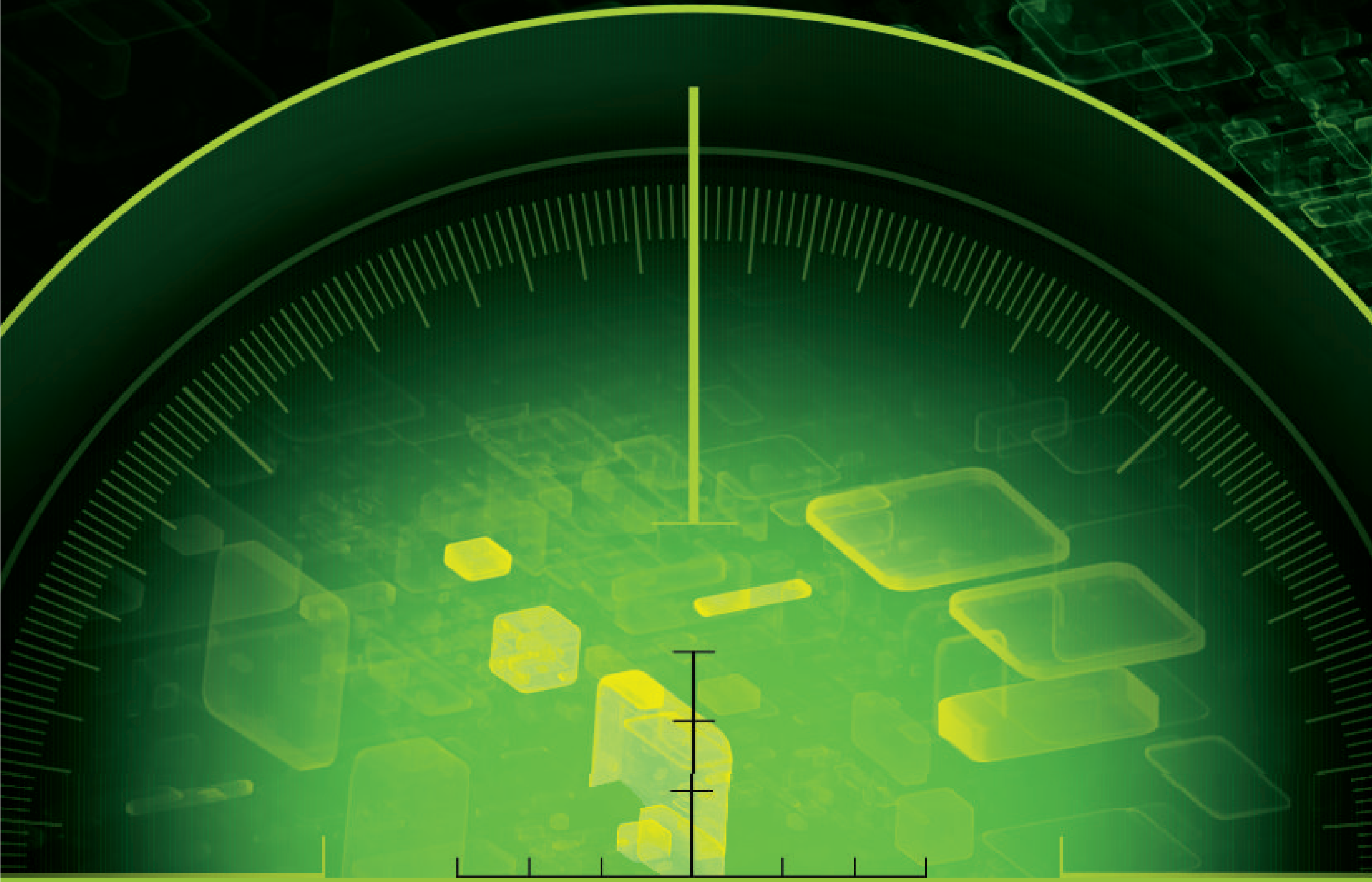
'eScan™

Anti-Virus & Content Security

# Anti-Virus
## with Cloud Security
# User Guide



www.escanav.com sales@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 agreement.

Document number: 5bug/15.01.2015/14.x

Current software version: 14.x.x

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.

| | |
|---|---|
| Technical support: | support@eScanav.com |
| Sales: | sales@eScanav.com |
| Forums: | http://forums.eScanav.com |
| EScan wiki: | http://www.eScanav.com/wiki |
| Live chat: | http://www.eScanav.com/english/livechat.asp |
| Printed by: | MicroWorld |
| Date: | 15th January, 2015 |

# Contents

# Welcome

MicroWorld's eScan 14 is a revolutionary anti-virus software and information security product that is designed to provide zero-day protection to computers from malicious software and several other security threats.

The new version of eScan is a feature-rich and user-friendly product that comes with several customizable settings. It has a trendy new design that is both intuitive and easy to understand. In addition, eScan 14 introduces a host of new features that are aimed at safeguarding your computer from new and emerging threats, such as malware, phishing web sites and e-mails, and hackers. To achieve this, eScan employs cutting-edge technologies, such as MicroWorld Winsock layer (mwl), non-intrusive learning patterns (nilp), domain ip reputation check (dirc), eScan security network (esn), and proactive malware detection.

MicroWorld is committed to provide 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 14.

Thank you for choosing eScan.

The eScan team

# About this guide

In the past few years, there has been a sudden increase in the number of it related crimes. Almost every other day, one gets to hear reports of hackers stealing trade secrets or viruses bringing down entire networks. Because of this, organizations are turning to anti-virus and content security solutions for keeping their data safe from security threats.

This guide provides you detailed information on eScan anti-virus (av) version 14.x. It provides you information on how to prepare for installation, procedure of installation, familiarizes you with the trendy user interface, features, and so on.

Contents

## Intended audience

This document is intended for system administrators, customers, and users. It aims at helping them use the product efficiently and effectively.

## Conventions used

The following typographical conventions are used in this document.

| Convention | Description |
|---|---|
| ✍ Note | It indicates the special instructions, which can be useful in addition to the current information. |
| Bold | It indicates name of the user interface like options, buttons, links, windows, dialog boxes, and so on. |
| Hypertext blue | It indicates link to a topic or to a website. |
| [default] | It indicates the default settings. |

# Pre-installation process

This section provides you information on how to configure a test environment for using eScan. Please make sure that your system meets the following pre-requisites and system requirements before installing eScan.

Contents

## Pre-requisites for installing eScan

Before installing eScan, please ensure that you perform the following tasks.

- For first-time installation
    - Ensure that you have administrator rights or equivalent privileges for the user logged on to the computer.
    - Close all the open applications or programs.
    - Uninstall all other anti-virus or anti-spyware software.
    - Disable or uninstall windows® defender.
    - Disable or uninstall any existing firewall software, including windows® firewall.
    - Determine the largest free drive or partition and then install eScan on it.
    - Additional tasks:
        - Recommended: MicroWorld recommends that the computer on which eScan is being installed is connected to the internet during the installation process. This will ensure that eScan downloads all the latest updates from eScan update servers.
        - Optional: ensure that you know the ip address of the mail server to which eScan should send warning messages. If authentication for the mail server is mandatory for accepting e-mails, you will need authentication user name and password to send e-mails.
        - Optional: ensure that the critical operating system and security patches are installed on the computer.

- For renewal or upgrade installation
    - You should perform the same set of tasks that were performed while installing eScan for the first time. Then, you can upgrade to the newer version without uninstalling the existing version.

- For reinstalling after uninstalling the existing version
  - If you have uninstalled an existing version of eScan, you must restart the computer before you can reinstall it.

## System requirements

Your computer must meet the following minimum system requirements.

- **Operating system**

  Windows® 10 / 8.1 / 8 / 7 / vista® /xp service pack 2 or higher / 2000 professional [all 32-bit & 64-bit editions]

- **CPU:** 1 Ghz recommended
- **Disk space:** 1 GB
- **Memory:** 1 GB recommended
- **Version:** 14.x – Multilingual

# Understanding the User Interface

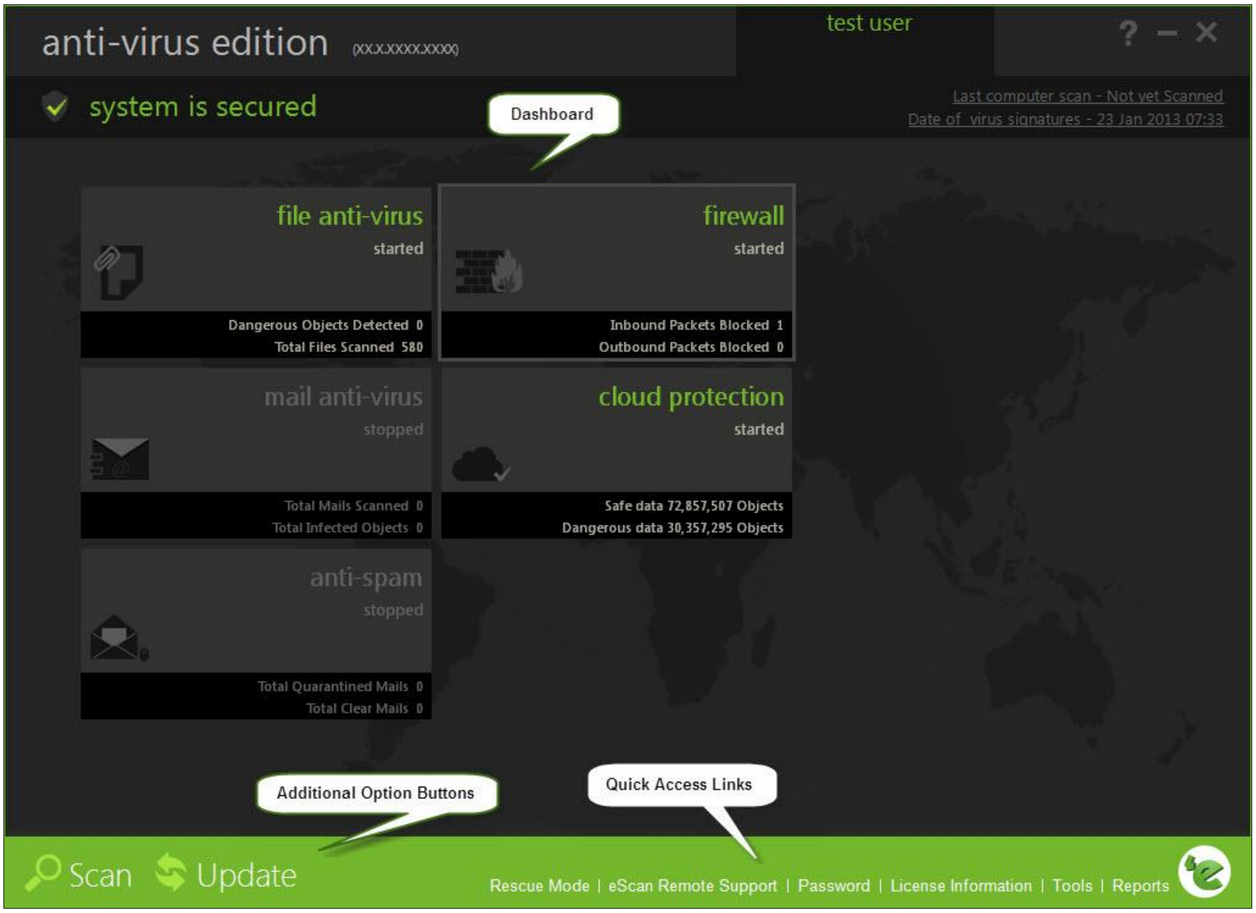
This section introduces you an overview of eScan for av user interface.

Contents

## Graphical User Interface (GUI)

eScan for AV is the main application window of eScan. It has a new GUI that is pleasantly straightforward and is designed to suit the needs of both novice and expert users. It provides you an option to switch back and forth between languages on your application, wherein you can choose the language of your choice, by using the keyboard. If you want to switch from language to English press shift + f12 and if you want to switch from language to native press shift + f5.

The main window is the dashboard. Dashboard is a special page that summarizes information on the modules. It contains product name, version number, real-time protection status (as √ system is secured in green color or x system is not secured in red color), date of last computer scanned, date of virus signatures, modules displaying the status information, additional option buttons, and quick access links.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ×
system is secured
Last computer scan - Not yet Scanned
Date of virus signatures - 23 Jan 2013 07:33
file anti-virus
started
Dangerous Objects Detected 0
Total Files Scanned 580
firewall
started
Inbound Packets Blocked 1
Outbound Packets Blocked 0
mail anti-virus
stopped
Total Mails Scanned 0
Total Infected Objects 0
cloud protection
started
Safe data 72,857,507 Objects
Dangerous data 30,357,295 Objects
anti-spam
stopped
Total Quarantined Mails 0
Total Clear Mails 0
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Dashboard

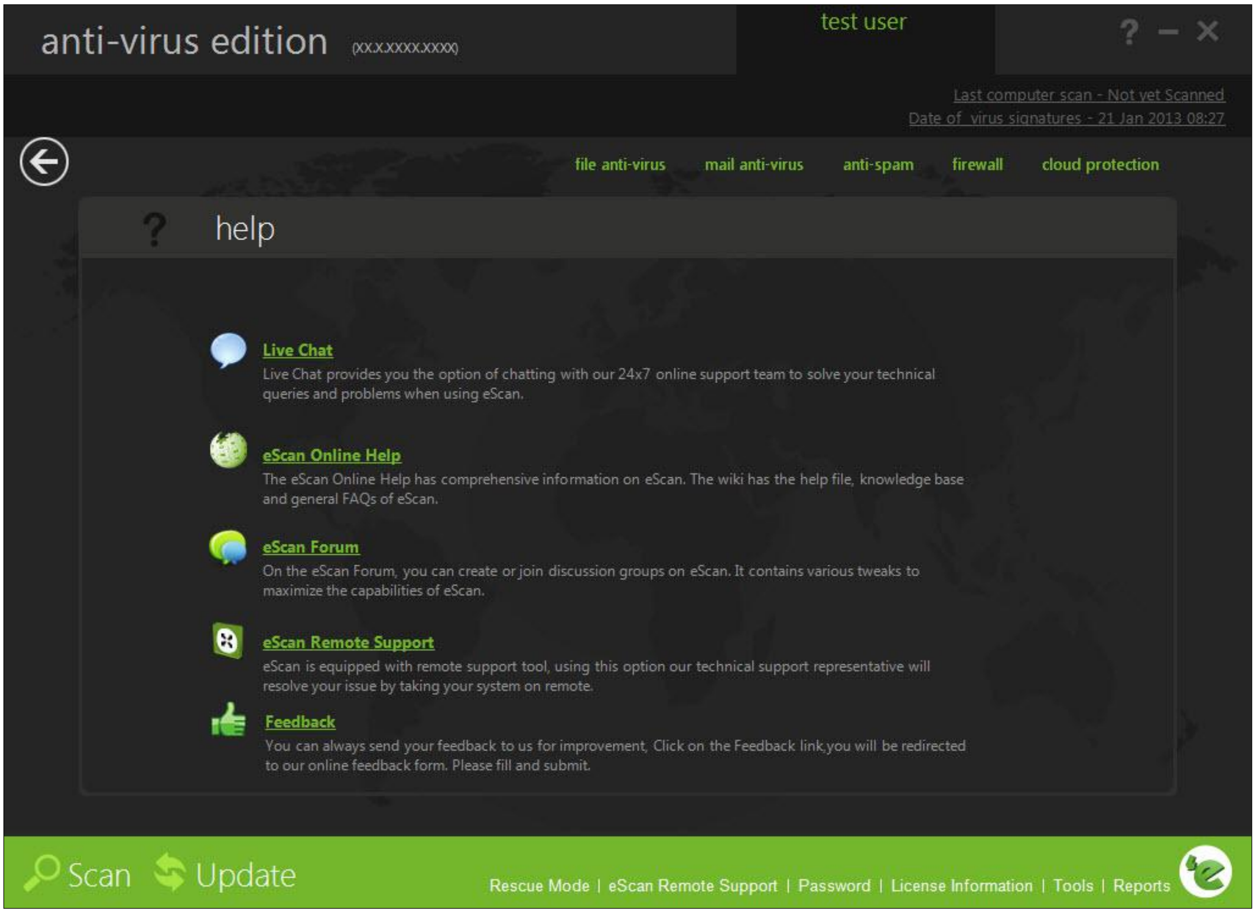
Additional Option Buttons

Quick Access Links

**Figure 1**

On upper-left corner of the screen, you can view message as "√ system is secured" in green color, only if the file anti-virus (real-time protection) is in start mode and if file anti-virus (real-time protection) is in stop mode, the "x system is not secured" message is displayed in red color.

On upper-right corner of the screen, you can view the name of the user, help button, minimize button and close button. When you click help button, the following window appears.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ×
Last computer scan - Not yet Scanned
Date of virus signatures - 21 Jan 2013 08:27
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
help
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Live Chat
Live Chat provides you the option of chatting with our 24x7 online support team to solve your technical queries and problems when using eScan.

eScan Online Help
The eScan Online Help has comprehensive information on eScan. The wiki has the help file, knowledge base and general FAQs of eScan.

eScan Forum
On the eScan Forum, you can create or join discussion groups on eScan. It contains various tweaks to maximize the capabilities of eScan.

eScan Remote Support
eScan is equipped with remote support tool, using this option our technical support representative will resolve your issue by taking your system on remote.

Feedback
You can always send your feedback to us for improvement, Click on the Feedback link,you will be redirected to our online feedback form. Please fill and submit.

**Figure 2**

- Help: click this button, to access live chat, eScan online help, MicroWorld forum, eScan remote support, and feedback.
  - Live chat: you need to have internet connection, to access this feature. You can contact eScan 24 x 7 online technical support team through chat either by clicking the live chat button or by visiting the following link.

    Http://www.eScanav.com/english/livechat.asp
  - EScan online help: you need to have internet connection, to access this feature. EScan online help is located on the eScan wiki. It provides you with comprehensive information about products and features of eScan.

    You can visit eScan online help pages either by clicking the eScan online help button or by visiting the following link.

    Http://www.eScanav.com/wiki

    eScan for AV also provides you context-sensitive help, where you can find information on any specific feature while accessing the eScan for av application you can press f1 button, then the relevant page is displayed.

- EScan forums: you need to have internet connection, to access this feature. You can click this button to join the eScan forum and read the discussion threads on eScan.
- EScan remote support: click this link, if you want to access the eScan remote support for troubleshooting queries or product assistance through remote connection.
- Feedback: click this option to visit the eScan web site, where you can provide your feedback on various eScan products and send it to the eScan's quality assurance team.

On upper-right corner of the screen, you can view the date, month, year, and time of when the last computer is scanned in the dd/mm/yyyy min: sec format.

It also displays the date, month, year, and time of when the latest virus signatures are updated in the dd/mm/yyyy min: sec format.

## Modules

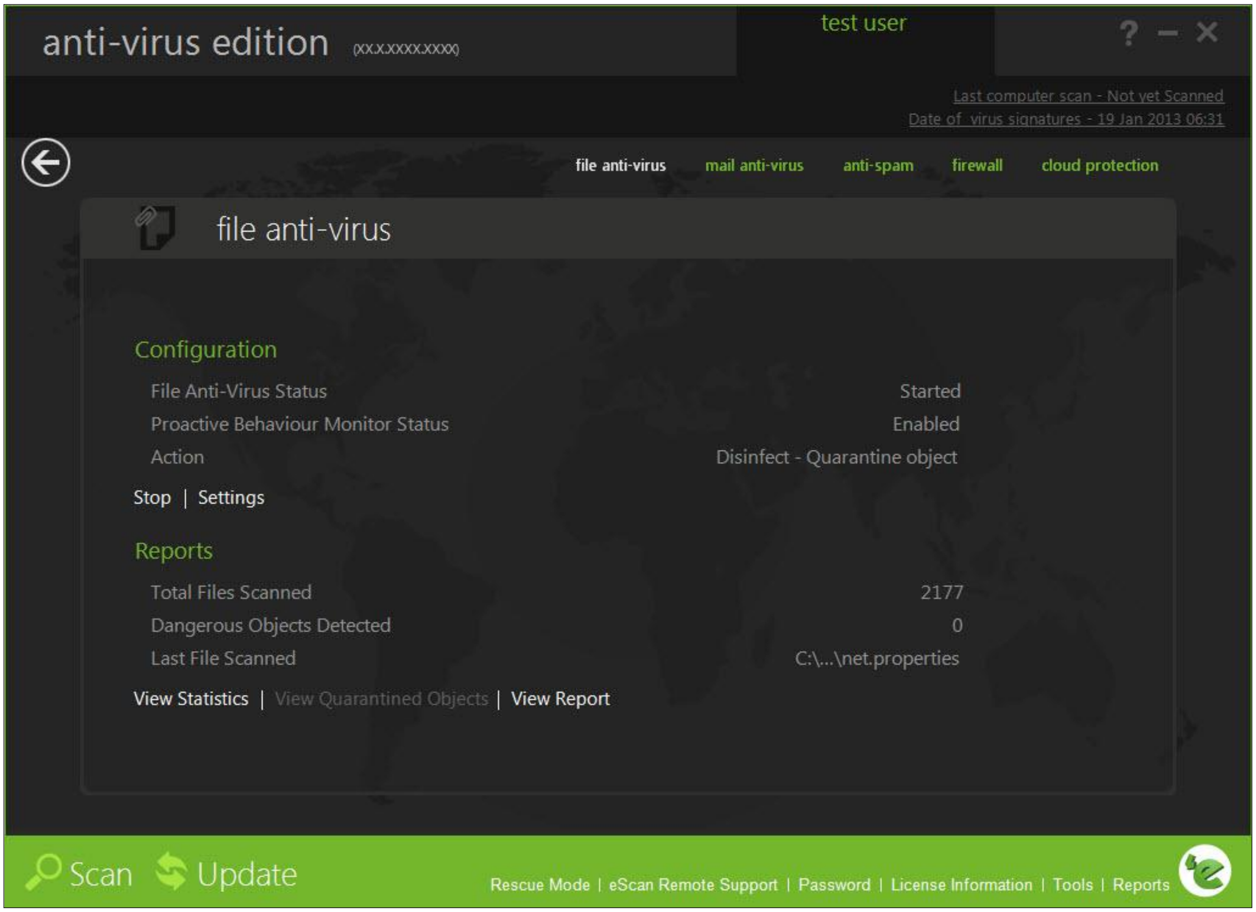
EScan for av provides you access to the following five modules:

- File anti-virus: this module provides real-time protection to the files and folders existing on your computer.
- Mail anti-virus: this module prevents infected e-mails and attachments from reaching your inbox, and thus protects your computer from malicious programs that propagate through e-mails.
- Anti-spam: this module helps you create and configure filters that filter spam based on keywords and phrases that appear within e-mails.
- Firewall: this module helps you apply various expert rules for blocking specific ports, programs, or services on your computer.
- Cloud protection: this module helps you connect to all the eScan users around the world. The eScan security network (esn) technology monitors, identifies, and blocks new threats with prompt response before they become widespread ensuring complete protection.

On the dashboard all the modules are displayed in sections. Each section represents the module of the eScan for av. You can click the individual section to view and access the protection status settings for the file anti-virus, mail anti-virus, anti-spam, firewall, and cloud protection modules. By default, the file anti-virus, firewall, and cloud protection modules are only enabled.

The names of the modules are highlighted in green color whose protection is in start mode and those modules whose protection is in stop mode are highlighted in grey color.

Whichever module you want to view and access, just click that particular section from the dashboard. For example, on the dashboard if you click file anti-virus section, the file anti-virus screen appears. If you want to go back to the previous screen, click the back ⬅ icon on left-corner of the menu bar.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - Not yet Scanned
Date of virus signatures - 19 Jan 2013 06:31
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
file anti-virus
Stop | Settings
View Statistics | View Quarantined Objects | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

| | |
|---|---|
| File Anti-Virus Status | Started |
| Proactive Behaviour Monitor Status | Enabled |
| Action | Disinfect - Quarantine object |

Reports

| | |
|---|---|
| Total Files Scanned | 2177 |
| Dangerous Objects Detected | 0 |
| Last File Scanned | C:\...\net.properties |

**Figure 3**

When you click any of the particular section, a separate screen is displayed with all the modules in the form of a tab. On the tabbed page, each module tab screen displays information regarding the selected module. The screen is divided into two sections — configuration and reports. These two sections are available only for file anti-virus, mail anti-virus, anti-spam, firewall modules and update option button.

- Configuration: this is the first section displayed on the tabbed page of each module. This section displays the status of the module, based on the settings that you configure with the help of the available buttons. The buttons are different for all the modules.
- Reports: this section helps you view the reports generated by the corresponding module.

## Additional option buttons

On lower-left corner of the screen, you can view the two additional option buttons — scan and update, which helps you to configure settings for scanning and updates.

**Figure 4**

- Scan: click this button, to access scan features, configure scheduled scans, or to run on-demand scans.
- Update: click this button to configure daily updates. However, to download the latest updates, your computer needs to be connected to the internet.

## Quick access links

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

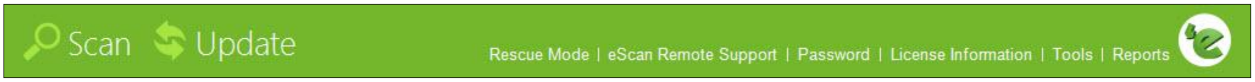

Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

**Figure 5**

- Rescue mode: click this link, if you want to run the system in rescue mode. It is specifically designed to scan and clean your 32 and 64 bit operating systems, which have been infected. This mode is used when the infection is in memory or not able to remove by anti-virus or malware removal tools. Rescue mode does not need any usb or cd/dvd.

  In rescue mode malware does not get loaded in memory, it can also update its database, if system is using internet. It reverts damage done by malwares like task manager, registry editor is disabled.
- EScan remote support: click this link, if you want to access the eScan remote support for troubleshooting queries or product assistance through remote connection. This feature helps you request the assistance of an eScan technical support representative through a remote connection to your computer. It allows the eScan technical support representative to remotely take control and troubleshoot the eScan-related issues on your computer.

  For more information, refer http://wiki.eScanav.com/wiki/index.php/remote_support link.
- Password: click this link, if you want to change the administrator password for eScan for av.
- License information: click this link, if you want to register and activate the license key.
- Tools: click this link, if you want to access the eScan for av tools, such as create eScan rescue iso image file, download latest hotfix (eScan), safe mode protection, download latest hotfix (microsoft windows os), send debug information, restore windows default settings, upload samples, and usb vaccination.
- Reports: click this link, if you want to generate and view reports of file anti-virus, mail anti-virus, anti-spam, firewall, and eScan cloud modules.

# Accessing tools

The tools link is located on lower-right corner of the screen. It provides various options, which helps you to quickly access the tools at ease.

Each tool contains certain activities to perform, which are explained below.

## Creating eScan rescue iso image file

Click this button to open the eScan rescue file creation wizard, which helps you to create a windows®-based rescue disk file. The rescue disk file helps you create a clean bootable cd to provide you a clean boot on infected computers running the windows® operating system. You can then eradicate rootkits and file infectors that cannot be cleaned in the normal windows® mode.

Once the eScan rescue disk is downloaded, you can now also update it using this wizard.

For more information on how to create the eScan rescue disk file, visit the following link.

Http://download1.mwti.net/download/wikifiles/eScan_rescue_disk.pdf

## Downloading latest eScan hotfix

You need to have internet connection, to access this feature. When you click this button, eScan opens the MicroWorld download manager and starts downloading the latest hotfix from eScan update servers.

## Running safe mode protection

EScan safe mode protection is available if you have Microsoft windows workstation operating system installed on your computer.

It allows you to password protect Microsoft windows safe mode booting option, as to restrict the user to boot in to safe mode directly. The operating system becomes vulnerable in safe mode as in safe mode many of the drivers are not loaded and also the essential security features like firewall, anti-virus real time protection, and so on may not work correctly.

## Downloading latest Microsoft windows OS hotfix

When you click this button, eScan opens the MicroWorld download manager and starts downloading the latest critical hotfix for the windows® operating system from the Microsoft® web site.

## Sending debug information

Click this button to open the please type your problem here! Dialog box. It allows you to specify the eScan-related problem and generate the debuges.zip file. The debuges.zip file is a special file that contains critical eScan files and settings. It is stored in the program files\eScan\debug folder. You can send the problem description along with the debuges.zip file to eScan's technical support team, so that they can analyze it and assist you in resolving the problem.

To send the description of the problem, you need to specify the following information in appropriate fields.

- Mail from: [default: eScanuser@eScanav.com] type e-mail address of the sender.
- Mail to: [default: support@eScanav.com] type e-mail address of the recipient. The recipient of this e-mail is usually the eScan's technical support team.
- Smtp server: [default: mail.mwti.net] type ip address of the smtp server.
- Smtp port: [default: 25] type port number of the smtp port.
- User authentication (opt.): type the user name, however adding this information is optional.
- Authentication password (opt.): type the password, however adding this information is optional.

Click the ok button to send an e-mail along with the debuges.zip file to eScan's technical support team.

## Restoring 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.

## Uploading samples

This feature helps you to submit the virus samples to the eScan support team. Click the upload samples link, if you want to upload the virus samples. When you click this link, a new web page opens, where you have to click the samples option, click the next >> button, fill up the details in the submit a ticket form, and then click submit button.

## Vaccinating usb devices

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 case, eScan 14 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.

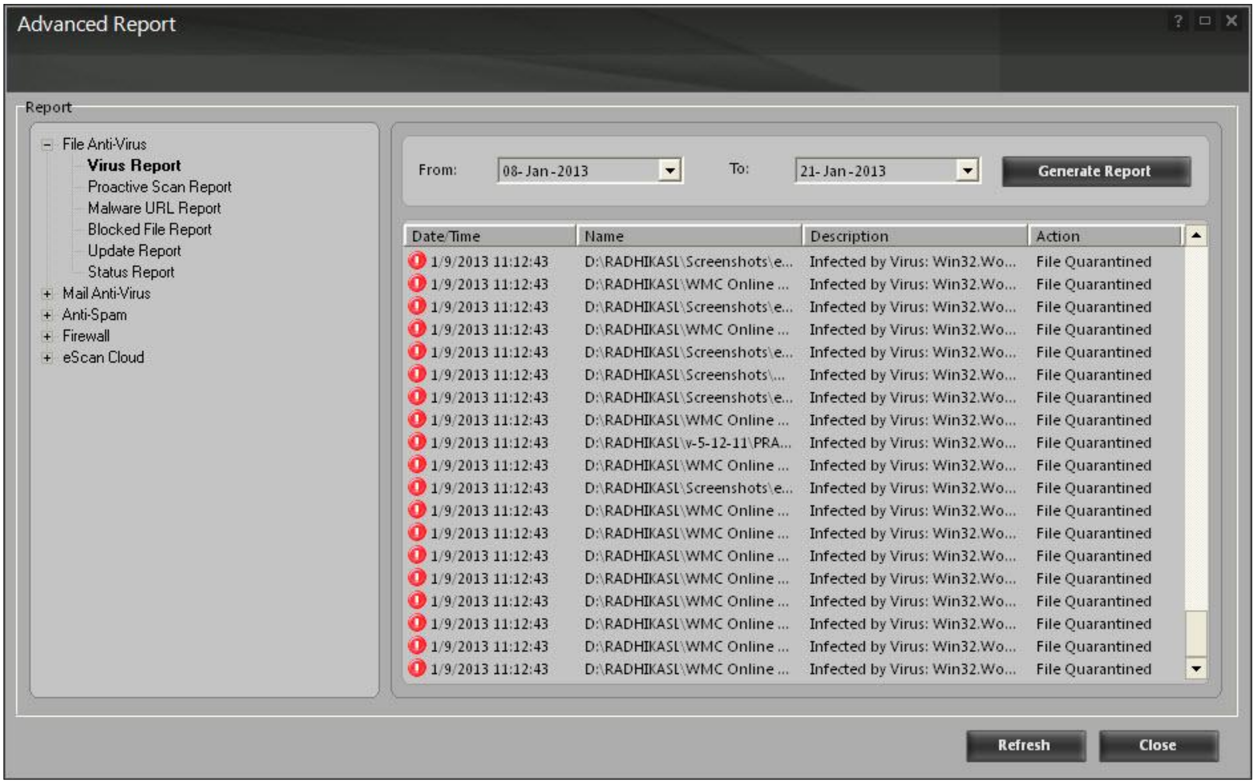
To vaccinate, select an appropriate usb drive, which you want to vaccinate from the choose a usb drive drop-down list, and click the vaccinate button.

# Generating and viewing reports

The eScan helps you generate reports for file anti-virus, mail anti-virus, anti-spam, firewall, and eScan cloud modules.

The advanced report window is displayed showing the list of reports on the left pane. You can view name of the reports under each module. To generate and view the report, click an appropriate report.

You can generate the report based on the dates specified. You can select the from date and till date for which you want to generate the report. To generate report date-wise select an appropriate date from the from: field from which date you want to view and to: date till which you want to view, by clicking the drop-down icon and then select the date. After selecting the date, click the generate report button to view the report.



From: 08-Jan-2013 To: 21-Jan-2013

| Date/Time | Name | Description | Action |
|---|---|---|---|
| 1/9/2013 11:12:43 | D:\RADHIKASL\Screenshots\e... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\Screenshots\e... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\Screenshots\e... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\Screenshots\... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\Screenshots\e... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\v-5-12-11\PRA... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\Screenshots\e... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |
| 1/9/2013 11:12:43 | D:\RADHIKASL\WMC Online ... | Infected by Virus: Win32.Wo... | File Quarantined |

**Figure 6**

# Overview of eScan features

EScan epitomizes the next generation of anti-virus software products that handle security threats from a new dimension without compromising the performance of your computer. It uses powerful technologies, such as the MicroWorld winsock layer (mwl) technology, domain and ip reputation checker (dirc) technology, non-intrusive learning pattern (nilp) technology, eScan security network (esn), proactive malware detection, and sophisticated heuristics algorithms to detect and clean malware. In addition, it includes a comprehensive set of powerful management tools, such as the eScan management console (emc) and eScan protection center (epc). These tools help you configure eScan to safeguard your data and computers based on your requirements.

Contents

## New features in eScan 14

EScan 14 includes several improvements over its predecessor in terms of its user interface, performance, resource utilization, and data protection features. These new features are described as follows:

- New trendy gui

  EScan 14 has a trendy new gui that is extremely simple and easy to use. It is elegant in terms of its design and is well suited to the needs of both expert and novice users. The new gui is extremely light on system resources and requires very less memory space to run efficiently. It thus provides you with a secured and pleasant computing experience without compromising on the performance of the computer.

- EScan security network (esn)

  The cloud-based eScan security network collects information from millions of eScan participant user's computers around the world when they are online, to safeguard your digital world from latest and unknown threats. It provides fast response to the latest virus threats without waiting for daily or traditional virus signature updates.

- Proactive malware detection

  With new proactive malware detection technology and highly sophisticated heuristics algorithms, eScan effectively scans and detects unknown malware that are continuously released by malware writers. It also detects and warns you about applications that behave in a suspicious manner, thus providing protection from zero-day threats.

- Usb vaccination

  This feature helps you timely vaccine the usb devices, by preventing them from becoming a source of infection.

- Rescue mode (without using usb/cd media)

  EScan 14 allows you to boot your system without the need of any usb or cd rom device.

- Switch languages on the fly

  EScan 14 allows you to switch back and forth between languages on your application, wherein you can choose the language of your choice. You can use the combination of these keys - shift + f12 / shift + f5.

# Installation process

This section provides you an overview of the eScan product installation.

Contents

## Overview of eScan product installation cd

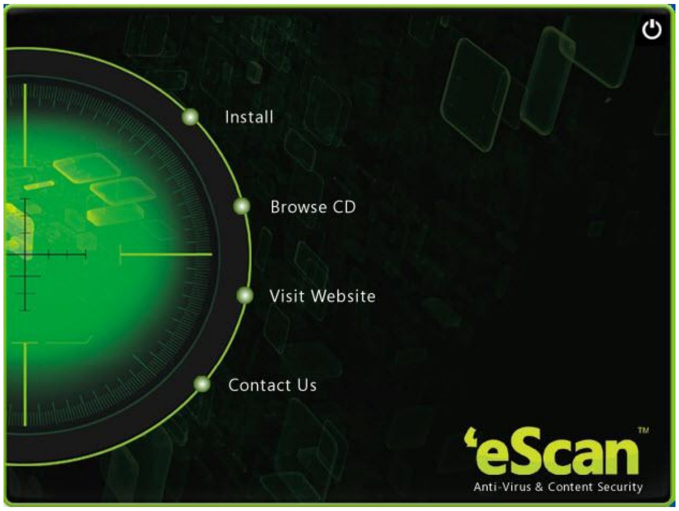


**Figure 7**

The eScan product installation cd comes with a set of installation setup files and a bootable rescue disk. You can use the bootable rescue disk to boot your computer, if the operating system cannot be loaded.

The rescue disk also includes the eScan anti-virus toolkit (formerly mwav), which runs automatically when you boot the computer using the disk. It helps you scan the computer's memory, system folders and some registry values. In addition, it helps you run the command.exe file and execute commands for formatting the hard disk, partitioning any drive, or checking the hard disk for errors.

The eScan product installation cd contains an autorun.exe file. You can view the contents of the cd and install eScan by using this cd.

When you double-click autorun.exe, the cd menu will open, refer figure 7.

The cd's menu shows the following options.

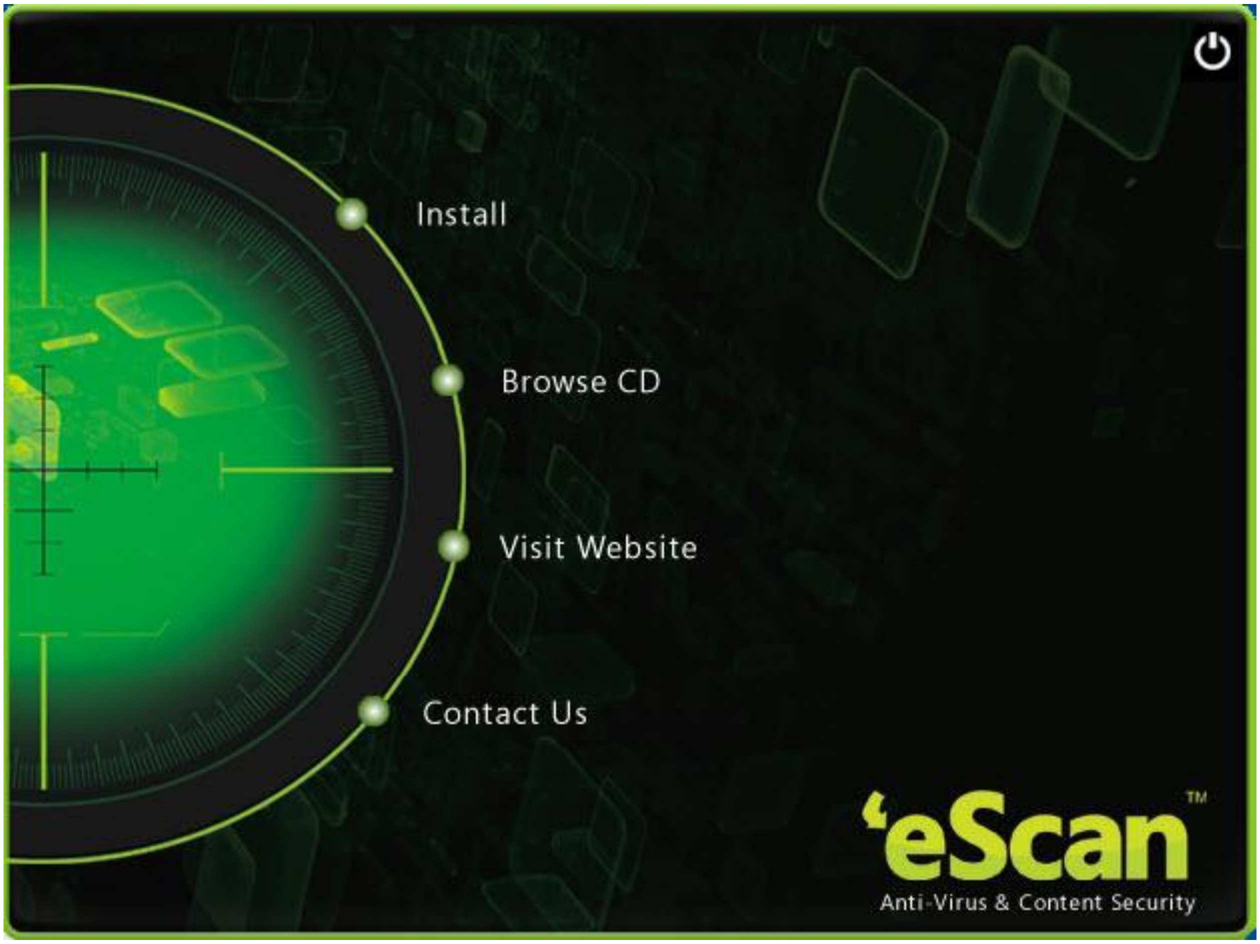


**Figure 8**

- Install: click on install to start the installation process on to your computer.
- Browse cd: you can click this button to view the contents of the cd.
- Visit eScan web site: [requires internet connectivity.] You can click this button to visit the eScan web site http://www.eScanav.com
- Contact us: you can click this button to view the contact information for MicroWorld's offices.

