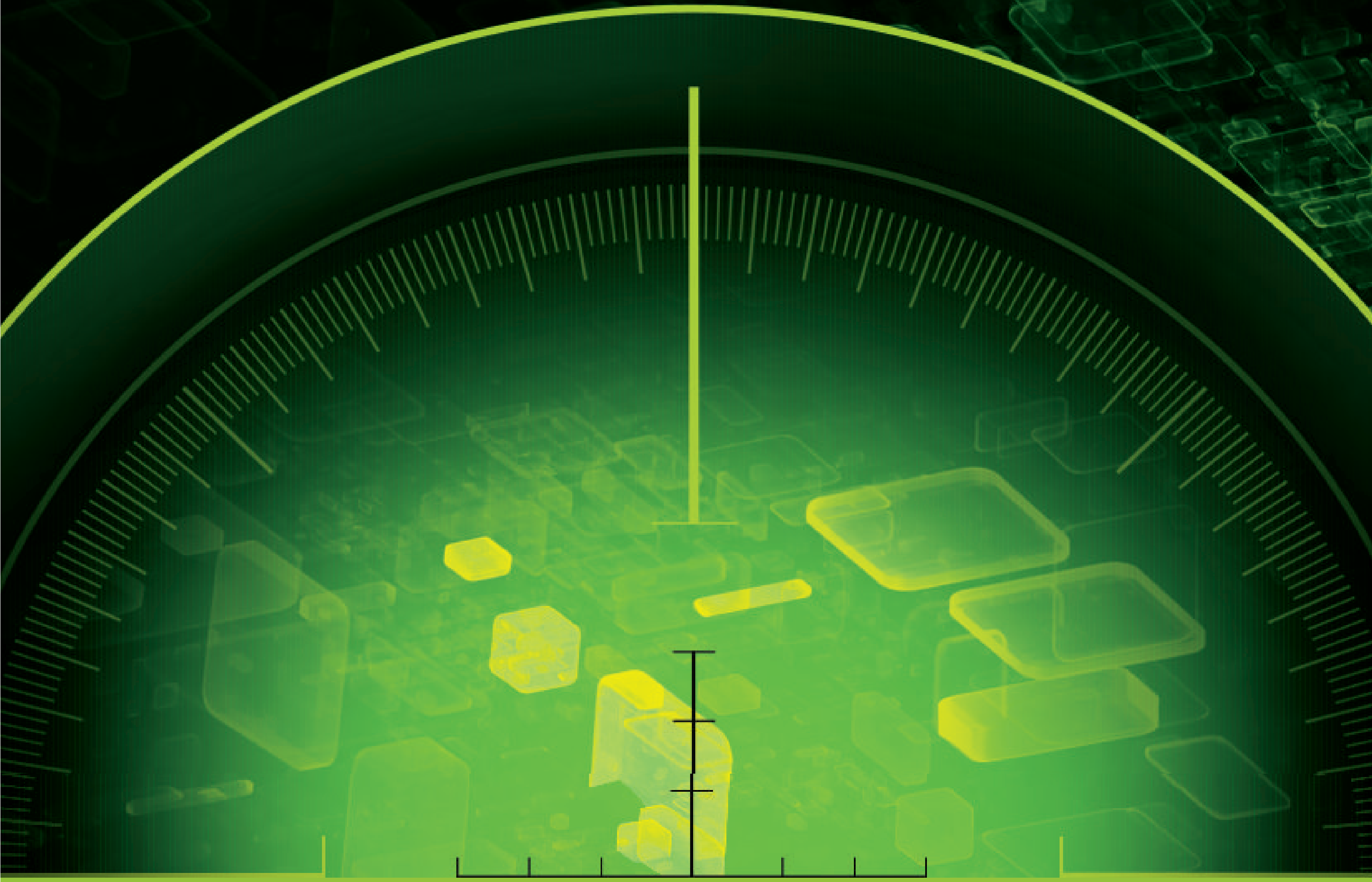
‘eScan™

Anti-Virus & Content Security

Internet Security Suite

with Cloud Security

User Guide



www.escanav.com

sales@escanav.com

Document Number: 5BUG/10.01.2013/14.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:	2nd March, 2013

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, e-mails, and hackers. To achieve this, eScan employs cutting-edge technologies, such as MicroWorld Winsock Layer (MWL), Non Intrusive Learning Pattern (NILP), Domain and IP Reputation Check (DIRC), eScan Security Network (ESN), and Proactive Malware Detection.

MicroWorld 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 Internet Security Suite (ISS) 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 an 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.
- Check for sufficient space on your Hard Disk for Installing eScan. (Check Minimum Hardware Requirement)
- 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.

