



Anti-Virus
(Cyber Vaccine Edition)

User Guide



24x7 FREE
Online Technical Support
support@escanav.com
<https://forums.escanav.com>

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

Document Number: 5BUG/21.07.2021/22.0

Current Software Version: 22.0.xxxx.xxxx

Copyright Notice: Copyright © 2021. All rights reserved.

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

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

Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of MicroWorld.

Trademarks: The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, MailScan are trademarks of MicroWorld.

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

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical Support	: support@escanav.com
Sales	: sales@escanav.com
Forums	: http://forums.escanav.com
eScan Wiki	: https://www.escanav.com/wiki
Live Chat	: http://www.escanav.com/english/livechat.asp
Printed By	: MicroWorld
Date	: July 2021

Welcome

eScan's next-gen antivirus solution protects the home network from viruses, malware, ransomware, bots, and more, using a layered approach. With a unique combination of basic and modern techniques, eScan blocks a broad range of attacks. It comprises everything right from web filtering, signature-based malware detection, application control, and behavior analysis to innovative techniques like deep learning malware detection, exploit prevention, heuristic scanning, and many more.

From powerful anti-ransomware technology to cutting-edge AI malware detection with deep learning, protect your computers from never-before-seen threats. eScan offers advanced defense capabilities against malware that includes script, macro, and polymorphic viruses, Trojans, Internet worms, malicious Java applets, and ActiveX code. It also provides smart parental controls to keep your kids safe online by limiting their time and content filtering wherever they go.

The feature-rich new offering from eScan comes with a user-friendly interface along with several customizable settings. Its design is both intuitive and easy to understand. Additionally, the product introduces a myriad of new features that are fashioned to secure your systems from emerging and updated threats, such as, malware, phishing web sites, emails, and hackers.

To counter these pernicious threats, eScan embeds its products with futuristic edge technologies, such as MicroWorld Winsock Layer (MWL), Non-Intrusive Learning Pattern (NILP), Domain and IP Reputation Check (DIRC), eScan Security Network (ESN), and Proactive Malware Detection.

MicroWorld designs its security solutions with the aim of providing a safe and secure computing environment for all eScan users. This guide is designed to help you use/evaluate the features and tools included in eScan 22.

Thank you for choosing eScan.

The eScan Team

Contents

Contents	4
Overview	6
Key Features	6
What's new	7
Prerequisite for installing eScan	8
First Time Installation	8
Renewal and Upgrade	8
System Requirements	9
Operating System	9
Minimum Hardware Requirements	9
Installation Steps	10
Product Activation	12
Adding and Activating the License Key	13
Activating the license key through offline mode (using eScan TPN app)	17
Getting Started	22
Graphical User Interface (GUI)	22
File Anti-Virus	23
Configuration	24
Reports	34
Mail Anti-virus	39
Configuration	39
Anti-spam	50
Configuration	51
Reports	59
Firewall	62
Configuration	63

Reports	77
Cloud Protection	81
Scan.....	84
Scan memory, registry and services.....	85
Scan computer.....	85
Scan USB Drives	85
Scan CD-ROM.....	85
Scan Mobile	85
Custom Scan	85
Options.....	85
Scheduler.....	88
Logs	94
Update.....	95
Configuration	96
Reports	102
Quick Access Links	103
Rescue Mode.....	103
eScan Remote Support.....	104
Password	105
License Information.....	106
Tools	108
Reports	115
Contact Us.....	117
Chat Support	117
Forum Support	117
Email Support	117

Overview

eScan Anti-Virus (Cyber Vaccine Edition) protects the home network by providing real-time protection. With constantly evolving security threats such as malware, spyware, ransomware, rootkit, and several other threats, eScan keeps an eye on the behavior of all the activities to make sure they don't go rogue. It's packed with sophisticated threat-detection, machine-learning virus protection, and home network security that won't slow down the PC. It also consists of an advanced two-way firewall, spam filter, gaming mode, and several other techniques that will keep the computer safe, clean, and optimized.

Key Features

Real-time Protection

eScan provides a sophisticated layer of real-time protection to prevent any possible spread of malicious programs. It constantly monitors the system for malware, spyware, ransomware, and various other threats. It detects and restricts malicious threats from accessing the system and exploits the personal data. eScan's Real-Time protection has the potential to keep cyber threats away by continuously monitoring the online/real-time activities.

Optimized Performance

eScan is equipped with advanced security technologies to reduce the memory and hard drive being used, which eventually minimize the CPU overhead. This, in turn, enhances the speed and performance of the computer making regular tasks go more quickly. Moreover, using cache technology the scan time is minimized without causing any lag to the system.

Powerful Anti-Ransomware

eScan's effective Anti-Ransomware feature uses Proactive Behavior Analysis Engine (PBAE) technology to monitors the activity of all the processes. The Intelligent Shadow Backup mechanism is triggered during any eventuality. This helps users to protect their crucial data and overcome the aftershock of ransomware attacks.

Windows Essential Updates

eScan checks for missing security patches on the system OS by matching the installed patches with the released patch list in the database. Then, it automatically installs the missing critical Windows security patch updates. This helps to keep the system away from latest threats and maintain the security of the home network.

Two-way Firewall

eScan's Two-way Firewall is equipped with a pre-defined set of rules that helps in detection of incoming and outgoing network requests, enabling you to monitor every inbound and outbound connection that is being established. This locks out hackers from connecting to the systems and defends the connection of undesired apps to the internet.

Quicker On-demand Scan

eScan's advanced On-Demand Scanner has built-in Whitelisting and Cache technology that allows scanning of files, memory, folders, and all other storage devices, more efficient and quick. Being

lightweight, it minimizes the consumption of CPU and memory resources during the scanning process.

Advanced Anti-Spam

eScan is equipped with an intelligent mail protection and filtering engine that blocks spam, viruses, and malware threats from breaching the email. It has powerful email protection against zero-day threats, which is efficient for minimizing exposure towards emerging email threats.

What's new

eScan Anti-Virus (Cyber Vaccine Edition) Security has introduces the following new features:

- Advanced Malware Detection
- Highly Optimized Performance
- A Sophisticated Threat-Detection Mechanism
- Powerful and Layered Anti-Ransomware Technology
- Quicker On-demand Scan
- Advanced Anti-Spam

Prerequisite for installing eScan

Please check the pre-requisites before installing eScan Anti-Virus on your system.

First Time Installation

- Ensure that you have Administrator Rights on the system where you wish to install eScan Anti-Virus.
- Ensure that the System Requirements for installing eScan are met.
- Please uninstall all other similar type of security application like Antivirus, Anti-Spyware or Anti Malware to avoid software conflict.
- Please ensure that sufficient space is available on your drive for installation; please check [System Requirements](#) for more details.
- We recommend that your system is connected to internet at the time of Installation; this will ensure that eScan is updated with all the recent virus signature from our Update Servers (eScan automatically checks and update the latest virus signature available on the Update Servers after installation).
- Ensure that critical operating system and security patches are installed on your system.

Renewal and Upgrade


- **Renewal:** You need to have a License Key for Renewing eScan, you can purchase the license key from any dealer nearby your vicinity or you can purchase it online directly from eScan at www.escanav.com.
- **Upgrade:** If a newer version is available, eScan can be upgraded by downloading and installing eScan from our website.

System Requirements

The following are the software and hardware requirements for installing and using eScan.

Operating System

- Windows® 11
- Windows® 10
- Windows® 8.1
- Windows® 8
- Windows® 7
- Windows® Vista®
- Windows® XP Service Pack 2 or higher
- Windows® 2000 Professional Service Pack 4
[All 32-bit & 64-bit Editions]

 NOTE	eScan 22 SOHO products do not support Server Operating systems.
--	---

Minimum Hardware Requirements

Component	Requirement
Processor	Intel or AMD single core x86 or x64
CPU	1 GHz recommended
Memory (RAM)	1 GB recommended
Disk Space	1GB recommended

Installation Steps

Install eScan Anti-Virus (AV) either by using the eScan setup file or by using the eScan product installation CD/DVD. To download the eScan setup file, visit the following link:

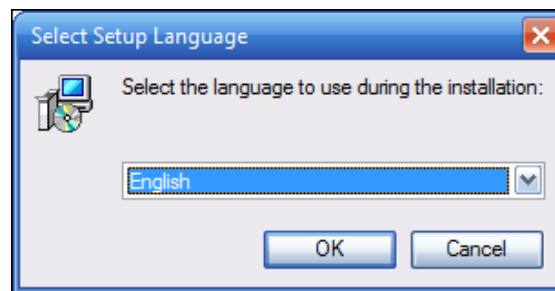
<https://www.escanav.com/en/windows-antivirus/best-antivirus-for-windows.asp>

Installing Anti-Virus from the CD/DVD is very simple. Just insert the CD/DVD into the ROM and wait for few seconds for auto run to start the installation process and follow the instructions on screen. In case, installation does not start on its own, click Install option on the CD ROM. This will open the one click installation wizard setup of Anti-Virus on your computer.

After downloading the eScan setup file. Double-click on the **Awnxxxxxxx.exe** file and follow the below steps:


1. Click **Next** to continue or click **Cancel** if you want to quit the installation.
2. The installation wizard runs in a language that is specified as Home location of a **Region > Location** setting of your operating system (or **Current location** of a **Region and Language > Location setting** in older systems).

Use the drop-down menu to select Product language in which your eScan AV will be installed.

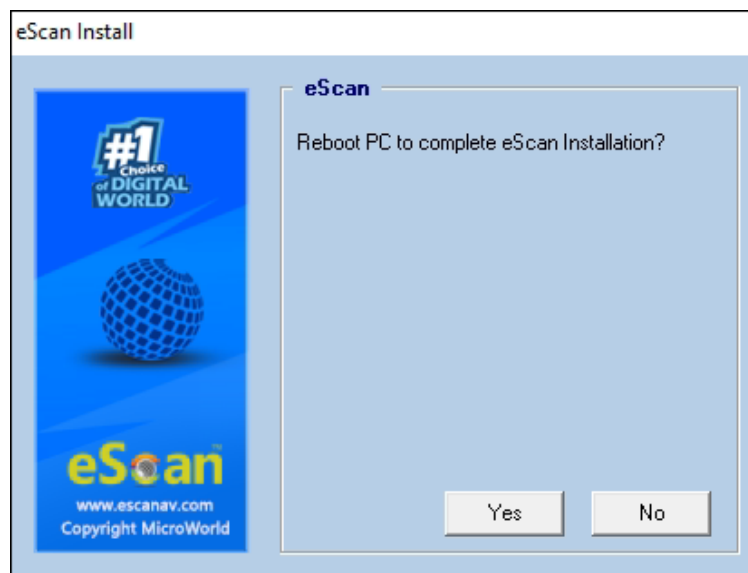



3. Click **Install** to begin the installation.




 NOTE	Default Path for eScan installation on a 32-bit PC – C:\Program Files\escan Default path for eScan installation on a 64-bit PC – C:\Program Files (x86)\escan
---	--

4. After completing the installation process, the wizard asks you to restart your PC.



5. To restart PC, select option **Yes**. When the installation finishes, eScan GUI starts and tray icon  is displayed in the notification area (system tray).

 NOTE	It is recommended that you restart the PC to run the eScan services effectively.
--	--

Product Activation

The product comes with a 30 days trial period. You should purchase the product license key before the trial period expires, wherein you receive a license key for registration. You can also renew the product, as per your requirement. To know information of registration and renewing your eScan product, visit the below link:

<https://www.escanav.com/register>

When the installation is complete, you will be prompted to activate the product.

You can use any of the following methods to activate the eScan Anti-Virus.


Enter the License Key

A unique string 30-character valid license key (in the format XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX) which is used for identification of the license owner and for activation of the license.

Offline License Key Activation

Using eScan TPN application, you can activate the License key even when the internet is not available in the system. A unique string 60-character is generated that is used for activation.

To use this feature, you need to install the eScan TPN for Android devices from [Play Store](#) or for iOS devices from [App Store](#) on your smart device.

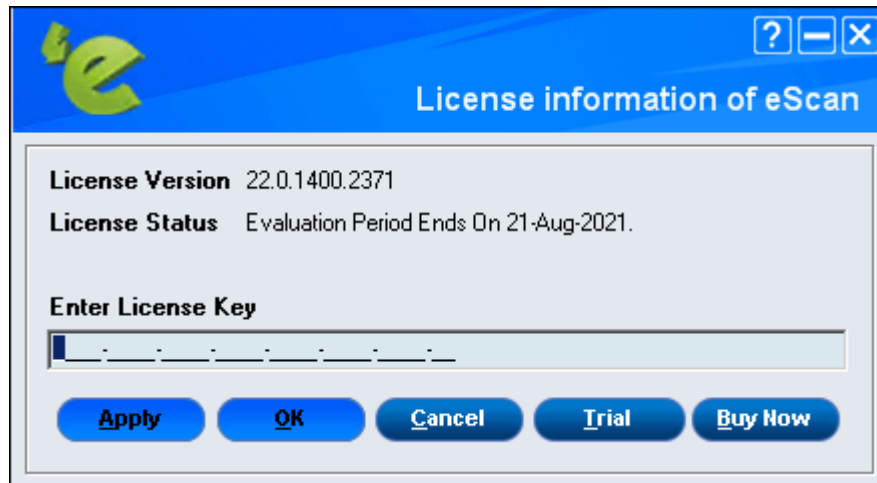
 NOTE	<p>If you type an invalid license key, a warning message appears.</p> <p>In some cases, if any of the character is missing or typed incorrectly it accepts at first instance, but gives an error message that Key not present in our database, while activation.</p> <p>While activating license key online via eScan TPN, it is mandatory to have active internet connection on your smart device.</p>
--	--

Adding and Activating the License Key

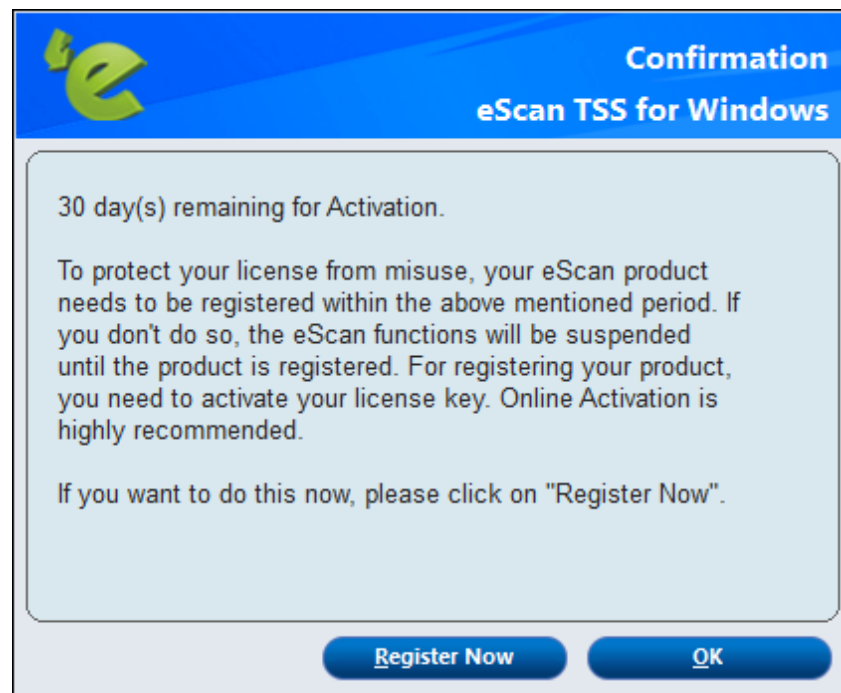
eScan allows you to add about two license keys at a time and it is mandatory that you activate at least one of them. Because once you activate one license key you can add more. Follow the below steps to add license key:

1. Click **Start**, point to **All Programs**, point to **eScan for Windows**, and then click **eScan Registration**.

The License information of eScan window appears.

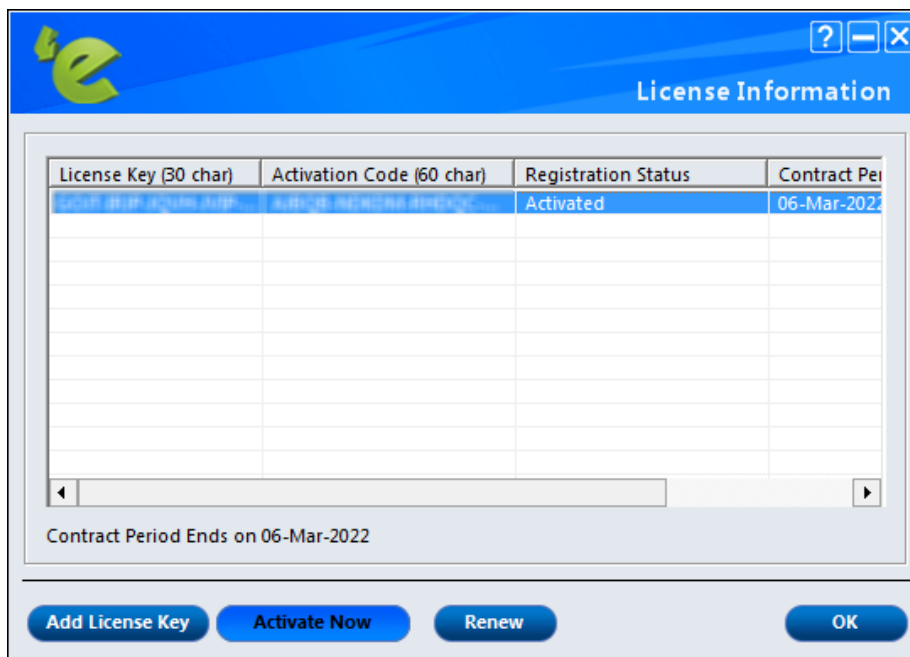


2. Type the 30-character valid license key in the **Enter License Key** field.
3. Click **Apply** and then click **OK**.




After following above procedure, let's activate the license key through online mode. To do same follow the below steps:

1. After adding the license key, a confirmation window appears. Do one of the following:
 - **Register Now:** Click this button, if you want to activate the license key immediately.
 - **OK:** Click this button, if you have the activation code or want to activate the product later.
2. When you click the **Register Now**.
The License Information window appears.



3. To add new license key, click the **Add License Key** and to activate click the **Activate Now**.

 NOTE	Alternatively right-click the license key from the list and then click the Add License Key or Activate Now .
--	--

- 4. When you click the **Activate Now**.
Online Activation window appears.

License Key: [XX] [Privacy Policy](#)

I want to activate online
 I have Activation Code

Enter Activation Code
[]

Name
[]

Customer Mobile No. * [] Email Id []

Email Subscription Yes No

Note: Enter valid email id in order to receive backup copy of your license details.

Country [India] State [Maharashtra]
City [Pune]

Dealer Mobile No. []

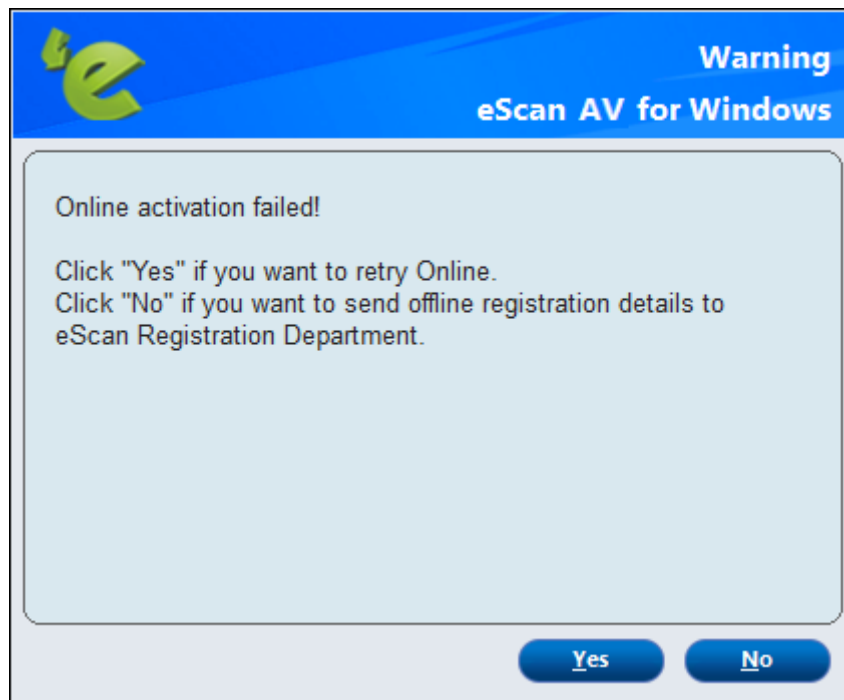
* Mandatory fields

To Continue, click Activate

QRCode Activate Cancel

5. Specify the details of the following fields:
 - **I want to activate online:** By default, this option is selected. When you click this option Name, Email Id *, Confirm Email Id*, Email Subscription, Country, State, and Dealer Mobile Number* fields are available.

Click this button to activate the eScan product online. You need to have active internet connection to activate online. In case, if you do not have internet connection the online activation fails and displays the following dialog box.



Click **No**, an **OnlineRegister.TXT** file gets generated with registration details. You have to send the **OnlineRegister.TXT** file to register@escanav.com, wherein you receive an activation code to the specified email ID.

- **I have Activation Code:** When you click this option only **Enter Activation Code** field is available. To learn more [click here](#). Click this option, if you already have activation code received through an email from register@escanav.com. In the **Enter Activation Code** field, type or copy and paste the activation code. This enables you to activate the eScan product immediately.
6. Click **Activate**.
The license key gets activated.

Activating the license key through offline mode (using eScan TPN app)

After adding the license key using above procedure, when you select **I have Activation Code** option, perform the follow the below steps:

1. After entering the license key, specify the details.

License Key: [blurred] [Privacy Policy](#)

I want to activate online
 I have Activation Code

Enter Activation Code
[text input]

Name
[text input]

Customer Mobile No. * [text input] Email Id [text input]

Email Subscription Yes No

Note: Enter valid email id in order to receive backup copy of your license details.

Country [India] State [Maharashtra]
City [Pune]

Dealer Mobile No. [text input]


* Mandatory fields

To Continue, click Activate

[QRCode](#) [Activate](#) [Cancel](#)

2. Click **QRCode** to get the registration details.

QR Code

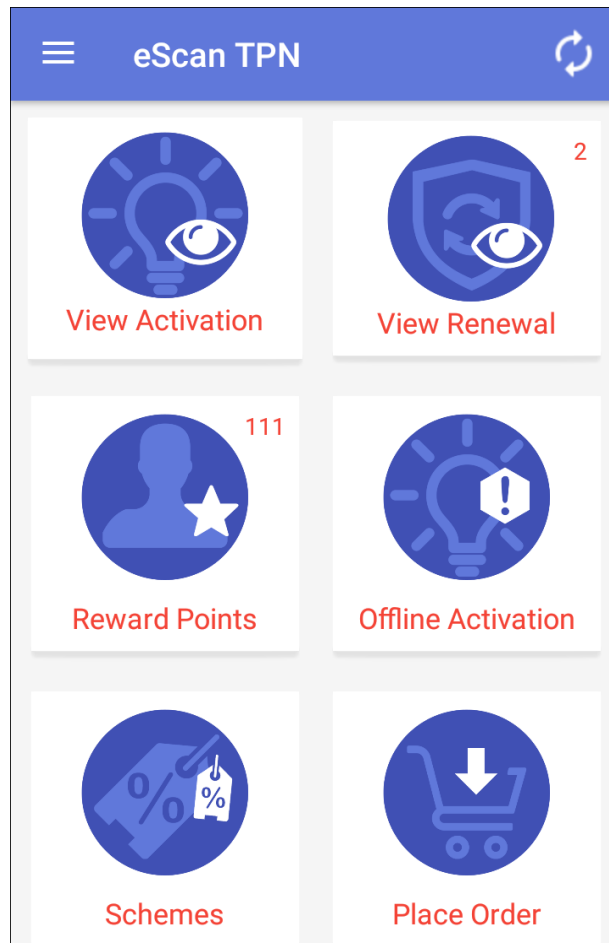


Registration Details

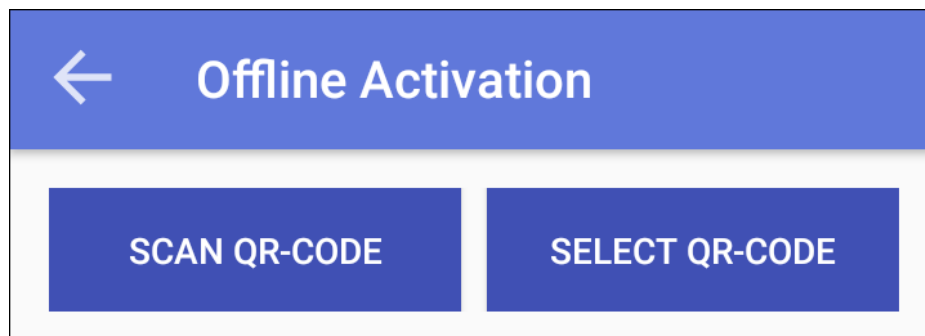
Name	:	Prashant
Company Name	:	
City	:	Mumbai
State	:	Maharashtra
Country	:	India
Phone No	:	
Mobile No	:	
Fax No	:	
Postal Code	:	
Email Id	:	prashant@escanav.com
Email Subscription	:	Yes
Reseller / Dealer	:	
Machine Code	:	6-1038-1153-758-8526-7962-5
Standard Key	:	
AKI	:	00000000000000000000000000000000-UF
Current Date	:	07/21/2021
eScan Version	:	22.0.1438.2371
Customer Mobile Number	:	98 40000000

[Close](#)

3. In the eScan TPN app, tap **Offline Activation**.



4. Tap **SCAN QR-CODE**, to scan the generated QR Code.



5. Scan the QR code using your smart device. After scanning, the form will be filled with details automatically.

← Offline Activation

SCAN QR-CODE SELECT QR-CODE

*** Indicate mandatory fields**

*Name
Subhalaxmi

*Email
example@example.com

*Mobile Number

Address

Postal Code

City
Pune

*State
Maharashtra

*Country
India

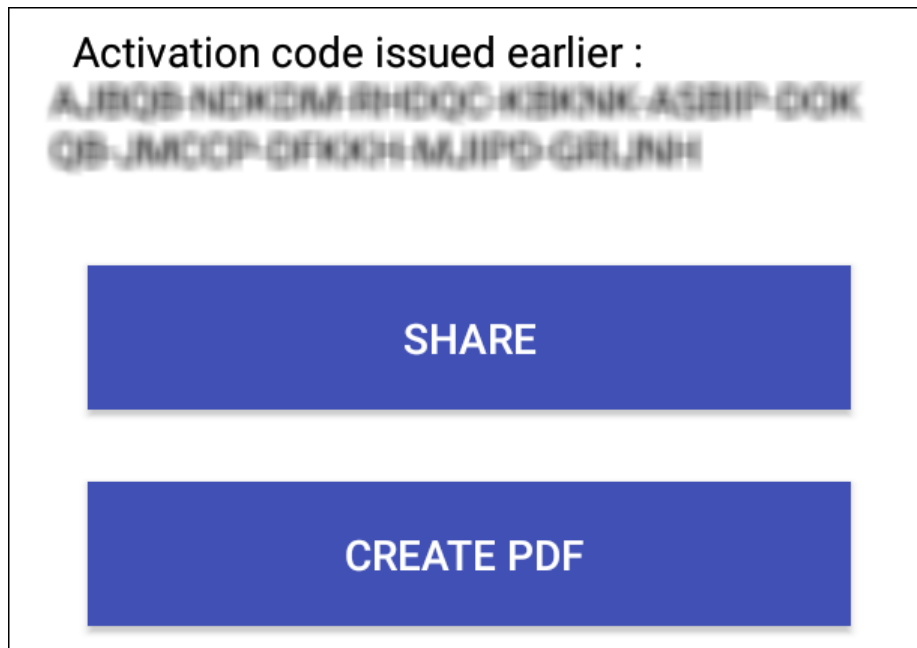
*License Key
G0JTRUPJQVHJVHPHPTPBYHCUE

*Machine Code
5-1816-2110-615-7226-7776-7

Machine Code with eScan
DHFD0FCD0FNDFED0FJDFNDFEJE

SUBMIT

6. Click **SUBMIT**. An activation code will be issued.



7. You can share the code via various modes such as email, WhatsApp, PDF, and more.
8. Now, select **I have Activation Code** option in the **Online Activation** window.
9. Enter the issued activation code and click **Activate**.
The license key gets activated.

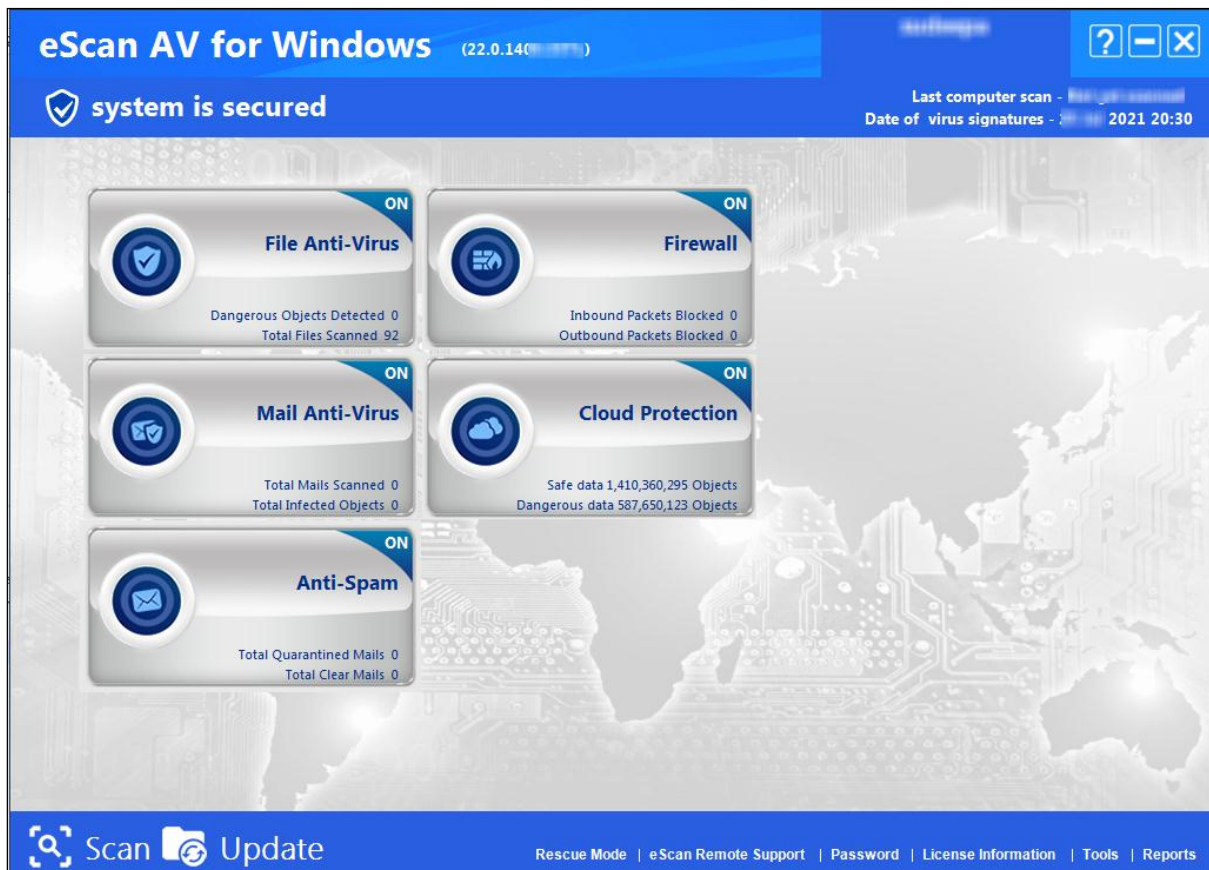
Getting Started

The following sections will give you the detailed description and configuration procedure of all the eScan GUI and Modules presents in the eScan Anti-Virus.

Graphical User Interface (GUI)

eScan 22 is not only equipped with the latest innovative technology but also has very simple yet trendy GUI. It is packed modules that gives brief details about the file scanned, quarantined, infected, and many more. It displays the date on which the computer was last scanned and virus signature updated.

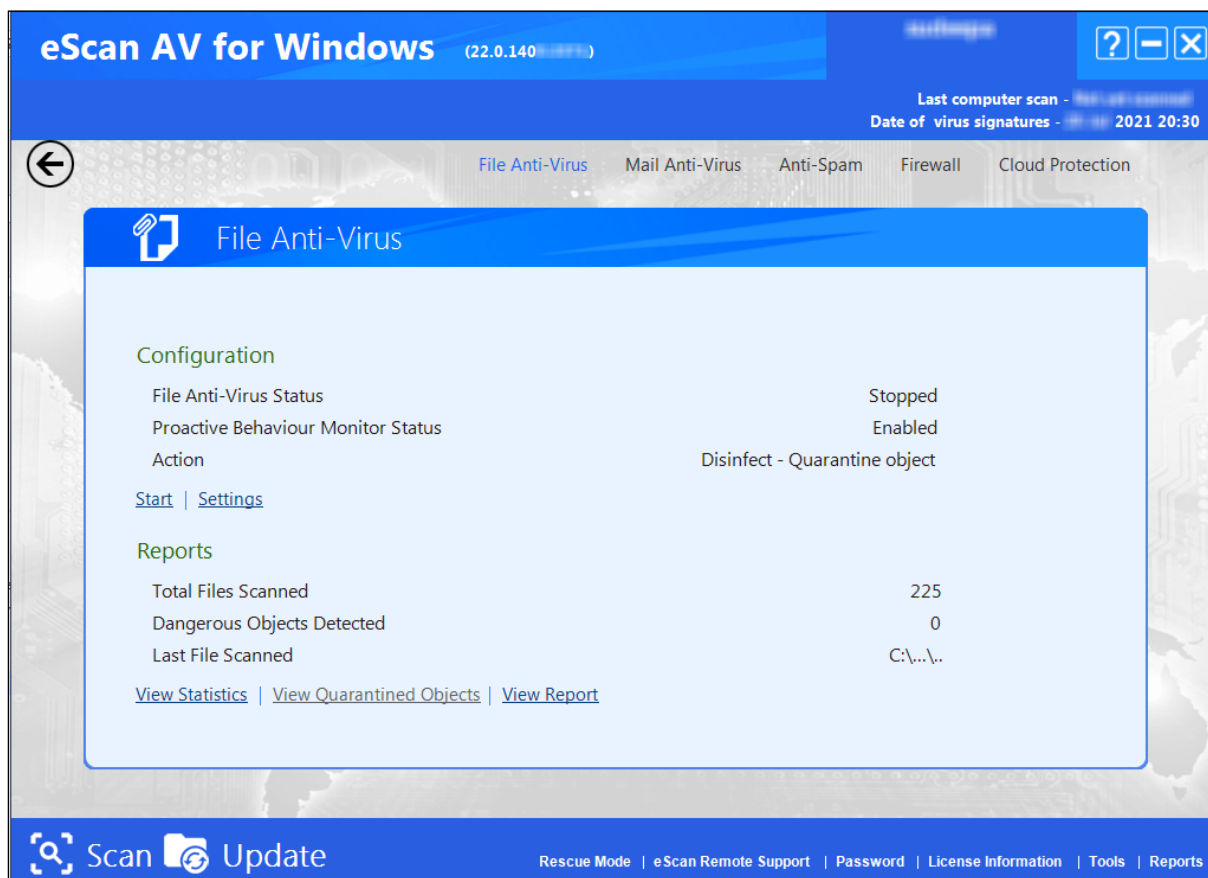
eScan displays the real-time status of the computer (secured or not secured) along with additional options buttons and quick access links.