Additional requirements

Internet connectivity is required for a few buttons to function properly.

# Overview of the installation process

You can install eScan anti-virus (av) either by using the eScan setup file or by using the eScan product installation cd.

To download the eScan setup file, visit the following link.

Http://www.eScanav.com/downloads/soho14.asp

To begin the eScan installation, insert the eScan product installation cd into the cd-rom drive of your computer. This will start the setup automatically.

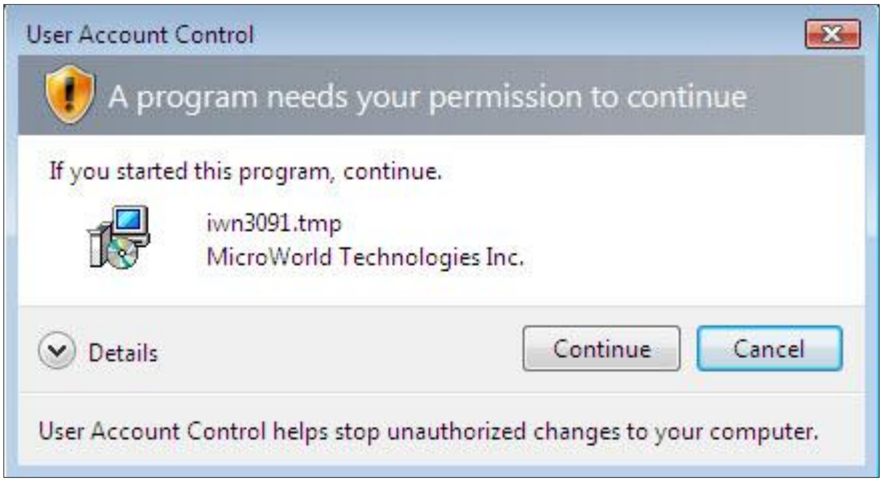
On some computers auto run of cd/dvd option is disabled. In such cases, you can manually start the installation by double-clicking the autorun.exe in the cd-rom drive window. This will display a dialog box containing options for selecting the language.

EScan uses the interactive installation wizard for its installation. This wizard has a simple and intuitive gui that guides you through the installation process.

To install eScan av on your computer

Special instructions for installing eScan av on computers running the windows vista® operating system with user access control (uac) enabled on them.

When you double-click the setup file for installing eScan av, a user access control dialog box appears asking you for permission to run awn2[xxxx].tmp file. Here, the [*xxxx*] represents the last four characters, which may be arbitrary. This is a valid eScan file. To proceed with the installation, click continue.



User Account Control

A program needs your permission to continue

If you started this program, continue.

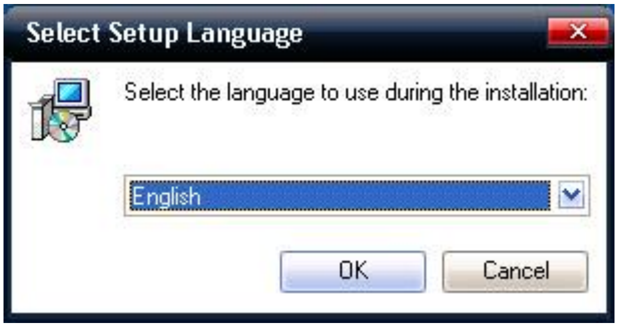
iwn3091.tmp
MicroWorld Technologies Inc.

User Account Control helps stop unauthorized changes to your computer.

**Figure 9**

## Step 1 – choosing the language

EScan for av is available in many languages, such as English, German, French, Nederland's, italiano, portuguese, spanish, Turkish, Chinese simplified, Chinese traditional, Greek, Korean, Norwegian, Russian, polish, and Latin spanish.



Select Setup Language

Select the language to use during the installation:

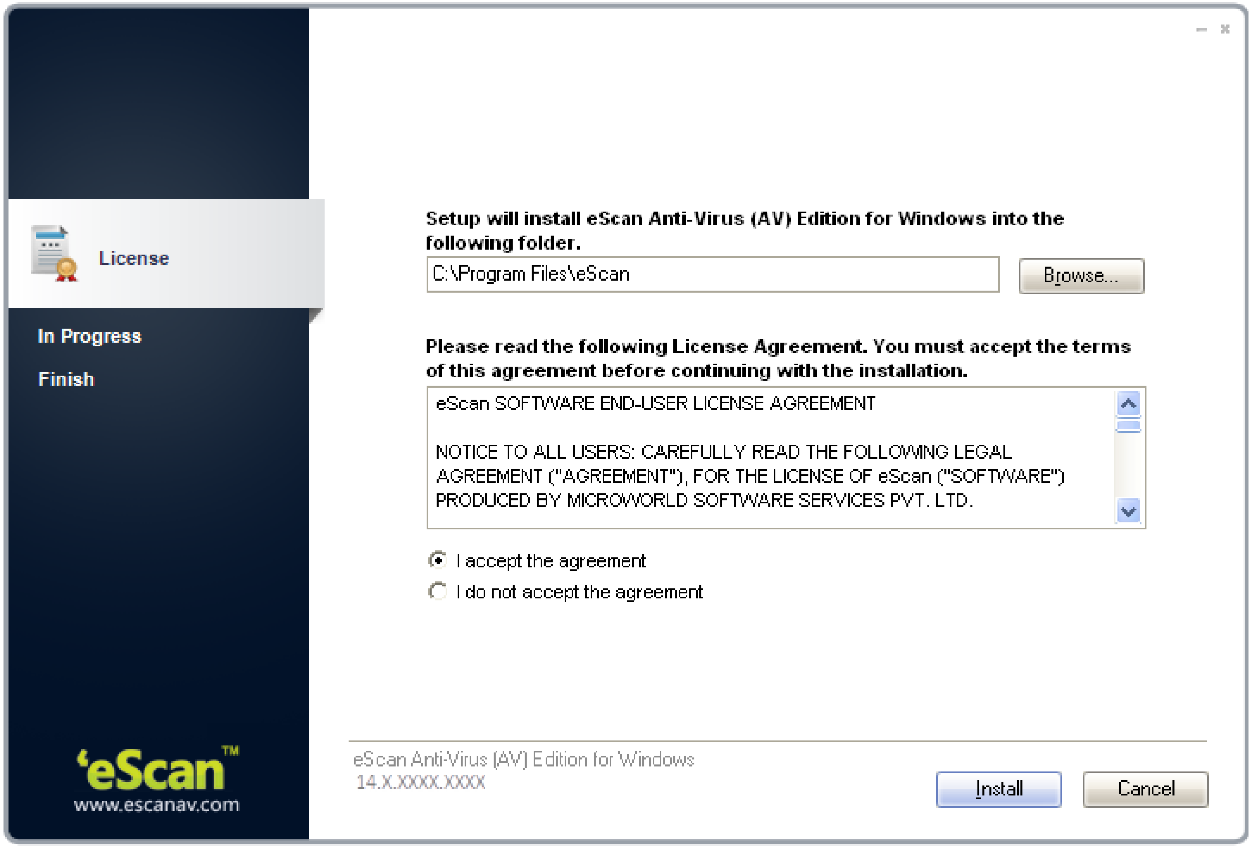
English

Figure 10

Select the preferred language from the drop-down list, and then click ok.

## Step 2 - license agreement

Type the path of the folder or click browse to browse to the folder, and then click i accept the agreement, and click install. EScan antivirus for windows installation will begin.



Setup will install eScan Anti-Virus (AV) Edition for Windows into the following folder.

C:\Program Files\eScan

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

eScan SOFTWARE END-USER LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF eScan ("SOFTWARE") PRODUCED BY MICROWORLD SOFTWARE SERVICES PVT. LTD.

● I accept the agreement

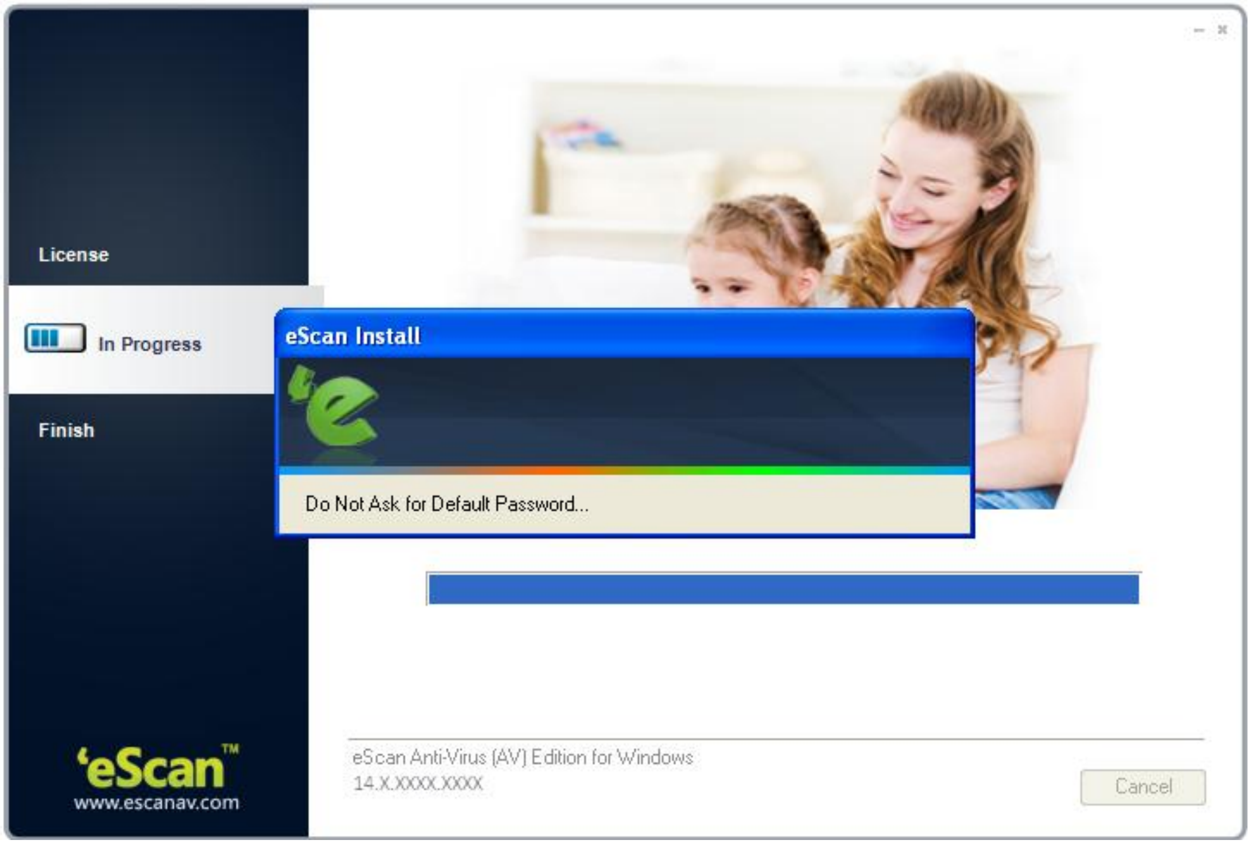
○ I do not accept the agreement

eScan Anti-Virus (AV) Edition for Windows
14.X.XXXX.XXXX

Figure 11

## Step 3 – install eScan

The eScan installation process starts; the eScan setup runs eScan anti-virus toolkit. This tool scans and removes the viruses and spyware found on your computer.



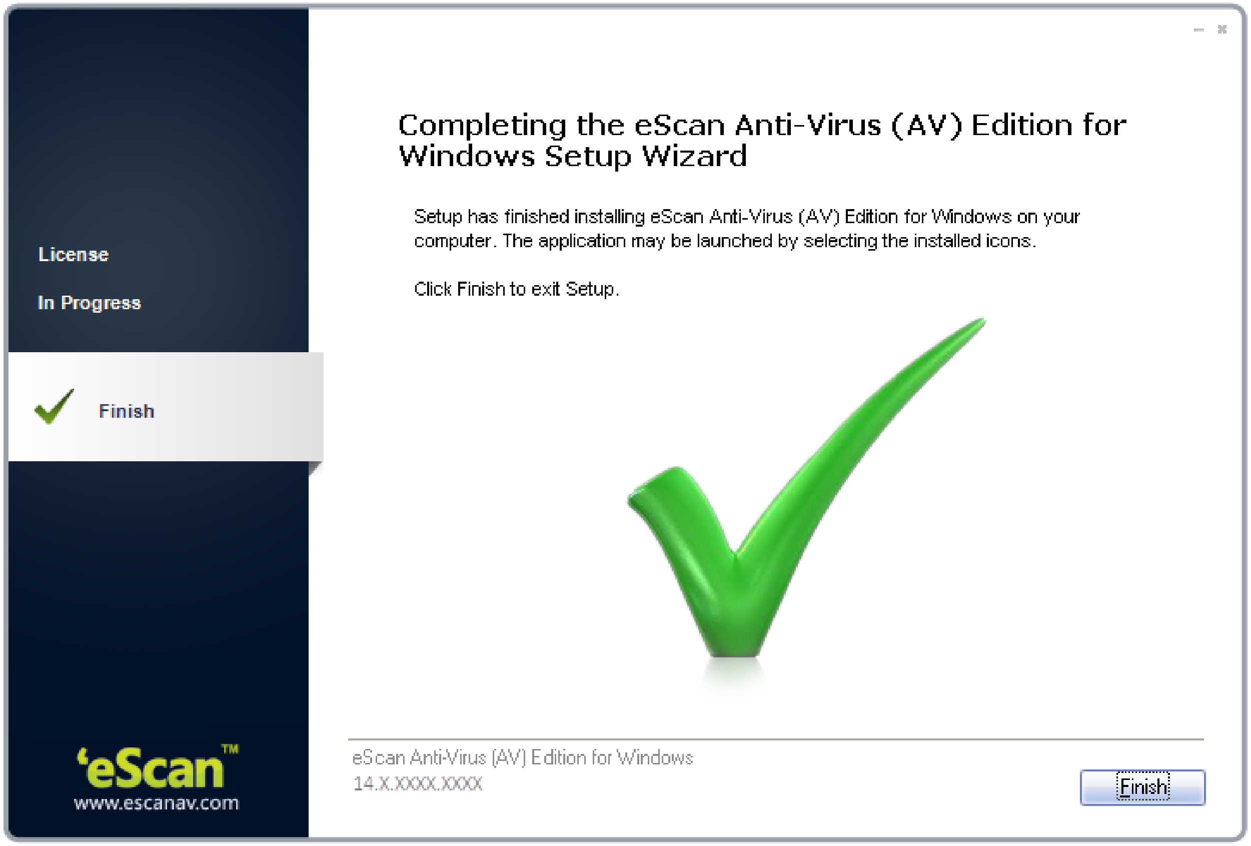
Do Not Ask for Default Password...

eScan Anti-Virus (AV) Edition for Windows
14.X.XXXX.XXXX

Figure 12

## Step 7 - completing the installation

After completing all the tasks, the eScan gets installed on your computer.



Completing the eScan Anti-Virus (AV) Edition for Windows Setup Wizard

Setup has finished installing eScan Anti-Virus (AV) Edition for Windows on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

eScan Anti-Virus (AV) Edition for Windows
14.X.XXXX.XXXX

**Figure 13**

# Verifying the eScan installation

When the installation is complete, a red shield icon appears in the system tray. The shield icon indicates the protection status of the computer. The cross mark icon indicates that the eScan's real-time protection is either paused or disabled and the red shield icon indicates that the eScan's real-time protection is active.

You can find the version of eScan installed on your computer by placing the mouse pointer on red shield icon. In addition, you can right-click the red shield icon, to view a context menu. This menu contains various options like pausing eScan's real-time protection, enabling gaming mode, scanning local computer, downloading updates, and so on.

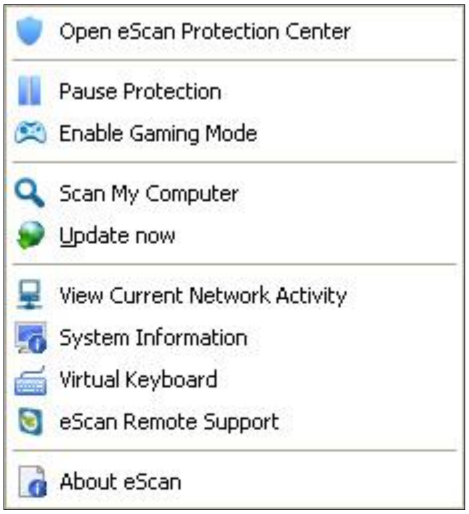


**Figure 14**

You can access eScan for av either by clicking red shield icon or by right-clicking red shield icon, and then clicking open eScan protection center option. However, before you can access this window, you need to specify the administrator password if it has been set. The default administrator password for eScan settings is admin. As a best practice, for additional security, you should change the password, after you install eScan.

The administrator password window also contains a read only button. You can click this button if you need to prevent changes or modifications from being made to the settings. This mode enables you to access eScan protection center in the restricted or read-only mode.

# Managing the license key

This section provides you information on how to add and activate the license key. The eScan anti-virus for home and small office product activation comes for 30 days trial period. You should purchase the product license key before the trial period expires, wherein you receive a license key for registration. Apart from activation, you can also renew the product for the next period, as per your requirement.

To know information on registration and renewing your eScan product, refer to know how to register your product section on this link - http://www.eScanav.com/register

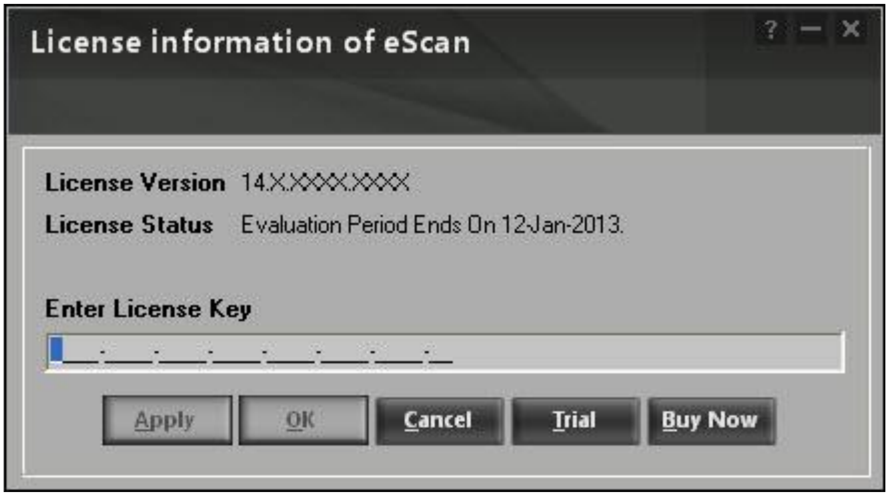
Contents

## Adding the license key

It enables you to add licenses for eScan. You can add only two licenses at a time, it is mandatory that you at least activate one license, because unless and until you activate a license you cannot add more licenses.

To add license

1. Click start, point to all programs, point to eScan for windows, and then click eScan registration. The license information of eScan window appears.



License information of eScan

License Version 14.X.XXXX.XXXX

License Status Evaluation Period Ends On 12-Jan-2013.

Enter License Key

**Figure 15**

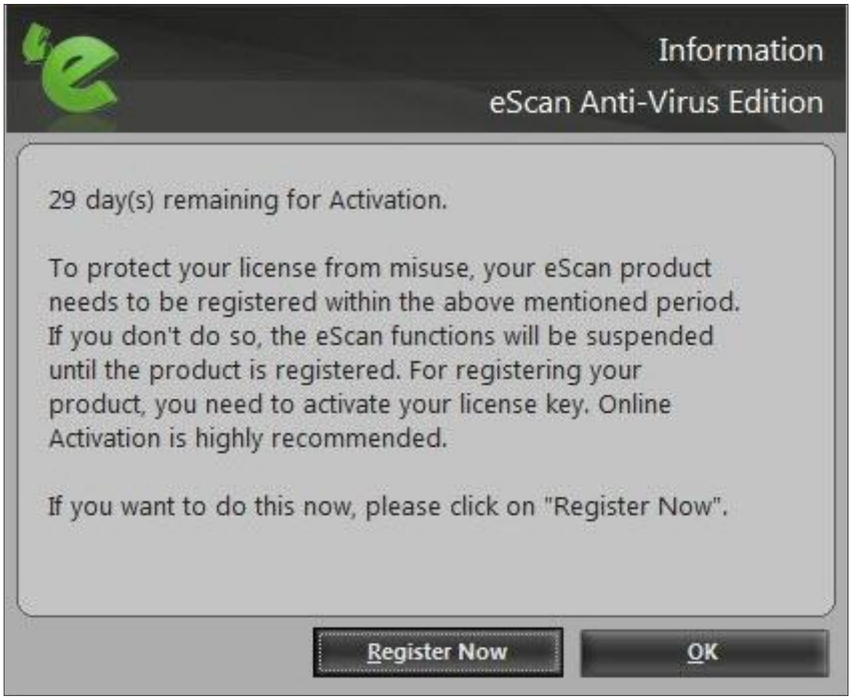
2. Type the 30-character valid license key in the enter license key field.

✍ While entering license key please ensure that there are no spaces in between the character. Abcd-efgh-abcd-efgh-abcd-efgh-abcd-ef

✍ If you type an invalid license key, a warning message appears, and

✍ 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.

3. Click the apply button, and then click the ok button.
   The information dialog box appears.



29 day(s) remaining for Activation.

To protect your license from misuse, your eScan product needs to be registered within the above mentioned period. If you don't do so, the eScan functions will be suspended until the product is registered. For registering your product, you need to activate your license key. Online Activation is highly recommended.

If you want to do this now, please click on "Register Now".

**Figure 16**

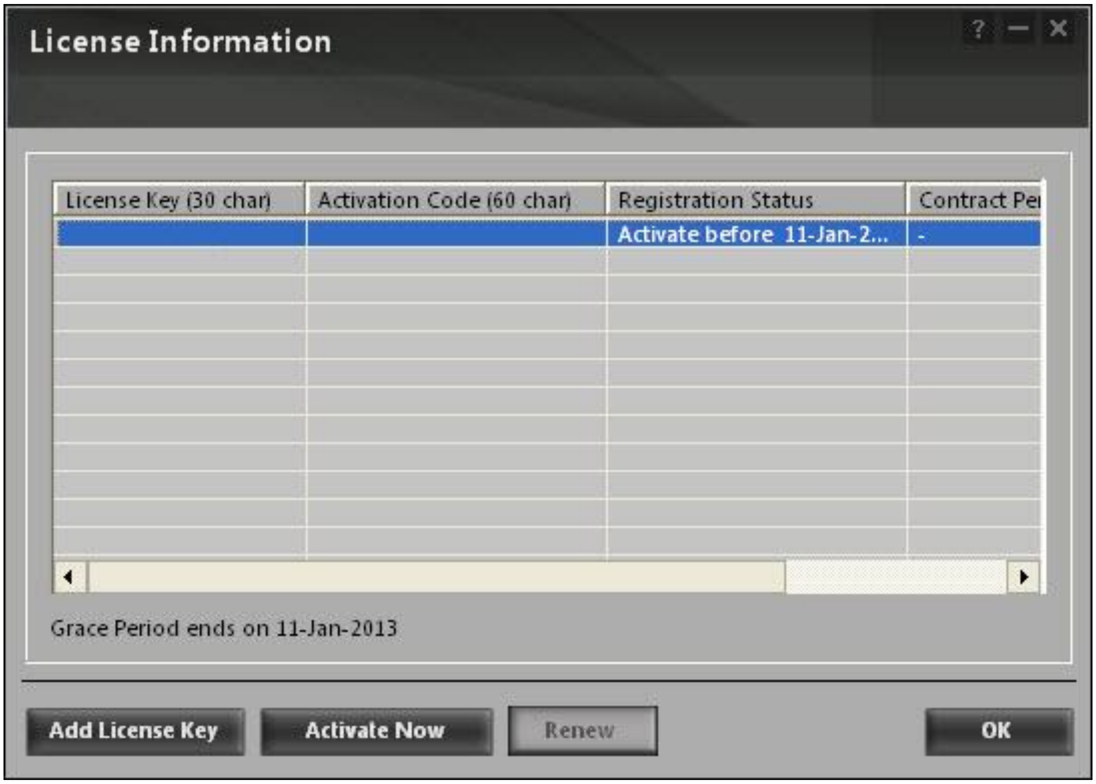
4. Click the ok button.
   The license information gets updated.

## Activating the license key

After entering a valid license key, you get an information message with an option to register now or later, for which you need to activate the license key.

To activate the license key

1. Perform the steps from 1 to 4 from the adding the license key section.
2. On the confirmation dialog box, do any one of the following: refer Figure .
   - 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.
3. When you click the register now button.
   The license information window appears.



| License Key (30 char) | Activation Code (60 char) | Registration Status | Contract Pe |
|---|---|---|---|
| | | Activate before 11-Jan-2... | - |

Grace Period ends on 11-Jan-2013

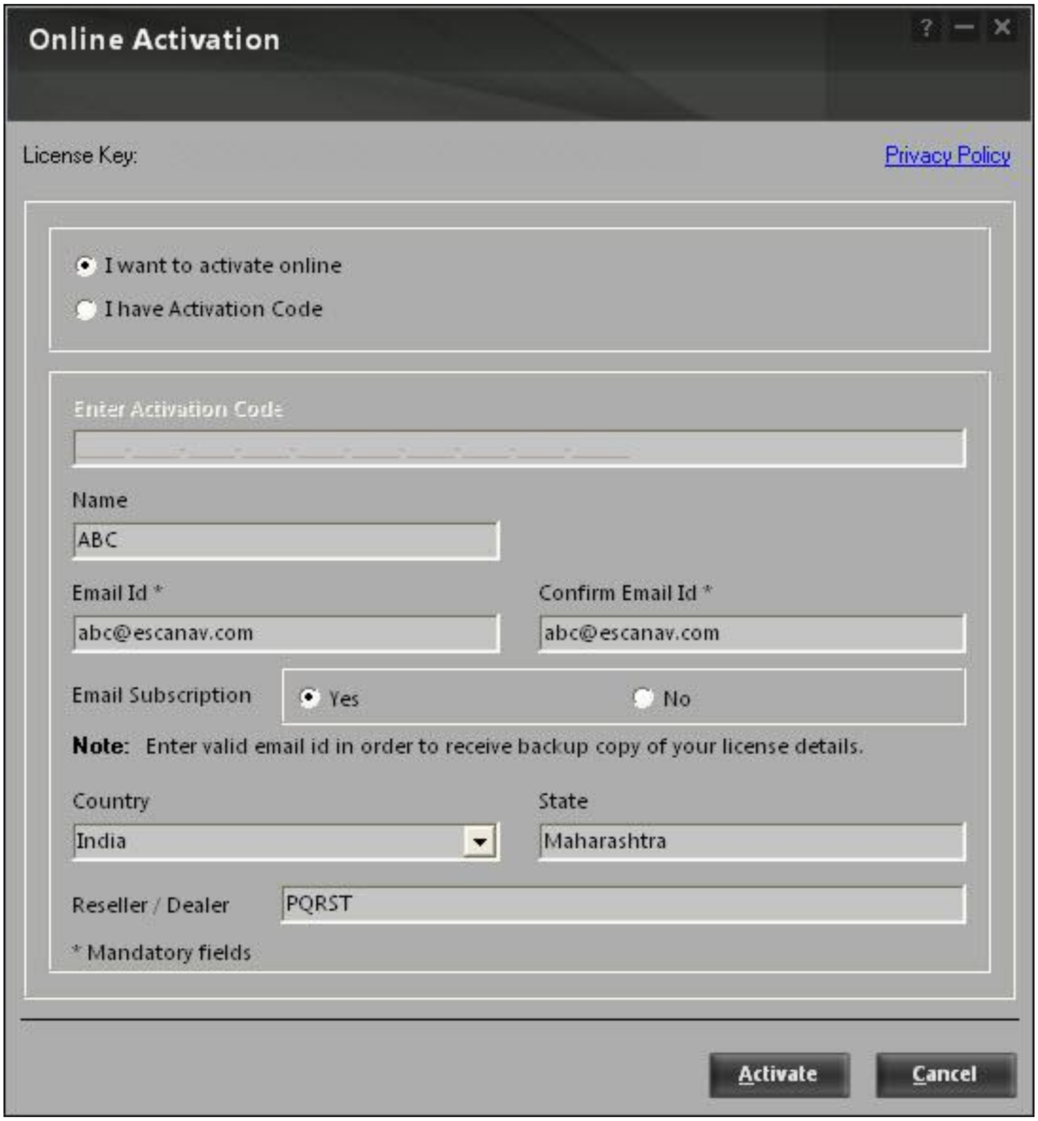
**Figure 17**

4. Click the license key from the list and then click the add license key button or activate now button as per your requirement.

   To add new license key, click the add license key button and to activate click the activate now button

Alternatively right-click the license key from the list and then click the add license key button or activate now button.

5. When you click the activate now button.
   The following window appears.



Online Activation

License Key:

Privacy Policy

● I want to activate online

○ I have Activation Code

Enter Activation Code

Name: ABC

Email Id *: abc@escanav.com

Confirm Email Id *: abc@escanav.com

Email Subscription: ● Yes ○ No

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

Country: India

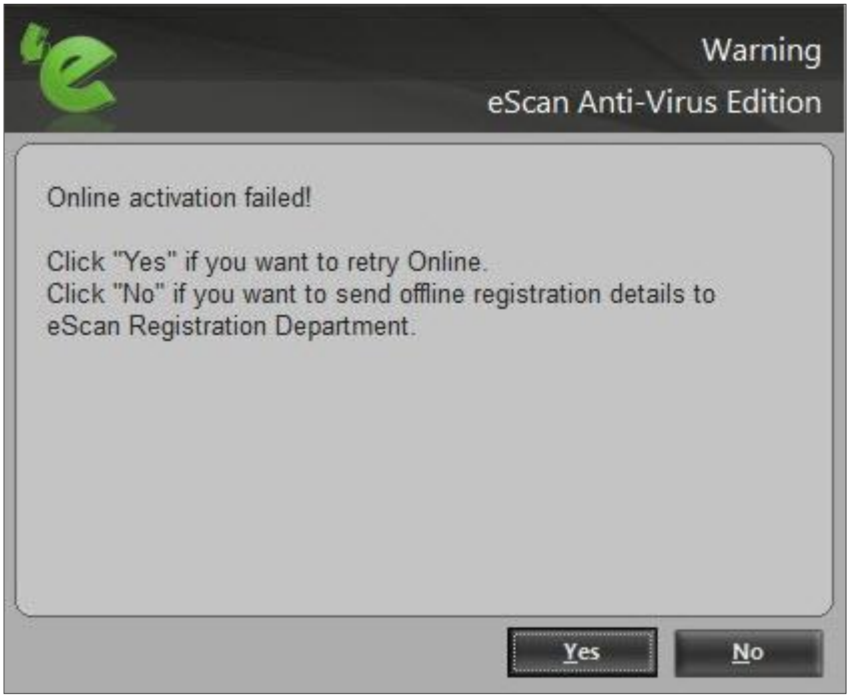
State: Maharashtra

Reseller / Dealer: PQRST

* Mandatory fields

**Figure 18**

6. Specify the following field details.

| Field | Description |
|---|---|
| I want to activate online | By default, this option is selected. When you click this option name, email id *, country, state, and reseller/dealer * fields are available.<br>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.<br><br>Warning<br>eScan Anti-Virus Edition<br>Online activation failed!<br>Click "Yes" if you want to retry Online.<br>Click "No" if you want to send offline registration details to eScan Registration Department.<br> <br> <br>**Figure 19**<br>Click the no button, an onlineregister.txt file gets generated with registration details,<br>You have to send the onlineregister.txt file to register@eScanav.com, wherein you receive an activation code to the specified e-mail id. |
| I have activation code | When you click this option only enter activation code field is available.<br>Click this option, if you already have activation code received through an e-mail from register@eScanav.com.<br>In the enter activation code field, type or copy and paste the activation code. This enables you to activate the eScan product immediately. |

| Field | Description |
|---|---|
| Enter activation code | Type the activation code. |
| Name | Type the name. |
| Email id * | Type the valid e-mail id, as you receive the backup copy of license<br>Details on the specified e-mail id. This is a mandatory field. |
| Confirm email id * | This field is available only when you type e-mail id in the email id * field.<br>Re-type the e-mail id for confirmation. This is a mandatory field. |
| Email subscription | This field is available only when you type e-mail id in the email id * field.<br>Click an appropriate option.<br>● Yes: click this option if you want to subscribe for e-mails.<br>● No: click this option if you do not want to subscribe for e-mails. |
| Country | Type the country name or select it from the drop-down list. |
| State | Type the state. |
| Reseller/dealer * | Type the reseller/dealer name. |

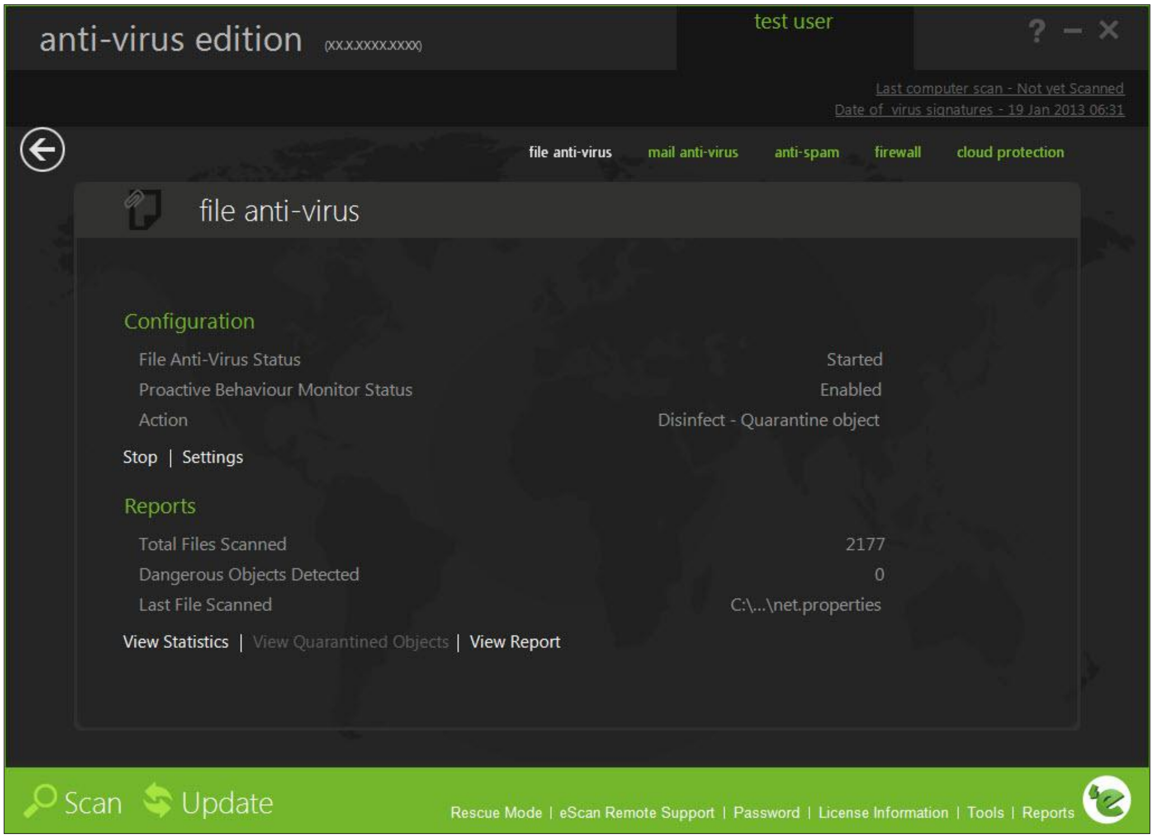
7. Click the activate button.
   The license key gets activated.

# EScan for av features

The eScan anti-virus for home and small office contains five comprehensive modules — file anti-virus, mail anti-virus, anti-spam, firewall, and cloud protection and two additional option buttons — scan and update.

## File anti-virus

File anti-virus is the first module of the eScan for av. This module monitors and safeguards your computer on a real-time basis from all kinds of malicious software as files are accessed, copied, or executed. This module includes the proactive scanning feature, which helps you block applications that perform suspicious activities. File anti-virus also includes the block files feature, which allows you to block or quarantine files from being accessed from local or network drives. In addition, file anti-virus also allows you to enable folder protection, which prevents users from creating, deleting, or updating files or sub-folders within specified folder list.



Last computer scan - Not yet Scanned
Date of virus signatures - 19 Jan 2013 06:31

Configuration

| | |
|---|---|
| File Anti-Virus Status | Started |
| Proactive Behaviour Monitor Status | Enabled |
| Action | Disinfect - Quarantine object |

Reports

| | |
|---|---|
| Total Files Scanned | 2177 |
| Dangerous Objects Detected | 0 |
| Last File Scanned | C:\...\net.properties |

**Figure 20**

This page provides you with options required to configure the module. You can configure the settings from the following 2 sections:

- Configuration

This section displays the following information.

- File anti-virus status: it displays the status of whether file anti-virus module is started or stopped.

- Proactive scan status: it displays the status of the proactive scanning.
- Action: it displays the type of action taken by file anti-virus module.

Start/stop:

Click an appropriate option to enable or disable file anti-virus module.

Settings:

When you click this button, the file anti-virus settings window appears. On the file anti-virus settings window, you have four tabs – objects, options, block files, and folder protection, which are as follows:

✍ On below the screen of all the tabs contains four buttons — default, ok, cancel, and apply, which you have to use after configuring the settings based on your requirement.

Default: click this button to apply the default settings.

