on Managed Computers.

Enable eScan Remote Support in Non-Administrator mode (1 = Enable/0 = Disable) This option lets you enable/disable eScan Remote Support in Non-Administrator Mode. eScan will not prompt for entering Administrator Password to start eScan Remote Support from Managed Computers.

Define Virus Alert Time (in seconds)

This option lets you define time period in seconds to display Virus Alert on Managed Computers.

Show Malware URL Warning (1 = Show/0 = Hide)

This option lets you show or hide Malware URL warning messages on Managed Computers.

Protect Windows Hosts File (1 = Allow/0 = Block)

Use this option to Allow/Block modifications to Windows Host Files.

Search for HTML Scripts (1 = Allow/0 = Block)

Use this option to Allow/Block search for html script (infection) in files. This option will have impact on system performance.

Show Network Executable block alert (1 = Show/0 = Hide)

This option lets you show/hide Network executable block alerts on Managed Computers.

Show USB Executable Block Alert (1 = Show/0 = Hide)

This option lets you show/hide USB executable block alerts on Managed Computers.

Show eScan Tray Icon on Terminal Client (1 = Show/0 = Hide)

This option lets you show/hide eScan Tray Icon on Terminal Clients on Managed Computers.

Enable eScan Self Protection (1 = Enable/0 = Disable)

This option lets you Enable/Disable eScan Self Protection on Managed Computers, if this feature is enabled, no changes or modifications can be made in any eScan File.

Enable eScan Registry Protection (1 = Enable/0 = Disable)

This option lets you Enable/Disable eScan Registry Protection. User cannot make changes in protected registry entries if it is enabled on Managed Computers.

Enable backup of DLL files (1 = Enable/0 = Disable)

This option lets you Enable/Disable backup of DLL files on Managed Computers.

Integrate Server Service dependency with Real-time monitor (1 = Enable/0 = Disable)

This option lets you Integrate Server Service dependency with real-time monitor.

Send Installed Software Events (1 = Enable/0 = Disable)

This option lets you receive Installed Software Events from Managed Computers.

Enable Cloud (1 = Enable/0 = Disable)

This option lets you Enable/Disable eScan Cloud Security Protection on Managed Computers.





Enable Cloud Scanning (1 = Enable/0 = Disable)

This option lets you Enable/Disable Cloud Scanning on Managed Computers.

Remove LNK (Real-Time) (1 = Enable/0 = Disable)

This option lets you Enable/Disable Removal of LNK on real-time basis.

Whitelisted AutoConfigURL

This option lets you whitelist AutoConfigURLs. Enter comma separated URLs that need to be whitelisted.

Disable Add-ons/Extension blocking (1 = Enable/0 = Disable)

Selecting this option disables Add-ons and Extension blocking.

Include files to scan for archive (Eg: abc*.exe)

This option lets you add file types that needs to be when archive scanning enabled.

Block Date-Time Modification (1 = Enable/0 = Disable)

This option lets you block the modification of the system date and time.

Allow CMD-Registry for Date-Time blocking (Depends upon Block Date-Time Modification) (1 = Enable/0 = Disable)

Selecting this option lets you block date-time modification from the CMD-Registry.

Domain list for exclusion of Host file scanning (e.g. abc.mwti)

Selecting this option lets you add the list of domains to be excluded from host file scanning.

Disable Pause Protection and Open Protection center on Right Click (Set 192 for disable)

This option disables Pause Protection and Open Protection center on Right Click if you set it to 192.

Enable Share Access Control (1 = Enable/0 = Disable)

It enables Share Access Control. Network Shares ReadOnly Access and Network Shares NoAccess options will work only if this option is selected.

Only if it is enabled the setting "NetworkSharesReadOnlyAccess" and "NOTE "NetworkSharesNoAccess" will be referred

List of comma-separated servers and/or shares and/or wildcards which needs to be given NO ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp*.doc or *.doc (Work only when ''Enable Share Access Control'' is set)

Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should not be accessible.

List of comma-separated servers and/or shares and/or wildcards which needs to be given READ ONLY ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp*.doc or *.doc (Work only when "Enable Share Access Control" is set)

Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should be given only view access and not be editable.

Whitelist IP Address (Depends on IP Address Change Allowed) (E.G 192.168.1.* You can put comma-separated list)

Selecting this option lets you add the list of IP addresses separated by commas to whitelist them.

Block Access to Control Panel (1 = Enable/0 = Disable)

Selecting this option lets you block the user from accessing the control panel.





Enable logging of sharing activity from suspected malware system (WSmbFilt.log on client system) (1 = Enable/0 = Disable)

Enabling this option directs eScan to log any sharing activity performed by suspected malware system. By default, this feature is enabled.

Allow Uninstallers (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable use of third party uninstallers.

Block Renaming of Hosts files (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable block Hostname renaming.

Restricted Environment enabled (1 = Enable/0 = Disable) Selecting this option lets you enable/disable restrict environment settings.

Block eternal blue (wannacry) exploits (1 = Enable/0 = Disable) Selecting this option lets you block eternal blue (wannacry) exploits. By default, this option is enabled.

Enable Winsock Protection (Require Restart) (1 = Enable/0 = Disable) This option lets you Enable/Disable protection at the Winsock Layer.

This option lets you Enable/Disable protection at the winsock La

Block Registry Editor (1 = Enable/ 0 = Disable)

This option lets you Enable/Disable block Registry Editor.

Allow RDP (1=Enable/0=Disable) This option lets you Enable/disable RDP.

Block Powershell

This option lets you enable/disable Powershell.





Mail Antivirus

Mail Anti-Virus is a part of the Protection feature of eScan. This module scans all incoming and outgoing emails for viruses, spyware, adware, and other malicious objects. It lets you send virus warnings to client computers on the Mail Anti-Virus activities. By default, Mail Anti-Virus scans only the incoming emails and attachments, but you can configure it to scan outgoing emails and attachments as well. Moreover, it lets you notify the sender or system administrator whenever you receive an infected email or attachment. This page provides you with options for configuring the module.

Start Start Sto	p	
Block Attachmen PRETTY*.EXE NAVI*.EXE KAK.HTA FIX200*.EXE MINE.* TRY*.EXE SUPP*.EXE THE_FLY.* Y2K.EXE	ts Types Add Delete Advanced	Action Disinfect Delete Quarantine Infected Files
Port Settings Port Settings Outgoing Mail Incoming Mail Scan Out	(SMTP)	

Scan Options

This tab lets you select the emails to be scanned and action that should be performed when a security threat is encountered during a scan operation. This tab lets you configure following settings:

Block Attachments Types

This section provides you with a predefined list of file types that are often used by virus writers to embed viruses. Any email attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your requirements. As a best practice, you should avoid deleting the file extensions that are present in the **Block Attachments Types** list by default. You can also configure advanced settings required to scan emails for malicious code.

Action

This section lets you configure the actions to be performed on infected emails. These operations are as follows:





Disinfect [Default]

Select this option if you want Mail Anti-Virus to disinfect infected emails or attachments. **Delete**

Select this option if you want Mail Anti-Virus to delete infected emails or attachments.

Quarantine Infected Files [Default]

Select this option if you want Mail Anti-Virus to quarantine infected emails or attachments. The default path for storing quarantined emails or attachments is –

C:\Program Files\eScan\QUARANT. However, you can specify a different path for storing quarantined files, if required.

Port Settings for email

You can also specify the ports for incoming and outgoing emails so that eScan can scan the emails sent or received through those ports.

Outgoing Mail (SMTP) [Default: 25] You need to specify a port number for SMTP.

Incoming Mail (POP3) [Default: 110] You need to specify a port number for POP3.

Scan Outgoing Mails Select this option if you want Mail Anti-Virus to scan outgoing emails as well.





Advanced

Clicking **Advanced** displays Advanced Scan Options dialog box. This dialog box lets you configure the following advanced scanning options:

	×				
Advanced Scan Options					
 Delete all Attachments in eMail if Disinfection is not possible Delete entire eMail if Disinfection is not possible Delete entire eMail if any Virus is found Quarantine Blocked Attachments Delete entire eMail if any Blocked Attchement is found Quarantine eMail if Attachments are not Scanned Quarantine Attachments if they are Scanned Exclude Attchements (White List) 					
Add					
Delete					
Save Cancel					

Delete all Attachments in email if disinfection is not possible

Select this option to delete all the email attachments that cannot be cleaned.

Delete entire email if disinfection is not possible [Default]

Select this option to delete the entire email if any attachment cannot be cleaned.

Delete entire email if any virus is found

Select this option to delete the entire email if any virus is found in the email or the attachment is infected.

Quarantine blocked Attachments [Default]

Select this option to quarantine the attachment if it bears extension blocked by eScan.

Delete entire email if any blocked attachment is found [Default]

Select this option to delete an email if it contains an attachment with an extension type blocked by eScan.

Quarantine email if attachments are not scanned

Select this checkbox to quarantine an entire email if it contains an attachment not scanned by Mail Anti-Virus.

Quarantine Attachments if they are scanned

Select this checkbox if you want eScan to quarantine attachments that are scanned by Mail Anti-Virus.

Exclude Attachments (White List)

This list is empty by default. You can add file names and file extensions that should not be blocked by eScan. You can also configure eScan to allow specific files even though if the file type is blocked. For example, if you have listed *.PIF in the list of blocked attachments and you need to allow an attachment with the name ABC, you can add abcd.pif to the Exclude Attachments list. Add D.PIFing *.PIF files in this section will allow all *.PIF to be delivered. MicroWorld recommends you to add the entire file name like ABCD.PIF.





Anti-Spam

Anti-Spam module filters junk and spam emails and sends content warnings to specified recipients. Here you can configure the following settings:

dvance		
1	Send Original Mail to User	
	Do not check content of Replied or Forwarded Mails	
	Check Content of Outgoing mails	Phrases
	Spam Filter Configuration	
1	Check for Mail Phishing	
1	Treat Mails with Chinese/Korean character set as SPAM	
-	Treat Subject with more than 5 whitespaces as SPAM	
1	Check content of HTML mails	
1	Quarantine Advertisement mails	Advanced
	Mail Tagging Options	
\bigcirc	Do not change email at all.	
	Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is in Body.	s embeddeo
\bigcirc	"X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.	
۲	Only [Spam] tag is added in Subject. Body is left unchanged.	
\bigcirc	"X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.	

Advanced

This section provides you with options for configuring the general email options, spam filter configuration, and tagging emails in Anti-Spam.

Send Original Mail to User [Default]

This checkbox is selected by default. eScan delivers spam mail to your inbox with a spam tag. When an email is tagged as SPAM, it is moved to this folder. Select this checkbox, if you want to send original email tagged as spam to the recipient as well.

Do not check content of Replied or Forwarded Mails

Select this checkbox, if you want to ensure that eScan does not check the contents of emails that you have either replied or forwarded to other recipients.

Check Content of Outgoing mails

Select this checkbox, if you want Anti-Spam to check outgoing emails for restricted content.





Phrases

Click **Phrases** to open the **Phrases to Check** dialog box. This dialog box lets you configure additional email related options. In addition, it lets you specify a list of words that the user can either allow or block.

User specified whitelist of words/phrases (Color Code: GREEN)

This option indicates the list of words or phrases that are present in the whitelist. A phrase added to the whitelist cannot be edited, enabled, or disabled.

User specified List of Blocked words/phrases: (Color Code: RED)

This option indicates the list of words or phrases that are defined in block list.

User specified words/phrases disabled: (Color Code: GRAY)

This option indicates the list of words or phrases that are defined to be excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

Action List

- Add Phrase: Option to add phrase to quarantine or delete the mail.
- Edit Phrase: To modify existing phrase added in list.
- **Enable Phrase:** By default, it is enabled. After being disabled, you can use this option to enable it.
- Disable Phrase: Disable existing phrase added in list.
- Whitelist: This will allow email to deliver to inbox when phrase is found in the email.
- Block list: This will delete email when it contains the phrase.
- **Delete:** Delete the phrase added in list.

Spam Filter Configuration

This section provides you with options for configuring the spam filter. All options in this section are selected by default.

Check for Mail Phishing [Default]

Select this option if you want Anti-Spam to check for fraudulent emails and quarantine them.

Treat Mails with Chinese/Korean character set as SPAM [Default]

When this option is selected, emails are scanned for Chinese or Korean characters. This check is based on the research data conducted by MicroWorld's various spam email samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their emails.

Treat Subject with more than 5 whitespaces as SPAM [Default]

In its research, MicroWorld found that spam emails usually contain more than five consecutive white spaces. When this option is selected, Anti-Spam checks the spacing between characters or words in the subject line of emails and treats emails with more than five whitespaces in their subject lines as spam emails.

Check content of HTML mails [Default]

Select this option if you want Anti-Spam to scan emails in HTML format along with text content.

Quarantine Advertisement mails [Default]

Select this option if you want Anti-Spam to check for advertisement types of emails and quarantine them.





Advanced

Clicking **Advanced** displays Advanced Spam Filtering Options dialog box. This dialog box lets you configure the following advanced options for controlling spam.

Advanced Spam Filtering Options						
Enable Non Intrusive Learning Pattern (NILP) chee	ck					
Enable eMail Header check						
Enable X-Spam Rules check	C Enable X-Spam Rules check					
Enable Sender Policy Framework (SPF) check						
Enable Spam URI Realtime Blacklist (SURBL) chec						
Enable Real-time Blackhole List (RBL) check						
RBL Servers Add bl.spamcop.net b.barracudacentral.org Remove All	Auto-Spam Whitelist Add *@analytics.bounces.goog *@irctc.co.in *@vm.vonage.com					
Save Cancel						

Enable Non- Intrusive Learning Pattern (NILP) check [Default]

Non-Learning Intrusive Pattern (NILP) is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user.

Enable email Header check [Default]

Select this option if you want to check the validity of certain generic fields likes From, To, and CC in an email and marks it as spam if any of the headers are invalid.

Enable X Spam Rules check [Default]

X Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a particular score. The Spam Rules Check technology matches X Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.

Enable Sender Policy Framework (SPF) check

SPF is a world standard framework adopted by eScan to prevent hackers from forging sender addresses. It acts as a powerful mechanism for controlling phishing mails. Select this checkbox if you want Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.





Enable Spam URI Real-time Blacklist (SURBL) check [Default]

Select this option if you want Anti-Spam to check the URLs in the message body of an email. If the URL is listed in the SURBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.

Enable Real-time Blackhole List (RBL) check

Select this option if you want Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.

RBL Servers

RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.

Auto Spam Whitelist

Unlike normal RBLs, SURBL scans emails for names or URLs of spam websites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid email addresses that can bypass the above Spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

Mail Tagging Options

Anti-Spam also includes some mail tagging options, which are described as follows:

Do not change email at all

Select this option if you want to prevent Anti-Spam from adding the [Spam] tag to emails that have been identified as spam.

Both subject and body are changed: [Spam] tag is added in Subject: Actual spam content is embedded in Body

This option lets you identify spam emails. When you select this option, Anti-Spam adds a [Spam] tag in the subject line and the body of the email that has been identified as spam.

"X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body

This option lets you add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.

Only [Spam] tag is added in Subject: Body is left unchanged [Default]

This option lets you add the [Spam] tag only in the subject of the email, which has been identified as spam.

"X MailScan Spam: 1" header line is added: Body and subject both remain unchanged

This option lets you add a header line to the email. However, it does not add any tag to the subject line or body of the email.





Web Protection

Web Protection module scans the website content for specific words or phrases. It lets you block websites containing pornographic or offensive content. Administrators can use this feature to prevent employees from accessing non-work related websites during preferred duration.

Filtering Options Scanning	Options Define	e Time-Restriction				
Status • Active			 🔘 віс	ock Web Access		
Filter Categories	Allow	Block	Site Names			
Category Name	Type	Status	playboy.com			
Pornography	Block V	Customize				
Gambling	Block V	Customize				
Alcohol	Block V	Customize				
Violence	Block V	Customize				
Drugs	Block V	Customize				
Ratings block category	Block V	Customize				
Add Delete			Add	Delete	Save	
Filtering Options			 1			

You can configure the following settings:

Filtering Options

This tab has predefined categories that help you control access to the Internet.

Status

This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as **Active** or **Block** web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, only **Filtering Options** and **Pop-up Filter** tabs are available.

Filter Categories

This section uses the following color codes for allowed and blocked websites.

Green

It represents an allowed websites category.

Red

It represents a blocked websites category. The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings_block_category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.





Category Name

This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filtering Options

This section includes the **Add sites rejected by the filter to Block category checkbox**. Select this option if you want eScan to add websites that are denied access to the Block category database automatically.

Scanning Options

This tab lets you enable log violations and shutdown program if it violates policies. It also lets you specify ports that need monitoring.

Web Protection	🛐 Help
● Start ○ Stop	Start Phishing Filter Start Malware URL Filter
Filtering Options Scanning Options Define Time-Restriction Actions Image: Construction of the second	Port Setting Internet Access (HTTP Port) 80,8080,3128,6588,4480,88
Default Advanced Setting OK Cancel	

Actions

This section lets you select the actions that eScan should perform when it detects a security violation.

Log Violations [Default]

This checkbox is selected by default. Select this option if you want Web Protection to log all security violations for your future reference.

Shutdown Program in 30 Secs

Select this option if you want Web Protection to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.

Port Setting

This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

Internet Access (HTTP Port)

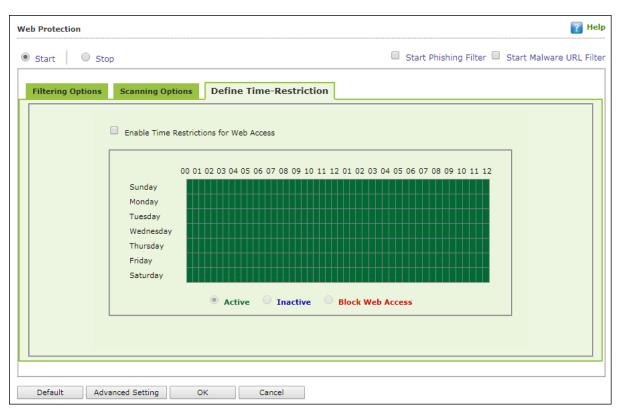
Web browsers commonly use the port numbers 80, 8080, 3128, 6588, 4480, and 88 for accessing the Internet. You can add port numbers to the **Internet Access (HTTP Port)** box to monitor the traffic on those ports.





Define Time Restriction

This section lets you define policies to restrict access to the Internet.



Enable Time Restrictions for Web Access

Select this option if you want to set restrictions on when a user can access the Internet. By default, all the fields appear dimmed. The fields are available only when you select this option.

The time restriction feature is a grid-based module. The grid is divided into columns based on the days of the week vertically and the time interval horizontally.

Active

Click **Active** and select the appropriate grid if you want to keep web access active on certain days for a specific interval.

Inactive

Select this option if you want to keep web access inactive on certain days for a specific interval.

Block Web Access

Select this option if you want to block web access on certain days for a specific interval.

Phishing and Malware URL Filter

Under Web Protection eScan also provides options to enable Phishing and Malware filters which will detect and prevent any phishing attempts on the system and block all malware attacks. To enable the filters, select **Start** and then select the respective checkboxes.

Web Protection	🝸 Help
Start Stop	Start Phishing Filter Start Malware URL Filter





Advanced Setting

Ignore IP address from Web-scanning Select this option to enter IP address form Web-Scanning. **Enable Unknown Browsers detection** Select this option to enable/disable unknown browser detection. Enable allowing of WhiteListed Site during BlockTime Select this option to enable/disable white listed site during block time. **Enable Online Web-Scanning Module** Select this option to enable/disable online web-scanning module. **Disable Web Warning Page** Select this option to enable/disable web warning page. **Enable HTTPS Popup** Select this option to enable/disable HTTPS Popup. Show External Page for Web blocking (Page to be define under External Page) Select this option to enable/disable external page for web blocking. External Page Link for Web blocking (Depends on Show External Page) Select this option to enter external page link for web blocking. Force inclusion of Application into Layer scanning (MW Layer) Select this option to enter Force inclusion of Application into Layer scanning. **Enable HTTP Popup (1 = Enable/0 = Disable)** Select this option to enable/disable HTTP pop-ups. **Ignore Reference of sub-link** Select this option to enable/disable Ignore Reference of sub-link. Allow access to SubDomain for Whitelisted sites (Only HTTP Sites) Select this option to enable/disable access to SubDomain for Whitelisted sites. Allow access to SubDomain for Whitelisted sites (Only HTTPS Sites) Select this option to enable/disable access to SubDomain for Whitelisted sites. Enable logging of visited websites Select this option to enable/disable logging of visited websites. **Block EXE download from HTTP Sites (1 = Enable/0 = Disable)** Select this option to enable/disable block download of .exe files from HTTP websites. **Block HTTP Traffic only on Web Browser** Select these options to enable/disable block HTTP Traffic on Web Browser. Allow website list (Depends on "Block HTTP Traffic only on Web Browser") Select this option to enter to block HTTP Traffic on Web Browser. Block Microsoft EDGE Browser (1 = Enable/0 = Disable) Select this option to enable/disable blocking Microsoft Edge browser. Enable Web Protection using Filter driver (1 = Enable/0 = Disable) Select this option to enable/disable web protection using filter driver. Force Disable Web Protection using Filter driver (1 = Enable/0 = Disable) Select this option to force enable/disable web protection using filter driver. WFP Exclude IP List (1 = Enable/0 = Disable) Select this option to enable/disable excluding IP list from Web Filter Protection.