File Anti-Virus

File Anti-Virus module prevents infection of the computer's file system. This module starts on the startup of the operating system and continuously monitors and scans all the files that opened, saved, or launched along with all the connected devices. The Proactive Behavior Monitoring system blocks any application that behaves maliciously or might be malicious.

eScan offers **Block Files** feature, which allows to block or quarantine the file from being accessed. It also comprises of **Folder Protection** function that prevents user from creating, updating, or deleting files/subfolders within the specified folder.



The File Anti-Virus window will have the following sections that can be configured.

- Configuration
- Reports

Configuration

This section displays the following information:

- **File Anti-Virus Status:** Displays the status of the File Anti-Virus module, that is, started or stopped.
- **Proactive Behaviour Monitor Status:** Displays the status of the proactive scanning.
- **Action:** It displays the type of action to be taken by File Anti-Virus module.
- **Start/Stop:** Click an appropriate option to start/stop or enable/disable File Anti-Virus module.
- **Settings:** To learn more, [click here](#).

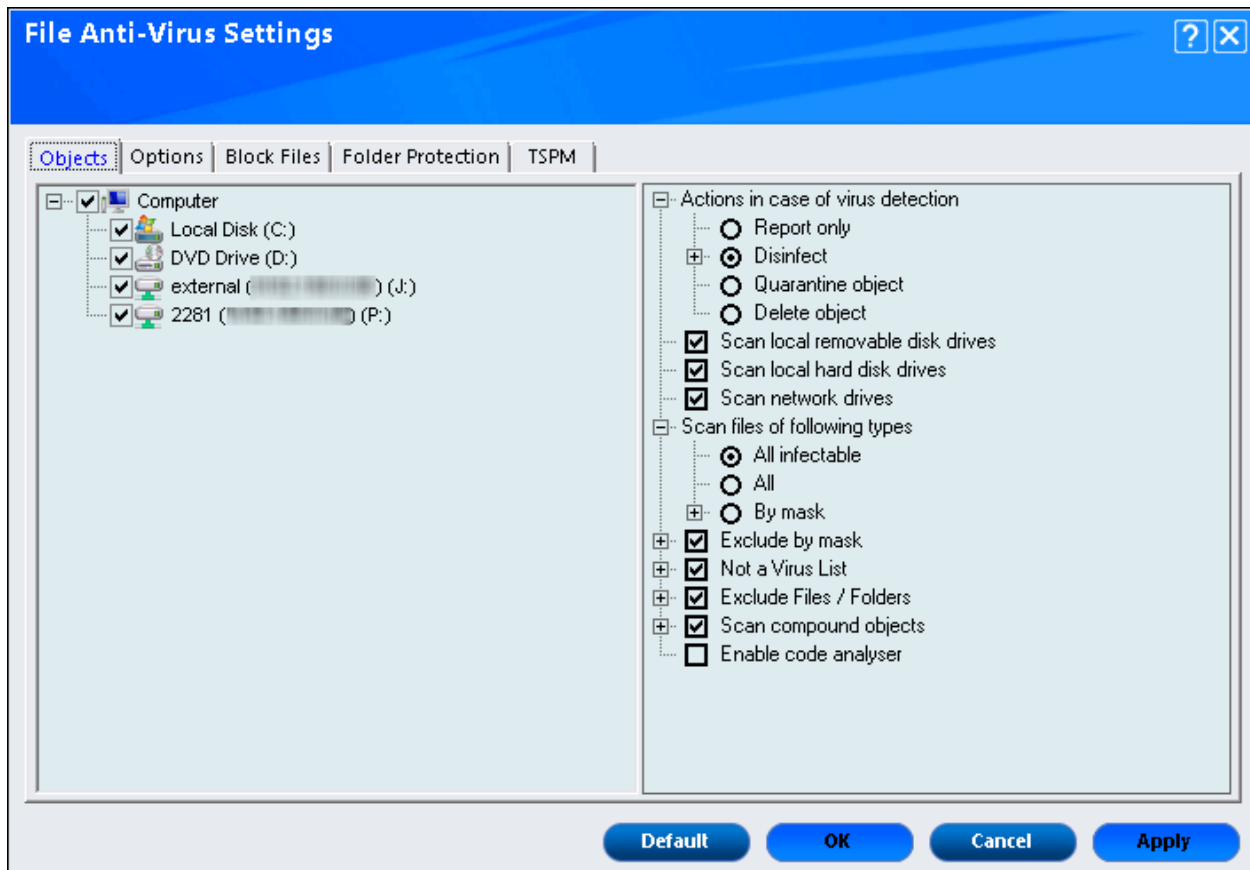
Settings

Configure settings for File Anti-virus using the settings option present under configuration. Following tabs are available for configurations:

- Objects
- Options
- Block Files
- Folder Protection
- TSPM

Objects

This tab will provide various options for fine tuning the settings available under File Anti-Virus. It provides options such as scanning a specific storage devices or excluding given file from scanning.



Actions in case of virus definition

Displays the different actions that can be performed in case of any infection detected. The actions are:

- **Report only:** Reports to you on a popup without taking any action on the file in case of virus detection.
- **Disinfect:** Automatically disinfect any infected file on detection. Under this action, following two options are available:
 - **Make backup file before disinfection:** This check box allows to make backup file before disinfection.
 - **If disinfection is impossible:** You can configure from the following options, in case of disinfection is impossible:
 - **Report Only:** This option reports if it is not able to disinfect any particular virus.
 - **Quarantine object:** This option quarantines the infected object (isolate the objects) if it is not able to disinfect a virus.
 - **Delete object:** This option deletes the object if it is not able to disinfect a virus.

By default the **Disinfect** option is selected.

- **Quarantine object:** Quarantines the file whenever an infection is detected (isolate the file). You can restore the **Quarantine/Backup** file by using the below procedure:

- Click **View Quarantine Objects** option present on the main interface of File Anti-virus. You will be forwarded to the **Quarantine** window, click object name that you wish to restore. Now click **Restore** button to restore. File will be restored instantly.
- **Delete object:** Automatically delete the file whenever an infected file is detected.

The following are the options that allow to scan specific disk or drive:

- **Scan local removable disk drives:** This check box allows to monitor the real-time scanning of all the local removable drives attached to the computer. This option is enabled by default.
- **Scan local hard disk drives:** This check box allows to monitor the real-time scanning of all the local hard drives installed on the computer. This option is enabled by default.
- **Scan network drives:** This check box allows to monitor the real-time scanning of all the network drives including mapped folders and drives that are connected to the computer. This option is enabled by default.

Scan files of following types

This check box allows to choose the type of file to monitor while real-time scanning. It have 3 options to select files for scanning, whether **All infectable**, **All**, or **By mask**. The files listed in **By mask** option are the default file extensions that are defined by eScan. To add or delete files by mask, select and double-click **Add/Delete** option, and then add or delete files as required.

Exclude by mask

This check box allows to monitors all the excluded object in the **Exclude by mask** list during real-time monitoring or scanning. You can add or delete a file or a particular file extension by double-clicking the **Add/Delete** option. This option is enabled by default.


Not a Virus List

File Anti-Virus is able to detect the riskware. Riskware are legitimate program that are not strictly malicious, but pose some sort of risk for the user in another way. 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 double-clicking the **Add / Delete** option, if you are certain that they are not malicious. By default, this option is enabled and riskware list is empty.

Exclude Files/Folders

This option excludes the listed files, folders, and subfolders, while monitoring or scanning the folders. You can add or delete folders from the existing list of folders by double-clicking the **Add / Delete** option. This option is enabled by default.

Scan compound objects

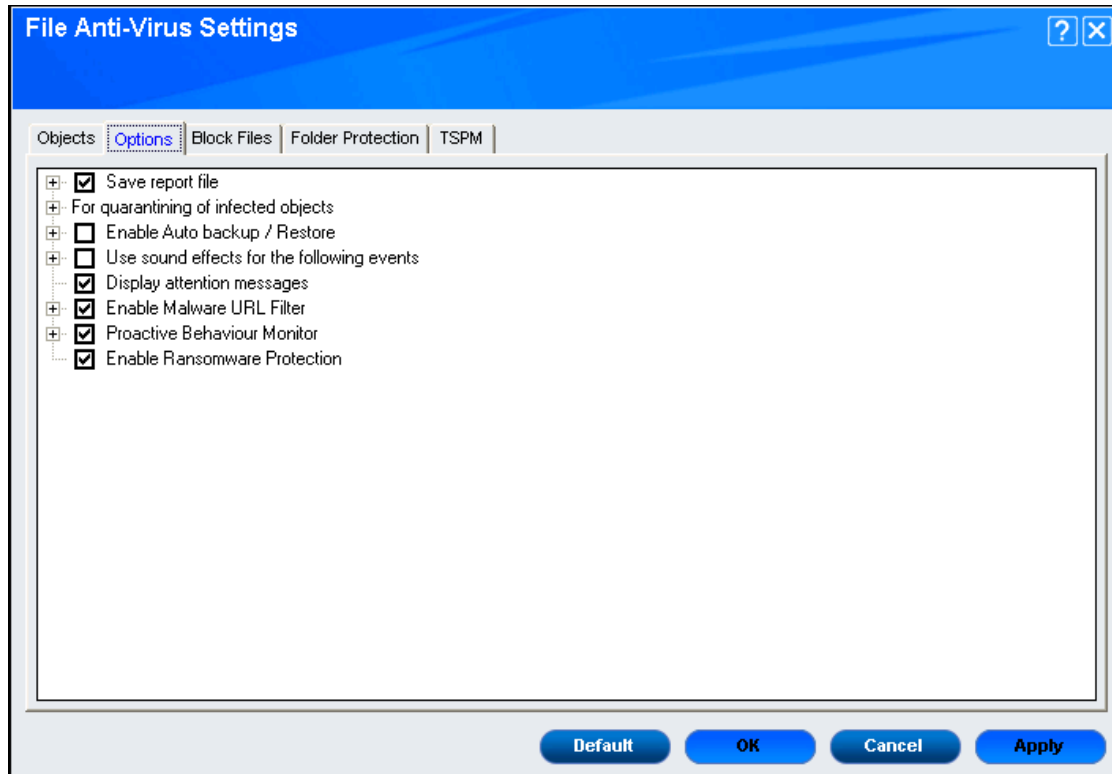
This option allows to scan the archives and packed files during the scan. The **Archive** check box allows to scan archive files. The depth level of an archived file up to which you want to scan can be defined in **Archive Depth Level** field. By default, value is 16, but you can change it by double-clicking the  icon, and then type value in the size box. By default, **Packed** is selected. This option is enabled by default.

Enable code analyser

This option uses heuristic analyzer during the real-time scan of the computer for suspicious objects or unknown infections. It not only scans and detects infected objects by using the definitions or updates, but it also checks for suspicious files stored on the computer.

Options

This tab will allow to configure the basic settings such as the maximum size of log files and path of the destination folder for storing log files, quarantined objects, and report files.



It provides the following options for configuration:

Save report file

This option allows to save the generated reports. The generated report consists of logs information about the scanned files and the action taken when an infected file is detected. This option is enabled by default and it also allows to configure following settings:


- **Show pack info in the report (Monvir.log):** This option is enabled by default and it allows to add details about the scanned compressed files, such as .ZIP and .RAR files to the Monvir.log file.
- **Show clean object info in the report (Monvir.log):** This option allows to add details about uninfected files found during a scan operation to the **Monvir.log** file. This option helps to find out which files are not infected.
- **Limit size to (KB) (avpM.rpt):** This option helps to set the size limit of the **avpM.rpt** file. To specify the size of the log file, double-click the size box and define the size. The default value is **50 KB**.

For quarantining of infected objects

This option helps to specify the destination for storing quarantined objects. By default, the quarantined objects are stored in the **C:\Program Files\eScan\INFECTED [32-bit]** OR **C:\Program Files (x86)\eScan\ INFECTED [64-bit]** folder. You can change the location of the destination folder if required.

Enable Auto backup / Restore

This option allows to takes automatic backup of critical files of the Windows® operating system installed on the computer and to restore the clean files when it finds an infection in any of the system files, which cannot be disinfected. This option allows to configure the following settings:

- **For backup of clean objects:** eScan allows to backs up uninfected objects and store them in a given folder. By default, these objects are stored in a folder named Fbackup on the drive that has maximum free space. You can change the path of the destination folder if desired.
- **Do not backup files above size (KB):** This option is enabled by default and helps to prevent File Anti-Virus from creating backup of files that is larger than the defined file size. The default value is set to **32768** KB.
- **Minimum disk space (MB):** This option is enabled by default and enables to set the minimum free hard disk space up to which you want eScan to take backup of files. By default, value is **1** MB, but you can change it by double-clicking the  icon, and then type value in the size box.

Use sound effects for the following events

This check box option allows to configure eScan to play a sound file and show the details regarding the infection within a message box when any malicious software is detected. However, you need to ensure that the computer speakers are switched on.

Display attention messages

This option allows to displays an alert, which consist the path, name of the infected object, and the action taken. This option is enabled by default.

Enable Malware URL Filter

This option blocks the access to malicious websites/URL.

Proactive Behaviour Monitor

This option allows to monitor the executable files that are running on your system. In case, if eScan finds any executable files suspicious that may cause any harm to your system, it alerts the user with a pop-up message. To access the suspicious file, you can White list them anytime.

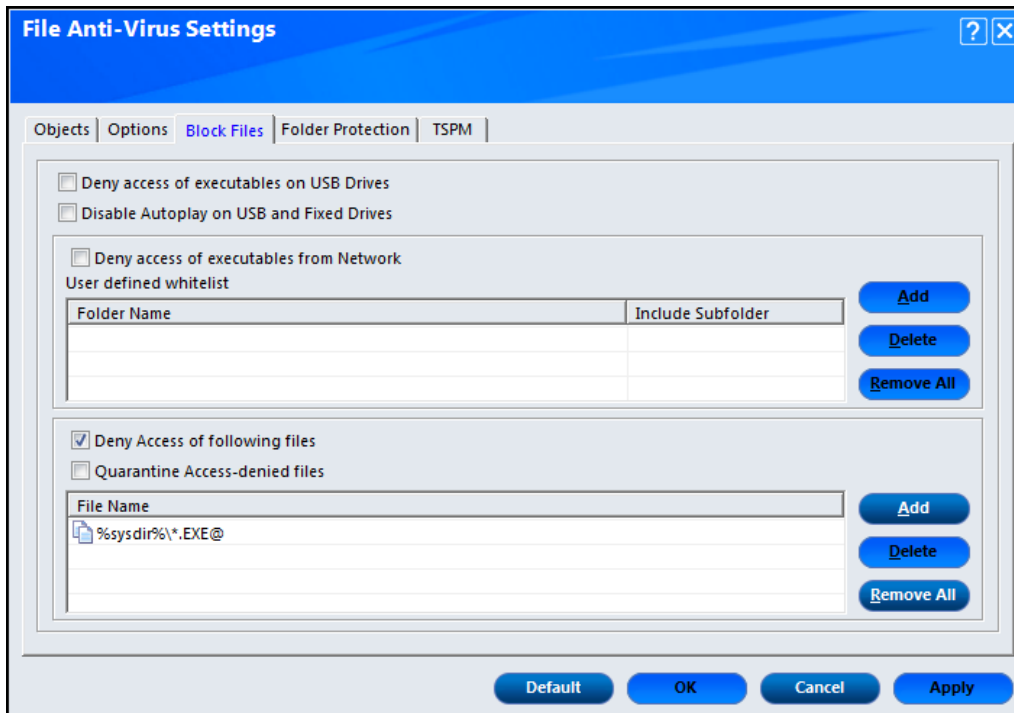
It also allows to view the list of files that are blocked from executing on the system. You can add a file to White list or Block list using this option.

Enable Ransomware Protection

This check box enables the protection against ransomware and enabled by default.

Block Files

This tab allows to configure the settings for preventing executable and files, such as autorun.inf, on network drives, USB drives, and fixed drives from accessing your computer.



It provides the following options for configuration:

Deny access of executables on USB Drives

This check box option helps to prevent executables stored on USB drives from being executed.

Disable Autoplay on USB and Fixed Drives

This check box option helps to disable Autoplay on USB and Fixed Drives.

Deny access of executables from Network

This check box option helps to prevent executables from network from being executed on the computer. This option also allows to whitelist the folder/subfolder on the network as per the requirement. The whitelisted folder/subfolder can be access the executable from them.

Deny Access of following files

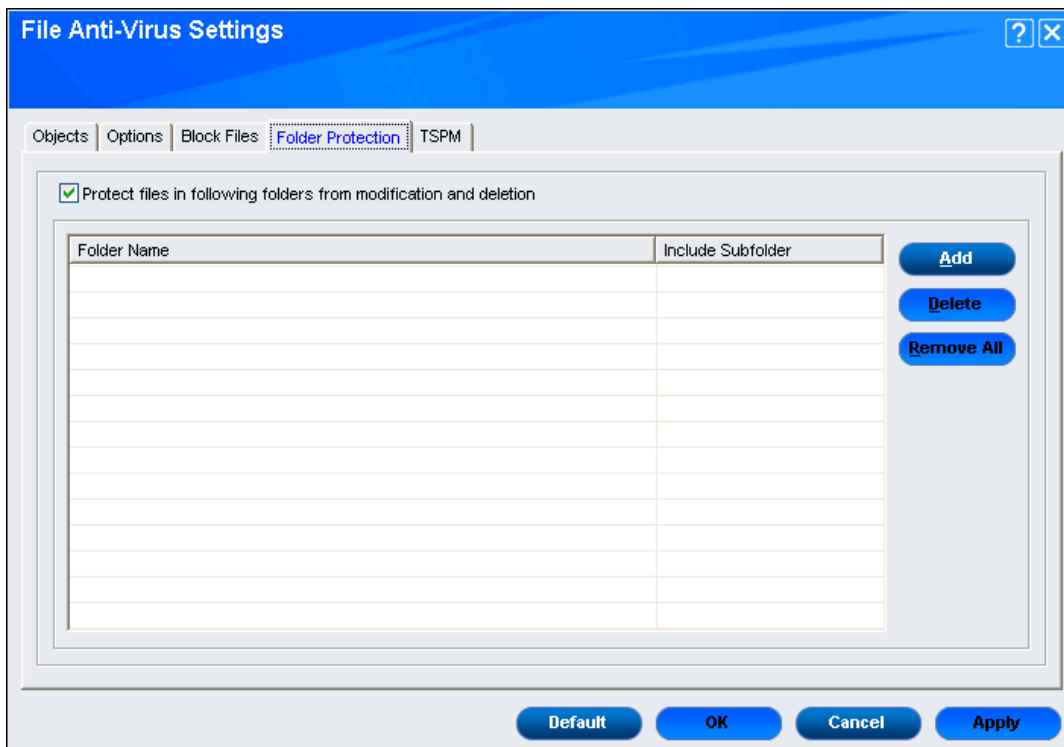
This check box option helps to prevent the files in the list from running on the computer. This option is enabled by default.

Quarantine Access-denied files

This check box option allows to quarantine files that have been denied access. To prevent specific files from running on the computer by adding them to the Block Files list. By default, this list contains the value `%sysdir%*.EXE@`.

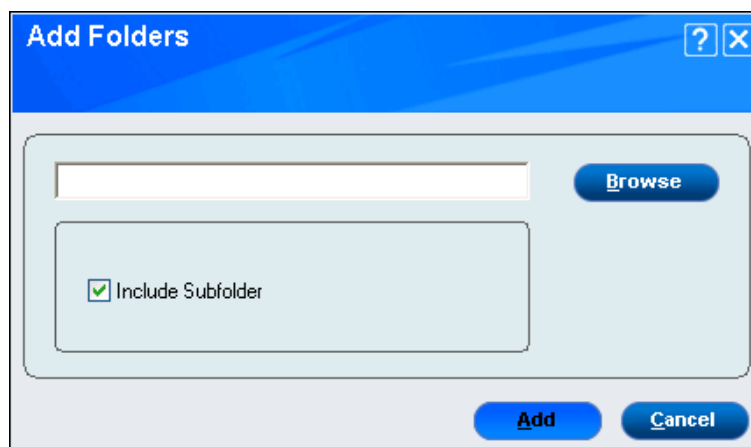
Folder Protection

This tab helps to protect specific folders from being modified or deleted by adding them to the Folder Protection list.

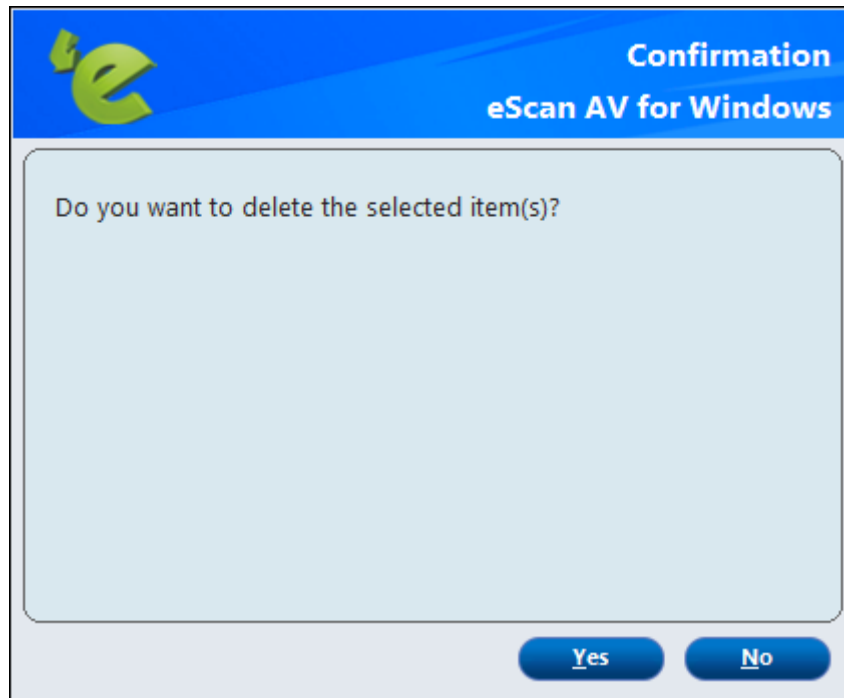


It provides the following options for configuration:

- **Protect files in following folders from modification and deletion:** This option is enabled by default. It protects the files in specific folders from being modified or deleted. Once you enable this check box, it will automatically enable the following buttons:
 - **Add:** It allows you Add folders to be protected. Browse the folders and Add in the Folder List. If you want to include sub folder of a folder, select **Include Subfolder** check box.



- **Delete:** You can delete the folder from Folder List. Click on the **Delete** button. A confirmation window appears.

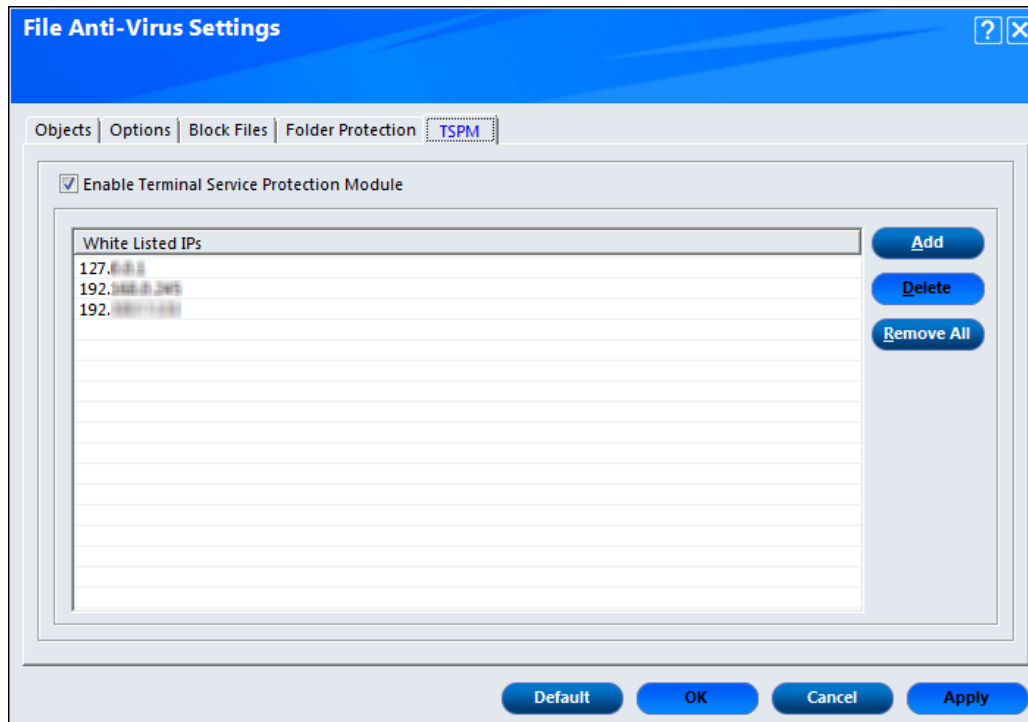


Click **Yes**, the folder will be deleted.

- **Remove All:** You can remove/delete all the folders in the list at once.

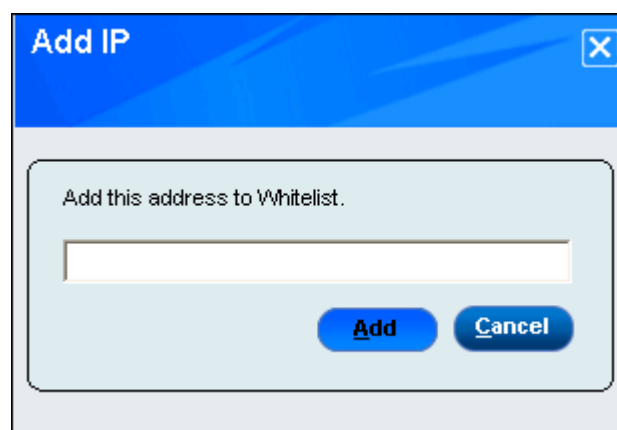
TSPM

TSPM – Terminal Services Protection Module by eScan detects brute force attempts and heuristically identifies suspicious IP Addresses/Hosts and blocks any attempts to access the system. In order to safeguard the systems from future attacks, the IP addresses and Hosts from these attacks are banned from initiating any further connections to the system.



Enable Terminal Service Protection Module


This option enables Terminal Service Protection Module. This will open a popup window from where you can add the IP address of the system you want to Whitelist.



After adding the IP address, click on **Add** button. It will be added in the list.

To delete the particular IP address, select the IP address and click **Delete** button.

To delete all the IP addresses at once, click **Remove All** button.

 At the bottom of the screen of all the tabs — **Default**, **OK**, **Cancel**, and **Apply** buttons are

NOTE	present that you can use after configuring the settings based on your requirement.
-------------	--

- **Default:** Click this button to apply the default settings.
- **OK:** Click this button after you click the Apply button to apply the configured settings.
- **Cancel:** Click this button to cancel the configured settings or to close the window.
- **Apply:** Click this button to apply the configured settings.

Reports

This section displays the information along with the reports, which are as follows:

Total Files Scanned

It shows the total number of files scanned by the real-time File Anti-Virus monitor.

Dangerous Objects Detected

It shows the total number of viruses or malicious software detected by the File Anti-Virus monitor on a real-time basis.

Last File Scanned

It shows the name of last file scanned by File Anti-Virus monitor on real-time basis.

View Statistics

When you click this button, the statistics dialog box is displayed, which displays the latest activity report of the real-time monitor. The report contains information under two sections:

- **Scanned:** This section shows scanned details of objects of Virus bodies, Disinfected, Deleted, Quarantined etc.

- **Found:** This section shows Virus details such as Virus bodies, Disinfected, Deleted, Quarantined, etc.

Statistics
?
✕

Tuesday, February 23, 2021 05:14:37 PM	
Anti-Virus bases were loaded. Known viruses:	eScan Anti-Virus Monitor is loaded 9758802

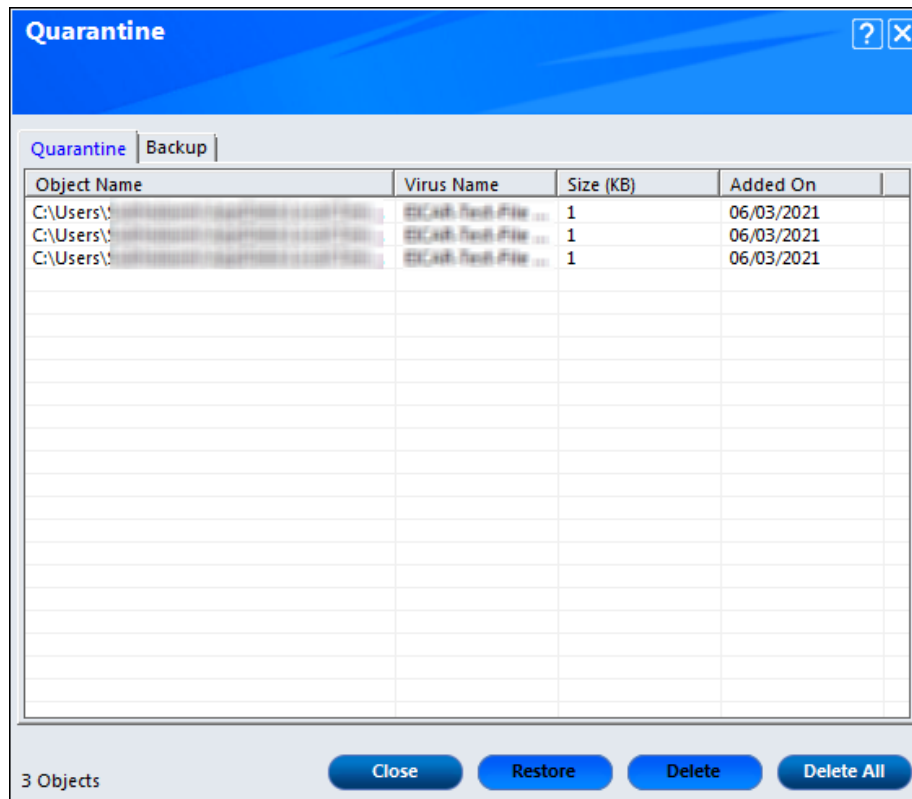
Scanned:	
Objects	95
Compound objects	0
Packed objects	0
Last object	C:\WINDOWS\system32\cabview.dll
Virus Name	
Clean objects	95
Found:	
Known Virus	0
Virus bodies	0
Disinfected	0
Deleted	0
Quarantined	0
Suspicious	0
Corrupted	0
I/O Errors	0

Refresh
Close

View Quarantined Objects

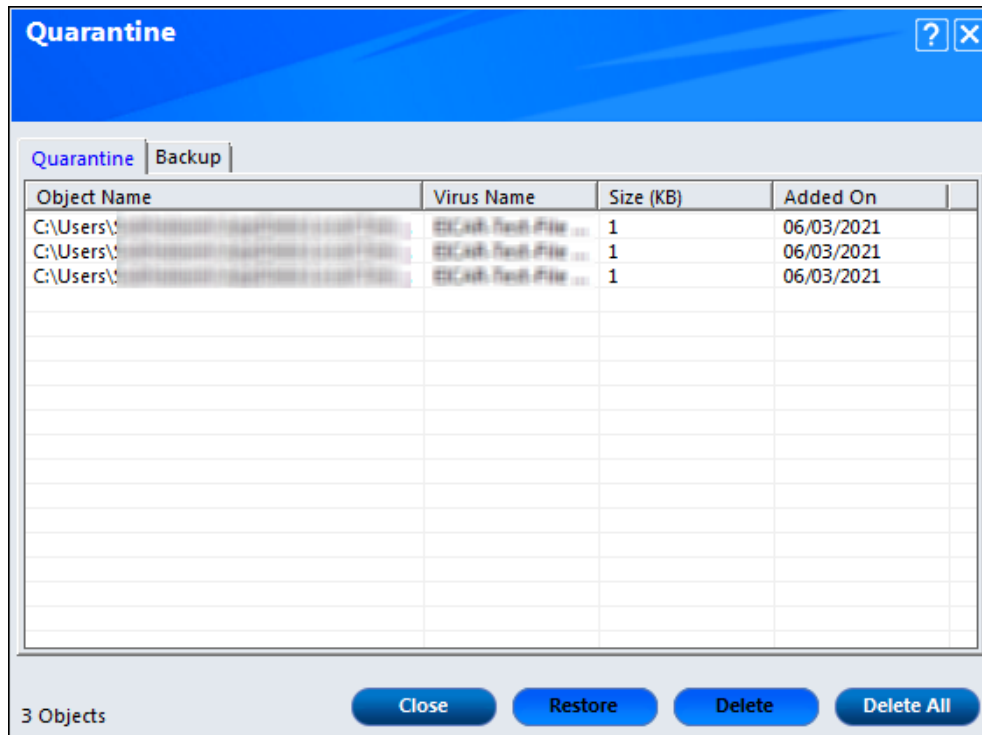
Click on **View Quarantined Objects**, Quarantine popup gets displayed. It displays all the quarantined objects. There are two tabs present, Quarantine and Backup.

- **Quarantine:** This tab displays the files that have been quarantined. You can restore or delete the quarantined objects by right-clicking the object, and then clicking an appropriate option.



- **Close:** This option close the Quarantine window.
- **Restore:** It will allow you to restore the quarantined files.
- **Delete:** This button delete the selected quarantined file.
- **Delete All:** This button removes all the quarantined files at once.

- Backup:** This tab displays the files that were backed up by File anti-virus before it tried to disinfect them. You can restore or delete the objects that were backed up by right-clicking the object, and then clicking an appropriate option. Before clicking any of these buttons, you should ensure that you have selected an appropriate row in the table for which you need to perform the action.



- Close:** This option close the Quarantine window.
- Restore:** It will allow you to restore the backup files.
- Delete:** This button delete the selected backup file.
- Delete All:** This button removes all the backup files at once.

View Report

When you click this button, the report for File anti-virus window is displayed. This window displays the report for the File anti-virus module for a given range of dates in a tabular format when you click the **Generate Report** button.

The screenshot shows a window titled "Report For File Anti-Virus". At the top right are help, print, and close icons. Below the header is a form with three dropdown menus: "From:" (10-Mar-2021), "To:" (10-Mar-2021), and "Filter by:" (All Users). A "Generate Report" button is to the right. Below the form is a table with the following data:

Date/Time	User	Name	Description	Action
3/10/2021 09:07:58	Sutthal...	eScan Monitor	New virus database ta...	Update...
3/10/2021 09:07:58	Sutthal...	eScan Monitor	eScan monitor succes...	No Acti...
3/10/2021 10:13:59	Sutthal...	eScan Monitor	New virus database ta...	Update...
3/10/2021 10:13:59	Sutthal...	eScan Monitor	eScan monitor succes...	No Acti...