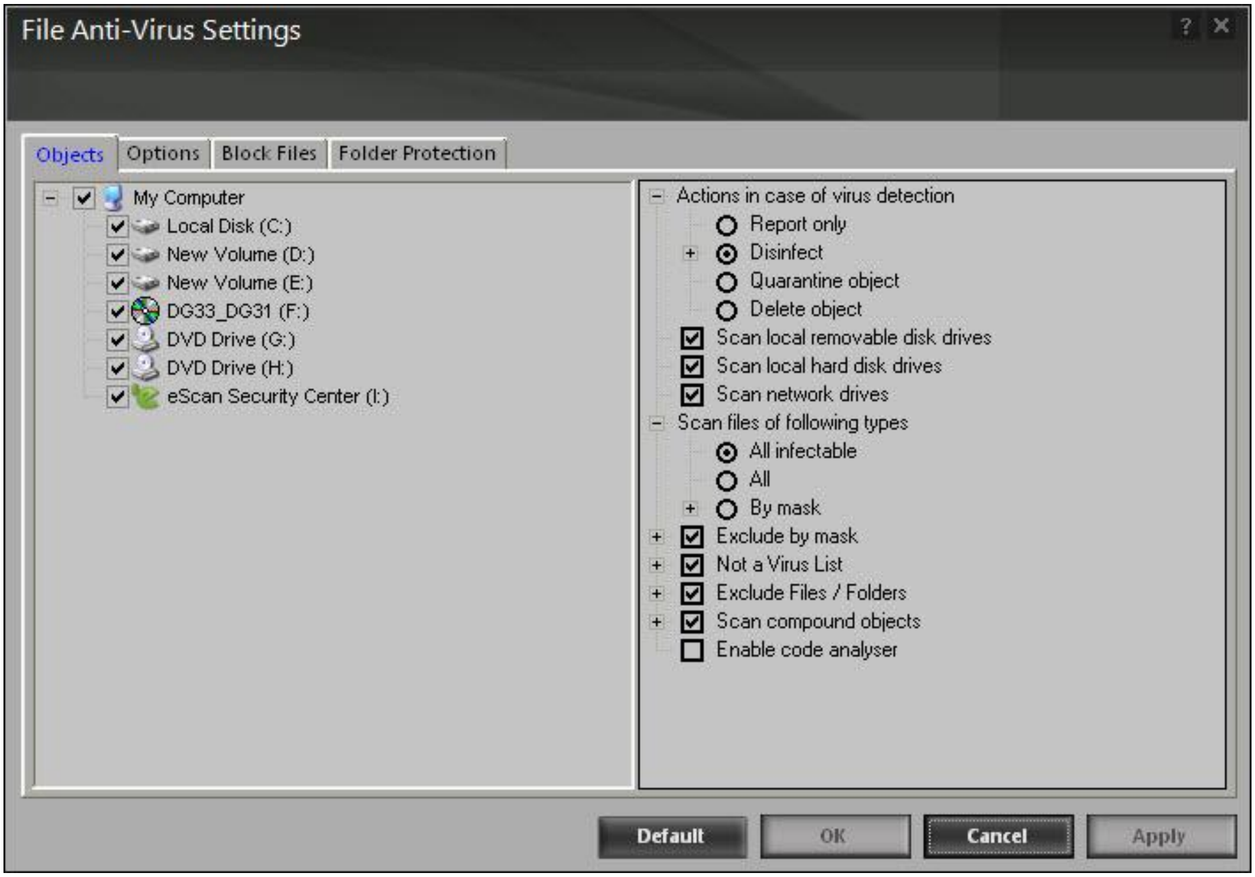
Ok: click this button after you click the apply button to apply the configured settings.

Cancel: click this button to cancel the configured settings or to close the window.

Apply: click this button to apply the configured settings.

- ### Objects

  This tab provides you with a number of settings for fine-tuning the file anti-virus module as per your requirement. For example, you can configure module to scan specific storage devices or exclude files of a given file type.



- ☑ My Computer
  - ☑ Local Disk (C:)
  - ☑ New Volume (D:)
  - ☑ New Volume (E:)
  - ☑ DG33_DG31 (F:)
  - ☑ DVD Drive (G:)
  - ☑ DVD Drive (H:)
  - ☑ eScan Security Center (I:)

- Actions in case of virus detection
  - ○ Report only
  - ● Disinfect
  - ○ Quarantine object
  - ○ Delete object
- ☑ Scan local removable disk drives
- ☑ Scan local hard disk drives
- ☑ Scan network drives
- Scan files of following types
  - ● All infectable
  - ○ All
  - ○ By mask
- ☑ Exclude by mask
- ☑ Not a Virus List
- ☑ Exclude Files / Folders
- ☑ Scan compound objects
- □ Enable code analyser

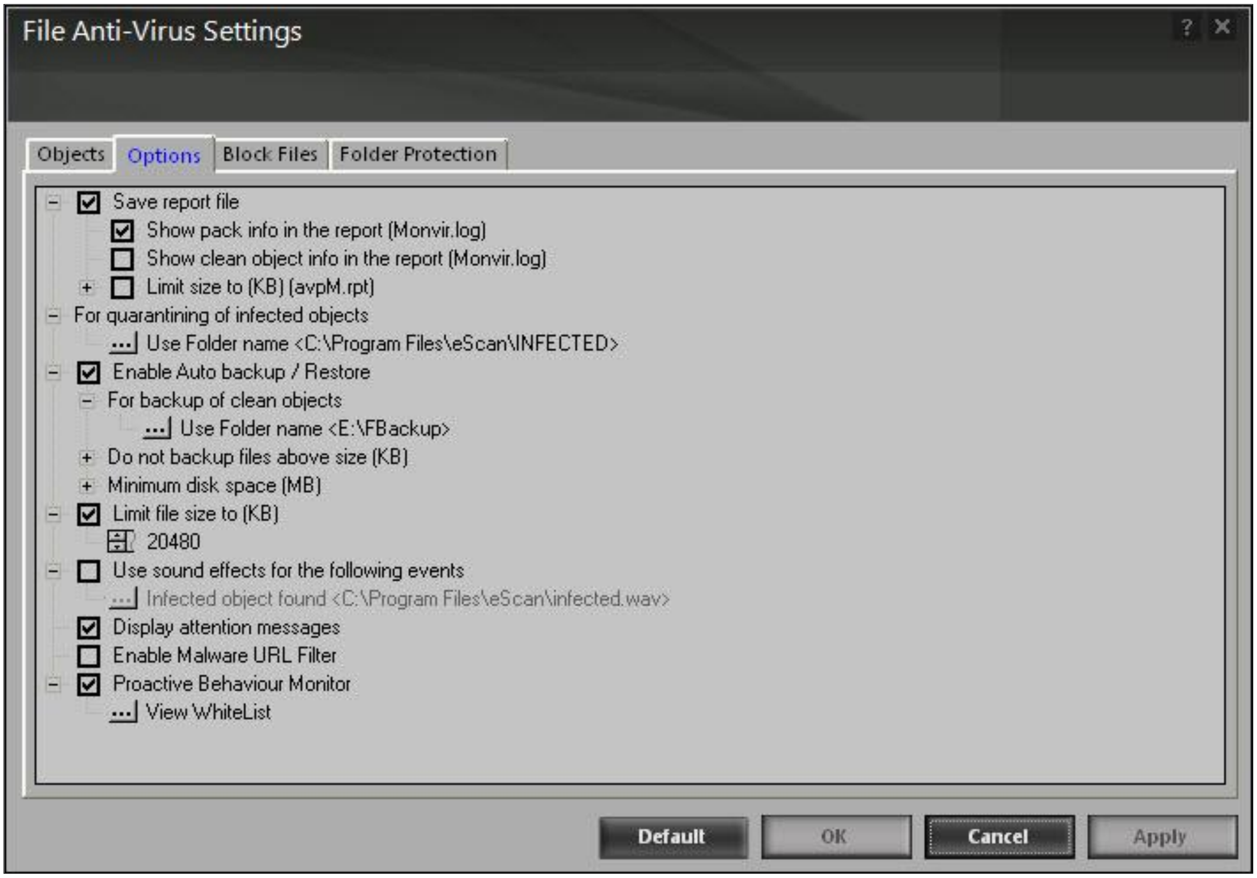
**Figure 21**

- Actions in case of virus detection: this section lists the different actions that file anti-virus can perform when it detects a virus infection. These actions are report only, disinfect, quarantine, and delete object. Out of these, the disinfect option is selected by default. By default, the quarantined files are saved in c:\program files\eScan\infected folder
- Scan local removable disk drives: [default] select this check box if you want the real time monitor to scan all the local removable drives attached to the computer.
- Scan local hard disk drives: [default] select this check box if you want the real time monitor to scan all the local hard drives installed on the computer.
- Scan network drives: [default] select this check box if you want the real time monitor to scan all the network drives including mapped folders and drives that are connected to the computer.
- Scan files of following types: it indicates the type of file that you want the real time monitor to scan. You have 3 options where you can select files for scanning, whether all infectable, all files, 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, double-click add/delete option, and then add or delete files as required.

- Exclude by mask: [default] select this check box if you want the file anti-virus monitor to exclude all the objects 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.
- Not a virus list: [default] file anti-virus is capable of detecting riskware. Riskware refers to a software that is originally not intended to be malicious, but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote admin software to the riskware list in the not a virus list dialog box by double-clicking the add / delete option, if you are certain that they are not malicious. The riskware list is empty by default.
- Exclude files/folders: [default] select this check box if you want file anti-virus to exclude all the listed files, folders, and sub-folders, while it is monitoring or scanning folders. You can add or delete folders from the existing list of folders by double-clicking the add / delete option.
- Scan compound objects: [default] select this check box if you want eScan to scan archives and packed files during scan operations. Select archive check box, if you want eScan to scan archive files. You can define the depth level of an archived file upto which you want to scan. 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.
- Enable code analyser: select this check box if you want the real time monitor to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. When this check box is selected, file anti-virus not only scans and detects infected objects by using the definitions or updates, but it also checks for suspicious files stored on your computer.

### Options

This tab helps you configure the basic settings for the file anti-virus module, such as the maximum size of log files and path of the destination folder for storing log files, quarantined objects, and report files.



☑ Save report file
- ☑ Show pack info in the report (Monvir.log)
- □ Show clean object info in the report (Monvir.log)
- □ Limit size to (KB) (avpM.rpt)

For quarantining of infected objects
- Use Folder name <C:\Program Files\eScan\INFECTED>

☑ Enable Auto backup / Restore
- For backup of clean objects
  - Use Folder name <E:\FBackup>
- Do not backup files above size (KB)
- Minimum disk space (MB)

☑ Limit file size to (KB)
- 20480

□ Use sound effects for the following events
- Infected object found <C:\Program Files\eScan\infected.wav>

☑ Display attention messages

□ Enable Malware URL Filter

☑ Proactive Behaviour Monitor
- View WhiteList

**Figure 22**

You can configure the following settings:

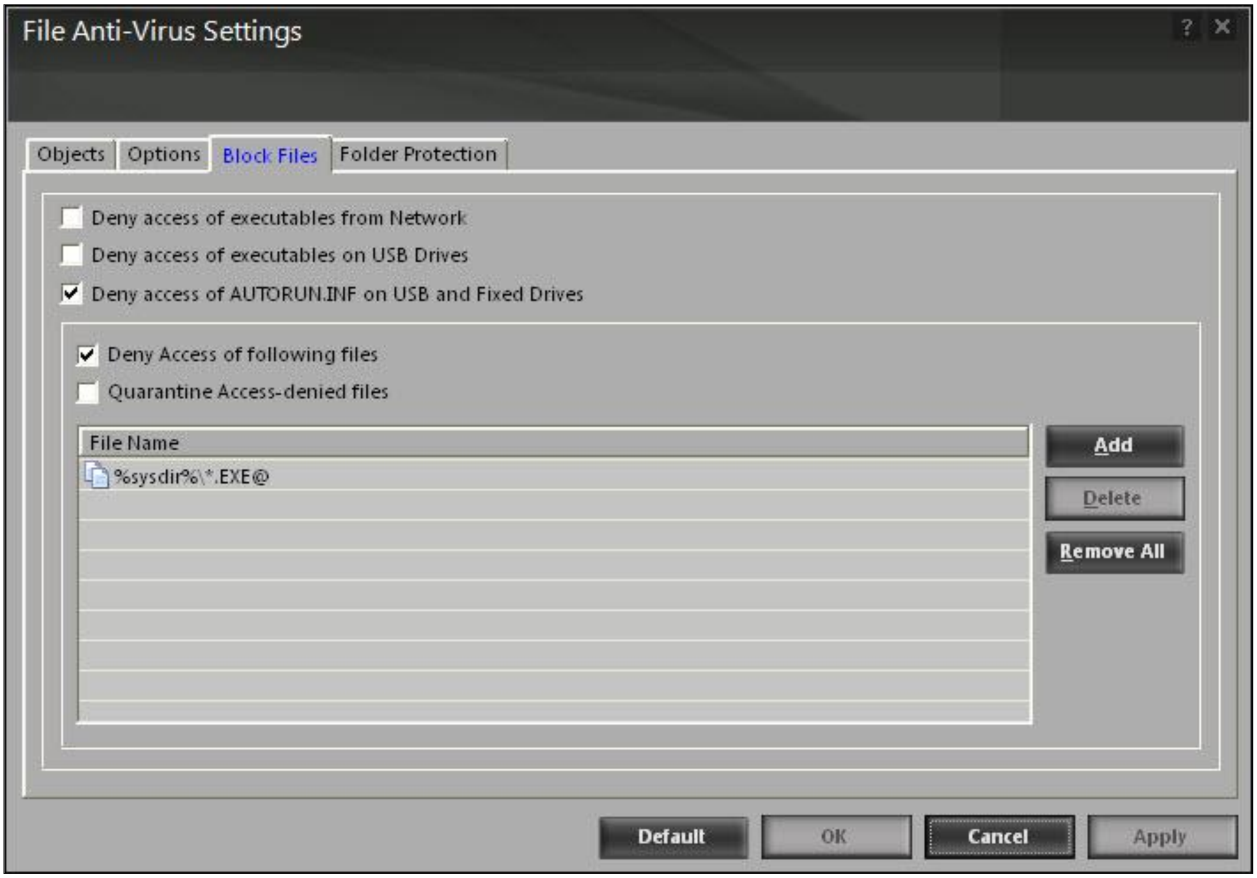
- Save report file: [default] select this check box if you want eScan to save the reports generated by the file anti-virus module. The report file logs information about the scanned files and the action taken by file anti-virus when an infected file was found during the scan.
  - Show pack info in the report (monvir.log): [default] select this check box if you want file anti-virus to add information regarding scanned compressed files, such as .zip and .rar files to the monvir.log file.
  - Show clean object info in the report (monvir.log): select this check box if you want file anti-virus to add information regarding uninfected files found during a scan operation to the monvir.log file. You can select this option to find out which files are not infected.
  - Limit size to (kb) (avpm.rpt): select this check box if you want file anti-virus to limit the size of the avpm.rpt file. You can double-click the size box and specify the size of the log file. The default value is 50 kb
- For quarantining of infected objects: this option helps you specify the destination for storing quarantined objects. By default, the quarantined objects are stored in the c:\program files\eScan\infected folder. You can change the location of the destination folder if required.

- Enable auto backup / restore: [default] select this check box if you want eScan to take automatic backup of critical files of the windows® operating system installed on your computer and to restore the clean files when it finds an infection in any of the system files, which cannot be disinfected. You can do the following settings:
  - For backup of clean objects: you can back up uninfected objects and store them in a given folder. By default, these objects are stored in the e:\fbackup folder. You can change the destination of the backed up objects if necessary.
  - Do not backup files above size (kb): [default] this option helps you prevent file anti-virus from creating backup of files that are larger than the file size that you have specified. The default value is set to 32768 kb
  - Minimum disk space (mb): [default] it enables you to set the minimum free hard disk space upto which you want eScan to take backup of files. By default, value is 500 kb, but you can change it by double-clicking the ⊟ icon, and then type value in the size box.
- Limit file size to (kb): [default] this check box enables you to set a size limit for the objects or files to be scanned. The default value is set to 20480 kb.
- Use sound effects for the following events: this check box helps you configure eScan to play a sound file and show you the details regarding the infection within a message box when any malicious software is detected by file anti-virus. However, you need to ensure that the computer speakers are switched on.
- Display attention messages: [default] when this option is selected, eScan displays an alert, which displays the path and name of the infected object and the action taken by the file anti-virus module.
- Enable malware url filter: select this check box, if you want to block access to malicious websites/url's.
- Proactive behavior monitor: select this check box, if you want eScan to monitor the executable files you are running on your system.

  In case, if eScan finds any executable files suspicious or may cause any harm to your system, it pops-up with a message. If you want to access the suspicious file, you can white list them anytime.

### ▪ Block files

This tab helps you configure settings for preventing executable and files, such as autorun.inf, on network drives, usb drives, and fixed drives from accessing your computer.



□ Deny access of executables from Network

□ Deny access of executables on USB Drives

☑ Deny access of AUTORUN.INF on USB and Fixed Drives

☑ Deny Access of following files

□ Quarantine Access-denied files

%sysdir%*.EXE@

Figure 23

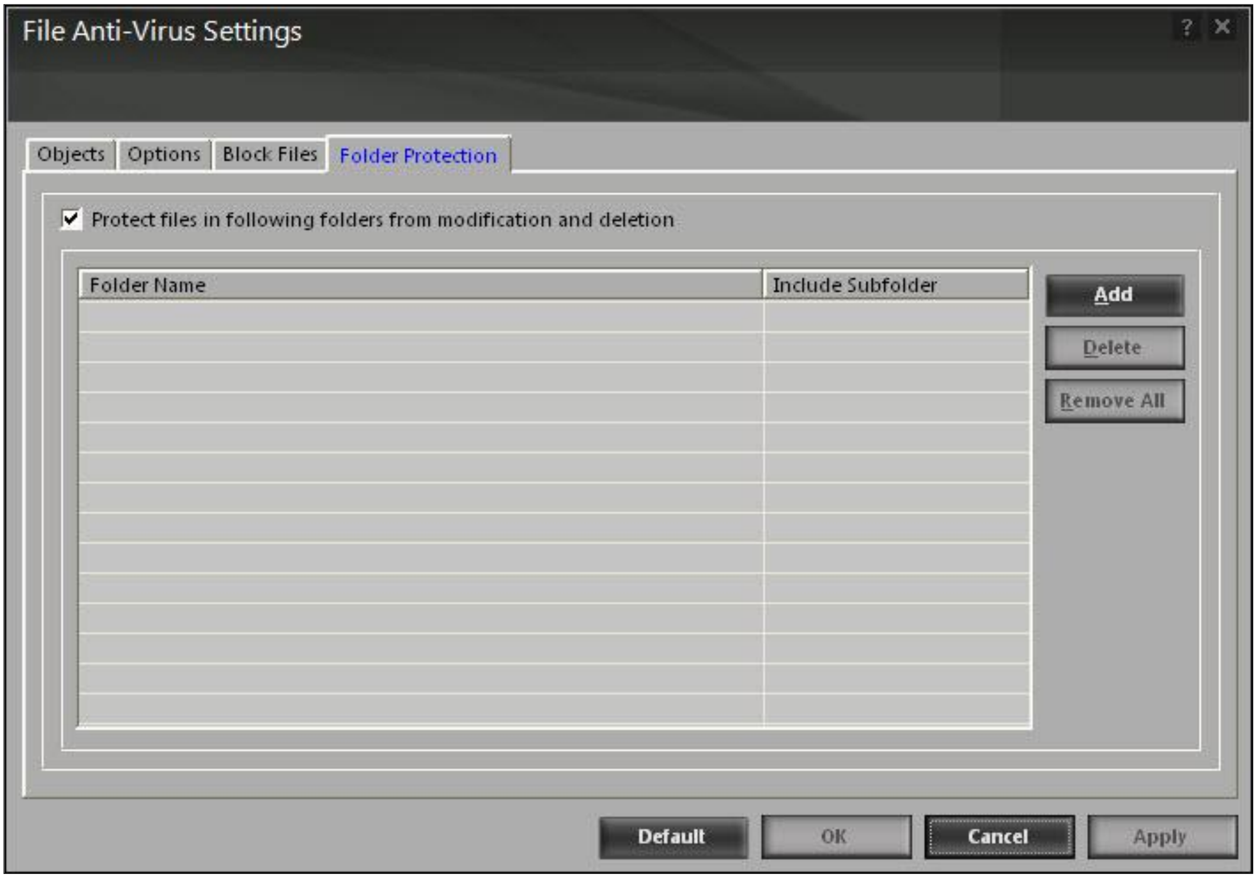
You can configure the following settings:

- Deny access of executable from network: select this check box if you want to prevent executables on your computer from being accessed from the network.
- Deny access of executables on usb drives: select this check box if you want to prevent executables stored on usb drives from being accessed.
- Deny access of autorun.inf on usb and fixed drives: [default] select this check box if you want to prevent executable from usb and fixed drives from being accessed.
- Deny access of following files: [default] select this check box if you want to prevent the files in the list from running on your computer.
- Quarantine access-denied files: select this check box if you want to quarantine files that have been denied access.

You can prevent specific files from running on your computer by adding them to the block files list. By default, this list contains the value %sysdir%*.exe@.

- ### Folder protection

This tab helps you protect specific folders from being modified or deleted by adding them to the folder protection list.



File Anti-Virus Settings

☑ Protect files in following folders from modification and deletion

| Folder Name | Include Subfolder |
|---|---|

**Figure 24**

It allows you to configure the following setting:

- Protect files in following folders from modification and deletion: [default] this option is selected by default. Select this check box if you want the file anti-virus module to protect files in specific folders from being modified or deleted.

- Reports

  This section displays the following information.

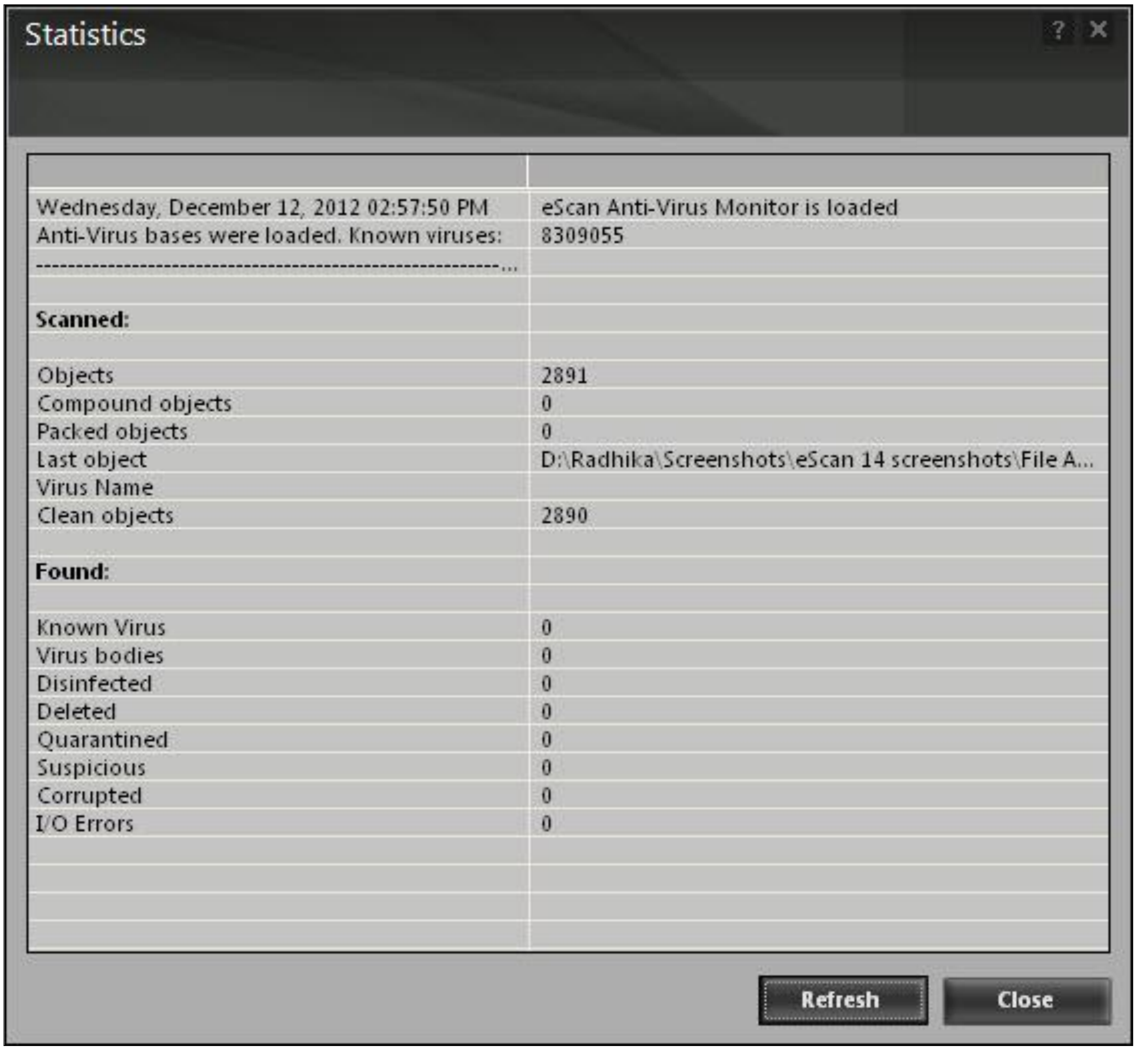
  - Total files scanned: it shows the total number of files scanned by the real-time file anti-virus monitor.

- 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.

In addition, you can view the following reports:

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 and found, under scanned, the number of scanned objects, compound objects, packed objects, clean objects, and so on are displayed, and under found, the number of known virus, virus bodies, deleted, quarantined, and so on are displayed.



Statistics

| | |
|---|---|
| Wednesday, December 12, 2012 02:57:50 PM | eScan Anti-Virus Monitor is loaded |
| Anti-Virus bases were loaded. Known viruses: | 8309055 |
| -----------------------------------------------------------... | |
| **Scanned:** | |
| Objects | 2891 |
| Compound objects | 0 |
| Packed objects | 0 |
| Last object | D:\Radhika\Screenshots\eScan 14 screenshots\File A... |
| Virus Name | |
| Clean objects | 2890 |
| **Found:** | |
| Known Virus | 0 |
| Virus bodies | 0 |
| Disinfected | 0 |
| Deleted | 0 |
| Quarantined | 0 |
| Suspicious | 0 |
| Corrupted | 0 |
| I/O Errors | 0 |

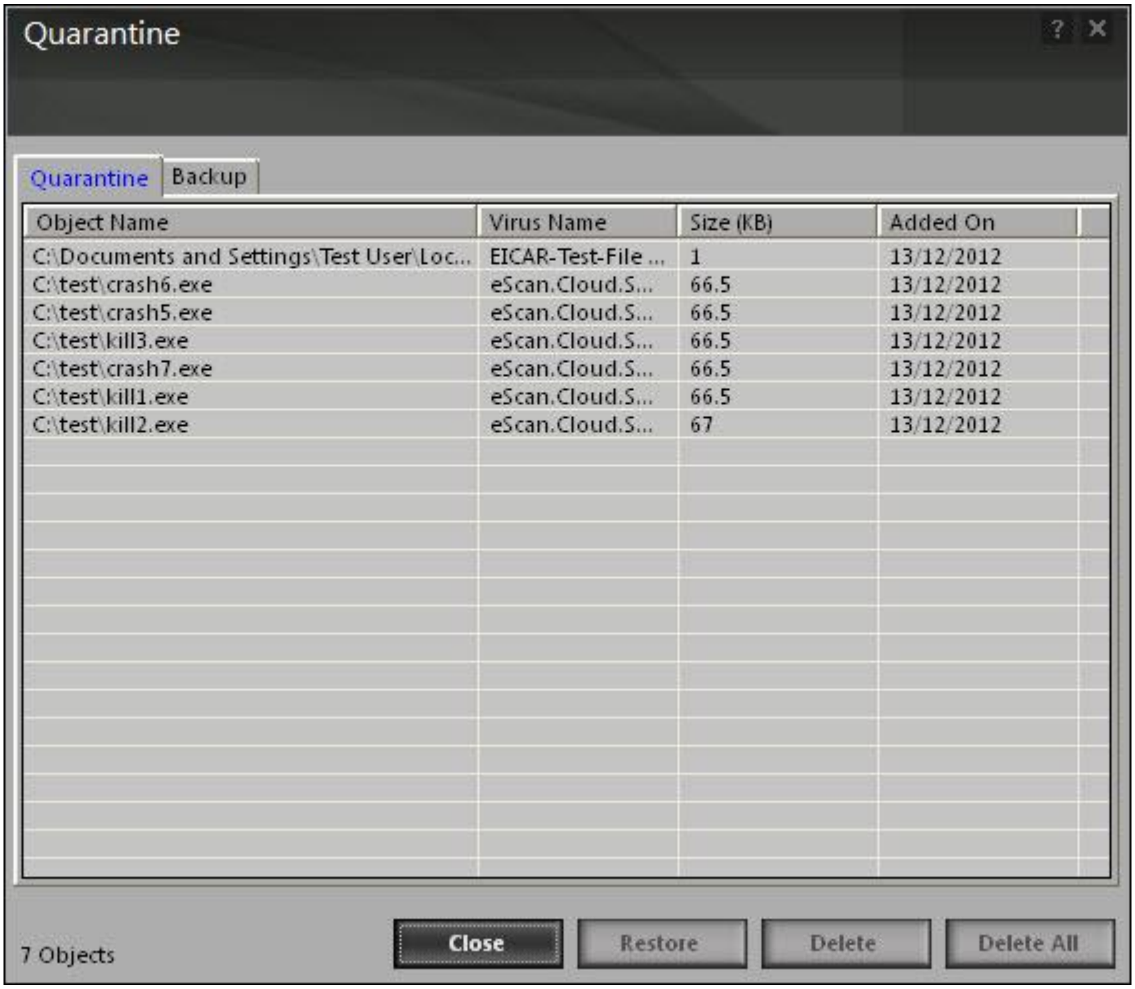
**Figure 25**

In addition, it displays the following information:

- The current details of the system date, time, and whether the eScan anti-virus monitor is running or not.
- The number of viruses detected.
- The results of most recent scan, such as the last object scanned and name of the virus detected.

View quarantined objects:

When you click this button, the quarantine dialog box is displayed, which displays the quarantined files and backup files. This dialog box has the following tabs:.



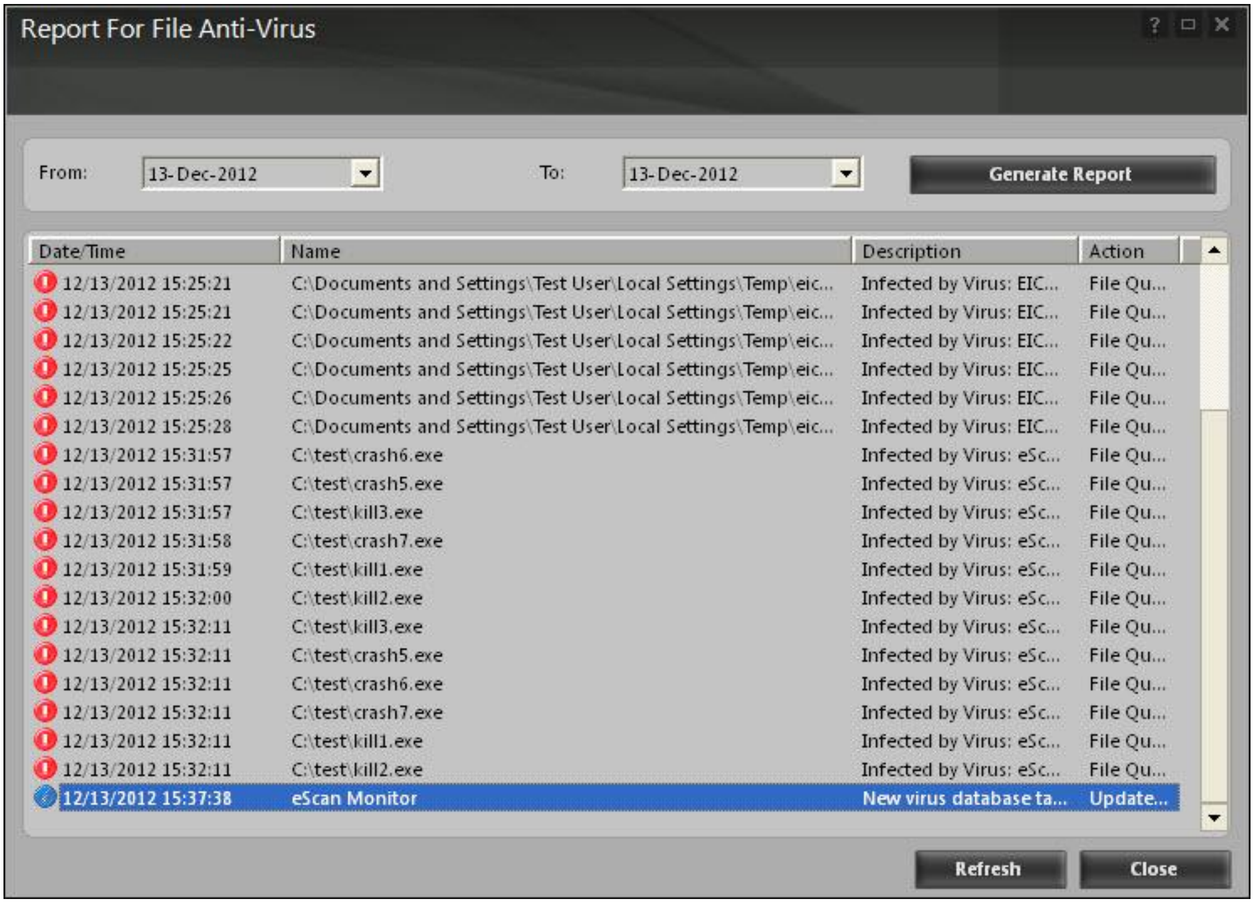
| Object Name | Virus Name | Size (KB) | Added On |
|---|---|---|---|
| C:\Documents and Settings\Test User\Loc... | EICAR-Test-File ... | 1 | 13/12/2012 |
| C:\test\crash6.exe | eScan.Cloud.S... | 66.5 | 13/12/2012 |
| C:\test\crash5.exe | eScan.Cloud.S... | 66.5 | 13/12/2012 |
| C:\test\kill3.exe | eScan.Cloud.S... | 66.5 | 13/12/2012 |
| C:\test\crash7.exe | eScan.Cloud.S... | 66.5 | 13/12/2012 |
| C:\test\kill1.exe | eScan.Cloud.S... | 66.5 | 13/12/2012 |
| C:\test\kill2.exe | eScan.Cloud.S... | 67 | 13/12/2012 |

**Figure 26**

- 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.
- 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.

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.



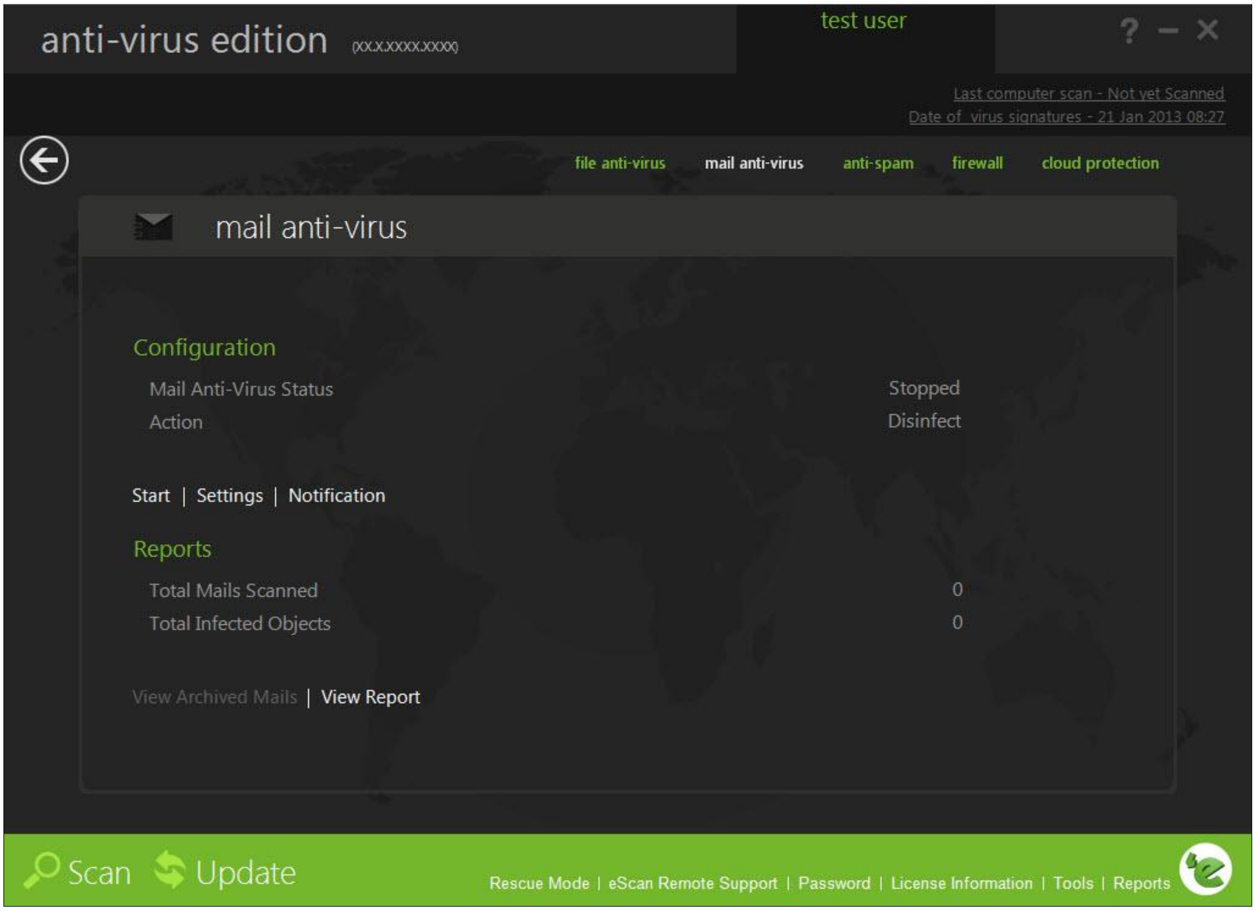
From: 13-Dec-2012 To: 13-Dec-2012

| Date/Time | Name | Description | Action |
|---|---|---|---|
| 12/13/2012 15:25:21 | C:\Documents and Settings\Test User\Local Settings\Temp\eic... | Infected by Virus: EIC... | File Qu... |
| 12/13/2012 15:25:21 | C:\Documents and Settings\Test User\Local Settings\Temp\eic... | Infected by Virus: EIC... | File Qu... |
| 12/13/2012 15:25:22 | C:\Documents and Settings\Test User\Local Settings\Temp\eic... | Infected by Virus: EIC... | File Qu... |
| 12/13/2012 15:25:25 | C:\Documents and Settings\Test User\Local Settings\Temp\eic... | Infected by Virus: EIC... | File Qu... |
| 12/13/2012 15:25:26 | C:\Documents and Settings\Test User\Local Settings\Temp\eic... | Infected by Virus: EIC... | File Qu... |
| 12/13/2012 15:25:28 | C:\Documents and Settings\Test User\Local Settings\Temp\eic... | Infected by Virus: EIC... | File Qu... |
| 12/13/2012 15:31:57 | C:\test\crash6.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:31:57 | C:\test\crash5.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:31:57 | C:\test\kill3.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:31:58 | C:\test\crash7.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:31:59 | C:\test\kill1.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:00 | C:\test\kill2.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:11 | C:\test\kill3.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:11 | C:\test\crash5.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:11 | C:\test\crash6.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:11 | C:\test\crash7.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:11 | C:\test\kill1.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:32:11 | C:\test\kill2.exe | Infected by Virus: eSc... | File Qu... |
| 12/13/2012 15:37:38 | eScan Monitor | New virus database ta... | Update... |

Figure 27

## Mail anti-virus

Mail anti-virus is the second module of the eScan for av. This module scans all incoming and outgoing e-mails 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 e-mails and attachments, but you can configure it to scan outgoing e-mails and attachments as well. Moreover, it helps you notify the sender or system administrator, whenever you receive an infected e-mail or attachment.


anti-virus edition (XX.X.XXXX.XXXX)
test user
Last computer scan - Not yet Scanned
Date of virus signatures - 21 Jan 2013 08:27
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
mail anti-virus
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

| | |
|---|---|
| Mail Anti-Virus Status | Stopped |
| Action | Disinfect |

Start | Settings | Notification

Reports

| | |
|---|---|
| Total Mails Scanned | 0 |
| Total Infected Objects | 0 |

View Archived Mails | View Report

**Figure 28**

This page provides you with options required for configuring the module. You can configure the settings from the following 2 sections:

- Configuration

  This section displays the following information:

  - Mail anti-virus status: it displays the status of 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 enable or disable mail anti-virus module.