Firewall

Firewall module is designed to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. Therefore, the Firewall feature first checks the rules, analyzes network packets, and filters them on the basis of the specified rules. When you connect to the Internet, you expose your computer to various security threats.

Fire Wall						
Zone Rule Expert Rule Trusted MAC Address Local IP List Application Rule						
Name	IP Address/Host Name	Туре	Zone			
Allow Local Network 192.168.*.*		IP Range	Trusted			
Add Host Name Add IP Add IP Rang	Add Host Name Add IP Add IP Range Modify Remove					
Image: Show Application Alert Default Rules Advanced Setting OK Cancel						

The Firewall feature of eScan protects your data when you:

- Connect to Internet Relay Chat (IRC) servers and join other people on the numerous channels on the IRC network.
- Use Telnet to connect to a server on the Internet and then execute the commands on the server.
- Use FTP to transfer files from a remote server to your computer.
- Use Network Basic Input Output System (NetBIOS) to communicate with other users on the LAN connected to the Internet.
- Use a computer that is a part of a Virtual Private Network (VPN).
- Use a computer to browse the Internet.
- Use a computer to send or receive email.

By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and **Interactive Filter** to monitor incoming and outgoing traffic. The eScan Firewall also lets you specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. You can configure the following settings to be deployed to the eScan client systems:

Allow All – Clicking **Allow All** disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

Limited Filter – Clicking **Limited Filter** enables eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed or blocked as per the conditions or rules defined in the Firewall.





Interactive Filter – Clicking **Interactive Filter** enables eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Following tabs are available:

- Zone Rule
- Expert Rule
- Trusted MAC Address
- Local IP List
- Application Rule

Ignore Zone Rules & Local IP List – This option allows you to override the Zone Rule configuration that has whitelisted IP ranges. It also overrides the Local IP list that consists of trusted local IP addresses. By selecting this checkbox, all the IP addresses listed under Zone Rule and Local IP List will be monitored by Firewall as per selected filter type.

Zone Rule

This is a set of network access rules to make the decision of allowing/blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked.

Buttons to configure a zone rule:

Add Host Name – This option lets you add a "host" in the zone rule. After clicking Add Host Name, enter the HOST name of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click OK to create the zone rule.

Add IP – This option lets you add an IP address of a system to be added in the zone rule. After clicking **Add IP**, enter the IP address of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the Zone Rule.

Add IP Range – This option lets you add an IP range to be added in the zone rule. After clicking Add IP Range, add the IP Range (i.e. a range of IP that the zone rules should be applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click OK to create the zone rule.

Modify – To modify/change any listed zone rule (s), select the zone rule to be modified and then click **Modify**.

Remove - To remove any listed zone rule (s), select the zone rule and then click **Remove**.





Expert Rule

This tab lets you specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source IP address and port, destination IP address and port, and ICMP types. You can create new expert rules.

However, configure these rules only if you are familiar with firewalls and networking protocols.

- Source IP Address/Host Name
- Source Port Number
- Destination IP Address/Host Name
- Destination Port Number





Buttons to configure an Expert Rule:

1. Add – Click Add to create a new Expert Rule. In the Add Firewall Rule Window:

Add Firewall Rule	×
General Source Destination Advanced	
Rule Name	
Rule1	
Rule Action • Permit Packet Protocol TCP and UDP	
Apply Rule on Interface	
Any Interface	
	1
OK Cancel	

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

Protocol – Select the network protocol (e.g. TCP, UDP, ARP) on which the Rule will be applied.

Apply rule on Interface – Select the Network Interface on which the Rule will be applied.





Source tab

In this section, specify/select the location from where the outgoing network traffic originates. **Source IP Address**

My Computer – The rule will be applied for the outgoing traffic originating from your computer.

Host Name – The rule will be applied for the outgoing traffic originating from the computer as per the host name specified.

Single IP Address – The rule will be applied for the outgoing traffic originating from the computer as per the IP address specified.

Whole IP Range – To enable the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the outgoing traffic from the computer(s) which is within the defined IP range.

Any IP Address – When this option is selected, the rule will be applied for the traffic originating from ANY IP address.

My Network – The rule will be applied for the outgoing traffic to the networked computer(s).

Source Port

Any – When this option is selected, the rule gets applied for outgoing traffic originating from any port.

Single Port – When this option is selected, the rule gets applied for the outgoing traffic originating from the specified/defined port.

Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

Port List – A list of port can be specified. The rule will be applied for the outgoing traffic originating from the ports as per specified in the list.

The rule will be applied when the selected Source IP Address and Source Port matchesNOTE together.

Destination tab

In this section, specify/select the location of the computer where the incoming network traffic is destined.

Destination IP Address

My Computer – The rule will be applied for the incoming traffic to your computer.

Host Name – The rule will be applied for the incoming traffic to the computer as per the host name specified.

Single IP Address – The rule will be applied for the incoming traffic to the computer as per the IP address specified.

Whole IP Range – To apply the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the incoming traffic to the computer(s) which are within the defined IP range.

Any IP Address – When this option is selected, the rule will be applied for the incoming traffic to ANY IP Addresses.





My Network – The rule will be applied for the incoming traffic to the networked computer(s).

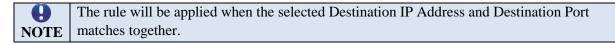
Destination Port

Any – After selecting this option, the rule will be applied for the incoming traffic to ANY port.

Single Port – After selecting this option, the rule will be applied for the incoming traffic to the specified/defined port.

Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the incoming traffic to the port which is within the defined range of ports.

Port List – A list of port can be specified/added. The rule will be applied for incoming traffic originating from the ports as per specified in the list.



Advanced tab

This tab contains advance setting for Expert Rule.

Enable Advanced ICMP Processing		
- ICMP Type		
	In	Out
Destination Unreachable		
Echo Reply (ping)		
Echo Request (ping)		
Information Reply		
Information Request		
Parameter Problem		
Redirect		
Source Quench		
TTL Exceeded		
 The packet must be from/to a trusted MAC adds Log information when this rule applies 	ress	

Enable Advanced ICMP Processing - This is activated when the ICMP protocol is selected in the General tab.

The packet must be from/to a trusted MAC address – When this option is selected, the rule will only be applied on the MAC address defined/listed in the Trusted MAC Address tab.

Log information when this rule applies – This will enable to log information of the Rule when it is applied.

Following are additional buttons the Expert Rule tab provides:





Modify – Clicking Modify lets you modify any Expert Rule.

Remove – Clicking **Remove** lets you delete a rule from the Expert Rule.

Shift Up and Shift Down – The UP and DOWN arrow button will enable to move the rules up or down as required and will take precedence over the rule listed below it.

Enable / Disable- These buttons lets you enable or disable a particular selected rule from the list.





Trusted MAC Address

This section contains the information of the MAC address of the system. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the Advance Tab of the Expert Rule).

Buttons (to configure the Trusted MAC Address)

Add - To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-

Edit – To modify/change the MAC Address, click Edit.

Remove – To delete the MAC Address, click **Remove**.

Clear All – To delete the entire listed MAC Address, click Clear All.

Local IP List

This section contains a list of Local IP addresses.

Fire	eWall	🝸 Help						
Allow All O Limited Filter O Interactive Filter								
			I					
	Zone Rule Expert Rule Trusted MAC Address Local IP List Application Rule							
	0000:0000:0000:0000:0000:0000:0000							
	127.*.*.*							
	192.168.*.*							
	FE80:0000:0000:0000:0000:0000:0000							
	Add Remove Clear All							
4	Show Application Alert							
Default Rules Advanced Setting OK Cancel								
De	efault Rules Advanced Setting OK Cancel		•					

Add – To add a local IP address, click Add.

Remove – To remove a local IP address, click **Remove**.

Clear All – To clear all local IP addresses, click Clear All.

Default List – To load the default list of IP addresses, click Default List.





Application Rule

In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.

Fire Wall		🝸 Help
Allow All Eimited Filter Interactive Filter		
Zone Rule Expert Rule Trusted MAC Address Local IP List Application Rule		
Application Description	Path	Access
Add Remove Clear All		
Show Application Alert		
Default Rules Advanced Setting OK Cancel		

Defining permission for an application

- To define permission for an application:
 - 1. Click Add.
 - 2. Add New Application window appears.

		×
Add New Applicatio	n	
Application name	with path	
Ask	Permit	O Deny
OK Car	ncel	

- 3. Enter the application name with path and select permission.
- 4. Click OK.

The permission for the application will be defined.

Removing permission of an application

Select an application and then click **Remove**. The application will no longer have the permission.





Other Buttons:

- Clear All This option will clear/delete all the information stored by the Firewall cache.
- **Show Application Alert** Selecting this option will display an eScan Firewall Alert displaying the blocking of any application as defined in the Application Rule.
- **Default Rules** This button will load/reset the rules to the Default settings present during the installation of eScan. This will remove all the settings defined by user.
- Advanced Settings: This button allows you to configure below mentioned advanced settings:
 - **Disable Trojan Rule:** It allows you to disable the blocking of programs that are either Trojan malware or follow Trojan rule.
 - Block Portscan: It allows you to block the scanning of network ports.





Endpoint Security

Endpoint Security module protects your computer or Computers from data thefts and security threats through USB or FireWire® based portable devices. It comes with Application Control feature that lets you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that lets you determine which applications and portable devices are allowed or blocked by eScan.

Start Stop Application Control Device Cor	itrol DLP	
Enable Application Control		
Block List White List Defi	ne Time-Restrictions	
Enter Application to Block		
List of Blocked Applications		
+ Custom Group	Allow This Group	Block
+ Computer Game	Allow This Group	Delete
+ Instant Messengers	Allow This Group	Delete
+ Music Video Players	Allow This Group	
+ P2P Applications	Allow This Group	

This page provides you with information regarding the status of the module and options for configuring it.

• **Start/Stop:** It lets you enable or disable Endpoint Security module. Click the appropriate option.

There are two tabs - Application Control, Device Control, and DLP which are as follows:





Application Control

This tab lets you control the execution of programs on the computer. All the controls on this tab are disabled by default. You can configure the following settings:

Enable Application Control

Select this option if you want to enable the Application Control feature of the Endpoint Security module.

Block List

Enter Application to Block: It indicates the name of the application you want to block from execution. Enter the full name of the application to be blocked.

List of Blocked Applications

This list contains blocked executables of applications that are predefined by MicroWorld. Each of the applications listed in the predefined categories are blocked by default. In addition, you can also add executables that you need to block only to the Custom Group category. If you want, you can unblock the predefined application by clicking the **Unblock** link. The predefined categories include computer games, instant messengers, music & video players, and P2P applications. The **Allow This Group** checkbox in front of each group allows that entire group.

White List

Enable Whitelisting

Select this checkbox to enable the whitelisting feature of the Endpoint Security module.

Enter Application to whitelist

Enter the name of the application to be whitelisted.

White Listed Applications

This list contains whitelisted applications that are predefined by MicroWorld. Each of the applications listed in the predefined categories are allowed by default. If you want to block the predefined applications, select the **Block** option.

Define Time Restrictions

This option lets you enable/disable application control feature. This feature lets you define time restriction when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day.

For example, the administrator can block computer games, instant messengers, for the whole day but allow during lunch hours without violating the Application Control Policies.

Datewise Restrictions

This feature lets you define datewise restrictions when you want to allow or block access to the applications based on specific dates and between pre-defined hours during that date.





Device Control

The Endpoint Security module protects your computer from unauthorized portable storage devices prompting you for the password whenever you plug in such devices. The devices are also scanned immediately when connected to prevent any infected files running and infecting the computer.

USB Settings		
Block USB Ports	Ask for Password	
Use eScan Administrator Use Other Password	r Password	
Do Virus Scan	Allow user to cancel scan	
Read Only - USB	Disable AutoPlay	
Record Files Copied To U Record Files Copied To N Whitelist	etwork 🔽 Ignore System Drive	
Record Files Copied To N Whitelist Scan Whitelisted USB De	etwork Ignore System Drive	3 Device
Record Files Copied To N Whitelist	etwork 🔽 Ignore System Drive	
Record Files Copied To N Whitelist Scan Whitelisted USB De	etwork Ignore System Drive	Add Import Edit
Record Files Copied To N Whitelist Scan Whitelisted USB De	etwork Ignore System Drive	Add Import Edit Delete
Record Files Copied To N Whitelist Scan Whitelisted USB De	etwork Ignore System Drive	Add Import Edit
Record Files Copied To N Whitelist Scan Whitelisted USB De	etwork Ignore System Drive	Add Import Edit Delete RemoveAll

You can configure the following settings:

Enable Device Control [Default]

Select this option if you want to monitor all the USB storages devices connected to your endpoint. This will enable all the options in this tab.

USB Settings

This section lets you customize the settings for controlling access to USB storage devices.

Block USB Ports

Select this option if you want to block all the USB storage devices from sharing data with endpoints.





Ask for Password

Select this option, if you want eScan to prompt for a password whenever a USB storage device is connected to the computer. You have to enter the correct password to access USB storage device. It is recommended that you always keep this checkbox selected.

- Use eScan Administrator: This option is available only when you select the Ask for Password checkbox. Click this option if you want to assign eScan Administrator password for accessing USB storage device.
- Use Other Password: This option is available only when you select the Ask for Password checkbox. Click this option if you want assign a unique password for accessing USB storage device.

Do Virus Scan [Default]

When you select this option, the Endpoint Security module runs a virus scan if the USB storage device is connected. It is recommended that you always keep this checkbox selected.

Allow user to cancel scan

Select this option to allow the user to cancel the scanning process of the USB device.

Read Only - USB

Select this option if you want to allow access of the USB device in read-only mode.

Disable AutoPlay [Default]

When you select this option, eScan disables the automatic execution of any program stored on a USB storage device when you connect the device.

Record Files Copied To USB

Select this option if you want eScan to create a record of the files copied from the system to USB drive.

Record Files Copied To Network

Select this option if you want eScan to create a record of the files copied from managed computers to the network drive connected to it.

Record Files Copied To Local

Select this option if you want eScan to create a record of the files copied from the one drive to another drive of the system. Please note that if you have selected "Ignore System Drive" along with this option no record will be captured if the files are copied from system drive (the drive in which OS is installed) to another drive.

Ignore System Drive

Select this option in case of you do not want eScan to record files that are copied from system drive of managed computers to either network drive or any local drive.

Whitelist

eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password but will directly display the files or folders stored on the device. This section displays the serial number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking **Add**. The Whitelist section displays the following button:

Scan Whitelisted USB Devices

By default, eScan does not scan whitelisted USB devices. Select this option, if you want eScan to scan USB devices that have been added to the whitelist.





Remove Read Only access for Whitelisted USB Device

Select this option to remove the read-only access for the whitelisted USB Device.

Add

Click **Add** to whitelist USB devices. USB Whitelist window appears.

USB White	elist					
-	Serial No.	Device Name	2	<u>Host Name</u>	<u>Client Date and</u> <u>Time</u>	<u>Description</u>
No Recor	rd Found					

To whitelist a USB device, its details are required. If a USB device is connected to any eScan installed endpoint, the USB details are sent to the server. The administrator will have to manually whitelist the USB device.

To manually add a USB device in USB Whitelist without connecting to an endpoint, click Custom.

	3
USB Whitelist	
Serial No.	
Device Name	
Description	
OK Cancel	

Enter the USB details and then click OK. The USB device will be added and whitelisted.

Import

To whitelist USB devices from a CSV file, click **Import**. Click **Choose File** to import the file with the list.

The list should be in following format: Serial No 1, Device Name 1, Device Description 1 (Optional)





Serial No 2, Device Name 2

E.g. SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by xyzDFRGHHRS54456HGDF347OMCNAK, Flash Drive 2.2

Disable Web Cam: Select this option to disable Webcams.

Disable SD Cards: Select this option to disable SD cards.

Disable Bluetooth: Select this option to disable Bluetooth.

Disable Hotspot: Select this option to disable Hotspot.

CD / DVD Settings

Block CD / DVD: Select this option to block all CD/DVD access.

Read Only - CD / DVD: Select this option to allow read-only access for CD/DVD.

Click **Default** to apply default settings done during eScan installation. It loads and resets the values to the default settings.





DLP

The DLP tab lets you control attachment flow within your organization. You can block/allow all attachments the user tries to send through specific processes that can be defined. You can exclude specific domains/subdomains that you trust, from being blocked even if they are sent though the blocked processes mentioned before.

Att	tachment Allowed	
O Att	tachment Blocked	
Enter Pr	rocess Name : Eg. Thunderbird.exe	_
Ad	dd Delete	
Ad	Delete	
Blacklis	sted Process 🗹 Ignore Whitelisted Sites only for Blacklisted process	
P	Process Name Allow Only Whitelisted Site	
Attachm	nents will be allowed from below sites irrespective of the above settings	
Enter Si	ite Name : Eg. Gmail.com,Yahoo	
Ad		
Whitelis	sted sites	
		-
Γ□,	Attachment / Email report	
	Report for attachment allowed O Report for all email (including Attachment)	





Attachment Control

The Attachment Control tab lets you control attachment flow within your organization.

Attachment Allowed [Default]

Select this option if you want attachments to be allowed through all processes except a user specified set of processes.

Attachment Blocked

Select this option if you want attachments to be blocked through all processes except a user specified set of processes.

Enter Process Name

Enter the name of the processes that should be excluded from the above selection. Enter process name and then click **Add**. To delete the added process, select particular process in Blacklisted Process column and then click **Delete**.

Blacklisted Process

This will display a list of process you excluded when you selected the **Attachment Allowed** option. eScan will block all attachments through this process.

Whitelisted Process

This will display a list of process you excluded when you selected the **Attachment Blocked** option. eScan will allow all attachments through this process.

Ignore Whitelisted Sites only for Blacklisted process [Default]

Select this checkbox to ignore the whitelisted sites for process mentioned in Blacklist.

Enter Site Name

Enter the name of the websites through which attachments should be allowed irrespective of the above settings. To add site, enter site name and then click **Add**. To delete the added whitelisted site, select particular site in Whitelisted sites section and then click **Delete**.

Whitelisted Sites

The websites added above to be white listed are displayed in this list.

Attachment / Email report

Report for Attachment Allowed

This will list all the attachment allowed along with Application used to send attachment. E.g. Chrome, Firefox, Outlook, Skype, Yahoo messenger, etc.

Report for all email (Including Attachment)

This will list all the email attachment uploaded along with Application used and subject of the email.





Content Control

This tab enables the administrator to monitor & control the type of information which can be sent outside of the endpoints.

plication	Control Device Control DLP
Attach	ment Control Content Control
🖵 🗹 En	able Blocking
O Blo	ock O Monitor
2	ontent list
	Indian PAN Card
	Indian Passport
	Indian Voter ID
	International Bank Account Number (IBAN)
	American Express - Credit Card Mastercard - Credit Card
	Mastercard Credit Card
C	hannels ·
	board Protection
	Chat Applications
	All Applications
	plication File Access Protection
	Password Protected Archives Password Protected Documents
	Scan Archives
Rer	novable Storage Protection
	Removable Storage
	ter Protection
	Printers
	Printers





Enable Blocking

Select this option if you want to block all types of content, such as identity cards, personal details connected to your endpoint. This will enable all the options on this tab.

Block:

Monitor:

Content List

Select this option to block sensitive information from all the listed documents like Credit/Debit Card, Passport, Pan Card, and Driving License.

Channels

You can configure all types of channel, where you can transfer the content through this.

Clipboard Protection

- Chat Applications [Default]: Select this option to deny all chat applications from sharing the data.
- Allow Drag and Drop [Default]: Select this option to allow the Drag and Drop function of sensitive content.
- All Applications: Select this option to deny all the applications from sharing the data.