At the bottom of the window are three buttons: "Export", "Refresh", and "Close".

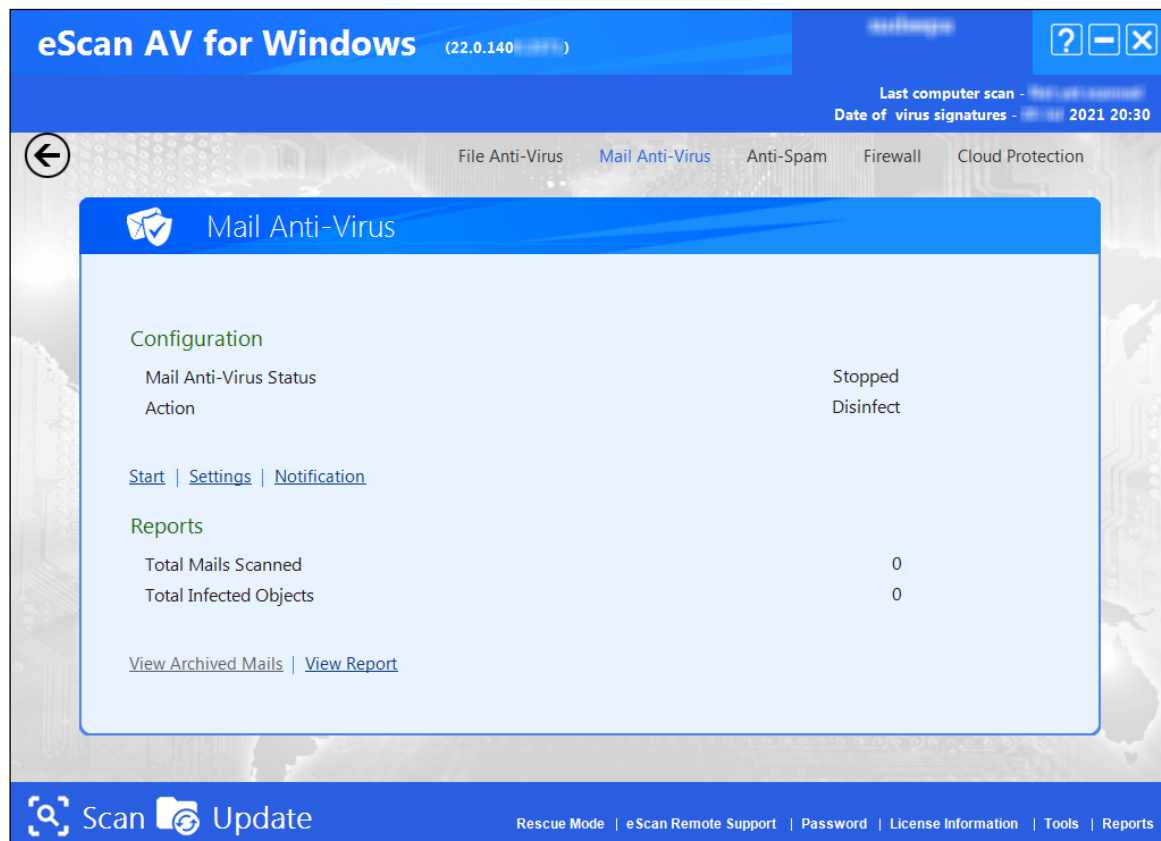
To refresh the generated report, click **Refresh** button. Click **Close**, to close report window. You can export the generated report using **Export** button.

You can export reports in the following formats:

- PDF
- HTML
- CSV

Mail Anti-virus

Mail Anti-Virus scans all incoming and outgoing emails for viruses, spyware, adware, and other malicious objects. It helps 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 helps you notify the sender or system administrator, whenever you receive an infected email or attachment.



This page provides you with options required for configuring the module. You can configure the settings from the following sections.

Configuration

This section displays the following information:

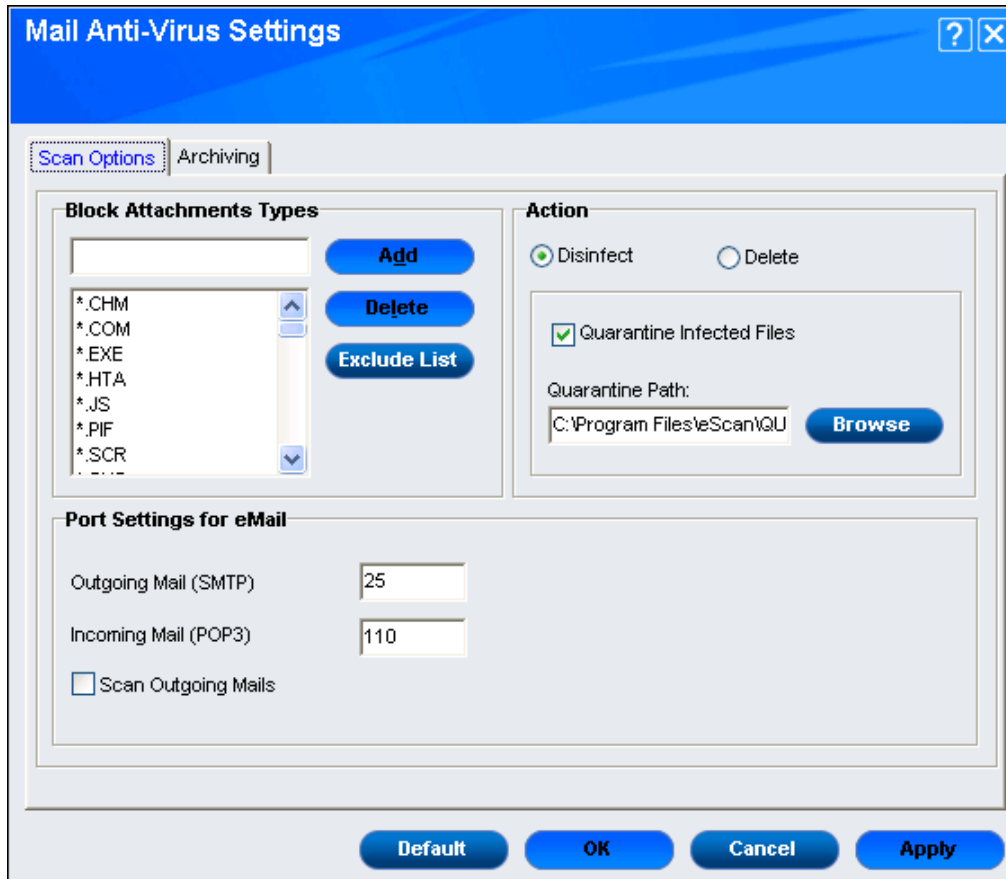
- **Mail Anti-Virus Status:** It displays the status whether Mail Anti-Virus module is started or stopped.
- **Action:** It displays the type of action set in the Mail Anti-Virus module.
- **Start/Stop:** Click an appropriate option to start/stop or enable/disable Mail Anti-Virus module.
- **Settings:** To learn more [click here](#).
- **Notification:** To learn more [click here](#).

Settings

When you click this button, the Mail Anti-Virus Settings window appears. On the Mail Anti-Virus Settings window, you have two tabs – Scan Options and Archiving.

Scan Options

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



This tab helps you to configure the following setting:

Block Attachments Types

This section provides you with a pre-defined 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 host level. You can add file extensions to this list as per your requirement. 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. There are three options present in this setting:

- **Add:** You can add the extension that need to be blocked while scanning the emails.
- **Delete:** You can delete the extension from the Block Attachments Types list by default.
- **Exclude List:** You can click this button to whitelist attachments.

Action

This section helps you configure the actions to be performed on infected emails which are as follows:

- **Disinfect:** This option is selected by default. Click this option if you want Mail Anti-Virus to disinfect infected emails or attachments.
- **Delete:** Click this option if you want Mail Anti-Virus to delete infected emails or attachments.

In both of the above cases you can **Quarantine Infected Files** which is selected by default. Select this check box 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** which you can specify in **Quarantine Path**. However, you can specify a different path for storing quarantined files, if required.

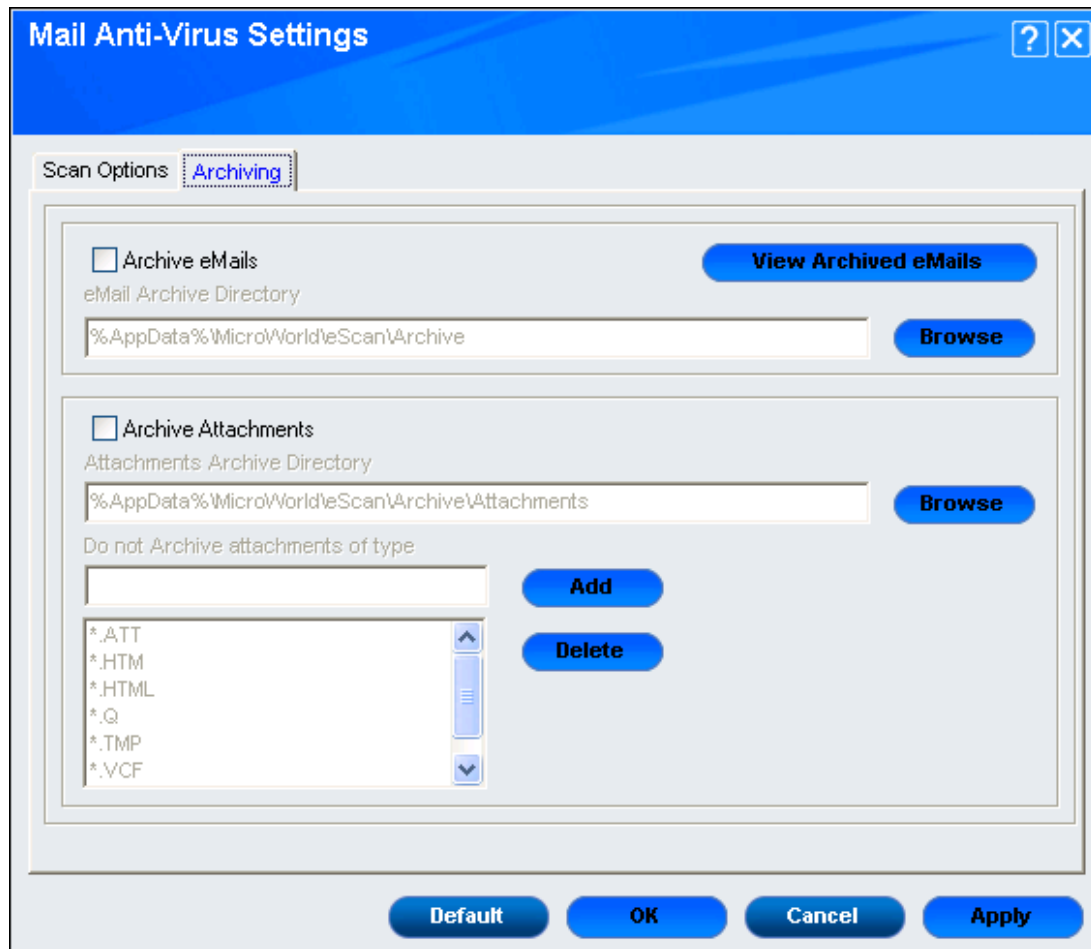
Port Settings for eMail

This section allows you to specify the ports for incoming and outgoing emails, so that eScan can scan the emails sent or received through those ports. You can configure the ports for the mail connections:

- **Outgoing Mail (SMTP):** You need to specify a port number for SMTP. The default port number for SMTP is 25.
- **Incoming Mail (POP3):** You need to specify a port number for POP3. The default port number for POP3 is 110.
- **Scan Outgoing Mails:** Select this check box if you want the Mail Anti-Virus to scan outgoing emails.

Archiving

This tab helps you configure settings for archiving emails and email attachments.



The following configuration options are available:

Archive eMails

This check box option helps you archive or back up all scanned emails that you have sent or received.

The Mail Anti-Virus provides you with the facility of backing up your emails to a given folder. The default path for storing archived emails is **%appdata%\MicroWorld\eScan\Archive**.

You can also change the default path by clicking on **Browse** button and provide the path.

Click on **View Archived eMails** button to view archived mails in report format.

The screenshot shows a window titled "Archived eMails" with a blue header. Below the header is a toolbar with buttons: Refresh, Stop, View, Find, Delete, and Message Source. There is also a checkbox for "Include Subfolders". Below the toolbar is a "Folder Path" field with a "Browse" button and a "File Types" field with a dropdown menu. There are also checkboxes for "Show Attachment(s)" and "Open eMail(s) with MailClient". Below these fields is a table with the following columns: From, To, Cc, Subject, Received, Size (Bytes), Attachment(s), and File. The table contains two rows of data. At the bottom of the window, there is a status bar that says "Total Mails found: 2".

From	To	Cc	Subject	Received	Size (Bytes)	Attachment(s)	File
Gurdeep Singh ...	<gaur@es...>		Re: TSPM disable	Tue, 12 Jan 202...	3465		Re
<gaur@es...>	<gaur@es...>		Regarding upd...	Fri, 22 Mar 201...	1846		Re

Following are the options to configure archived emails:

- **Refresh:** This button refreshes the whole list.
- **Stop:** Click on this button to stop from refreshing list.
- **View:** It displays the detail of email that has been archived.
- **Find:** To search the particular email from the list, click this button.
- **Delete:** Click this button to delete existing archived mail.
- **Message Source:** This button gives you the source of the email.
- **Include Subfolder:** If you want to include sub folder of a folder, select this check box.


It has the following fields:

- **From:** Contains the email address of the sender.
- **To:** Contains the email address of the recipients.
- **Cc:** Contains the email address of the recipients cced in the email.
- **Subject:** Contains the subject of the email.
- **Received:** shows you date/time of received the email.
- **Size (Bytes):** Gives you the size of the email in bytes.
- **Attachment(s):** Gives you the details of the attachments in the email.
- **Filename:** Gives you the Filenames of the attachment present in the email.
- **URLs:** Gives you the URLs present in the email if any.

Archive Attachments

This check box option helps you to archive or back up all sent or received email attachments to a given folder. However, to specify the path of the backup folder, you need to select the **Archive Attachments** check box. By default, the **Attachments Archive Directory**, **Do not Archive attachments of type**, and **Browse** button appear dimmed. These fields are available only when you select the Archive Attachments check box. The default path for storing archived email attachments is **%AppData%\MicroWorld\eScan\Archive\Attachments** that can be changed if needed. At times, you may not require email attachments of a specific file type. In that case, you can exclude certain file types, such as *.VCF, *.HTM, and *.HTML, from being archived by adding them to the **Do not Archive attachments of type** list. This option provides two buttons:

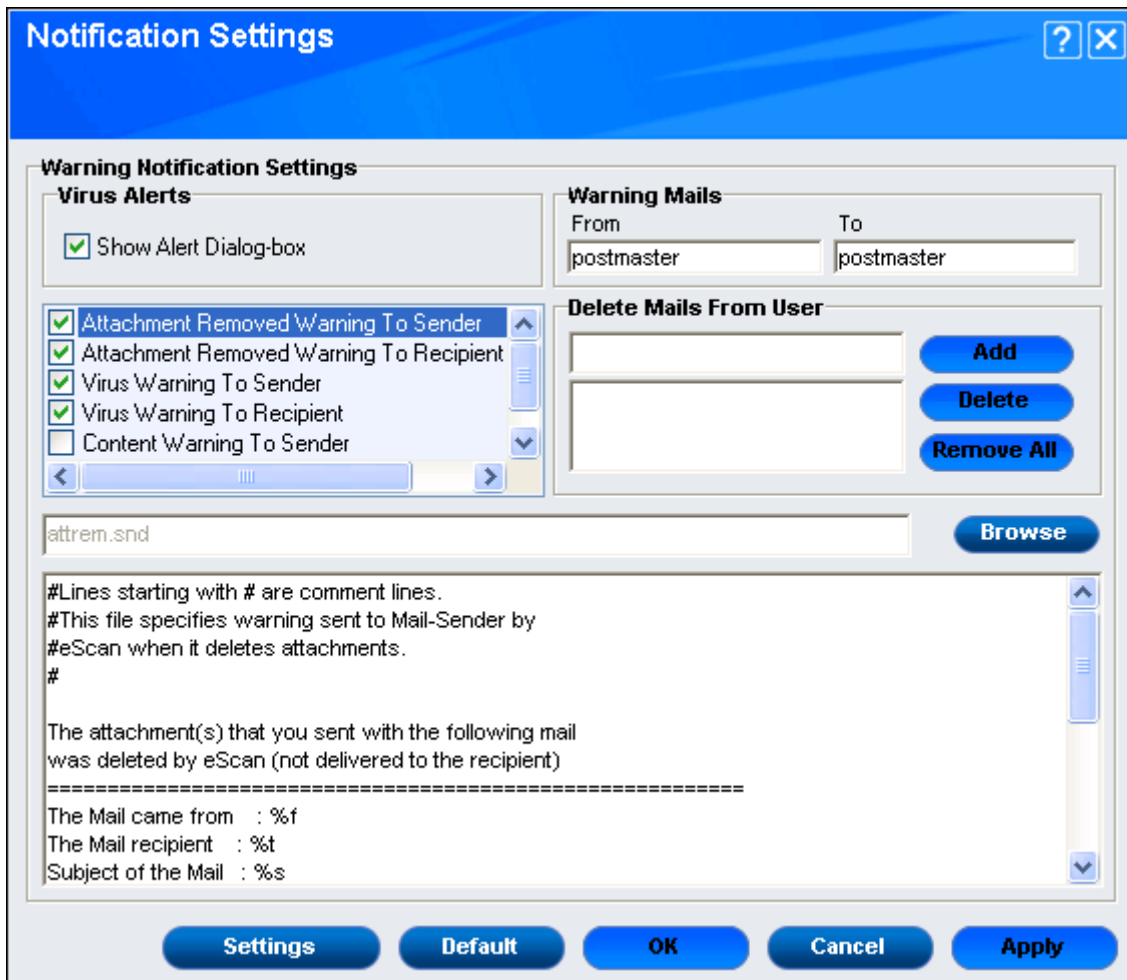
- **Add:** You can add extension that you want to exclude from being archived.
- **Delete:** You can delete the extension that you want to remove from the exclude list.

 NOTE	At the bottom of the screen of all the tabs — Default , OK , Cancel , and Apply buttons are present that you can use after configuring the settings based on your requirement.
--	--

- **Default:** Click this button to apply the default settings.
- **OK:** Click this button after you click the Apply button to apply the configured settings.
- **Cancel:** Click this button to cancel the configured settings or to close the window.
- **Apply:** Click this button to apply the configured settings.

Notification

This option opens the Notification Settings dialog box, which helps you configure the notification settings. By configuring, you can send emails to specific recipients when malicious code is detected in an email or email attachment. This helps you to configure the Virus Alerts, Warning Mails, Delete emails From Users, Settings, Default, OK, Cancel, and Apply options.



You can configure the Warning Notification Settings:

Virus Alerts

This setting has **Show Alert Dialog-box** option that is selected by default. Select this check box if you want Mail Anti-Virus to alert you when it detects a malicious object in an email. It has more options to configure the alerts which are as follows:

- **Attachment Removed Warning To Sender:** Select this check box if you want Mail Anti-Virus to send a warning message to the sender of an infected attachment. The Mail Anti-Virus sends this email when it encounters a virus-infected attachment in an email. The content of the email that is sent is displayed in the preview box. This option is selected by default.
- **Attachment Removed Warning To Recipient:** Select this check box if you want Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The content of the email that is sent is displayed in the preview box. This option is selected by default.

- **Virus Warning To Sender:** Select this check box if you want Mail Anti-Virus to send a virus-warning message to the sender. The content of the email that is sent is displayed in the preview box. This is selected by default.
- **Virus Warning To Recipient:** Select this check box if you want Mail Anti-Virus to send a virus-warning message to the recipient. The content of the email that is sent is displayed in the preview box. This option is selected by default.
- **Content Warning To Sender:** Select this check box if you want Mail Anti-Virus to send a content warning message to the sender. The content of the email that is sent is displayed in the preview box. This option is selected by default.
- **Content Warning To Recipient:** Select this check box if you want Mail Anti-Virus to send a content warning message to the recipient. The content of the email that is sent is displayed in the preview box. This option is selected by default.

Warning Mails

You can configure this setting if you want Mail Anti-Virus to send warning emails and alerts from sender to a given recipient. The default sender (**From** field) is postmaster and the default recipient (**To** field) is postmaster.

Delete emails From User

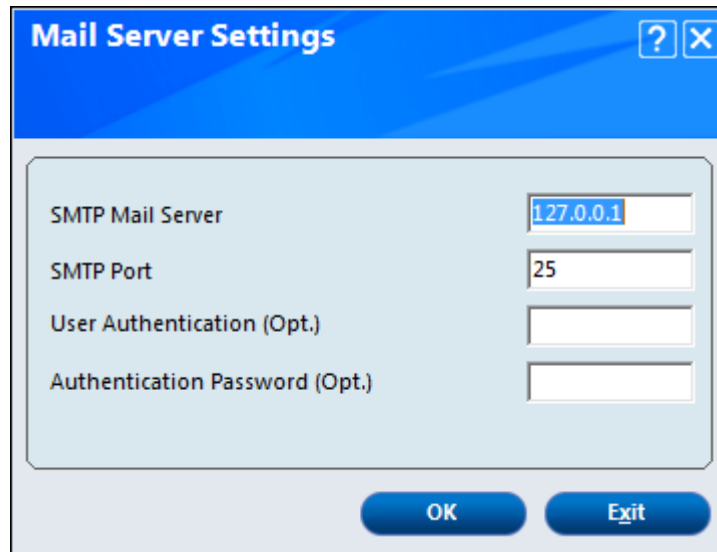
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the mail addresses of such users to the **Delete emails From User** list. By default, the **Delete emails From User** section fields are unavailable; it is available only when you type in some text in the Delete emails From User field. It has three buttons:

- **Add:** You can add email addresses of the users so that it deletes the email from that users.
- **Delete:** You can delete the email addresses of the users that is already present in the list.
- **Remove All:** You can remove all the email addresses at once by clicking on this button.

Settings

Click on Settings to configure Mail Server settings. This has following configuration:

- **SMTP Mail Server:** Enter SMTP Mail Server details
- **SMTP Port:** Enter the port number for SMTP.
- **User Authentication (Opt.):** This is optional field. You can enter the username for authentication, if set.
- **Authentication Password (Opt.):** This is optional field. You can enter the password for same username for authentication.



The image shows a dialog box titled "Mail Server Settings" with a blue header bar containing a question mark icon and a close button. The main area is light blue and contains four input fields: "SMTP Mail Server" with the value "127.0.0.1", "SMTP Port" with the value "25", "User Authentication (Opt.)", and "Authentication Password (Opt.)". At the bottom, there are two buttons: "OK" and "Exit".

This dialogue box has two buttons:

- **OK:** To save the configured setting.
- **Exit:** To exit the dialogue box without saving the configuration.

Default

Click this button to apply the default settings.

OK

Click this button after you click the Apply button to apply the configured settings.

Cancel

Click this button to cancel the configured settings or to close the window.

Apply

Click this button to apply the configured settings.

Reports

This section displays following information along with the reports:

Total Mails Scanned

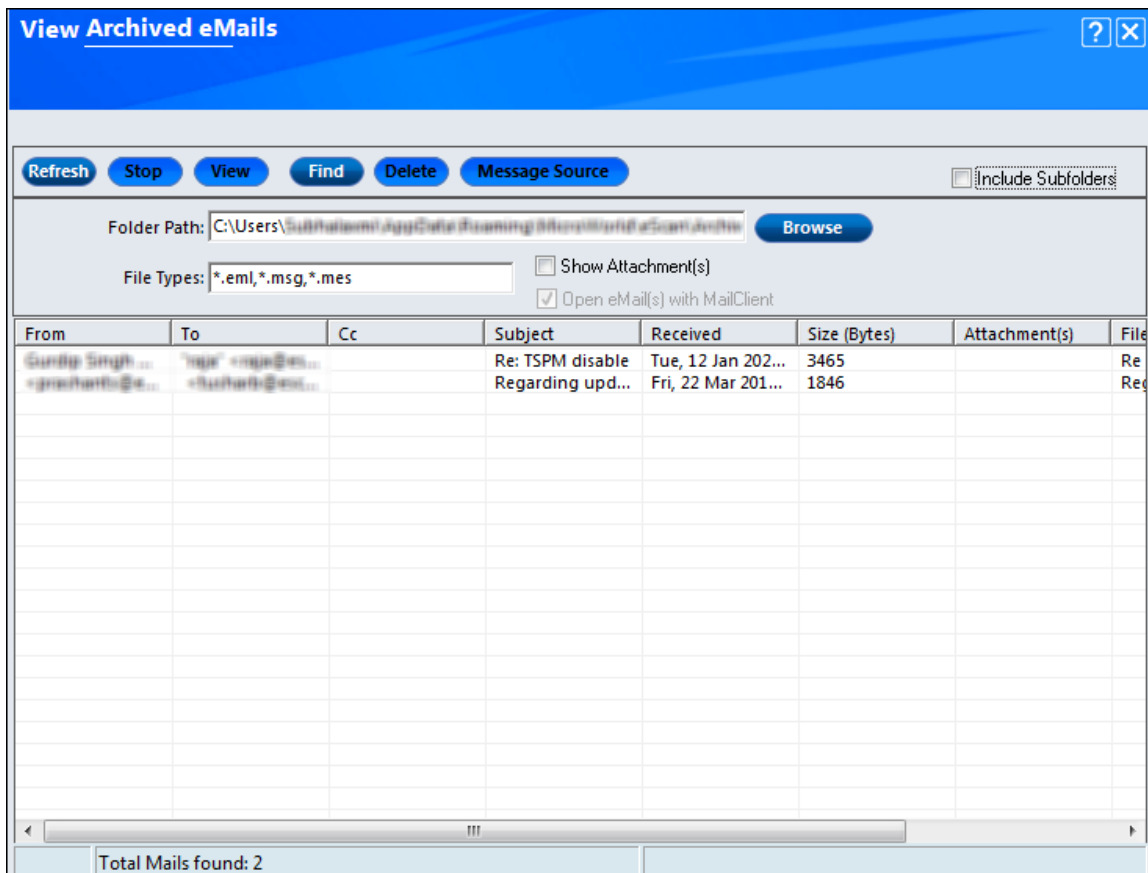
It displays total emails scanned by Mail Anti-Virus module on a real-time basis.

Total Infected Objects

It displays total number of infected objects found by Mail Anti-Virus module on a real-time basis.

View Archived Mails

You can click this button to open the View Archived eMails window (for more information on archived email settings, refer archived tab under Mail Anti-Virus settings window).

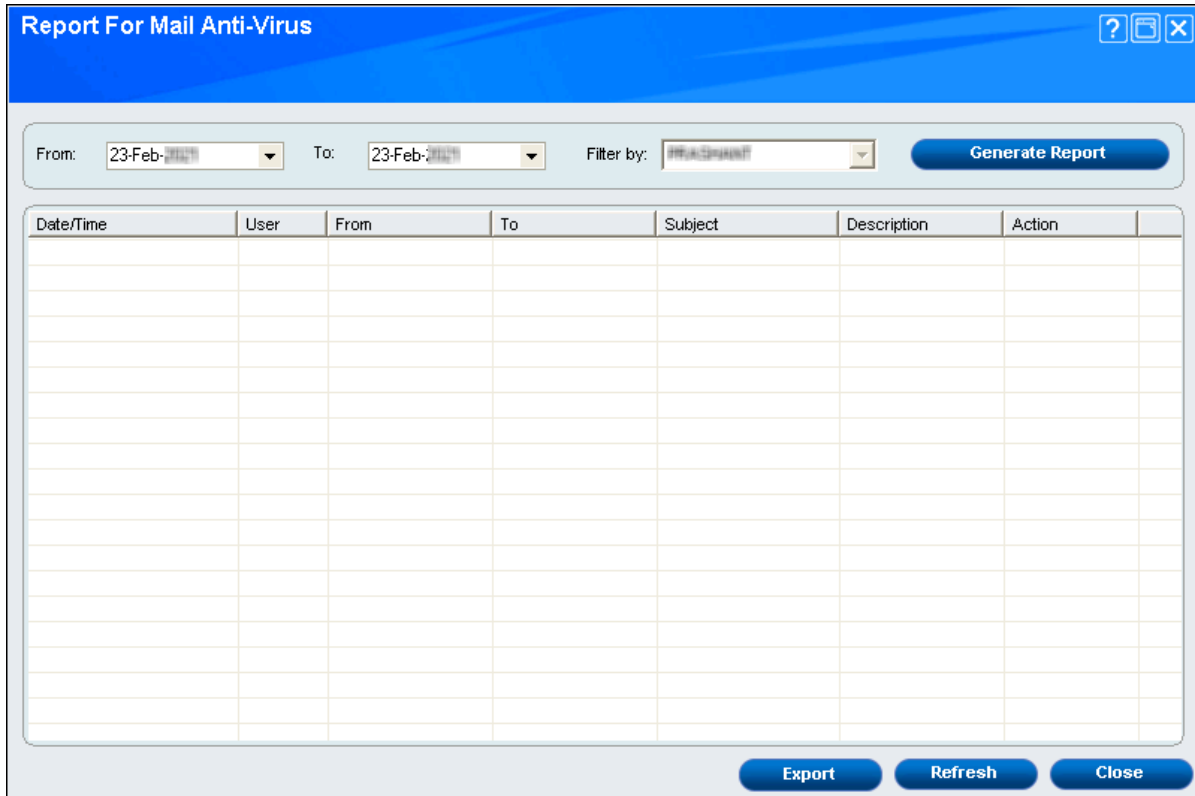


Following are the options to configure archived emails:

- **Refresh:** This button refreshes the whole list.
- **Stop:** Click on this button to stop from refreshing list.
- **View:** It displays the detail of archive mails.
- **Find:** To search the particular email from the list, click this button.
- **Delete:** Click this button to delete existing archived mail.
- **Message Source:** This button gives you the source of the email.
- **Include Subfolder:** If you want to include sub folder of a folder, select this check box.

View Report

This button is used to open the **Report For Mail Anti-Virus** window. This window displays the summary of infected emails and the action taken on such emails for a given range of dates in a tabular format when you click the **Generate Report** button.



Report For Mail Anti-Virus

From: 23-Feb-2024 To: 23-Feb-2024 Filter by: #1A-Quarant...

Date/Time	User	From	To	Subject	Description	Action

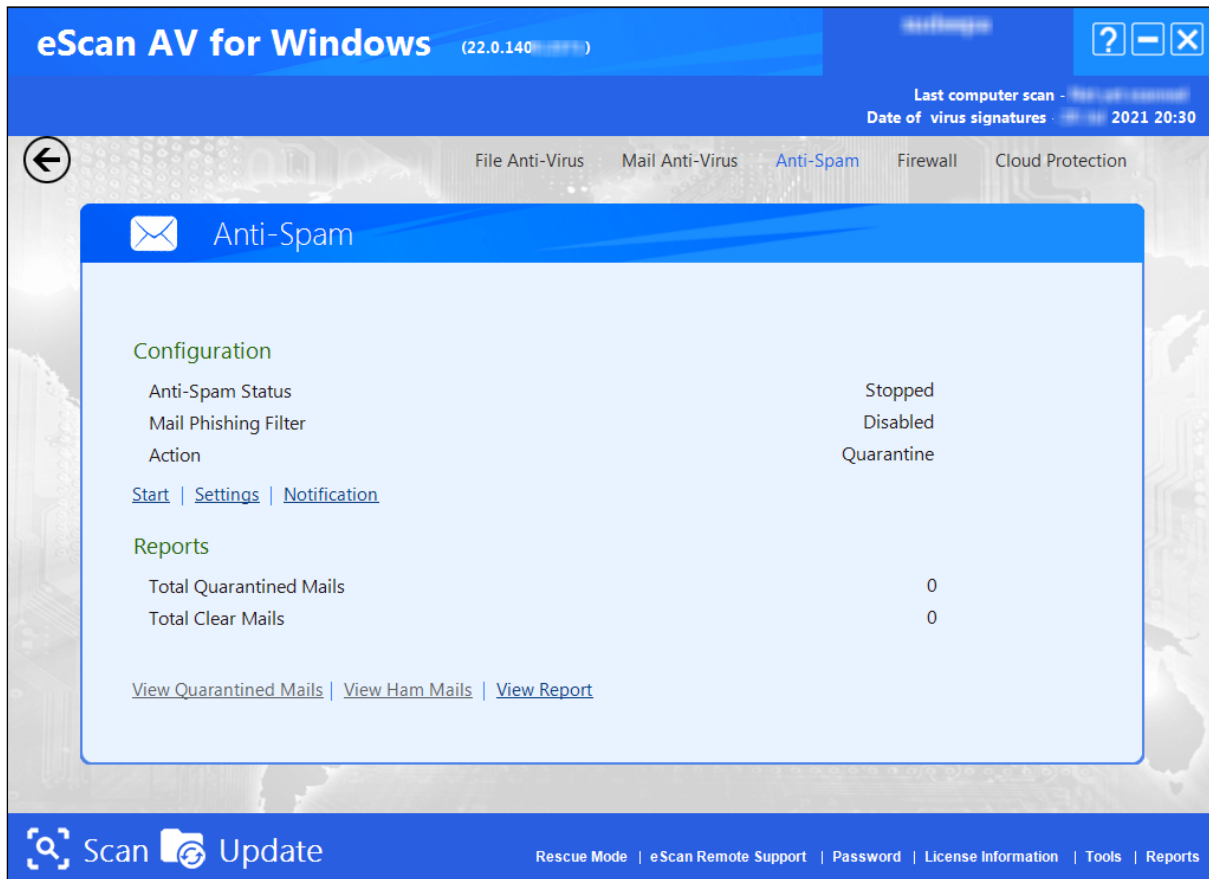
Export Refresh Close

You can export the reports in the following format:

- PDF
- HTML
- CSV

Anti-spam

Anti-Spam module filters all your junk and spam emails by using the NILP technology and sends content warnings to specified recipients.



NOTE Anti-Spam does not provide protection for email accounts that you access through a web-based email service.

This page provides you with options required to configure the module. You can configure the settings from the following sections.