Minimum Software Requirements

- Operating System
  - Windows® 10 / 8.1 / 8 Family
  - Windows® 7 Family
  - Windows Vista® Family
  - Windows® XP Family Service Pack 2 or higher
  - Windows® 2000 Professional Service pack 4 Rollup patch 1

✍ eScan 14 SOHO products do not support Server Operating Systems.

Minimum Hardware Requirements

- CPU
  - Windows 8 requires 1 GHz
  - Windows 7 requires 1 GHz
  - Windows Vista requires 1 GHz
  - Windows XP requires 450 MHz (1 GHz recommended)

- Memory
  - Windows 8 requires 1 GB
  - Windows 7 requires 1 GB
  - Windows Vista requires 1 GB
  - Windows XP requires 512 MB (1GB recommended)

- Disk Space
    - 750 MB

Other Requirements

- **Web Browser:** Microsoft Internet Explorer 7.0 or 8.0 or higher.
- **Display:** High-color display with a resolution of 640x480 pixels or higher

Understanding the User Interface

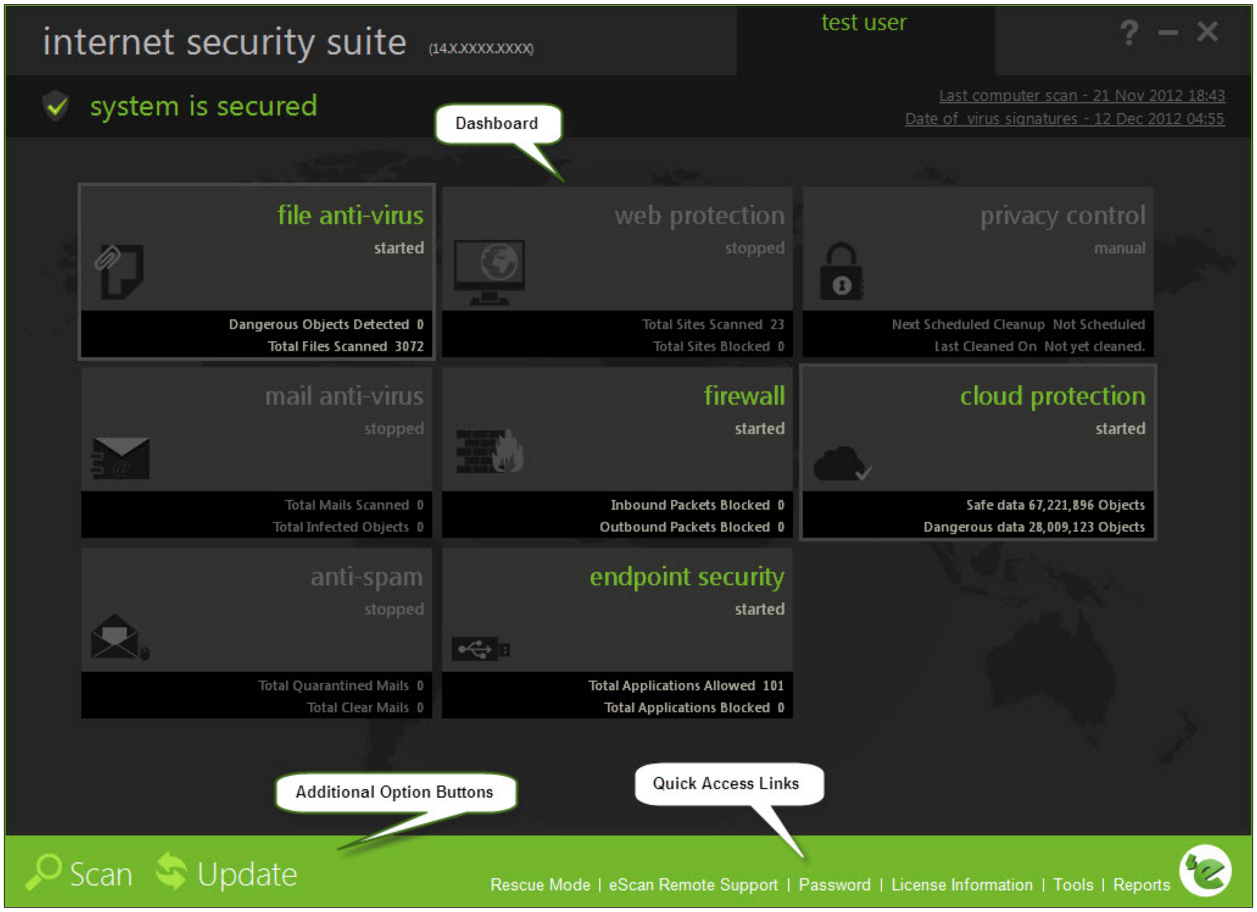
This section introduces you an overview of eScan for ISS user interface.