Application File Access Protection

- **Password Protected Archives [Default]:** Select this option to block all password protected archives and from sharing it.
- **Password Protected Document [Default]:** Select this option to block all password protected document and from sharing it.
- Scan Archives [Default]: Select this option to scan all the archives files.

Removable Storage Protection

- **Removable Storage:** select this option to deny all removable storage attached to the computer from accessing the personal information.
- **CD/DVD:** Select this option to deny all CD/DVD access to confidential data.

Printer Protection

• Printers: Select this option to deny the use of networked printers to print the sensitive data.





Advanced Settings

Clicking Advanced displays Advanced Settings.

Name	Value	
Allow Composite USB Device	1 .	
Allow USB Modem	1 🔻	
Enable Predefined USB Exclusion for Data Outflow	1 .	
Enable CD/DVD Scanning	1 🔻	
Enable USB Whitelisting option on prompt for eScan clients	0	
Enable USB on Terminal Client	1 🔻	
Enable Domain Password for USB	0 🔻	
Show System Files Execution Events	0 .	
Allow mounting of Imaging device	1 .	
Block File Transfer from IM	1 🔻	
Allow WIFI Network	1 .	
Whitelisted WIFI SSID (Comma Separated)		
Allow Network Printer	1 .	
Whitelisted Network Printer list(Comma Separated)		
Disable Print Screen	0 .	
Allow eToken Devices	1 7	
Include File Extension for File Activity Monitoring (e.g EXE)		

Allow Composite USB Device (1 = Enable/0 = Disable)

Select this option to allow/block use of composite USB devices.

Allow USB Modem (1 = Enable/0 = Disable)

Select this option to allow/block use of USB modem.

Enable Predefined USB Exclusion for Data Outflow (1 = Enable/0 = Disable)

Select this option to enable/disable use of predefined USB.

Enable CD/DVD Scanning (1 = Enable/0 = Disable)

Select this option enable/disable scanning of CD/DVD.

Enable USB Whitelisting option on prompt for eScan clients (1 = Enable/0 = Disable) Select this option to enable/disable USB Whitelisting option on prompt for eScan clients.

Enable USB on Terminal Client (1 = Enable/0 = Disable) Select this option to enable/disable USB on terminal client.

Enable Domain Password for USB (1 = Enable/0 = Disable)

Select this option to enable/disable domain password for USB.

Show System Files Execution Events (1 = Enable/0 = Disable) Select this option allow/block system files execution events.

Allow mounting of Imaging device (1 = Enable/0 = Disable) Select this option to allow/block mounting of imaging devices.





Block File Transfer from IM (1 = Enable/0 = Disable) Select this option to allow/block file transfer from Instant Messengers.

Allow Wi-Fi Network (1 = Enable/0 = Disable) Select this option to allow/block use of Wi-Fi networks.

Whitelisted WIFI SSID (Comma Separated) Select this option to whitelist WIFI SSID. Enter the WIFI SSID in comma separated format.

Allow Network Printer (1 = Enable/0 = Disable) Select this option to allow/block use of network printers.

Whitelisted Network Printer list (Comma Separated) Select this option to whitelist network printer list. Enter the name of printers in comma separated format.

Allow eToken Devices (1 = Enable/0 = Disable) Select this option to allow/block use of eToken devices.

Include File Extension for File Activity Monitoring (e.g EXE) Select this option to include File Extension for File Activity Monitoring.

Exclude File Extension for File Activity Monitoring (e.g EXE) Select this option to exclude File Extension for File Activity Monitoring (e.g EXE).

Auto Whitelist BitLocker encrypted USB Devices (1 = Enable/0 = Disable) Select this option to allow/block auto whitelist BitLocker encrypted USB devices.

Ask Password for whitelisted Devices only (1 = Enable/0 = Disable) Select this option to allow/block ask password for whitelisted devices.

Disable Print Screen (1 = Enable/0 = Disable)

Select this option to enable/disable use of printer screen.

Block Software Installation/Uninstallation (1 = Enable/0 = Disable)

Select this option to enable/ disable for block software installation/uninstallation.

Click **Default** to apply default settings done during eScan installation. It loads and resets NOTE the values to the default settings.

A





Privacy Control

Privacy Control module protects your confidential information from theft by deleting all the temporary information stored on your computer. This module lets you use the Internet without leaving any history or residual data on your hard drive. It erases details of the sites and web pages you have accessed while browsing. This page provides you with options for configuring the module.

vacy Control		? •
General Advanced Scheduler Options You can set to run this Tool Automatically Options Below.	at Various times. Select the times you would like Auto Erase to run from the	
Run at System Startup	Run Everyday at 0:00 am	
Auto Erase Options Clear Auto-Complete Memory Clear Last Run Menu	Clear Recent Documents	
 Clear Temporary Folders Clear Last Find Computer Clear Browser Address Bar History 	 Clear Files & Folders Clear Open/Save Dialog Box History Empty Recycle Bin Clear History Select All 	
Default OK Cancel		

It consists following tabs:

- General
- Advanced

General tab

This tab lets you specify the unwanted files created by web browsers or other installed softwares that should be deleted. You can configure the following settings:

Scheduler Options

You can set the scheduler to run at specific times and erase private information, such as the browsing history from your computer. The following settings are available in the **Scheduler Options** section.

- **Run at System Startup**: It auto executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.
- **Run Everyday at**: It auto-executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.





Auto Erase Options

The browser stores traceable information of the websites that you have visited in certain folders. This information can be viewed by others. eScan lets you remove all traces of websites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. You can select the following options based on your requirements.

Clear Auto Complete Memory

Auto Complete Memory refers to the suggested matches that appear when you enter text in the Address bar, the Run dialog box, or forms in web pages. Hackers can use this information to monitor your surfing habits. When you select this checkbox, Privacy Control clears all this information from the computer.

Clear Last Run Menu

When you select this option, Privacy Control clears this information in the Run dialog box.

Clear Temporary Folders

When you select this option, Privacy Control clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive and boosts the performance of the computer.

Clear Last Find Computer

When you select this option, Privacy Control clears the name of the computer for which you searched last.

Clear Browser Address Bar History

When you select this checkbox, Privacy Control clears the websites from the browser's address bar history.

Clear Last Search Menu

When you select this option, Privacy Control clears the name of the objects that you last searched for by using the Search Menu.

Clear Recent Documents

When you select this checkbox, Privacy Control clears the names of the objects found in Recent Documents.

Clear Favorites

When you select this checkbox, Privacy Control clears the names of the objects found in Favorites.

Clear Open/Save Dialog box History

When you select this checkbox, Privacy Control clears the links of all the opened and saved files.

Empty Recycle Bin

When you select this checkbox, Privacy Control clears the Recycle Bin.



Use this option with caution as it permanently clears the recycle bin.

Clear Cache

When you select this checkbox, Privacy Control clears the Temporary Internet Files.

Clear Cookies

When you select this checkbox, Privacy Control clears the Cookies stored by websites in the browser's cache.





Clear Plugins

When you select this checkbox, Privacy Control removes the browser plug-in.

Clear ActiveX

When you select this checkbox, Privacy Control clears the ActiveX controls.

Clear History

When you select this checkbox, Privacy Control clears the history of all the websites that you have visited.

In addition to these options, the Auto Erase Options section has below option as well.

Select All/ Unselect All

Click this button to select/unselect all the auto erase options.

Advanced tab

This tab lets you select unwanted or sensitive information stored in MS Office, other Windows files and other locations that you need to clear.

Privacy Control		👔 Help
General Advance MS Office MS Word MS Excel MS PowerPoint MS FrontPage MS Access	d Windows Temp files of Scan Disk Temp Files Clipboard Data Start Menu Order History Registry Streams MRU (Most recently used) Application Log	Others Windows Media Player Play List Windows Media Player History
		<u>Select All</u>
Default OK	Cancel	

MS Office

The most recently opened MS office files will be cleared if these options are selected.

Windows

The respective unwanted files like temp files will be cleared.

Others

The unwanted files in the Windows media player will be cleared.

Select All/ Unselect All

Click this button to select/unselect all the options in Advanced tab.

Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

Policy Details also lets you do the following for Windows Operating System.





Administrator Password

Administrator Password policy in eScan Enterprise EDR - Cloud lets you create and change password for administrative login of eScan Protection Center and Two-Factor Authentication.

eScan Password

Select the option **Set Password** and define a password as per your choice. It also lets you keep the password as blank, wherein you can login to eScan Protection Center without entering any password for read-only access.

Add/Change Password	🝸 Help
eScan Password Two-Factor Authentication	
Set Password Enter new Password	
Confirm new Password Password is case-sensitive	
Use separate uninstall password Enter uninstall password Confirm uninstall password	
Default Advanced Setting OK Cancel	

Below are the mandatory criteria for strong password creation:

Password length: The password length should be of minimum 8 characters.
Lowercase: The password must contain at least 1 letter in Lowercase (a-z).
Uppercase: The password must contain at least 1 letter in Uppercase (A-Z).
Numeric: The password must contain at least 1 digit (0-9).
Special character: The password must contain at least 1 special character (\$ @ ! % * # ? _ &).
Password match: Both the entered passwords should be matching.

Additionally, there is an option to set an uninstall password. An uninstall password prevents unauthorized uninstallation of eScan client from the endpoint. Upon selecting Uninstall option, eScan





asks for uninstall password before proceeding further. To set an uninstall password, select checkbox **Use separate uninstall password**.

Two-Factor Authentication

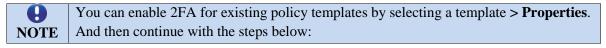
Your default system authentication (login/password) is Single-Factor Authentication which is considered less secure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode after entering the system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized access.

With the 2FA feature enabled, the system will be protected with basic system login and eScan 2FA. After entering the system credentials, eScan Authentication screen will appear as shown in the below image. The personnel will have to enter the 2FA passcode to access the system. A maximum of three attempts are allowed to enter the correct passcode. If the 2FA login fails, the personnel will have to wait for 30 seconds to log in again. Read about managing 2FA license.

eScan Auther	ntication
	Two-Factor Authentication
	Enter your passcode:
eSoari	Verify
www.escanav.com Copyright MicroWorld	Wed, 04 Aug 2021 01:17:00 PM UTC

To enable the Two-Factor Authentication feature, follow the steps given below:

- 1. In the eScan web console, go to Managed Computers.
- 2. Click **Policy Templates** > **New Template**.



- 3. Select Administrator Password checkbox and then click Edit.
- 4. Click **Two-Factor Authentication** tab. Add/Change Password window appears.





Scan Password	Two-Factor Auth	entication	
Enable Two-F	actor Authentication		
RDP	Safe Mode	Local Logon	Unlock
Use Other	Administrator Password Password Two-Factor Authentication		

5. Select the checkbox **Enable Two-Factor Authentication**. The Two-Factor Authentication feature gets enabled.

Login Scenarios

The 2FA feature can be used for all the following login scenarios:

RDP

RDP stands for Remote Desktop Protocol. Whenever someone takes remote connection of a client's system, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Safe Mode

After a system is booted in Safe Mode, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Local Logon

Whenever a system is powered on or restarted, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Unlock

Whenever a system is unlocked, the personnel will have to enter login credentials and 2FA passcode to access the system.

Password Types

If the policy is applied to a group, the 2FA passcode will be same for all group members. The 2FA passcode can also be set for specific computer(s). You can use following all password types to log in:

Use eScan Administrator Password

You can use the existing eScan Administrator password for 2FA login. This password can be set in **eScan Password** tab besides the **Two-Factor Authentication** tab.





Use Other Password

You can set a new password which can be combination of uppercase, lowercase, numbers, and special characters.

Use Online Two-Factor Authentication

This option can be enabled for all users or for particular user according to the requirement. To learn more about adding user and enabling the 2FA, <u>click here</u>.

O NOTE	Users can be added via Settings > Two-Factor Authentication > Users for 2FA option.
------------------	--

To use this feature, follow the steps given below:

- 1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
- 2. Open the Authenticator app and tap Scan a barcode.
- 3. Select the checkbox Use Online Two-Factor Authentication.
- 4. Go to **Managed Computers** and below the top right corner, click **QR code for 2FA**. A **QR** code appears.
- Scan the onscreen QR code via the Authenticator app. A Time-based One-Time Password (TOTP) appears on smart device.
- 6. Forward this TOTP to personnel for login.





Advanced Setting

Clicking Advanced Setting displays Advance setting.

ance	ed Setting	
	Name	Value
	Enable Automatic Download	1 .
	Enable Manual Download	1 .
	Enable Alternate Download	1 .
	Set Alternate Download Interval(In Hours)	6
	Disable download from Internet for Update Agents	0 .
	Stop Auto change for download from Internet for Update Agents	1 .
	Enable Download of AntiSpam update first on clients	1 .
	No password for pause protection	0 .

Enable Automatic Download (1 = Enable/0 = Disable)

It lets you Enable/Disable Automatic download of Antivirus signature updates.

Enable Manual Download (1 = Enable/0 = Disable)

It lets you Enable/Disable Manual download of Antivirus signature updates.

Enable Alternate Download (1 = Enable/0 = Disable)

It lets you Enable/Disable download of signatures from eScan (Internet) if eScan Server is not reachable.

Set Alternate Download Interval (In Hours)

It lets you define time interval to check for updates from eScan (Internet) and download it on managed computers.

Disable download from Internet for Update Agents (1 = Enable/0 = Disable)

Selecting this option lets you disable Update Agents from downloading the virus signature from internet.

Stop Auto change for download from Internet for Update Agents (1 = Enable/0 = Disable)

This option is used when an Update Agent didn't find the primary server to download virus signature, then it tries to get virus signature from internet, so to stop Update Agent from downloading from internet this option is to be set to 1(one).

Enable Download of Anti-Spam update first on clients (1 = Enable/0 = Disable)

Normally while updating a system for virus signatures, we first download the anti-virus signature and then anti-spam signature. This option lets you first download Anti-spam updates on clients.





No password for pause protection

Selecting this option lets you pause the eScan protection without entering password.

Download Signature Updates from Internet and policy from Primary Server (1= Enable/0 Disable)

Selecting this option lets you download Signature Updates from Internet and policy from Primary Server.

Change ICON to eScan (1= Enable/0=Disable)

Selecting this option will allow you to change the icon of the eScan.

Stop Patch Notification (1= Enable/ 0 = Disable)

This option allows you to enable/disable the patch notification option.

Set IPONLY (1=Enable/0=Disable)

Select enable/disable to set the IP ONLY option.

Enable HTTPS Download (1=Enable/0=Disable)

This option allows you to enable/ disable the HTTPS Download option.

Show Protection Center in Read Only Mode (Applicable only on icon Click) Select enable/ disable to show Protection Center in Read Only Mode option.

Enable Policy REAPP (1=Enable/0=Disable) Select this option to enable Policy REAPP option.

Disable Policy REAPP REG Only (1=Enable/0=Disable) Select this option to disable the Policy REAPP REG only option.

Enable Win Patch download (1=Enable/0=Disable) Select this option to enable Win Patch Download option.

Enable ALL Win Patch Download (1=Enable/0=Disable) Select this option to enable ALL Win Patch Download option.





ODS/Schedule Scan

ODS (On Demand Scanning)/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

It consists following tabs:

- Options
- Scheduler

Options Scheduler		
Virus Check Alert		
In the case of an infection:	Automatic	~
Priority of scanner:	Normal (normal runtime)	~
File types:	Automatic type recognition	~
Use separate exclude list for ODS:	Add / Delete	
Limit CPU Usage	Enable for ODS only	~
CPU Percentage Value :	20 🗸	

Options

Options tab lets you make the settings for checking viruses and receiving alerts. There are two tabs – Virus Check and Alerts. You can do the following activities:

- Virus Check
- Alerts





Virus Check

It lets you configure the settings for checking viruses. To set Virus Check:

- 1. Specify the following field details:
 - In the case of an infection: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and Automatic [Default]. If the option Automatic is selected, eScan will quarantine the infected file. In this case, if the action Delete object is selected in File Anti-Virus module, the object will be deleted.
 - **Priority of scanner**: Select an appropriate option from the drop-down list. For example,
 - High (short runtime)
 - o Normal (normal runtime) [Default]
 - o Low (long runtime)
 - **File types**: Select an appropriate option from the drop-down list. For example, \[Default\] Automatic type recognition and Only program files.
 - Use separate exclude list for ODS: Select this option to add a list of file/folders that should be excluded from scan.
 - Limit CPU Usage: You can limit the CPU usage during the scan by selecting the appropriate option from the drop-down list.
 - o Disable for all scan instances
 - o Enable for ODS only
 - \circ Enable for all scan instances
 - **CPU Percentage Value:** Allocate the maximum threshold (in %) from the dropdown for CPU usage during the scan.
- 2. Click Save.

Alerts tab

It lets you configure the settings for virus alert. You can also create a log of the infected viruses. To set alerts,

- 1. Under Alert section, Select the [Default] Warn, if virus signature is more than x day's old checkbox, and then enter the number of days in the x day's old field, if you want to receive alerts when virus signature exceeds the specified days. By default, value 3 appears in the field.
- 2. Select the **Warn**, **if the last computer analysis was more than** x days ago checkbox, and then enter the number of days in the x days ago field, if you want to receive alerts when last computer analysis exceeds the specified days. By default, 3 appear in the field.
- 3. Under **Log Settings** section, select the [Default] **Prepare Log** checkbox, if you want to prepare log of the infected files, and then select an appropriate option.
- 4. Click Save.

Click Default to apply default settings, which are done during installation of eScan. It loadsNOTE and resets the values to the default settings.





Scheduler

Scheduler tab lets you create/delete various tasks in the scheduler for automatic virus scanning.

Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

Clear All - This button will clear all the listed tasks.

Add Task

Scheduler		
Name So	chedule	Next start
Clear All Ad	dd task Delete task	Edit

Automatic Virus Scan window lets you do following activities:

- a) Creating job
- b) Setting analysis extent
- c) Scheduling virus execution
- d) Scheduling virus scan

a) Job

It lets you create the job details for virus scanning.

- 1. Click the **Job** tab.
- 2. Specify the following field details.
 - Name: Enter a name for the task.
 - Active [Default]: Select this checkbox, if you want to allow the client to schedule the task.
 - **Start in foreground [Default]**: Click this option if you want to view scanning process running in front of you. When this option is selected, the **Scan only when idle** option becomes unavailable.
 - Start in background: Click this option if you want scanning process to run in the background. By default, **Do not quit if virus is detected** option is selected. When you select this option, the Quit drop-down list becomes unavailable.
- 3. Click Save.





b) Analysis Extent

It lets you configure analysis extent settings for virus scanning.

Automatic virus scan
Job Analysis extent Schedule Virus scan
 Scan Startup Scan memory, registry and services Scan local hard drives Scan System Drive Scan Data Drives Scan network drives
Save Cancel

- 1. Click the Analysis Extent tab.
- 2. Select the Scan Startup option, if you want to scan all startup entries.
- 3. Select the **Scan memory, registry** and **services** option, if you want to scan memory, registry and services.
- 4. Select the [Default] Scan local hard drives option, if you want to scan local hard drives.
- 5. Select **Scan network drives** option, if you want to scan network drives. Users should note that scanning a network drive may affect system performance.
- 6. Click Save.





c) Scheduling

It lets you schedule the date and time of execution for virus scanning.

	atic virus scan	?	Help
	Job Analysis extent	Schedule Virus scan	
	Execute		
	Once	O Weekly	
	Hourly	O Monthly	
	Daily	 With system startup 	
	Date and time		
	09/26/2019	12:00 pm	
Sav	Cancel		

- 1. Click Schedule tab.
- 2. Under Execute section, select an appropriate option. For example, [Default] Once, weekly, hourly, and so on.
- 3. Under Date and time section, click the calendar icon. The calendar appears.
- 4. Select an appropriate date from the calendar.

Click the left < and right > sign to navigate to the previous or next month and year from the calendar respectively.

- 5. Click the **Time** icon. The Timer appears.
- 6. Click the **AM** tab to view the before noon time and **PM** tab to view the afternoon time, and then select an appropriate time from the list.
- 7. Click Save.





d) Virus Scan

It lets you schedule virus scanning.

Automatic virus scan	🝸 Help
Job Analysis extent Schedule	Virus scan
In the case of an infection:	Automatic V
Priority of scanner:	Normal (normal runtime)
File types:	Automatic type recognition
Log Settings Prepare Log Only infection to be logged Full log	
Save Cancel	

- 1. Click the **Virus Scan** tab.
- 2. Specify the following field details:
 - In the case of an infection: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
 - **Priority of scanner**: Select an appropriate priority from the drop-down list.
 - **File types**: Select an appropriate option from the drop-down list. For example, [Default] Automatic type recognition and Only program files.
- 3. Under Log Settings section, select the [Default] Prepare Log checkbox, if you want to prepare log of the infected files, and then click an appropriate option.
- 4. Click Save.