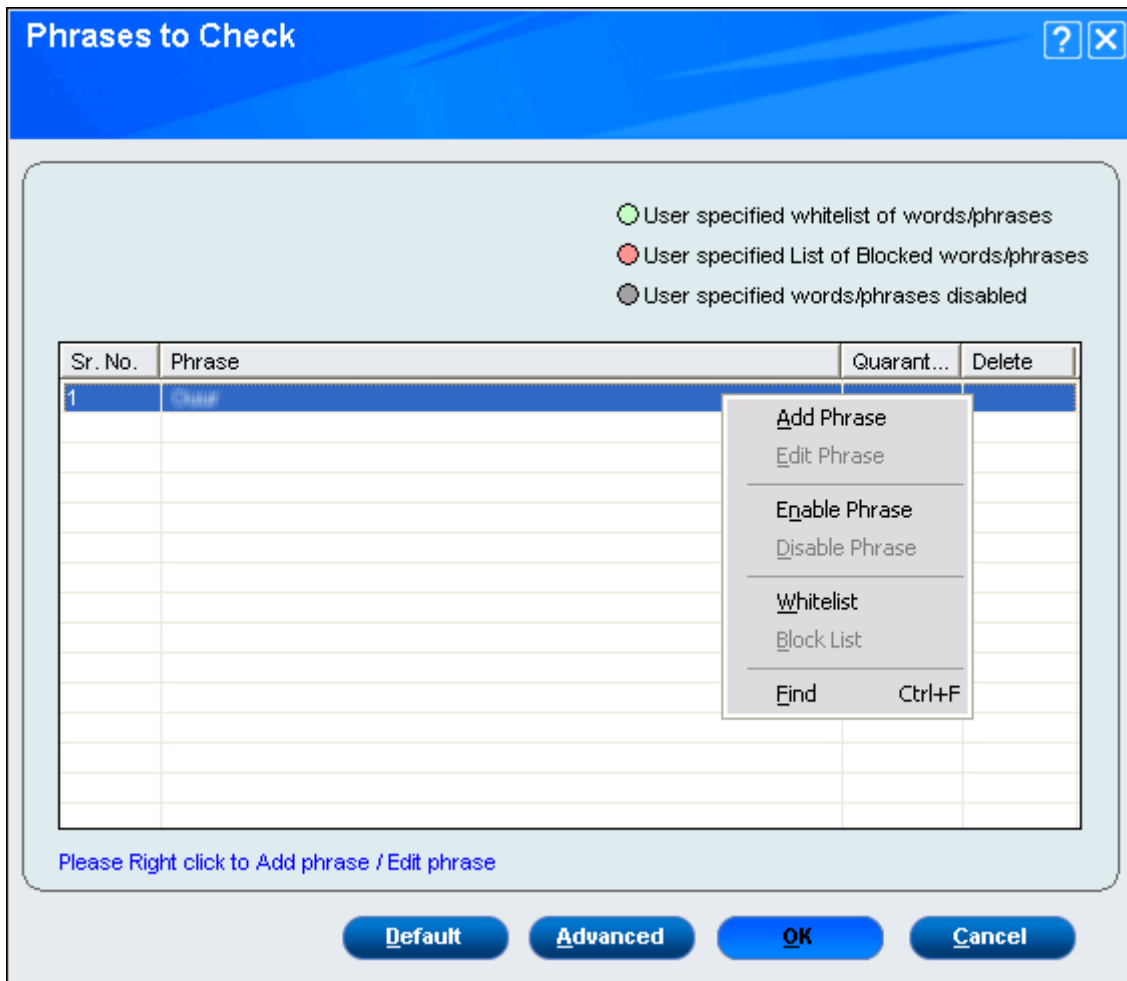
Configuration

This section displays the following information:

- **Anti-Spam Status:** It displays the status whether Anti-Spam module is started or stopped.
- **Mail Phishing Filter:** It displays the status of Mail phishing filter.
- **Action:** It displays the type of action taken by Anti-Spam module.
- **Start/Stop:** This option is used to enable or disable Anti-Spam module.
- **Settings:** To learn more [click here](#).
- **Notification:** To learn more [click here](#).

Settings

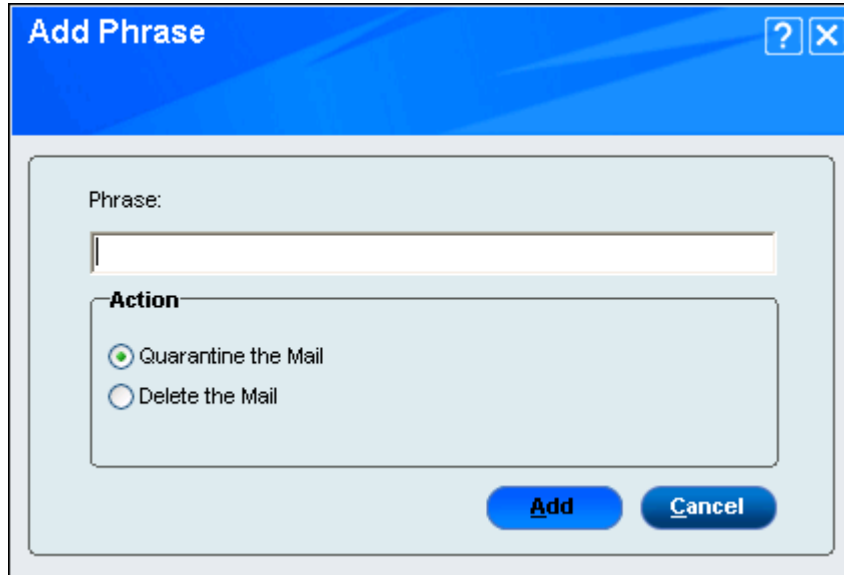
When you click this button, the **Anti-Spam Settings** window appears. The following section explains the same in detail:



You can configure the following settings:

Right click to Add phrase/ Edit phrase

When you right-click on the table you will get a popup window. In the popup click on **Add Phrase**, Add Phrase dialogue box appears.

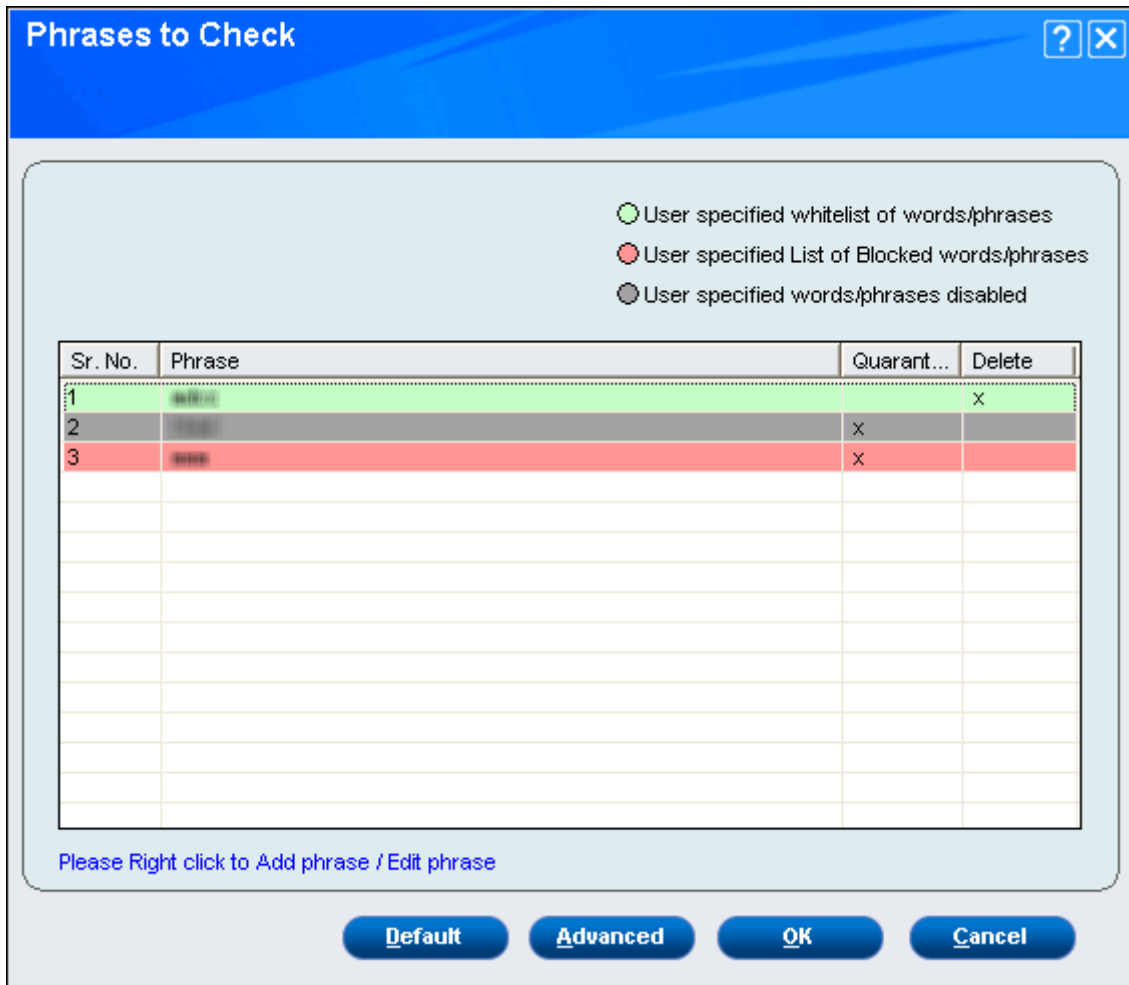


Phrase: You can add certain words or phrases, so that mails containing those words or phrases in the subject, header, or body part of an email are recognized as spam. Once you add the phrase you can edit the phrase along with the actions defined by you, which are as follows:

- **Quarantine the Mail:** This option is selected by default. Select this option to the quarantine mail that contains the above phrase.
- **Delete the Mail:** Select this option to automatically delete the mail with the above phrase.

In addition, it allows you to specify a list of words that you can either allow or block. This list is called the **whitelist**. The dialog box uses the following color codes to categorize emails:

- ✓ **User specified whitelist of words/phrases:** (Color Code: **GREEN**) Click this option to select the starting row of whitelisted words or phrases. A phrase that is added to the whitelist cannot be edited, enabled, or disabled.
- ✓ **User specified List of Blocked words/phrases:** (Color Code: **RED**) Click this option to select the starting row of the words or phrases that are defined in block list.
- ✓ **User specified words/phrases disabled:** (Color Code: **GRAY**) Click this option to select the starting row 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.

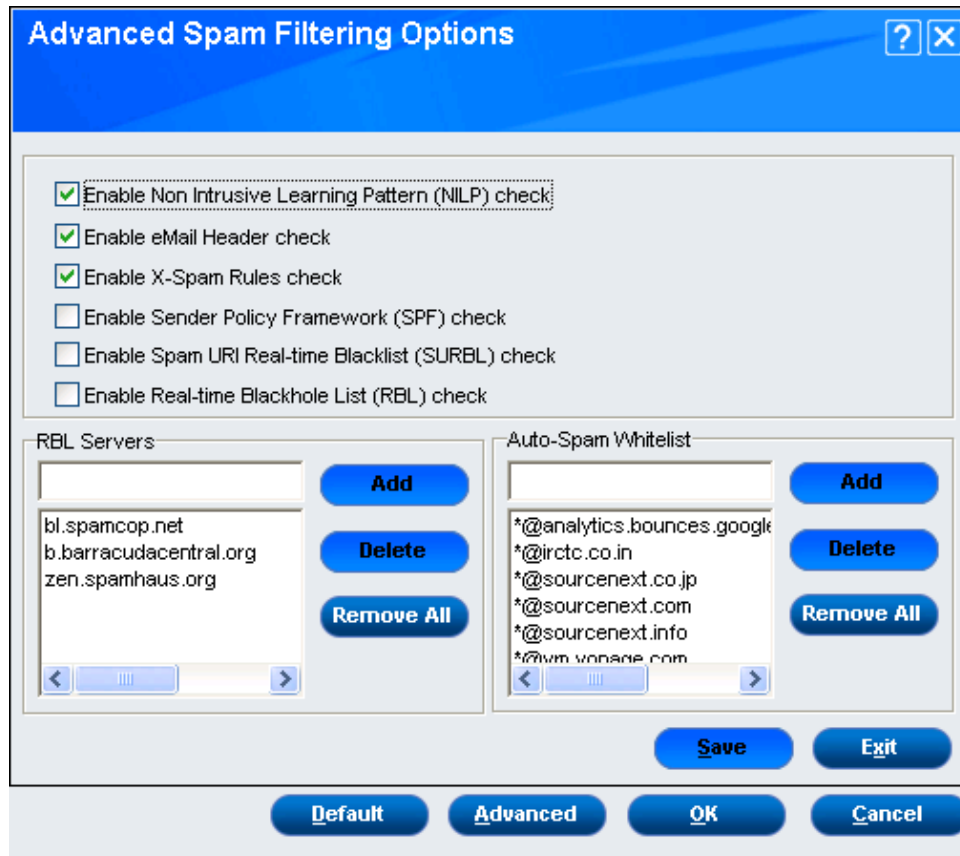


Default

Click this button to apply the default settings.

Advanced

This section provides you with options for configuring the general email options, spam filter configuration, and tagging emails in Anti-Spam. By click **Advanced** button the **Advanced Spam Filtering Options** dialog box opens. This dialog box helps you configure the following advanced options for controlling spam.



- Enable Non Intrusive Learning Pattern (NILP) check:** This option is selected by default. 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. Select this check box if you want to enable NILP check.
- Enable eMail Header check:** This option is selected by default. Select this check box if you want to check the validity of certain generic fields, such as From, To, and CC in an email and marks it as spam if any of the headers are invalid.
- Enable X-Spam Rules check:** This option is selected by 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 score or threshold. The X-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 that is adopted by eScan to prevent hackers from forging sender addresses. It acts a powerful mechanism for controlling phishing mails. Select this check box 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 URL Realtime Blacklist (SURBL) check:** Select this check box 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 Realtime Blackhole List (RBL) check:** Select this check box 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.
 - **Add:** You can add servers and sites that contain information of spammers.
 - **Delete:** You can delete a specific server or site from the list.
 - **Remove All:** You can remove all the servers and sites from list at once.
- **Auto-Spam Whitelist:** Unlike normal RBLs, SURBL scans emails for names or URLs of spam web sites 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.
 - **Add:** You can add valid email addresses that can bypass the above spam filtering.
 - **Delete:** You can delete the specific email address from the list.
 - **Remove All:** You can remove all the email addresses from list at once.
- **Save:** You can save the configuration by clicking on this button.
- **Exit:** You can exit the **Advanced Spam Filtering Options** without saving the configuration.

OK

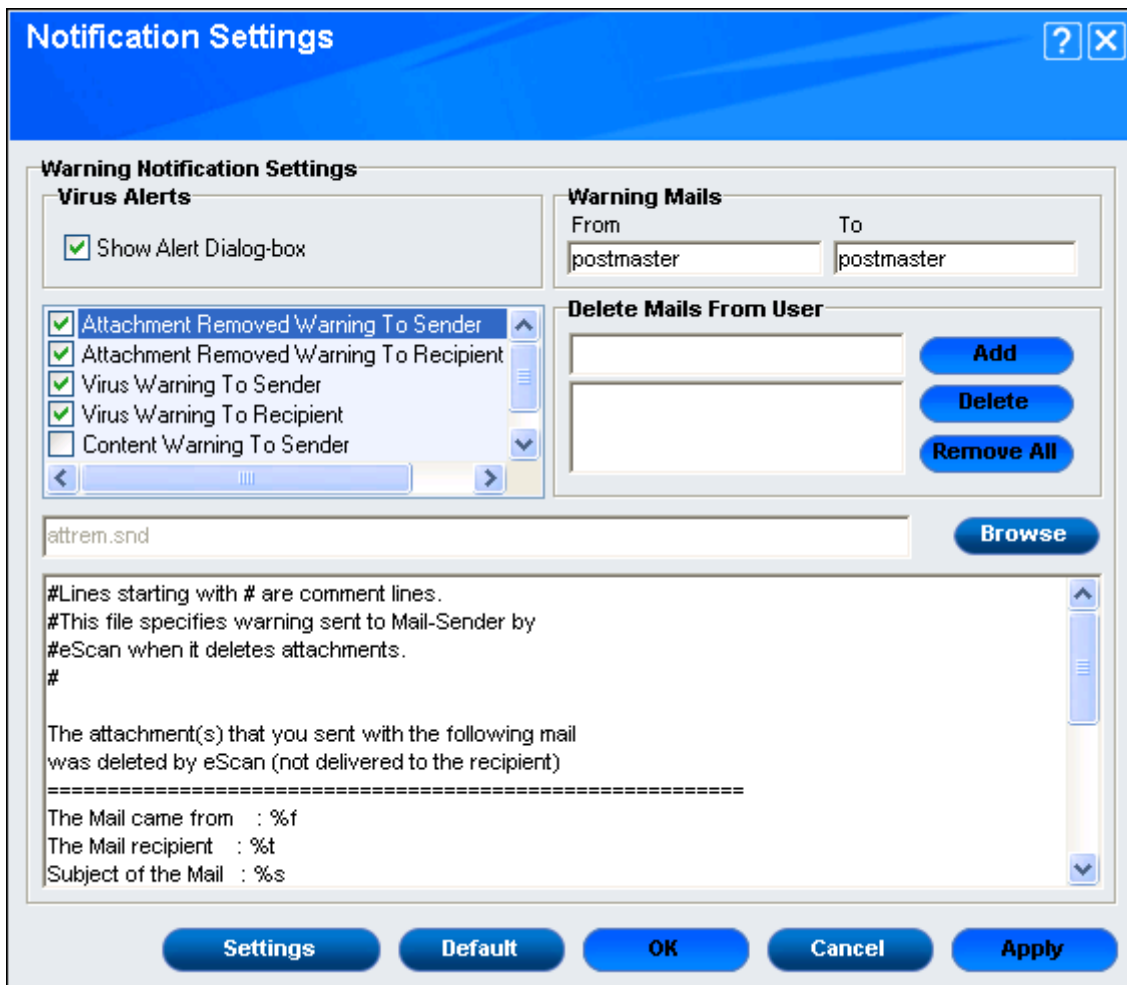
Click this button after you click the Apply button to apply the configured settings.

Cancel

Click this button to cancel the configured settings or to close the window.

Notification

This button opens the **Notification Settings** dialog box. You can configure the notification settings by using this dialog box. By configuring this module, you can send emails to specific recipients when a particular event occurs.



The following are the warning notification settings that you can configure:

Virus Alerts

This setting has **Show Alert Dialog-box** option that is selected by default. This option helps you to display an alert box notifying you of a virus infection. It has more options to configure the alerts which are as follows:

- **Attachment Removed Warning To Sender:** This option is selected by default and it sends a warning message to the sender of an infected attachment. It sends an email when a virus-infected attachment is encountered in an email. The content of the email that is sent is displayed in the preview box.
- **Attachment Removed Warning To Recipient:** This option is selected by default and it sends a warning message to the recipient when it removes an infected attachment. The content of the email that is sent is displayed in the preview box.
- **Virus Warning To Sender:** This option is selected by default and it sends a virus warning message to the sender. The content of the email that is sent is displayed in the preview box.
- **Virus Warning To Recipient:** This option is selected by default and it sends a virus warning message to the recipient. The content of the email that is sent is displayed in the preview box.

- **Content Warning To Sender:** This option is selected by default and it sends a content warning message to the sender. The content of the email that is sent is displayed in the preview box.
- **Content Warning To Recipient:** This option is selected by default and it sends a content warning message to the recipient. The content of the email that is sent is displayed in the preview box.

Warning Mails

This option is used to configure this setting to send warning emails and alerts from given sender to recipient. The default sender (**From** field) is postmaster and the default recipient (**To** field) is postmaster.

Delete emails From User

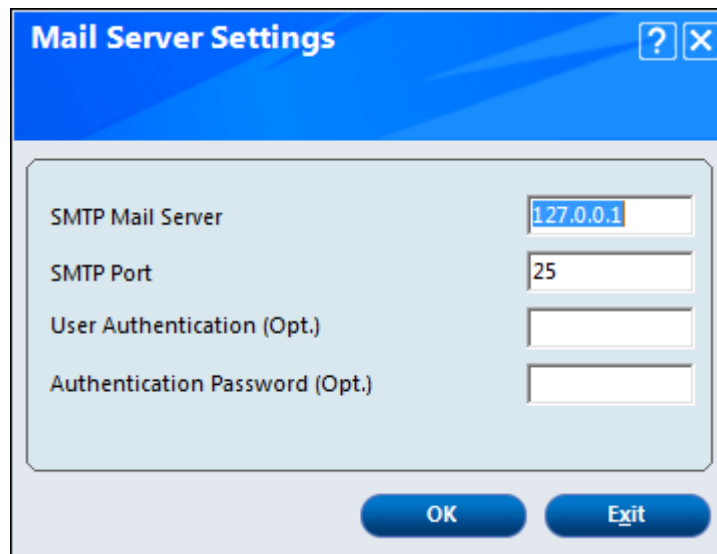
This option is used to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete emails From User** list. By default, the **Delete emails From User** section fields are unavailable, it is available only when you type in some text in the **Delete emails From User** field and add email addresses. It has three buttons:

- **Add:** You can add email addresses of the users so that it deletes the email from that users.
- **Delete:** You can delete the email addresses of the users that are already present in the list.
- **Remove All:** You can remove all the email addresses at once by clicking on this button.

Settings

Click on Settings to configure Mail Server settings. This has following configuration:

- **SMTP Mail Server:** Enter SMTP Mail Server details.
- **SMTP Port:** Enter the port number for SMTP.
- **User Authentication (Opt.):** This is optional field. You can enter the username for authentication, if set.
- **Authentication Password (Opt.):** This is optional field. You can enter the password for same username for authentication.



The image shows a dialog box titled "Mail Server Settings" with a blue header bar containing a question mark icon and a close button. The main area is light blue and contains four input fields: "SMTP Mail Server" with the value "127.0.0.1", "SMTP Port" with the value "25", "User Authentication (Opt.)", and "Authentication Password (Opt.)". At the bottom, there are two buttons: "OK" and "Exit".

This dialogue box has two buttons:

- **OK:** To save the configured setting.
- **Exit:** To exit the dialogue box without saving the configuration.

Default

Click this button to apply the default settings.

OK

Click this button after you click the Apply button to apply the configured settings.

Cancel

Click this button to cancel the configured settings or to close the window.

Apply

Click this button to apply the configured settings.

Reports

Total Quarantined Mails

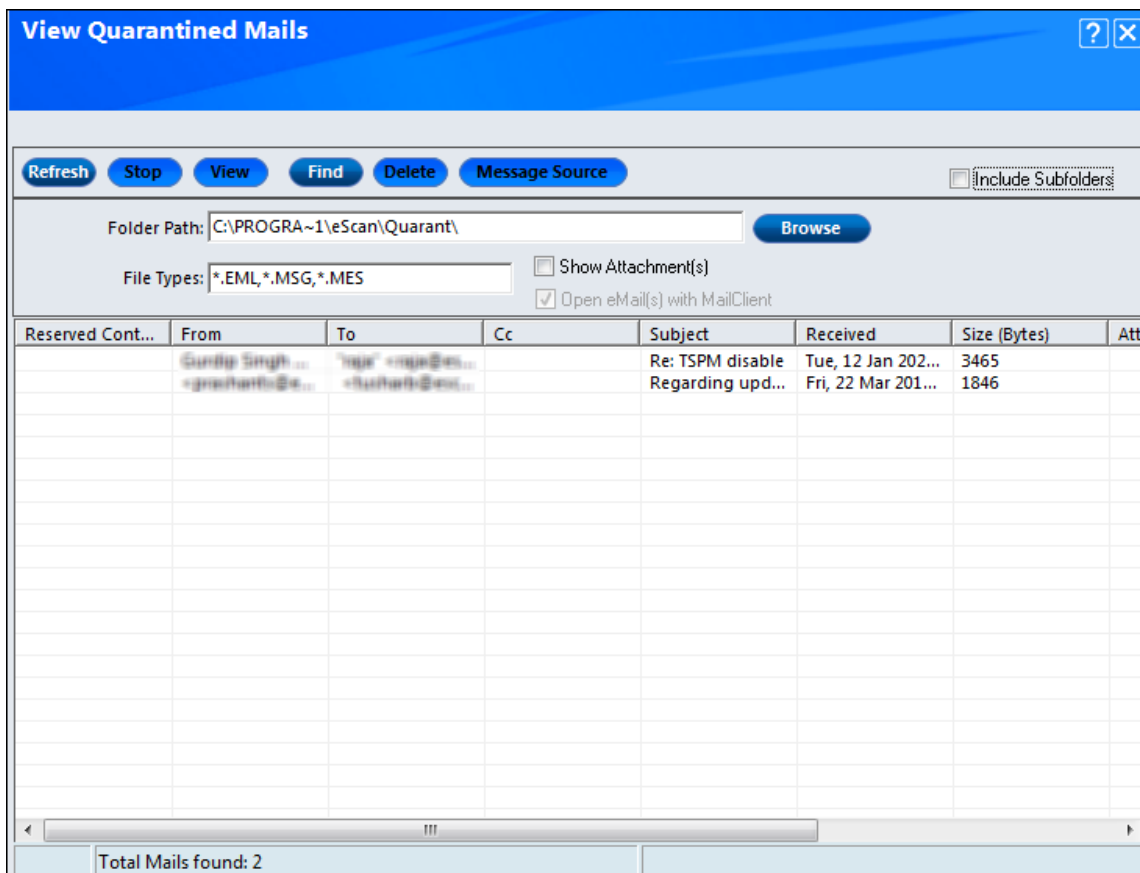
It shows the total number of quarantined mails monitored by Real-Time scanning.

Total Clear Mails

It shows the total number of clear mails on a Real-Time basis monitoring.

View Quarantined Mails

This button opens the **View Quarantined Mails** window, which displays the list of emails that have been quarantined.

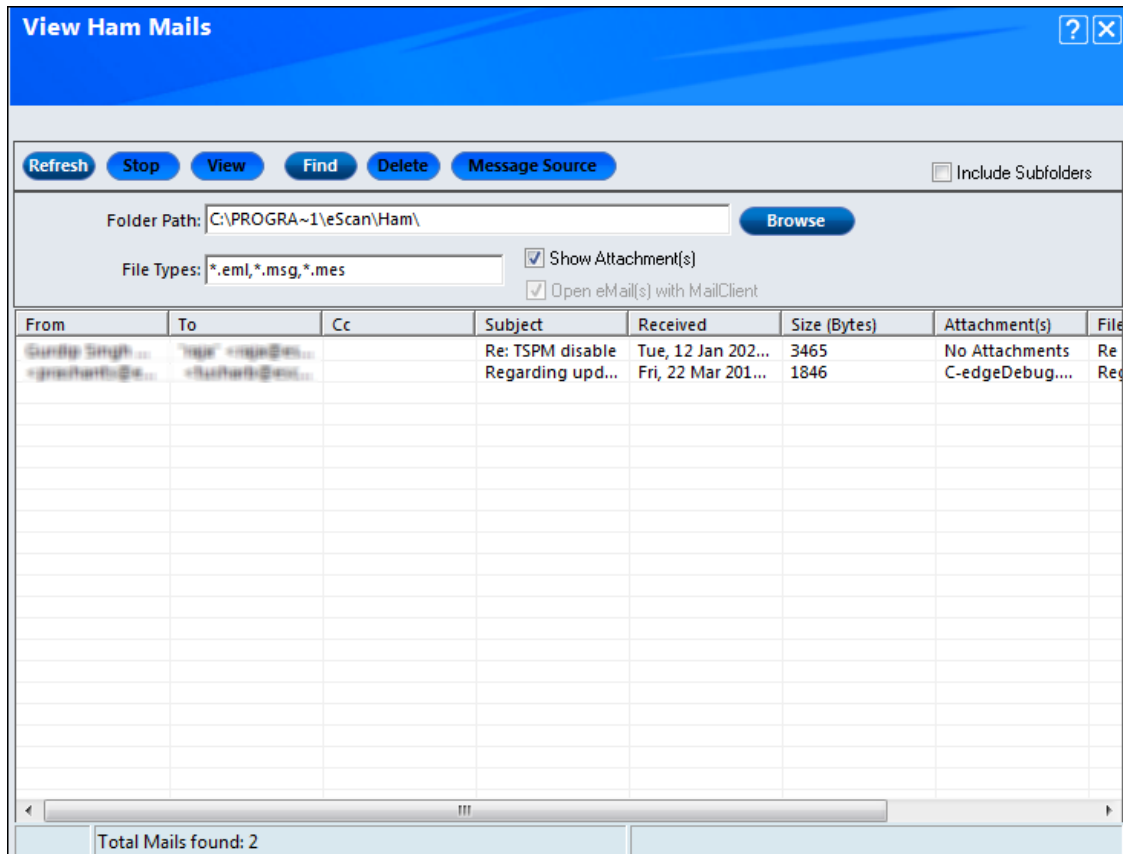


Following are the options to configure quarantined emails:

- **Refresh:** This button refreshes the whole list.
- **Stop:** Click on this button to stop from refreshing list.
- **View:** It displays the detail of email that has been quarantined.
- **Find:** To search the particular email from the list, click this button.
- **Delete:** Click this button to delete existing quarantined mail.
- **Message Source:** This button gives you the source of the email.
- **Include Subfolder:** If you want to include sub folder of a folder, select this check box.

View Ham Mails

This button opens the View Ham Mails window, which displays the ham emails identified by eScan and have been archived by Mail Anti-Virus. As in the case of quarantined mails, you can specify the path of the folder where you need to store the archived emails and can also specify the format for storing emails.

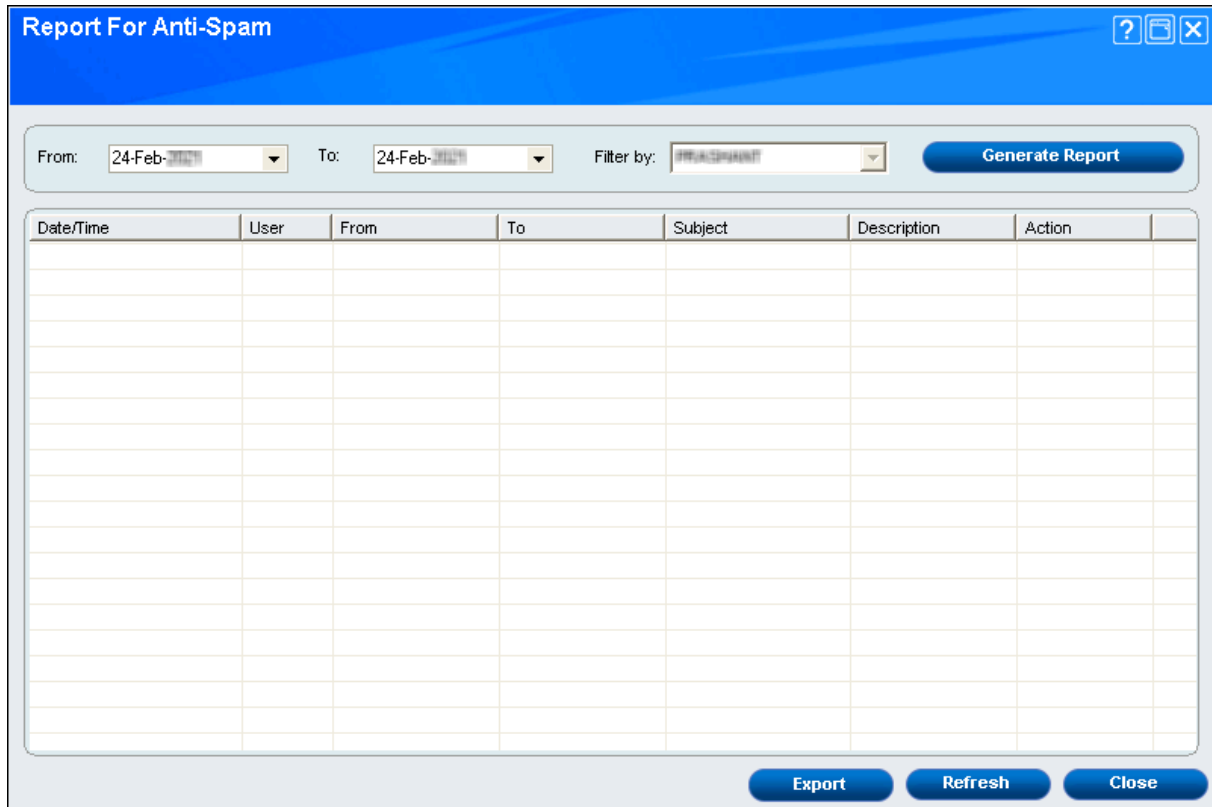


Following are the options to configure ham emails:

- **Refresh:** This button refreshes the whole list.
- **Stop:** Click on this button to stop from refreshing list.
- **View:** It displays the detail of email that has been detected as ham.
- **Find:** To search the particular email from the list, click this button.
- **Delete:** Click this button to delete existing ham mail.
- **Message Source:** This button gives you the source of the email.
- **Include Subfolder:** If you want to include sub folder of a folder, select this check box.

View Report

This section displays the Report For the Anti-Spam window and provides report for the Anti-Spam module between the given ranges of dates in a tabular format when you click the **Generate Report** button.



The screenshot shows a window titled "Report For Anti-Spam" with a blue header and standard window controls. Below the header is a form with "From:" and "To:" date pickers both set to "24-Feb-2021", a "Filter by:" dropdown menu, and a "Generate Report" button. Below the form is a table with the following columns: Date/Time, User, From, To, Subject, Description, and Action. The table is currently empty. At the bottom right of the window are three buttons: "Export", "Refresh", and "Close".

You can export the reports in the following format:

- PDF
- HTML
- CSV

Firewall

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

The screenshot shows the eScan AV for Windows Firewall interface. The window title is "eScan AV for Windows (22.0.1400.1000)". The interface includes a navigation bar with "File Anti-Virus", "Mail Anti-Virus", "Anti-Spam", "Firewall", and "Cloud Protection". The "Firewall" section is active, showing the following configuration:

Configuration	Value
Firewall Status	Stopped
Filtration System	Allow All

Below the configuration, there are links for "Allow All", "Limited Filter", "Interactive Filter", "Block All", and "Settings".

The "Reports" section shows:

Report	Count
Inbound Packets Blocked	0
Outbound Packets Blocked	0

A "Network Traffic in KB/sec" graph is also present, showing a flat line at 0 for both Incoming and Outgoing traffic.

At the bottom of the interface, there are links for "View Current Network Activity", "View Summary", and "View Report".

This Firewall module provides you with options required for configuring the module. You can configure the settings from the following sections.

Configuration

This section displays the following information and modes to allow, block, and configure this module:

- **Firewall Status:** This option shows whether the Firewall module is running or not. By default, Firewall runs in the **Allow All** mode.
- **Filtration System:** This option shows the filtration system is used by Firewall module.