Contents

Graphical User Interface (GUI)

The GUI 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 your native language to English press SHIFT + F12 and for switching from English to your native Language 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 colour or **X** system is not secured in red colour), date of last computer scanned, date of virus signatures, modules displaying the status information, additional option buttons, and quick access links. Refer Figure 1.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
system is secured
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55

file anti-virus: started
Dangerous Objects Detected 0
Total Files Scanned 3072

web protection: stopped
Total Sites Scanned 23
Total Sites Blocked 0

privacy control: manual
Next Scheduled Cleanup Not Scheduled
Last Cleaned On Not yet cleaned.

mail anti-virus: stopped
Total Mails Scanned 0
Total Infected Objects 0

firewall: started
Inbound Packets Blocked 0
Outbound Packets Blocked 0

cloud protection: started
Safe data 67,221,896 Objects
Dangerous data 28,009,123 Objects

anti-spam: stopped
Total Quarantined Mails 0
Total Clear Mails 0

endpoint security: started
Total Applications Allowed 101
Total Applications Blocked 0

Dashboard

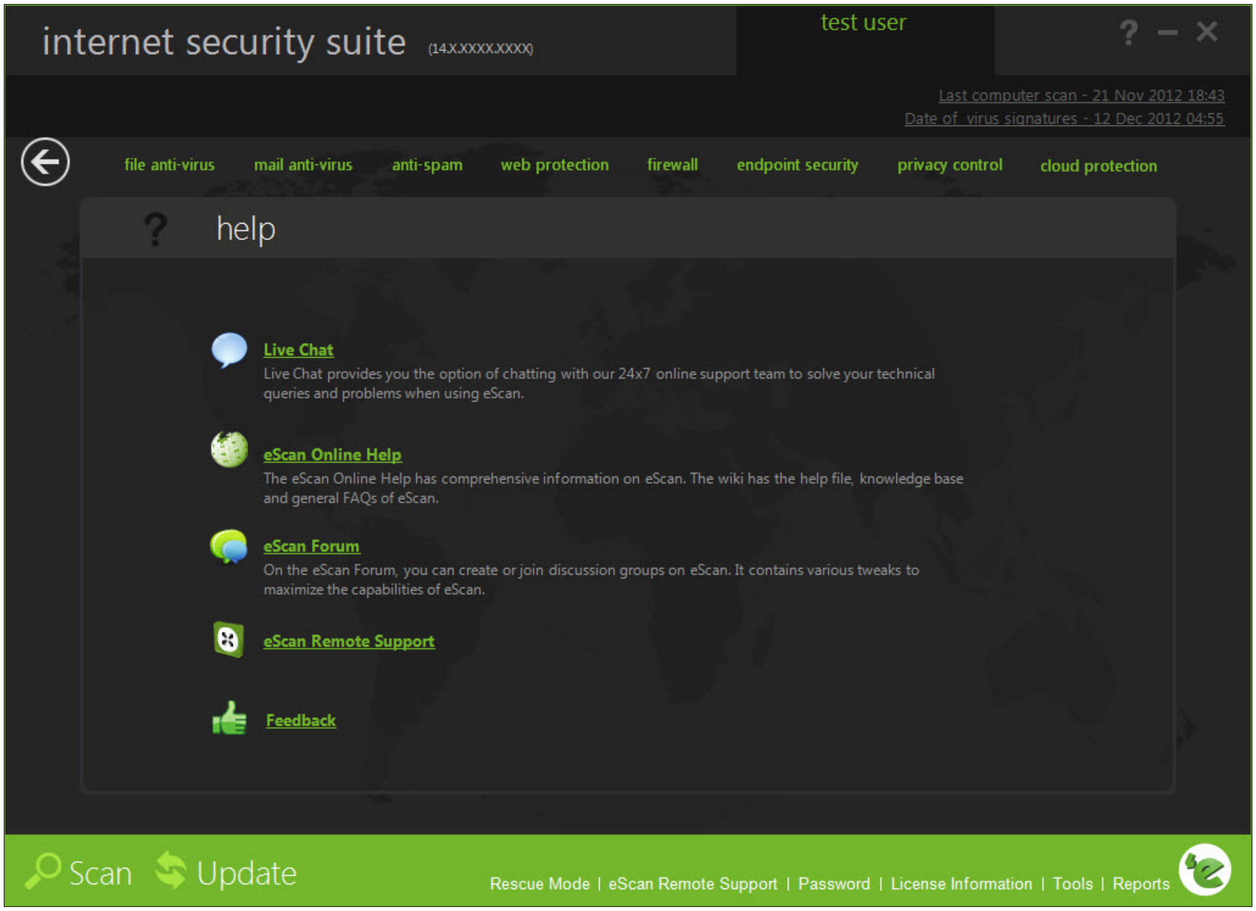
Additional Option Buttons

Quick Access Links

Figure 1

On upper-left corner of the screen, you can view message as "√ system is secured" in green colour, only if the File anti-virus (real-time protection) is in enabled mode and if File anti-virus (real-time protection) is in disabled mode, the "**X** system is not secured" message is displayed in red colour.