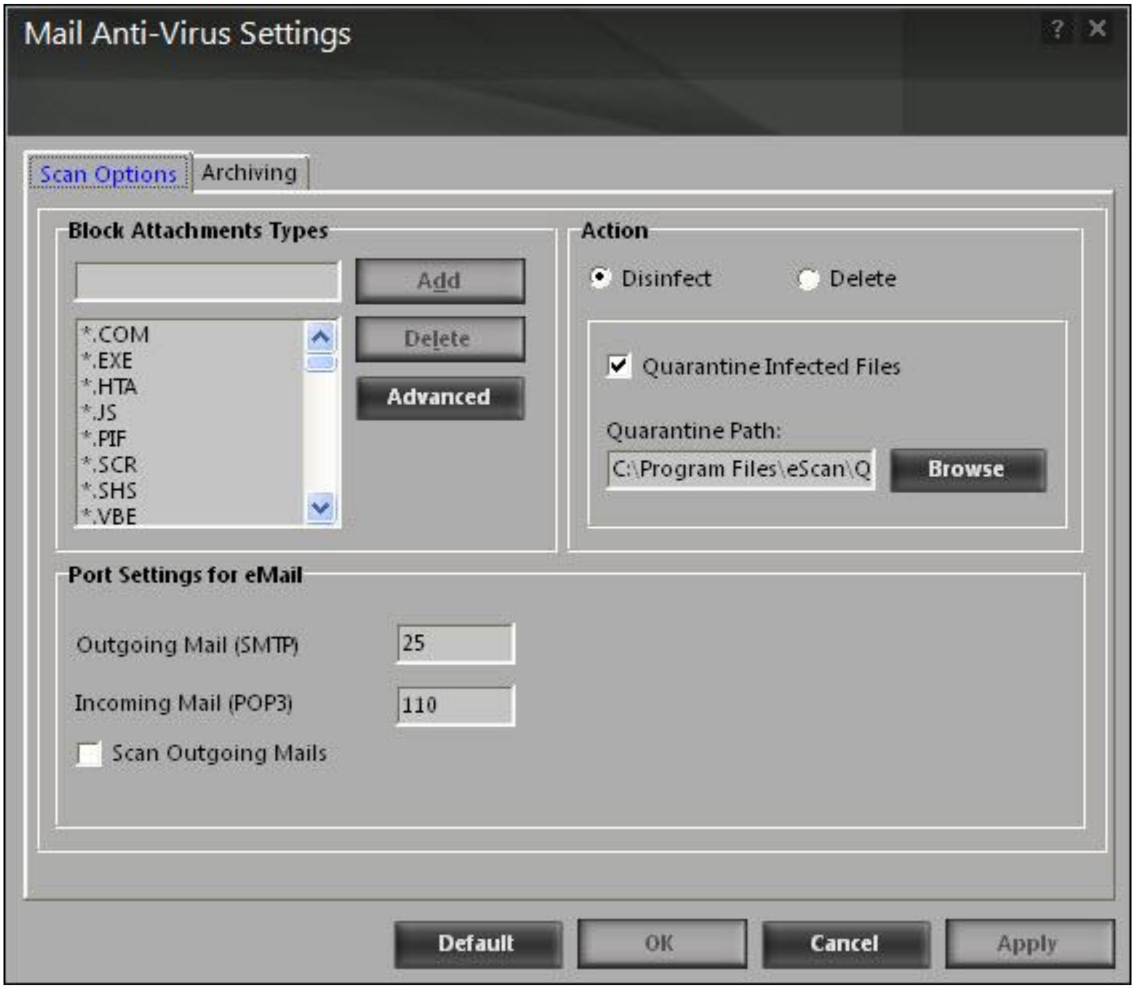
Settings:

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 which are as follows:

> ✍ On below the screen of all the tabs contains four buttons — default, ok, cancel, and apply, which you have to 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.

- ### Scan options

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



Mail Anti-Virus Settings

Scan Options | Archiving

**Block Attachments Types**

*.COM
*.EXE
*.HTA
*.JS
*.PIF
*.SCR
*.SHS
*.VBE

**Action**

● Disinfect ○ Delete

☑ Quarantine Infected Files

Quarantine Path: C:\Program Files\eScan\Q

**Port Settings for eMail**

Outgoing Mail (SMTP): 25

Incoming Mail (POP3): 110

□ Scan Outgoing Mails

**Figure 29**

This tab helps you configure the following settings:

- 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 e-mail attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your 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 e-mails for malicious code.
  - Advanced: you can click this button to open the advanced scan options dialog box. This dialog box helps you configure the following advanced scanning options:
    - Delete all attachment in email if disinfection is not possible: select this check box if you want to delete all the e-mail attachments that cannot be cleaned.

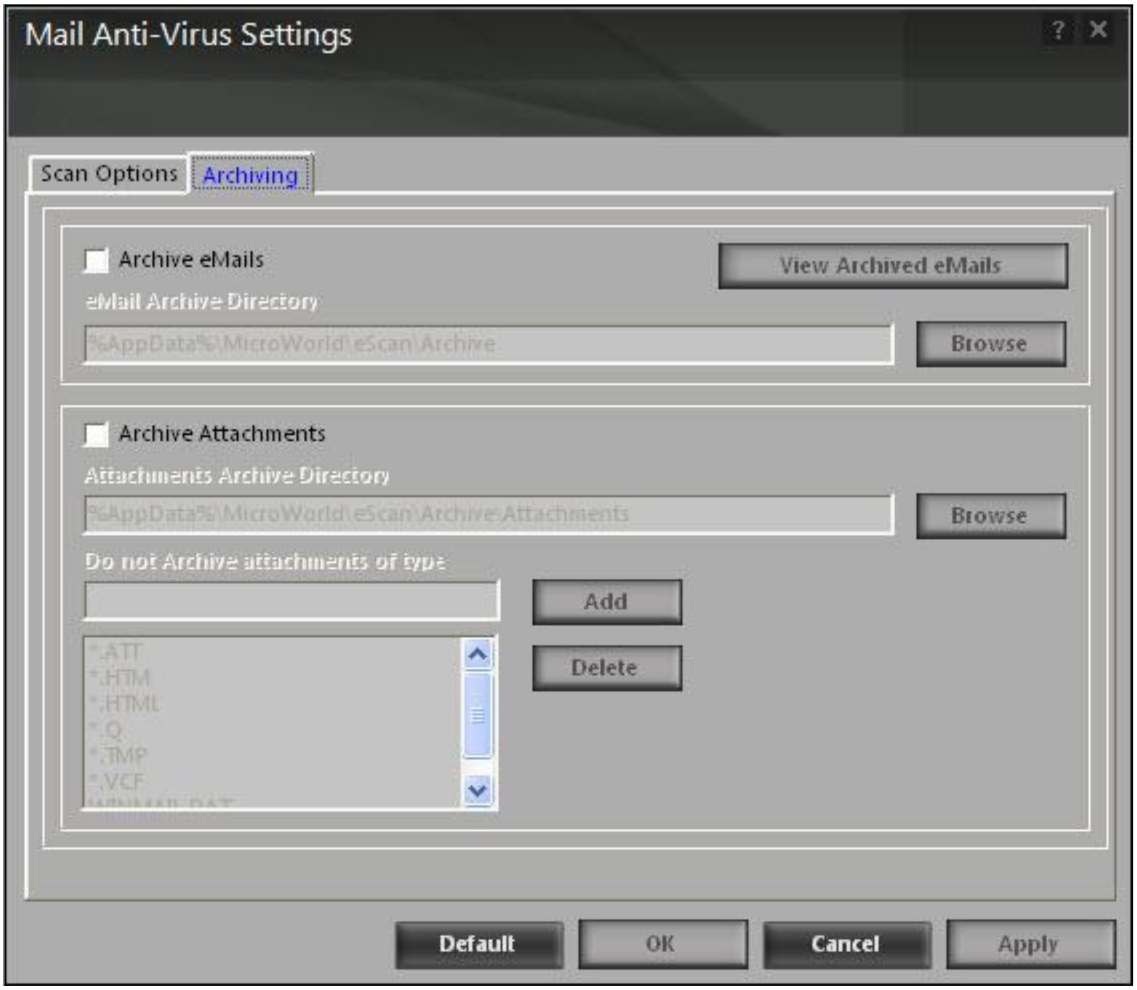
- Delete entire email if disinfection is not possible: [default] select this check box if you want to delete the entire e-mail if any attachment cannot be cleaned.
- Delete entire email if any virus is found: select this check box if you want to delete the entire e-mail if any virus is found in the email or the attachment is infected.
- Quarantine blocked attachments: [default] select this check box if you want to quarantine the attachment if it has an extension that is blocked by eScan.
- Delete entire email if any blocked attachment is found: [default] select this check box if you want to delete an e-mail if it contains an attachment with an extension type that is blocked by eScan.
- Quarantine email if attachments are not scanned: select this check box if you want to quarantine an entire e-mail if it contains an attachment that is not scanned by mail anti-virus.
- Quarantine attachments if they are not scanned: select this check box if you want to quarantine attachments that are not scanned by mail anti-virus.
- Exclude attachments (whitelist): this list is empty by default. You can add file names and file extensions that should not be blocked by eScan. You can also configure eScan to allow specific files even though if the file type is blocked. For example, if you have listed *.pif in the list of blocked attachments and you need to allow an attachment with the name abc, you can add abc.pif to the exclude attachments list. Add *.pif files in this section will allow all *.pif to be delivered. MicroWorld recommends you to add the entire file name like abcd.pif.

- Action: this section helps you configure the actions to be performed on infected e-mails.
  - Disinfect: [default] click this option if you want mail anti-virus to disinfect infected e-mails or attachments.
  - Delete: click this option if you want mail anti-virus to delete infected e-mails or attachments.
  - Quarantine infected files: [default] select this check box if you want mail anti-virus to quarantine infected e-mails or attachments. The default path for storing quarantined e-mails or attachments is c:\program files\eScan\quarant. However, you can specify a different path for storing quarantined files, if required.

- Port settings for email: you can also specify the ports for incoming and outgoing e-mails, so that eScan can scan the e-mails sent or received through those ports.
  - Outgoing mail (smtp): [default: 25] you need to specify a port number for smtp.
  - Incoming mail (pop3): [default: 110] you need to specify a port number for pop3.
  - Scan outgoing mails: select this check box if you want the mail anti-virus to scan outgoing e-mails.

### Archiving

This screen helps you configure settings for archiving e-mails and e-mail attachments..



☐ Archive eMails

eMail Archive Directory: %AppData%\MicroWorld\eScan\Archive

☐ Archive Attachments

Attachments Archive Directory: %AppData%\MicroWorld\eScan\Archive\Attachments

Do not Archive attachments of type:

*.ATT
*.HTM
*.HTML
*.Q
*.TMP
*.VCF
WINMAIL.DAT

**Figure 30**

The following configuration options are available on this screen:

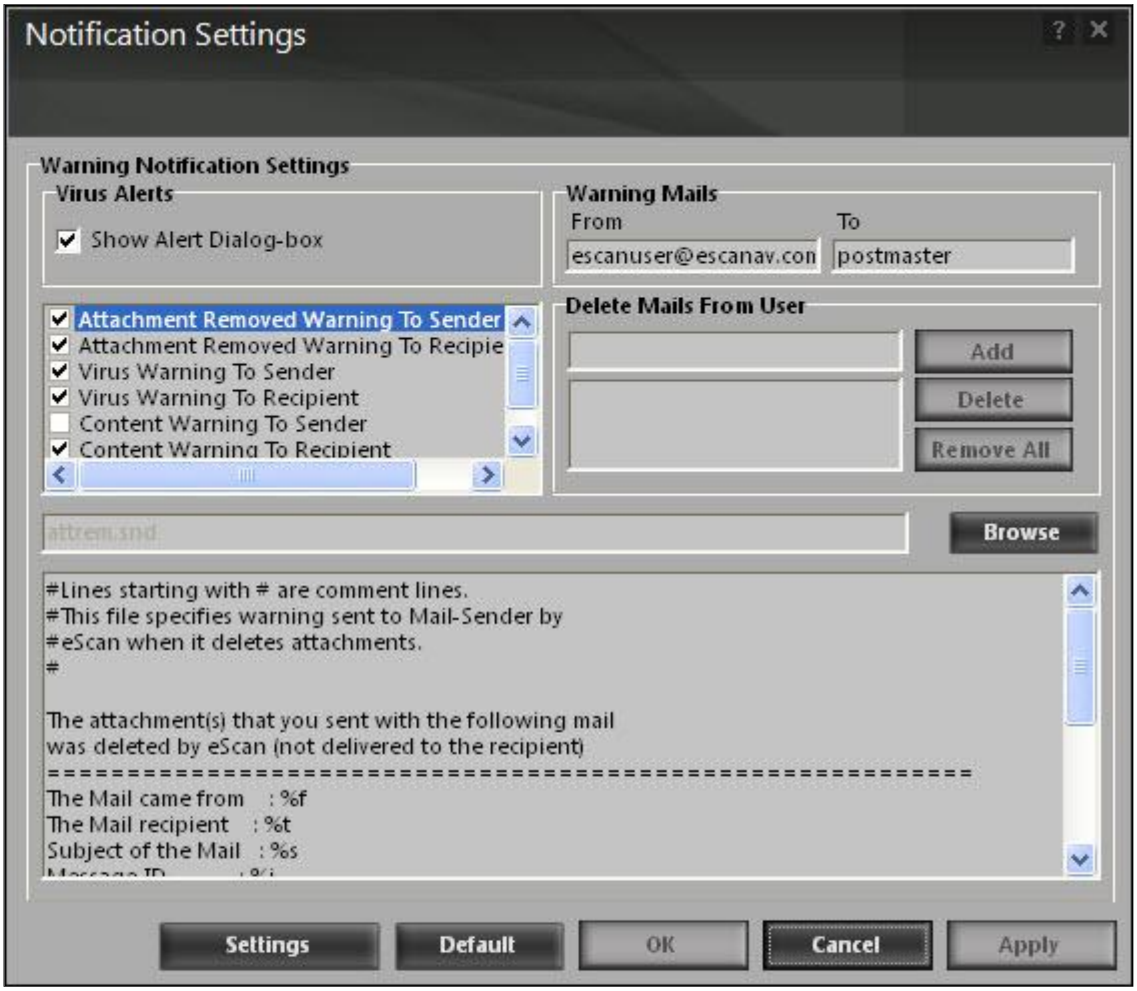
- Archive emails: this option helps you archive or back up all scanned e-mails that you have sent or received. Mail anti-virus provides you with the facility of backing up your e-mails to a given folder. The default path for storing archived e-mails is %appdata%\MicroWorld\eScan\archive. By default, the email archive directory field, view archived emails button, and browse button appears dimmed. It is available only when you select the archive emails check box. Select the archive emails check box to specify the path of the backup folder. You can type or click the browse button to select the path. Click the view archived emails button, to view the list of archived e-mails.

- Archive attachments: select this check box if you want to archive or back up all sent or received e-mail 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 check box, do not archive attachments of type check box, and browse button appears dimmed. These fields are available only when you select the archive attachments check box.  The default path for storing archived e-mail attachments is

%appdata%\MicroWorld\eScan\archive\attachments. At times, you may not require e-mail attachments of a specific file type. In that case, you can excluded certain file types, such as *.vcf, *.htm, and *.html, from being archived by adding them to the do not archive attachments of type list.

Notification:

You can click this button to open the notification settings dialog box, which helps you configure the notification settings for the mail anti-virus module. By configuring this module, you can send e-mails to specific recipients when malicious code is detected in an e-mail or e-mail attachment. This dialog box helps you configure the notification settings for sending alerts and warning messages to the senders or recipients of an infected message.



Notification Settings

Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

☑ Attachment Removed Warning To Sender
☑ Attachment Removed Warning To Recipie
☑ Virus Warning To Sender
☑ Virus Warning To Recipient
□ Content Warning To Sender
☑ Content Warning To Recipient

Warning Mails

From: escanuser@escanav.con

To: postmaster

Delete Mails From User

attrem.snd

```
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#eScan when it deletes attachments.
#

The attachment(s) that you sent with the following mail
was deleted by eScan (not delivered to the recipient)
=======================================================
The Mail came from    : %f
The Mail recipient    : %t
Subject of the Mail   : %s
```

**Figure 31**

You can configure the following notification settings:

- Virus alerts

    - Show alert dialog-box: [default] select this check box if you want mail anti-virus to alert you when it detects a malicious object in an e-mail.
    - Attachment removed warning to sender: [default] select this check box if you want mail anti-virus to send a warning message to the sender of an infected attachment. Mail anti-virus sends this e-mail when it encounters a virus-infected attachment in an e-mail. The content of the e-mail that is sent is displayed in the preview box.
    - Attachment removed warning to recipient: [default] 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 e-mail that is sent is displayed in the preview box.
    - Virus warning to sender: [default] select this check box if you want mail anti-virus to send a virus-warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
    - Virus warning to recipient: [default] select this check box if you want mail anti-virus to send a virus-warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
    - 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 e-mail that is sent is displayed in the preview box.
    - Content warning to recipient: [default] select this check box if you want mail anti-virus to send a content warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
  - Warning mails: you can configure this setting if you want mail anti-virus to send warning e-mails and alerts to a given sender or recipient. The default sender (from field) is postmaster and the default recipient (to field) is postmaster.
  - Delete mails from user: you can configure eScan to automatically delete mails that have been sent by specific users. For this, you need to add the mail addresses of such users to the delete mails from user list. By default, the delete mails from user section fields are unavailable, it is available only when you type in some text in the delete mails from user field and add mail addresses.

- Reports

  This section displays the following information:

  - Total mails scanned: it shows the total number of e-mails scanned by mail anti-virus on a real-time basis.
  - Total infected objects: it shows the total number of infected objects found by mail anti-virus on a real-time basis.

In addition, you can view the following reports:

View archived mails:

You can click this button to open the view archived emails window. (for more information on archived e-mail settings, refer archived tab under mail anti-virus settings window.)

View report:

You can click this button to open the report for mail anti-virus window. This window displays the summary of infected e-mails and the action taken by mail anti-virus on such e-mails for a given range of dates in a tabular format when you click the generate report button.

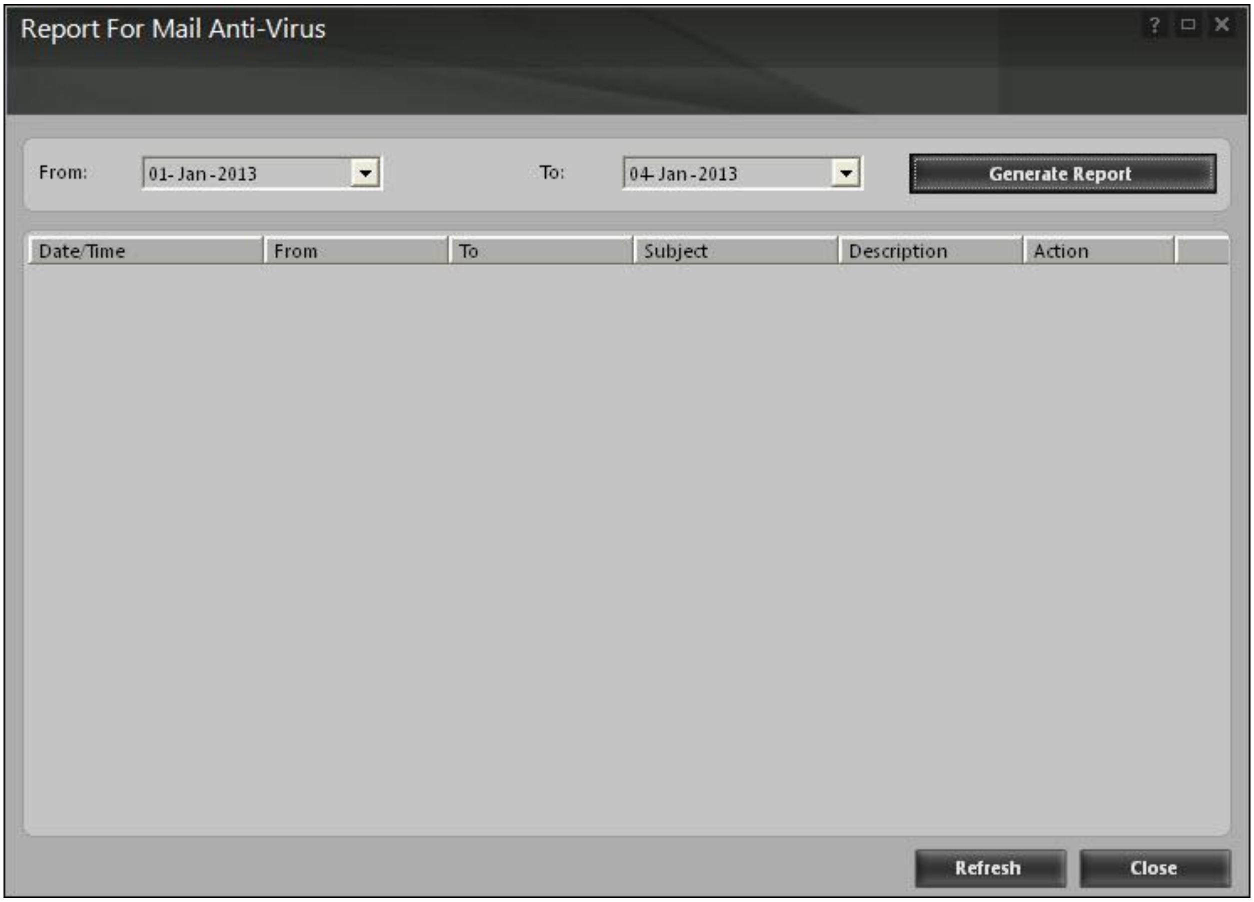
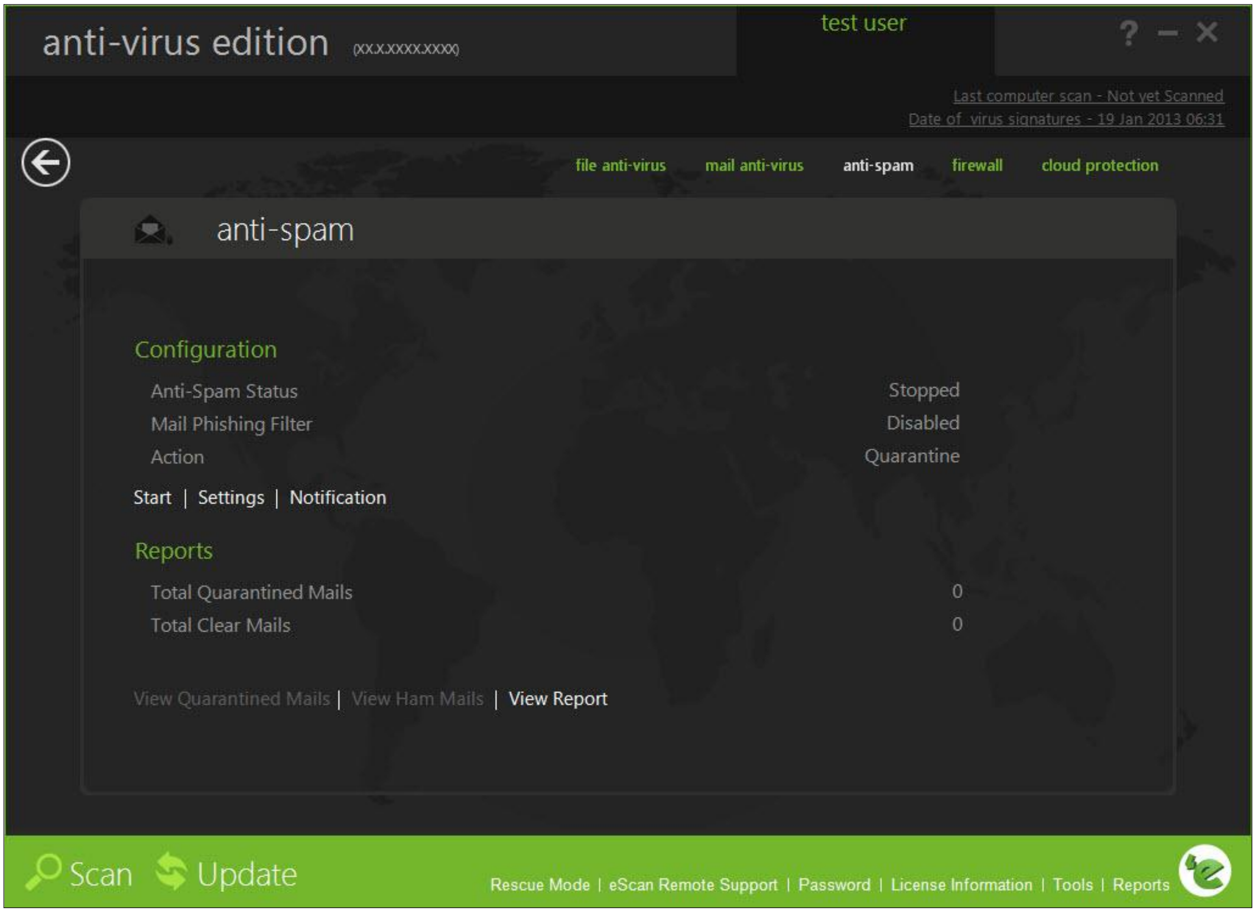


Figure 32

## Anti-spam

Anti-spam is the third module of the eScan for av. This module filters all your junk and spam e-mails by using the nilp technology and sends content warnings to specified recipients.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - Not yet Scanned
Date of virus signatures - 19 Jan 2013 06:31
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
anti-spam
Start | Settings | Notification
View Quarantined Mails | View Ham Mails | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

| | |
|---|---|
| Anti-Spam Status | Stopped |
| Mail Phishing Filter | Disabled |
| Action | Quarantine |

Reports

| | |
|---|---|
| Total Quarantined Mails | 0 |
| Total Clear Mails | 0 |

**Figure 33**

This page provides you with options required to configure the module. You can configure the settings from the following 2 sections:

- Configuration

  This section displays the following information:

  - Anti-spam status: it displays the status of 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:

Click an appropriate option to enable or disable anti-spam module.

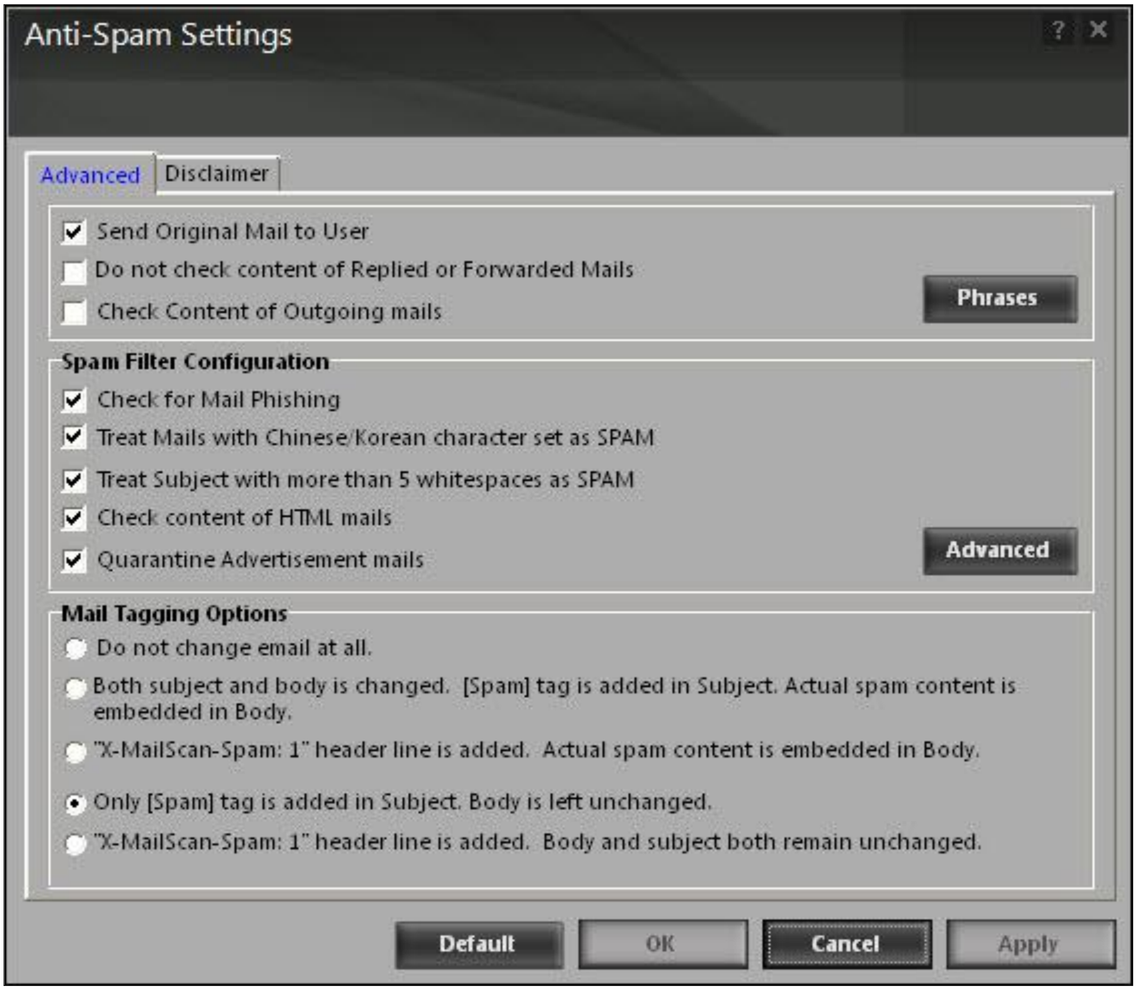
Settings:

When you click this button, the anti-spam settings window appears. On the anti-spam settings window, you have two tabs – advanced and disclaimer, which are as follows:

> ✍ On below the screen of all the tabs contains four buttons — default, ok, cancel, and apply, which you have to 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.

### Advanced

This section provides you with options for configuring the general e-mail options, spam filter configuration, and tagging e-mails in anti-spam.


Anti-Spam Settings

☑ Send Original Mail to User

□ Do not check content of Replied or Forwarded Mails

□ Check Content of Outgoing mails

Spam Filter Configuration

☑ Check for Mail Phishing

☑ Treat Mails with Chinese/Korean character set as SPAM

☑ Treat Subject with more than 5 whitespaces as SPAM

☑ Check content of HTML mails

☑ Quarantine Advertisement mails

Mail Tagging Options

○ Do not change email at all.

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

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

● Only [Spam] tag is added in Subject. Body is left unchanged.

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

**Figure 34**

- Send original mail to user: [default] this check box is selected by default. EScan creates spam folder within the e-mail client. When an e-mail is tagged as spam, it is moved to this folder. Select this check box, if you want to send original e-mail that is tagged as spam to the recipient as well.

- Do not check content of replied or forwarded mails: select this check box, if you want to ensure that eScan does not check the contents of e-mails that you have either replied or forwarded to other recipients.

- Check content of outgoing mails: select this check box, if you want anti-spam to check outgoing e-mails for restricted content.
  - Phrases: you can click the phrases button to open the phrases dialog box. This dialog box helps you configure additional e-mail-related options. In addition, it allows you to specify a list of words that the user can either allow or block. This list is called the user specified whitelist. You can specify certain words or phrases, so that mails containing those words or phrases in the subject, header, or body are recognized as spam and are quarantined or deleted. All the

fields are available only when you select the enable e-mail content scanning check box. The dialog box uses the following color codes to categorize e-mails.

- User specified whitelist of words/phrases: (color code: green) click this option to list the words or phrases that are present in the whitelist. 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 list the words or phrases that are defined in block list.
- User specified words/phrases disabled: (color code: gray) click this option to list the words or phrases that are defined excluded during scans. The options in the phrases to check dialog box are disabled by default.

- Spam filter configuration: this section provides you with options for configuring the spam filter. All options in this section are selected by default.
  - Check for mail phishing: [default] select this check box, if you want anti-spam to check for fraudulent e-mails and quarantine them.
  - Treat mails with chinese /korean character set as spam: [default] when this check box is selected, eScan scans e-mails with chinese or korean characters. This check is based on the research data conducted by MicroWorld's various spam e-mail samples collected from around the globe. From these samples, it was observed that spammers often use chinese or korean characters in their e-mails.
  - Treat subject with more than 5 whitespaces as spam: [default] in its research, MicroWorld found that spam e-mails usually contain more than five consecutive white spaces. When this check box is selected, anti-spam checks the spacing between characters or words in the subject line of e-mails and treats e-mails with more than five whitespaces in their subject lines as spam e-mails.
  - Check content of html mails: [default] select this check box when you want anti-spam to scan e-mails in html format along with textual content.
  - Quarantine advertisement mails: [default] select this check box when you want anti-spam to check for advertisement types of e-mails and quarantine them.
    - Advanced: click this button to open the advanced spam filtering options dialog box. This dialog box helps you configure the following advanced options for controlling spam.
      - Enable non-intrusive learning pattern (nilp) check: [default] nilp is MicroWorld's revolutionary technology that uses bayesian filtering and works on the principles of artificial intelligence (ai) to analyze each e-mail and prevents spam and phishing e-mails 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 e-mail 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: [default] select this check box if you want to check the validity of certain generic fields, such as from, to, and cc in an e-mail and marks it as spam if any of the headers are invalid.
      - Enable x-spam rules check: [default] x-spam rules are rules that describe certain characteristics of an e-mail. It checks whether the words in the

content of e-mails 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 e-mail 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 e-mails and takes action on them.

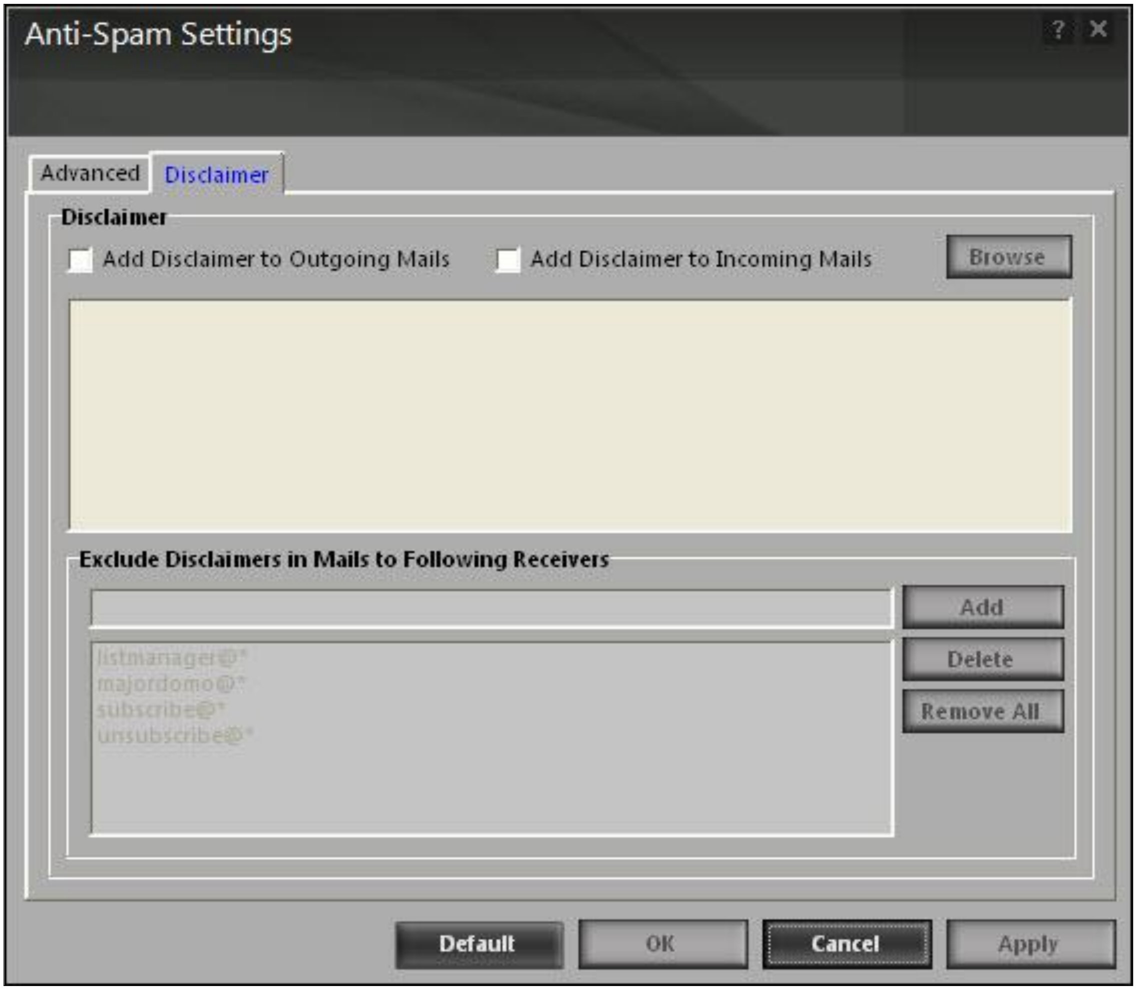
- Enable sender policy framework (spf) check: spf is a world-standard framework that is adopted by eScan to prevent hackers from forging sender addresses. It acts a powerful mechanism for controlling phishing mails. Select this check box if you want anti-spam to check the spf record of the sender's domain. However, your computer should be connected to the internet for this option to work.
- Enable spam uri realtime blacklist (surbl) check: select this check box if you want anti-spam to check the urls in the message body of an e-mail. If the url is listed in the surbl site, the e-mail 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 e-mail will be blocked from being downloaded. However, your computer should be connected to the internet for this option to work.
- Rbl servers: rbl is a dns server that lists ip addresses of known spam senders. If the ip of the sender is found in any of the blacklisted categories, the connection is terminated. The rbl servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.
- Auto-spam whitelist: unlike normal rbls, surbl scans e-mails 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 e-mail addresses that can bypass the above spam filtering options. It thus allows e-mails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

- Mail tagging options: anti-spam also includes some mail tagging options, which are described as follows:
  - Do not change email at all: click this option if you want to prevent anti-spam from adding the [spam] tag to e-mails that have been identified as spam.
  - Both subject and body is changed: [spam] tag is added in subject: actual spam content is embedded in body: this option helps you identify spam e-mails. When you select this option, anti-spam adds a [spam] tag in the subject line and the body of the e-mail that has been identified as spam.
  - "x-mailscan-spam: 1" header line is added: actual spam content is embedded in body: this option helps you add a [spam] tag in the body of the e-mail that has been identified as spam. In addition, it adds a line in the header line of the e-mail.

- Only [spam] tag is added in subject: body is left unchanged: [default] this option helps you add the [spam] tag only in the subject of the e-mail, which has been identified as spam.
- "x-mailscan-spam: 1" header line is added: body and subject both remain unchanged: this option helps you add a header line to the e-mail. However, it does not add any tag to the subject line or body of the e-mail.

### Disclaimer

The disclaimer is a footer or signature that is appended to all e-mails. The disclaimer can be added in the space provided.