Modes that are available are as follows:

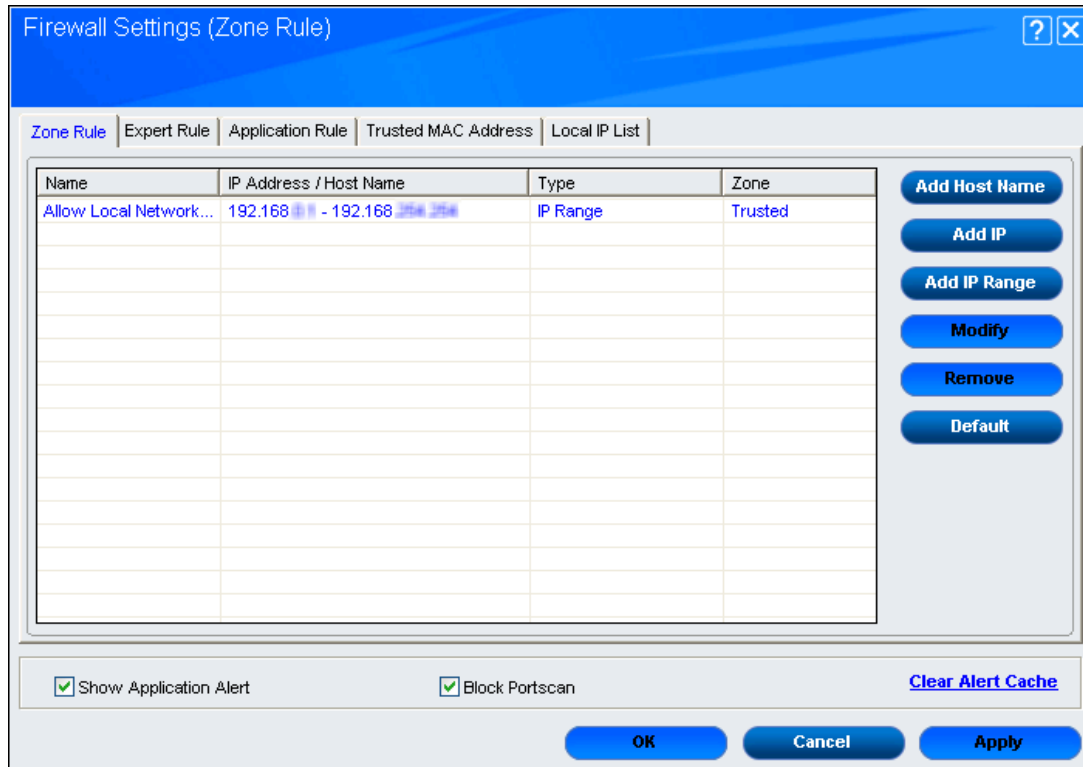
- **Allow All:** This option is turned on by default and you can disable Firewall if you want to.
- **Limited Filter:** This option enables the **Limited Filter** mode. When this mode is enabled, it monitors all incoming traffic and helps you allow or block traffic as per the defined conditions or rules.
- **Interactive Filter:** This option enables the **Interactive Filter** mode. When this mode is enabled, it needs user intervention. It monitors all the incoming and outgoing network traffic and allows or blocks traffic as per configured conditions and rules.
- **Block All:** This option blocks all the incoming and outgoing network traffic.
- **Settings:** To learn more, [click here](#).

Settings

You can configure the Firewall setting here. When you click this option, the **Firewall Settings (xxx)** window appears. The **xxx** indicates the name of a tab. By default, **Zone Rule** tab appears. On the **Firewall Settings (xxx)** window, you have five tabs **Zone Rule, Expert Rule, Application Rule, Trusted MAC Address, and Local IP List**. Let's discuss them in detail.

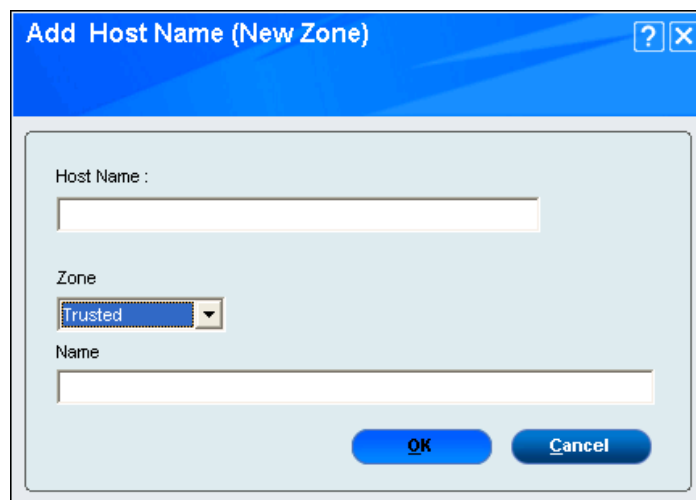
Zone Rule

This tab helps you configure network access rules that specify which IP address, host name, or IP range of computers can access your computer.



This tab includes the following buttons:

- Add Host Name:** This button is used to add a zone rule for a given host. To add the zone rule, you must provide name of the host for which you are adding the zone rule; the type of zone, whether it is **Trusted** or **Blocked** and specify a name for the zone rule. Clicking **OK** will add the host in zone rule and **Cancel** to exit the popup window.



- **Add IP:** This button is used to add a zone rule for a given IP address. To add the zone rule, you must provide the IP address for which you are adding the zone rule, the type of zone, whether it is **Trusted** or **Blocked** and specify a name for the zone rule. By selecting **IPv6 Address** check box you will enable IPv6 Protocol. Click **OK** to save configuration and **Cancel** to exit the popup window.

The screenshot shows a dialog box titled "Add IP (New Zone)". It has a blue header bar with a question mark icon and a close button (X). The main content area is light blue and contains the following fields:

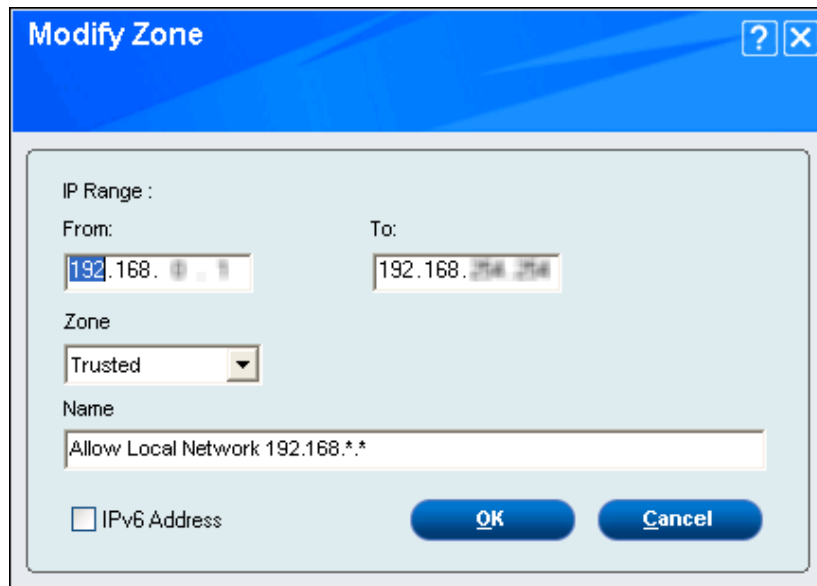
- IP Address:** A text input field with a dotted cursor.
- Zone:** A dropdown menu currently showing "Trusted".
- Name:** A text input field.
- IPv6 Address:** A checkbox that is currently unchecked.
- Buttons:** Two buttons at the bottom right, "OK" and "Cancel", both with blue backgrounds and white text.

- **Add IP Range:** This button is used to add a zone rule for a range of IP addresses. To add the zone rule, you must provide the range of IP address for which you are adding the zone rule, start IP address in the range, end IP address in the range. The type of zone, whether it is **Trusted** or **Blocked** and specify a name for the zone rule. By selecting **IPv6 Address** check box you will enable IPv6 Protocol. This has 2 buttons, namely, **OK** to save changes and **Cancel** to exit the popup window.

The screenshot shows a dialog box titled "Add IP Range (New Zone)". It has a blue header bar with a question mark icon and a close button (X). The main content area is light blue and contains the following fields:

- IP Range :** A label above two text input fields: "From:" and "To:", both with dotted cursors.
- Zone:** A dropdown menu currently showing "Trusted".
- Name:** A text input field.
- IPv6 Address:** A checkbox that is currently unchecked.
- Buttons:** Two buttons at the bottom right, "OK" and "Cancel", both with blue backgrounds and white text.

- **Modify:** This button is used to modify zone rules related to the host name, IP address, or range of IP addresses which is already added in the list. By selecting **IPv6 Address** check box you will enable Internet Protocol. Click **OK** to save modifications and **Cancel** to exit the popup window.



The screenshot shows a 'Modify Zone' dialog box with the following fields and controls:

- IP Range :**
 - From:** 192.168.0.1
 - To:** 192.168.254.254
- Zone:** Trusted (dropdown menu)
- Name:** Allow Local Network 192.168.*.*
- IPv6 Address
- OK** button
- Cancel** button

- **Remove:** This button is used to remove the record from list.
- **Default:** This button is used to load default settings.

Expert Rule

This tab allows you to specify advanced rules and settings for the 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, you should configure these rules only if you have a good understanding of firewalls and networking protocols.

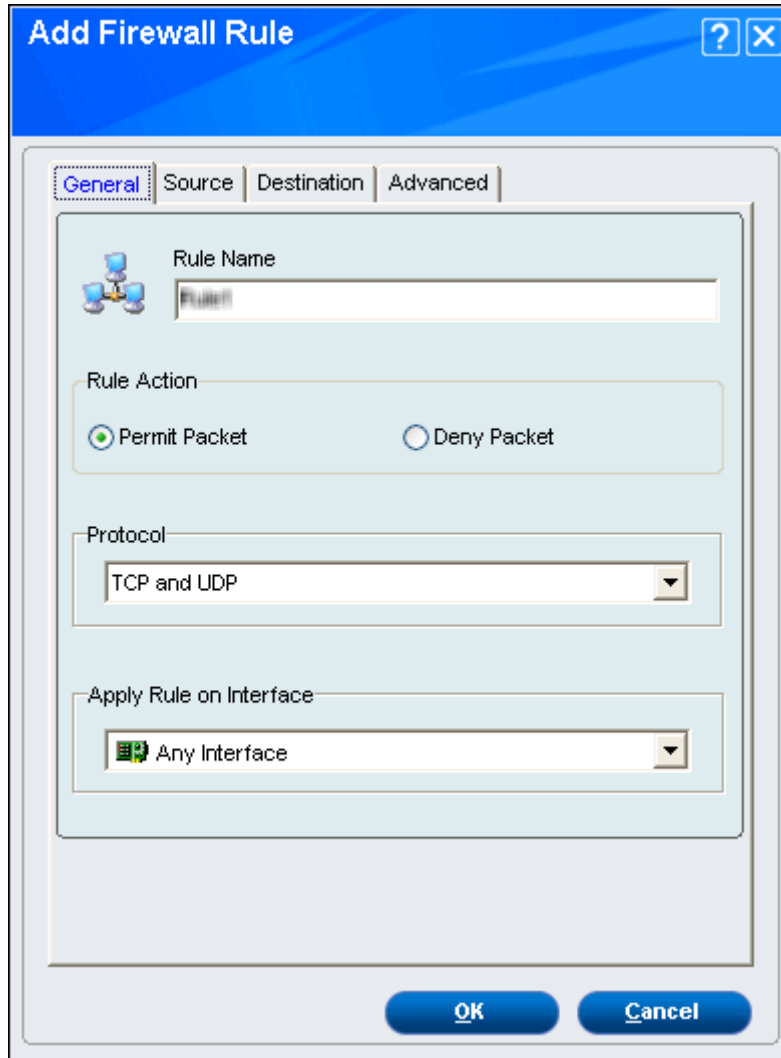
Firewall Rule	Rule Action Summary
✓ UDP Rule	Permits UDP packets on Any Interface between "My Network:Any"
✓ ARP packet exchange - For mappi...	Permits ARP packets on Any Interface
✓ NetBios (LAN File Sharing) - Acce...	Permits TCP and UDP packets on Any Interface between "My Com.
✗ NetBios (LAN File Sharing) - Acce...	Blocks TCP and UDP packets on Any Interface between "Any Add
✓ ICMP messages	Permits ICMP packets on Any Interface between "My Network" an.
✓ ICMPV6 messages	Permits ICMPV6 packets on Any Interface
✓ ICMP messages for 192.168.*.* (pi...	Permits ICMP packets on Any Interface between "My Network" an.
✓ DHCP/BOOTP packet exchange	Permits UDP packets on Any Interface between "Any Address:68"
○ FTP Control - For downloading and...	Permits TCP packets on Any Interface between "My Network:Any"
○ FTP Data - For downloading and u...	Permits TCP packets on Any Interface between "Any Address:20"
✗ RPC Service	Blocks TCP and UDP packets on Any Interface between "Any Add
✓ DNS name resolution - For accessi...	Permits UDP packets on Any Interface between "My Network:Any"
✓ E-Mail (SMTP, POP3, IMAP) - For se...	Permits TCP packets on Any Interface between "My Network:Any"
✓ WWW (HTTP & HTTPS) - For acce...	Permits TCP packets on Any Interface between "My Network:Any"
✓ News (NNTP)	Permits TCP packets on Any Interface between "My Network:Any"

This tab has various button and settings:

- **Add:** This button adds new rules.
- **Modify:** This button modifies the already existing rules in the list.
- **Remove:** This button removes the existing rules from the list.
- **Default:** This button resets the all the configuration settings.
- **Green arrow buttons:** This buttons can be used to prioritize the expert rule based on the specific need of the user.

Adding new rule

This section will describe how to add new rule. Click on **Add** button, Add Firewall Rule window appears.



General

This tab enables you to define rules and its actions. Specify the following field details:

- **Rule Name:** Type the name for rule.
- **Rule Action:** Click any one of the following types of actions for setting rules.
 - **Permit Packet:** This option is selected by default and it allows you to permit packets.
 - **Deny Packet:** This option allows you to deny packets.
- **Protocol:** This option lets you to select an appropriate type of protocol from the drop-down list. By default, **TCP and UDP** is selected.
- **Apply Rule On Interface:** This option lets you to select Interface to apply the rule. By default, **Any Interface** is selected.

Source

This tab enables you to type the source IP address and port wherever applicable. You can select the appropriate option. By default, **My Network** under **Source IP Address** section and **Any** under **Source Port** section are selected.

The screenshot shows the 'Add Firewall Rule' dialog box with the 'Source' tab selected. The dialog has a blue header with a question mark and close button. Below the header are four tabs: 'General', 'Source', 'Destination', and 'Advanced'. The 'Source' tab is active and contains two sections: 'Source IP Address' and 'Source Port'. In the 'Source IP Address' section, the 'My Network' radio button is selected. In the 'Source Port' section, the 'Any' radio button is selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Add Firewall Rule [?] [X]

General | **Source** | Destination | Advanced

Source IP Address

- My Computer
- Host Name
- Single IP Address
- Whole IP Range
- Any IP Address
- My Network

Source Port

- Any
- Single Port
- Port Range
- Port List

OK Cancel

Destination

This tab enables you to type the destination IP address and port wherever applicable. You can select the appropriate option. By default, **My Network** under **Destination IP Address** section and **Any** under **Destination Port** section are selected.

The screenshot shows the 'Add Firewall Rule' dialog box with the 'Destination' tab selected. The dialog has a blue header with a question mark and close button. Below the header are four tabs: 'General', 'Source', 'Destination', and 'Advanced'. The 'Destination' tab is active and contains two sections: 'Destination IP Address' and 'Destination Port'. In the 'Destination IP Address' section, the 'My Network' radio button is selected. In the 'Destination Port' section, the 'Any' radio button is selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Add Firewall Rule [?] [X]

General | Source | **Destination** | Advanced

Destination IP Address

- My Computer
- Host Name
- Single IP Address
- Whole IP Range
- Any IP Address
- My Network

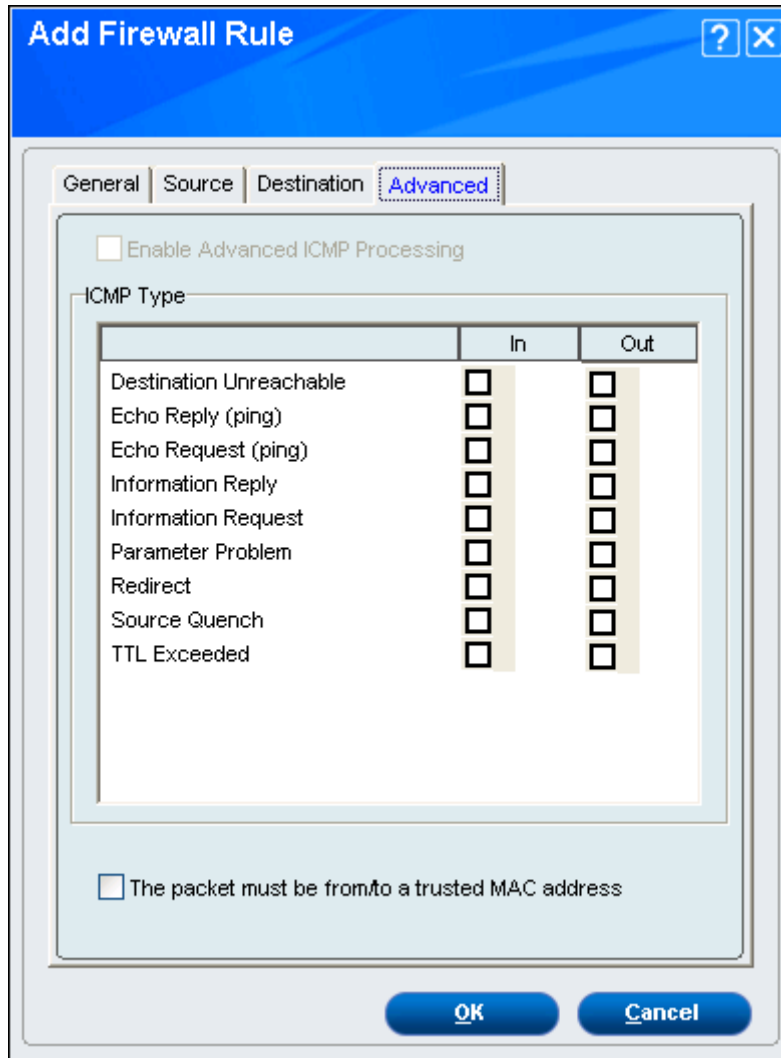
Destination Port

- Any
- Single Port
- Port Range
- Port List

OK Cancel

Advanced

This tab is specifically meant for ICMP processing. ICMP processing is only applicable when ICMP protocol is selected in General section. Select the check box of **Enable Advanced ICMP Processing** to enable ICMP Type options.

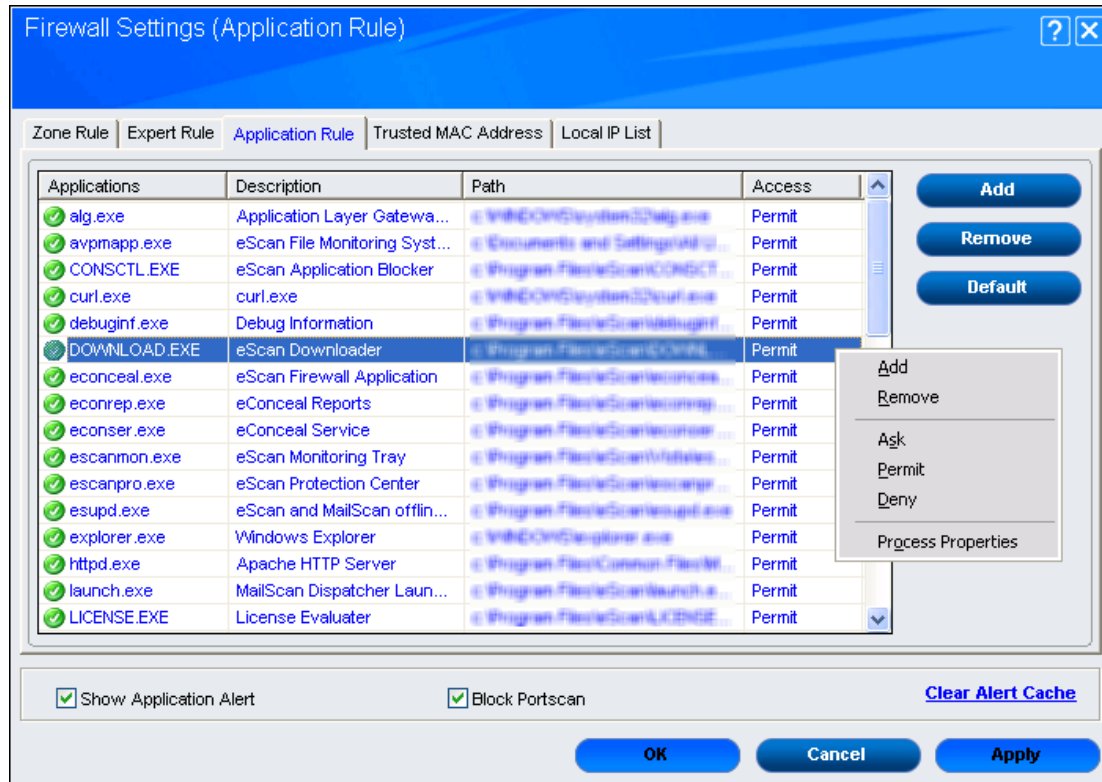


ICMP Type	In	Out
Destination Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Echo Reply (ping)	<input type="checkbox"/>	<input type="checkbox"/>
Echo Request (ping)	<input type="checkbox"/>	<input type="checkbox"/>
Information Reply	<input type="checkbox"/>	<input type="checkbox"/>
Information Request	<input type="checkbox"/>	<input type="checkbox"/>
Parameter Problem	<input type="checkbox"/>	<input type="checkbox"/>
Redirect	<input type="checkbox"/>	<input type="checkbox"/>
Source Quench	<input type="checkbox"/>	<input type="checkbox"/>
TTL Exceeded	<input type="checkbox"/>	<input type="checkbox"/>

After configuring all the tab according to your need, click on **OK** to add the new rule. It will be added in the list. Click **Cancel** to close the window.

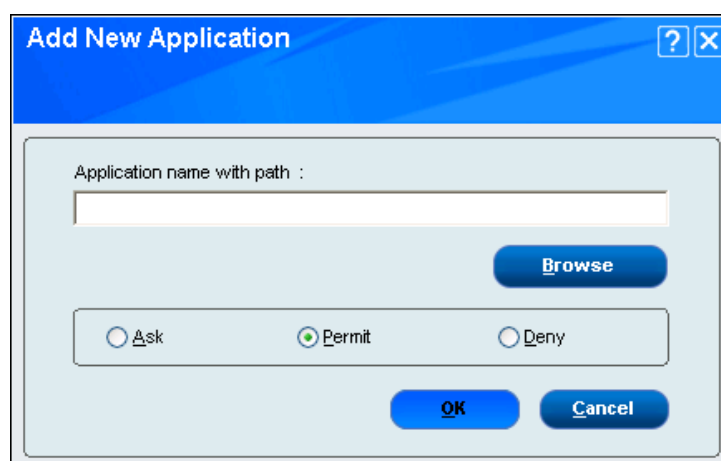
Application Rule

An Application Rule is based on programs or applications that are allowed to or denied access to the internet or any network-based service. The **Application Rule** tab provides you with a default list of rules by eScan and options for configuring application rules.

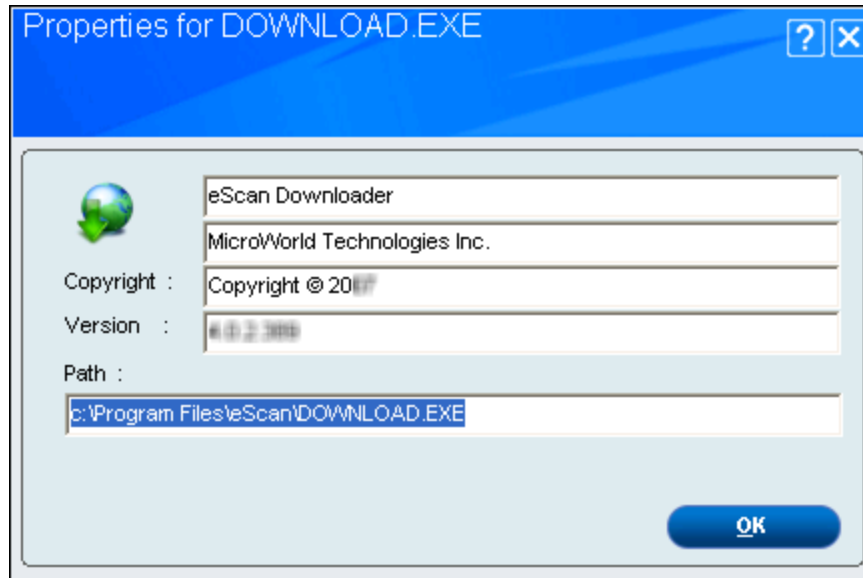


The context menu shows the following additional options when you right-click any rule in the table:

- **Add:** Use this option to add new application to the Application Rule list. Click **Browse** button to select name of the application that you want to add.

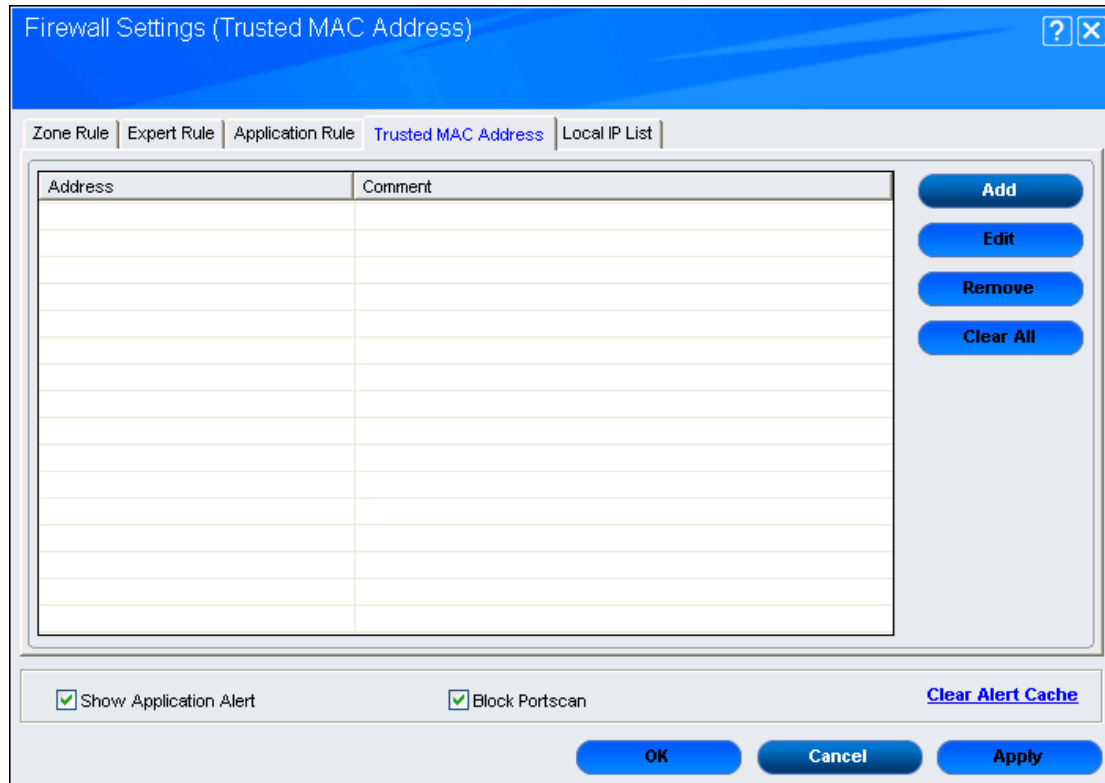


- **Remove:** This option is used to remove existing application from the Application Rule list.
- **Ask:** This option is used to ask for your permission to permit or deny network access.
- **Permit:** This option is used to permit any added Application for network access.
- **Deny:** This option is used to deny network access to any application present in the Application Rule list.
- **Default:** This option is used to reset the configuration to the default.
- **Process Properties:** This option displays the properties of the selected process or file, which include the name of the file, owner of the file, copyright information, version, and path of the file.



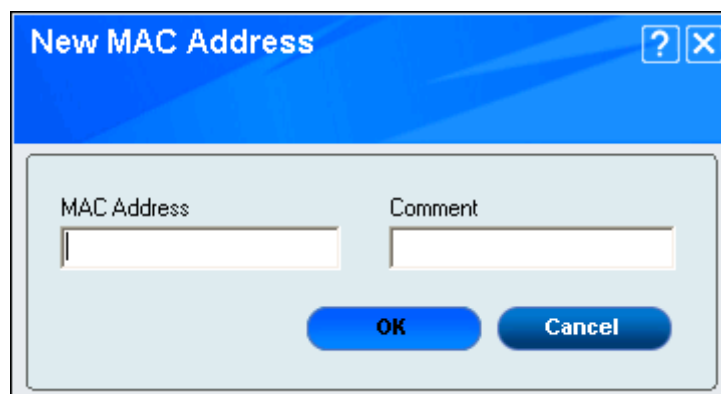
Trusted MAC Address

This section contains a list of Trusted Mac Addresses. A Mac address is a hardware address that uniquely identifies each node of a network.



This tab has 4 buttons which are as follows:

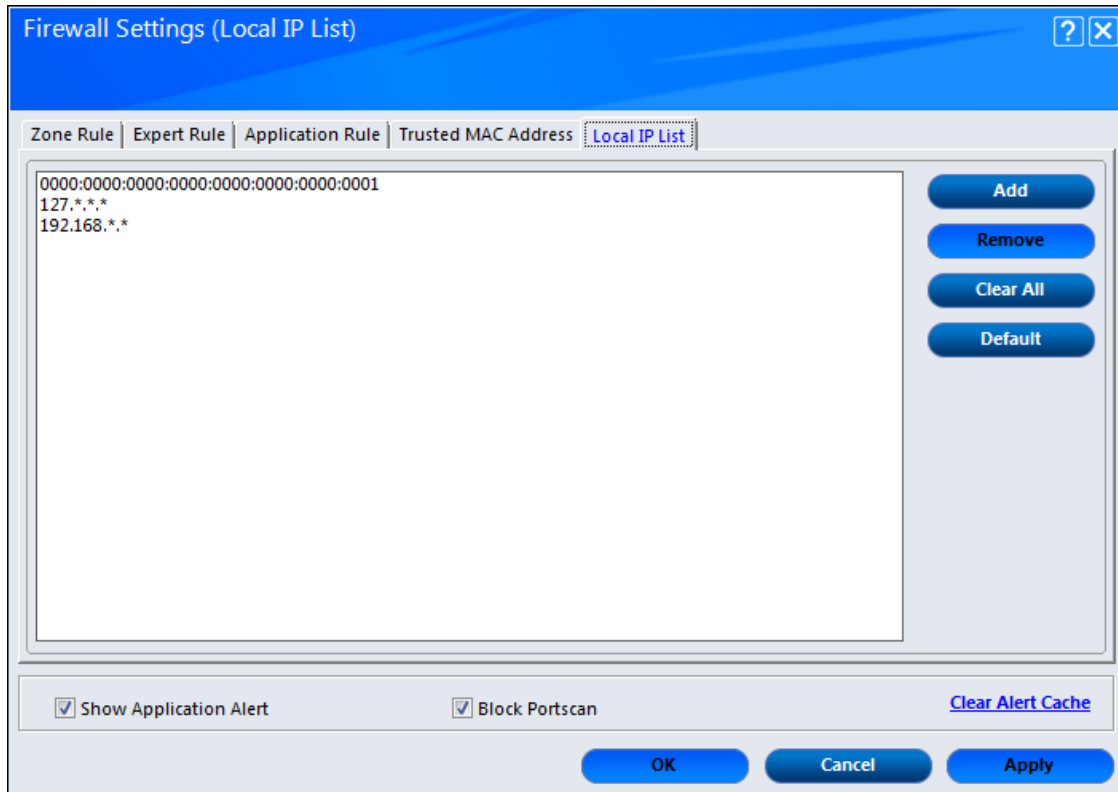
- **Add:** You can add new Mac address using this button. Once this button is clicked, you will see a **New MAC Address** dialogue box. Enter the **MAC Address** and **Comment** in this dialogue box and click **OK**.



- **Edit:** This button edits the existing entries in the list.
- **Remove:** This button removes the individual existing Mac entries from the list.
- **Clear All:** This button clears all the Mac addresses in the list.

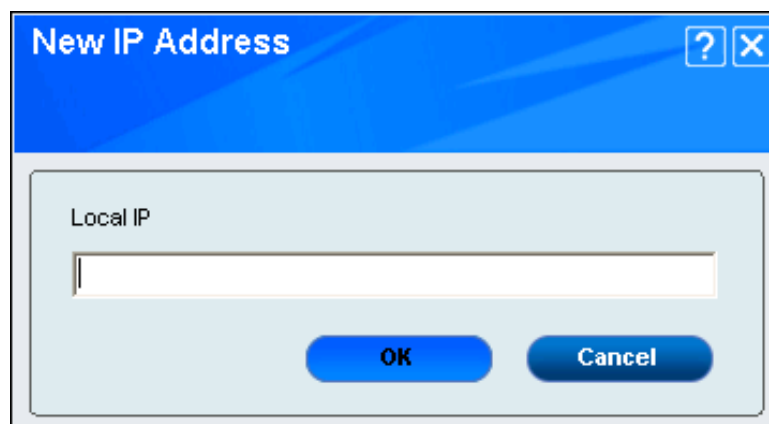
Local IP List

The local IP addresses are the devices that are connected to the same network within your organization. This tab displays the list of all local IP addresses and wildcard mask.



This tab has 4 buttons which are as follows:

- **Add:** You can add new IP address, Wildcard mask using this button. Once this button is clicked, you will see a **New IP Address** dialogue box. Enter the **IP Address and Wildcard mask** in this dialogue box and click **OK**.



- **Remove:** This button removes the existing individual IP entries from the list.
- **Clear All:** This button clears all the IP addresses in the list.
- **Default:** Click this button, to load default local IP list.

Show Application Alert

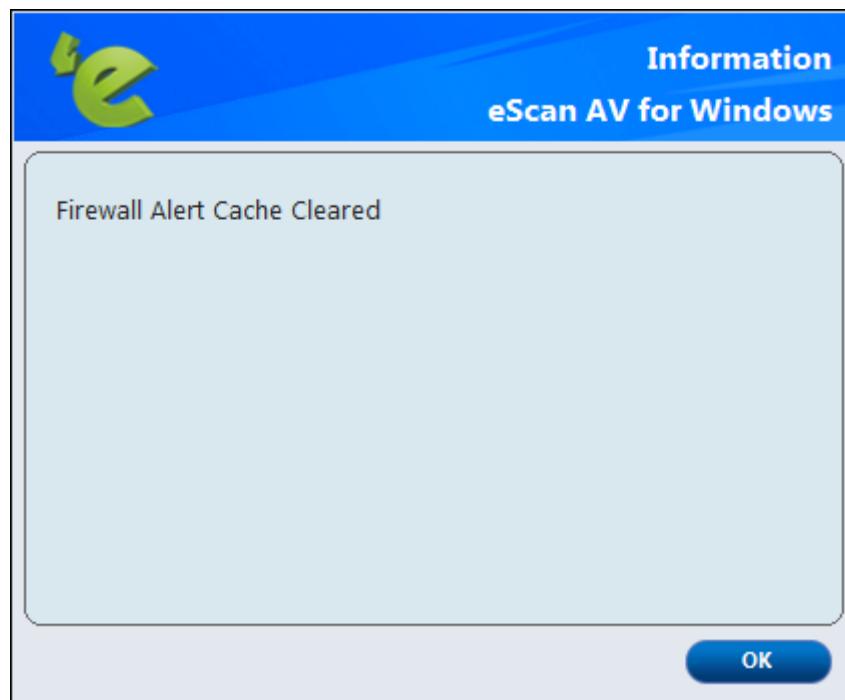
This check box is selected by default and provides you firewall alert when an application is blocked as per an application rule.