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. Refer Figure 2.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
help
Live Chat
eScan Online Help
eScan Forum
eScan Remote Support
Feedback
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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

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

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

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 ISS also provides you context-sensitive help, where you can find information on any specific feature while accessing the eScan for ISS 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/Month/yyyy min: sec format.

It also displays the date, month, year, and time when the latest virus signatures are updated in the dd/Month/yyyy format.

Modules

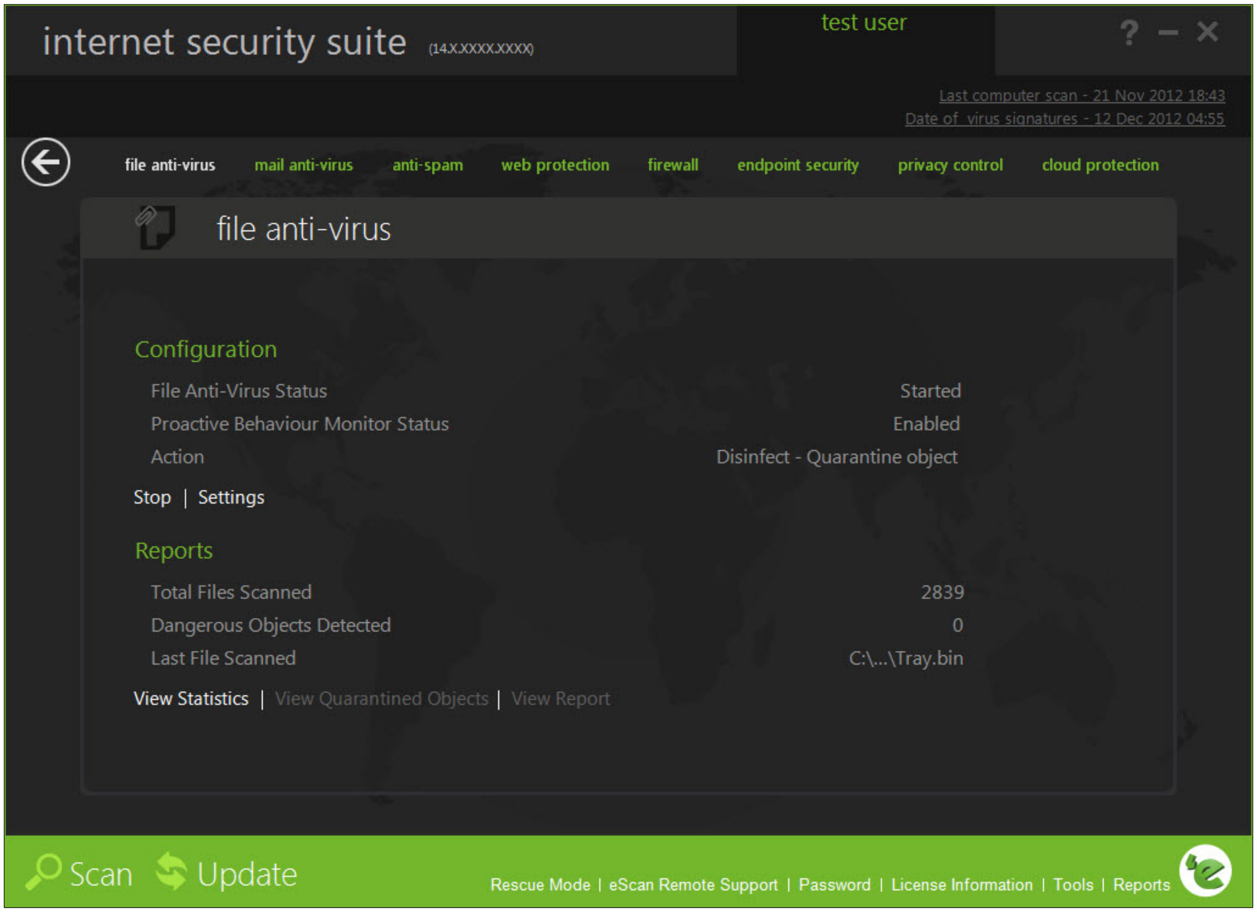
eScan for ISS provides you access to the following eight modules:

- **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 emails based on keywords and phrases that appear within e-mails.
- **Web Protection:** This module helps you prevent offensive or pornographic content from appearing within a web browser.
- **Firewall:** This module helps you apply various expert rules for blocking specific ports, programs, or services on your computer.
- **Endpoint Security:** This module helps you protect your computer from infected devices like USBs, SD cards, Web cams, and CD/DVD ROM's and also to control access to various applications through the blocking and whitelisting feature.
- **Privacy Control:** This module helps you clear your browser cache, history, cookies, and other personal information that may be stored within temporary files 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 ISS. You can click the individual section to view and access the protection status settings for the File Anti-Virus, Mail Anti-Virus, Privacy Control, Firewall, Endpoint Security, Cloud Protection, Anti-Spam, and Web Protection modules. By default, the File Anti-Virus, Firewall, Endpoint Security, and Cloud Protection modules are only enabled.