Delete Task - Clicking Delete Task lets you delete the particular task from the list.

Edit – Clicking Edit lets you edit the properties of the particular task from the list.

Advanced Settings

Autorun System Scanning if System not scanned for days defined

This option let you define days for autorun system scanning if system is not scanned.

Ignore Battery Status

Select this option to Ignore Battery Status.

Scan USB when All Drive option selected

Select this option to scan USB when all drive options are selected.

Remove LNK

This option lets you Enable/Disable Removal of LNK.

Start Background Scan in System Mode

Select this option to start background scan in system mode.





Enable Scan Caching This option lets you Enable/Disable scanning of cache.

Check for Corrupted Files

Select this option to check for corrupted files.

Scan in low Priority Mode

It lets you Enable/Disable the scan in low priority mode on the computer.

Enable Unhiding of USB Files & Folder

This option let you enable/disable unhiding USB files & folders.

Enable Missed schedule scan JOB's to run

This option let you enable/disable missed schedule scan JOB's to run.





MWL (MicroWorld WinSock Layer)

eScan's "MicroWorld-WinSock Layer" (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It has changed the way the world deals with Content Security threats. Unlike the other products and technologies, MWL tackles a threat before it reaches your applications. MWL is technically placed above the WinSock layer and acts as a "Transparent Gatekeeper" on the WinSock layer of the operating system. All content passing through WinSock has to mandatorily pass through MWL, where it is checked for any security violating data. If such data occurs, it is removed and the clean data is passed on to the application.

MWL Inclusion List

Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.

8

Click Default to apply default settings, done during eScan installation. It loads and resets **NOTE** | the values to the default settings.

You can do the following activities.

- ٠ Adding files to Inclusion List
- **Deleting files** from Inclusion List
- ٠ Removing all files from Inclusion List

MWL Inclusion List		🝸 Help
	_	Add
telnet.exe	<u> </u>	Delete
msimn.exe		
outlook.exe		RemoveAll
eudora.exe		
winpm-32.exe		
phoenix.exe		
thebat.exe		
jrew.exe		
Jre.exe		
inetinfo.exe	-	
Default Ok Cancel		

Add files to Inclusion List

To add executable files to the Inclusion List, follow the steps given below:

- 1. Enter the executable file name and then click **Add**. The executable file will be added to the Inclusion List.
- 2. Click OK.





Delete files from Inclusion List

To delete executable files from the Inclusion List, follow the steps given below:

- 1. Select executable files, and then click **Delete**.
 - A confirmation prompt appears.
- 2. Click **OK**. The executable file will be deleted from the Inclusion List.

Remove all files from Inclusion List

To remove all executable files from the Inclusion List, follow the steps given below:

- 1. Click **Remove All**. A confirmation prompt appears.
- 2. Click **OK**. All executable files will be removed from the Inclusion List.

MWL Exclusion List

MWL (MicroWorld WinSock Layer) Exclusion List contains the name of all executable files which will not bind itself to **MWTSP.DLL**.

Click **Default** to apply default settings, which are done during installation of eScan. It loads **NOTE** and resets the values to the default settings.

You can do the following activities:

- Adding files to Exclusion List
- **Deleting files** from Exclusion List
- **Removing all files** from Exclusion List

MWL Exclusion List	👔 Help
INETINFO.EXE	Add
VHTTPD32.DLL	Delete
NS-ADMIN.EXE	RemoveAll
NS-SLAPD.EXE	
TCPSVCS.EXE	
SVCHOST.EXE	
ESERV.EXE	
DOWNLOAD.EXE	
RP.EXE	
SPOOLER.EXE	
Default Ok Cancel	





Adding files to Exclusion List

To add executable files to the Exclusion List:

- 1. Enter the executable file name and then click **Add**. The executable file gets added to the Exclusion List.
- 2. Click **OK**.

Deleting files from Exclusion List

To delete executable files from the Exclusion List:

- 1. Select the appropriate file checkbox, and then click **Delete**. A confirmation prompt appears.
- 2. Click **OK**. The executable file gets deleted from the Exclusion List.

Removing all files from Exclusion List

To remove all executable files from the Exclusion List:

- 1. Click **Remove All**. A confirmation prompt appears.
- 2. Click **OK**. All executable files get removed from the Exclusion List.





Notifications and Events

Notifications & Events		🝸 Help
Notifications Events		
Varning Notification Settings	From To	
Mail Server Settings SMTP Mail Server SMTP Port User Authentication(Opt.) Authentication Password(Opt.)	Delete Mails From User Add Delete RemoveAll	
Attachment Removed Warning To Sender Attachment Removed Warning To Recipient Virus Warning To Sender Virus Warning To Recipient Content Warning To Sender Content Warning To Recipient		_
attrem.snd #Lines starting with # are comment lines. #This file specifies warning sent to Mail-Sender by #Scan when it deletes attachments. # The attachment(s) that you sent with the following mail was deleted by eScan (not delivered to the recipient) The Mail came from : %f The Mail came from : %f The Mail recipient : %t Subject of the Mail : %s Message-ID : %i Received : %r		
Default Advanced Setting Ok	Cancel	

Notifications

Notifications tab lets you configure the notification settings. It lets you send emails to specific recipients when malicious code is detected in an email or email attachment. It also lets you send alerts and warning messages to the sender or recipient of an infected message. You can configure the following settings:

Virus Alerts [Default]

This section contains **Show Alert Dialog box** option. Select this option if you want Mail Anti-Virus to alert you when it detects a malicious object in an email.

Warning Mails

Configure this setting if you want Mail Anti-Virus to send warning emails and alerts to a given sender or recipient. The default sender is **postmaster** and the default recipient is **postmaster**.

Attachment Removed Warning to Sender [Default]

Select this checkbox if you want Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this email when it encounters a virus infected attachment in an email. The email content is displayed in the preview box.





Attachment Removed Warning to Recipient [Default]

Select this checkbox if you want Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The email content is displayed in the preview box.

Virus Warning to Sender [Default]

Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the sender. The email content is displayed in the preview box.

Virus Warning to Recipient [Default]

Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the recipient. The email content is displayed in the preview box.

Content Warning to Sender

Select this checkbox if you want Mail scanner to send a content warning message to the sender. The email content is displayed in the preview box.

Content Warning to Recipient [Default]

Select this checkbox if you want Mail scanner to send a content warning message to the recipient. The email content is displayed in the preview box.

Delete Mails from User

You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete Mails From User** field, the buttons get enabled.

Events

Events tab lets you define the settings to allow/restrict clients from sending alert for following events:

- Executable Allowed
- Website Allowed
- Cleaned Mail
- Application Stopped
- Application Started

By default, all events are selected.

Notifications & Events	?	Help
Notifications Events		
Do not allow client to send event for		1
Executable Allowed		
VebSite Allowed		
Cleaned Mail		
Application Stopped		
Application Started	-	
Default Advanced Setting Ok Cancel		





Advanced Settings

d Setting	
Name	Value
Enable Caching of Unsent Events	1 🗸
Show 'Secured by eScan' on startup	1 ¥
Show eScan Splash window	0 🗸
Send Only Defined Event Ids	
Enable Gaming Mode	0 🗸
Enable Gaming Mode	0 🗸

Enable Caching of Unseen Events (1 = Enable/0= Disable)

It lets you Enable/Disable automatic caching of unseen events.

Show 'Secured by eScan' on startup (1 = Enable/0= Disable)

It lets you Enable/Disable the display of 'Secured by eScan' at the startup of the computers.

Show eScan Splash window (1 = Enable/0= Disable)

It lets you Enable/Disable display of eScan Splash Window.

Send Only Defined Event Ids

It lets you send only the defined events such as File Antivirus IDs, Mail Antivirus IDs, and more.

Enable Gaming Mode (1 = Enable/0 = Disable)

It lets you Enable/Disable the gaming mode on the computer.





Schedule Update

The Schedule Update lets you schedule eScan database updates.

Automatic Dow	nload	O Scł	nedule Download	
Daily				
Weekly	Mon	Tue	Wed	🔲 Thu
	Fri Fri	Sat Sat	Sun	
Monthly	1 .			
	12:00			
🖻 At	12:00 am	<u>O</u> v		

The updates can be downloaded automatically with **Automatic Download** option. -OR-

The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

Advanced Settings

Set bandwidth limit for download (in kb/sec)

It lets you define bandwidth limit for download on managed computers, if you have limited internet connection or other network issues.

Retry schedule download (Default retry interval is 15 minutes)

It lets you define time to retry for download updates (Default retry interval is 15 minutes) on managed computers.





Tools

The Tools lets you configure eBackup setting.

Tools			<u>?</u> Help
EBackup			
Add Backup Set	ackup Set 前 Delete Backup Set		
Backup Name	Next Start	Created On	^
			-
Ok Cancel			

eBackup

Taking regular backup of your critical files stored on your computer is very important, as files may get misplaced or damaged due to issues such as virus outbreak, modification by a ransomware or another user. This feature of eScan allows you to take backup of your important files stored on your computer such as documents, Photos, media files, music files, contacts, and so on. It allows you to schedule the backup process by creating tasks. The backed up data is stored in an encrypted format in a folder secured by eScan's real-time protection. You can create Backup jobs by adding files, folders to take a backup either manually or schedule the backup at a defined time or day.

With eBackup feature you can:

- Create, schedule, edit, and delete backup jobs as per requirement.
- Take a backup of specific folder(s)/file extension(s) on local endpoint, external drives or network drive.
- Exclude specific folder(s)/file extension(s) from being backed up.
- Add specific file extensions to be backed up along with regular backup as per requirement.
- Save the backup data in external hard drive or local drive.

The eBackup option has following tabs to configure:

Job

Using this tab you can schedule the eBackup task.





l Backup Set		<u>?</u> I
Job Backup Source and Exclu	usion Backup location	
Active		
Name		
Cheduler		
Once	O Weekly	
O Hourly	O Monthly	
O Daily	O With system startup	
Date and time	· · ·	
	Date 08/01/2024 Time 10:26 AM	
		_
Set Restore Password		
	Note* : Password can be set only while adding new job.	
Save Cancel		

Active

Select this option to set the configuring eBackup option as active.

Scheduler

This option allows you to schedule the eBackup to repeat the process such as Once, Hourly, Daily, Weekly, Monthly, or with system startup.

Date and time

This option allows you to select the day, time, and date for running the scheduled eBackup task.

Set Restore Password

Select this option to set a password for restoring backup file on the computer.





Backup Source and Exclusion

This tab allows to include and exclude the folder and files for backup.

Job	Backup Source and Exc	Backup locatio	n		
Backup	Source				
	Folder		Ive	<u></u>	Add Delete RemoveAll Edit
Add F	Settings 	<u>Customize</u>	File/Folder Exclusion Add File/Folder Folder C Exclude by mask File/Folder T	VRE 1	Add Delete RemoveAll
				•	

Backup Source

This option allows you to add the folder path(s) on which the backup has to be performed. Apart from that you can select the document types to be backed up from these particular folders.

Folder Settings

- Add File Type for Backup: Select the type of files for backup. By default, Office Documents option is selected.
- **File/Folder Exclusion**: In this section, you can exclude a specific folder or a file format from getting backed up. You can add, delete, and remove the files for the same.





Backup Location

This tab allows to define the storage location for the backup created.

lob Backup Sou	ce and Exclusion	Backup location	1	
Local/Network	Google Drive	oropBox OneDri	ve	
Local Drive Settings	n Local/Network drive Backed up Files.		UserName	Password
Eg: 1. "c:\"	me or full UNC path is A 96\external\backup"	lowed.		

Local/Network

Administrator can save the backup set in the Local/Network Drive by providing the path of the drive and Username and password for the network drive.

P NOTE Network storage of backup set will be available in the trial period. To continue the use of this feature user need to avail the license for the same.

In case of system crash or hardware failure, user can recover the created data backup, so storing the backup in the network drive, mapped drive, or NAS drive would be useful in such scenarios.





Google Drive

Administrator can save the backup set in the Google Drive by selecting the appropriate Gmail account and password for the same.

Local/Network Google D	ive DropBox OneDrive		
Store backup on Google Driv	e.		
Google drive settings			
Select gmail account :		×	×
Refresh token :			
	Check Storage Log	n	
Remove gmail account :			/
	Mark for deletion Un	mark	
*Note: the selected email will be	permantly deleted only after saving the polic	y.	
Note: To store backup on the Go	gle Drive, select the appropriate Google acco you want to use account other than your exis	unt. If you have a Google account, click "Login". Additionally, the	"Login" button

•	To store backup on the G
	a Google account, click "
NOTE	an account if you want to

Google Drive, select the appropriate Google account. If you have 'Login". Additionally, the "Login" button also lets you create if you want to use account other than your existing accounts.





DropBox

Administrator can save the backup set in the DropBox by selecting the appropriate DropBox account and password for the same.

Job Backup Source and Exclu		
Local/Network Google Drive	e DropBox OneDrive	
Store backup on DropBox.		
DropBox settings		
Select DropBox account :	×	
Refresh token :		
Kerresh token :		
	Check Storage Login	
Remove dropbox account :	×	
	Mark for deletion Unmark	
*Note: the selected email will be p	permantly deleted only after saving the policy.	
Note: To store backup on the Drop	oBox, select the appropriate DrooBox account. If you have a DrooBox account, click "Login". Additionally, the "Login" butto	
also lets you create an account if	you want to use account other than your existing accounts.	
Note: To store backup on the Droj Ilso lets you create an account if	pBox, select the appropriate DropBox account. If you have a DropBox account, click "Login". Additionally, the "Login" butto you want to use account other than your existing accounts.	,



To store backup on the DropBox, select the appropriate DropBox account. If you have a DropBox account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts.





OneDrive

Administrator can save the backup set in the OneDrive by selecting the appropriate OneDrive account and password for the same.

ob Backup Source and Exclu			
Local/Network Google Drive	DropBox OneDrive		
Store backup on OneDrive.			
OneDrive Settings			
Select OneDrive account :		~	1
Refresh token :			
	Check Storage Login		
Remove onedrive account :		~	*
	Mark for deletion Unmark		
	Mark for deletion Unmark		
*Note: the selected email will be	ermantly deleted only after saving the policy.		
also lets you create an account if	orive, select the appropriate OneDrive account. If you want to use account other than your existing a	you have a OneDrive account, click "Login". Additionally, the accounts.	2 Login button



To store backup on the OneDrive, select the appropriate OneDrive account. If you have OneDrive account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts.

Add Backup Set

To create a Backup Set:

- 1. Go to Managed Computers.
- 2. Click **Policy Templates** > **New Template.**

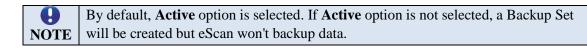
You can add the backup set for existing Policy Templates by selecting a Policy Template **NOTE** and then clicking **Properties**. Then, follow the steps given below:

- 3. Select **Tools** checkbox and then click **Edit**.
- 4. Click Add Backup Set.

Add Backup Set window appears.

- 5. In Job tab, enter a name.
- 6. In the Scheduler section, select a preferred interval for backup execution.
- 7. Click Backup Source and Exclusion tab and configure the same accordingly.
- 8. Click **Backup Location** tab, select the appropriate option to save the backup file.
- 9. Click Save.

The Backup Set will be created.



Edit Backup Set To edit a Backup Set:





- 1. Select a Backup Set.
- 2. Click Edit Backup Set.
- 3. After making the necessary changes, click **Save**. The Backup Set will be edited and saved.

Delete Backup Set

To delete a Backup Set:

- 1. Select a Backup Set.
- 2. Click **Delete Backup Set**. A confirmation prompt appears.
- 3. Click **OK**. The Backup Set will be deleted.





Configuring eScan Policies for Linux and Mac Computers

eScan lets you define settings for File Anti-Virus, Endpoint Security, On Demand scanning and Schedule Scan module for Linux and Mac computers connected to the network. Click **Edit** to configure the eScan module settings for computers with respective operating systems.

File Anti-Virus 🗙 🎬 Assign From Select Policy	Edit	EndPoint Security 👧 🌇 Edit	
On Demand Scanning 👧 🎬	Edit	Schedule Scan 👧 🎬 Edit	
Schedule Update 🙇	Edit	Administrator Password A Edit Assign From Select Policy	
Web Protection Assign From Select Policy	Edit	Network Security Edit Assign From Select Policy	

Icons next to every module displays that the settings are valid for the respective operating systems only.

It lets you define settings for Scanning; you can also define action to be taken in case of an infection. It also lets you define the number of days for which the logs should be kept as well as create list for Masks, Files or Folders to be excluded from scanning.

0

NOTE





File Anti-Virus

n the case of an infection:	Disinfect (if not possible, quarantine) 🗸	
	Scan Settings	
🗌 Archives 👧 😃	🗌 Mails 😃	
🗹 Packed 👧 🏨	🗌 Cross file system 👧	
🗌 Follow symbolic links 👧		
Display attention messages		
umber of days log should be k	ept 365	
🗌 Exclude by mask 🌋		
	Add	
	Delete	
	RemoveAll	
	·	
🗌 Exclude Files / Folders 👧 些		
🗠 Exadae mes y roideis 👧 🔤	Add	
	Delete	
	RemoveAll	٦,
Add Directory for realtime so	an 🗖	
	bbA	
/home	Delete	
/tmp	RemoveAll	ה

Actions in case of infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection.

File	e Anti-Virus 👧 🖺		
	In the case of an infection:	Disinfect (if not possible, quarantine) 🔻	
		Log only Disinfect (if each an arithm land)	
		Disinfect (if not possible, log) Disinfect (if not possible, delete file)	
	📃 Archives 👧 🏨	Disinfect (if not possible, quarantine)	
		Delete	
	🗹 Packed 👧 🖺	Quarantine	
	📃 Follow symbolic links 👧		





By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- Log Only: This option indicates or alerts the user about the infection detected (No Action is taken; only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** This option deletes the infected object.
- Quarantine: This option quarantines the infected object.

Scan Settings

- **Mails** It indicates scanning the mail files. By default, it is selected. Select this checkbox if you want eScan real-time protection to scan mails.
- Archives It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed** It indicates the compressed executable. Select this checkbox if you want eScan realtime protection to scan packed files.
- Cross File System that facilitates scanning of files over cross-file systems.
- Follow Symbolic Links: scans the files following the symbolic links.

Exclude by Mask (file types) - Select this option if you want eScan real-time protection to exclude specific file extensions.

Exclude Folders and files - Select this option if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Add Directory for Real-Time Scan - If you want eScan to perform real-time scan on any of the directories add them in this list.

You can restore default eScan settings by clicking Default.





Endpoint Security

The Endpoint Security module lets you centrally manage all endpoints on your network and closely monitor all USB activities in real-time. With eScan USB control, you can prevent data theft by blocking all except your trusted USB storage devices and Stop your files from being taken away on thumb drives, iPod, mp3 players and portable USB hard drives.

Application Control

The Application Control tab allows to block the execution of application or package.

Endpoint Security	<table-cell> Help</table-cell>
● Start │ ○ Stop	
Application Control Device Control File Integrity Monitor	
Enable Application Control 🙇	
Enter Application/Package to Block	
root	
List of Blocked Applications/Packages Application/Package Name	bbA
	Delete Remove All
Default OK Cancel	

Enable Application Control

Select the checkbox to enable the application control feature.

Enter Application/Package to block

Enter the application or package name to add them in the list of application/packages blocked. To delete the application/package, select the specific app/package and click **Delete**. To delete all the application from the list, click **Remove All**.





Device Control

The Device Control tab enables you to allow/block the access to the USB devices and the CD/DVD in client computers.

	tion Control Devic	ce Control File Inte	grity Monitor	
A 🗳				
	Enable Device Control			
			Block All	Ask Password
	Use Escan Administrat		BIOCK AII	Ask Password
	Use Other Password		•••••	
Г	Blacklist			
	Block Blacklisted US	B Devices		
	Serial No.	Device Name	Description	Add
	Senar No.	Derive Herric	D'abaripatori	
	Senar No.	<u>Bene nome</u>		Import
	Senai No.			Edit
	Serial No.			
	Senar No.			Edit Delete
	Senal No.			Edit Delete RemoveAll
	<u>Serial No.</u>	<u>File Itels</u>		Edit Delete RemoveAll
	<u>Serial No.</u>			Edit Delete RemoveAll
				Edit Delete RemoveAll
	Monitor to USB		Autoscan to USB	Edit Delete RemoveAll
	Monitor to USB			Edit Delete RemoveAll
				Edit Delete RemoveAll

Enable Device Control: Select this checkbox to configure the Device Control settings.