Disclaimer

□ Add Disclaimer to Outgoing Mails □ Add Disclaimer to Incoming Mails

Exclude Disclaimers in Mails to Following Receivers

listmanager@*
majordomo@*
subscribe@*
unsubscribe@*

**Figure 35**

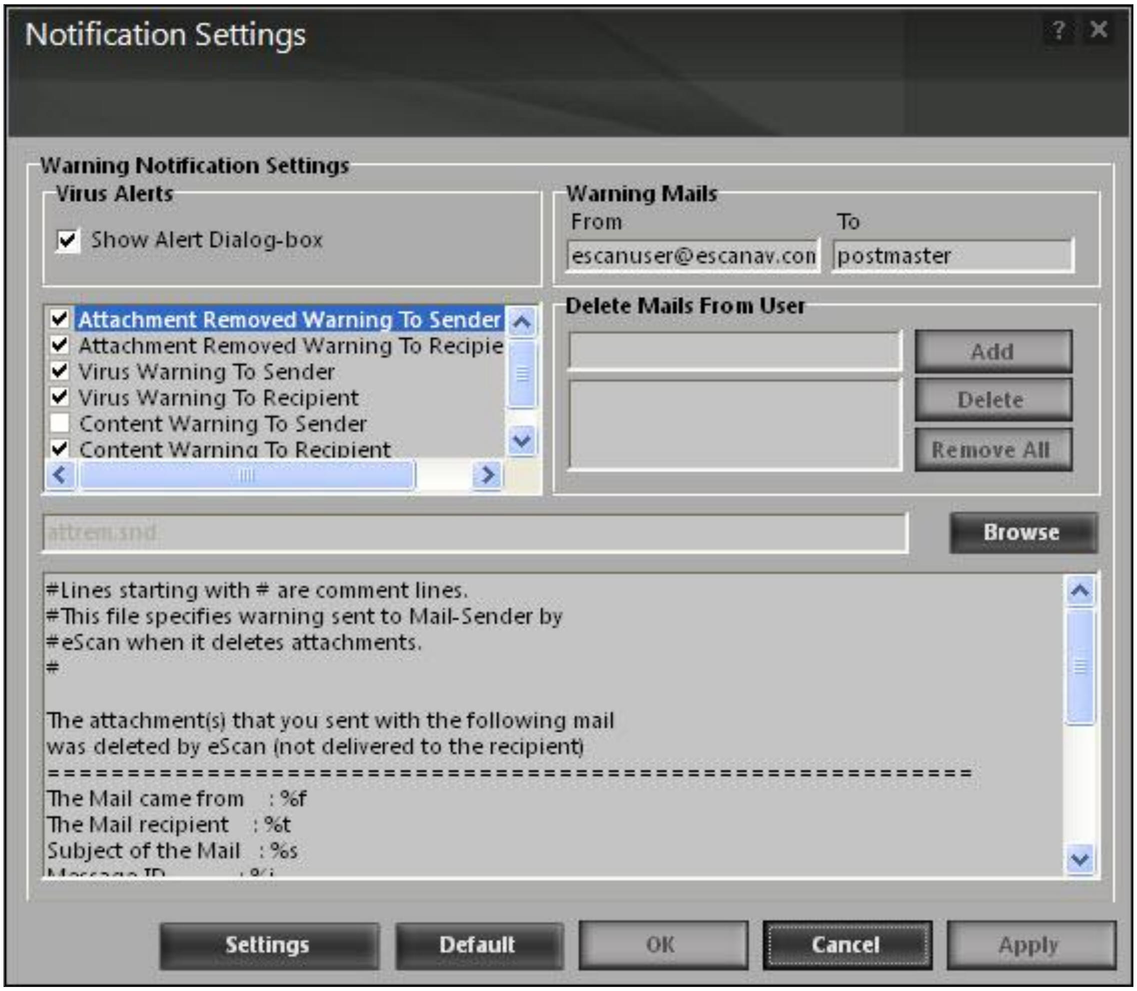
The disclaimer tab helps you configure the following settings.

- Add disclaimer to outgoing mails: select this check box if you want to add a disclaimer to all outgoing mails. This helps to make the recipient aware that the e-mail is scanned and free of viruses.

- Add disclaimer to incoming mails: select this check box if you want to add a disclaimer to all incoming mails. Thus, you make the recipient aware that the e-mail is scanned and free of viruses. You can add a custom disclaimer by either typing the text of the disclaimer in the disclaimer box or by selecting the file containing the disclaimer text by clicking browse.
- Exclude disclaimers in mails to following receivers: by default, this section appears dimmed, it is available only when you select add disclaimer to outgoing mails check box. It enables you to restrict anti-spam from appending the disclaimer to specific mail addresses or domains by adding them to a list.

Notification:

This button opens the notification settings dialog box. You can configure the notification settings for the anti-spam module by using this dialog box. By configuring this module, you can send e-mails to specific recipients when a particular event occurs.



Notification Settings

Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

Warning Mails

From: escanuser@escanav.con

To: postmaster

☑ Attachment Removed Warning To Sender
☑ Attachment Removed Warning To Recipie
☑ Virus Warning To Sender
☑ Virus Warning To Recipient
☐ Content Warning To Sender
☑ Content Warning To Recipient

Delete Mails From User

attrem.snd

```
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#eScan when it deletes attachments.
#

The attachment(s) that you sent with the following mail
was deleted by eScan (not delivered to the recipient)
==============================================================
The Mail came from    : %f
The Mail recipient    : %t
Subject of the Mail   : %s
```

Figure 36

The warning notification settings that you can configure on this screen are as follows:

- Virus alerts
    - Show alert dialog-box: [default] select this check box if you want anti-spam to display an alert box notifying you of a virus infection.
    - Attachment removed warning to sender: [default] select this check box if you want anti-spam to send a warning message to the sender of an infected attachment. Anti-spam sends this e-mail when it encounters a virus-infected attachment in an e-mail. The content of the e-mail that is sent is displayed in the preview box.
    - Attachment removed warning to recipient: [default] select this check box if you want anti-spam to send a warning message to the recipient when it removes an infected attachment. The content of the e-mail that is sent is displayed in the preview box.
    - Virus warning to sender: [default] select this check box if you want anti-spam to send a virus warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
    - Virus warning to recipient: [default] select this check box if you want anti-spam to send a virus warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
    - Content warning to sender: select this check box if you want anti-spam to send a content warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
    - Content warning to recipient: [default] select this check box if you want anti-spam to send a content warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- Warning mails: you can configure this setting if you want anti-spam to send warning e-mails and alerts to a given sender or recipient. The default sender (from field) is postmaster and the default recipient (to field) is postmaster.
- Delete mails from user: you can configure eScan to automatically delete mails that have been sent by specific users. For this, you need to add the e-mail addresses of such users to the delete mails from user list. By default, the delete mails from user section fields are unavailable, it is available only when you type in some text in the delete mails from user field and add mail addresses.

- Reports

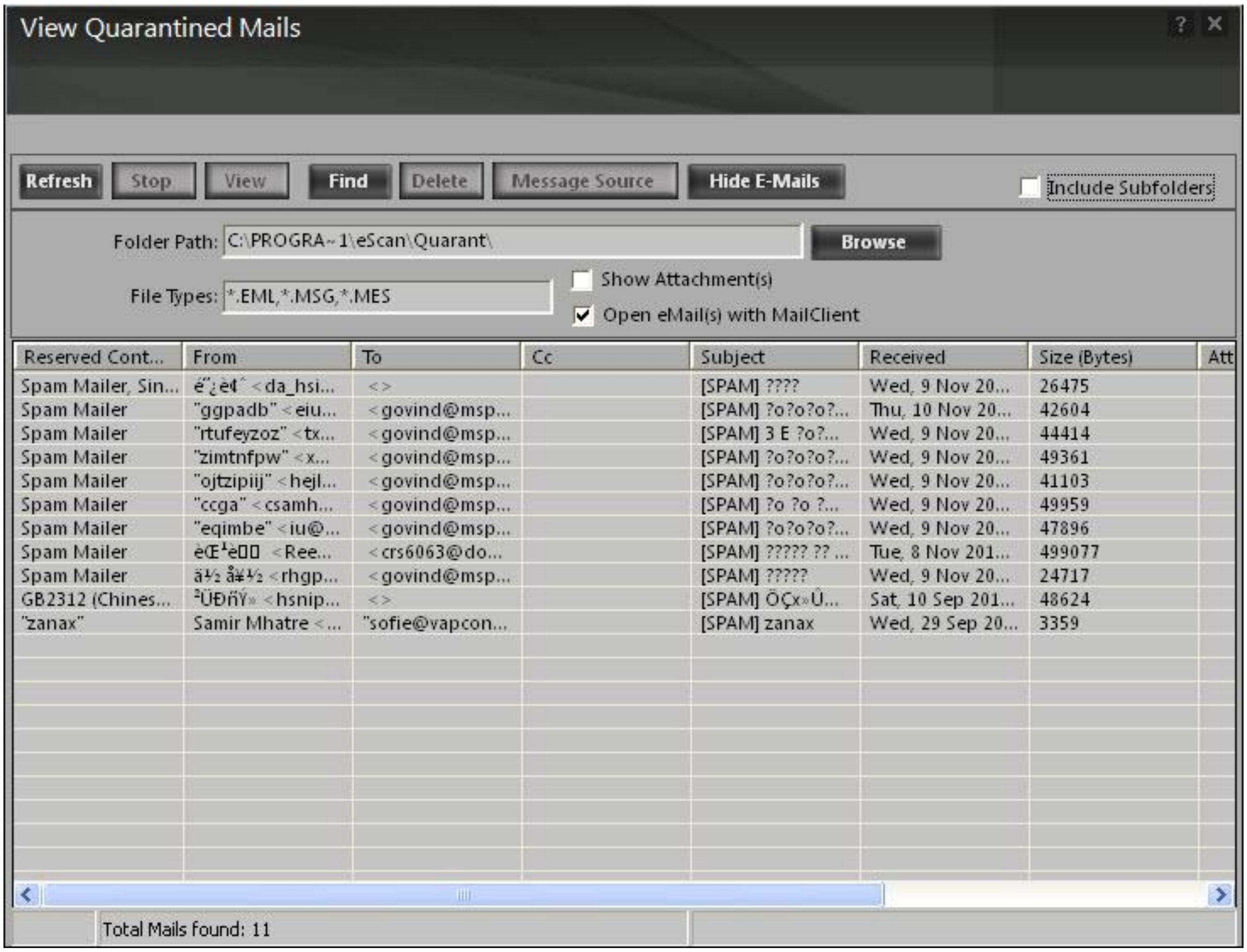
  This section displays the following information:

    - Total quarantined mails: it shows the total number of files scanned by the real-time anti-spam monitor.
    - Total clear mails: it shows the total number of viruses or malicious software detected by the anti-spam monitor on a real-time basis.

In addition, you can view the following reports:

View quarantined mails:

This button opens the view quarantined mails window, which displays the list of e-mails that have been quarantined by anti-spam. With the help of this window, you can configure the settings by specifying the path of the folder where you need to store the archived e-mails and specifying the format for storing e-mails. In addition, you can view the contents of e-mails, add sender's e-mail id to the white list or add reserve content of the selected e-mail to the hide e-mail list.



□ Include Subfolders

Folder Path: C:\PROGRA~1\eScan\Quarant\

File Types: *.EML,*.MSG,*.MES

□ Show Attachment(s)

☑ Open eMail(s) with MailClient

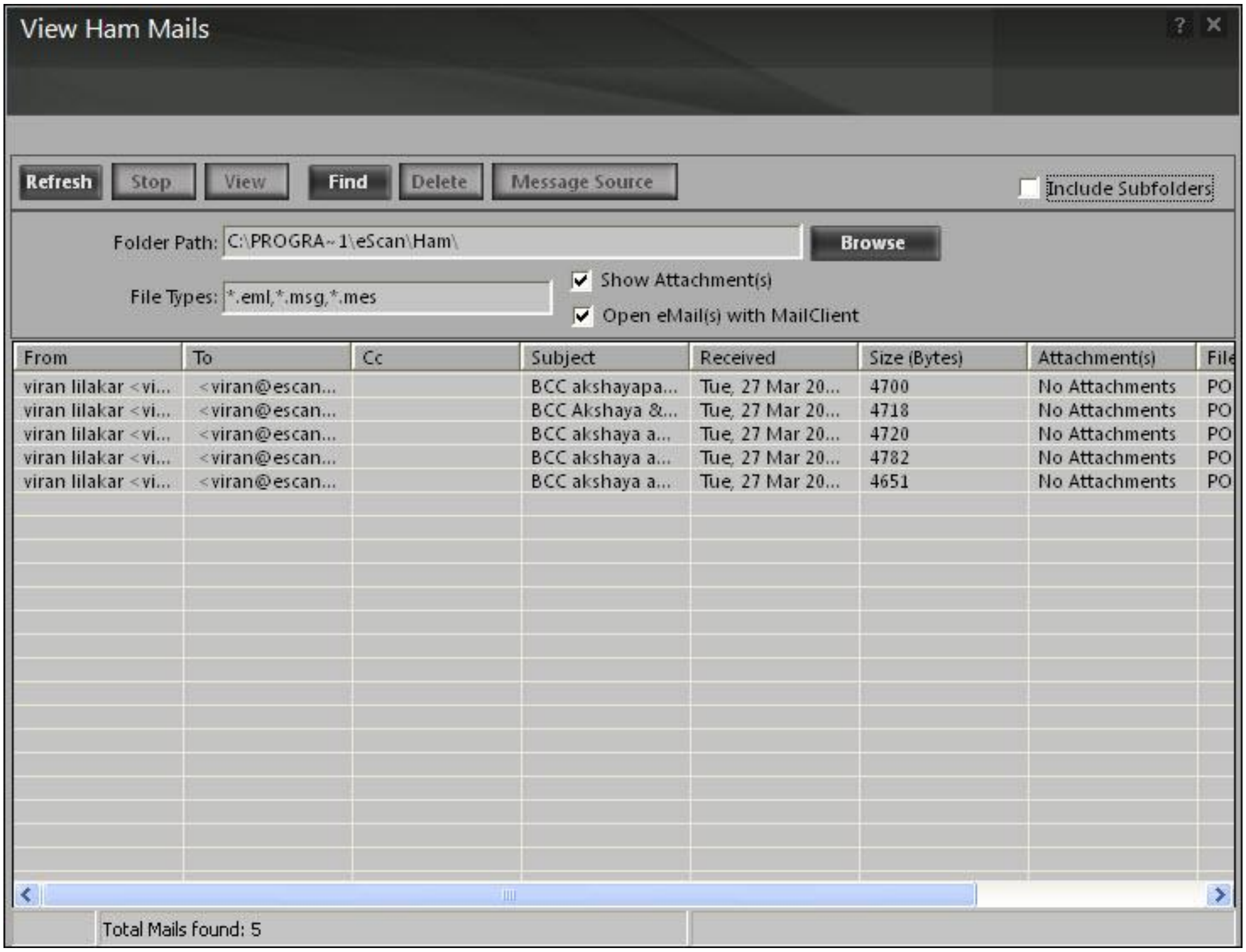
| Reserved Cont... | From | To | Cc | Subject | Received | Size (Bytes) | Att |
|---|---|---|---|---|---|---|---|
| Spam Mailer, Sin... | é"¿è¢ˆ <da_hsi... | <> | | [SPAM] ???? | Wed, 9 Nov 20... | 26475 | |
| Spam Mailer | "ggpadb" <eiu... | <govind@msp... | | [SPAM] ?o?o?o?... | Thu, 10 Nov 20... | 42604 | |
| Spam Mailer | "rtufeyzoz" <tx... | <govind@msp... | | [SPAM] 3 E ?o?... | Wed, 9 Nov 20... | 44414 | |
| Spam Mailer | "zimtnfpw" <x... | <govind@msp... | | [SPAM] ?o?o?o?... | Wed, 9 Nov 20... | 49361 | |
| Spam Mailer | "ojtzipiij" <hejl... | <govind@msp... | | [SPAM] ?o?o?o?... | Wed, 9 Nov 20... | 41103 | |
| Spam Mailer | "ccga" <csamh... | <govind@msp... | | [SPAM] ?o ?o ?... | Wed, 9 Nov 20... | 49959 | |
| Spam Mailer | "eqimbe" <iu@... | <govind@msp... | | [SPAM] ?o?o?o?... | Wed, 9 Nov 20... | 47896 | |
| Spam Mailer | èŒ¹è□□ <Ree... | <crs6063@do... | | [SPAM] ????? ?? ... | Tue, 8 Nov 201... | 499077 | |
| Spam Mailer | ä½ å¥½ <rhgp... | <govind@msp... | | [SPAM] ????? | Wed, 9 Nov 20... | 24717 | |
| GB2312 (Chines... | ²ÜÐñÝ» <hsnip... | <> | | [SPAM] ÖÇx»Û... | Sat, 10 Sep 201... | 48624 | |
| "zanax" | Samir Mhatre <... | "sofie@vapcon... | | [SPAM] zanax | Wed, 29 Sep 20... | 3359 | |

Total Mails found: 11

**Figure 37**

View ham mails:

This button opens the view ham mails window, which displays the report of all ham e-mails 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 e-mails and can also specify the format for storing e-mails.



□ Include Subfolders

Folder Path: C:\PROGRA~1\eScan\Ham\

File Types: *.eml,*.msg,*.mes

☑ Show Attachment(s)

☑ Open eMail(s) with MailClient

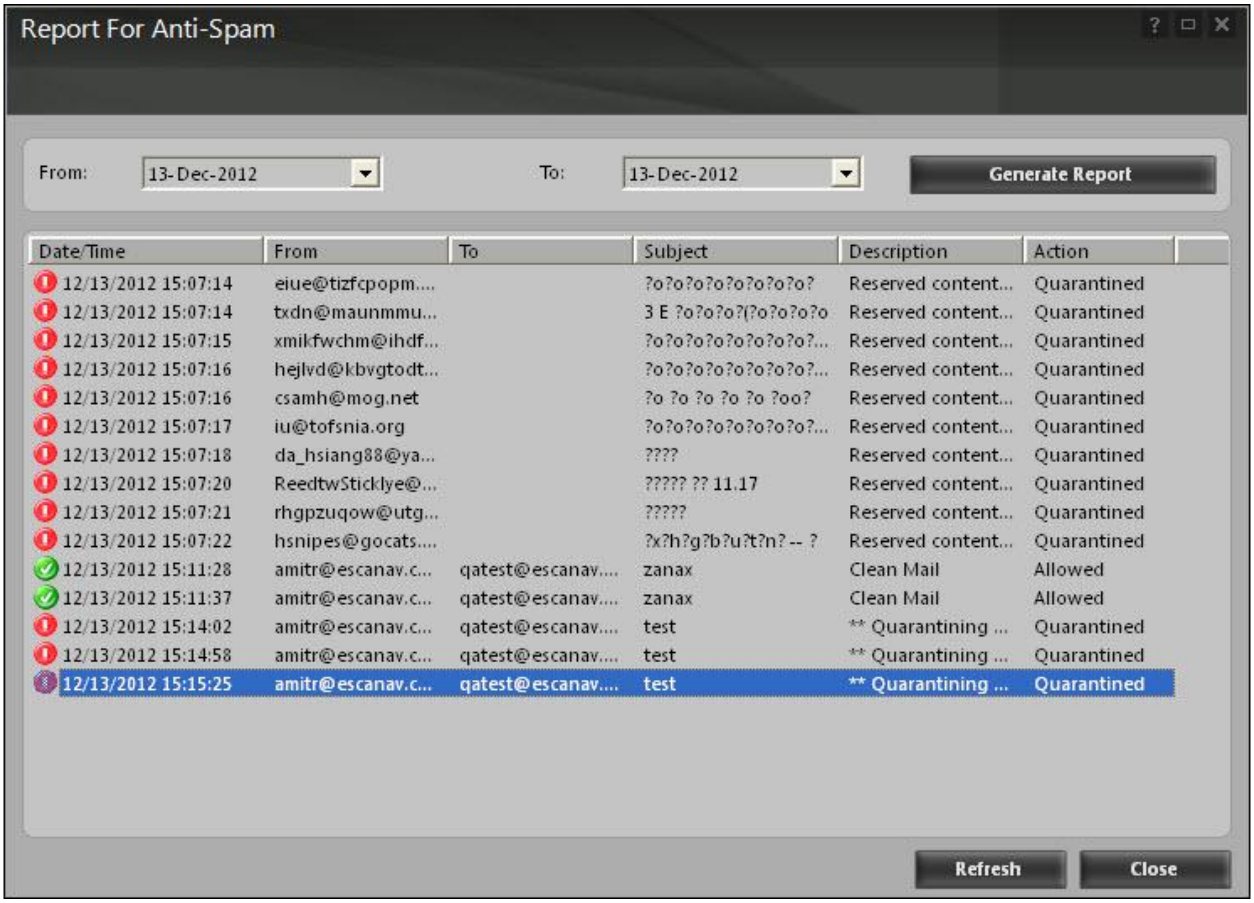
| From | To | Cc | Subject | Received | Size (Bytes) | Attachment(s) | File |
|---|---|---|---|---|---|---|---|
| viran lilakar <vi... | <viran@escan... | | BCC akshayapa... | Tue, 27 Mar 20... | 4700 | No Attachments | PO |
| viran lilakar <vi... | <viran@escan... | | BCC Akshaya &... | Tue, 27 Mar 20... | 4718 | No Attachments | PO |
| viran lilakar <vi... | <viran@escan... | | BCC akshaya a... | Tue, 27 Mar 20... | 4720 | No Attachments | PO |
| viran lilakar <vi... | <viran@escan... | | BCC akshaya a... | Tue, 27 Mar 20... | 4782 | No Attachments | PO |
| viran lilakar <vi... | <viran@escan... | | BCC akshaya a... | Tue, 27 Mar 20... | 4651 | No Attachments | PO |

Total Mails found: 5

**Figure 38**

View report:

This button displays the report for the anti-spam window. This window displays report for the anti-spam module for a given range of dates in a tabular format when you click the generate report button.



Report For Anti-Spam

From: 13-Dec-2012

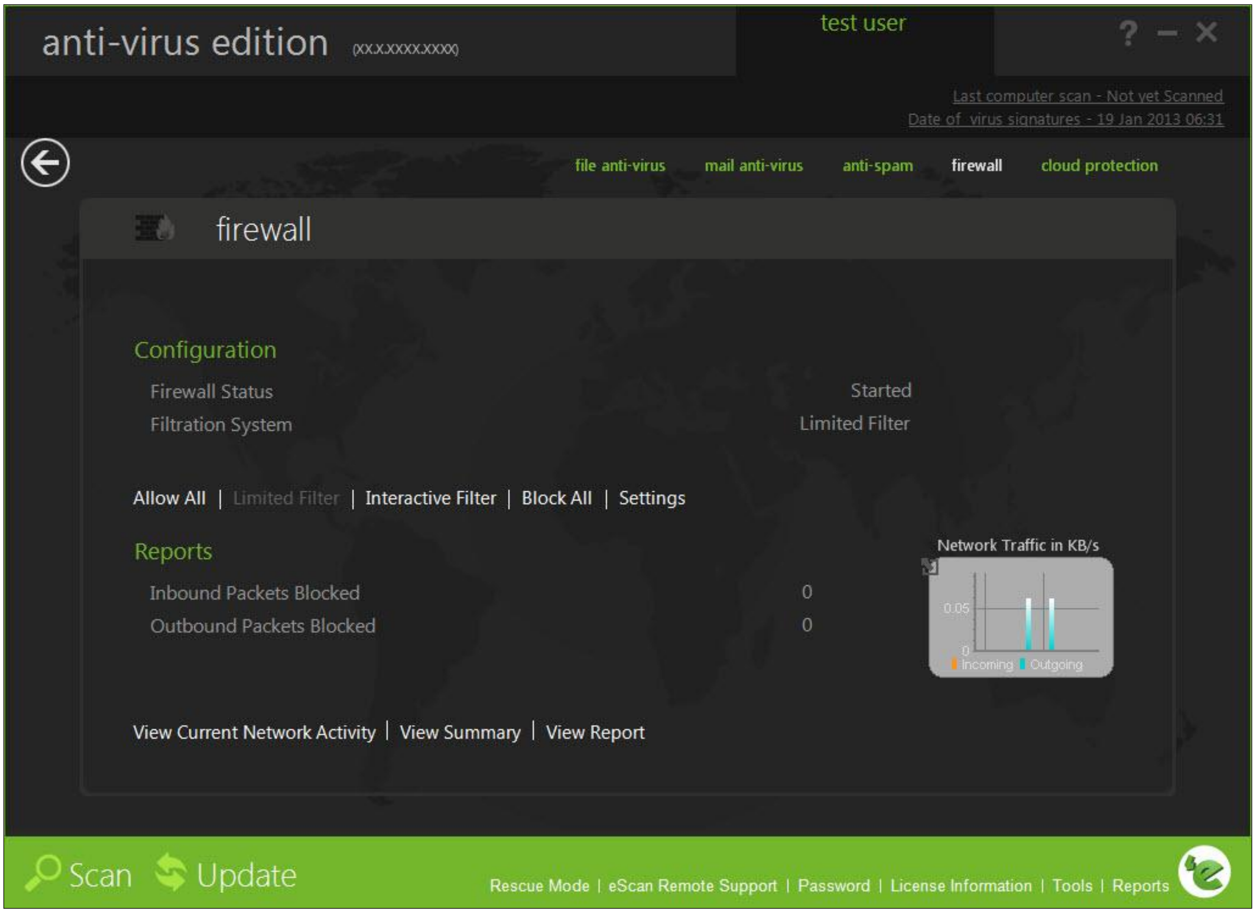
To: 13-Dec-2012

| Date/Time | From | To | Subject | Description | Action |
|---|---|---|---|---|---|
| ! 12/13/2012 15:07:14 | eiue@tizfcpopm.... | | ?o?o?o?o?o?o?o? | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:14 | txdn@maunmmu... | | 3 E ?o?o?o?(?o?o?o?o | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:15 | xmikfwchm@ihdf... | | ?o?o?o?o?o?o?o?... | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:16 | hejlvd@kbvgtodt... | | ?o?o?o?o?o?o?o?... | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:16 | csamh@mog.net | | ?o ?o ?o ?o ?o ?oo? | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:17 | iu@tofsnia.org | | ?o?o?o?o?o?o?o?... | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:18 | da_hsiang88@ya... | | ???? | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:20 | ReedtwSticklye@... | | ????? ?? 11.17 | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:21 | rhgpzuqow@utg... | | ????? | Reserved content... | Quarantined |
| ! 12/13/2012 15:07:22 | hsnipes@gocats.... | | ?x?h?g?b?u?t?n? -- ? | Reserved content... | Quarantined |
| ✓ 12/13/2012 15:11:28 | amitr@escanav.c... | qatest@escanav.... | zanax | Clean Mail | Allowed |
| ✓ 12/13/2012 15:11:37 | amitr@escanav.c... | qatest@escanav.... | zanax | Clean Mail | Allowed |
| ! 12/13/2012 15:14:02 | amitr@escanav.c... | qatest@escanav.... | test | ** Quarantining ... | Quarantined |
| ! 12/13/2012 15:14:58 | amitr@escanav.c... | qatest@escanav.... | test | ** Quarantining ... | Quarantined |
| ● 12/13/2012 15:15:25 | amitr@escanav.c... | qatest@escanav.... | test | ** Quarantining ... | Quarantined |

**Figure 39**

# Firewall

Firewall is the fourth module of the eScan for av. It is designed to monitor all incoming and outgoing network traffic and protect your computer from all types of network-based attacks. EScan includes a set of 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.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ✕
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
firewall
Allow All | Limited Filter | Interactive Filter | Block All | Settings
Network Traffic in KB/s
0.05
0
Incoming
Outgoing
View Current Network Activity | View Summary | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - Not yet Scanned
Date of virus signatures - 19 Jan 2013 06:31

Configuration

| | |
|---|---|
| Firewall Status | Started |
| Filtration System | Limited Filter |

Reports

| | |
|---|---|
| Inbound Packets Blocked | 0 |
| Outbound Packets Blocked | 0 |

**Figure 40**

Benefits of the firewall feature

When you connect to the internet, you expose your computer to various security threats. The firewall feature of eScan protects your data when you:

- Connect to internet relay chat (irc) servers and join other people on the numerous channels on the irc network.
- Use telnet to connect to a server on the internet and then execute the commands on the server.
- Use ftp to transfer files from a remote server to your computer.
- Use network basic input/output system (netbios) to communicate with other users on the lan 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 e-mail.

By default, the firewall operates in the allow all mode. However, you can customize the firewall by using options like limited filter for filtering only incoming traffic and interactive filter to turn off and block all. The eScan firewall also allows you to specify different set of rules for allowing or blocking incoming or outgoing traffic.

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

- Configuration

  This section displays the following information:

  - Firewall status: it shows whether the firewall module is running or not. By default, firewall runs in the allow all mode.
  - Filtration system: it shows the filtration system in use by firewall module.

Allow all: [default]

Click this option, if you want to disable firewall.

Limited filter:

You can click this option to enable the limited filter mode. When the firewall module is in this mode, it monitors all incoming traffic and helps you allow or block traffic as per the defined conditions or rules.

Interactive filter:

You can click this option to enable the interactive filter mode. When the firewall module is in this mode, it needs user intervention. It monitors all the incoming and outgoing network traffic and allows or blocks traffic as per your choice.

Block all:

You can click this button to block all the incoming and outgoing network traffic.

Settings:

When you click this button, 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, which are as follows:

✍ On below the screen of all the tabs contains four buttons — default, ok, cancel, and apply, which you have to use after configuring the settings based on your requirement.

Default: click this button to apply the default settings.

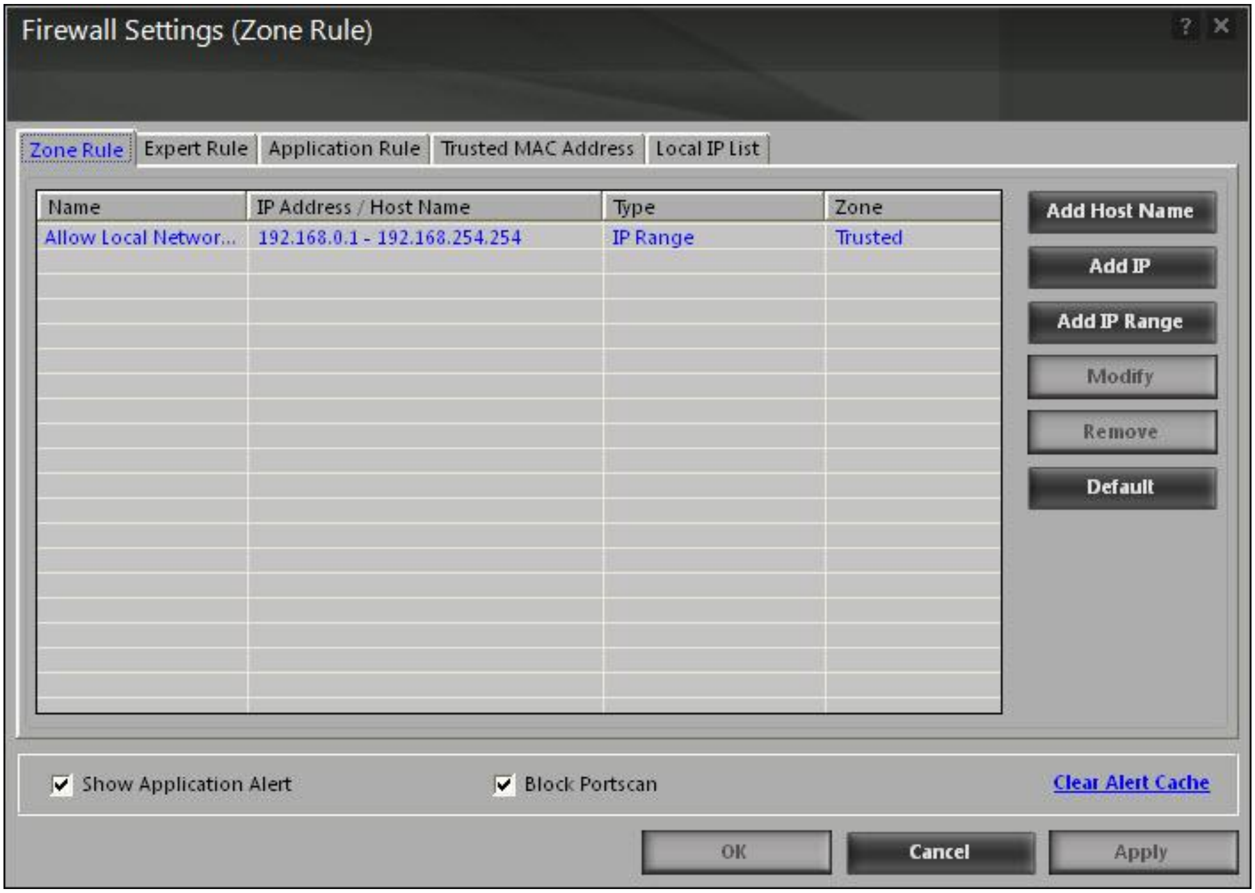
Ok: click this button after you click the apply button to apply the configured settings.

Cancel: click this button to cancel the configured settings or to close the window.

Apply: click this button to apply the configured settings.

### Zone rule

This tab contain settings that help you configure network access rules that specify which ip address, host name, or ip range of computers can access your computer.



Firewall Settings (Zone Rule)

| Name | IP Address / Host Name | Type | Zone |
|---|---|---|---|
| Allow Local Networ... | 192.168.0.1 - 192.168.254.254 | IP Range | Trusted |

☑ Show Application Alert

☑ Block Portscan

**Figure 41**

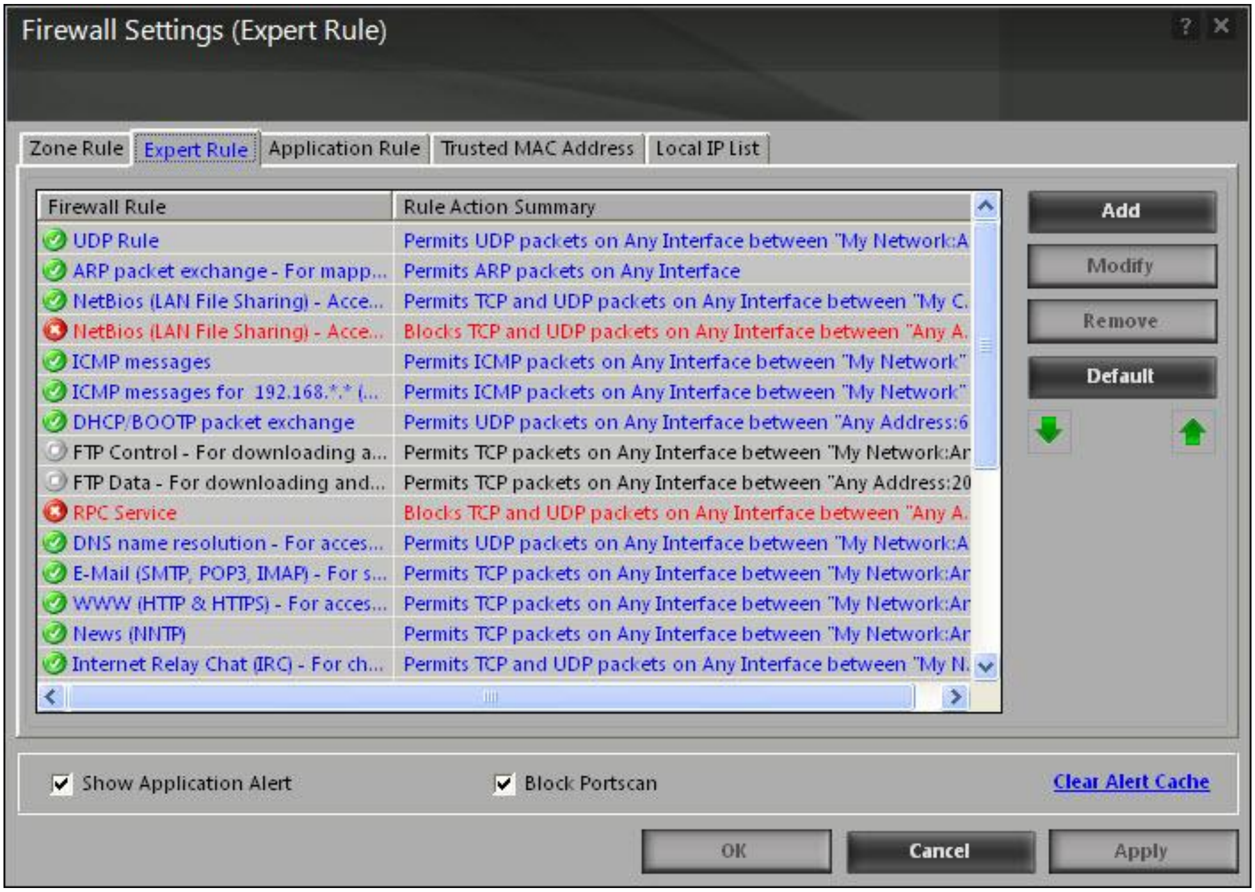
This tab includes the following buttons:

- Add host name: you can click this button 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.
- Add ip: you can click this button 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.
- Add ip range: you can click this button 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.

- Modify: you can click this button to modify zone rules related to the host name, ip address, or range of ip addresses.

### Expert rule

This tab allows you to specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source ip address and port, destination ip address and port, and icmp types.  You can create new expert rules. However, you should configure these rules only if you have a good understanding of firewalls and networking protocols.



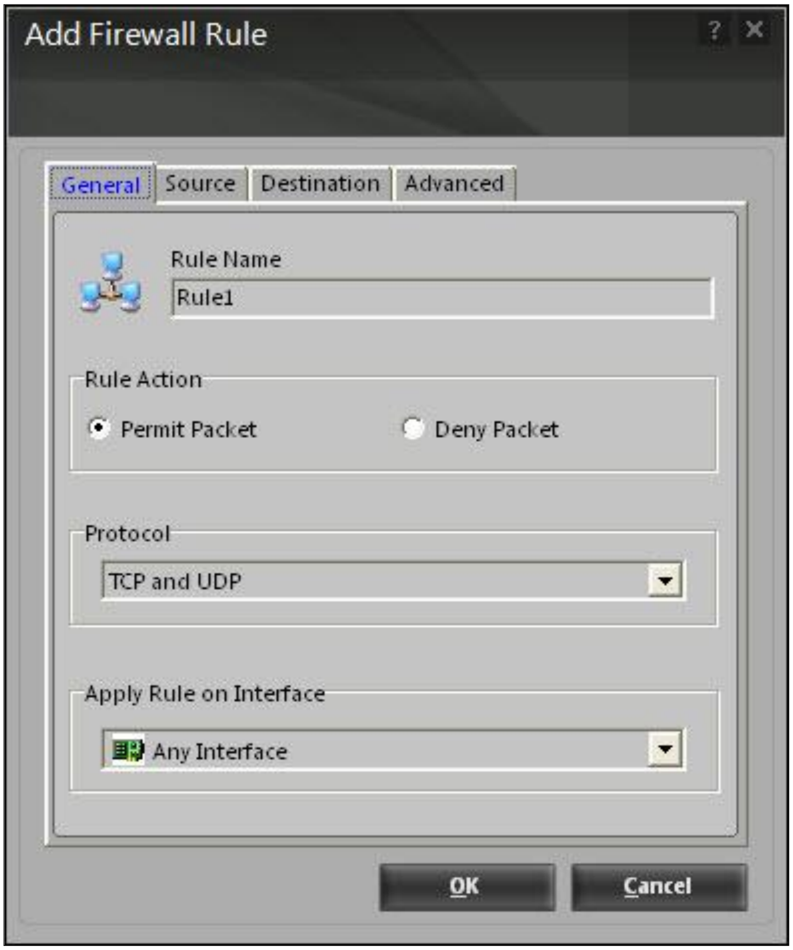
| Firewall Rule | Rule Action Summary |
|---|---|
| ✓ UDP Rule | Permits UDP packets on Any Interface between "My Network:A |
| ✓ ARP packet exchange - For mapp... | Permits ARP packets on Any Interface |
| ✓ NetBios (LAN File Sharing) - Acce... | Permits TCP and UDP packets on Any Interface between "My C. |
| ✗ NetBios (LAN File Sharing) - Acce... | Blocks TCP and UDP packets on Any Interface between "Any A. |
| ✓ ICMP messages | Permits ICMP packets on Any Interface between "My Network" |
| ✓ ICMP messages for 192.168.*.* (... | Permits ICMP packets on Any Interface between "My Network" |
| ✓ DHCP/BOOTP packet exchange | Permits UDP packets on Any Interface between "Any Address:6 |
| ○ FTP Control - For downloading a... | Permits TCP packets on Any Interface between "My Network:Ar |
| ○ FTP Data - For downloading and... | Permits TCP packets on Any Interface between "Any Address:20 |
| ✗ RPC Service | Blocks TCP and UDP packets on Any Interface between "Any A. |
| ✓ DNS name resolution - For acces... | Permits UDP packets on Any Interface between "My Network:A |
| ✓ E-Mail (SMTP, POP3, IMAP) - For s... | Permits TCP packets on Any Interface between "My Network:Ar |
| ✓ WWW (HTTP & HTTPS) - For acces... | Permits TCP packets on Any Interface between "My Network:Ar |
| ✓ News (NNTP) | Permits TCP packets on Any Interface between "My Network:Ar |
| ✓ Internet Relay Chat (IRC) - For ch... | Permits TCP and UDP packets on Any Interface between "My N. |

☑ Show Application Alert

☑ Block Portscan

**Figure 42**

- Click the add button to add new rules. The add firewall rule window appears.