Block Portscan

This check box is selected by default and blocks all Portscan attempts made by Hackers.

Clear Alert Cache

You can click this button to clear all the information, such as previous actions taken or blocked programs stored in the firewall's cache.



Reports

This settings gives you following details:

Inbound Packets Allowed

It shows the total number of inbound packets that are allowed by the firewall.

Outbound Packets Allowed

It shows the total number of outbound packets allowed by the firewall.

Inbound Packets Blocked

It shows the total number of inbound packets that were blocked by the firewall.

Outbound Packets Blocked

It shows the total number of outbound packets that were blocked by the firewall.

This setting also has following links available:

View Current Network Activity

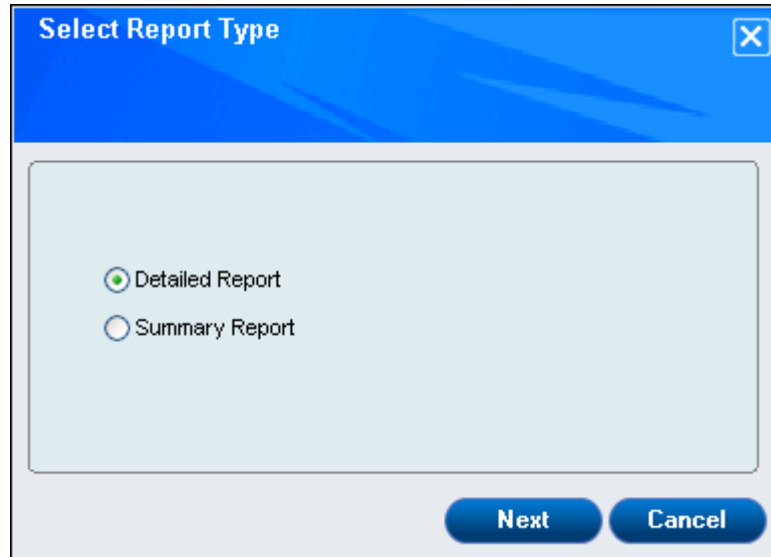
You can click this button to open the View TCP tool, which displays real-time activity report of the all active connections and established connections. It also provides you with information regarding the process, protocol, local address, remote address, and status of each network connection.

Process	Protocol	Local Address	Remote Address	Status
svchost.exe:1184	TCP	escan-comp:135 (epmap)	escan-comp:0	Listening
System:4	TCP	escan-comp:445 (microsoft-ds)	escan-comp:0	Listening
MWAGENT.EXE:612	TCP	escan-comp:2222	escan-comp:0	Listening
svchost.exe:1104	TCP	escan-comp:3389	escan-comp:0	Listening
alg.exe:732	TCP	127.0.0.1:1127	escan-comp:0	Listening
MWAGENT.EXE:612	TCP	127.0.0.1:2226	escan-comp:0	Listening
MWAGENT.EXE:612	TCP	127.0.0.1:2226	escan-comp:0	Listening
escanmon.exe:1600	TCP	127.0.0.1:2226	escan-comp:0	Listening
System:4	TCP	192.168.0.222:135 (epmap)	escan-comp:0	Listening
escanmon.exe:1600	TCP	192.168.0.222:1434	192.168.0.10:3127	Close_Wait
svchost.exe:1104	TCP	192.168.0.222:3389	192.168.0.245:45401	Established
System:4	UDP	escan-comp:445 (microsoft-ds)	xxxxxx	-
Isass.exe:936	UDP	escan-comp:500 (isakmp)	xxxxxx	-
svchost.exe:1444	UDP	escan-comp:1025	xxxxxx	-
sqlbrowser.exe:784	UDP	escan-comp:1434 (ms-sql-m)	xxxxxx	-
svchost.exe:1444	UDP	escan-comp:3434	xxxxxx	-
Isass.exe:936	UDP	escan-comp:4500	xxxxxx	-
svchost.exe:1444	UDP	escan-comp:5365	xxxxxx	-
svchost.exe:1296	UDP	127.0.0.1:1127 (alg)	xxxxxx	-
svchost.exe:1568	UDP	127.0.0.1:1900	xxxxxx	-
MWAGENT.EXE:612	UDP	127.0.0.1:2226	xxxxxx	-
svchost.exe:1296	UDP	192.168.0.222:127 (alg)	xxxxxx	-
System:4	UDP	192.168.0.222:135 (epmap)	xxxxxx	-
System:4	UDP	192.168.0.222:136 (epmap-dga)	xxxxxx	-
svchost.exe:1568	UDP	192.168.0.222:1900	xxxxxx	-

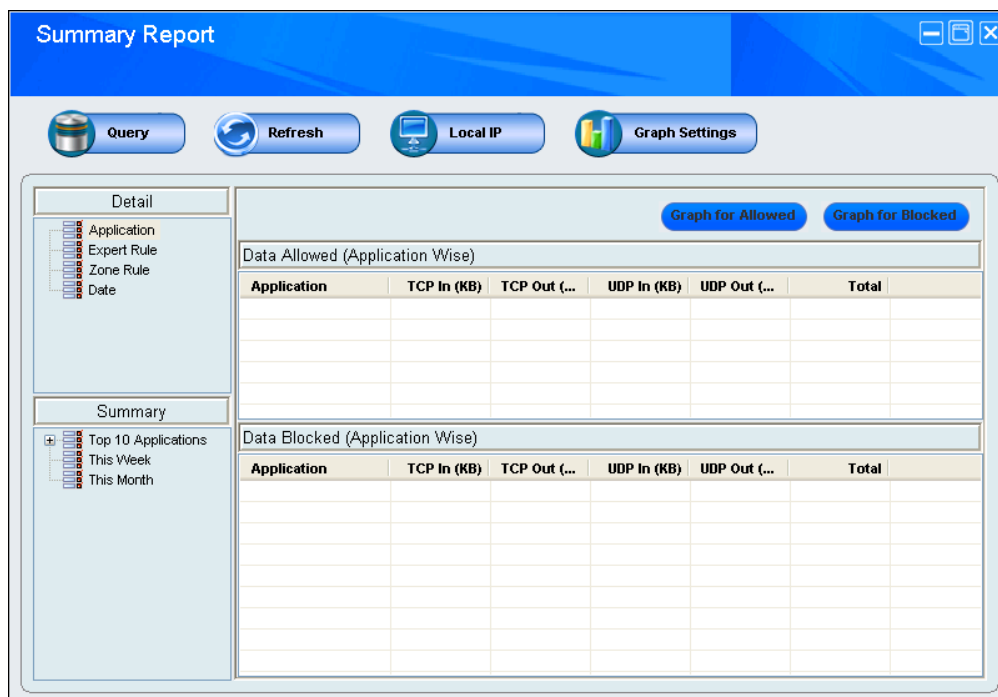
- **Active Connections:** It shows all active connections in the system.
- **Established Connections:** It shows all established connections in the system.

View Summary

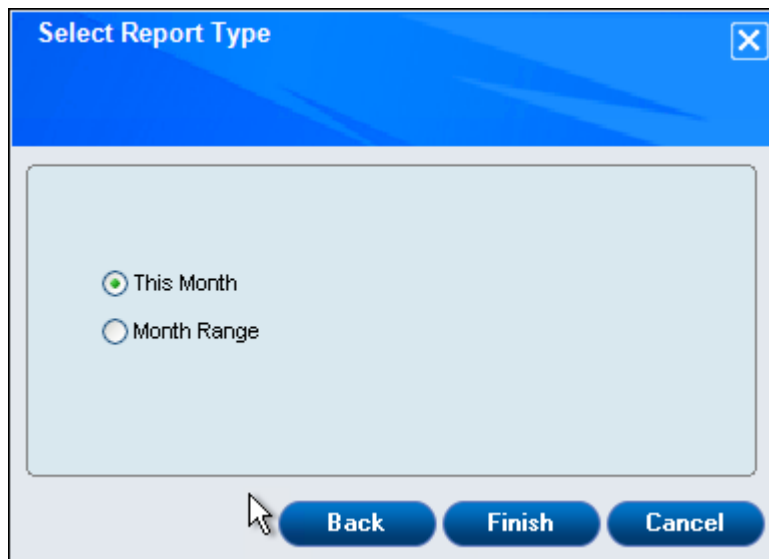
This button helps to view the Firewall reports, here you can choose report either in the form of Detailed or a Summary.



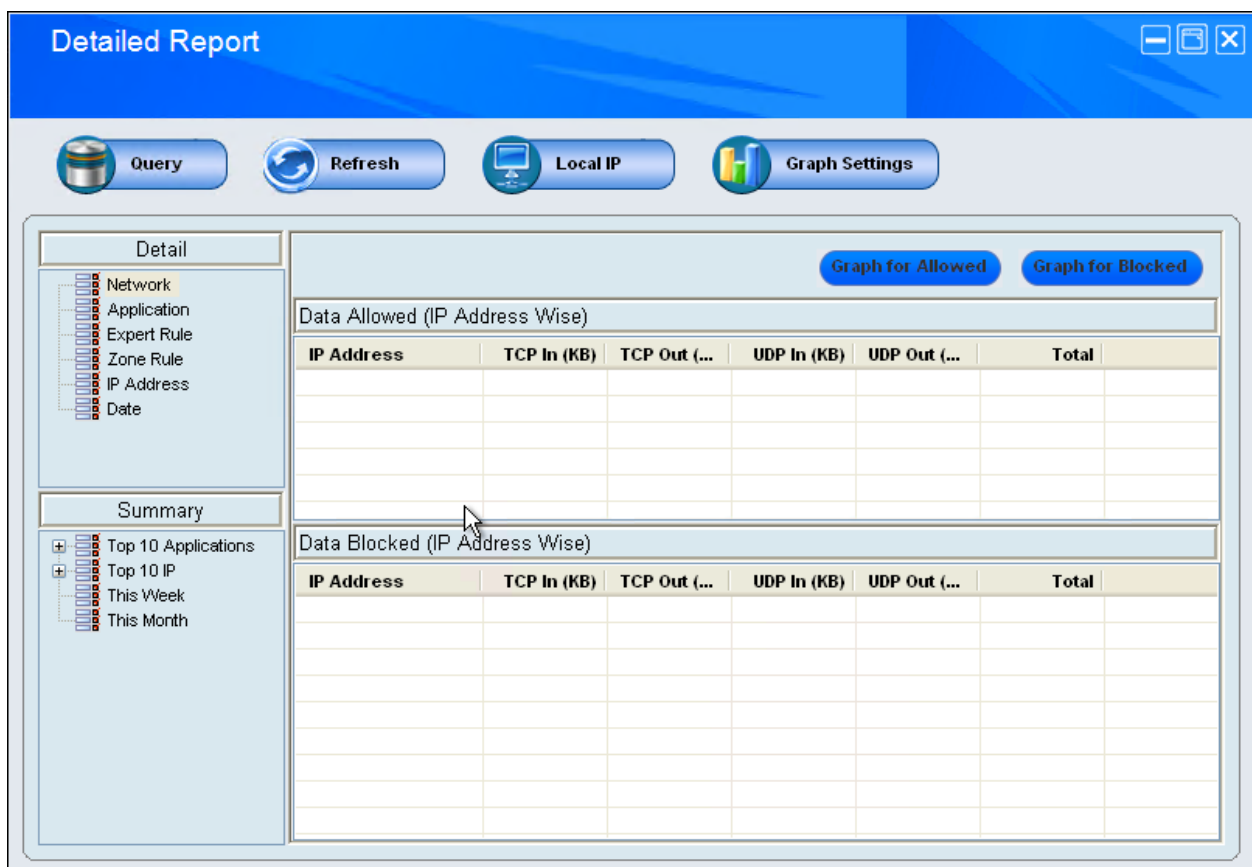
After selecting **Summary Report**, you will get the summary report of the blocked applications.



If you select **Detailed Report** in the **Select Report Type**, you will get option to select the month range or current month.

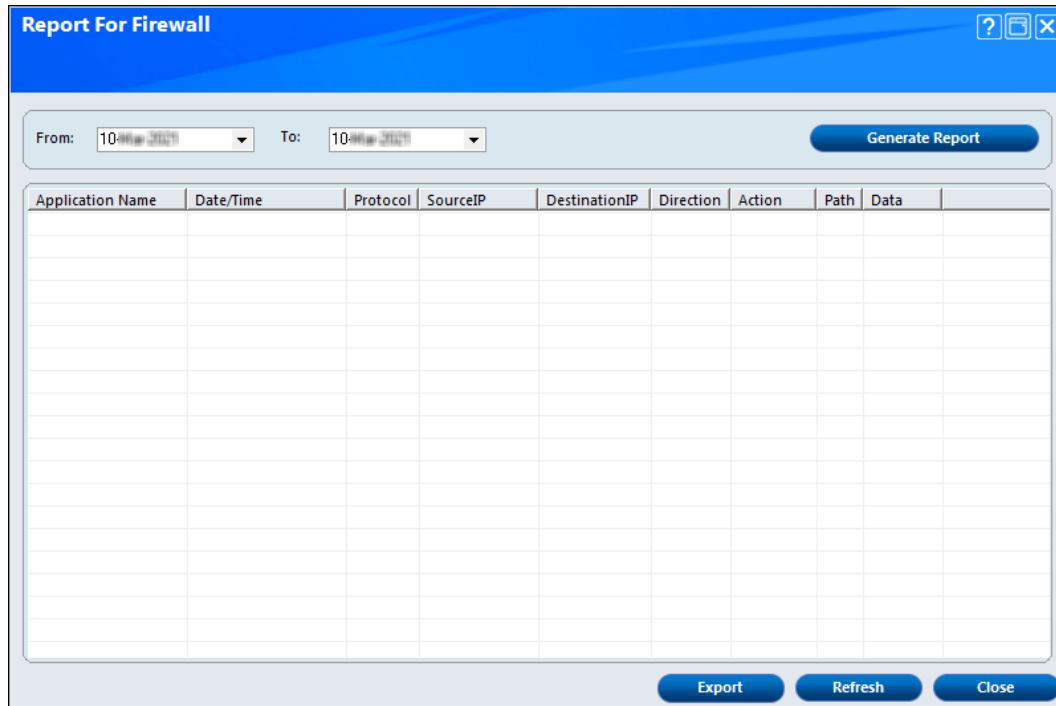


You will get the detailed report of the same.



View Report

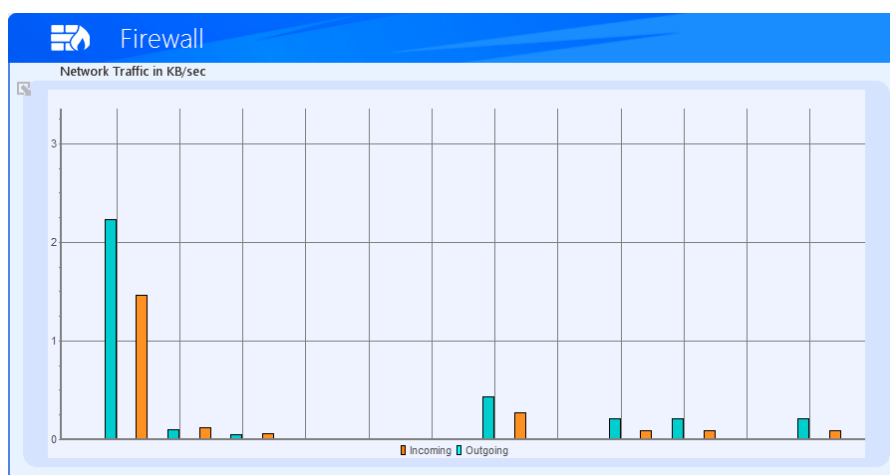
You can click this button to open the Report For Firewall window. This window displays the report for the Firewall module for a given range of dates in a tabular format when you click the **Generate Report** button.



You can export reports in the following format:

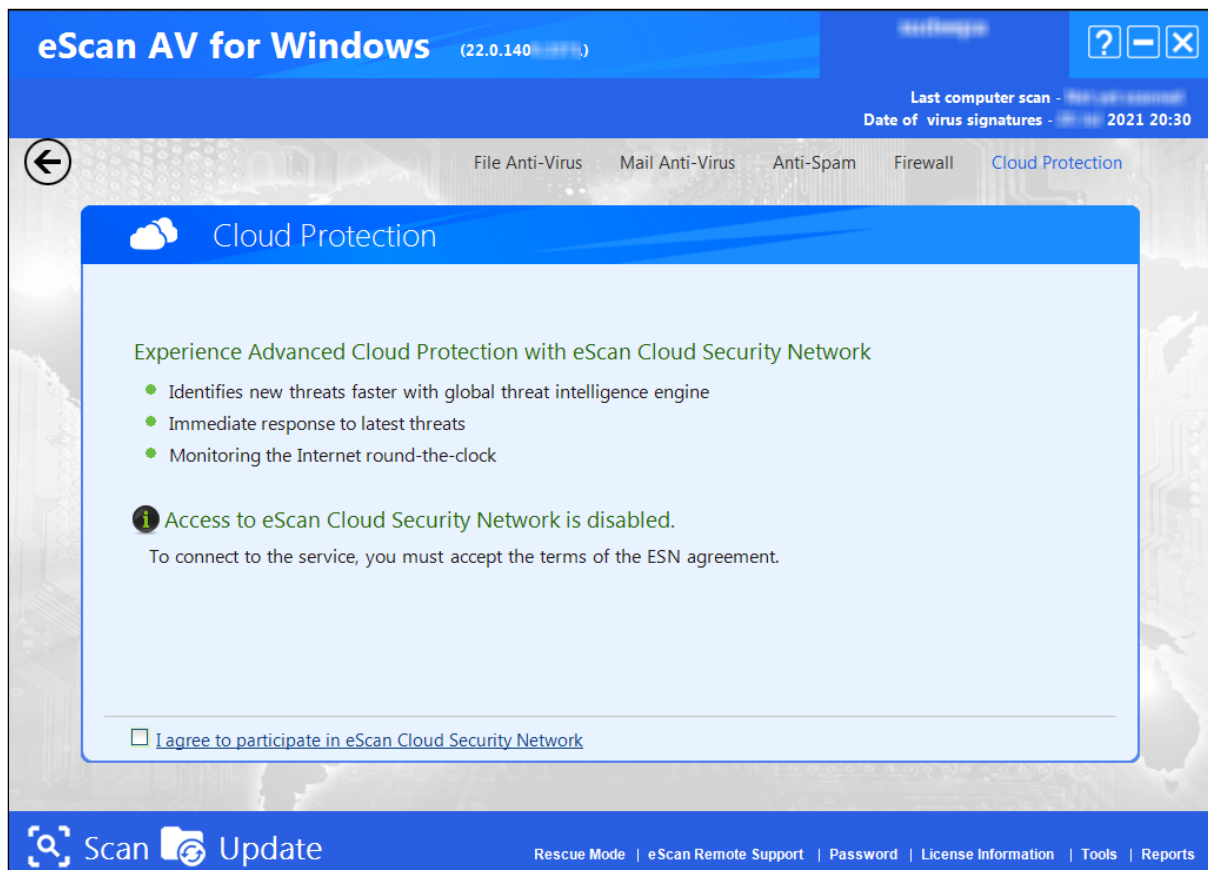
- PDF
- HTML
- CSV

The report section also contains a Network Traffic graph, which shows the incoming and outgoing network traffic in Kilobytes per second (KBps).



Cloud Protection

The eScan Anti-Virus for Windows introduces cloud-based security through eScan Security Network (ESN) technology. The cloud-based eScan Security Network ensures protection against current threats, such as viruses, worms, and Trojans. It identifies and blocks new threats before they become widespread. When it comes to new malware, it makes a prompt response with an advanced level of detection that provides superior protection, monitors internet round the clock.



The following are the basics of cloud-based ESN:


- Continuous global monitoring of real-life threats and immediate delivery of collected data to eScan host servers.
- Analysis of collected data and the creation of protection measures against new threats, and the fast distribution of those measures to users.
- ESN automatically collects information and sends the data to eScan labs. Information about suspicious files downloaded and executed on computers is also collected, regardless of their source, such as websites, email attachments, peer-to-peer networks, and so on.

This is done strictly voluntarily and confidentially – the user of any one of eScan SOHO products has to agree to participate in the system. In any case, strict confidentiality is maintained and no personal information, such as user names, passwords, or any other personal details are collected.

The decision on the safety of a program is made based on internal algorithms like the file is having a valid digital signature or not and number of other factors.

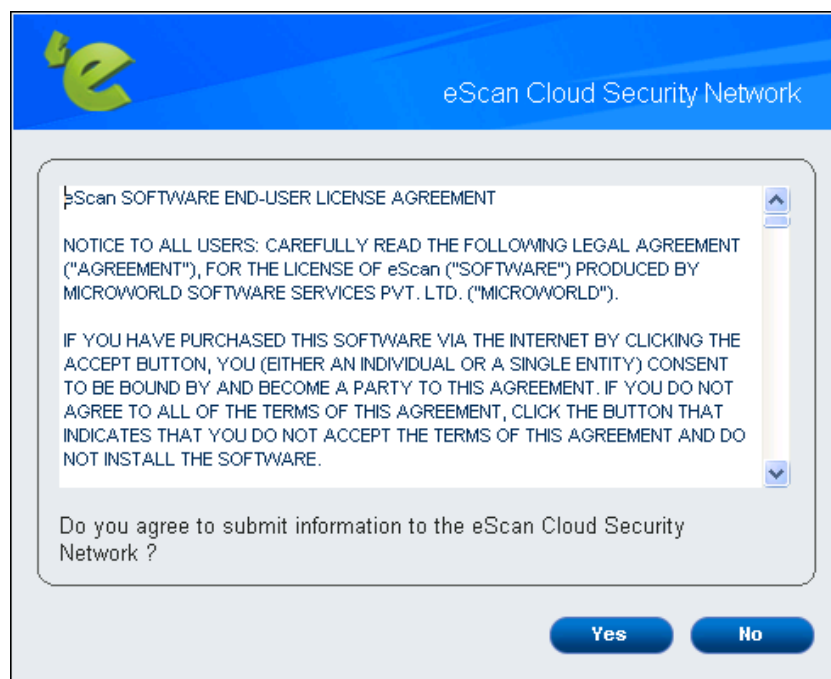
As soon as a program is declared malicious or unsafe, the information becomes available to eScan product users even before the signature for that piece of malware is created and updated on their computers.

Thus, eScan clients receive prompt information about new and unknown threats minutes after the launch of a cyber-attack, compared to hours for traditional signature database update.

 NOTE	The Cloud Protection module is enabled, by default.
--	---

You need to have internet connection, to access this feature. Perform the following steps to enable the cloud protection service:

1. To use the cloud protection service you need to first accept the terms of eScan Security Network (ESN) agreement. On the Cloud Protection screen, at lower-left corner of the screen select **I agree to participate in eScan Cloud Security Network** check box. The eScan Cloud Security Network dialog box appears.

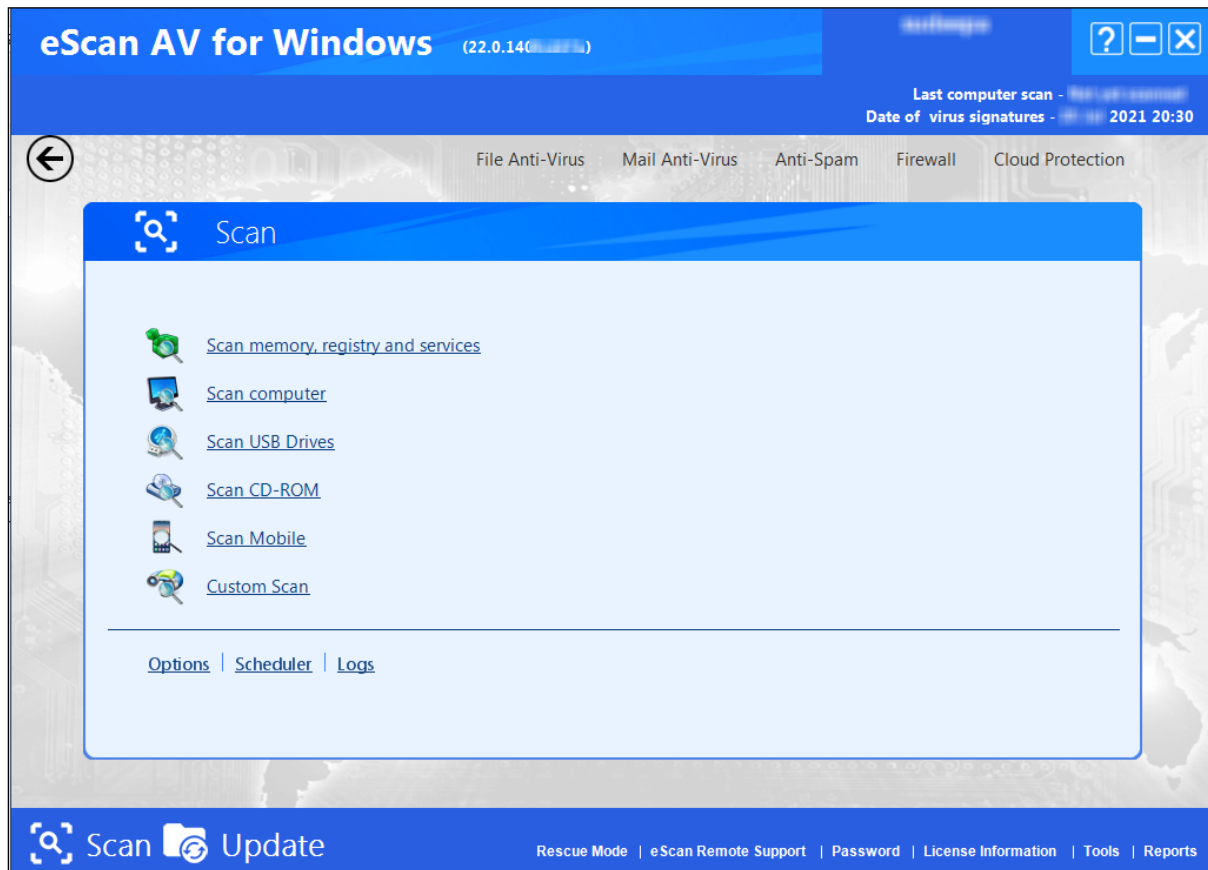


2. Click the **Yes** button. The eScan Security Network starts functioning and displays the current eScan Cloud Security Network statistics such as number of safe data, dangerous data, total data, and unprocessed data objects along with last synchronization date.



Scan

The Scan module helps you perform on-demand scans on files, folders, storage devices, and the registry and schedule automatic scans. It checks your computer for security threats, such as viruses, spyware, and other malicious software and creates logs of all scan operations.



When you click the Scan button, the Scan page is displayed. This page provides you with options for scanning the computer and peripheral storage devices, configuring the Scan module, and scheduling scans. We have more options under this module which is explained below.

Scan memory, registry and services

This option provides scanning options for memory, registry, and services. By clicking on this link, you will get a popup window.

Scan computer

This option scans entire system as whole. By clicking on this link, you will get a popup of Option window, to learn more [click here](#).

Scan USB Drives

This option scans USB drives attached to your system.

Scan CD-ROM

This option scans CD-ROM once it is inserted in your system.

Scan Mobile

This option will scan the mobile devices connected through USB to the computer.

Custom Scan

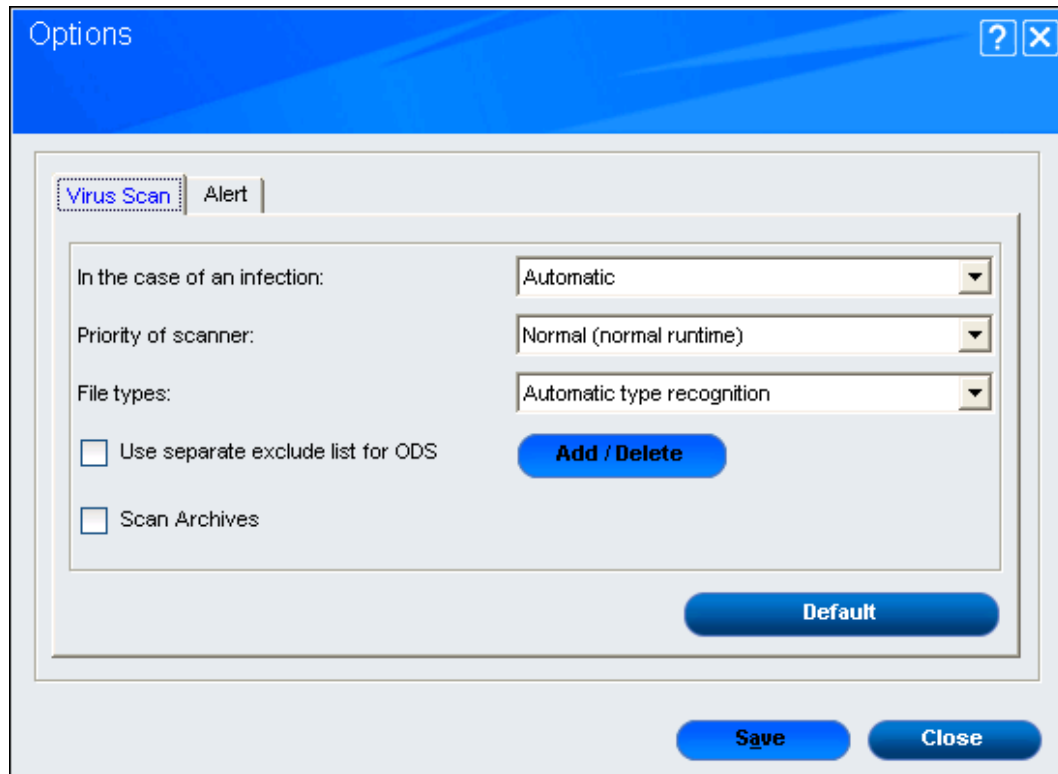
This option helps you to configure the scan according to the specific need of the users.

Options

You can configure **Scan** options by clicking the **Options** button. This will display the **Options** dialog box, which provides you with options for configuring the Scan module. This dialog box has two panes: **Virus Scan** and **Alert**. Let's discuss them in detail.

Virus Scan

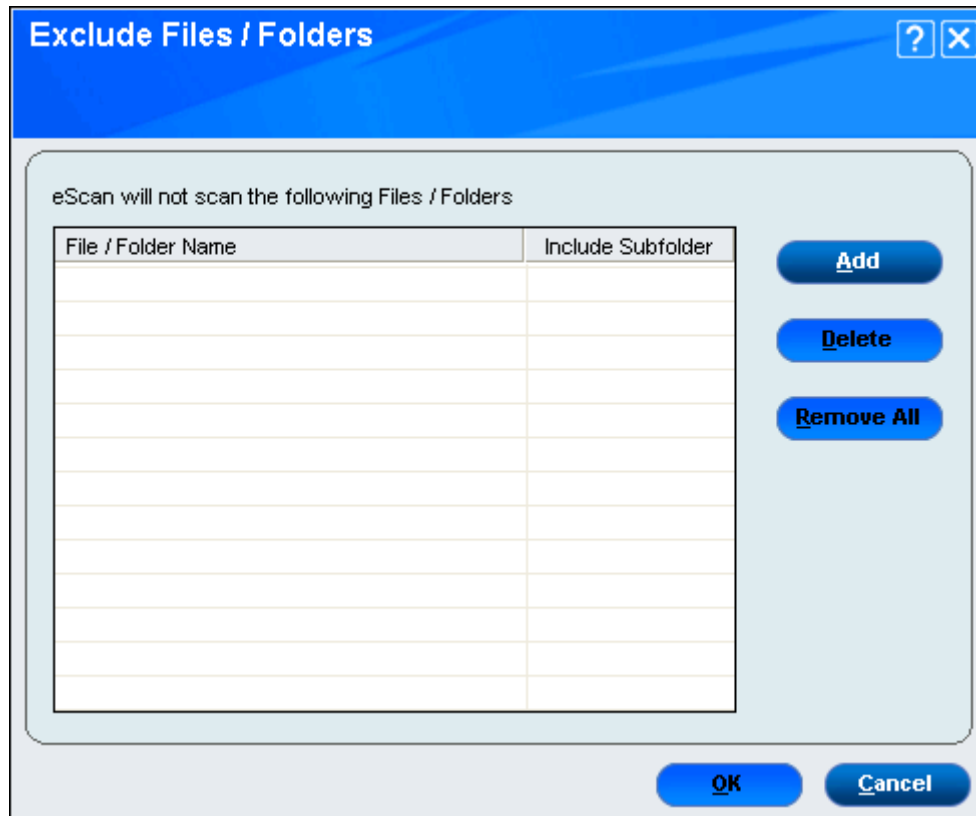
This tab helps you configure the actions that should be performed when an infection is detected. It allows you to set priority of the scan process as **High**, **Normal**, or **Low**. It also helps you to automatically recognize either all file types or only program files.



This tab has following options to configure your scan:

- **In the case of an infection:** This list helps you configure the action that should be performed on the file when it finds that it is infected. The actions are as follows:
 - **Log only:** This option only logs the occurrence of the virus infection without taking any action.
 - **Delete infected file:** This option deletes the infected file.
 - **Automatic:** This action is set by default and tries to clean the file. If it is not possible to disinfect the file, it quarantines or deletes the file.
- **Priority of scanner:** This option helps you set the priority of the scanner in relation to other processes running on the computer. The priority level can be **High (short runtime)**, **Normal (normal runtime)**, or **Low (long runtime)**. By default, the scanner runs with Normal (normal runtime) priority.
- **File types:** This option helps you to select the type of files that should be scanned by **On-demand Scan**. The options available are:
 - **Automatic type recognition:** This option is selected by default and scans all files, but will ignore the files that cannot be infected.
 - **Only program files:** This option scans only the program files or executables stored on your computer.

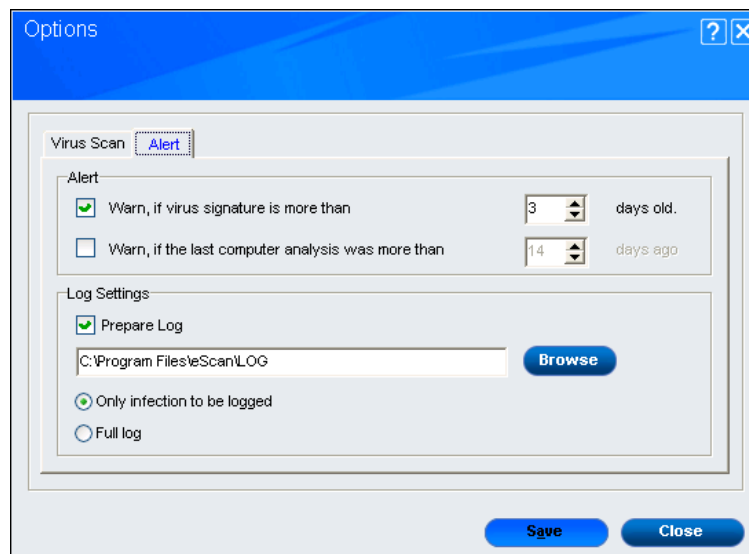
- **Use separate exclude list for ODS:** Select this check box to exclude all the listed files, folders, and sub folders from monitoring during the on-demand scan. This option helps eScan to separate the exclude list of on-demand scanning from real-time scanning exclude list. Once you click on **Add/Delete** button, you can add or delete the files, folders, and subfolders.