- **USB Control**: This option lets you allow, block, or set password for the USB device connected to the endpoint. It has following options:
 - Allow All: Select this option to allow all the connected USB devices.
 - Block All: Select this option to block all the connected USB devices.
 - Ask Password: Select this option to set password for the connected USB devices. This will ask password before allowing USB devices to connect to the system. You can either set a password or use the administrator password using the options Use
 Other Password and Use Escan Administrator Password respectively.
- **Blacklist:** This option lets you add USB devices to the blacklist. You can add, delete, modify USB devices using the following options:





• Add: Use this button to enter USB serial number, name, and description of the USB devices in order to blacklist it.

×
USB Whitelist
Serial No.
Device Name
Description
Description
OK Cancel

- Import: It allows you to blacklist multiple USB devices at once using CSV file.
- Edit: It allows you to edit the details of the USB devices.
- Delete: It allows you to remove the USB device from the list.
- **Remove All**: It allows you to remove all the USB devices from the list.
- **Print**: It allows you to print the USB device list along with their details.
- Whitelist: This option lets you add USB devices to the whitelist. You can add, delete, modify USB devices using the following options:
 - Add: Use this button to enter USB serial number, name, and description of the USB devices in order to whitelist it.

	×
USB Whitelist	
Serial No.	
	1
Device Name	1
Description	1
]
OK Cancel	

- Import: It allows you to whitelist multiple USB devices at once using CSV file.
- Edit: It allows you to edit the details of the USB devices.
- **Delete**: It allows you to remove the USB device from the list.
- **Remove All**: It allows you to remove all the USB devices from the list.
- **Print**: It allows you to print the USB device list along with their details.
- **Monitor to USB:** Select this checkbox to monitor all the USB devices connected to the endpoints.
- Autoscan to USB: Select this option to auto-scan all the USB devices connected to the endpoints.





CD/DVD Settings

This option lets administrator to block, allow, and disable the CD/DVD settings. You have following options to configure:

- Block CD/DVD: This option blocks CD/DVD inserted in the computer.
- **Read Only CD/DVD:** This option allows limited (only reading) access to the user for the data stored in inserted CD/DVD.
- **Disable:** This option disables the configured settings for CD/DVD.

File Integrity Monitor

Endpoint Security	🝸 Help			
Start O Stop				
Application Control Device Control File Integrity Monitor				
Enable FIM 👧				
File Integrity Check Alert Create New Baseline				
Enter Directory Name				
	Add			
Directories Name	Delete			
/lib	Remove All			
/etc				
/bin				
/sbin				
Default OK Cancel				

Enable FIM

Select this checkbox to enable the File Integrity Monitor option.

- **File Integrity Check Alert**: This checkbox will check the file integrity and alert the admin accordingly.
- **Create New Baseline**: This checkbox will create a baseline for the selected directories and the FIM will begin monitoring changes for the selected directories.

Enter Directory Name

Enter the directory name to add it to the integrity monitoring.

You can also select the directory name from the pre-defined list in the below table to add them to monitoring.

To delete a specific directory from monitoring, select the directory, and click **Delete**.

To remove all the directory from monitoring, click Remove All.

Default

This button will reset all the settings of the window to their default values.





ODS Settings

With ODS Settings you can define actions in case of infection, you can also define list of files by mask, Files or Folders to be excluded from Scanning. It also lets you configure settings for various other Scan options like Include Sub directories, Mails, Archives Heuristic Scanning etc. by selecting respective options.

In the case of an infection:	Disinfect (if not possible, quarantine) 🗸
Priority of scanner:	Normal (normal runtime) 🗸
Exclude by mask	
	Add
	Delete
	RemoveAll
Exclude Files / Folders	
	Add
	Delete
	RemoveAll
Scan Options	
Include sub directories	Mails
Heuristic	Archives
Cross filesystem	Packed
Follow symbolic links	Memory Scan

Actions in the case of infection [Drop-down]

It indicates a type of action which you want eScan real-time protection to take, in case of virus detection.

In the case of an infection:	Disinfect (if not possible, quarantine) 🗸
Priority of scanner:	Log only Disinfect (if not possible, log)
<u> </u>	Disinfect (if not possible, delete file)
Exclude by mask	Disinfect (if not possible, Rename File) Disinfect (if not possible, quarantine) Delete Infected File
	Rename Infected File
	Quarantine

By default, Disinfect (if not possible, quarantine file) option is selected. Following actions can be taken:

• Log Only: It indicates or alerts the user about the infection detected.





- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, Rename file):** It tries to disinfect and if disinfection is not possible it renames the infected object.
- **Disinfect (if not possible, quarantine):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- Delete Infected File: It deletes the infected object.
- Rename Infected File: It renames the infected object.
- Quarantine: It quarantines the infected object.

Priority of Scanner – You can select the priority of scanning as **High (short runtime)**, **Normal (normal runtime)**, or **Low (long runtime)**.

- **High (short runtime)** Has a short runtime.
- Normal (normal runtime) Has a normal runtime.
- Low (long runtime) Has a long runtime.

Exclude by Mask – Select this checkbox if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.

Exclude Files / Folders – Select this checkbox if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required during On Demand Scanning.

Scan options

- **Include Sub Directories [Default]** This option ensures eScan scans all the sub directories recursively under every directory and not only the first level of directories.
- **Heuristic [Default]** Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- Cross File System that facilitates scanning of files over cross-file systems.
- Follow Symbolic Links scans the files following the symbolic links.
- **Mails** It indicates scanning the mail files. Select this checkbox if you want eScan real-time protection to scan mails.
- Archives [Default] It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed** [**Default**] It indicates the compressed executable.
- **Memory / Services [Default]** This option ensures eScan scans the system's memory for any infection from malwares.

You can restore default eScan settings by clicking Default.





Schedule Scan 🙆 🛎

	Scan 👧 🖺		👔 Help
	Name	Schedule Type Schedule On	
	Clear All	Add task Delete task Edit	
Sav	e Cancel		

It lets you add a task for scheduling a scan.

Adding a task - It lets you schedule and define options for Analysis extent and the files or folders to be scanned.

Automatic Virus Scan

Schedule

Schedule Analysis extent Virus scan
Execute Once Hourly Daily
 Once Weekly Hourly Monthly Daily
O Hourly O Monthly O Daily
O Daily
Date and time
Month : 4 💙 Date : 21 💙 12:00 pm 🕑 🖤





Using this tab you can define the task name and schedule it as desired. You can schedule the scan once, weekly basis, every hour, monthly or daily. It also lets you schedule virus scan at desired date and time.

Analysis Extent

	🔀 🔽 Help
Automatic virus scan	
Schedule Analysis extent Virus scan Scan Options Include sub directories Include sub directories Heuristic Cross filesystem Follow symbolic links 	 Mails Archives Packed Memory Scan
Save Cancel	

Using this tab you can define the scan options for Linux and Mac computers connected to the network.

- **Include sub Directories [Default]** This option lets you include sub directories while conducting an automatic scan.
- **Heuristic Scan [Default]** Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- Cross File System facilitates scanning of files over cross-file systems.
- Follow symbolic links scans the files following the symbolic links.
- **Mails** It indicates scanning the mail files. By default, it is selected. Select this checkbox if you want eScan real-time protection to scan mails.
- Archives [Default] It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed [Default]** It indicates the compressed executable. Select this checkbox if you want eScan real-time protection to scan packed files.
- Memory / Services [Default] This option will only scan the memory of the system.





Virus Scan

me	
Schedule Analysis extent Vin	us scan
In the case of an infection: 👧 监	Disinfect (if not possible, quarantine) 💙
Priority of scanner: 👧 🖺	Normal (normal runtime)
🗌 Exclude by mask 👧 🏨	
	Add
	Delete
	RemoveAll
🗌 Exclude Files / Folders 👧 💃	
	Add
	Delete
	RemoveAll

Actions in case of Infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection. By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- Log Only: It indicates or alerts the user about the infection detected.
- Delete Infected File: Infected objects are deleted with this option.
- Rename Infected File: This option allows you to rename the infected files.
- Quarantine: Infected objects are quarantined with this option.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Disinfect (if not possible, Rename file):** It tries to disinfect and if disinfection is not possible it renames the infected object.





Exclude by Mask - Select this checkbox if you want eScan real-time protection to exclude specific files, and then add the directories and files that you want to exclude by clicking **Add**. eScan lets you Remove any or all Added Files whenever required.

Exclude Files / Folders - Select this checkbox if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Schedule Update (1)

This module lets you schedule the updates for Linux computers.

dule Update		?
- O Automatic D Start at	12:00 pm OV Every 1 V hours(s)	
- 🔍 Schedule Do	wnload	
Once	O Weekly	
O Hourly	O Monthly	
O Daily		
Date and time Month : 1	♥ Date : 1 ♥ 12:00 AM	
Default	Ok Cancel	

- The updates can be downloaded automatically with Automatic Download option.
- The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.





Administrator Password **(A)**

Administrator Password lets you create and change password for administrative login of eScan protection center for Linux computers. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password. It also lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password.

hange Password	
eScan Password	
O Set Password	Blank Password
Enter new Password	
Confirm new Password	
Password is case-sensitive	
Use separate uninstall password Enter uninstall password	
Confirm uninstall password	
efault OK Cancel	

To Add/Change eScan administrator password:

Set Password

Click this option, if you want to set password.

Blank Password

Click this option, if you do not want to set any password for login. When you click this option, the **Enter new Password** and **Confirm new Password** fields become unavailable.

Enter new Password

Enter the new password.

Confirm new Password Re-enter the new password for confirmation.

Use separate uninstall password

Click this option, if you want to set password before uninstallation of eScan Client.

Enter uninstall Password

Enter the uninstallation password.

Confirm uninstall Password

Re-enter the uninstallation password for confirmation.





After filling all fields, click **OK**. The Password will be saved.

Web Protection

Web Protection module lets you block websites containing pornographic or offensive material for Linux computers. This feature is extremely beneficial to parents because it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours. You can configure the following settings:

Start/Stop

It lets you enable/disable Web-Protection module. Click the appropriate option.

Start 🖲 Stop			
Allow O Block		<u> </u>	
Filter Categories	📕 Allow 📕 Block	Site Names	
Category Name	Туре		-
Pornography	Block T		
Gambling	Block V		
Alcohol	Block V		
Violence	Block V		
Drugs	Block V		
Ratings block category	Block 🔻 🔻		-
Add Delete		Add Delete Save	
		_ [

You can configure the following settings.

Filtering Options

This tab has predefined categories that help you control access to the Internet.

Status

This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as **Active** or **Block** web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, only **Filtering Options** and **Pop-up Filter** tabs are available.

Filter Categories

This section uses the following color codes for allowed and blocked websites.

• Green: It represents an allowed websites category.





• **Red**: It represents a blocked websites category.

The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings block category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

Category Name

This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.





Network Security

Network Security module helps to set Firewall configuration to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. It also prevents the Reverse Shell Exploits and blocks the Port Scan. Enabling this features will prevents Zero-day attacks and all other cyber threats.

Network Security 🧕			👔 Help		
FireWall Reverse Shell Block Port Scan					
O Allow All Imited Filter O Interactive Filter Zone Rule Expert Rule Trusted MAC Address	Local IP List				
Name	IP Address/Host Name	Туре	Zone		
Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted		
Add IP Add IP Range Mod	dify Remove				
Enable Trojan Rule					
Default Save Cancel					





Firewall

This tab is designed to monitor all incoming and outgoing network traffic and protect your endpoint from all types of network based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list.

Network Security 👰			👔 Help			
FireWall Reverse Shell Block Port Scan						
O Allow All O Limited Filter O Interactive Filter						
Zone Rule Expert Rule Trusted MAC Address	Local IP List	(
Name	Name IP Address/Host Name Type Zone					
Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted			
Add IP Add IP Range Modify Remove						
Add IP Add IP Range Mo	dify Remove					
Default Save Cancel						

You can configure the following settings to be deployed to the eScan client systems. Allow All – Clicking Allow All disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

Limited Filter – Clicking **Limited Filter** enables eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Interactive – Clicking **Interactive** enables eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Following tabs are available:

- Zone Rule
- Expert Rule
- Trusted MAC Address
- Local IP List

Zone Rule

This is a set of network access rules to make the decision of allowing/blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked. The following buttons are available for configuring zone rule:

- Add IP This option lets you add an IP address of a system to be added in the zone rule. After clicking Add IP, enter the IP address of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click OK to create the Zone Rule.
- Add IP Range This option lets you add an IP range to be added in the zone rule. After clicking Add IP Range, add the IP Range (i.e. a range of IP that the zone rules should be





applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

- **Modify** To modify/change any listed zone rule(s), select the zone rule to be modified and then click **Modify**.
- **Remove** To remove any listed zone rule(s), select the zone rule and then click **Remove**.

Expert Rule

This tab lets you specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source IP address and port, destination IP address and port, and ICMP types. You can create new expert rules.

) aii	Wall Reverse Si low All Limi Rule Expert	ited Filter O Inte	ractive Filter	ist			
	Firewall Rule				Rule Action Summary	^	
	UDP Rule				Permits UDP packets on Any Interface betwee	n "1	
	ARP packet exchange - For mapping IP address to a hardware (MAC) address				Permits ARP packets on Any Interface		
	NetBios (LAN File Sh	aring) - Access files and t	s, from your computer	Permits TCP and UDP packets on Any Interface be			
	NetBios (LAN File Sh	aring) - Access files and t	Blocks TCP and UDP packets on Any Interface bet				
	ICMP messages				Permits ICMP packets on Any Interface between "		
	ICMPV6 messages				Permits ICMPV6 packets on Any Interface betwee		
	DHCP/BOOTP packet exchange				Permits UDP packets on Any Interface between "A		
	FTP Control - For do	wnloading and uploading	files		Permits TCP packets on Any Interface betwee	n "N -	
	Add Enable	Modify Disable	Remove	Shift up	Shift down		
	able Trojan Rule						

However, configure these rules only if you are familiar with firewalls and networking protocols.

- Source IP Address/Host Name
- Source Port Number
- Destination IP Address/Host Name
- Destination Port Number

The following buttons are available to configure an Expert Rule:

1. Add – Click Add to create a new Expert Rule. In the Add Firewall Rule Window:





(Add Firewall Rule
General Source Destination Advanced
Rule Name Rule 1 Rule Action Image: Permit Packet O Deny Packet
TCP and UDP Apply Rule on Interface Any Interface
OK Cancel

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

Protocol – Select the network protocol (e.g. TCP, UDP, ARP) on which the Rule will be applied.

Apply rule on Interface – Select the Network Interface on which the Rule will be applied.





Source tab

In this section, specify/select the location from where the outgoing network traffic originates.

	×
Firewall Rule	
General SOURCE Destination Advanced	
Source IP Address	
O My Computer	
O Single IP Address	
O Whole IP Range	
O Any IP Address	
My Network	
Source Port	
Any	
○ Single Port	
O Port Range	
O Port List	
OK Cancel	

Source IP Address:

My Computer – The rule will be applied for the outgoing traffic originating from your computer.

Single IP Address – The rule will be applied for the outgoing traffic originating from the computer as per the IP address specified.

Whole IP Range – To enable the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the outgoing traffic from the computer(s) which is within the defined IP range.

Any IP Address – When this option is selected, the rule will be applied for the traffic originating from ANY IP address.

My Network – The rule will be applied for the outgoing traffic to the networked computer(s).

Source Port:

Any – When this option is selected, the rule gets applied for outgoing traffic originating from any port.

Single Port – When this option is selected, the rule gets applied for the outgoing traffic originating from the specified/defined port.

Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.





Port List – A list of port can be specified. The rule will be applied for the outgoing traffic originating from the ports as per specified in the list.

•	The rule will be applied when the selected Source IP Address and Source Port matches
NOTE	together.

Destination tab

In this section, specify/select the location of the computer where the incoming network traffic is destined.

Destination IP Address:

My Computer – The rule will be applied for the incoming traffic to your computer.

Single IP Address – The rule will be applied for the incoming traffic to the computer as per the IP address specified.

Whole IP Range – To apply the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the incoming traffic to the computer(s) which is within the defined IP range.

Any IP Address – When this option is selected, the rule will be applied for the incoming traffic to ANY IP Addresses.

My Network – The rule will be applied for the incoming traffic to the networked computer(s).

Destination IP Port:

Any – After selecting this option, the rule will be applied for the incoming traffic to ANY port.

Single Port – After selecting this option, the rule will be applied for the incoming traffic to the specified/defined port.

Port Range – To enable the rule on a group of ports in series, you can specify a range of ports.

Port List – A list of port can be specified/added. The rule will be applied for incoming traffic originating from the ports as per specified in the list.

The rule will be applied when the selected Destination IP Address and Destination Port matches together.

Advanced tab

This tab contains advance setting for Expert Rule.





eneral Source Destination Advanced		
Enable Advanced ICMP Processing - ICMP Type		
	In	Out
Destination Unreachable		
Echo Reply (ping)		
Echo Request (ping)		
Information Reply		
Information Request		
Parameter Problem		
Redirect		
Source Quench		
TTL Exceeded		
The packet must be from/to a trusted MAC address		

Enable Advanced ICMP Processing - This is activated when the ICMP protocol is selected in the General tab.

The packet must be from/to a trusted MAC address – When this option is selected, the rule will only be applied on the MAC address defined/listed in the Trusted MAC Address tab.

Use the following buttons in this tab as and when required:

Modify - Clicking Modify lets you modify any Expert Rule.

Remove – Clicking Remove lets you delete a rule from the Expert Rule.

Shift Up and Shift Down– The UP and DOWN arrow button will enable to move the rules up or down as required and will take precedence over the rule listed below it.

Enable Rule/Disable Rule – These buttons lets you enable or disable a particular selected rule from the list.

Trusted MAC Address

This section contains the information of the MAC address of the system. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the *Advance Tab* of the Expert Rule). The following buttons are available to configure the Trusted Mac Address:





- Add To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-
- **Edit** To modify/change the MAC Address, click **Edit**.
- **Remove** To delete the MAC Address, click **Remove**.
- Clear All To delete the entire listed MAC Address, click Clear All.

Local IP List

This section contains a list of Local IP addresses.

Network Security 👧	_? Help
FireWall Reverse Shell Block Port Scan	
O Allow All Limited Filter	
Zone Rule Expert Rule Trusted MAC Address Local IP List	
FE80:0000:0000:0000:0000:0000	
192.168.*.* 127.*.*	
Add Remove Clear All	
Enable Trojan Rule	
Default Save Cancel	

Add – To add a local IP address, click Add.

Remove – To remove a local IP address, click **Remove**. **Clear All** – To clear all local IP addresses, click **Clear All**.

Enable Trojan Rule

Select this checkbox, to enable the Trojan Rule.





Reverse Shell

This tab allows you to block the reverse shell attacks by blocking the script languages that the attackers use to initiate remote shell connection with the networked endpoint.

Wall Reverse Shell Block Port Scan	
Start 💿 Stop	
Enable White List	
	Add
bash	Delete
python	RemoveAll
perl	_
Enable Black List	
Enable Black List	Add
apache	Delete
apache2	RemoveAll
httpd	
httpd	
httpd	

Start/Stop

It allows you enable/disable Network Security module.

After enabling this, you can configure the following settings:

Enable White List

Select this checkbox to whitelist the trusted script languages, such as bash, Python, Perl, and more. You can add and delete the script languages from whitelisting.

- Add: To add a script language, select the language and click Add.
- Delete: To delete a script language, select a language and click Delete.
- Remove All: To remove all the whitelisted script language, click Remove All.

Enable Black List

Select this checkbox to blacklist the untrusted and risky script languages.

- Add: To add a script language, select the language and click Add.
- **Delete**: To delete a script language, select a language and click **Delete**.
- Remove All: To remove all the blacklisted script language, click Remove All.





Block Port Scan

This tab allows admin to configure the port scan option.

vork Security 👰	👔 Help
ireWall Reverse Shell Block Port Scan	
Enable Block Port Scan	
Excluded IP(Port Scan) Add	
Delete	
RemoveAll	
Default Save Cancel	

Enable Block Port Scan

Select this checkbox to enable the port scan option. You can add and delete the IP addresses that need to exclude from the port scan.

- Add: To add an IP, enter the IP address and click Add.
- Delete: To delete an IP, select the IP address and click Delete.
- Remove All: To remove all the excluded IP addresses, click Remove All.