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

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. Refer Figure 3.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
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	2839
Dangerous Objects Detected	0
Last File Scanned	C:\...\Tray.bin

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, Web Protection, Firewall, Endpoint Security, Privacy Control 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. Refer Figure 4.

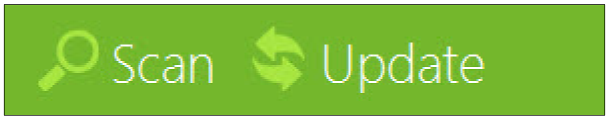


Figure 4

- **Scan:** Click this button, to access scan features, configure scheduled scans, or to run on-demand scans.
- **Update:** Click this button to configure daily/weekly/monthly 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: Refer Figure 5.

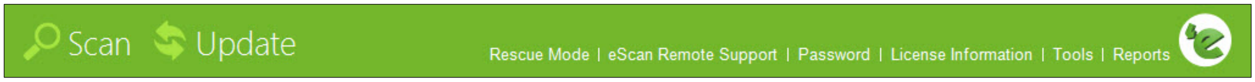

Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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 infection cannot be removed 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 connected to 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 ISS.
- **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 ISS 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, Web Protection, Firewall, Endpoint Security, 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 wizard 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 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.

The Download Latest Hotfix (eScan) option is greyed out if the latest hotfix is already installed.

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 on 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. By default, It is stored in a pre-defined Path given below –

- The default path for 32-bit computer: ***[Disk Drive]*\Program Files\eScan\Debug**
- The default path for 64-bit computers: ***[Disk Drive]*\Program Files (x86)\eScan\Debug**

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/Name of the SMTP server.
- **SMTP Port:** [Default: 25] Type port number of the SMTP server.
- **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.

(Information about "Do you want to send this debug to Administrator is missing)

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.

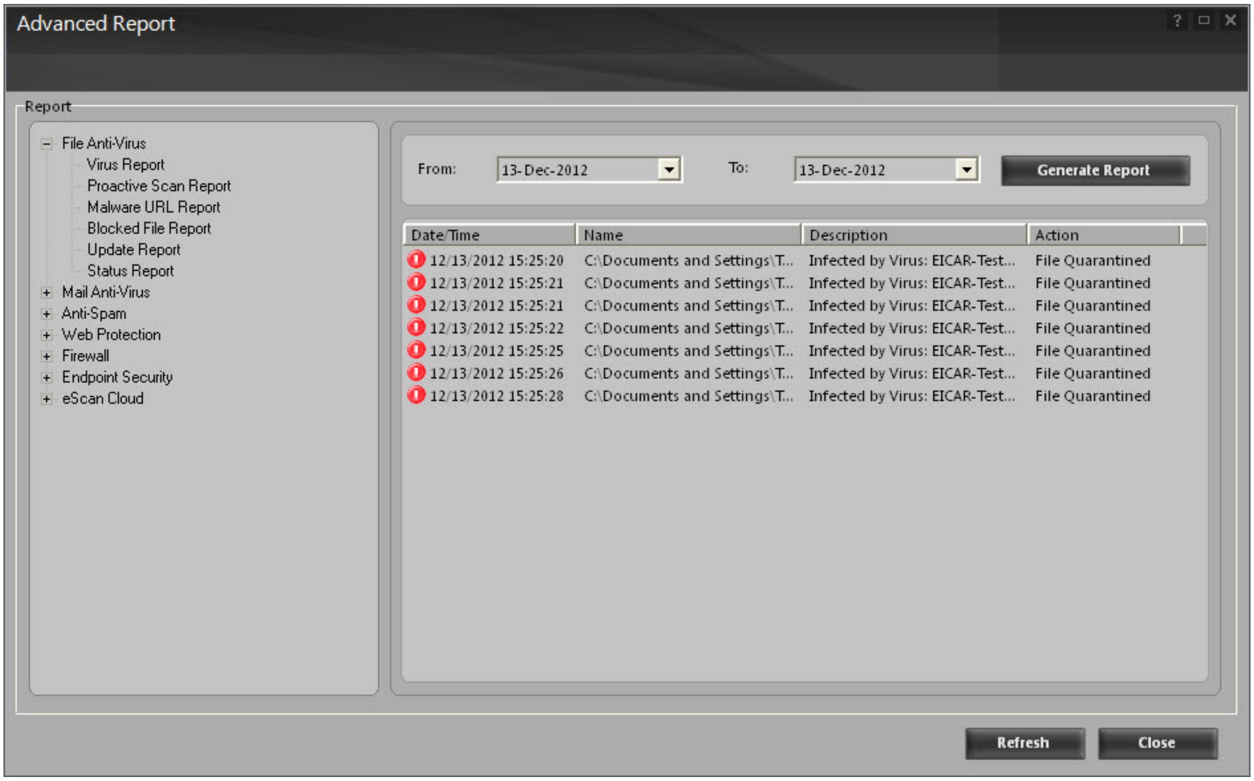
To vaccinate, select an appropriate USB drive, which you want to vaccinate from the **Choose a USB Drive** drop-down list, and click the **Vaccinate** button.