Add Firewall Rule

Rule Name: Rule1

Rule Action: ● Permit Packet ○ Deny Packet

Protocol: TCP and UDP

Apply Rule on Interface: Any Interface

**Figure 43**

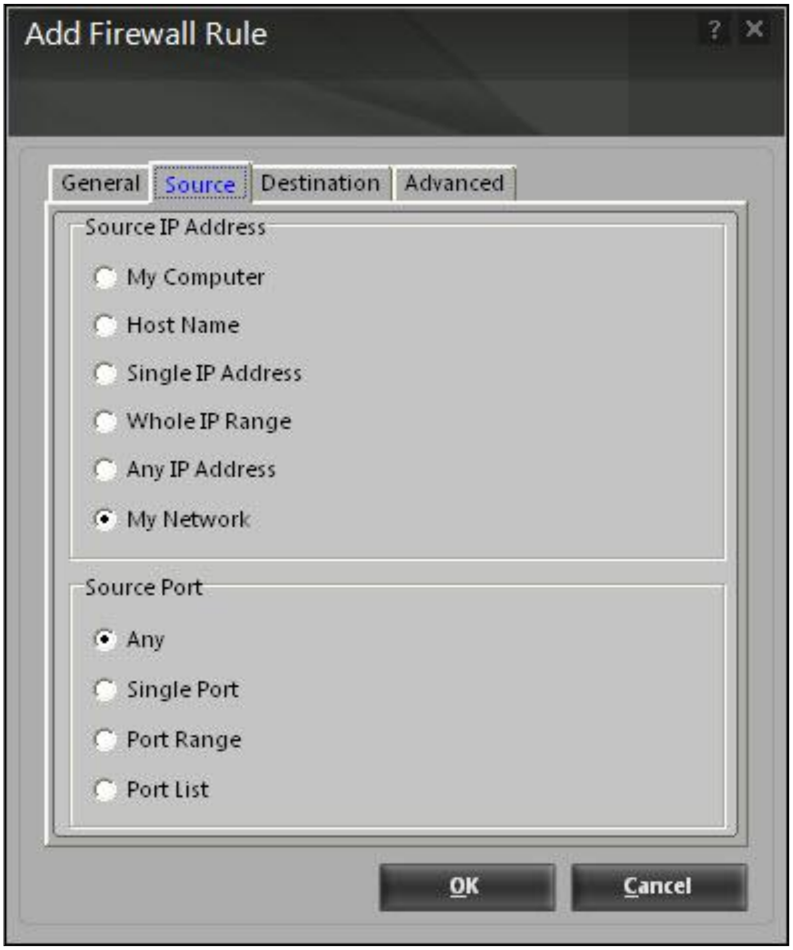
## General

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

- Rule name: type the rule name.
- Rule action: click any one of the following types of actions for setting rules.
  - Permit packet: [default] click this option, if you want to permit packets.
  - Deny packet: click this option, if you want to deny packets.
- Protocol: select an appropriate type of protocol from the drop-down list. By default, tcp and udp is selected.
- Apply rule on interface: select an appropriate rule that you want to apply on interface from the drop-down list. By default, any interface is selected.

- **Source**

This tab enables you to type the source ip address and port wherever applicable. Click an appropriate option. By default, my network under source ip address section and any under source port section are selected.



Add Firewall Rule

Source IP Address

○ My Computer
○ Host Name
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

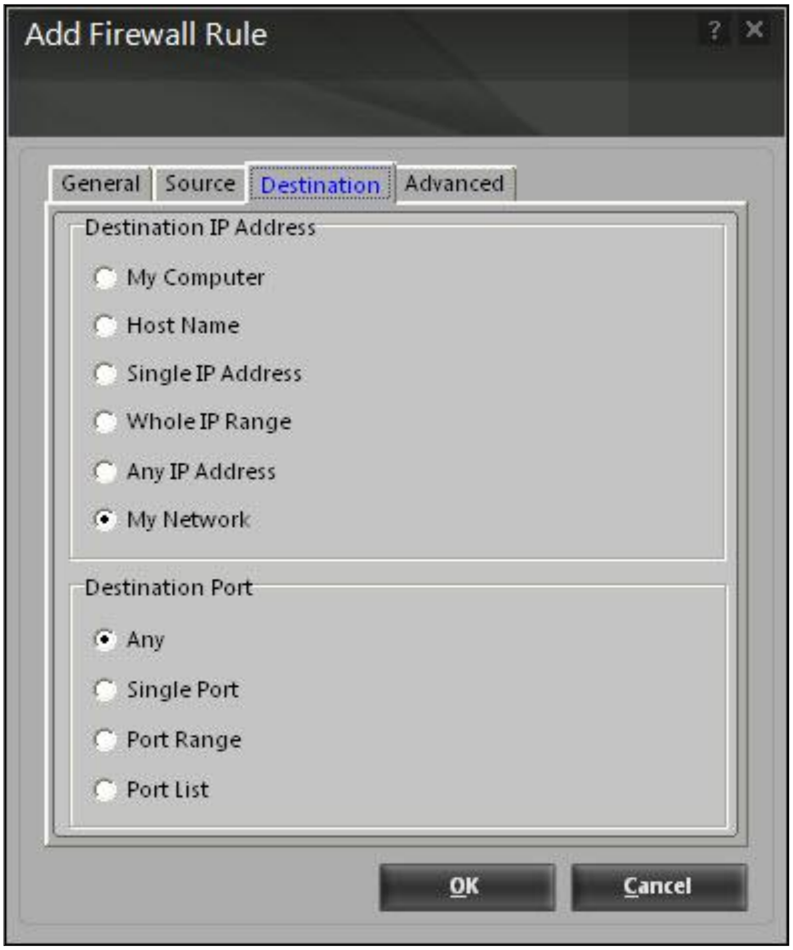
Source Port

● Any
○ Single Port
○ Port Range
○ Port List

**Figure 44**

- **Destination**

This tab enables you to type the destination ip address and port wherever applicable. Click an appropriate option. By default, my network under destination ip address section and any under destination port section are selected.



Add Firewall Rule

Destination IP Address

○ My Computer
○ Host Name
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

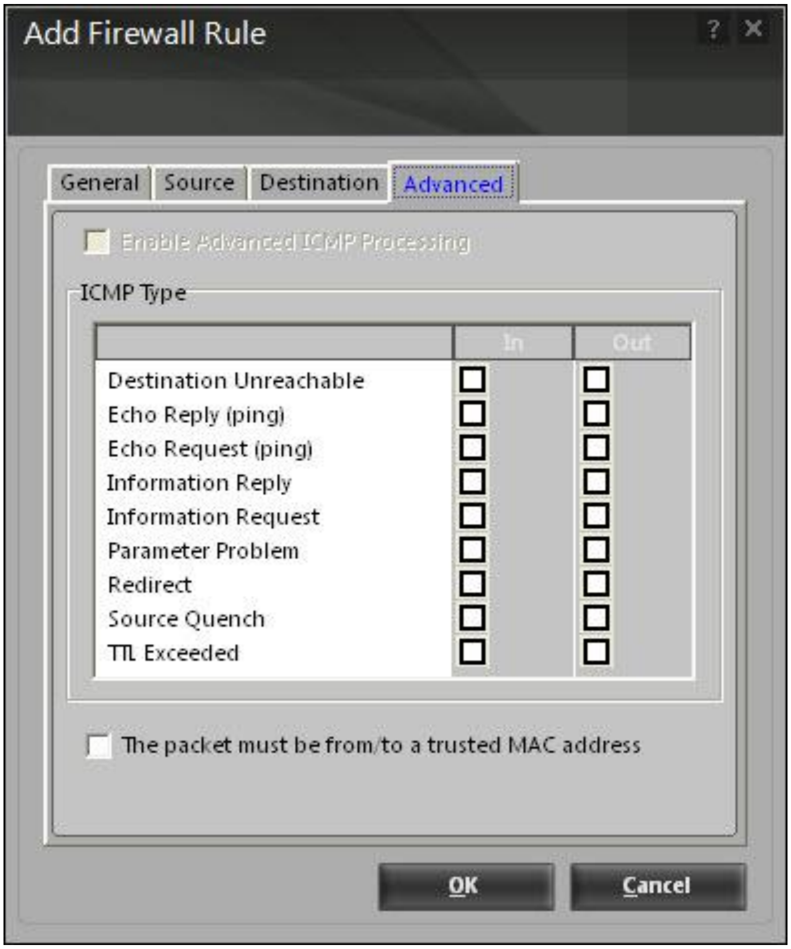
Destination Port

● Any
○ Single Port
○ Port Range
○ Port List

Figure 45

- **Advanced**

This tab is specifically meant for icmp processing, the fields on this tab are available only when you select icmp from protocol drop-down list, under general tab.



☐ Enable Advanced ICMP Processing

ICMP Type

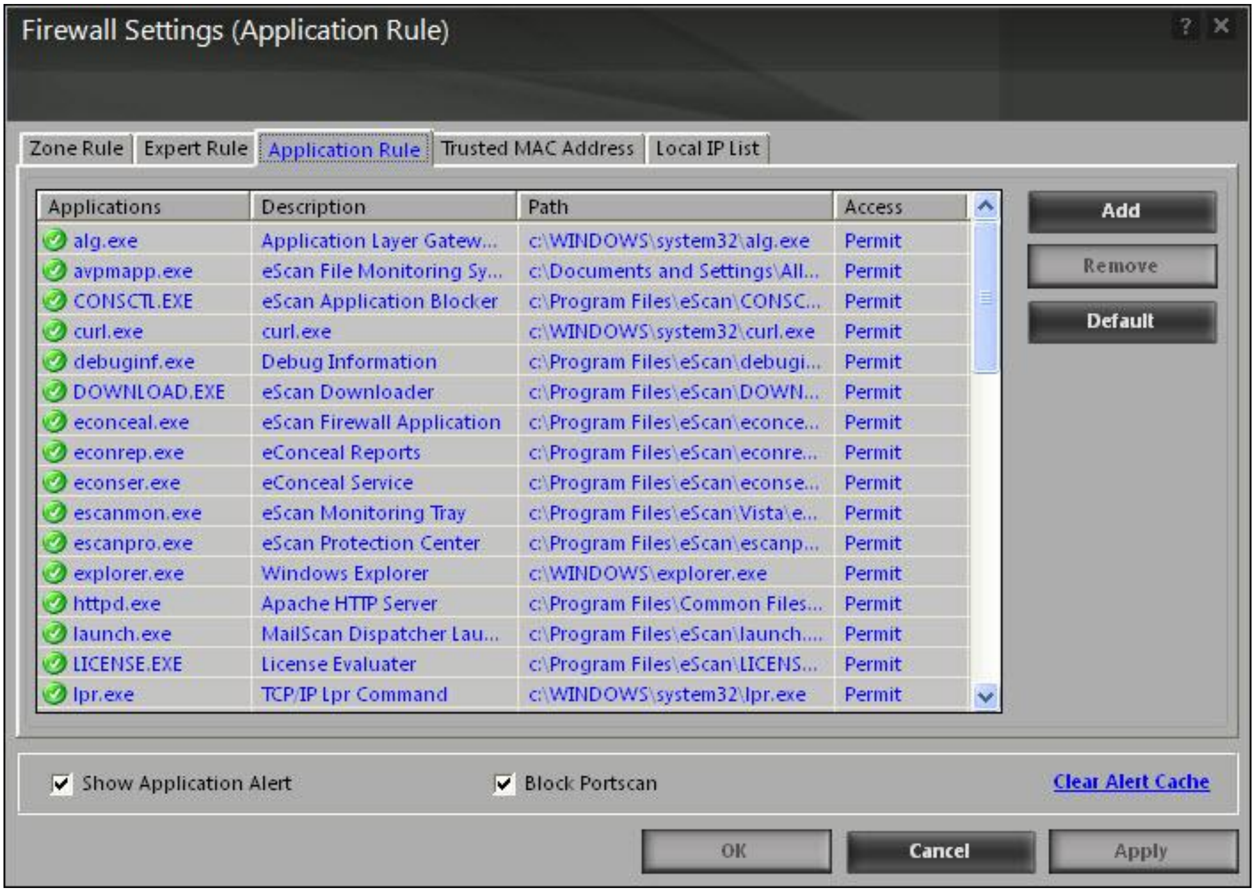
| | In | Out |
|---|---|---|
| Destination Unreachable | ☐ | ☐ |
| Echo Reply (ping) | ☐ | ☐ |
| Echo Request (ping) | ☐ | ☐ |
| Information Reply | ☐ | ☐ |
| Information Request | ☐ | ☐ |
| Parameter Problem | ☐ | ☐ |
| Redirect | ☐ | ☐ |
| Source Quench | ☐ | ☐ |
| TTL Exceeded | ☐ | ☐ |

☐ The packet must be from/to a trusted MAC address

Figure 46

- **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 and options for configuring application rules. While adding a new application rule, you must provide path of the application for which the rule is to be applied and to specify whether firewall module should allow the application to run.



| Applications | Description | Path | Access |
|---|---|---|---|
| alg.exe | Application Layer Gatew... | c:\WINDOWS\system32\alg.exe | Permit |
| avpmapp.exe | eScan File Monitoring Sy... | c:\Documents and Settings\All... | Permit |
| CONSCTL.EXE | eScan Application Blocker | c:\Program Files\eScan\CONSC... | Permit |
| curl.exe | curl.exe | c:\WINDOWS\system32\curl.exe | Permit |
| debuginf.exe | Debug Information | c:\Program Files\eScan\debugi... | Permit |
| DOWNLOAD.EXE | eScan Downloader | c:\Program Files\eScan\DOWN... | Permit |
| econceal.exe | eScan Firewall Application | c:\Program Files\eScan\econce... | Permit |
| econrep.exe | eConceal Reports | c:\Program Files\eScan\econre... | Permit |
| econser.exe | eConceal Service | c:\Program Files\eScan\econse... | Permit |
| escanmon.exe | eScan Monitoring Tray | c:\Program Files\eScan\Vista\e... | Permit |
| escanpro.exe | eScan Protection Center | c:\Program Files\eScan\escanp... | Permit |
| explorer.exe | Windows Explorer | c:\WINDOWS\explorer.exe | Permit |
| httpd.exe | Apache HTTP Server | c:\Program Files\Common Files... | Permit |
| launch.exe | MailScan Dispatcher Lau... | c:\Program Files\eScan\launch.... | Permit |
| LICENSE.EXE | License Evaluater | c:\Program Files\eScan\LICENS... | Permit |
| lpr.exe | TCP/IP Lpr Command | c:\WINDOWS\system32\lpr.exe | Permit |

☑ Show Application Alert

☑ Block Portscan

**Figure 47**

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

- 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 tab contains information on the mac addresses of devices connected to the computer. A mac address is a hardware address that uniquely identifies each node of a network. The trusted mac address list is checked along with the expert rule only when the packet must be from/to a trusted mac address check box is selected in the add firewall rule dialog box and the action is as per the action specified in the rule.

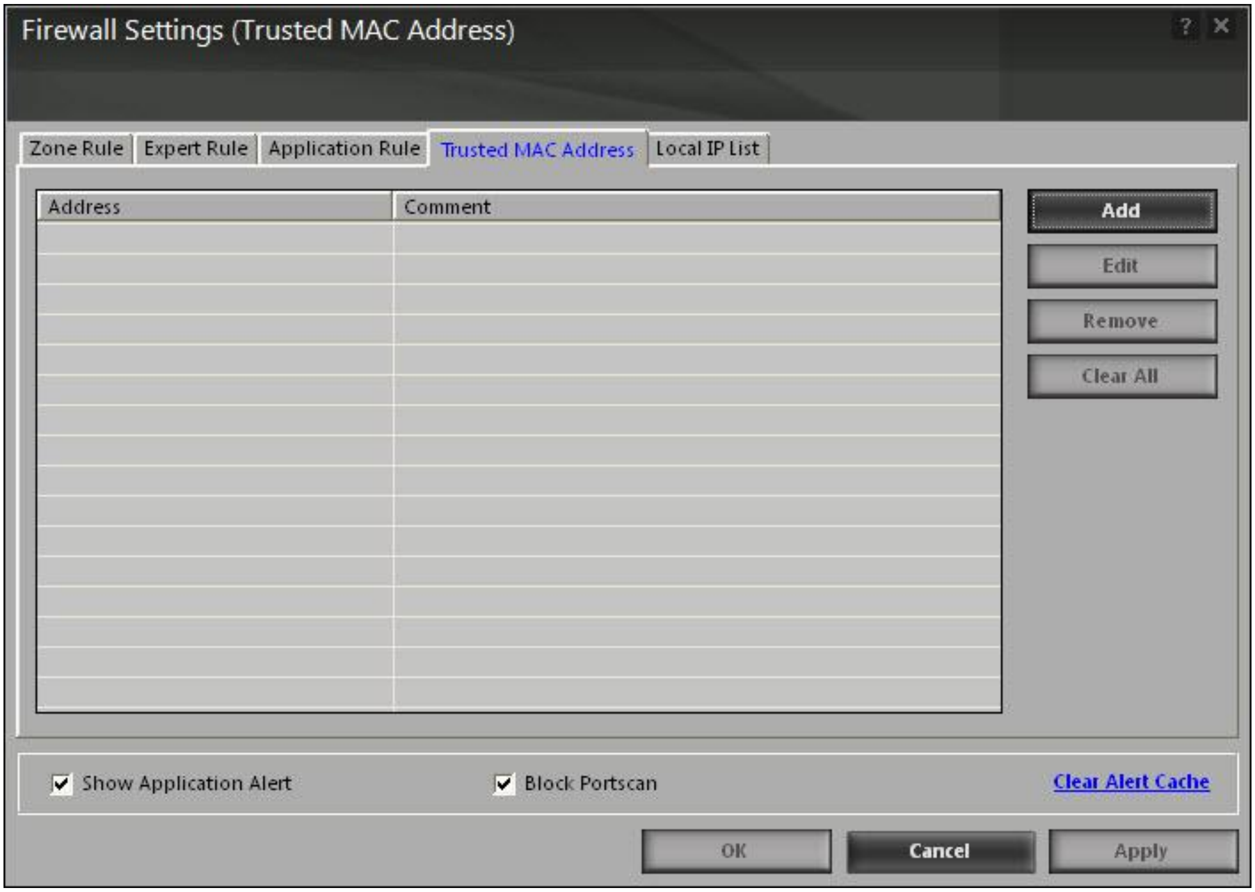
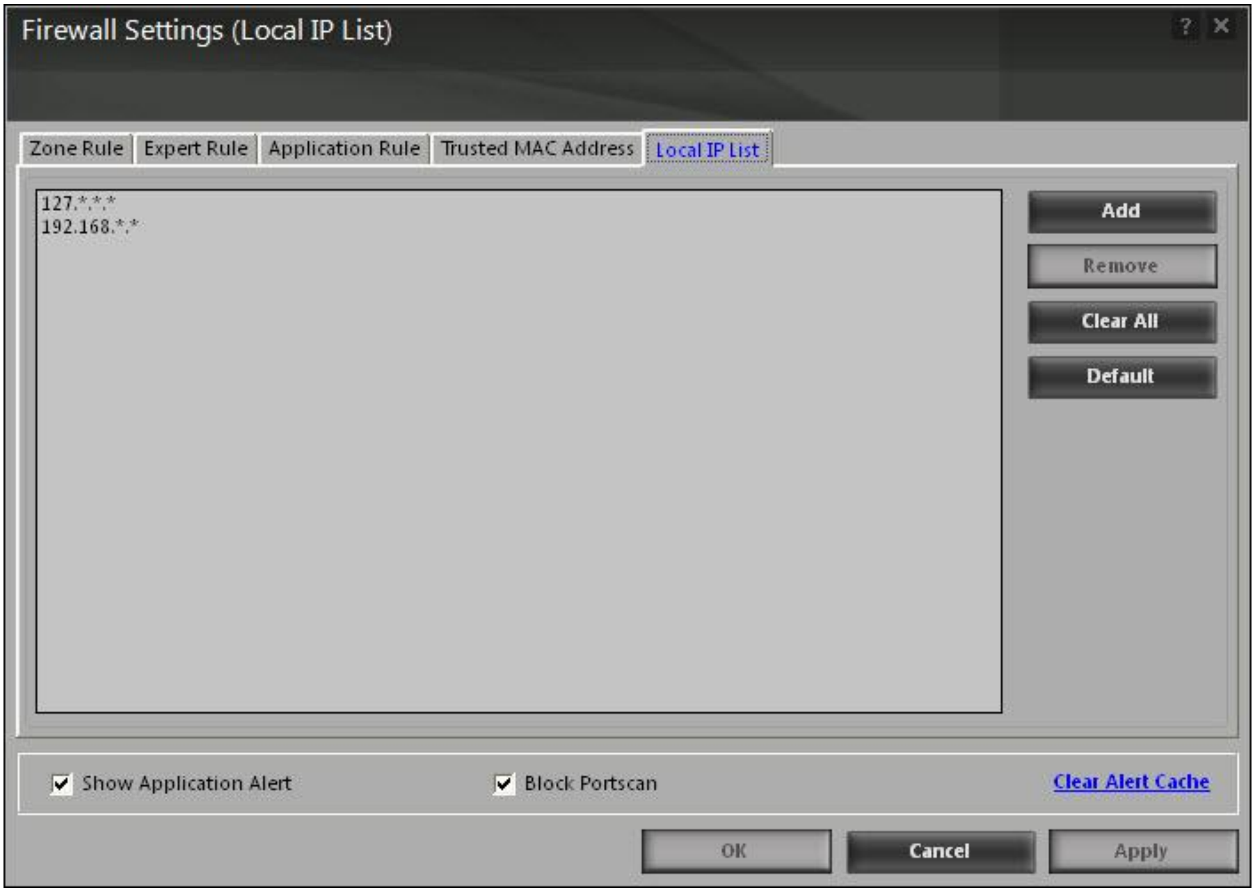


Figure 48

- ## Local ip list

This tab displays the list of all local ip addresses. You can configure the following setting:



127.*.*.*
192.168.*.*

☑ Show Application Alert

☑ Block Portscan

Figure 49

- Show application alert: [default] select this check box, if you want to receive firewall alert when an application is blocked as per an application rule.
- Block portscan: [default] select this check box, if you want to block port scanning. This feature helps you to protect your system from being hacked by hackers using ports.
- 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 section displays the following information:

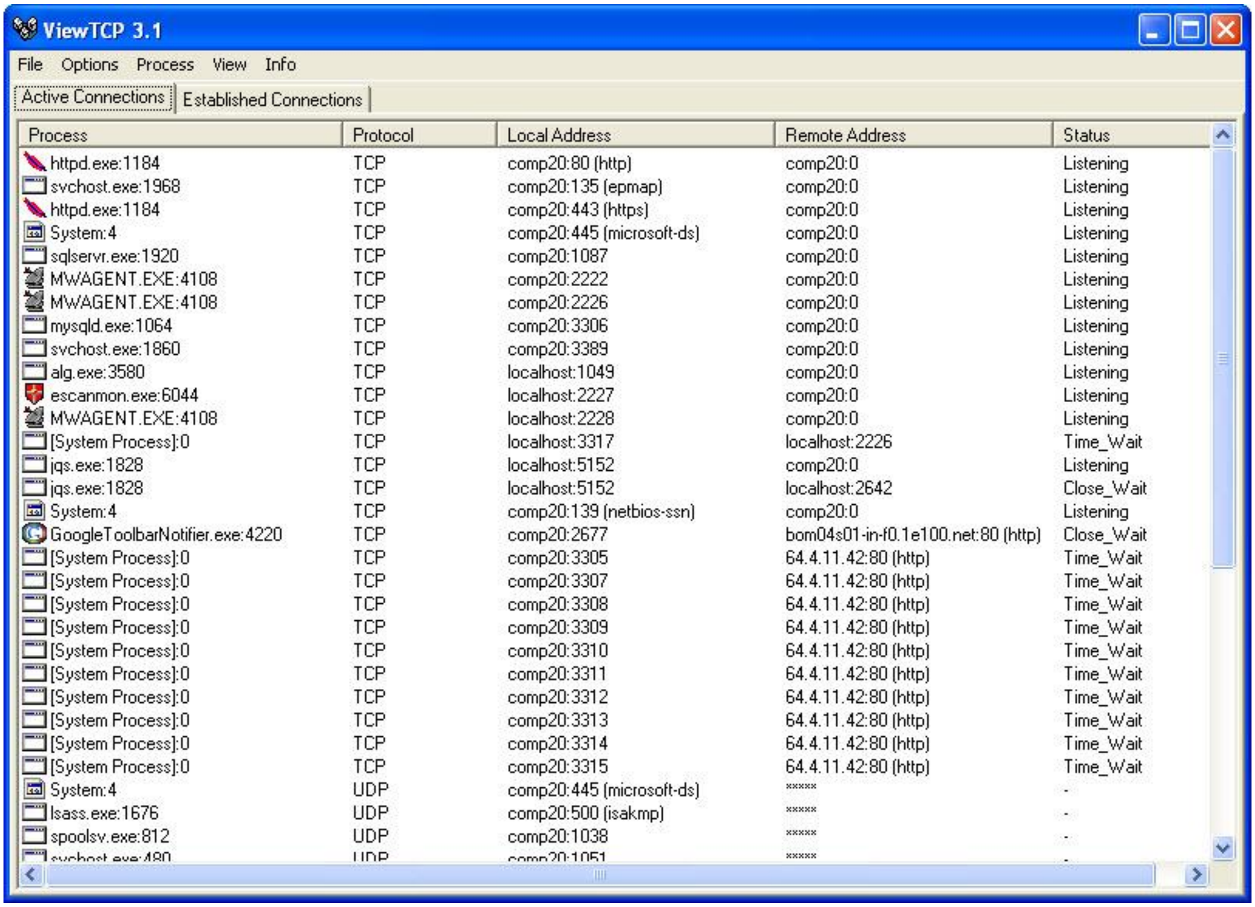
  - Inbound packets blocked: it shows the total number of inbound packets that were blocked by the firewall.
  - Outbound packets blocked: it shows the total number of outbound packets that were blocked by the firewall.

The report section also contains a network traffic graph, which shows the incoming and outgoing network traffic in kilobytes per second (kbps).

In addition, you can view the following reports:

View current network activity:

You can click this button to open the viewtcp 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.



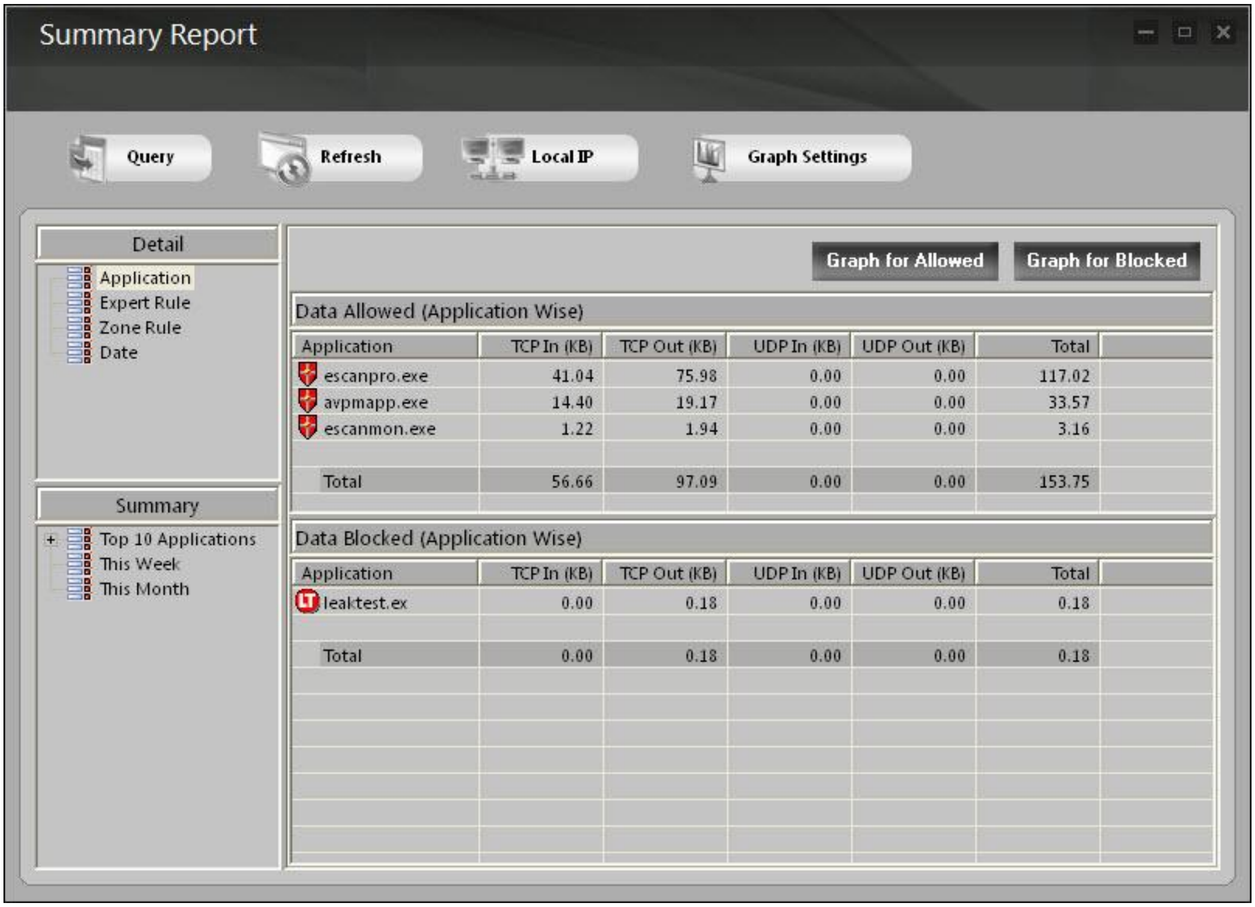
| Process | Protocol | Local Address | Remote Address | Status |
|---|---|---|---|---|
| httpd.exe:1184 | TCP | comp20:80 (http) | comp20:0 | Listening |
| svchost.exe:1968 | TCP | comp20:135 (epmap) | comp20:0 | Listening |
| httpd.exe:1184 | TCP | comp20:443 (https) | comp20:0 | Listening |
| System:4 | TCP | comp20:445 (microsoft-ds) | comp20:0 | Listening |
| sqlservr.exe:1920 | TCP | comp20:1087 | comp20:0 | Listening |
| MWAGENT.EXE:4108 | TCP | comp20:2222 | comp20:0 | Listening |
| MWAGENT.EXE:4108 | TCP | comp20:2226 | comp20:0 | Listening |
| mysqld.exe:1064 | TCP | comp20:3306 | comp20:0 | Listening |
| svchost.exe:1860 | TCP | comp20:3389 | comp20:0 | Listening |
| alg.exe:3580 | TCP | localhost:1049 | comp20:0 | Listening |
| escanmon.exe:6044 | TCP | localhost:2227 | comp20:0 | Listening |
| MWAGENT.EXE:4108 | TCP | localhost:2228 | comp20:0 | Listening |
| [System Process]:0 | TCP | localhost:3317 | localhost:2226 | Time_Wait |
| jqs.exe:1828 | TCP | localhost:5152 | comp20:0 | Listening |
| jqs.exe:1828 | TCP | localhost:5152 | localhost:2642 | Close_Wait |
| System:4 | TCP | comp20:139 (netbios-ssn) | comp20:0 | Listening |
| GoogleToolbarNotifier.exe:4220 | TCP | comp20:2677 | bom04s01-in-f0.1e100.net:80 (http) | Close_Wait |
| [System Process]:0 | TCP | comp20:3305 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3307 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3308 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3309 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3310 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3311 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3312 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3313 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3314 | 64.4.11.42:80 (http) | Time_Wait |
| [System Process]:0 | TCP | comp20:3315 | 64.4.11.42:80 (http) | Time_Wait |
| System:4 | UDP | comp20:445 (microsoft-ds) | ***** | - |
| lsass.exe:1676 | UDP | comp20:500 (isakmp) | ***** | - |
| spoolsv.exe:812 | UDP | comp20:1038 | ***** | - |
| svchost.exe:480 | UDP | comp20:1051 | ***** | - |

Figure 50

View summary:

You can click this button to view the firewall report either in the form of detailed report or a summary report.

A summary report displays information regarding the rules that has been invoked and applied by the firewall. These rules may include application rules, expert rules, and zone rules.



Data Allowed (Application Wise)

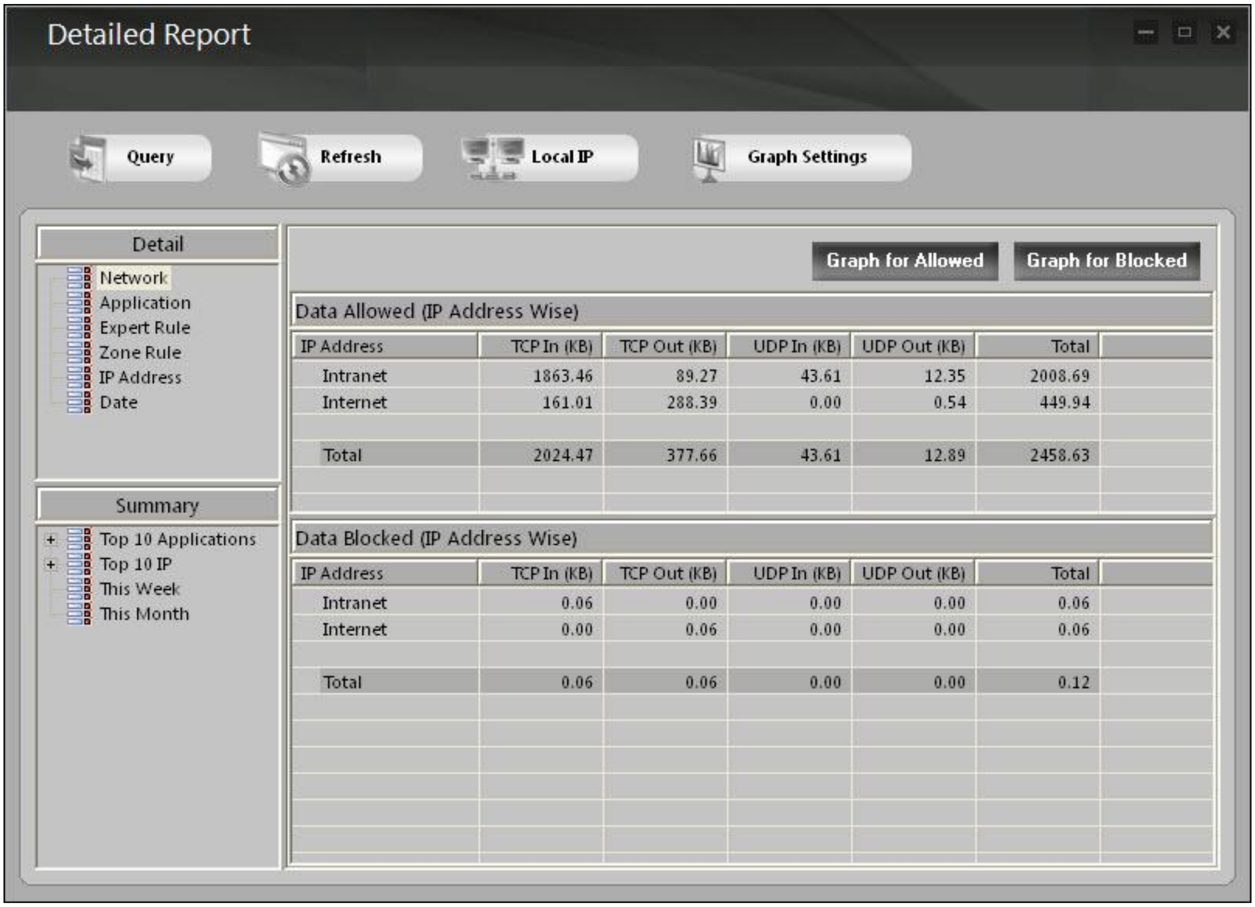
| Application | TCP In (KB) | TCP Out (KB) | UDP In (KB) | UDP Out (KB) | Total |
|---|---|---|---|---|---|
| escanpro.exe | 41.04 | 75.98 | 0.00 | 0.00 | 117.02 |
| avpmapp.exe | 14.40 | 19.17 | 0.00 | 0.00 | 33.57 |
| escanmon.exe | 1.22 | 1.94 | 0.00 | 0.00 | 3.16 |
| Total | 56.66 | 97.09 | 0.00 | 0.00 | 153.75 |

Data Blocked (Application Wise)

| Application | TCP In (KB) | TCP Out (KB) | UDP In (KB) | UDP Out (KB) | Total |
|---|---|---|---|---|---|
| leaktest.ex | 0.00 | 0.18 | 0.00 | 0.00 | 0.18 |
| Total | 0.00 | 0.18 | 0.00 | 0.00 | 0.18 |

**Figure 51**

A detailed report includes information about the rules regarding network activities and shows data in the form of graphs and charts.