Assigning Policy Template to a group

There are two ways to assign the policy template to group:

Method 1

To assign a Policy to a group:

- 1. In the Managed Computers screen, click **Policy Templates**. Policy Templates window appears.
- 2. In the **Policy Templates** window, select a policy template.

Polic	y Templates				🗢 Refresh 🛛 👔 Help
	New Template	perties 📄 Delete 🛃 Assign to (Group(s) Assign to Computer(s) Copy Template	
	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
	app block	Mar 22 2023 05:23:03 PM	Jun 18 2024 02:30:28 PM		DESKTOP-7MDM370
	Block All	Jul 30 2024 01:31:47 PM	Jul 30 2024 02:04:09 PM	Trail	
	Cloud Test	Aug 08 2023 04:45:49 PM	Jan 04 2024 03:53:59 PM		

3. Click **Assign to Group(s)**.

Select Group window appears.

ct Group	Help
Ē. □ 🔚 Managed Computers	
Ok Cancel	

4. Select the group(s) and then click **OK**.The policy will be assigned to the selected group(s).





Assigning Policy Template to Computer(s)

To assign a policy template to computers:

1. In the **Policy Templates** window, select a policy.

Polic	y Templates				🗢 Refresh	🝸 Help
•	New Template	perties 📄 Delete 🛃 Assign to 0	Group(s) Assign to Computer(s) Copy Template		
	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)	^
	app block	Mar 22 2023 05:23:03 PM	Jun 18 2024 02:30:28 PM		DESKTOP-7MDM370	
	Block All	Jul 30 2024 01:31:47 PM	Jul 30 2024 02:04:09 PM	Trail		
	Cloud Test	Aug 08 2023 04:45:49 PM	Jan 04 2024 03:53:59 PM			

- 2. Click Assign to Computer(s).
- 3. Assign Template to computer window appears.

	t Group	Help
6	±. 🗌 🧰 Managed Computers	
	Ok Cancel	

- 4. Click Managed Computers.
- Select the computer(s) and then click **OK**.
 The policy template will be assigned to the selected computers.





Copying a Policy Template

To copy a Policy Template:

1. In the Policy Templates window, select a policy.

Polic	y Templates				💲 Refresh 🛛 👔 He
	New Template	perties 📄 Delete 🛃 Assign to (Group(s) Assign to Computer(s	:) Copy Template	
	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
	app block	Mar 22 2023 05:23:03 PM	Jun 18 2024 02:30:28 PM		DESKTOP-7MDM370
	Block All	Jul 30 2024 01:31:47 PM	Jul 30 2024 02:04:09 PM	Trail	
	Cloud Test	Aug 08 2023 04:45:49 PM	Jan 04 2024 03:53:59 PM		

2. Click Copy Template.

New Template window appears displaying settings from the original template.

- 3. Enter a name for the template.
- 4. Make the necessary changes and then click **Save**. The template will be copied.





Report Templates

The Report Templates module lets you create template and schedule them according to your preferences. The module also consists of pre-loaded templates according to which the report can be created and scheduled.

Report Templates	💲 Refresh	👔 Help
Template Create Schedule Properties		
Template Name		
🗌 Virus Report 🚎 👧 🎬		
Update Report 🚎 👧 🌇		
🗌 Scan Report 🟭 👧 🌇		
🗌 Web Protection Report 🚛 👧		
Application Control Report		
Attachment Control Report		
Anti-Spam Report		
Aiil Anti-Virus Report		
🗌 USB Control Report 📬 🏚 🎬		
🗌 Group Summary Report 🚎 👧 🎬		
🗌 Hardware Report 📪 👧 🏨		
🗌 Software Report 🏭 🙇 🎬		
File Activity Report		
🗌 Computers with Critical Status Report 🚎 👧 🌇		
🗌 Asset Changes (Software) Report 🚛 👧 🎬		
🗌 Asset Changes (Hardware) Report 🌉 👧 🎬		
🗌 Top 10 Summary Report 🏣 👧 🎬		
🗌 Top 10 Summary Report 🏭 👧 📓		





Creating a Report Template

To create a Report Template, follow the steps given below:

- 1. In the navigation panel, click **Report Templates**.
- 2. Click **New Template**. New Template screen appears.

ate Name		
New Template Name :* New Template		
t Template		
Report Type	0	
🔍 Virus Report 🚝 👧 🎬	🔾 Anti-Spam Report 📫	
🔿 Update Report 🚝 👧 🎬	🔾 Mail Anti-Virus Report 🚝	
🔿 Web Protection Report 🚝 👧	🔿 USB Control Report 🚝 👧 🎬	
🔿 Group Summary Report 🟭 🙇 🎉	🔿 Application Control Report 🚛	
🔿 Hardware Report 🚛 👧 🎉	🔿 Attachment Control Report 🚝	
🔿 Scan Report 💶 👧 🏨	🔿 Software Report 🚛 👧 🎬	
🔿 Computers with Critical Status Report 💶 👩 🎉	🔿 File Activity Report 🚝	
🔿 Asset Changes (Hardware) Report 💶 🙍 🕵	🔿 Asset Changes (Software) Report 👥 🙍 🌋	
	🔿 Top 10 Summary Report 🏭 💁 些	
Period & Sort By Date Options Today This Month Since Installed Last Month	 This Week This Year Date Range 	
Sort By		
	O Virus	
Sort By	○ Virus ○ Action Taken	
Sort By		
Sort By Date Computer		

- 3. Enter a name for the template.
- 4. Select a report type.

Depending upon the report type, the additional setting varies.

5. After making the necessary selections/filling data, click **Save**. The template will be created according to your preferences.

Creating Schedule for a Report Template

The Report Template module lets you create a new schedule for the report templates. To learn more, <u>click here</u>.

Viewing Properties of a Report Template

To view the properties of Report Template, follow the steps given below:

- 1. Select the Report Template whose properties you want to view.
- 2. Click Properties. Properties screen appears.





Propertie	5			🝸 Hel
<u>Report Ten</u>	<u>mplates</u> > sample Properties			
Ge	eneral Report Period 8	k Sort By		
	Report Name			
	Report Name :	sample		
	Details			
	Selected Template Type:		100010000000000000000000000000000000000	
	Created:		5/29/2020 1:40:10 PM	
	Modified:		5/29/2020 1:40:10 PM	
<u> </u>				



Depending upon the Report Template enter, the Properties varies.

3. After making the necessary changes, click **Save**. The Report Template's properties will be updated.

Deleting a Report Template

To delete a Report Template, follow the steps given below:

- 1. Select the template you want to delete.
- 2. Click **Delete**. A confirmation prompt appears.
- 3. Click **OK**. The Report Template will be deleted.



Default Report Templates cannot be deleted.





Report Scheduler

The Report Scheduler module lets you create schedule, update and run the task according to your preferences.

Creating a Schedule

To create a Schedule:

1. In the Report Scheduler screen, click **New Schedule**. New Schedule screen appears.

<u>sport Scheduler</u> > New Schedule				
Report Name				
New Report Name :* New Report_1				
Settings				
Select a Template for creating a Report Image: Constraint of the selection Report				
🕑 🗌 Software Report 📫 👧 🎽	•			

- 2. Enter a name for the report.
- 3. In the Settings section, select preferred templates.
- 4. In the Select Condition section, select a condition for groups or specific computers.

Select Condition Generate a Report for Groups Generate a Report for a List of Computers
Select Target Groups
🗄 🗆 🥁 Managed Computers

5. In the Send Report by email section, fill the required information to receive reports via email.





Report Sender*:		
Report Recipient*:		Add
		Delete
Mail Server IP Address:		
Mail Server Port:	18	
User Authentication:	1011100	
Password Authentication:		
* For Example: user@your	company.com	
lect the Report Format		

- 6. Select the preferred report format.
- 7. In Report Scheduling Settings section, make the necessary changes.

Enable Scheduler	O Manual Start
Daily	
O Weekly	Mon Tue Wed Thu
	Fri Sat Sun
O Monthly	1 🗸
◯ Last Day of Month	

8. Click Save.

New schedule will be created.





Viewing Reports on Demand

To view a report or a set of reports immediately:

- 1. Click **Report Scheduler** > **View & Create**.
 - New Schedule screen appears.

New Schedule	👔 Help
Report Scheduler > New Schedule	
Settings	
Select a Template for creating a Report	
 Virus Report Web Protection Report Date Computer Websites Action Taken Anti-Spam Report Mail Anti-Virus Report Application Control Report USB Control Report Ugdate Report Group Symmary Report 	
 Generate a Report for Groups Generate a Report for a List of Computers Select Target Groups 	
Managed Computers Managed Computers Roaming Users Di Di	
Create Schedule Cancel View	ory Fields

- 2. Select the **Template** options, the **Condition** and the **Target Groups**.
- 3. Click View.
- 4. A new window appears displaying the created report.

Clicking Create Schedule lets you create a new Schedule.

Managing Existing Schedules

The Report Scheduler module lets you manage the existing schedules.

	Report Scheduler					
D	Start Task 🛛 🕞 Results 🔐 Properties 😭 Delete	New Schedule View & Create				
	Schedule Name	Report Recipient	Scheduler Type			
	Hardware	1000.000	Manually Start			
	New Report	ALTERNATION OF ALLER AND ALL AND AL	Manually Start			
	New Report_1		Automatic Scheduler			





Generating Task Report of a Schedule

To generate a task report, select the preferred report schedule name and then click **Start Task**. A task window appears displaying the name of the report being generated.

Viewing Results of a Schedule

To see the results of a schedule and its time stamp, select the report schedule and then click **Results**. Results screen appears.

Results(Hardware)				
Report Scheduler >Results				
Status	<u>Time</u>			
Completed	9/21/2019 12:25:25 PM			
Cancel				





Viewing Properties of a Schedule

To view the properties of a schedule:

- 1. Select a schedule.
- 2. Click **Properties**.

Properties screen appears.

Schedule Name :* New Report Created: 07/27/20 08:01:59 PM Status: Task Completed	perties		
Created: 07/27/20 08:01:59 PM	General Schedule Set	ings Groups	
Created: 07/27/20 08:01:59 PM			
	Schedule Name :*	New Report	
Status: Task Completed	Created:	07/27/20 08:01:59 PM	
	Status:	Task Completed	
	Status:	Task Completed	
	Ok Cancel		(*) Mandatory Fi

The properties screen displays general properties and lets you configure Schedule, Settings and Groups settings.

Deleting a Schedule

To delete a report schedule:

- 1. Select a schedule.
- 2. Click **Delete**.

A confirmation prompt appears.

	×
F	Report Scheduler
	Do you want to Delete the Selected Task(s) ?
[Ok Cancel

3. Click OK.

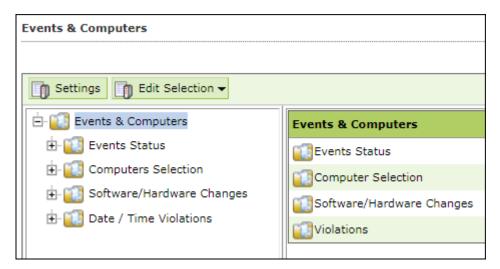
The schedule will be deleted.





Events and Computers

eScan Management Console maintains the record of all the events sent by the client computer. Through the events & computers module, the administrator can monitor the Events and Computers; the module lets you sort the computer with specific properties.



Events Status

The Event Status subfolder is divided into following sections:

- Recent
- Critical
- Information

Recent

The Recent section displays both Information and Critical events.

Critical 😂

The Critical section displays Critical events and immediate attention.

For example, Virus detection, Monitor disabled.

The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

Information 🕕

The Information section displays basic information events. For example, Virus database update, Status.





Computer Selection

The Computer Selection subfolder displays computers that fall under different categories. It lets you select the computer and take the preferred action. You can also set the criteria for each section and sort the computer accordingly.

Settings Edit Selection -	
🗄 🛄 Events & Computers	Computer Selection
🗄 🔃 Events Status	Computers with the "Critical Status"
Computers Selection	Computers with the Live Status
Critical Status Warning Status	Computers with the "Warning Status"
- 🚺 Database are Outdatedd	🔝 Database are Outdated
Many Viruses Detected	🔝 Many Viruses Detected
No eScan Antivirus Installed Not Connected for a long time	🔝 No eScan Antivirus Installed
- 📜 Not Scanned for a long time	12 Not Connected for a long time
	Dot Scanned for a long time
	Protection is off
	[Update Agent Status

The Computer Selection subfolder consists following sections:

- Computers with "Critical Status"
- Computers with "Warning Status"
- Database are Outdated
- Many Viruses Detected
- No eScan Antivirus Installed
- Not Connected for a long time
- Not Scanned for a long time
- Protection is off
- Update Agent Status

This section displays computers marked with Critical status.

Computers with critical status

This section displays computers marked with Critical status.

Computers with warning status

This section displays computer with a warning status.

Database are Outdated

This section displays computers whose virus database is outdated.

Many Viruses Detected

This section displays the computers whose virus count has exceeded.

No eScan Antivirus Installed





This section displays computers on which eScan is not installed.

Not connected for a long time

This section displays the computers which didn't connect to the eScan server for the set duration.

Not scanned for a long time

This section displays the computers which weren't scanned for the set duration.

Protection is off

This section displays the computers on which File Protection is disabled.

Update Agent Status

This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

Edit Selection

This drop-down menu allows to configure various option based on selected options. The following options are present in the menu:

• **Protection**: This option displays the protection status of the selected computer.

	×
Protection	Help
Computers Status Online	
Protection is off	
4	•
Close	

• Events: This option displays the events that were performed in particular computer.

Events & Computers								
Recent Events								
Date	<u>Time</u>	<u>User's name</u>	<u>Event Id</u>	Module Name	Description			
1 23-Jun-21	12:39:48	Account(Sapral)Sapra	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487			
1 23-Jun-21	12:38:57	Account(Sapra)(Sapra	Endpoint Security (102)	eScan EPS	Executable launched.			
1 23-Jun-21	12:29:48	Account(Sapra)(Sapra	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487			
1 23-Jun-21	12:19:49	Account(Sapra)(Sapra	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487			
1 23-Jun-21	12:09:49	Account/Dapral/Dapra	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487			
1 23-Jun-21	11:59:48	Account(Sapral/Sapra	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487			
1 23-Jun-21	11:49:49	Account/Dapral/Dapra	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487			
1 23-Jun-21	11:42:19	Account(Sapra)(Sapra	File Anti-Virus (1752)	eScan Monitor	QBMsgMgr Module			

- **Deploy/Upgrade Client**: To learn about this option, <u>click here</u>.
- Check Connection: This option will verify if the client machine is online or offline.





Connecting to Computer Connection : Successful

- **Remove from Group**: To learn about this option, <u>click here</u>.
- Force Download: To learn about this option, <u>click here</u>.
- On Demand Scanning: To learn about this option, <u>click here</u>.
- Send Message: To learn about this option, <u>click here</u>.
- **Properties**: To learn about this option, <u>click here</u>.

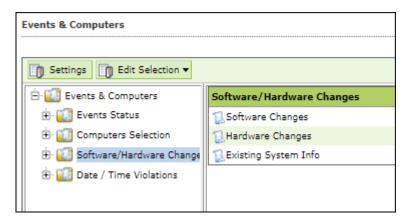




Software/Hardware Changes

This subfolder displays all software/ hardware changes that occurred on computers. It consists following sections:

- Software Changes
- Hardware Changes
- Existing System Info



Software Changes

This section displays software changes i.e. installation, uninstallation or software upgrades.

Hardware Changes

This section displays hardware changes that occurred on computers. For example, IP address. Hard Disk, RAM etc.

Existing System Info

This section displays a computer's existing hardware information.





Violations

Date/Time Violations

This subfolder consists Date/Time Violations that displays client computers whose users attempted to modify date and time.

vents & Computers								📚 Refresh	_? Helj
👔 Edit Selection 👻									
Events & Computers	Filter Criteria Export Option								
⊡ 🔃 Events Status ⊡ 🔃 🚺 Computers Selection	e / Time Violations Events 1 - 9 of 9 H page 1 of 1 H Rows per page: 10 V								
🗄 🔃 Software/Hardware Changes	<u>ite</u>	<u>Time</u>	Machine Name	IP Address	<u>User name</u>	Event Id	Module Name	Description	
12 Software Changes 12 Hardware Changes	3/6/2018	15:58:18	COMPLEX 💼	192.148/0.108	COMPLEXIV	File Anti-Virus (1801)	eScan Monitor	Date/Time Modification Disa	bled
) 3/6/2018	15:58:04	COMPLEX 📫	192.148.0.108	COMPLEXIV	File Anti-Vinus (1804)	eScan Monitor	Date/Time Modification Disa	bled
🗄 🔃 Violations) 3/6/2018	15:58:02	COMPLEX 1	192.148.0.108	COMPLEXIV	File Arth-Virus (1804)	eScan Monitor	Date/Time Modification Disa	bled
🛄 🔂 Date / Time Violations) 3/6/2018	14:50:16	WEA21217	192.148.7.84	MER237/com	File Anti-Virus (1885)	eScan Monitor	Date/Time Modification Disa	bled
	3/6/2018	12:30:35	WEADER	192.148/0.217	MERDER/Eur	File Anti-Virus (1805)	eScan Monitor	Date/Time Modification Disa	bled
) 3/6/2018	12:30:15	WEADER	192.148.7.79	MERGERYCH	File Anti-Virus (1801)	eScan Monitor	Date/Time Modification Disa	bled
	3/6/2018	12:30:15	WEADER I	192.148.7.79	WEALTH	File Anti-Virus (1801)	eScan Monitor	Date/Time Modification Disa	bled
) 3/6/2018	12:30:14	WEADER 💼	192.148.7.79	MEADER/COM	File Anti-Virus (1885)	eScan Monitor	Date/Time Modification Disa	bled
	3/6/2018	12:30:14	WEADER	192.148.7.79	-	File Anti-Virus (1805)	eScan Monitor	Date/Time Modification Disa	bled

Settings

You can define the Settings for Events, Computer Selection and Software/Hardware changes by clicking on the **Settings** option and defining the desired settings using the Tabs and options present on the Events and Computer settings window.

Event Status Setting

Basically, events are activities performed on client's computer.

Events & Computers Settings							
Events Status	Computer Selection	Software/Hardware Changes					
Events							
Events Nan	ne Recent 💌						
Number	Of Records	1000					
Save	Close						

On the basis of severity, the events are categorized in to the following types:

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

Perform the following steps to define event status settings:





- 1. Select the appropriate **Events Name**.
- 2. Enter the number of events that you want to view in a list, in the Number of Records field.
- 3. Click Save. The settings get saved.

Computer Selection

Events & Computers Settings	🝸 Help
Events Status Computer Selection Software/Hardware Changes	
Computers	
Computers Status 🗸	
Check for eScan Not Installed	
Check for Monitor Status	
Check for Not Scanned	
Check for Database Not Updated	
Check for Not Connected	
Database Not Updated from more than 7 days	
System Not Scanned from more than 7 days	
System Not Connected from more than 7 days	
Number Of Records 1000	
Save Close	

The **Computer Selection** lets you select and save the computer status settings. This module lets you perform the following activities:

Critical Status: It displays a list of computers that are critical in status as per the criteria's selected in computer settings. Specify the details in following fields:

- Check for eScan Not Installed: Select this checkbox to view the list of client systems under managed computers on which eScan has not been installed.
- **Check for Monitor Status**: Select this checkbox to view the client systems on which eScan monitor is not enabled.
- Check for Not Scanned: Select this checkbox to view the list of client systems which have not been scanned.
- Check for Database Not Updated: Select this checkbox to view the list of client systems on which database has not been updated.
- Check for Not Connected: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.
- Number Of Records: Enter the number of client systems that you want to view in the list.





Warning Status: It displays the list of systems which are warning in status, as per the criteria's selected in computer settings. Specify the following field details:

- Check for Not Scanned: Select this checkbox to view the list of client systems which has not been scanned.
- Check for Database Not Updated: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Check for Protection off**: Select this checkbox to view the list of client systems on which protection for particular module is inactive.
- **Check for Many Viruses**: Select this checkbox to view the list of client systems on which maximum viruses are detected.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.
- Number Of Virus: Enter the number of viruses detected on client system.
- Number Of Records: Enter the number of client system that you want to view in the list.

Database are Outdated: It displays a list of systems on which virus database is outdated. Specify the following field details:

- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- Number of Records: Enter the number of client system that you want to view in the list.