Generating and Viewing Reports

The eScan helps you generate reports for File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Firewall, Endpoint Security, 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 between desired dates. You can select **From** date and **To** date for which you want to generate the report. To generate report between two specific dates, select the desired dates using the **From** and **To** drop down menus present on the interface and click on the **Generate Report** button to view the report. Refer Figure 6.



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

Date/Time	Name	Description	Action
12/13/2012 15:25:20	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	File Quarantined
12/13/2012 15:25:21	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	File Quarantined
12/13/2012 15:25:21	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	File Quarantined
12/13/2012 15:25:22	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	File Quarantined
12/13/2012 15:25:25	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	File Quarantined
12/13/2012 15:25:26	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	File Quarantined
12/13/2012 15:25:28	C:\Documents and Settings\T...	Infected by Virus: EICAR-Test...	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. It also includes the eScan Protection Center (ePC). It allows you to configure the different modules of eScan.

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.

- Secure Delete

  You can now permanently delete files and folders without the fear of having the files retrieved by the use of third-party applications, thus preventing misuse of personal information.

- Dynamic Phishing Filter

The dynamic phishing filter ensures complete protection and keeps you safe online. It protects you from viewing fraudulent e-mails and websites, as eScan now checks and verifies all the websites viewed by you. It warns you before you open a suspicious mail or a website.

- 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

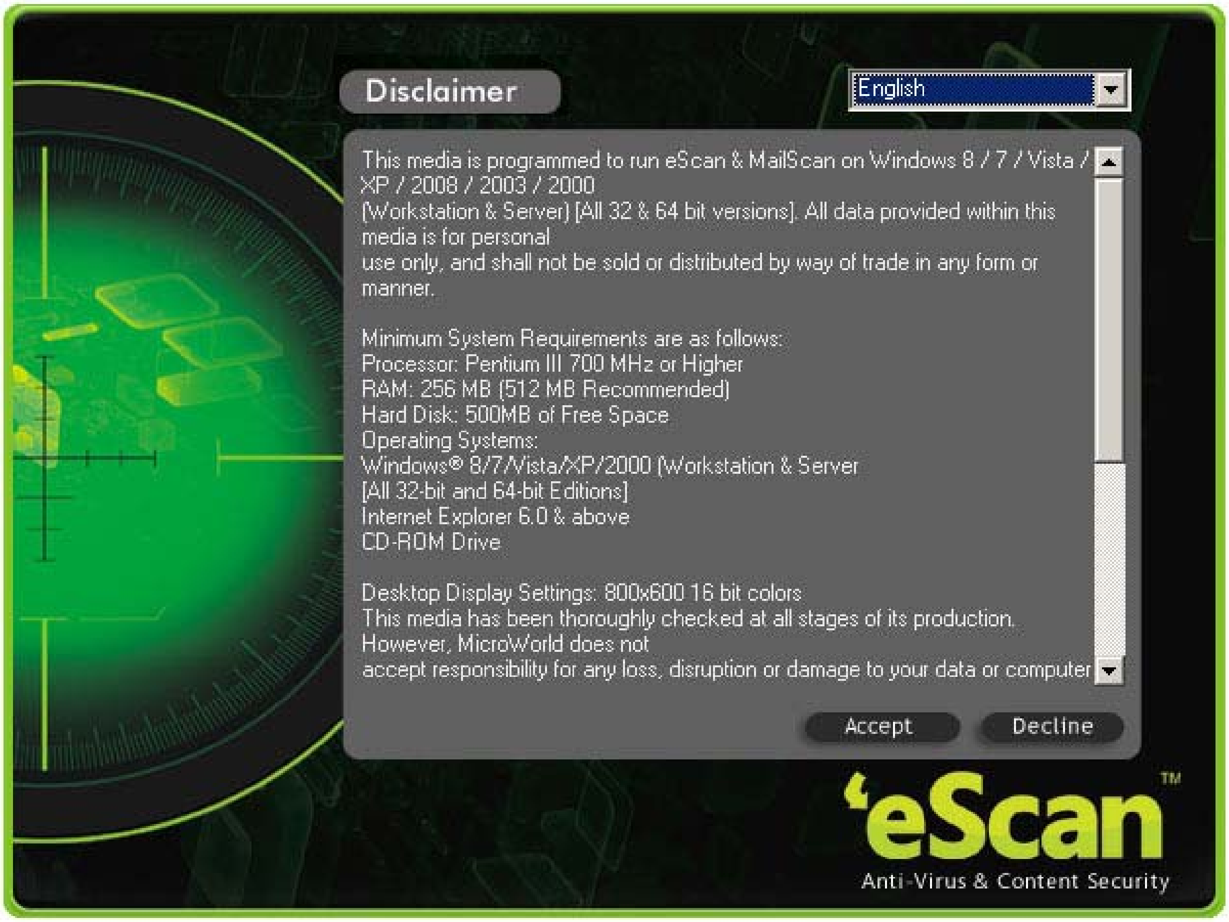
Overview of eScan Product Installation CD