Data Allowed (IP Address Wise)

| IP Address | TCP In (KB) | TCP Out (KB) | UDP In (KB) | UDP Out (KB) | Total |
|---|---|---|---|---|---|
| Intranet | 1863.46 | 89.27 | 43.61 | 12.35 | 2008.69 |
| Internet | 161.01 | 288.39 | 0.00 | 0.54 | 449.94 |
| Total | 2024.47 | 377.66 | 43.61 | 12.89 | 2458.63 |

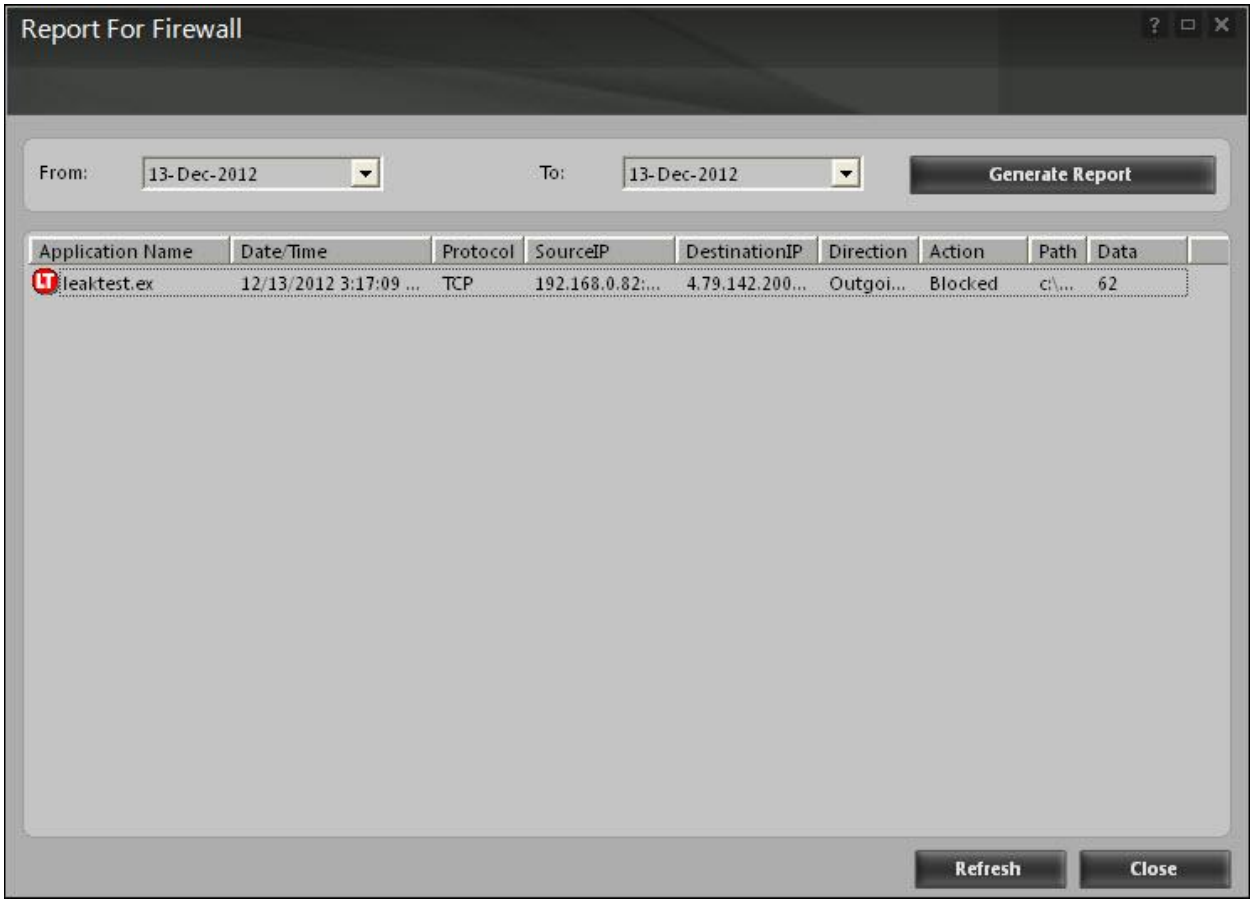
Data Blocked (IP Address Wise)

| IP Address | TCP In (KB) | TCP Out (KB) | UDP In (KB) | UDP Out (KB) | Total |
|---|---|---|---|---|---|
| Intranet | 0.06 | 0.00 | 0.00 | 0.00 | 0.06 |
| Internet | 0.00 | 0.06 | 0.00 | 0.00 | 0.06 |
| Total | 0.06 | 0.06 | 0.00 | 0.00 | 0.12 |

**Figure 52**

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.


Report For Firewall

From: 13-Dec-2012 To: 13-Dec-2012

| Application Name | Date/Time | Protocol | SourceIP | DestinationIP | Direction | Action | Path | Data |
|---|---|---|---|---|---|---|---|---|
| leaktest.ex | 12/13/2012 3:17:09 ... | TCP | 192.168.0.82:... | 4.79.142.200... | Outgoi... | Blocked | c:\... | 62 |

Figure 53

## Cloud protection

The cloud protection is the fifth module of the eScan for av. The eScan 14 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.

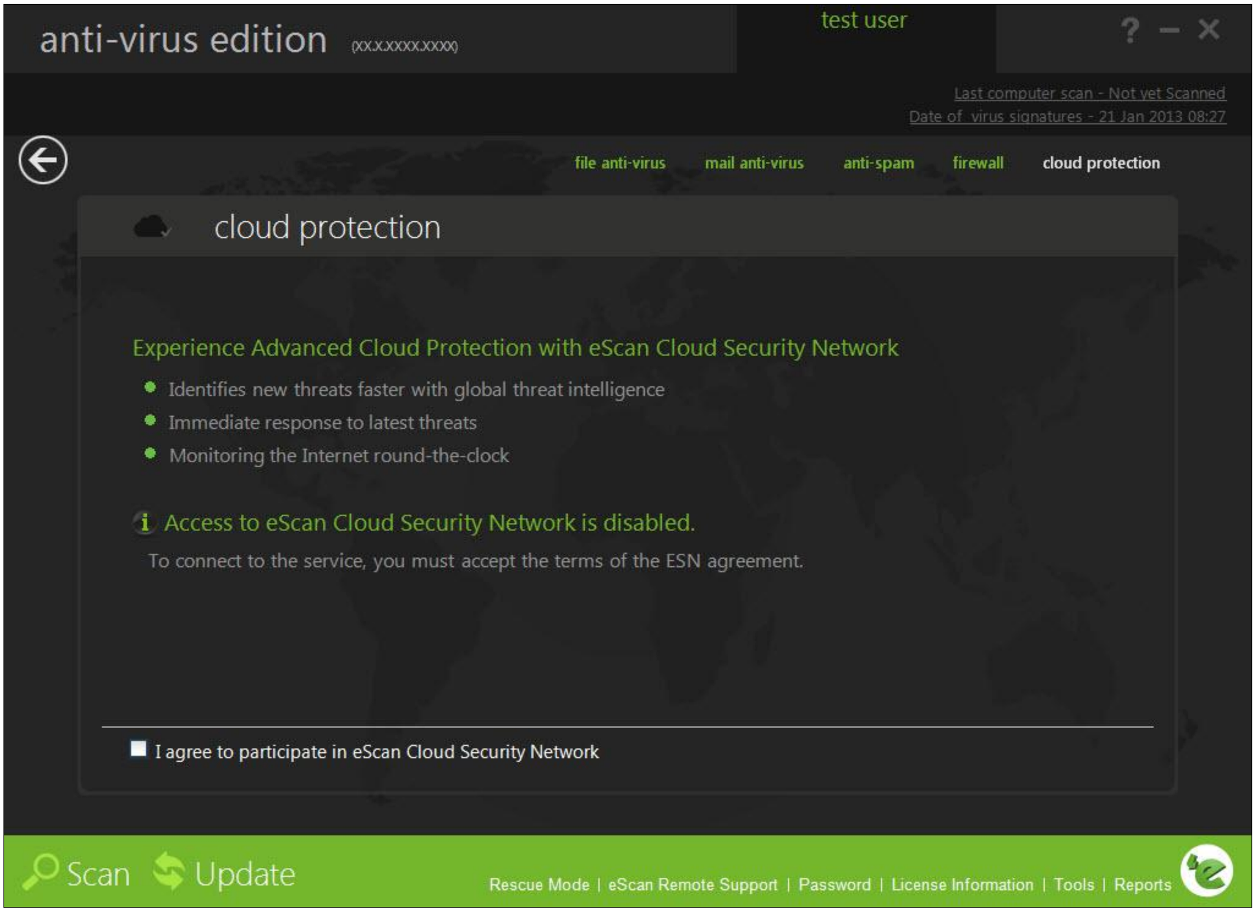
Basics of cloud-based eScan security network

1. Continuous global monitoring of real-life threats and immediate delivery of collected data to eScan host servers.
2. Analysis of collected data and the creation of protection measures against new threats, and the fast distribution of those measures to users.
3. EScan security network automatically collects information and sends the data to eScan labs. Information about suspicious files downloaded to and executed on computers is also collected,

regardless of their source, such as websites, e-mail attachments, peer-to-peer networks, and so on.

4. 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.
5. 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.
6. 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.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - Not yet Scanned
Date of virus signatures - 21 Jan 2013 08:27
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
cloud protection

Experience Advanced Cloud Protection with eScan Cloud Security Network

- Identifies new threats faster with global threat intelligence
- Immediate response to latest threats
- Monitoring the Internet round-the-clock

Access to eScan Cloud Security Network is disabled.

To connect to the service, you must accept the terms of the ESN agreement.

□ I agree to participate in eScan Cloud Security Network

Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

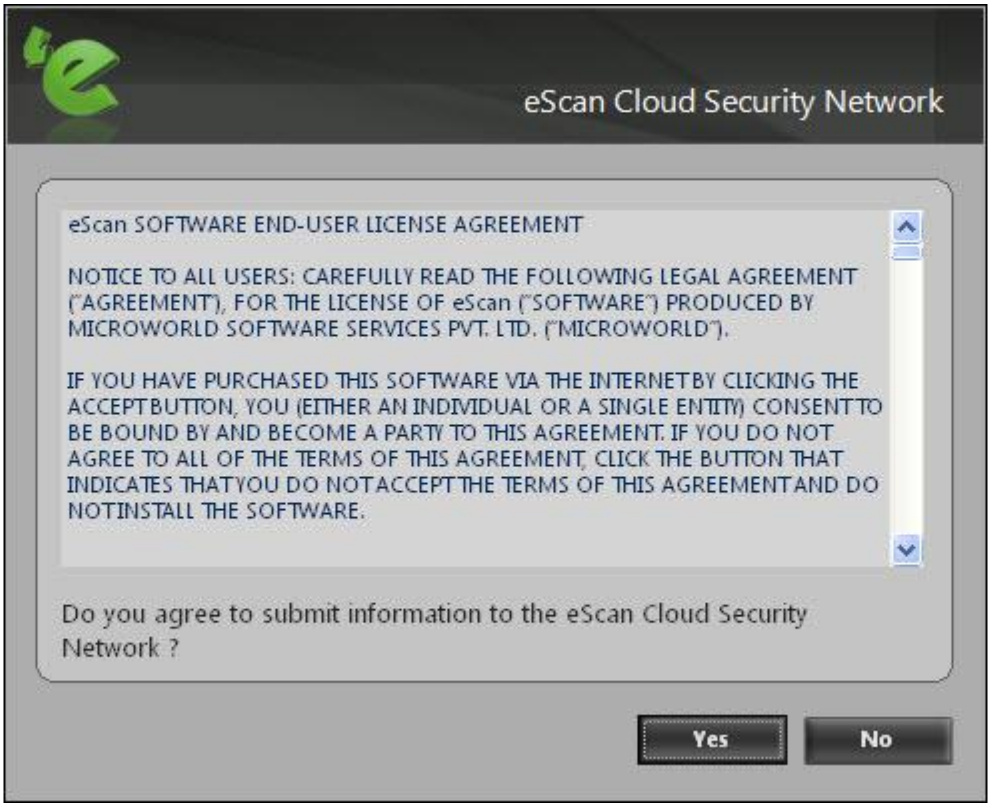
**Figure 54**

You need to have internet connection, to access this feature.

Perform the following steps to enable the cloud protection service:

To use the cloud protection service you need to first accept the terms of eScan security network (esn) agreement

1. On the cloud protection screen, at lower-left corner of the screen select the i agree to participate in eScan security network check box.
   The eScan cloud security network dialog box appears.



eScan Cloud Security Network

eScan SOFTWARE END-USER LICENSE AGREEMENT

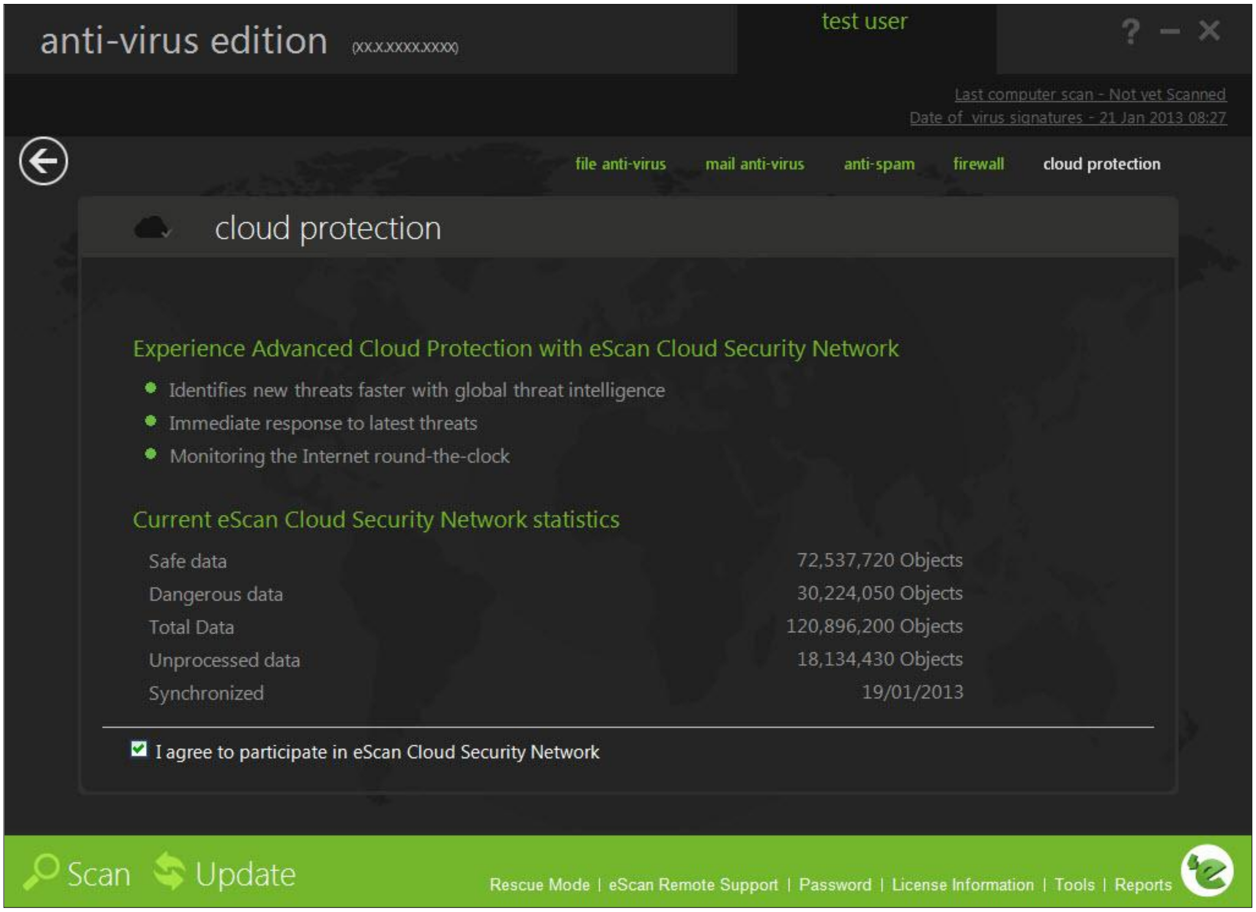
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF eScan ("SOFTWARE") PRODUCED BY MICROWORLD SOFTWARE SERVICES PVT. LTD. ("MICROWORLD").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

Do you agree to submit information to the eScan Cloud Security Network ?

Figure 55

2. Click the yes button.
   The eScan security network starts functioning and displays the current eScan security network statistics.


anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - Not yet Scanned
Date of virus signatures - 21 Jan 2013 08:27
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

cloud protection

Experience Advanced Cloud Protection with eScan Cloud Security Network

- Identifies new threats faster with global threat intelligence
- Immediate response to latest threats
- Monitoring the Internet round-the-clock

Current eScan Cloud Security Network statistics

| | |
|---|---|
| Safe data | 72,537,720 Objects |
| Dangerous data | 30,224,050 Objects |
| Total Data | 120,896,200 Objects |
| Unprocessed data | 18,134,430 Objects |
| Synchronized | 19/01/2013 |

☑ I agree to participate in eScan Cloud Security Network

**Figure 56**

## Scan

The scan option 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.

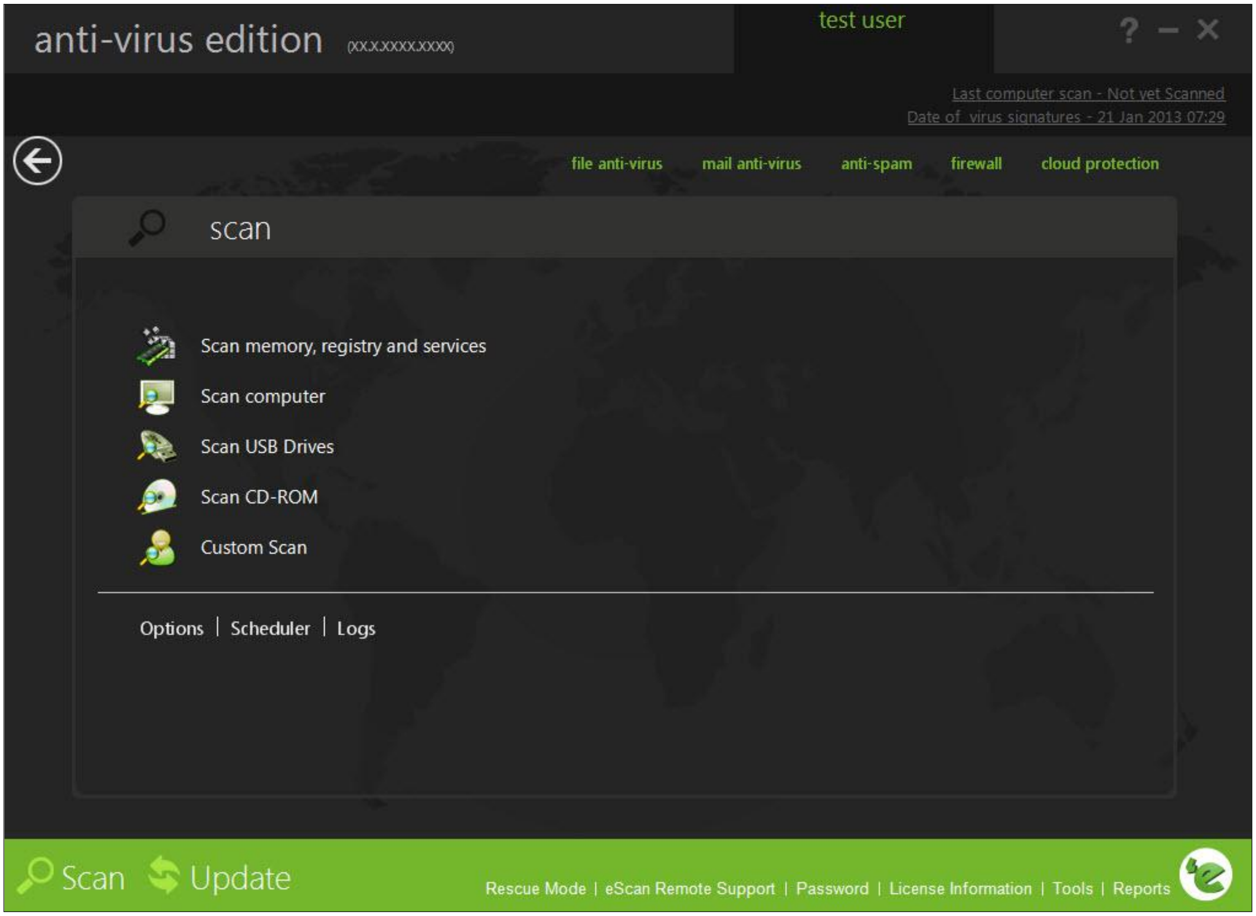
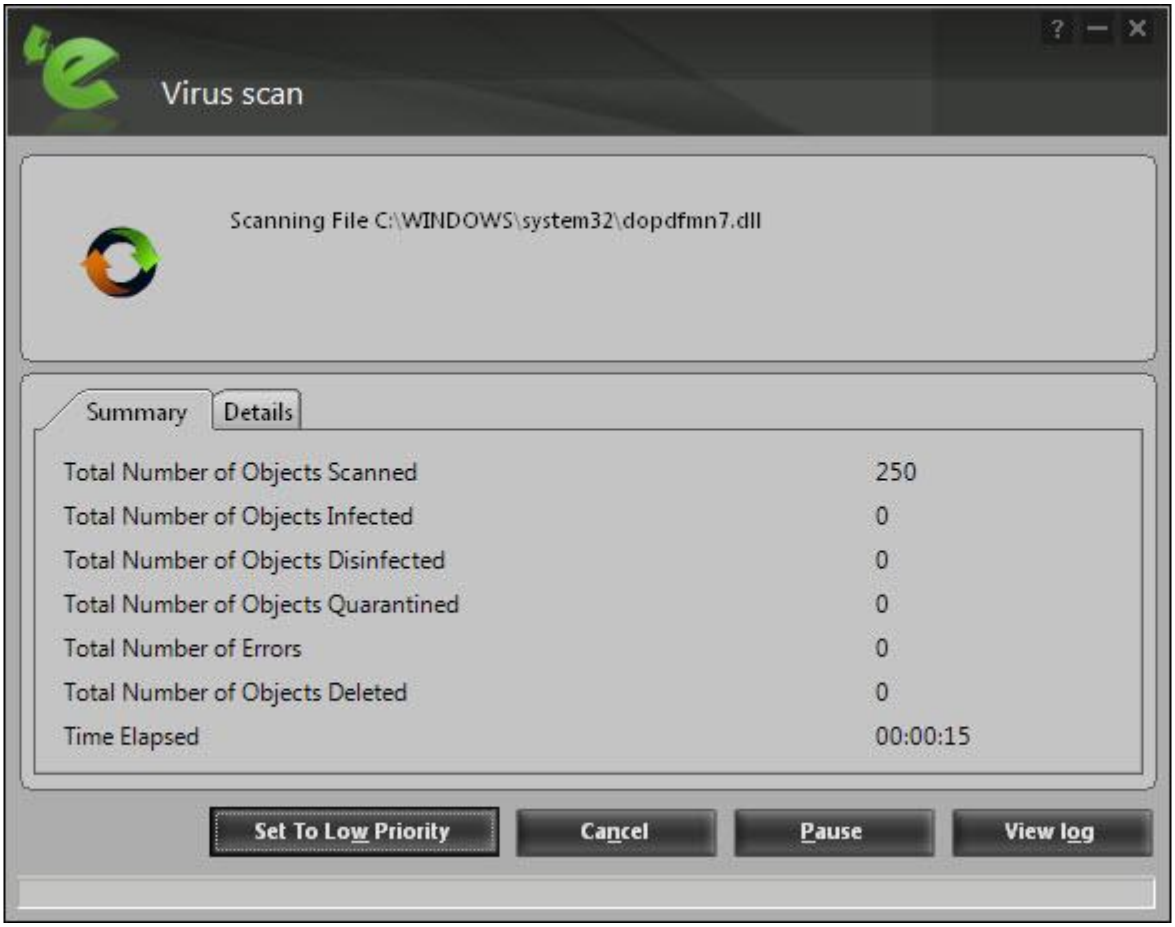

anti-virus edition (XX.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - Not yet Scanned
Date of virus signatures - 21 Jan 2013 07:29
file anti-virus
mail anti-virus
anti-spam
firewall
cloud protection
scan
Scan memory, registry and services
Scan computer
Scan USB Drives
Scan CD-ROM
Custom Scan
Options | Scheduler | Logs
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

**Figure 57**

When you click the scan button on the eScan for av, the scan tabbed page is displayed. This page provides you with options for scanning the computer and peripheral storage devices, configuring the scan option, and scheduling scans.

The virus scan dialog box contains options for scanning the memory, drives, peripheral storage devices, registry, and services running on the computer for viruses and other malware. It displays information about the total number of objects that have been scanned, infected, disinfected, quarantined, total number of errors, deleted, and time elapsed since the beginning of the scan. In addition, it provides you with an option to run scan in low-priority process by clicking the set to low priority button. After you have finished scanning the computer, you can view the log files by clicking the view log button.



Scanning File C:\WINDOWS\system32\dopdfmn7.dll

| | |
|---|---|
| Total Number of Objects Scanned | 250 |
| Total Number of Objects Infected | 0 |
| Total Number of Objects Disinfected | 0 |
| Total Number of Objects Quarantined | 0 |
| Total Number of Errors | 0 |
| Total Number of Objects Deleted | 0 |
| Time Elapsed | 00:00:15 |

**Figure 58**

You can click the custom scan options dialog box to perform customized scans by configuring eScan to scan the selected storage devices or objects for malicious software. This dialog box provides you with several scan options, such as scan cd-rom, scan usb drives, scan spyware and adware, scan startup, and scan memory, registry and services check boxes and scan local hard drives and scan following directories and files options to scan specific files and folders for malware.

In addition, on the scan screen you have the following buttons:

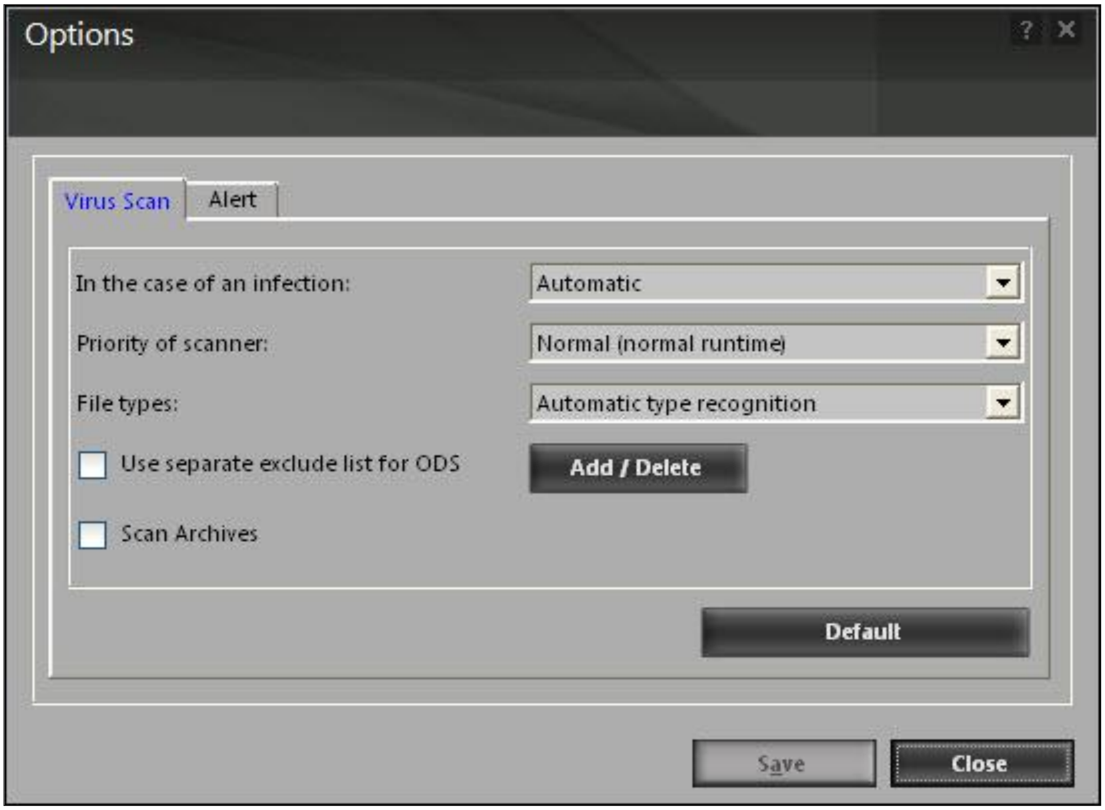
## Options

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 option. This dialog box has two panes: virus scan and alert.

After configuring all the required settings, click the save button.

## Virus scan

This tab helps you configure the actions that eScan should perform when an infection is detected. It allows you to set priority of the scan process as high, normal, or low. It also helps you configure eScan to automatically recognize either all file types or only program files.



Options

Virus Scan | Alert

In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

□ Use separate exclude list for ODS

□ Scan Archives

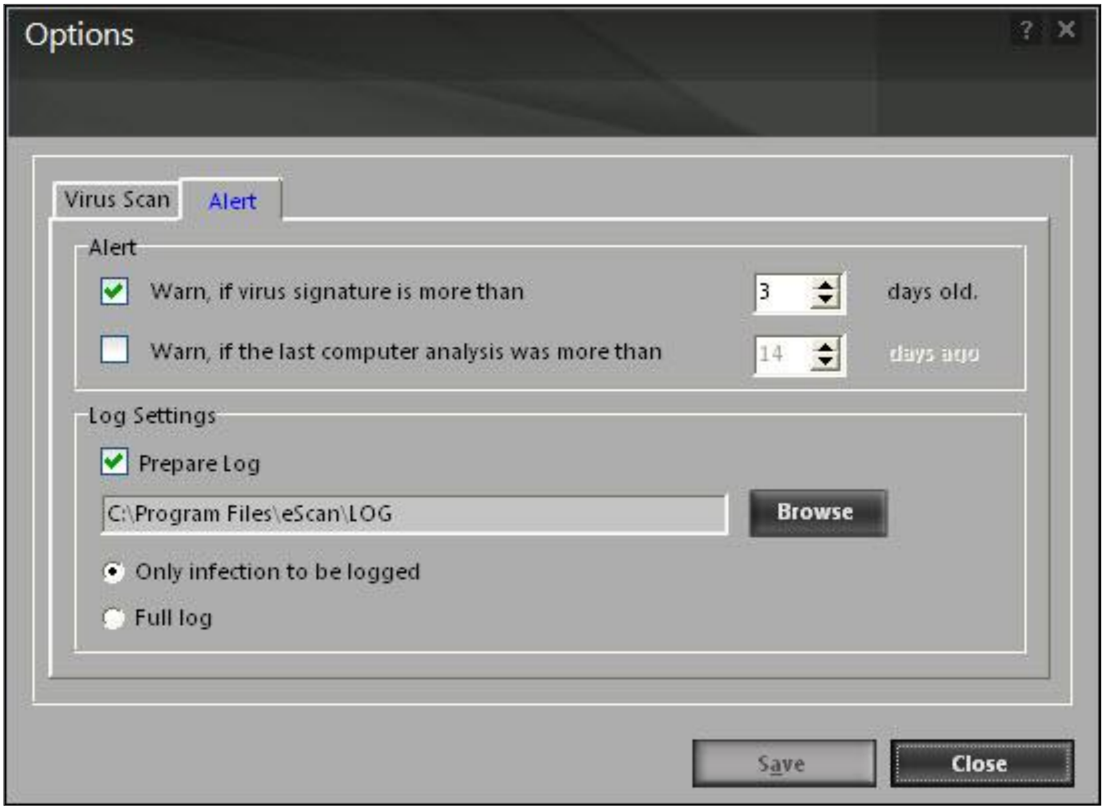
**Figure 59**

- In the case of an infection: this list helps you configure the action that eScan should perform on the file when it finds that it is infected. The actions are as follows:
  - Log only: when you select this option, eScan only logs the occurrence of the virus infection without taking any action.
  - Delete infected file: when you select this option, eScan deletes the infected file.
  - Automatic: [default] when you select this option, eScan first tries to clean the file. If it is not possible to disinfect the file, eScan quarantines or deletes the file.
- Priority of scanner: this option helps you 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 low priority.

- File types: this option helps you select the type of files that should be scanned by on-demand scan.
  - Automatic type recognition: [default] when you select this option, on-demand scan will scan all files, but will ignore files that cannot be infected.
  - Only program files: when you select this option, on-demand scan will scan only the program files or executable stored on your computer.
- Use separate exclude list for ods: [default] select this check box, if you want eScan 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.
- Add/delete: click this button, if you want to add or delete the files, folders, and sub folders. On the exclude folders dialog box, click the add button and click an appropriate object type, 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 sub folder check box.
  To delete any file/folder, click an appropriate file/folder from the list, and then click the delete button. To remove all the files/folders from the list, click the remove all button.
- Scan archives: select this check box, if you want eScan to scan both archived and packed files.

### Alert

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



Options

Alert

☑ Warn, if virus signature is more than 3 days old.

□ Warn, if the last computer analysis was more than 14 days ago

Log Settings

☑ Prepare Log

C:\Program Files\eScan\LOG

● Only infection to be logged

○ Full log

**Figure 60**

- Alert: in this section, you can configure when eScan should notify you when the virus definitions are outdated or when a specified number of days have elapsed since you have last scanned your computer.
  - Warn, if virus signature is more than: [default] when you select this check box, eScan will notify 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: when you select this check box, eScan will notify you when a specified number of days have elapsed since the computer was last analysed. By default, the value is 14.
- Log settings: in this section, you can configure the log settings for the scan option.
  - Prepare log: [default] when you select this check box, 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: [default] when this option is selected, eScan will log information only about infected files and the action taken on them in the on-demand scan log.
  - Full log: when this option is selected, the on-demand scan log will contain information about all the files scanned by eScan.

## 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. This dialog box includes an add task button, which helps you add a new scan task to the schedule.

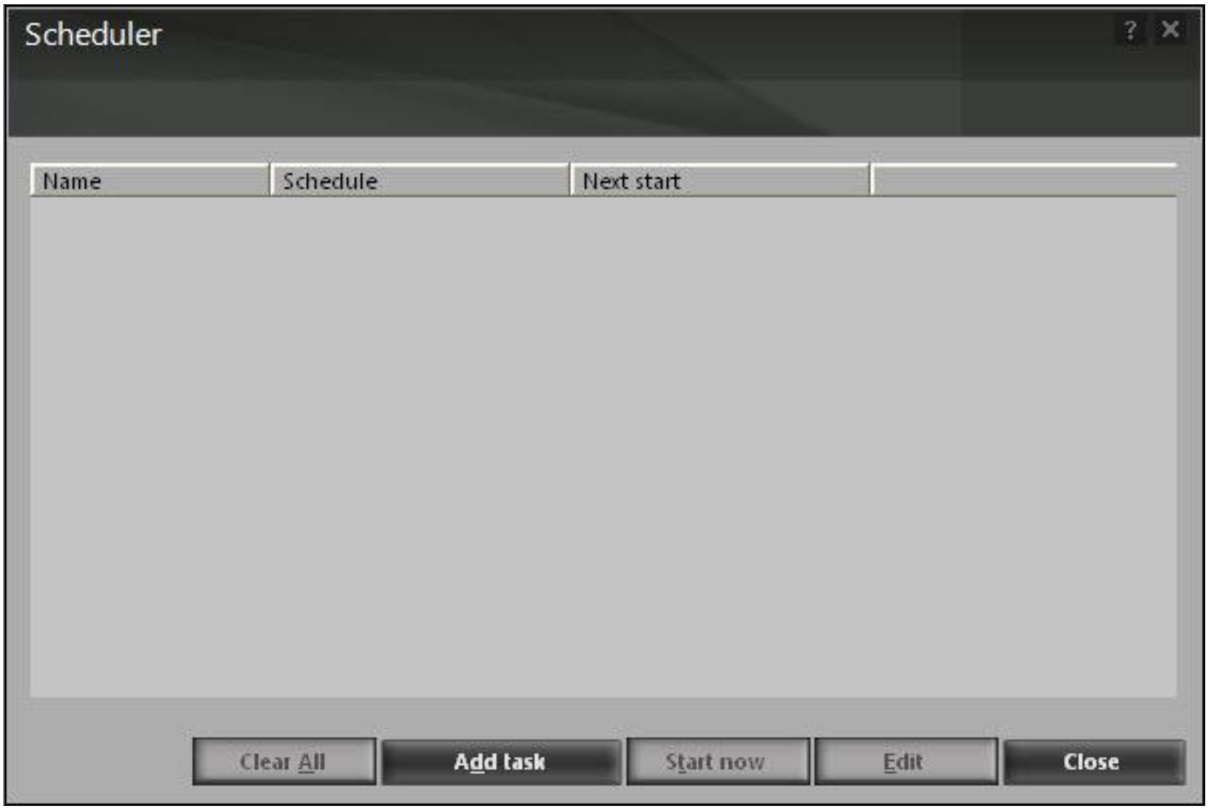
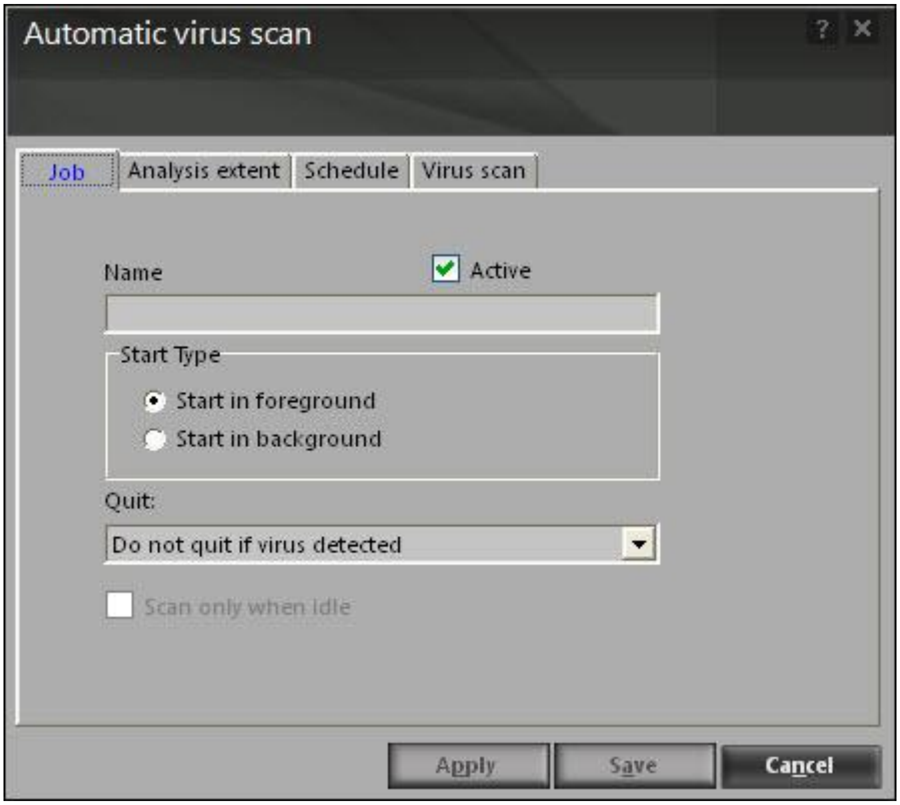


Figure 61

- Add task: 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.

> ✍ After configuring all the required settings on the automatic virus scan dialog box, click the apply button and then save button to save the settings and click the cancel button to cancel the configured settings or to close the dialog box.

  - Job: this tab helps you specify the name, start type, and termination condition for a new task. If you select the start type as start in foreground, task will run in the foreground, otherwise, task will run in the background and its window will be minimized. You can also select the termination condition for the task. For example, you can specify that the on-demand scan should always quit automatically after it has finished scanning.


Automatic virus scan

Name

☑ Active

Start Type

● Start in foreground

○ Start in background

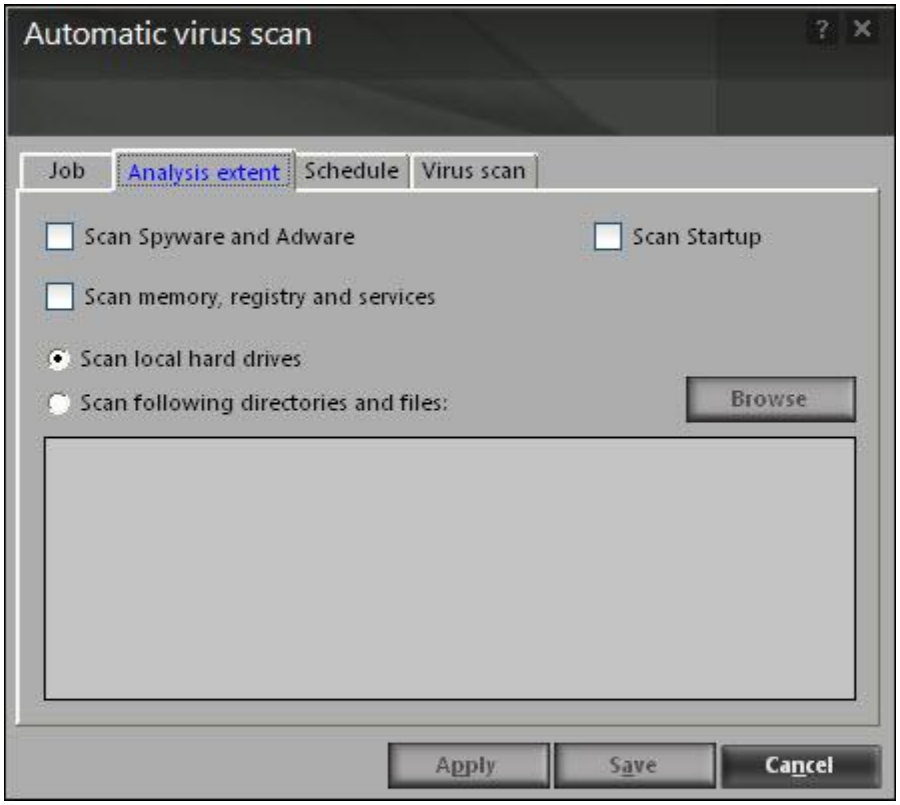
Quit:

Do not quit if virus detected

□ Scan only when idle

**Figure 62**

- Analysis extent: this tab presents you with options that help you select the type of scanning, and the list of directories, folders, or local hard drives to be scanned.