Many Viruses Detected: It displays a list of systems on which number of viruses exceeds the specified count in computer settings. Specify the following field details:

- Number of Virus: Enter the number of viruses detected on client system.
- Number of Records: Enter the number of client systems that you want to view in the list.

No eScan Antivirus Installed: It displays the list of systems on which eScan has not been installed. Specify the following field detail:

• Number of Records: Enter the number of client system that you want to view in the list.

Not Connected for a long time: It displays the list of systems which have not been connected from a long time, as specified in computer settings. Specify the following field details:

- **System Not Connected from more than:** Enter the number of days from when the system has not been connected.
- Number Of Record: Enter the number of client system that you want to view in the list.

Not scanned for a long time: It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Specify the following field details:

- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- Number of Records: Enter the number of client system that you want to view in the list.





Protection is off: It displays the list of systems on which protection is inactive for any module, as per the protection criteria's selected in computer settings. It shows the status as "Disabled" in the list. Specify the following field details:

- **Check for Monitor Status**: Select this checkbox if you want to view the client systems on which eScan monitor is not enabled.
- Check for Mail Anti-Phishing: Select this checkbox if you want to view the list of client systems on which Mail Anti-Phishing protection is inactive.
- Check for Mail Anti-Virus: Select this checkbox if you want to view the list of client systems on which Mail Anti-Virus protection is inactive.
- **Check for Anti-Spam**: Select this checkbox if you want to view the list of client systems on which **Anti-Spam** protection is inactive.
- Check for Endpoint Security: Select this checkbox if you want to view the list of client systems on which Endpoint Security protection is inactive.
- **Check for FireWall**: Select this checkbox if you want to view the list of client systems on which **FireWall** protection is inactive.
- **Check for Proactive**: Select this checkbox if you want to view the list of client systems on which **Proactive** protection is inactive.
- Check for Web Protection: Select this checkbox if you want to view the list of client systems on which the Web Protection is inactive.
- Number of Records: Enter the number of client system that you want to view in the list.

Update Agent Status: It displays the list of systems that has been assigned as an Update Agent. Specify the following in details:

• Number of Records: Enter the number of client system that you want to view in the list.

Steps to define computer settings

To save the computer settings, follow the steps given below:

- 1. Click **Computers Selection** tab.
- 2. Select a type of status for which you want to set criteria, from the **Computer status** dropdown.
- 3. Select the appropriate checkboxes, and then enter field details in the available fields. For more information, refer [Types and criteria of computer status] section.
- 4. Click **Save**. The settings will be saved.





Software/ Hardware Changes Setting

You can configure these settings to receive updates on any Software, Hardware, and existing system changes.

vents & Computers	-		김 Helj
Events Status	Computer Selection	Software/Hardware Changes	
Updates			
Software/I	Hardware Changes Soft	vare Changes 🔻	
Numbe	r Of Days	1 days	
Numbe	r Of Records	1000	
Save	Close		

The Software/ Hardware Changes enable you to do the following activities:

Type of Software/Hardware Changes:

- Software changes
- Hardware changes
- Existing system info

To Change software/hardware settings, follow the steps given below:

- 1. Click the **Software/Hardware Changes** tab.
- 2. Specify the following field details:
 - Software/Hardware Changes: Click the drop-down and select the changes made.
 - **Number of Days**: Enter the number of days, to view changes made within the specified days.
 - **Number of Records**: Enter the number of client systems that you want to view in the list.
- 3. Click **Save**. The settings get saved.

Performing an action for computer

To perform an action for a computer, follow the steps given below:

- 1. Select a computer.
- 2. Click Edit Selection drop-down. To learn more <u>click here</u>.
- 3. Click the preferred action.





Asset Management

This module displays list of hardware configuration, software installed, software version number and a Software report for Microsoft software installed on **Managed Computers**. The Asset Management module consists following tabs:

- Hardware Report
- Software Report
- Software License
- Software Report (Microsoft)

Hardware Report

The Hardware Report tab displays hardware configuration of all Managed Computers.

et Management				
Hardware Report	Software Report	Software License Software	Report (Microsoft)	
Filter Criteria			 Export Option 	
omputer Details			1 - 100 of 839 🔢 (p	age 1 of 9 🕨 Rows per page: 100 🕚
Computer Name	Group	IP Address	User's name	Operating System
Charlest - manufacture	Managed Computers			Windows 2008 R2 Standard Edition 64-bit
transmin 🖬	Managed Computers	10-10-10	100100000000000000000000000000000000000	Windows 7 Professional 32-bit
	Managed Computers			Windows 7 Professional 64-bit
	Managed Computers			Windows 7 Professional 32-bit
C0001 4	Managed Computers			Windows 10 Professional 64-bit
	Managed Computers		and a second second second	Windows 7 Professional 32-bit
ACC081	Managed Computers		CONTRACTOR AND A DESCRIPTION	Windows 10 Professional 64-bit

The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- User's name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model





- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Keyboard Vendor
- Software

To view the list of Software along with the version and installation dates, click **View** in Software column.

Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

▼ Filter Criteria		Export Option	
Filter Criteria			
Select All	Include All 💙		#Add Asset Information
Computer Name	* Include 🗸	Internet Explorer	* Include 🗸
🗹 User name	* Include 🗸	OS Version	* Include 🗸
Operating System	* Include 🗸	Processor	* Include 🗸
Motherboard	* Include 🗸	Local Adapter	* Include 🗸
RAM	* Include 🗸	🗹 Wifi Adapter	* Include 🗸
Group	* Include 🗸	USB Adapter	* Include 🗸
PC IdentifyingNumber	* Include 🗸	🗹 Motherboard Serial No	* Include 🗸
🗹 OS Type	* Include 🗸	🗹 нор	
IP Address	* Include 🗸	OS Installed Date	
Service Pack	* Include 🗸	Disk Free Space	
PC Manufacturer	* Include 🗸	PC Model	* Include 🗸
MB Manufacturer	* Include 🗸	Graphic Card Details	* Include 🗸
Machine Type	* 🔻 Include 🗸		
Host Name	* Include 🗸		
Search Reset			(*) View All Items

Select the parameters you want to be included in the filtered report.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.** The Hardware Report will be filtered according to your preferences.

Exporting Hardware Report

To export the Hardware Report, click Export Option. Export Option field expands.

▲ Filter Criteria	 Export Option 	
Export Option	• HTML	Export

Select the preferred format and then click **Export**. A success message appears with the link to Open/Download the file.







Software Report

The Software Report tab displays list of Software along with the number of computers on which they are installed.

Asse	t Management	💲 Refresh	👔 Help
Н	lardware Report Software Report Software License Software	Report (Microsoft)	
	Filter Criteria	Export Option	
s	oftware Details	1 - 100 of 1000 H (page 1 of 10) H Rows per page: 10	•
<u>s</u>	oftware Name	Computer Count	^
1	ClickDownloader	1	
2	007 Microsoft Office system	<u>16</u>	
2	in1 Coundition Zero 1.1&Counter-Strike 1.6(build 2738)	1	
3	.5G Connect V3.1	1	
3	.75G Digiconnect v2.0.8.1884	1	
3	DP Chip Lite v17.05	1	
3	DP Chip Lite v18.05	4	

To view the computers on which the specific software is installed, click the numerical in Computer Count column.

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date





Filtering Software Report

To filter Software Report, click **Filter Criteria** field. Filter Criteria field expands.

▼ Filter Criteria	 Export Option 	
Filter Criteria		
Software Name	* Include V Group By	
Computer Name	* Include V Software Name	
Host Name	* Include V Computer Name	
OS Type	* Include 🗸	
Search Reset		(*) View All Items

The Software Report can be filtered on the basis of Software Name or Computer Name.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

Host Name

Enter the Host Name displays suggestions. Select the appropriate key.

OS Type

Enter the OS type.

Group By

The results can be grouped by Software name, Computer name or Group. If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.

The Software Report will be filtered according to your preferences.

Exporting Software Report

To export the Software Report, click **Export Option**. Export Option field expands.

▲ Filter Criteria			✓ Export Option
Export Option	O PDF	• HTML	Export Export Detailed Report

Select the preferred option and then click **Export**. OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**. A success message appears.



Click the link to open/download the file.





Software License

The Software License tab displays list of Software Licenses of managed computers.

set Management		💲 Refresh 🛛 👔 He		
Hardware Report Software Report Sof	tware License Software Report (Microso	ft)		
Filter Criteria Export Option				
	1 - 3 of 3 ∢ (page 1 of 1))	Rows per page: 100 🗸		
License Key	Software Name	Computer Count		
WORLD MEMORY COLUMN SMERGET SYLLET	Windows 10 Professional 32-bit 📒	1		
W2ERH MFEM/EW/CRE-KRECT/TEREE	Windows 10 Professional 64-bit 📒	1		
WEAR DRUG MURIC WRITEDIAL	Windows XP Professional 32-bit 📒	1		

The log displays License Key, Software Name and Computer Count.

To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count Column.

Filtering Software License Report

To filter Software Report, click **Filter Criteria** field. Filter Criteria field expands.

▼ Filter Criteria	Export Option
Filter Criteria	
Software License Key	* Include V
Software Name	* Include 🗸
Computer Name	* Include 🗸
Host Name	* Include 🗸
IP Address	* Include 🗸
OS Type	* Include 🗸
Search Reset	(*) View All Items

Software License Key

Entering the license key displays suggestions. Select the appropriate key.

Software Name

Entering the Software name displays suggestions. Select the appropriate software.

Computer Name

Click the drop-down and select the preferred computer(s).

Host Name

Enter the Host Name displays suggestions. Select the appropriate key.





IP Address

Entering the IP address displays suggestions. Select the appropriate IP address.

OS Type

Enter the OS type.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After entering data in all fields, click **Search**. The Software License Report will be filtered according to your preferences.

Exporting Software License Report

To export the Software License Report, click **Export Option**. Export Option field expands.

Filter Criteria	 Export Option
Export Option	
Excel OPDF INTML	Export Detailed Report SWindows OS Microsoft Office

Select whether you want report for Windows OS and Microsoft Office.

Select the preferred option and then click **Export**. OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**. A success message appears.



Click the link to open/download the file.





Software Report (Microsoft)

The Software Report (Microsoft) displays details of the Microsoft Software installed on the computers.

Asset Management	📚 Refresh 🛛 👔 Help
Hardware Report Software Report Software License Software Report MS Office Software Report Microsoft 05 Microsoft 05 <t< th=""><th>Report (Microsoft)</th></t<>	Report (Microsoft)
Filter Criteria	Export Option
	1 - 23 of 23 H (page 1 of 1) H Rows per page: 100 ▼
Software Name	Computer Count
Microsoft Office	38
Microsoft Office 2003 Web Components	1
Microsoft Office 2007 Primary Interop Assemblies	19
Microsoft Office 2010 Primary Interop Assemblies	4
Microsoft Office 365 - en-us	2
Microsoft Office Access database engine 2007 (English)	2

The tab consists following subtabs:

MS Office Software Report – It displays Microsoft software name and computer count.

Microsoft OS – It displays Operating System, Service Pack, OS version and computer count.

Filtering Software Report (Microsoft)

To filter Software Report (Microsoft), click **Filter Criteria** field. Filter Criteria field expands.

Microsoft Office Info Microsoft OS		
		Export Option
Filter Criteria		
Software Name	Microsoft Office*	Include 💙
Computer Name	*	Include 🗸
Host Name	*	Include 🗸
Search Reset		

Software Name

Enter the preferred software name and click the drop – down.

Computer Name

Click the drop-down and select the preferred computer(s).

Group By

If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.

The Software Report (Microsoft) will be filtered according to your preferences.





Exporting Software Report (Microsoft)

To export the Software Report (Microsoft), click **Export Option**. Export Option field expands.

Filter Criteria			 Export Option
Export Option			
O Excel	O PDF	• HTML	Export Detailed Report

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**. A success message appears.



Click the link to open/download the file.

Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field. Filter Criteria field expands.

Microsoft Office Info Microsoft OS		
▼ Filter Criteria		 Export Option
Filter Criteria		
Operating System	*	Include 🗸
Computer Name	*	Include 🗸
Host Name	*	Include 🗸
Service Pack	*	Include 🗸
OS Version	*	Include 🗸
Search Reset		

Operating System

Entering the operating system name displays list of suggestions. Select the appropriate OS.

Computer Name

Click the drop-down and select the preferred computer(s).

Host Name

Enter the Host Name displays suggestions. Select the appropriate key.

Service Pack

Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.





OS Version

Entering the OS version displays list of suggestions. Select the appropriate OS version.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After filling all the fields, click **Search**. The Microsoft OS report will be filtered according to your preferences.

Exporting Microsoft OS Report

To export the Microsoft OS Report, click **Export Option**. Export Option field expands.

Filter Criteria		 Export Option
Export Option		
O Excel	• HTML	Export Export Detailed Report

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.





User Activity

The User Activity module lets you monitor Print, Session, and File activities occurring on the client computers. It also provides the reports of the running applications. It consists following submodules:

- Print Activity
- Session Activity Report
- File Activity Report
- Application Access Report

Print Activity

The Print Activity monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer, and Username. Furthermore, the module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The log report generated consists of Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.

int Activity	🛅 Settings 💲 Refresh 👔 Help
▲ Filter Criteria	 Export Option
	1 - 10 of 10 H (page 1 of 1) H Rows per page: 10 ▼
Printer Name	Copies Pages
BARRIAL (BRIT TRANSPORT	3 3
Hannand Press	<u>28</u> <u>34</u>
B1710-998 1	10 192

Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column. Print Activity window appears displaying the details.

Print Activity >>	A COLUMN TRADA							
Achine Name : *(Include) Export To:Select 🔻 Export								
1 - 3 of 3 4 (page 1 of 1) > Rows per page: 10 V								
Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies	Pages	
18/09/19 1:33:43 PM	and the second s	1001100011110	Account Sugar	Anna Anna	Mar // Miana// anterious ag, and anterious at a state	1	1	
18/09/19 12:40:41 PM	Street State Cale Proc.			Shritten (Bell (Bornar)	NAMES // TAILOR DE// PARTNER TO COMPAREMENT AND PARTNER AND PARTNE	1	1	
18/09/19 12:37:01 PM	In COLUMN TRAFFIC		menual Region Tragman	Balling - Bill - Branks	148g///illiand//administratingmologia.org/is/lingager/di-201804	1	1	

Exporting Print Activity Log

To export this generated log:

- 1. Click the **Export to** drop-down.
- 2. Select a preferred format.
- 3. Click Export.

A success message appears.







4. Click the link to open/download the file.

Filtering Print Activity Log

To filter the print activity log, click **Filter Criteria**. Filter criteria field expands.

•	Filter Criteria	•		Export Option
Г	Filter Criteria		_	
	Computer Name	*		Include Group By
	Printer	*	1	Include Printer
	User name	*][Include User name
	Ø Date Range			
	From (MM/DD/YYYY) 11/02/2019			
	То (ММ/DD/ҮҮҮҮ) 11/02/2019			
	Search Reset			(*) View All Items

Computer Name

Click the drop-down and select the preferred computer.

Printer

Enter the printer's name.

User Name

Enter the User's name.

Include/Exclude

Selecting Include/Exclude for a Machine or Printer lets you include or exclude it from the log.





Date Range

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click Search.

The Print activity log will be filtered and generated according to your preferences.

Group By

To view results by specific printer, select **Printer**, Date Range and then click **Search**. To view results by specific user name, select **User name**, Date Range and then click **Search**.

Exporting Print Activity Report

To export the generated log, click **Export Option**. Export Option field expands.

▲ Filter Criteria		▼ Export Option
Export Option		
O Excel	HTML	Export Detailed Report

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.





Session Activity Report

This submodule monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Client Date, Computer name/IP, Group, IP address and Description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

Viewing Session Activity Log

In the navigation panel, click User Activity > Session Activity Report.

The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

 Filter Criteria 			 Export Option 			
			'	1 - 100 of 251 🖂	(page 1 of	3) ▶ Rows per page: 100 ▼
<u>Operation Type</u>	Client Date	Computer Name/Ip		Group	IP Address	Description
Start up	18/09/19 7:21:44 PM			Marketing Team	-	
Session LogOn	18/09/19 7:21:44 PM			Marketing Team		User LogOn User name:
Shut Down	18/09/19 7:20:36 PM	NAMES OF CONTRACT		Support Department	-	
Session LogOff	18/09/19 7:20:32 PM			Support Department		User LogOff User name:
Session LogOff	18/09/19 7:13:01 PM			Programming\Android	10.10.00	User LogOff User name:
Shut Down	18/09/19 7:01:51 PM			Production Dept		

Filtering Session Activity Log

To filter session activities, click **Filter Criteria** field. Filter Criteria field expands.

▼ Filter Criteria		Export Option
Filter Criteria		
Computer Name	* v Include	▼ IP Address * Include ▼
Operation Type	* Turclude	▼ Group * Include ▼
Description		
Date Range		
From (MM/DD/YYYY)		
To (MM/DD/YYYY)	09/19/2019	
Search Reset		(*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Operation Type

Click the drop-down and select the preferred activities.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.





IP Address

Enter the IP address in this field.

Group

Enter the group's name or click and select a group.

Date Range

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

Exporting Session Activity Report

To export the generated log, click **Export Option**. Export Option field expands.

▲ Filter Criteria		 Export Option 	
Export Option			
Excel	O PDF	• HTML	Export

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.





File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

Viewing File Activity Log

In the navigation panel, click User Activity > File Activity Report.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

1 - 10 of 112848 ⊨ (page 1 of 11285) ⊨ Rows per page: 10 ▼								
<u>Client Date</u>	Computer Name/Ip	Group	IP Address	<u>User's name</u>	File Action Type	Drive Type	Source File	Destination File
4/20/2019 12:00:25 AM	111006-015-016-	110,00			CREATE	DRIVE_NETWORK	NewFile	\\ \Images\GR000
4/20/2019 12:00:25 AM	111006-010-010-	HARDE	01101-00		CREATE	DRIVE_NETWORK	NewFile	\\ \Images\GR000
4/20/2019 12:01:52 AM	10.000	HARDE	01100-000		CREATE	DRIVE_NETWORK	NewFile	\\ \images\GR000(
4/20/2019 12:01:52 AM	1111000-00-	- name	011011100	ALL AND A CONTRACTOR OF A CONTRACTOR	CREATE	DRIVE_NETWORK	NewFile	\\ \images\GR000(
4/20/2019 12:04:15 AM	111052-015-055	HALLAR			CREATE	DRIVE_NETWORK	NewFile	\\ \Images\GR000
4/20/2019 12:04:15 AM	111100-011-05-	-			CREATE	DRIVE_NETWORK	NewFile	\\ Images\GR000

Filtering File Activity Log

To filter file activities, click Filter Criteria field. Filter Criteria field expands.

 Filter Criteria 			 Export Option 		
Filter Criteria					
Computer Name	*	Include 🔻	IP Address	*	Include 🔻
User's name	*	Include 🔻	Group	*	Include 🔻
File Action Type	* •	Include 🔻	Drive Type	*	✓ Include ▼
Source File	*	Include 🔻	Destination File	*	Include 🔻
Application	*	Include 🔻			
🗹 Date Range					
From (MM/DD/YYYY)	09/19/	/2019			
To (MM/DD/YYYY)	09/19/	/2019			
Search Reset					(*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Username

Enter the username of the computer.

File Action type

Click the drop-down and select a preferred file action.

Source File

Enter the source file's name.

Application





Enter an application's name.

Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

IP Address Enter an IP address.

Group

Enter the group's name or click and select a group.

Drive Type

Click the drop-down and select the drive type.

Destination File

Enter the file path.

Date Range

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

Enable search by typing keywords on above fields

Select this checkbox to filter the report as per keyword for particular field.

After filling all fields, click **Search**.

The Activity Log will be displayed.

Exporting File activity Report

To export the generated report, click **Export Option**. Export Option field expands.

Filter Criteria		 Export Option 	
Export Option Excel	O PDF	• HTML	Export

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.





Application Access Report

The Application Access Report module gives the detailed view of all the applications accessed by the computers in the Managed Computers.

Viewing Application Access Report

In the navigation panel, click User Activity > Application Access Report.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

Filter Criteria	Export Option
	1 - 29 of 29 (page 1 of 1) > Rows per page: 100 N
Application Name	Total Duration (DD:HH:MM:SS)
adb.exe	00:00:05
Adobe Acrobat	00:00:00:15
Adobe Acrobat 8.0	00:00:0114
Adobe Acrobat Reader DC	00:00:10:17
Adobe Collaboration Synchronizer 20.12	00:00:00:23
Adobe RdrCEF	00:00:24:08
Adobe Reader	00:01:21:46
Adobe Reader 9.3	00:00:06:35
Bullzip PDF Printer	00:00:00:37
CutePDF Application	00:00:01:06
EAgent	00:04:34:53
esupdateBD.exe	00:00:00:10
TDS @nalyst Launcher	00:00:01:04
Firefox	00:00:33:49
Firefox Default Browser Agent	00:00:01:06
Firefox Software Updater	00:00:00:17
Google Chrome	00:15:59:19

By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.