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.

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 Disclaimer is displayed. Select your preferred language from the drop-down list. You can either accept the disclaimer to view the CD's menu or decline it to exit the screen. Refer Figure 7.



This media is programmed to run eScan & MailScan on Windows 8 / 7 / Vista / XP / 2008 / 2003 / 2000
(Workstation & Server) [All 32 & 64 bit versions]. All data provided within this media is for personal
use only, and shall not be sold or distributed by way of trade in any form or manner.

Minimum System Requirements are as follows:
Processor: Pentium III 700 MHz or Higher
RAM: 256 MB (512 MB Recommended)
Hard Disk: 500MB of Free Space
Operating Systems:
Windows® 8/7/Vista/XP/2000 (Workstation & Server
[All 32-bit and 64-bit Editions]
Internet Explorer 6.0 & above
CD-ROM Drive

Desktop Display Settings: 800x600 16 bit colors
This media has been thoroughly checked at all stages of its production.
However, MicroWorld does not
accept responsibility for any loss, disruption or damage to your data or computer

Figure 7

The CD's menu shows the following options. Refer Figure 8.

- **Products:** You can click this button to view information about eScan or install it on your computer.

> You can click the **QRG** button to view the Quick Reference Guide for eScan in the PDF format.

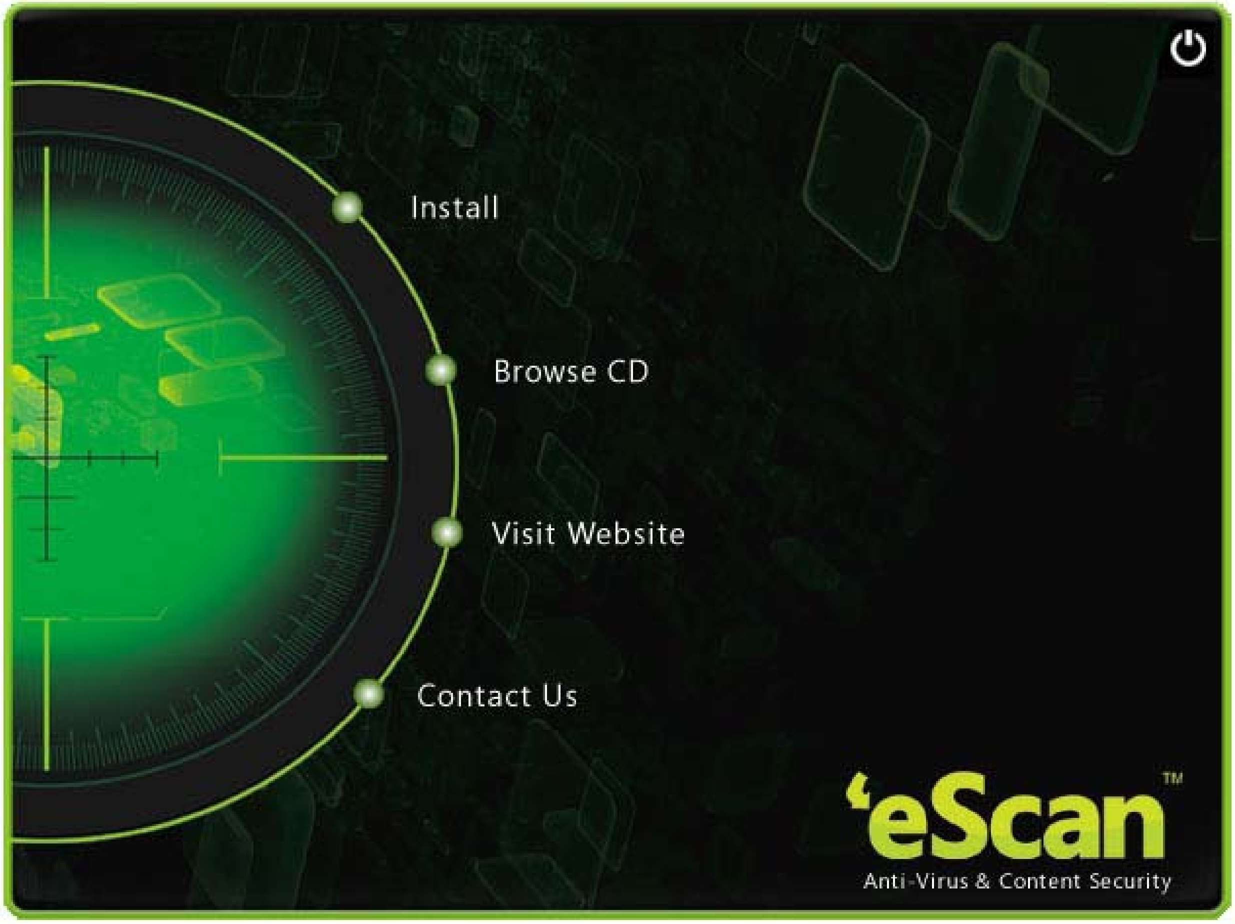