□ Scan Spyware and Adware

□ Scan Startup

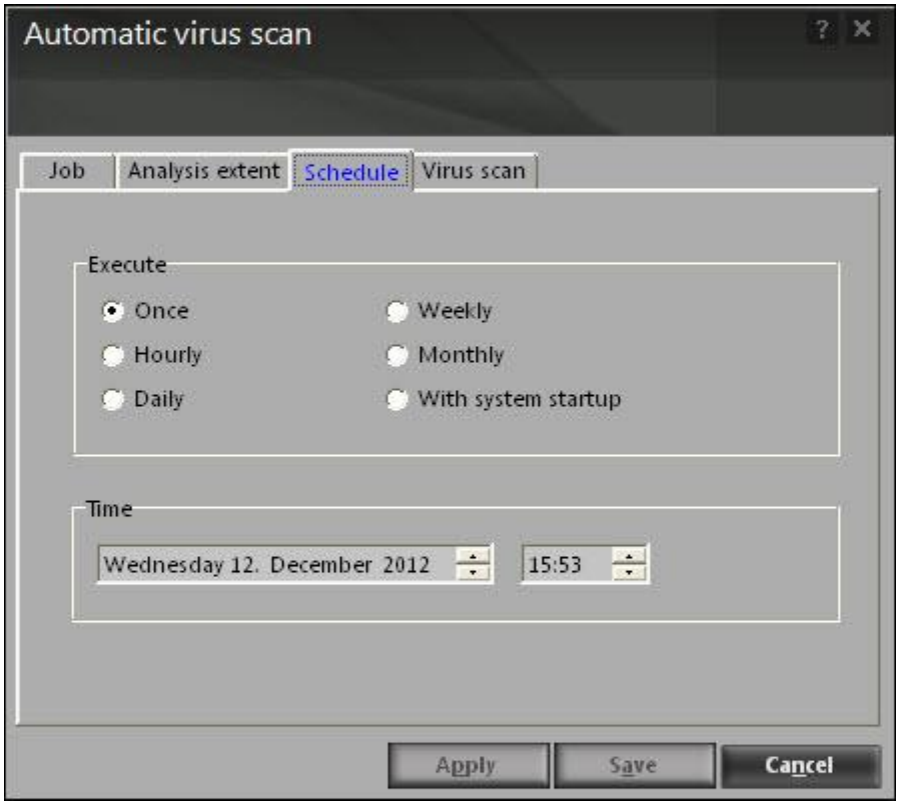
□ Scan memory, registry and services

● Scan local hard drives

○ Scan following directories and files:

**Figure 63**

- Schedule: this tab helps you 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.



Execute

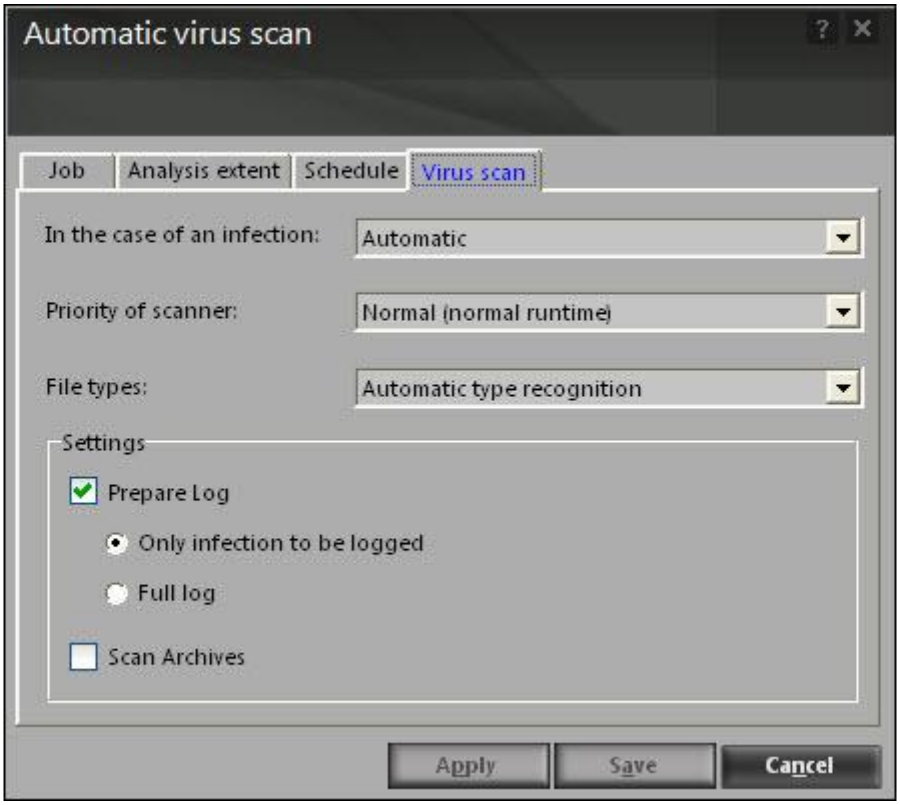
● Once
○ Hourly
○ Daily
○ Weekly
○ Monthly
○ With system startup

Time

Wednesday 12. December 2012
15:53

**Figure 64**

- Virus scan: this tab provides you with the same options as the ones present on the virus scan tab of the scan option. 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 low priority. In addition, you can configure on-demand scan to scan only program files or executable files.



In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

Settings

☑ Prepare Log

● Only infection to be logged

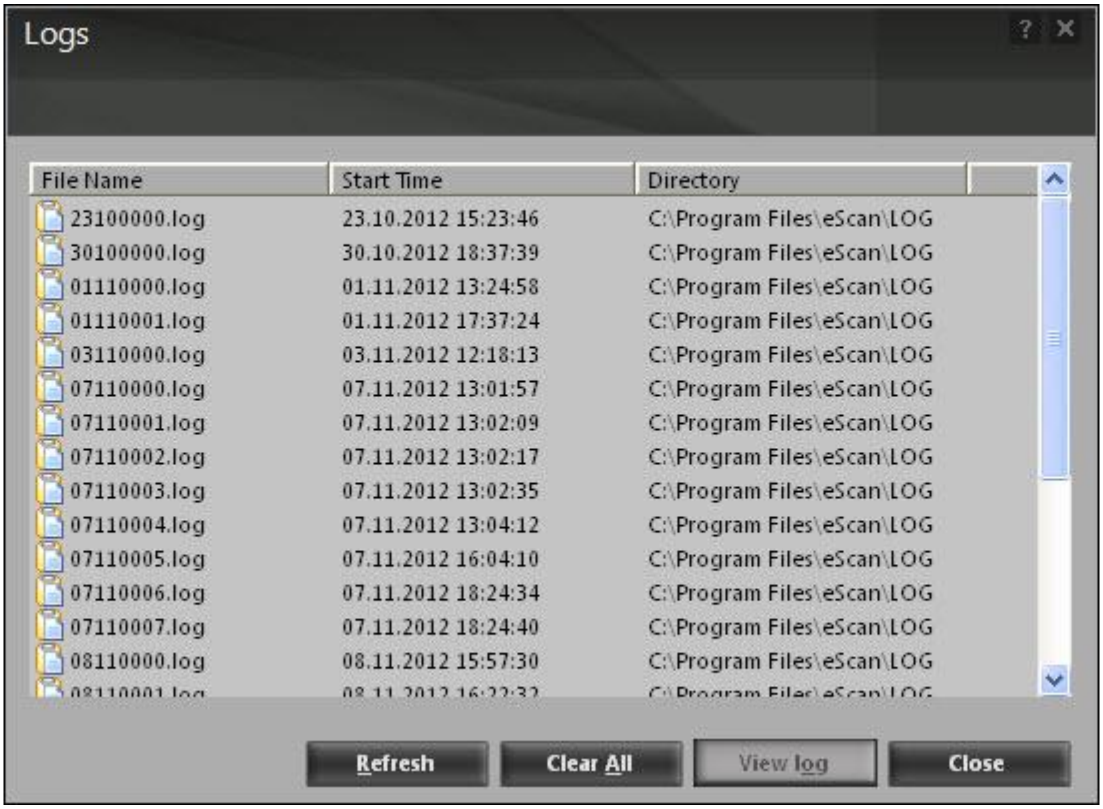
○ Full log

□ Scan Archives

Figure 65

Logs:

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

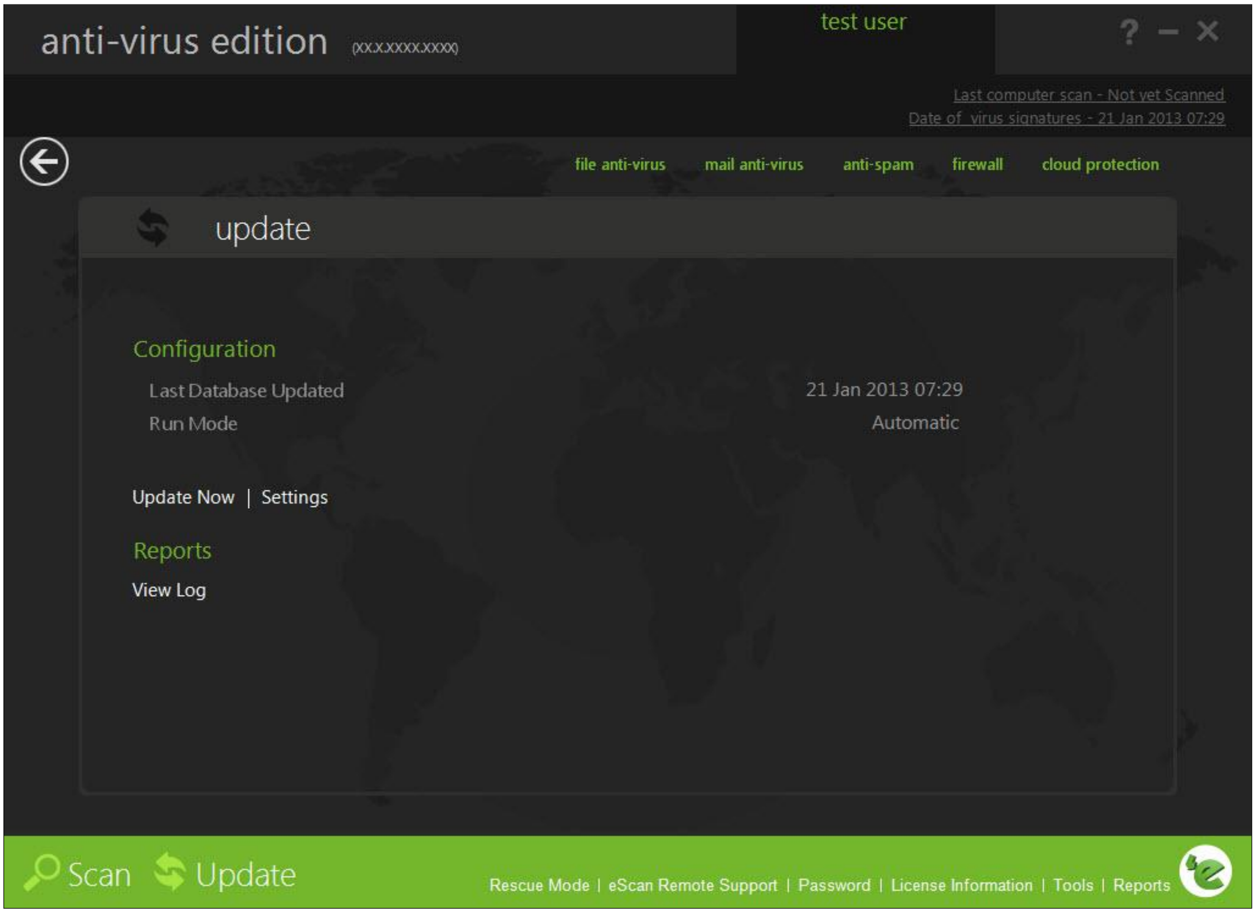


| File Name | Start Time | Directory |
|---|---|---|
| 23100000.log | 23.10.2012 15:23:46 | C:\Program Files\eScan\LOG |
| 30100000.log | 30.10.2012 18:37:39 | C:\Program Files\eScan\LOG |
| 01110000.log | 01.11.2012 13:24:58 | C:\Program Files\eScan\LOG |
| 01110001.log | 01.11.2012 17:37:24 | C:\Program Files\eScan\LOG |
| 03110000.log | 03.11.2012 12:18:13 | C:\Program Files\eScan\LOG |
| 07110000.log | 07.11.2012 13:01:57 | C:\Program Files\eScan\LOG |
| 07110001.log | 07.11.2012 13:02:09 | C:\Program Files\eScan\LOG |
| 07110002.log | 07.11.2012 13:02:17 | C:\Program Files\eScan\LOG |
| 07110003.log | 07.11.2012 13:02:35 | C:\Program Files\eScan\LOG |
| 07110004.log | 07.11.2012 13:04:12 | C:\Program Files\eScan\LOG |
| 07110005.log | 07.11.2012 16:04:10 | C:\Program Files\eScan\LOG |
| 07110006.log | 07.11.2012 18:24:34 | C:\Program Files\eScan\LOG |
| 07110007.log | 07.11.2012 18:24:40 | C:\Program Files\eScan\LOG |
| 08110000.log | 08.11.2012 15:57:30 | C:\Program Files\eScan\LOG |
| 08110001.log | 08.11.2012 16:22:32 | C:\Program Files\eScan\LOG |

**Figure 66**

## Update

The update option 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 ftp or http.



Last computer scan - Not yet Scanned
Date of virus signatures - 21 Jan 2013 07:29

Configuration

| | |
|---|---|
| Last Database Updated | 21 Jan 2013 07:29 |
| Run Mode | Automatic |

Reports

Figure 67

You can access tabbed page for the update option from eScan for av 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.

The tabbed page shows two sections: configuration and reports. These two sections are described as follows:

- Configuration

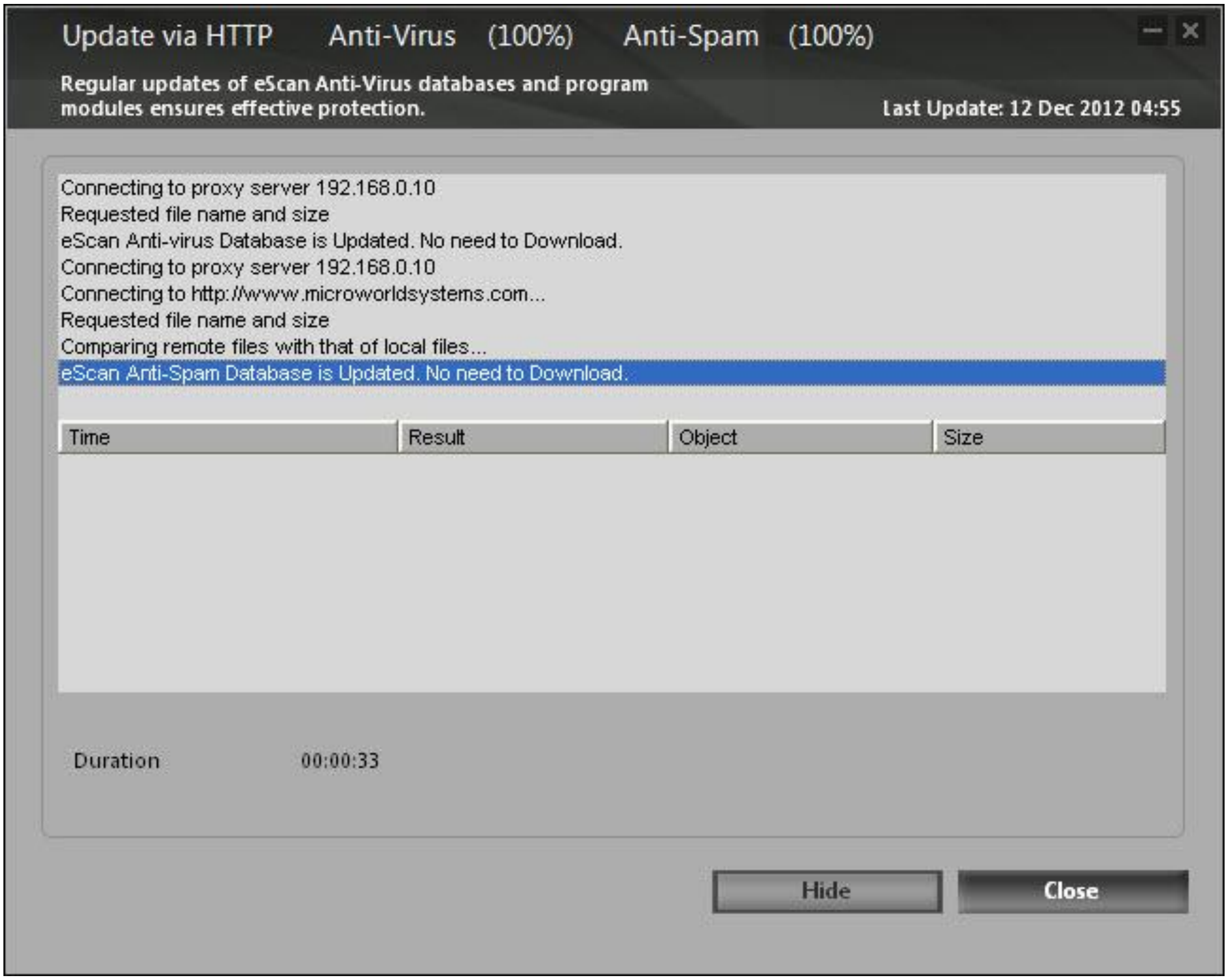
  This section displays the following information:

  - 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.

  In addition, you can click any one of the following buttons:

Update now:

You can click this button to update the anti-virus and anti-spam definitions through http, ftp, or network mode.



Update via HTTP Anti-Virus (100%) Anti-Spam (100%)
Regular updates of eScan Anti-Virus databases and program modules ensures effective protection.
Last Update: 12 Dec 2012 04:55
Time
Result
Object
Size
Duration 00:00:33
Hide
Close

```
Connecting to proxy server 192.168.0.10
Requested file name and size
eScan Anti-virus Database is Updated. No need to Download.
Connecting to proxy server 192.168.0.10
Connecting to http://www.microworldsystems.com...
Requested file name and size
Comparing remote files with that of local files...
eScan Anti-Spam Database is Updated. No need to Download.
```

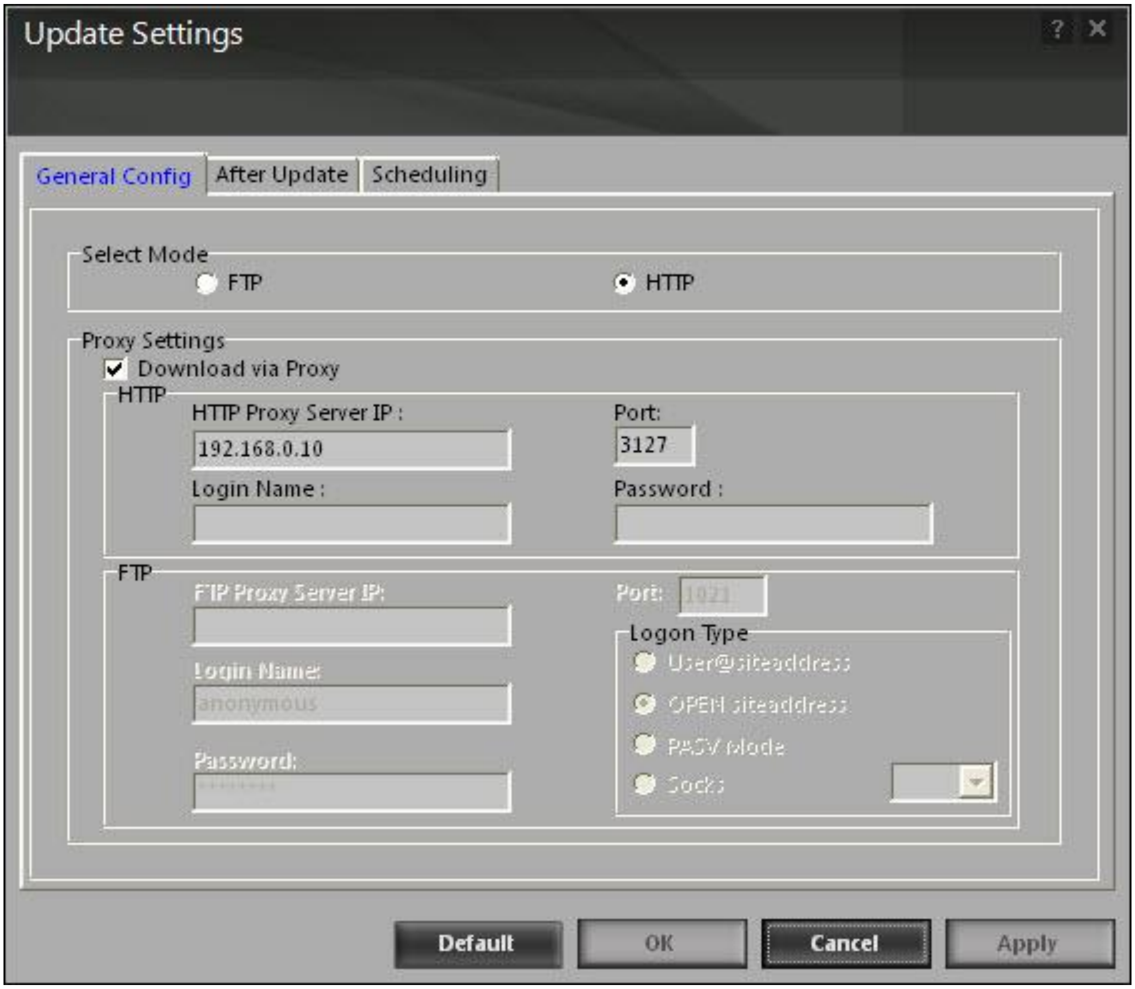
**Figure 68**

Settings:

You can click this button to open the update settings dialog box, which helps you configure the update option to download updates automatically. This dialog box has the following tabs.

- **General config**

  This tab provides you with general options for configuring the update option.



Update Settings

Select Mode
○ FTP ● HTTP

Proxy Settings
☑ Download via Proxy

HTTP
HTTP Proxy Server IP : 192.168.0.10
Port: 3127
Login Name :
Password :

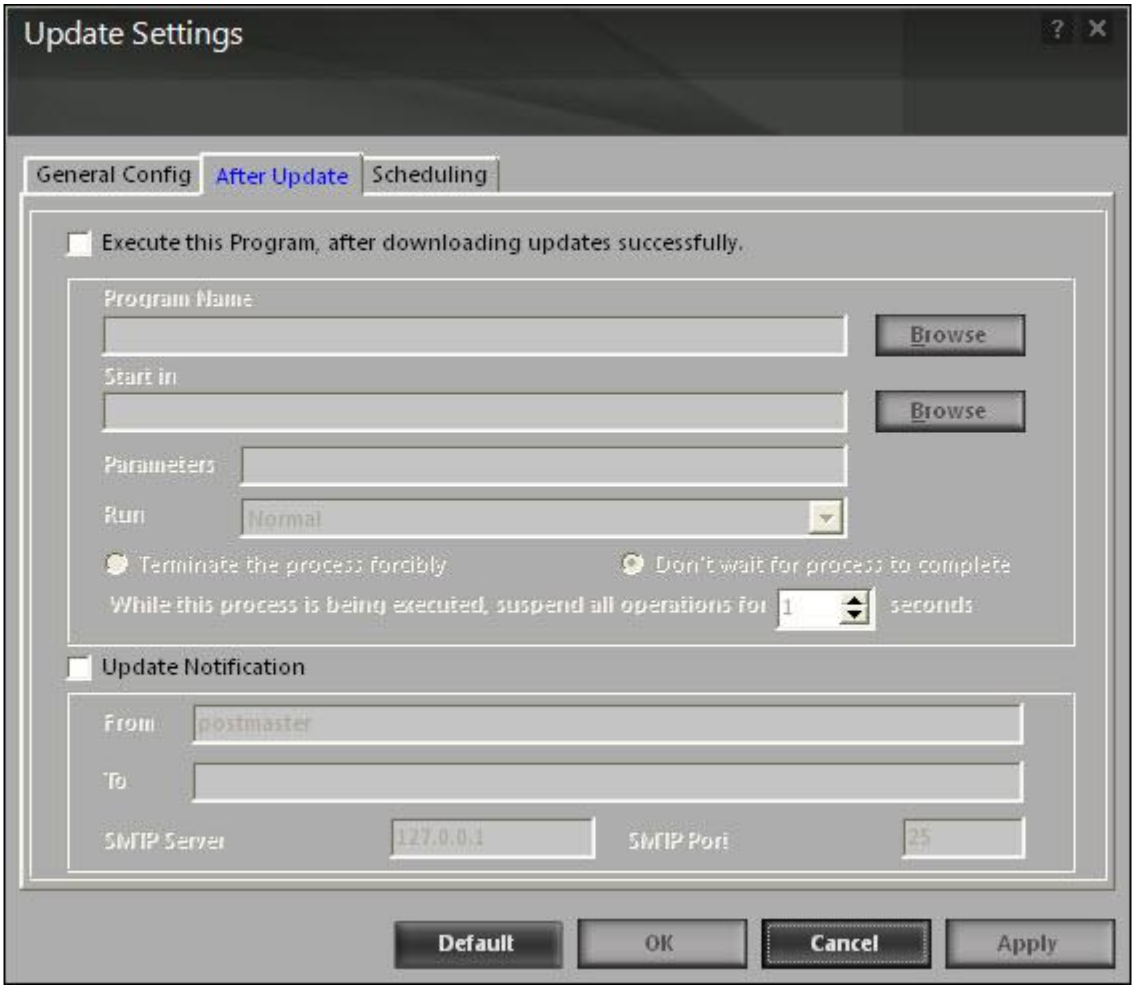
FTP
FTP Proxy Server IP:
Port: 1021
Login Name: anonymous
Password: ********
Logon Type
○ User@siteaddress
● OPEN siteaddress
○ PASV Mode
○ Socks

**Figure 69**

- Select mode: it indicates the mode for downloading updates from eScan update servers. The available modes are ftp, http, and network. Click an appropriate option.
- Proxy settings: in this section, you can configure the proxy settings for downloading updates through http proxy or ftp proxy servers. In both case, you need to provide the ip address of the proxy server if any, the port number, and the authentication credentials. In case of ftp servers, you also need to provide the format for the user id in the logon type section.

### ▪ After update

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



☐ Execute this Program, after downloading updates successfully.

Program Name

Start in

Parameters

Run: Normal

○ Terminate the process forcibly ○ Don't wait for process to complete

While this process is being executed, suspend all operations for 1 seconds

☐ Update Notification

From: postmaster

To

SMTP Server: 127.0.0.1 SMTP Port: 25

Figure 70

- 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 shows the following options:

  - 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.

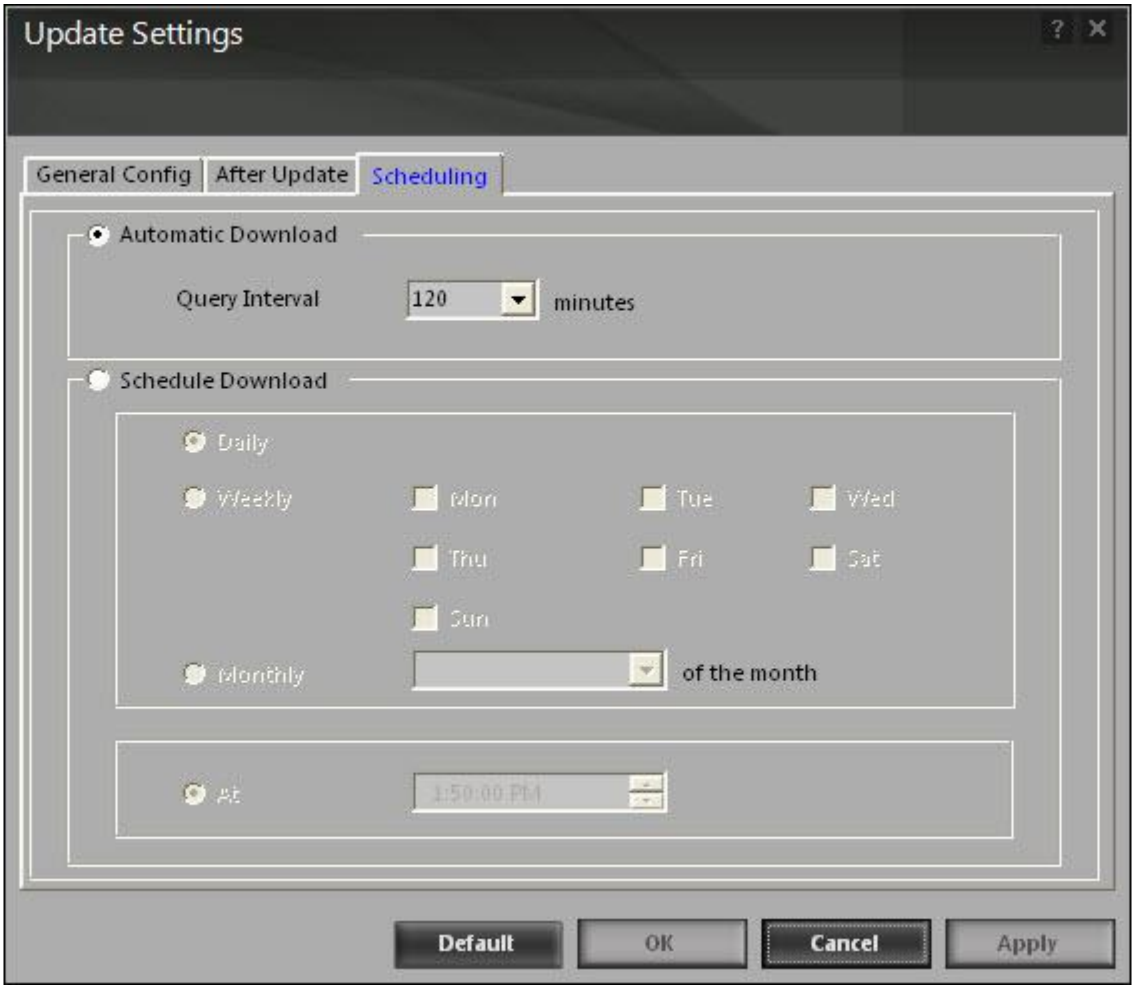
- Run: [default: normal] whenever a program runs, it runs in its own window. You can specify whether the window should be in the maximized, minimized, normal, or hidden state. The default state of the window is normal.
- Terminate the process forcibly: you can also forcibly terminate the process to free 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: [default: 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.

> ✍ The options in the execute this program, after downloading updates successfully section are disabled by default.

- Update notification: when you select this option, eScan sends an e-mail notification to the e-mail address specified in the to box in the update notification section.
  - From: [default: eScanuser@eScanav.com] you can specify the sender's e-mail address in the notification mail in this box.
  - To: you can specify the recipient's e-mail address in the notification mail in this box.
  - Smtp server: [default: 127:0:0:1] you can specify the ip address of the smtp server in this box.
  - Smtp port: [default: 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.



● Automatic Download

Query Interval 120 minutes

○ Schedule Download

○ Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

○ Monthly of the month

○ At 1:50:00 PM

Figure 71

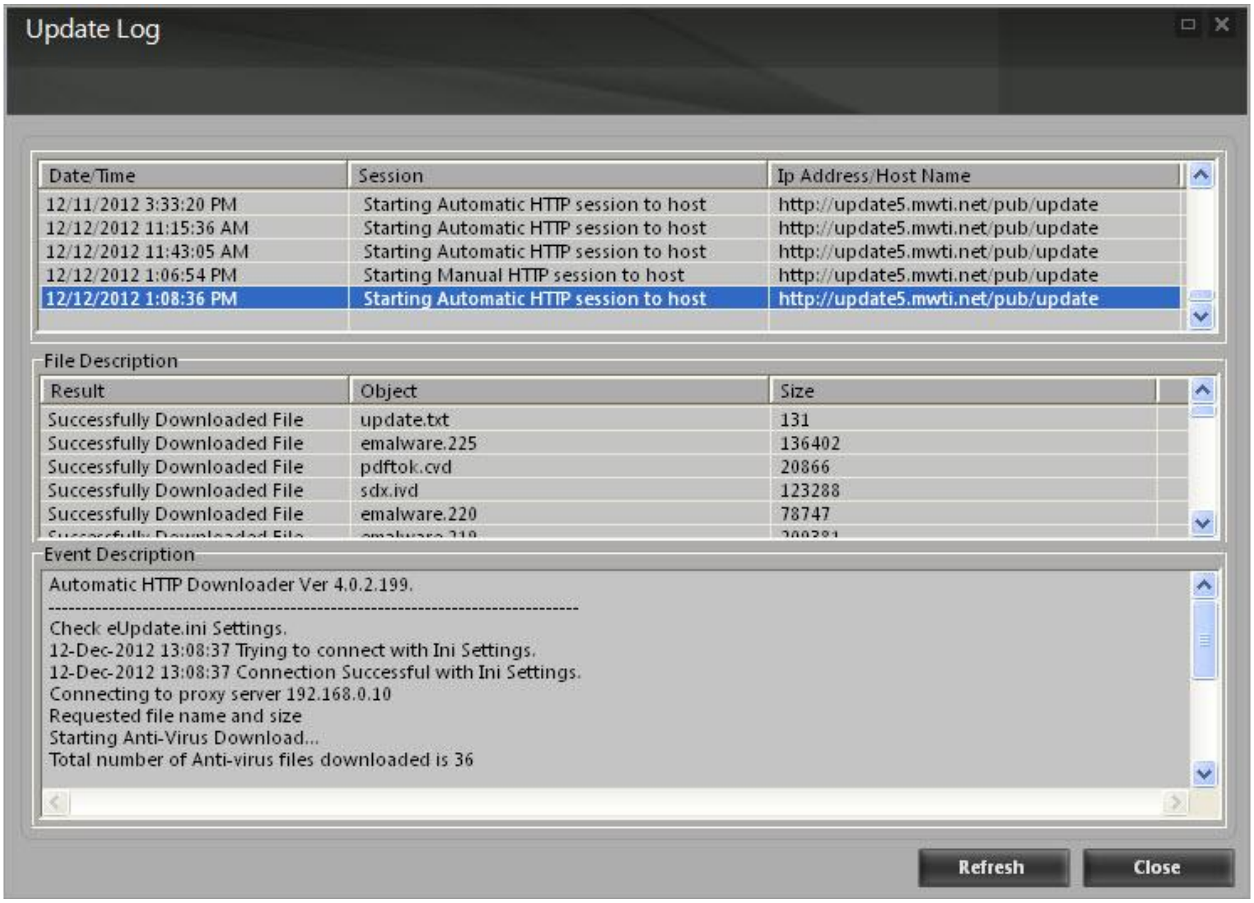
- Automatic download: [default] you can configure the update option to query and download the latest updates automatically from the MicroWorld web site. You can configure the query interval by using the following setting.
  - Query interval: [default: 120] you can set the interval in minutes, after which eScan should query the web site for latest updates.
- Schedule download: [default: daily] 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.
- Change server: you can click this button to download updates from another eScan server.

- Reports

  This section displays the following information.

  - View log: when you click this button, the view update log window is displayed. This window displays the latest activity report for the update option.



Update Log

| Date/Time | Session | Ip Address/Host Name |
|---|---|---|
| 12/11/2012 3:33:20 PM | Starting Automatic HTTP session to host | http://update5.mwti.net/pub/update |
| 12/12/2012 11:15:36 AM | Starting Automatic HTTP session to host | http://update5.mwti.net/pub/update |
| 12/12/2012 11:43:05 AM | Starting Automatic HTTP session to host | http://update5.mwti.net/pub/update |
| 12/12/2012 1:06:54 PM | Starting Manual HTTP session to host | http://update5.mwti.net/pub/update |
| 12/12/2012 1:08:36 PM | Starting Automatic HTTP session to host | http://update5.mwti.net/pub/update |

File Description

| Result | Object | Size |
|---|---|---|
| Successfully Downloaded File | update.txt | 131 |
| Successfully Downloaded File | emalware.225 | 136402 |
| Successfully Downloaded File | pdftok.cvd | 20866 |
| Successfully Downloaded File | sdx.ivd | 123288 |
| Successfully Downloaded File | emalware.220 | 78747 |
| Successfully Downloaded File | emalware.219 | 209381 |

Event Description

```
Automatic HTTP Downloader Ver 4.0.2.199.
--------------------------------------------------------------------------
Check eUpdate.ini Settings.
12-Dec-2012 13:08:37 Trying to connect with Ini Settings.
12-Dec-2012 13:08:37 Connection Successful with Ini Settings.
Connecting to proxy server 192.168.0.10
Requested file name and size
Starting Anti-Virus Download...
Total number of Anti-virus files downloaded is 36
```

**Figure 72**

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.

# Contact information

## Contact details

### Free technical support

We offer 24x7 free online technical support to our customers through e-mail and live chat. We also provide free telephonic support to our customers during business hours.

### Chat support

The eScan technical support team is available round the clock to assist you with your queries. You can contact our support team through live chat by visiting http://www.eScanav.com/english/livechat.asp link.

### Forums support

You can even join the MicroWorld forum at http://forums.eScanav.com to discuss all your eScan related problems with our experts.

### E-mail support

Please send your queries, suggestions, and comments about our products or this guide to support@eScanav.com.

### Important websites

- For sales enquiry, write to: sales@eScanav.com
- For support enquiry, write to: support@eScanav.com
- For forums, write to http://forums.eScanav.com
- For knowledge base, visit: http://forums.eScanav.com
- For eScan Wikipedia/help, visit: http://www.eScanav.com/wiki
- For live chat, visit: http://www.eScanav.com/english/livechat.asp

# Registered offices

**Asia Pacific**
MicroWorld software services Pvt. ltd.
plot no 80, road 15, MIDC, Marol,
Andheri (E), Mumbai
India

Tel : +91 22 2826 5701- 05,
Fax: +91 22 2830 4750
Technical Support (Toll Free No.) 1800 267 2900
E-mail : sales@eScanav.com
Web site: http://www.eScanav.com

**Malaysia**
MicroWorld Technologies Sdn.bhd.
(co.no. 722338-a)
E-8-6, Megan Avenue 1, 189, Jalan Tun Razak, 50400 Kuala Lumpur
Malaysia

Tel : +603 2333 8909/8910
Fax: +603 2333 8911
E-mail : sales@eScanav.com
Web site: http://www.eScanav.com

**South Africa**
MicroWorld technologies south Africa (Pty) ltd.
376 oak avenue
Block c (entrance from 372 oak avenue) Ferndale, Ransburg, Gauteng, South Africa
Tel : local 08610 eScan (37226)
International : +27 11 781 4235

Fax: +086 502 0482

E-mail : sales@MicroWorld.co.za

Web site: http://www.MicroWorld.co.za

**USA**

MicroWorld technologies inc.
33045 Hamilton Court East, Suite 105
Farmington hills, mi 48334-3385
USA
Tel : +1 248 855 2020 / 2021
Fax: +1 248 855 2024
E-mail : sales@eScanav.com

Web site: http://www.eScanav.com

Germany
MicroWorld technologies gmbh
Leopoldstr. 244
D-80807 munich
Germany
Tel : +49 72 40 94 49 0920
Fax: +49 72 40 94 49 0992
E-mail : sales@eScanav.de
Web site: http://www.eScanav.de