Application Name >> Adobe Acrobat			
	Export To:Select V Export		
1 - 1 of 1 ((page 1 of 1)) Rows per page: 100 ♥			
Computer Name	Total Duration (DD:HH:MM:SS)		
84-7268	00:00:05		

Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.

Computer List >> 10 Parts					
Export To:					
1 - 1 of 1 + (page 1 of 1 +)+ Rows per page: 100 🗸					
Application Name	Start Time	End Time	Total Duration (DD:HH:MM:SS)	Application Path	
Adobe Acrobat	03/12/20 10:37:38 AM	03/12/20 10:37:43 AM	00:00:00:05	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\Acrobat.exe	

You can export this report in PDF, CSV, and HTML format.





Filtering Application Access Report

To filter file activities, click Filter Criteria field. Filter Criteria field expands.

lication Activity Report					
Filter Criteria		 Export Option 			
Filter Criteria					
Application Name	*	Include 🗸	Group By		1
Computer Name	*	▼ Include ¥	Application Name		
IP Address	*	Include 🗸	O Computer Name		
Date Range					
	L/2024				
To (MM/DD/YYYY) 07/3	L/2024				
Search Reset			(*) View All Item	IS

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Application Name

Entering the Application name displays suggestions. Select the appropriate application.

Computer Name

Click the drop-down and select the preferred computer(s).

IP Address

Click the drop-down and select the preferred IP Address.

Group By

The results can be grouped by Application name or Computer name.

Date Range

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After entering data in all fields, click **Search**. The Application Access Report will be filtered according to your preferences.

Exporting Application Access Report

To export the generated report, click **Export Option**. Export Option field expands. Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.





Notifications

This module lets you configure notifications for different actions/incidents that occur on the server. The Notifications module consists following submodules:

- Event Alert
- Unlicensed Move Alert

Event Alert

This submodule lets you enable email notifications about any event that occurs on the client computers connected to the server.

Events Alert Settings	
Enable email alert Notification Enter Receipent Mail ID :	
Send Information only in subject line	

To enable the event alert:

- 1. In the navigation panel, click **Notifications** > **Event Alert**.
- 2. Select the checkbox Enable email alert Notification.
- 3. Select the events from the list for which you prefer an alert.





ts Alert Settings					
Enable email alert Notification					
Enter Receipent Mail ID :					
Send Information only in subject line					
Select E	vent Ids				
Select a	ctivities for wh	ich email alert is required			
	Event Id	Description			
	130	CONSCTL_FILE_COPIED_TO_USB			
	100	ESCAN_DUMMY_EVENT			
	1	MWAV_FOUND_MALWARE			
	2	MWAV_FOUND_VIRUS_AND_DELETED			
	3	MWAV_FOUND_VIRUS_AND_CLEANED			
	4	MWAV_FOUND_ADWARE			
	5	MWAV_FOUND_ERROR			
	6	MWAV_FOUND_VIRUS_AND_RENAMED			
	7	MWAV_FOUND_ADWARE_AND_DELETED			
	8	MWAV_LAST_COMPUTER_SCAN			
	9	MWAV_START			
	10	MWAV_SUMMARY			
	501	SCHED_MWAV_FOUND_MALWARE			
	502	SCHED_MWAV_FOUND_VIRUS_AND_DELETED			





4. Select the required hosts or group.

 All Hosts Selected Hosts 		
Select Computers	Computer Selected: 1	
♥ □ 🔤 Managed Computers		

5. Click Save.

The Event Alert Settings will be saved.

Unlicensed Move Alert

This sub module lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.

Unlicense I	Nove Alert Settings
	Send notification for unlicensed computers. Enter Receipent Mail ID :

To enable the unlicensed move alert:

- 1. In the navigation panel, click **Notifications** > **Unlicensed Move Alert**.
- 2. Select the checkbox **Send notification for unlicensed computers**.
- 3. After selecting the checkbox, enter the Recipients Mail ID in the textbox.
- 4. Click Save.

The Unlicensed Move Alert Settings will be saved.





Settings

The Settings module lets you to configure general settings using following submodules:

- Web Console Settings: This submodule lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Two-Factor Authentication**: This submodule lets you to add extra layer of protection to your endpoints.
- **Excluded Clients:** This submodule lets you configure the client list to exclude it from auto isolation.

Web Console Settings

Web Console Settings submodule lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression, Password Policy Settings, and Delete Log Settings.

Web Console Settings						
Web Console Timeout Setting						
Enable Timeout Setting						
Automatically log out the Web Console after	Automatically log out the Web Console after 60 v minutes					
DashBoard Setting						
Show Status for Last 3 days (1 - 365)						
Logo Settings						
Logo : eSsan The logo needs to have the size 200 x 65px, and needs to be in .png or .jpg (RGB Color) format. Change Default						
Deserved Deline Cattings						
Password Policy Settings						
Password Age :	90 days (30-180 days)	0 = Password Never Expires				
Password History :	3 (3-10 Passwords)	0 = No password history is maintained				
Maximum Failed login attempts :	3 (3-10 times)	0 = Unlimited failed attempts allowed				
Note: The above restrictions are not applicable	Default to "Root" login.					
Save Cancel						

Web Console Timeout Settings

To enable web console Timeout, select Enable Timeout Setting option.

After selecting the checkbox, click the drop-down and select the preferred duration.

Dashboard Setting

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.





Logo Settings

This setting allows you to add the organization logo in PNG or JPEG format. So the console and reports will have the uploaded logo for customization.

To have the default eScan logo, click Default.

To have customized logo, click Change.

Password Policy Settings

This setting allows the admin to configure the password settings for other users.

- **Password Age**: Enter the preferred value (between 30-180); this will prompt user to reset the password after specified number of days. Here, 0 indicates that password never expires.
- **Password History**: Enter the preferred value (between 3-10); this maintains the password history for specified count. Here, 0 indicates, no password history is maintained.
- **Maximum Failed login attempts**: Enter the preferred value (between 3-10); this will restrict the user from logging after specified attempts. Here, 0 indicates unlimited login attempts.

After making necessary changes, click **Save.** The web console Settings will be updated.





Excluded Clients

The Exclude Client module lets you to configure the client list to exclude it from auto isolation.

Excluded Clients	
Client(s) list excluded from Auto ad	ding under Managed Group(s)
	Add
A	Remove
· · · · · · · · · · · · · · · · · · ·	
e.g.: Host Name Host Name with wildcard	
IP Address	
IP Address Range	
Save Cancel	

- 1. You can add/remove clients list to exclude it from auto isolation in the below table. To do the same, refer the following:
 - Enter the host name, IP Address, or IP address range and click Add.
 - To delete a particular client, select the client and click **Remove**.
- 2. After configuring accordingly, click Save. Excluded Client Settings will be saved.





Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered less secured and it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users.

To use 2FA login feature, you need to install the Authenticator app for Android devices from <u>Play</u> <u>Store</u> or for iOS devices from <u>App Store</u> on your smart device. The Authenticator app needs camera access for scanning a QR code. If a COD or BYOD policy restricts you from using device's camera in your organization, enter the Account Key in the Authenticator app.



•	Ensure that the smart device's date and time matches with the system's date and time or
NOTE	else TOTPs generated by app won't get validated.

0	We recommend that you save/store the Account Key in offline storage or a
IMPORTANT	paperback copy, in case you lose the account access.





Enabling 2FA login

To enable 2FA login:

- $1. \quad Go \ to \ Settings > Two-Factor \ Authentication.$
- 2. Open the Authenticator app.

After basic configuration following screen appears on smart device.

÷		••••
	an account	
0	Scan a barcode	
	Enter a provided key	

3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**. After scanning the Account QR code or entering Account Key, the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.

Authenticator	
Account Added	
536151	13

4. Click Enable Two-Factor Authentication.





Verify T-OTP window appears.

	Two-Factor Authentication	
	Verify T-OTP	
	11:43:18 AM	
Enter 1	-otp Verify T-OTP	

- 5. Enter the TOTP displayed on smart device and then click **Verify TOTP**. The 2FA login feature gets enabled.
- 6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled as shown below.

X - 2FA Disabled

I - 2FA Enabled

Other Users Settings Users Fo	or 2FA
2FA Status	<u>User Specific QR Code</u>
· 🗙 👳	View
X 🔿	View
X 🔿	View
X 🔿	View
* •	View
X 🔿	View
× +	View
X 🔿	NA
	2FA Status X⊕ X⊕

- To enable 2FA login for an added user, click the button to check icon. The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
- 8. To view the QR Code of specific user, click **View** option in the User Specified QR Code column.





Disabling 2FA login

To disable 2FA login:

- $1. \quad Go \ to \ Settings > Two \ Factor \ Authentication.$
- 2. Click **Disable Two-Factor Authentication**.



Verify T-OTP window appears.

Two-Factor Authentication	
Verify T-OTP	
11:45:34 AM	
Enter T-OTP	
Verify T-OTP	

3. Enter the T-OTP and then click **Verify T-OTP**. The 2FA feature gets disabled.

•	After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated
NOTE	for added users.





Users For 2FA

This tab helps to add the users and apply 2FA to the endpoints via policy template. The users can be added directly or from Active Directory.

Factor Authentic	ation			[
2FA Settings	Manage Other Users Settings	Users For 2FA		
📑 Add User	Import Users			
User name	Description	Created Date	Assigned Policy Template	User Specific QR Code
	Support	8/9/2023 10:54:59 AM		View
	Added through import user	9/26/2023 11:56:33 AM		View

Method 1: Adding user

To add users for the same, follow the below steps:

- 1. Go to Settings > Two-Factor Authentication > Users For 2FA.
- 2. Click Add User.

Add User window appears.

		$\mathbf{\times}$
Add User		
Username Description		
Ok	Cancel	

- 3. Enter the **Username** and **Description**.
- 4. Click **OK**.





Method 2: Importing Users

To import the users, follow the below steps:

- 1. Go to Settings > Two-Factor Authentication > Users For 2FA.
- 2. Click **Import Users**. Import Users window appears.

Deleting Users

To delete the users, follow the below steps:

- 1. Go to Settings > Two-Factor Authentication > Users For 2FA.
- 2. Click **Delete**.

The Confirmation prompt appears.

Cancel

3. Click **OK**.

The user will be deleted.





Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow them to install eScan Client, implement Policies and Tasks.

The Administration module consists following submodules:

- User Accounts
- User Roles
- Audit Trail

User Accounts

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts submodule, you can create new user accounts and assign Administrator role to added users and reduce the workload. This submodule displays a list of users and their details like Domain, Role, Session Log and Status.

User	Accounts				💲 Refresh	👔 Help
	Create New Acco	unt Delete	1 - 1 of 1	age 1 of 1	Rows per page	: 100 🔻
	<u>User name</u>	Full Name	<u>Domain</u>	Role	Session Log	<u>Status</u>
	root	Administrator account created during installation		Administrator	<u>View</u>	~ .
	Create New Account Delete 1 - 1 of 1 H page 1 of 1 H Rows per page: 100 V					

Create New Account

To create a User Account:

1. In the User Accounts screen, click **Create New Account**. Create User window appears.

Create User Account Type and		😰 Helj
User name*: Full Name*: Password*: Confirm Passwo Email Address:*		Password must have: X • Minimum 8 characters X • Atleast 1 Lowercase letter [a-2] X • Atleast 1 Uppercase letter [A-2] X • Atleast 1 digit [0-9] X • Atleast 1 symbol [\$@!%*#?_8] X • Passwords must match. X
Account Role	dministrator	∨ _
Save	Cancel	(*) Mandatory Fields

After filling all the details, click Save.
 The user will be added to the User Accounts list.





Delete a User Account

To delete a user account:

1. In the User Accounts screen, select the user you want to delete.

User	User Accounts					
	Create New Account					
	User name Full Name					
	root	Administrator account created during installation				
	Sample user Sample User					
Create New Account						

2. Click **Delete**.

A confirmation prompt appears.

User Accounts
Do you want to delete the selected user account(s) ?
Ok Cancel

3. Click **OK**.

The User Account will be deleted.





User Roles

The User Roles submodule lets you create a role and assign it to the **User Accounts** with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights, Group Admin Role or a Read only Role.

User Roles	🗢 Refresh 🛛 👔 Help
Image: New Role Properties Image: Delete	
Role Name Descriptio	n
Administrator	

You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation/uninstallation of eScan Client on network computers or define Policies and tasks for the computers allocated to them.

New Role

To add a user role:

1. In the User Roles screen, click **New Role**. New Role form appears.

New Role				
<u>User Roles</u> >New Role				
Role Details				
New Role Name :*				
Description :				
Select Group :				
H □ □ Managed Computers				
Ok				

- 2. Enter name and description for the role.
- 3. Click **Managed Computers** and select the specific group to assign the role. The added role will be able to manage and monitor only the selected group's activities.





4. Click OK.

Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists the permissions for selected group(s) that the user is allowed to take further.

erties				?
Roles >Properties				
Details				
New Role Name :*	sample role			
Description :				
Select Group :				
Select Group Tree				
Select Group free				
nissions				
Main Tree Menu Clie	ent Tree Menu			
		View	Configure	
Menu				
DashBoard		V		
Managed Computers		V	V	
Report Templates				
Report Scheduler				
Events & Computers				
Asset Management				
User Activity				
Print Activity				
Session Activity Repor	t			
File Activity Report				
Notifications				
Unlicense Move Alert				
Settings				
Web Console Settings				
Excluded Clients				
Administration				
User Accounts				
User Roles				
License				
Policy Templates				

- 5. Select the checkboxes that will allow the role to view/configure the module.
- 6. After selecting the necessary checkboxes, click **Save**. The role will be added to the User Roles list.





View Role Properties

To view the properties of a role:

- 1. In the User Roles screen, select a role.
- 2. This enables **Properties** and **Delete** buttons.

	User Roles				
	Properties Delete				
		Role Name	Description		
		Administrator			
6		Monitor	For viewing activities		

3. Click Properties.

Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.

erties Roles >Properties			?		
• Details					
New Role Name :*	sample role				
Description :					
Select Group :					
Select Group Tree					
missions					
Main Tree Menu	Client Tree Menu				
Menu		View	Configure		
DashBoard					
Managed Computers			S		
Report Templates					
Report Scheduler					
Events & Computers					
Asset Management					
User Activity					
Print Activity					
Session Activity R					
File Activity Repor	t				
Notifications Event Alert					
Unlicense Move Al					
Settings	ert				
Web Console Setti	200				
Excluded Clients					
Administration					
User Accounts					
User Roles					
License					
Policy Templates					

4. To modify client configuration permissions, click **Client Tree Menu**. **Client Tree Menu**





Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, Select Policy Template, Policy Criteria, and Group Tasks.

Roles >Properties				
Role Name :*				
Description :	Eccan			
Select Group :				
Select Group Tree				
issions				
Main Tree Menu Client T	ree Menu			
Managed Computers				
	[Managed Computers/Escan]	Configure		
	Menu			
	Action List			
	New Sub Group			
	Remove Group Create Client Setup			
	Properties			
	Client Action List			
	Move to Group			
	Remove from Group			
	Manage Add-On License			
	Export			
	Show Installed Softwares			
	Create OTP			
	Properties			
	Anti-Theft Options			
	Disable Anti-Theft			
	Select Policy Template			

- 5. To let the role configure these actions, under the Configure column select the checkboxes of corresponding actions.
- 6. Click Save.

The Role Properties will be updated accordingly.





Delete a User Role

To delete a user role:

1. In the User Roles screen, select the user role you want to delete.

	User Roles					
_						
	New Role Properties					
		Role Name	Description			
		Administrator				
6	•	Monitor	For viewing activities			

2. Click **Delete**.

A delete confirmation prompt appears.

×
Delete Role
Do you want to delete the selected Role(s)?
Ok Cancel

3. Click OK.

The User Role will be deleted.





License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed licenses and remaining licenses with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of Add-On licenses along with the names. For example, as you can see here, there are 15 add-on licenses for eBackup feature. The eBackup, 2FA, and DLP features are available through Add-On license(s).

License Sefresh 👔 Help					
License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
	Activate Now	Activate before 01- Jun-2020	-	10	
1999 - 1999 - 1977 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -	NAME OF ALL AND A DESCRIPTION OF A	Activated	20-Apr-2021	200	EBackup+ RMM+ DLP+ 2FA
kanto de las calcos calendos de las seconos de las		Activated	13-May-2021	200	
o Add License <u>Click Here</u>	License		🖷 🌐 👧 🎬		
		License in Use License Remaining Total License Size	132 268 400		
		Manage License			

Adding and Activating a License

To add and activate a license:

1. In the License screen, click the **Click Here** link.

To Add License <u>Click Here</u>

Add License Key dialog box appears.

	×
Add 30 Character License Key.	
	OK Cancel

Enter the license key and then click **OK**.
 The license key will be added and displayed in the **Register Information** table.

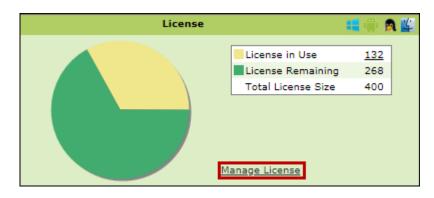




Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers:

1. In the License statistics box, click Manage License.



Manage License window appears.

					A 11-11-11-11-11-11-11-11-11-11-11-11-11-	
ice.	nsed Computers / Devices (132)	Filter License All	~		Move to Non-Lice	ns
	Machine Name		Group			
	😻		Rengel Conside	1110-1010		
	👷 us-7uss 🚛 🛄	Para ang at the complete of the second second				
	9	For the state of t				
	🔋 😫	the read - entry derivative ages				
		Personal Contractory and the second				
			Banger - Strauber	1000		
lon						
	-Licensed Computers / Devices (327)	Filter Licen	se All 🗸		Move to Lice	ns
	-Licensed Computers / Devices (327)	Filter Licen	se All 🗸	<u>Unlicense</u> Date Time	Move to Lice	ns
			se All V			ns
	Machine Name		se All V	Date Time 31/03/2018		ns

- 2. Under the Licensed Computers section, select the computer(s) that you want to move to Non-Licensed Computers section.
- 3. Click Move to Non-License.
- 4. The selected computer(s) will be moved to Non-Licensed Computers section.

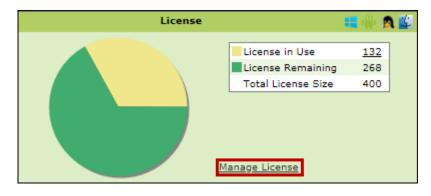




Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to Non-Licensed Computers, follow the steps given below:

1. In the License statistics box, click Manage License.



Manage License window appears.

nag	je License				👔 He		
ice	nsed Computers (385)			mov	e to Non-License		
	Machine Name		Group				
		Managed Computers					
	🗿 💷 an	Managed Computers					
		Managed Computers					
		Managed Computers					
		Managed Computers					
		Managed Computers					
Non	-Licensed Computers (2)			â	Move to License		
	Machine Name	<u>Group</u>		Unlicense Date Time	Description		
	🗊 🖛 🖬 💼 🖬 Managed Con		nputers	13/09/2019 17:13:16			
		Managed Con	nputers	13/09/2019 17:13:16			

- 2. Under the Non-Licensed Computers section, select the computer(s) that you want to move to Licensed Computers section.
- 3. Click Move to License.
- 4. The selected computer(s) will be moved to Licensed Computers section.





Contact Us

We offer 24/7 free online technical support to our customers through email and live chat. We also provide free telephonic support to customers during our business hours.

Before you contact technical support team, ensure that your system meets all the requirements and you have Administrator access to it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Ensure that you have the following information when you contact technical support:

- Endpoint hardware specifications
- Product version in use and patch level
- Network topology and NIC information
- Gateway, IP address and router details
- List of hardware, software and network changes if any carried out
- Step-by-step description of error/situation
- Step-by-step description of troubleshooting if any attempted
- Screenshots, error messages and log/debug files

In case you want the Technical Support team to take a remote connection:

• IP address and login credentials of the system

Forums

Join the **Forum** to discuss eScan related problems with experts.

Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries via **Live Chat**.

Email Support

If you have any queries, suggestions and comments regarding our products or this User Guide, write to us at **support@escanav.com**