- On the **Exclude Folders** dialogue box, you will find following buttons:
- **Add:** This button will give you a popup window **Add to Exclude List**. Click an appropriate object type such as **File** or **Folder**, and then type or click **Browse** button to select the file or folder that you want to exclude. If you want to include sub folder of a folder, select **Include Subfolder** check box. Then click on the **Add** button.
 - **Delete:** This button deletes any file/folder from the list.
 - **Remove All:** This button removes all the files/folders from the list.
 - **Scan Archives:** This check box scans both archived and packed files.
 - **Default:** This button resets the entire scan configuration to default settings.

Alert

This tab helps you to configure the alert when it detects malicious software on your computer.



This tab has following options to configure the setting:

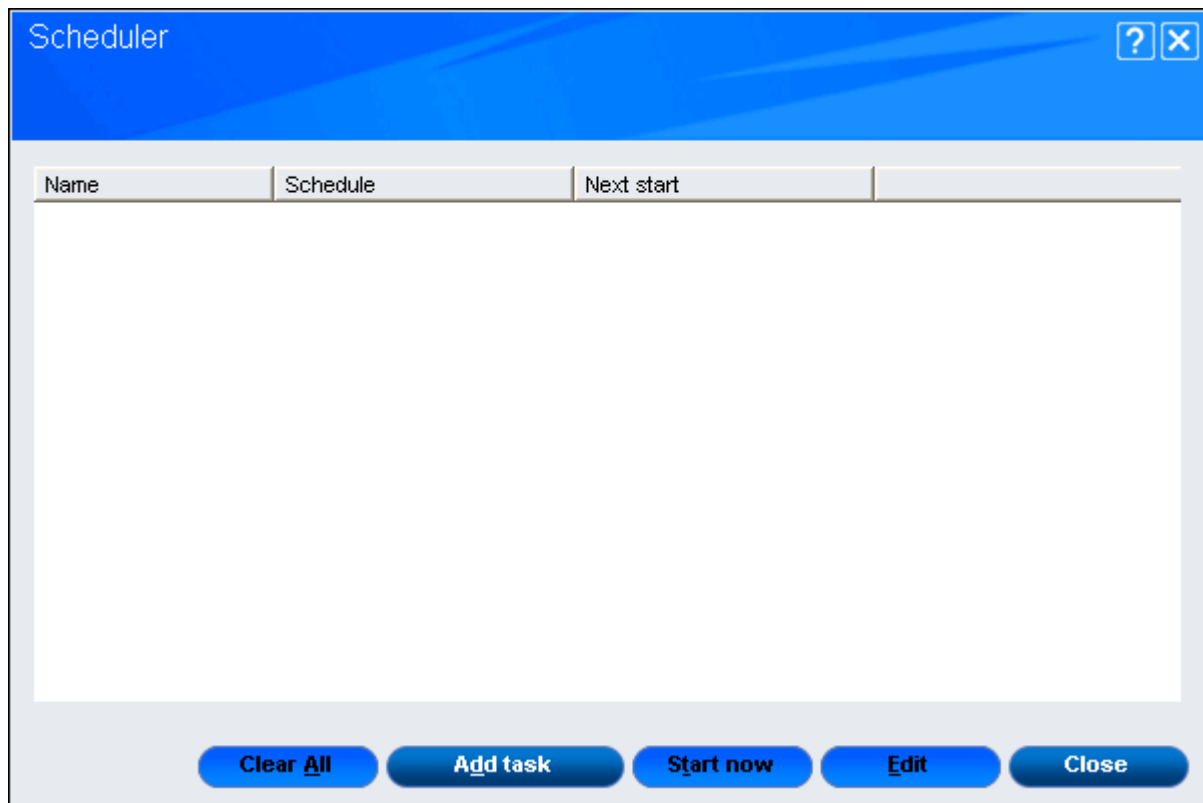
- **Alert:** In this section, you can configure the notification displayed when the virus definitions are outdated or when a specified number of days have elapsed since you have last scanned your computer. This section gives you following sub-options:
 - **Warn, if virus signature is more than:** This check box is selected by default and notifies you if the virus signature is older than the specified number of days. By default, eScan notifies you when your virus definitions are more than 3 days old.
 - **Warn, if the last computer analysis was more than:** This check box notifies you when a specified number of days have elapsed since the computer was last analyzed. By default, the value is 14.
- **Log Settings:** In this section, you can configure the log settings for the Scan module.
 - **Prepare log:** This check box is selected by default and eScan creates an On-demand Scan log file at the specified path. The default path is **C:\Program Files\eScan\LOG**.
 - **Only infection to be logged:** This option is selected by default and eScan will log information only about infected files and the action taken on them in the On-demand Scan log.
 - **Full log:** This option if selected, the On-demand Scan log will contain information about all the files scanned by eScan.

Both the tabs has 2 common buttons:

- **Save:** This button saves the configuration.
- **Close:** This button closes the popup window without saving the configuration.

Scheduler

In this section, you can schedule On-demand Scan to scan your computer and storage devices for malicious objects. It contains a table, which displays name of the schedule, frequency of occurrence, and the next time it will be run.



We can configure the following options:

- **Add task:** To learn more, [click here](#).
- **Clear All:** This option will clear all the task from the list.
- **Start now:** Once you select the task from the list, you can use this button to start the scanning.
- **Edit:** This option will allow you to edit the existing task from the list.
- **Close:** This option close the popup window without saving.

Adding a task

This button helps you add a new scan task to the schedule. When you click this button, eScan opens the **Automatic virus scan** dialog box. This dialog box includes the **Job**, **Analysis extent**, **Schedule**, and **Virus scan** tabs. Let see each of them in detail.

Job

This tab helps you configure and specify the basic configuration for adding task.

Automatic virus scan [?] [X]

Job | Analysis extent | Schedule | Virus scan

Name Active

Start Type

Start in foreground

Start in background

Quit:

Do not quit if virus detected

Never quit automatically

Do not quit if virus detected

Always quit

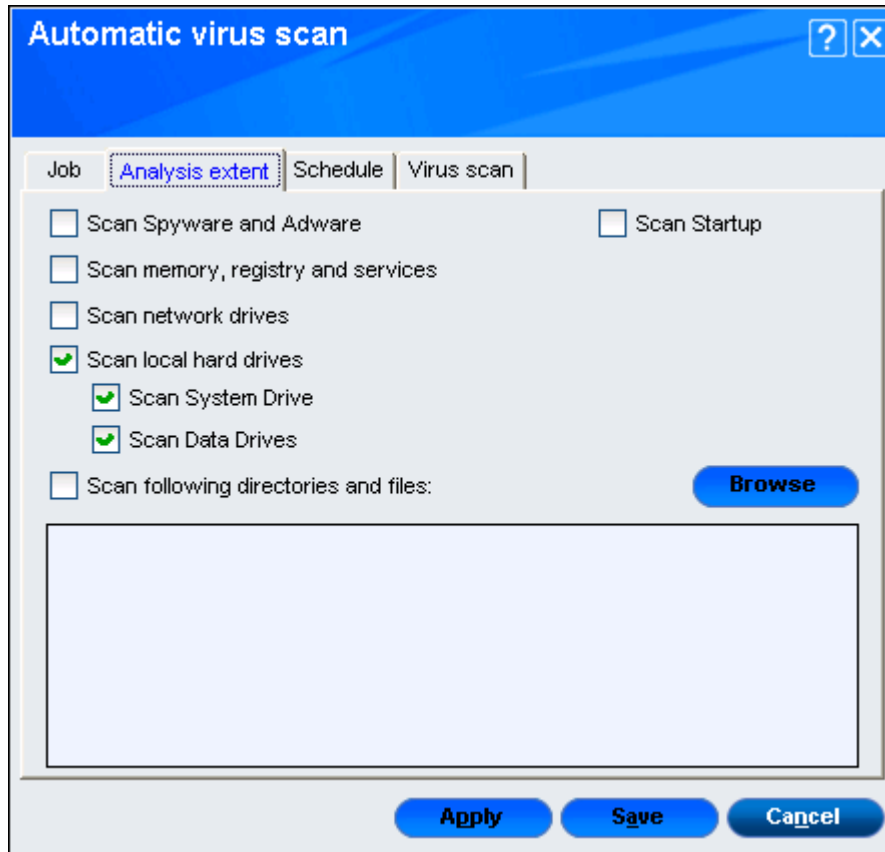
Apply Save Cancel

Specify the following details:

- **Name:** You can specify the name of the task.
- **Start Type:** You select the start type from the following options:
 - **Start in foreground:** This option runs the task in the foreground.
 - **Start in background:** This option runs the task in the background.
- **Quit:** This section will help you to select the termination condition for the task. It has following options:
 - **Do not quit if virus detected:** This option is selected by default and does not allow to quit automatically after it has finished scanning and a virus is detected.
 - **Never quit automatically:** This option does not allow On-demand Scan to quit automatically after it has finished scanning.
 - **Always quit:** This option allows On-demand Scan to quit automatically after it has finished scanning.

Analysis extent

This tab provides options that help you to select the type of scanning, and the list of directories, folders, or local hard drives to be scanned.

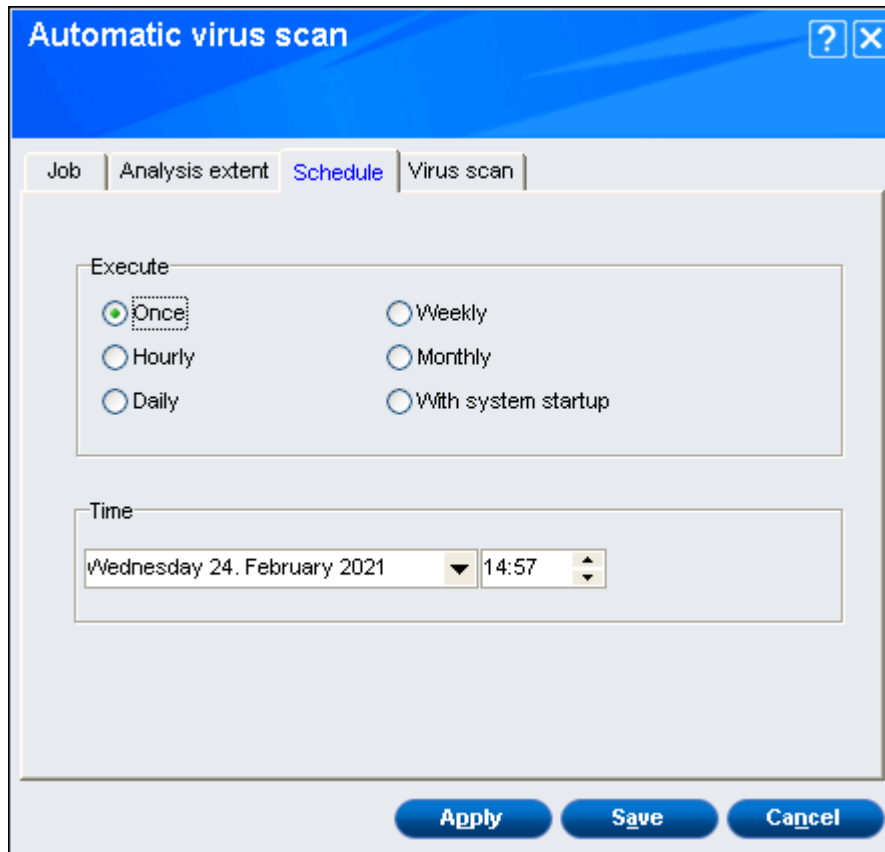


This has following options to configure:

- **Scan Spyware and Adware:** This option lets you to scan Spyware and Adware.
- **Scan memory, registry, and services:** This option provides scanning options for memory, registry, and services.
- **Scan network drives:** This option lets you to scan network drives.
- **Scan local hard drives:** This options is selected by default and lets you scan the local hard drives and has following sub-options:
 - **Scan System Drive:** This option lets you scan system drives.
 - **Scan Data Drives:** This option lets you scan data drives.
- **Scan following directories and files:** This option lets you add the directory and files you want to scan. You can add folders and files through **Browse** button.
- **Scan Startup:** This option scan startup files.

Schedule

This tab helps you to configure the options for scheduling system scans. You can schedule scans to run either once or on a daily, hourly, weekly, monthly basis, when the computer boots up, or on a given date at a specific time.

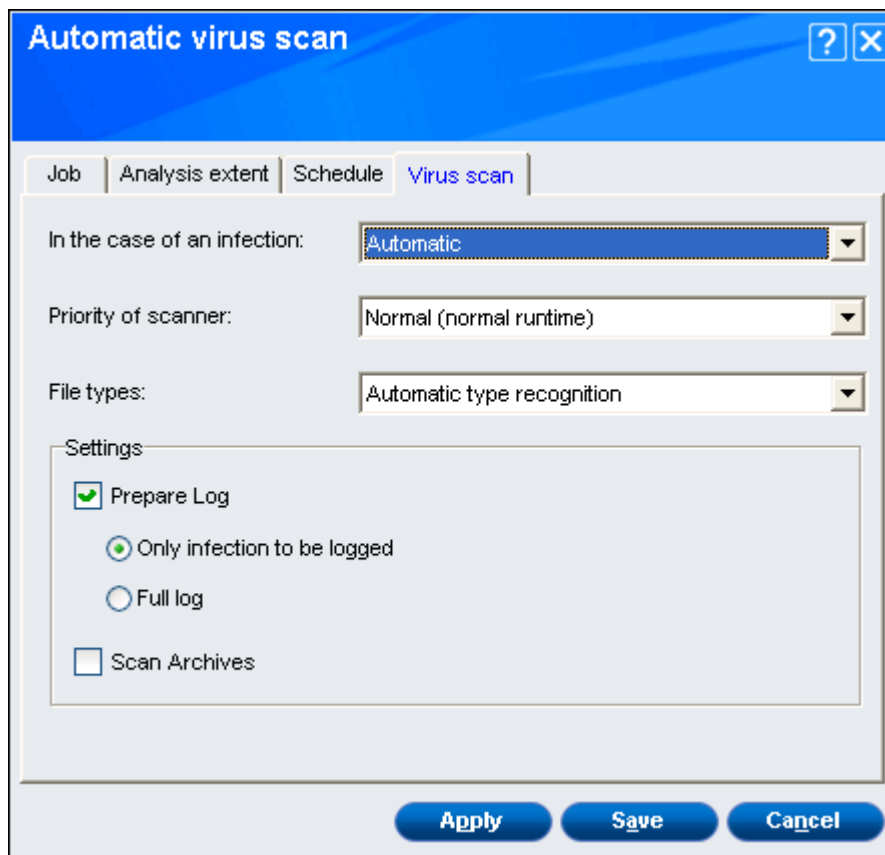


It has following options to configure:

- **Execute:** This options lets you schedule the scan to run Once, Hourly, Daily, Weekly, Monthly, and With system startup.
- **Time:** This option lets you provide the date and time to schedule the scan.

Virus scan

This tab provides the same options as the ones present on the **Virus scan** tab of the Scan module. You can configure On-demand Scan to perform a specific action when a virus infection is detected. You can also set the priority of the eScan scanner in relation to other processes running on the computer. The priority level can be high, normal, or low. By default, the scanner runs with normal priority. In addition, you can configure On-demand Scan to scan only program files or executable files.



To learn more, [click here](#).

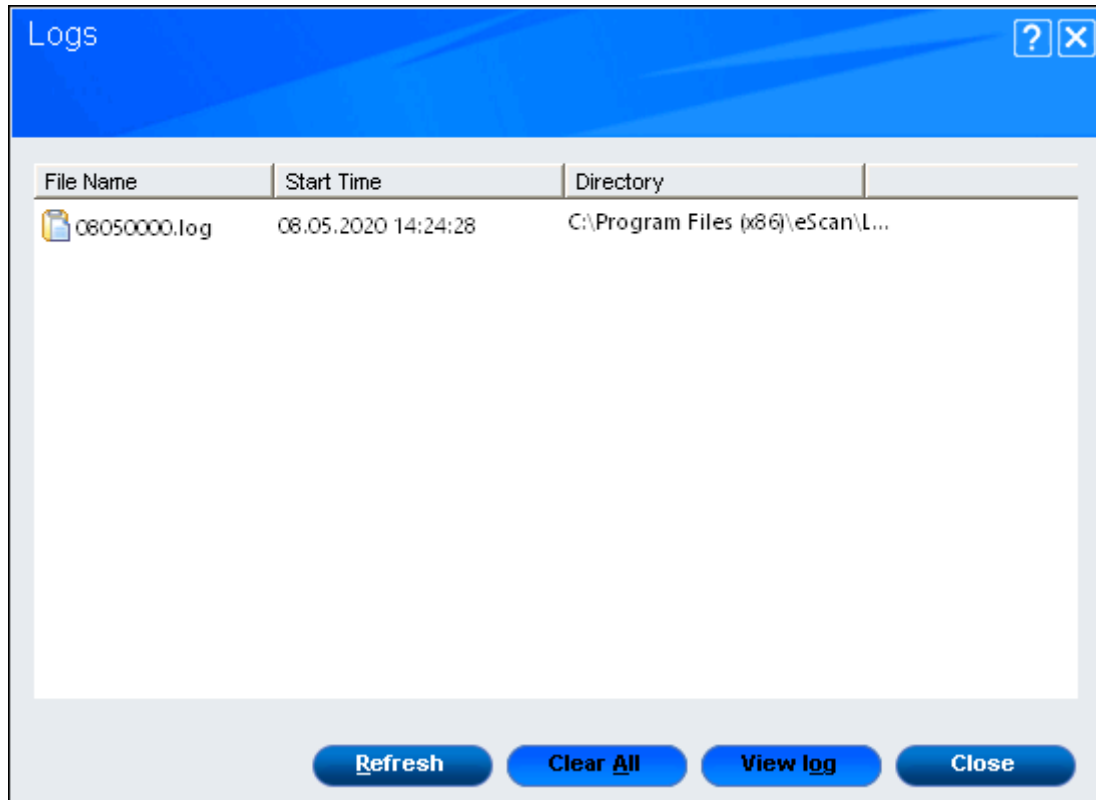
Apply: Click on this button, to apply the configured settings.

Save: Click on this button, to save the configuration.

Cancel: Click on this button to exist, without saving configuration.

Logs

You can view reports of the scheduled On-demand scans performed on your computer and storage devices in the **Logs** dialog box.

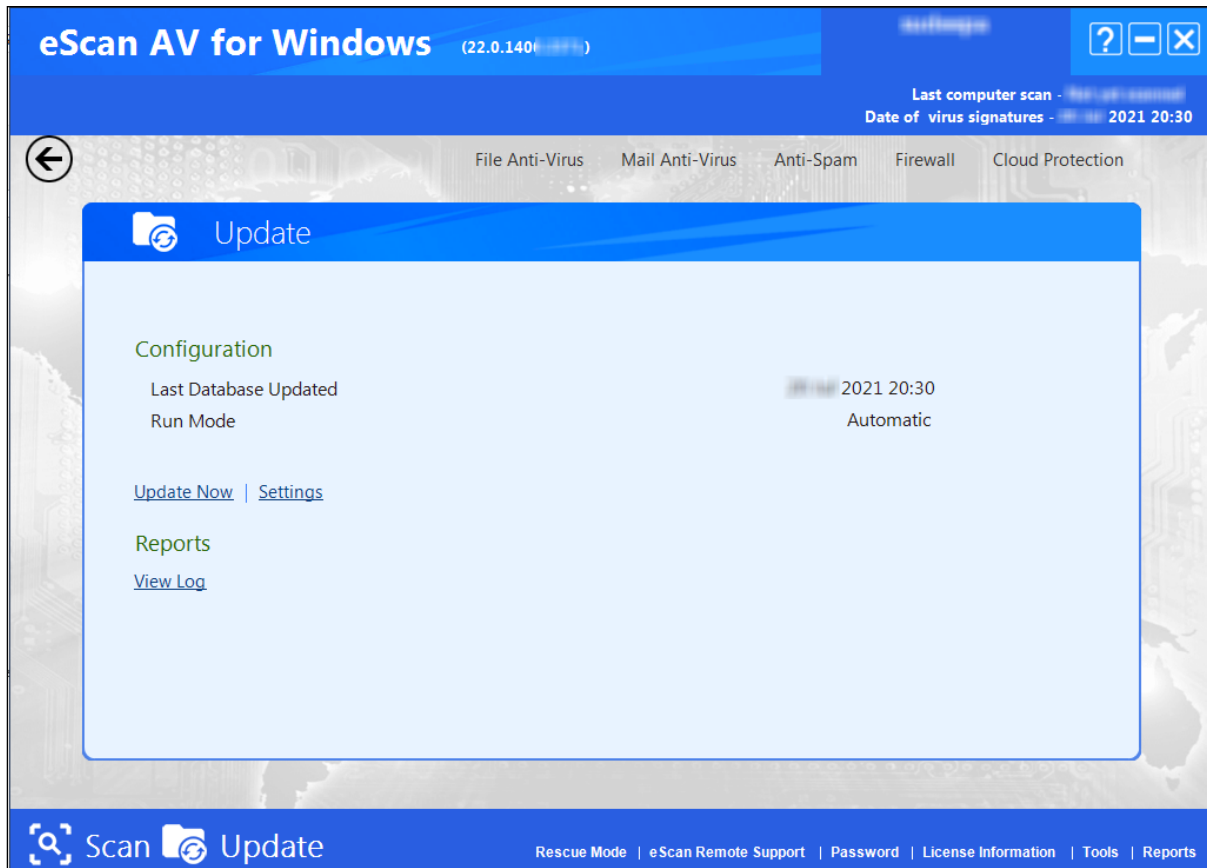


This dialogue box provides information of the generated logs such as File Name, Start Time, and Directory in which it is present. This also has following buttons:

- **Refresh:** This buttons refreshes the whole list.
- **Clear All:** This button clears all the generated log files.
- **View log:** This button is used to view the generated log file by selecting a log file from the list.
- **Close:** This button closes the popup window.

Update

The Update module automatically keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. You can configure eScan to download updates automatically either from eScan update servers or from local network by using UNC.



You can access tabbed page for the Update module by clicking the **Update** button. The update tabbed page provides you with information regarding the type of update mode and date on which the database was last updated. It also provides you with options for configuring the module and helps you view reports on recent scans performed by the module.

You can configure the following sections through this module.

Configuration

This section displays the following information:

- **Last Database Updated:** It shows when the eScan database was last updated.
- **Run Mode:** It displays the type of update mode used by eScan. The run mode can be either **Automatic** or **Scheduled**.
- **Update Now:** This button updates the Anti-Virus and Anti-Spam definitions through HTTP or FTP.

Time	Result	Object	Size
3/1/2021 10:34:53 AM	File Downloaded	exploits.avc3	51 Bytes
3/1/2021 10:34:53 AM	File Downloaded	settings.avc3	64 Bytes
3/1/2021 10:34:53 AM	File Downloaded	avc3.gx	1525 Bytes
3/1/2021 10:34:54 AM	File Downloaded	configuration.avc3	210 Bytes
3/1/2021 10:34:54 AM	File Downloaded	update.bin	35 Bytes

Downloading File: update.bin

Total Downloaded: 1.8 KB / 1.8 KB Duration: 00:00:11

Anti-Virus Status: Time Left: 00:00:00

Anti-Spam Status: Time Left: 00:00:00

Buttons: Hide, Stop Update

- **Settings:** To learn more, [click here](#).

Settings

This button opens the **Update Settings** dialog box, which helps you configure the Update module to download updates automatically. Let's see them in detail.

General Config

This tab provides you with general options for configuring the Update module.

The screenshot shows the 'Update Settings' dialog box with the 'General Config' tab selected. The 'Select Mode' section has radio buttons for FTP, HTTP (selected), and Network. The 'Proxy Settings' section has a checked 'Download via Proxy' checkbox. Under 'HTTP', there are fields for 'HTTP Proxy Server IP' (192.168.1.1), 'Port' (3128), 'Login Name', and 'Password'. Under 'FTP', there are fields for 'FTP Proxy Server IP', 'Port' (1021), 'Login Name' (anonymous), and 'Password' (masked). A 'Logon Type' section has radio buttons for 'User@siteaddress', 'OPEN siteaddress' (selected), 'PASV Mode', and 'Socks'. At the bottom, there is a 'Network' section with a 'Source UNC Path' field. Buttons for 'Default', 'OK', 'Cancel', and 'Apply' are at the bottom right.

It consists of following options to configure:

- **Select Mode:** It indicates the mode for downloading updates from eScan update servers. You can select the appropriate options from **FTP**, **HTTP**, and **Network**.
- **Proxy Settings:** In this section, you can configure the proxy settings for downloading updates through HTTP or FTP proxy servers. In both case, you need to provide the IP address of the proxy server, the port number, and the authentication credentials if any. In case of FTP servers, you also need to provide the format for the user ID in the **Logon Type** section. Logon ID is defined as User@siteaddress, OPEN siteaddress, PASV Mode, and Socks.
- **Network:** In this section, you need to provide **Source UNC Path**. This section will enable only if you select **Network** in the **Select Mode** section.

After Update

This tab helps you configure the actions that eScan should perform after Updater downloads the updates.

You can configure the following options:

- **Execute this Program, after downloading updates successfully:** When you select this check box, eScan runs a particular application or program after eScan updates are downloaded successfully.

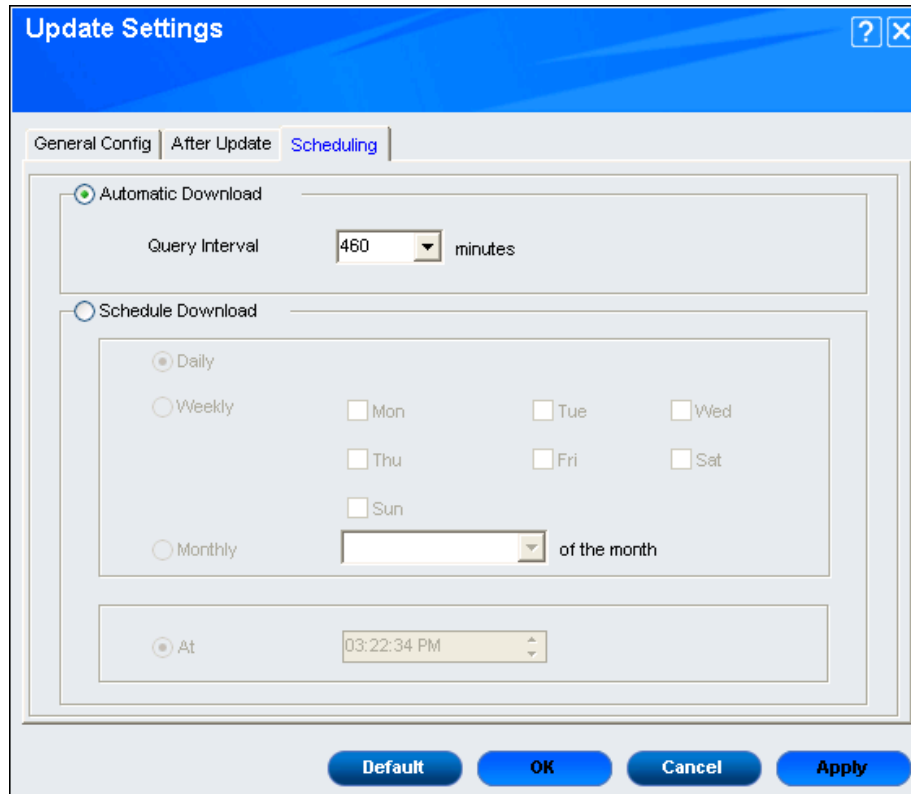
This section has the following options and will be enabled once you select **Execute this Program, after downloading updates successfully** check box:

- **Program Name:** Sometimes, you may need a particular program to run after you have downloaded updates for eScan. You can simply specify the path of the program in the **Program Name** box. Alternatively, you can use the **Browse** button to navigate to the path where the program executable is stored.
- **Start In:** You can also specify the program to execute from a given location. You can either specify the location in the **Start In** box or use the **Browse** button to navigate to the folder where the program should execute.
- **Parameters:** Some programs require additional parameters to execute. You can specify these start parameters in the **Parameters** box.


- **Run:** The default mode is normal mode. Whenever a program runs, it runs in its own window. You can specify whether the window should be in the maximized, minimized, normal, or hidden state. The default state of the window is normal.
- **Terminate the process forcibly:** You can also forcibly terminate the process to free system resources by selecting this option.
- **Don't wait for process to complete:** A process may require a long time to end. In such cases, you can allow other processes to run along with the specified process by selecting this option.
- **While this process is being executed, suspend all operations for <placeholder> seconds:** The default value is 1. You can also ensure that the no other process runs while the specified process is running for a given time interval by setting the interval in the box.
- **Update Notification:** When you select this option, eScan sends an email notification to the email address specified in the **To** box in the **Update Notification** section.
 - **From:** The default email address provided is `escanuser@escanav.com`. You can specify the sender's email address in the notification mail in this box.
 - **To:** You can specify the recipient's email address in the notification mail in this box.
 - **SMTP Server:** The default IP set is `127:0:0:1`. You can specify the IP address of the SMTP server in this box.
 - **SMTP Port:** The default port set is 25. You can specify the port number of the SMTP port in this box.

Scheduling

The Scheduler automatically polls the Web site for updates and downloads the latest updates when they are available. You can also schedule downloads to occur on specific days or at a specific time.



It has following options:

- **Automatic Download:** This option is selected by default and configures the Update module to query and download the latest updates automatically from the MicroWorld website. You can configure the query interval by using the following setting.
 - **Query Interval:** The default interval set is 120 minutes. You can set the interval in minutes, after which eScan should query the web site for latest updates.
- **Schedule Download:** This option is set as Daily by default. You can also schedule downloads to occur on specific days or on a daily, weekly, or monthly basis. In addition, eScan also provides you with the facility of downloading updates at a specific time. By default, the time is set to 1:50:00 P.M. Type or select the time at which you want eScan to download updates, by clicking the  icon. When you configure this setting, the Scheduler checks the MicroWorld Web site for latest updates at the specified time and downloads them if they are available.

All the tabs has 4 common buttons:

Default

This button reset the configuration.

OK

This button is clicked once you click on **Apply** button to apply the changes.

Cancel

This button closes the popup window without applying the configuration.

Apply

This button applies the changes in the configurations.

Reports

This section displays the following information:

- **View Log:** When you click this button, the **Update Log** window is displayed. This window displays the latest activity report for the Update module.

The screenshot shows the 'Update Log' window with the following data:

Date/Time	Session	Ip Address/Host Name
2/23/2021 4:24:08 PM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...
2/23/2021 5:29:11 PM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...
2/24/2021 1:13:48 AM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...
2/24/2021 8:58:48 AM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...

Result	Object	Size
Successfully Downloaded File	aitok.cvd	7850
Successfully Downloaded File	auto.cvd	30043
Successfully Downloaded File	cevakrnl.rv2	277382
Successfully Downloaded File	cevakrnl.rv8	68016
Successfully Downloaded File	e_spyw.i00	1062

Event Description

```

Automatic HTTP Downloader Ver 4.0.2.389.
-----
Check eUpdate.ini Settings.
24-Feb-2021 08:58:49 Connection Successful with Ini Settings.
Connecting to proxy server 192.168.1.11
Requested file name and size
[BDUpdCallBck]Update started
Starting Anti-Virus Download...
Total number of Anti-virus files downloaded is 48
    
```

This report includes the following information:

- The timestamp, session description, and host name or IP address.
- The description of file, such as result of the download, name of the object, and its size.
- The description of event, such as the number of files downloaded, time at which the connection was established or terminated, and the errors, if any.

This window has 2 buttons:

- **Refresh:** This button refreshes the window.
- **Close:** This button closes the popup window.

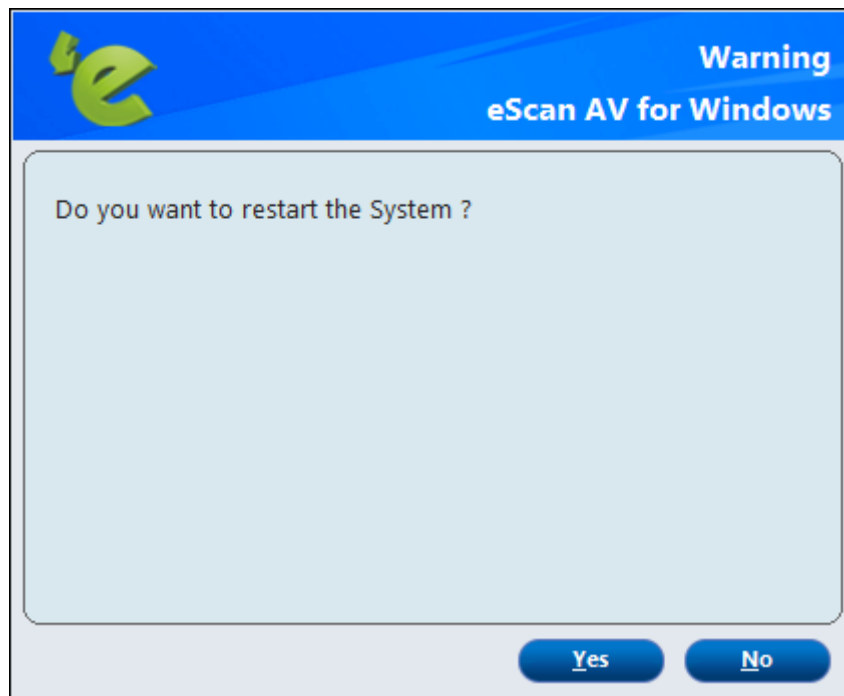
Quick Access Links

On lower-right corner of the screen, you can view the following quick access links:

[Rescue Mode](#) | [eScan Remote Support](#) | [Password](#) | [License Information](#) | [Tools](#) | [Reports](#)

Rescue Mode

Rescue Mode is an eScan feature that enables you to scan and disinfect all existing partitions on your hard drive inside and outside your operating system. Some sophisticated malware, like rootkits, need to be removed before Windows starts. Once eScan detects a threat that cannot be removed, it prompts you to reboot the computer in Rescue Mode for clean-up and restoration.



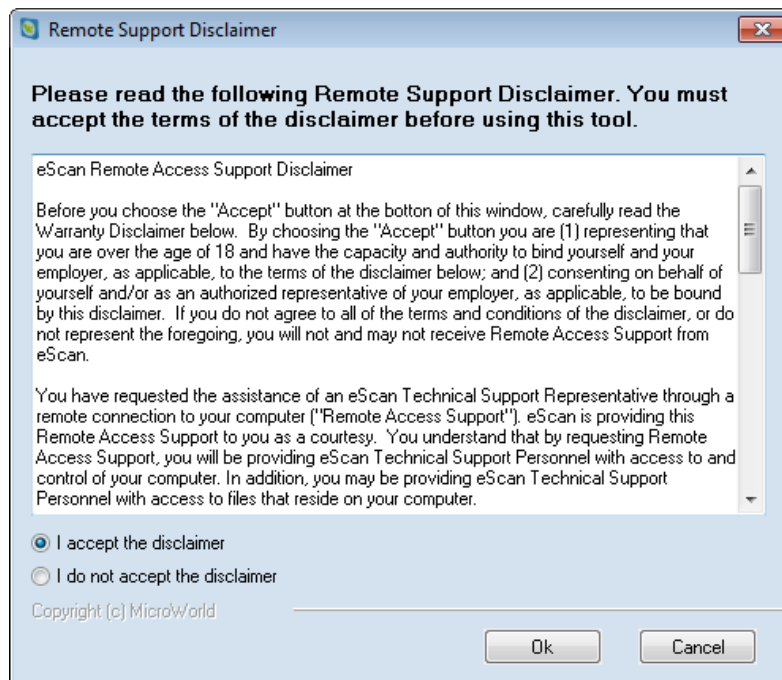
It allows you to boot into a secure environment during system startup without using any optical media. It uses Windows as well as Linux -based environment that not only helps you to scan and clean the system but also allows you to fix registry changes made by viruses and rootkits.

eScan Remote Support

eScan Remote support is the option to get Remote Help from our Support Center; the technical Support Executive will take control of your system for resolving the reported issue. It requires an active internet connection.

Steps for availing remote support:

1. Click on eScan remote support link at the bottom of the interface.
Remote Support Disclaimer window will be opened.



2. Read and accept the disclaimer and click **Ok**.
eScan Remote Support tool will open.
3. It will generate a user ID and password. Send this user id and password to the technical support executive. The executive will take remote support of your system.

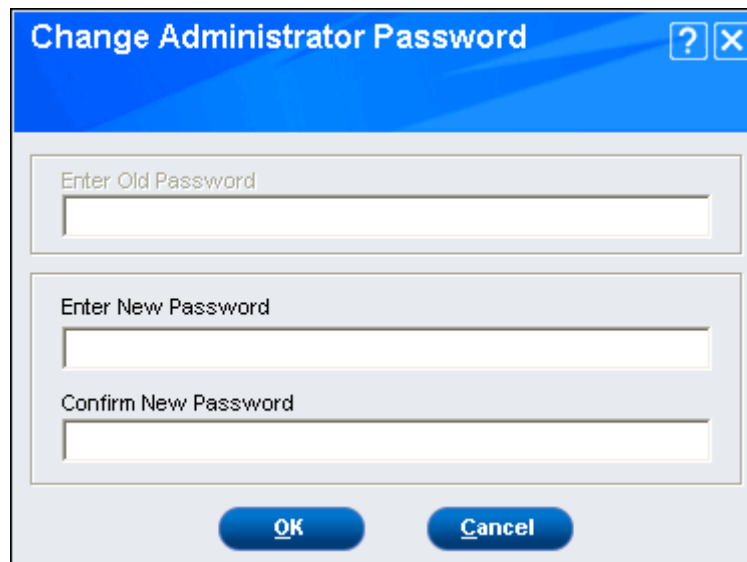
Password

Password will secure your system from making any unauthorized changes to the settings and configurations defined by you.

Using Password Protection for opening eScan

You can define a password for accessing eScan. Use the following steps for defining a password:

1. Open eScan Window.
2. Click **Password** link at the bottom of the interface.
3. Type a Password in the **Enter New Password** field. It is recommended to enter alphanumeric password.
4. Re-enter the Password in **Confirm New Password** field and click **OK**. You will have to enter this password to change any settings and also to open eScan.

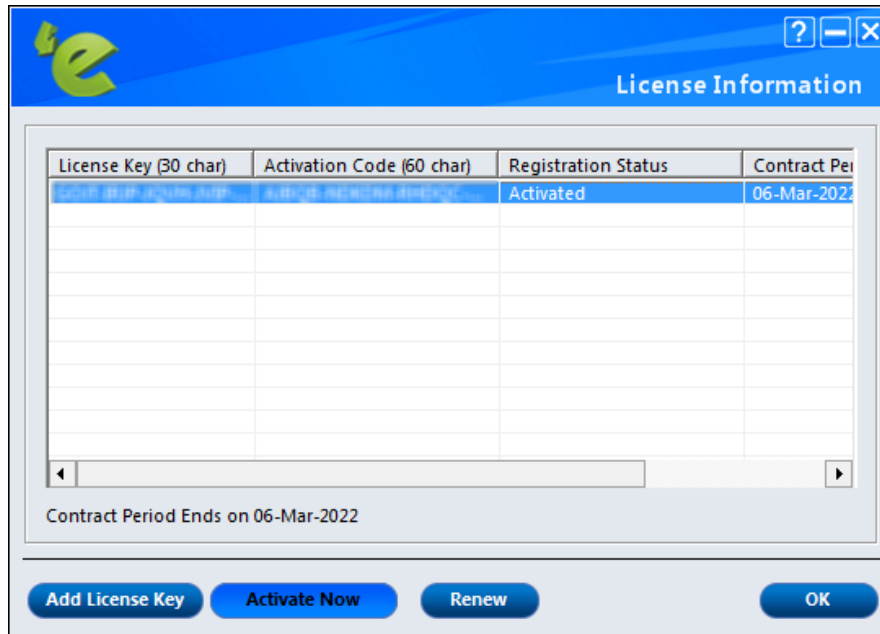



NOTE

For removing the password, Click the password link and enter current password in **Enter Old Password** field, leave **Enter New Password** and **Confirm New Password** fields as blank. Now click **OK**. The defined password will be removed and you will not be prompted to enter password to open eScan.

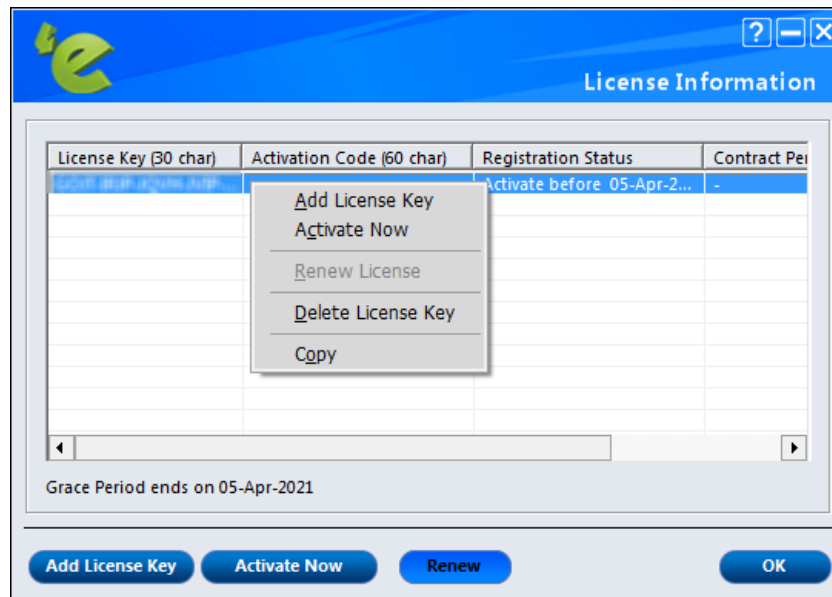
License Information

Click License Information link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to License information window, it displays following important information.



- **License Key:** Displays the License Key of the product.
- **Activation Code:** Displays the Activation Code of the product.
- **Registration Status:** Displays the registration status of the product, namely, Active, Trail, or Expired
- **Contract Period Ends on:** Displays the expiry date of the product activation.
- **Version:** Displays the version number of the antivirus software.

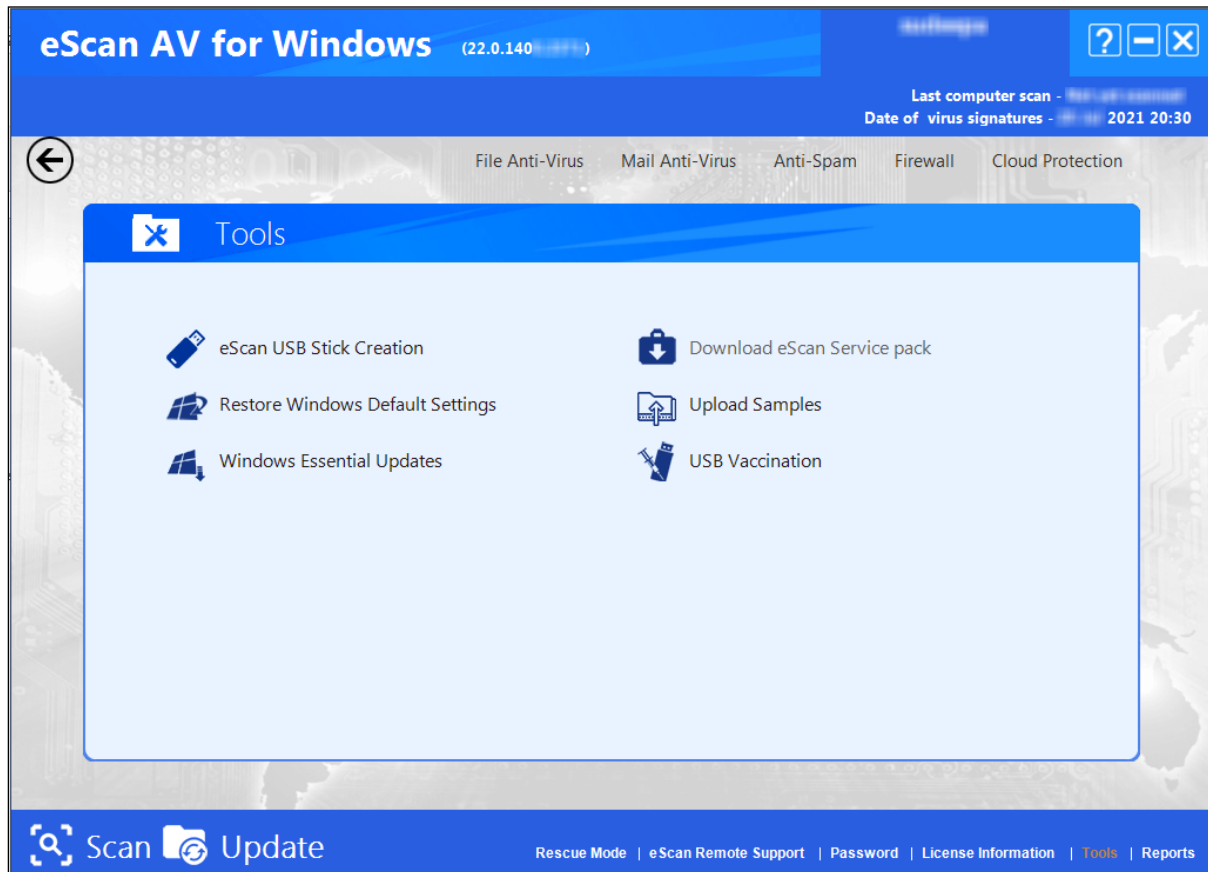
Additionally, it also allows you to perform following actions on right click.



- **Add License Key:** Click on this button to add license key.
- **Activate Now:** Click on this button to activate the license key.
- **Renew License:** Click on this button to renew the license key.
- **Delete License Key:** Click on this button to delete the added license key.
- **Copy:** This option will copy license key.

Tools

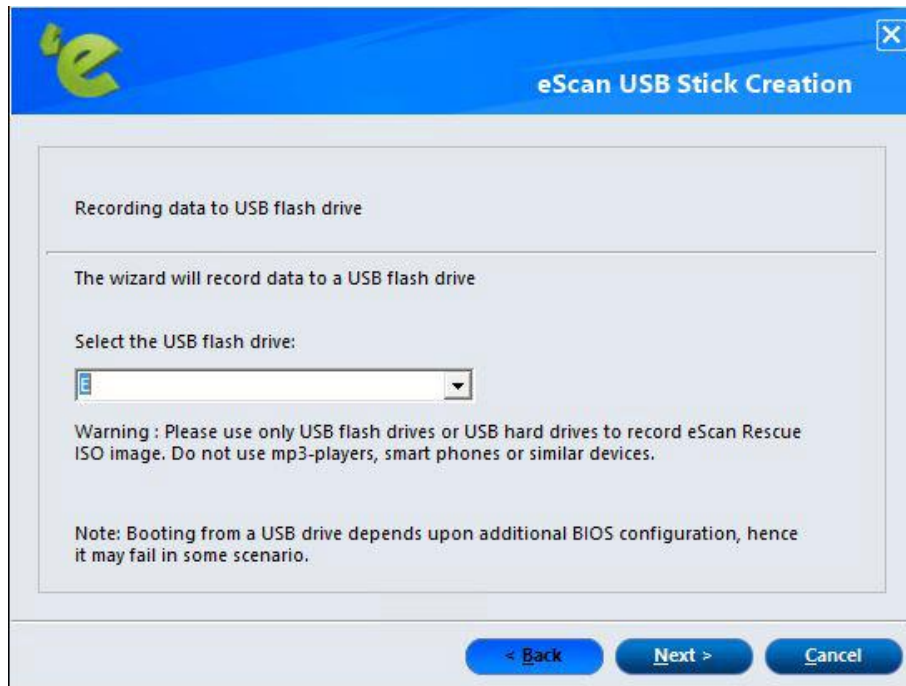
The tools link provides you with the options for easy and quick access to various tools for eScan and each tool will have its own functions.



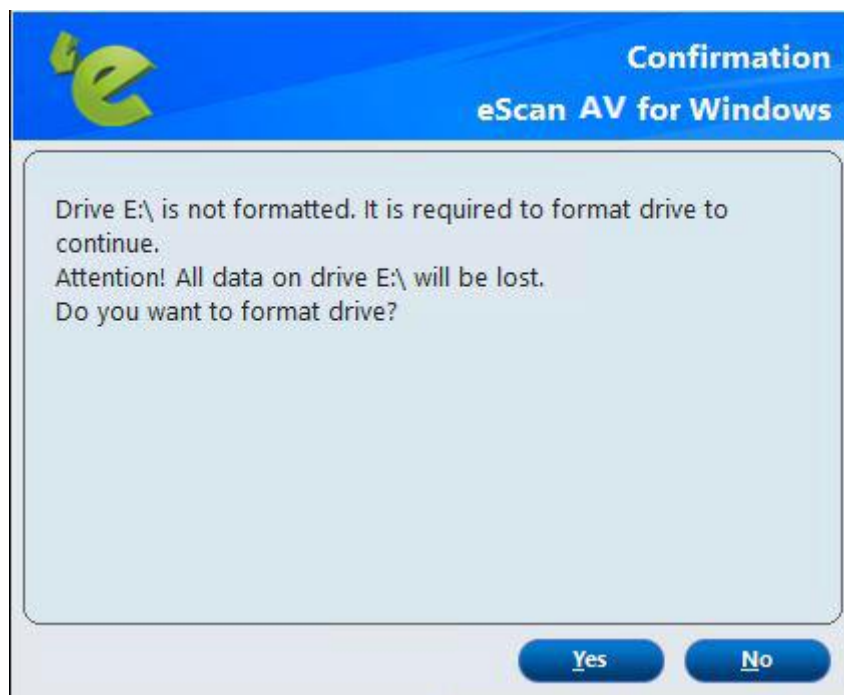
It gives you access to the various eScan AV tools and it performs the following actions.

eScan USB Stick Creation

You will have to burn the image on to a USB device before using it to repair/clean infected or damaged systems. You can connect your USB to the device and select the device from the drop-down menu.



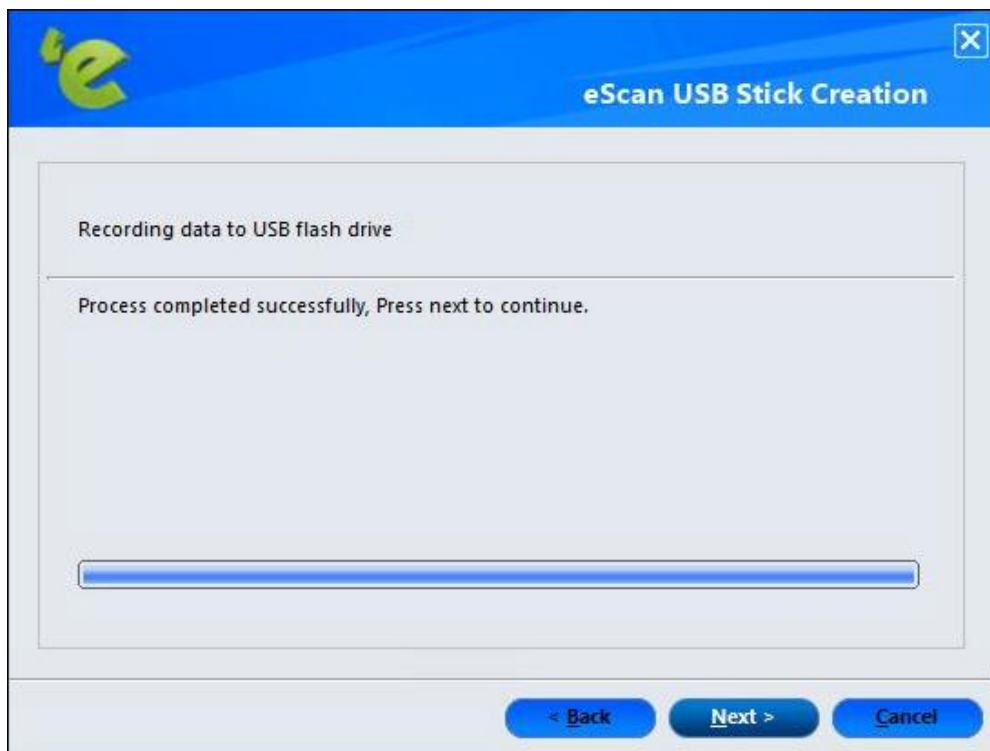
After selecting the device, click **Next>**. It will prompt you to format the USB drive.



Click **Yes**. The process of recording the data in the USB will be initialized and you will get the following screen:



Once the recording process is completed, you will get the following screen. Click **Next>**.



Completing the Rescue USB stick Creation Wizard appears. Click **Finish**. The Rescue USB stick will be created successfully.

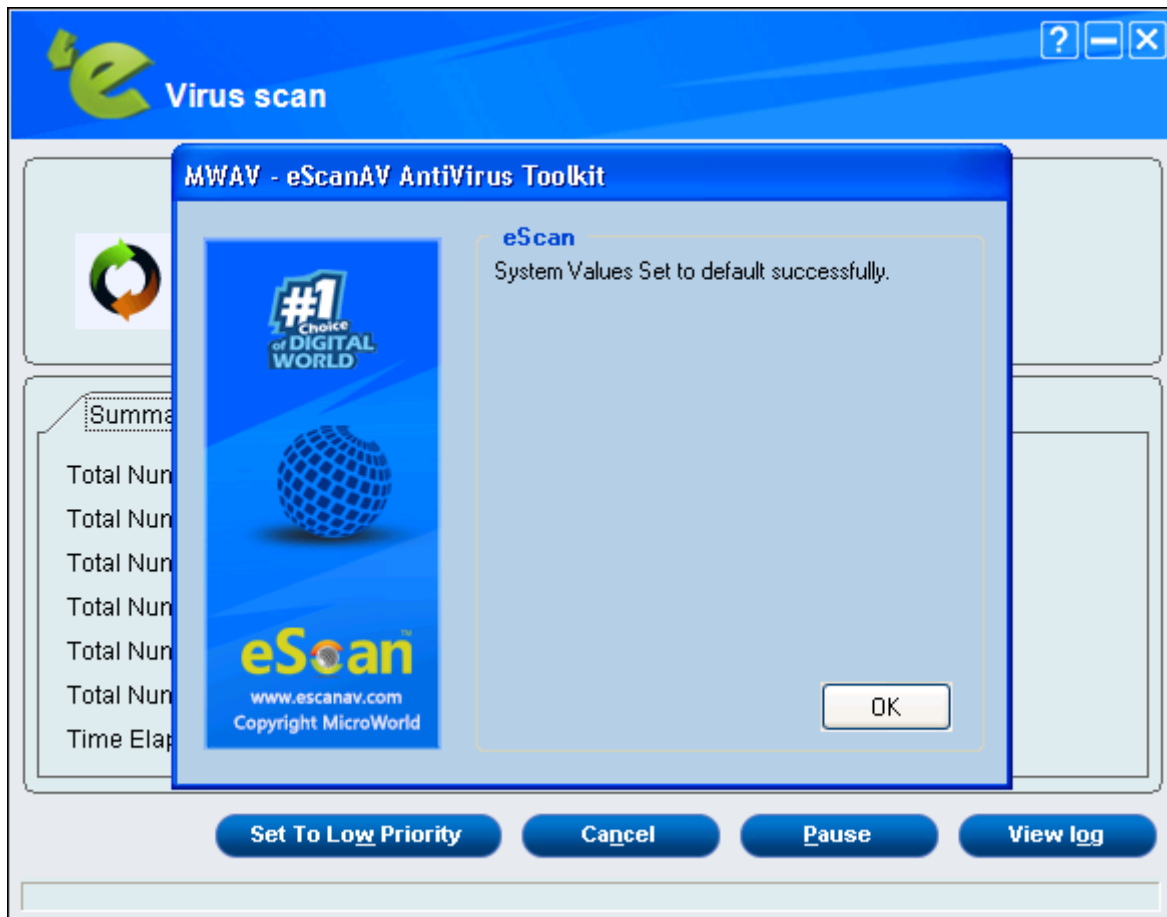


Download eScan service pack

You can download the latest eScan service pack directly from here. This will include all the latest updates.

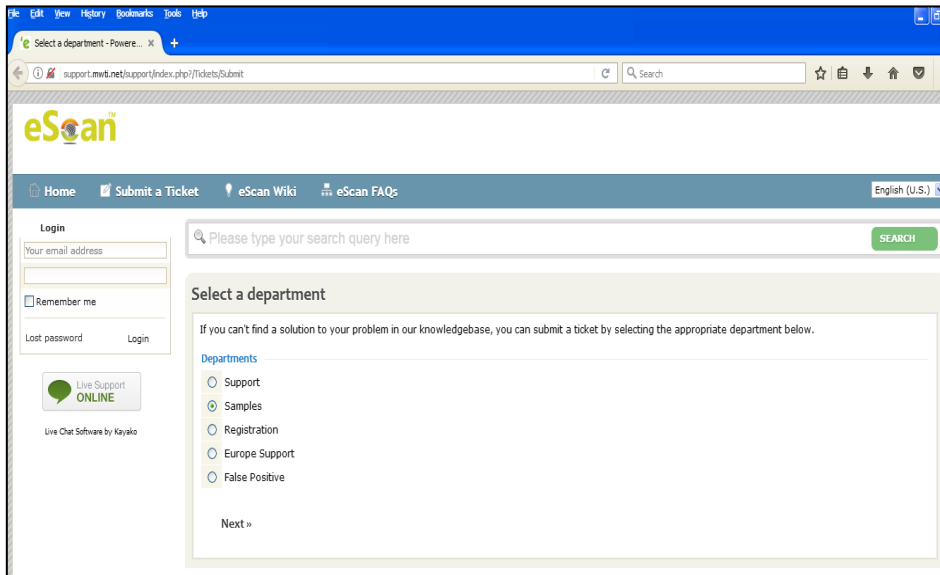
Restore Windows Default Settings

You can restore the Windows® operating system settings, such as desktop and background settings, to eliminate all the modifications made by a virus attack by using this button. eScan automatically scans your computer for viruses when you click this button and sets the system variables to their default values.



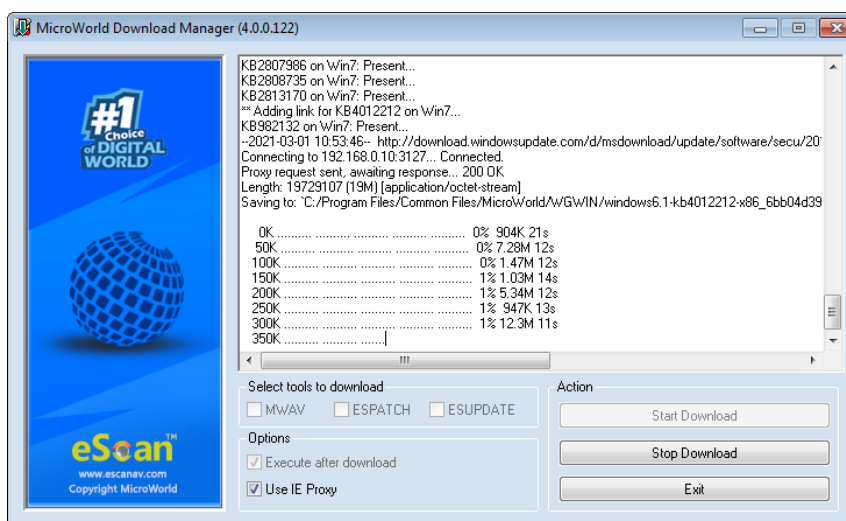
Upload Samples

This functionality will allow you upload the suspicious files that will be checked by eScan's R&D team. You can click on this link, it will be redirect to our website, where you can upload the sample and post your queries.



Windows Essential Updates

It will update your system with the latest windows patch updates. eScan maintains a list of critical Windows Update patches on every computer that are available for free, whenever the user clicks on **Download Latest Hotfix (Microsoft Windows OS)** option, it checks the computer for missing patches on the OS by matching the installed patches with the released patch list in the database. The missing critical Windows update patches are then downloaded and installed on the computer where eScan is running. The database list is categorized on the basis of the operating system.

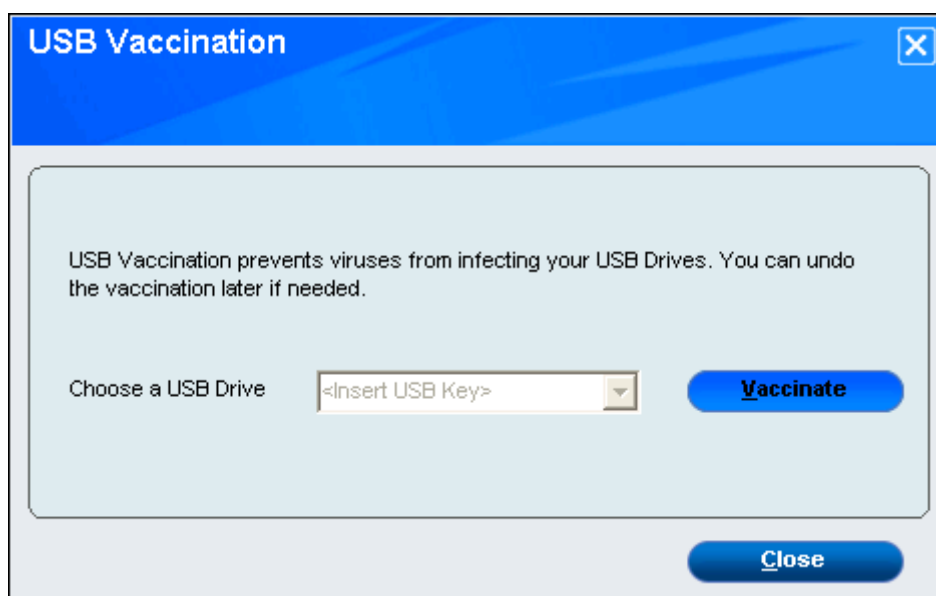


USB Vaccination

The USB devices are used for various purposes, but while using them you may not be aware that the system to which you are connecting is virus infected. When connected to such machines the USB devices also tend to get infected. So, to prevent such cases, eScan has introduced a feature wherein you can vaccinate USB device, whenever needed. Once vaccinated it stays protected even if you connect the flash drive to an infected system, it doesn't become a carrier to infection.

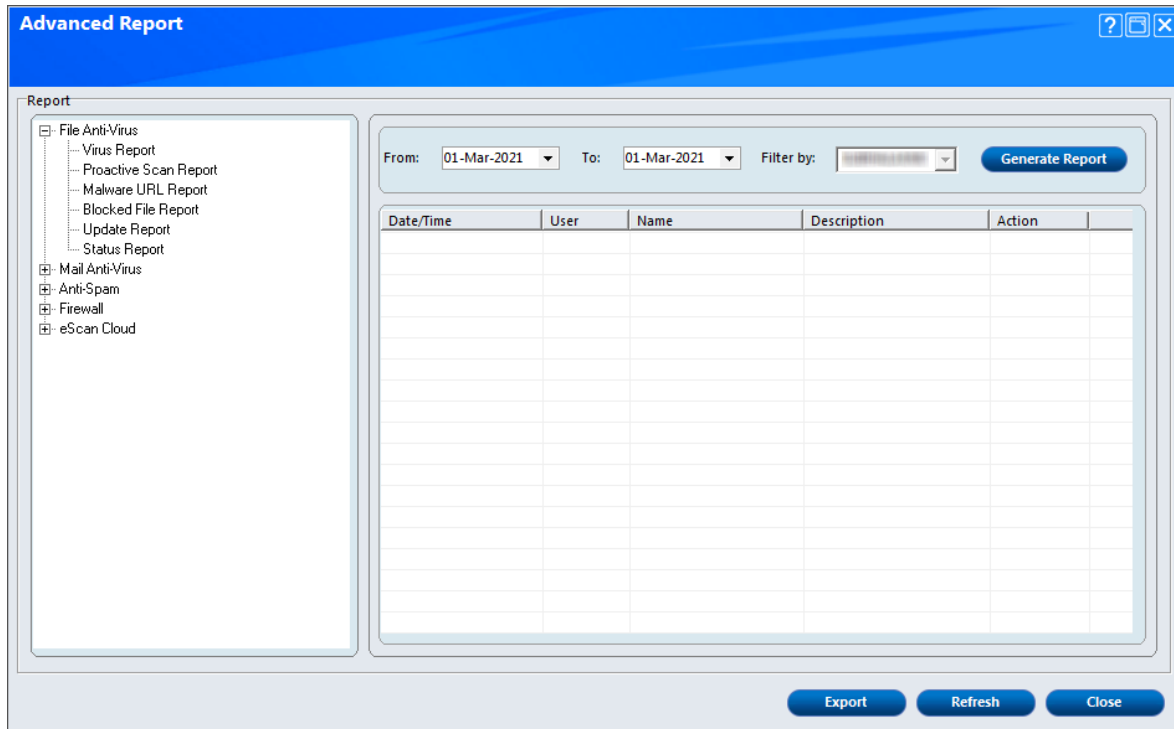
By default, the **Choose a USB Drive** drop-down list and **Vaccinate** button appears dimmed. It is available only when you connect any USB device to your system.

To vaccinate, select an appropriate USB drive, which you want to vaccinate from the **Choose a USB Drive** drop-down list, and click the **Vaccinate** button.



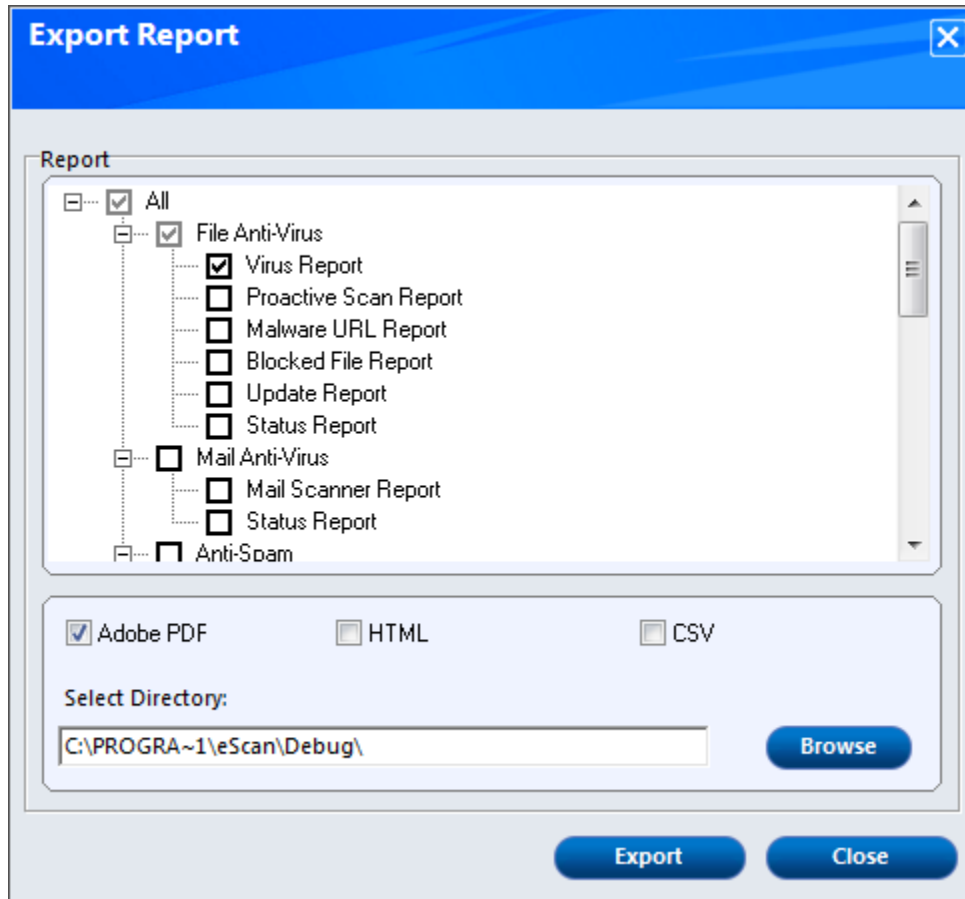
Reports

eScan generate reports for File Anti-Virus, Mail Anti-Virus, Anti-Spam, Firewall, and eScan Cloud modules. Click **Reports** link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to Advance Report window; it displays the report for all the modules of eScan Anti-virus.



- eScan generates reports of all its modules; you can View/Generate a report of any module through **Reports** link present in every module.
- eScan maintains a log of all the recent activities; it includes the date and timestamp, the user details, description and the action taken.

- It will also allow you to export the particular report as per your requirement or all the existing reports in PDF/ HTML/CSV format; it will also allow you to choose the path to save these reports on to your computer.



Procedure to export the report files

1. Select the particular files that you want to export or select the check box next to **All** option to select all the report.
2. Select the particular format of the file that you want to export; you can select from PDF/HTML/CSV file formats.
3. Click **Browse** and select the path where the file has to be saved.
4. Click **Export** to export the report files, or click **Close** to exit the window.

Contact Us

We offer 24/7 free online technical support to our customers through email and live chat. We also provide 24/7 free telephonic support to customers.

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.

Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries. You can contact our support team via Live Chat by clicking [here](#).

Forum Support

You can even join the MicroWorld Forum to discuss eScan related problems with eScan experts by clicking [here](#).

Email Support

If you have any queries, suggestions and comments regarding our products or this User Guide, please write to us at support@escanav.com