Figure 8

- 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 Internet Security Suite (ISS) 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.

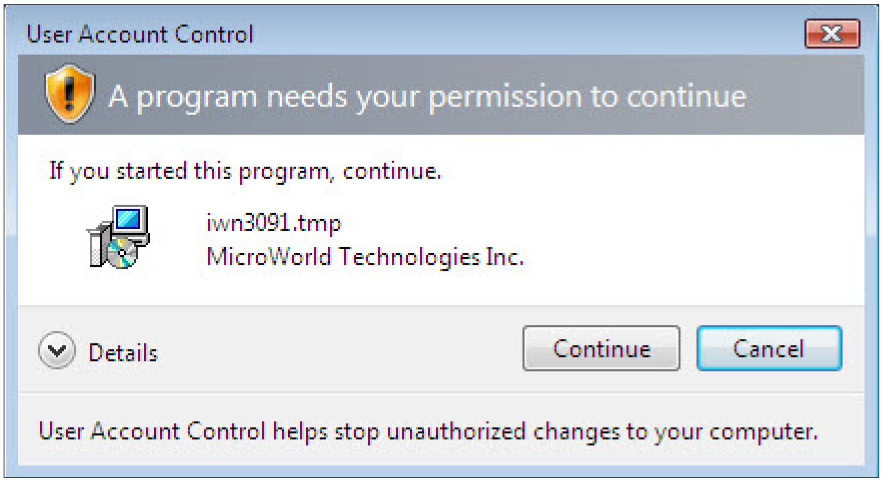
On some computers autorun of CD/DVD option is disabled. In such cases, you can manually start the installation by double-clicking the AUTORUN.exe in the CD-ROM drive window. This will display a dialog box containing options for selecting the language.

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 ISS on your computer

Special instructions for Installing eScan ISS 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 ISS, a **User Access Control** dialog box appears asking you for permission to run iwn2[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**. Refer Figure 9.



User Account Control

A program needs your permission to continue

If you started this program, continue.

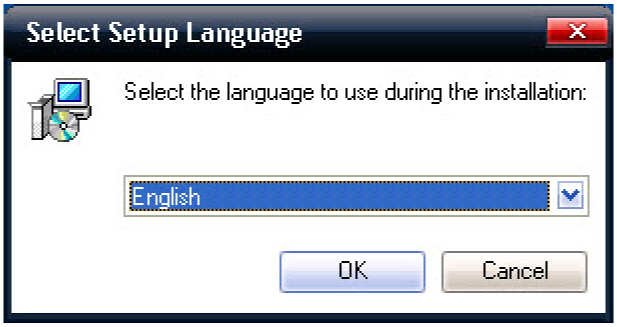
iwn3091.tmp
MicroWorld Technologies Inc.

User Account Control helps stop unauthorized changes to your computer.

Figure 9

STEP 1 – Choosing the Language

eScan for ISS is available in many languages, such as English, German, French, Netherlands, Italiano, Portuguese, Spanish, Turkish, Chinese Simplified, Chinese Traditional, Greek, Korean, Norwegian, Russian, Polish, and Latin Spanish. Refer Figure 10.



Select Setup Language

Select the language to use during the installation:

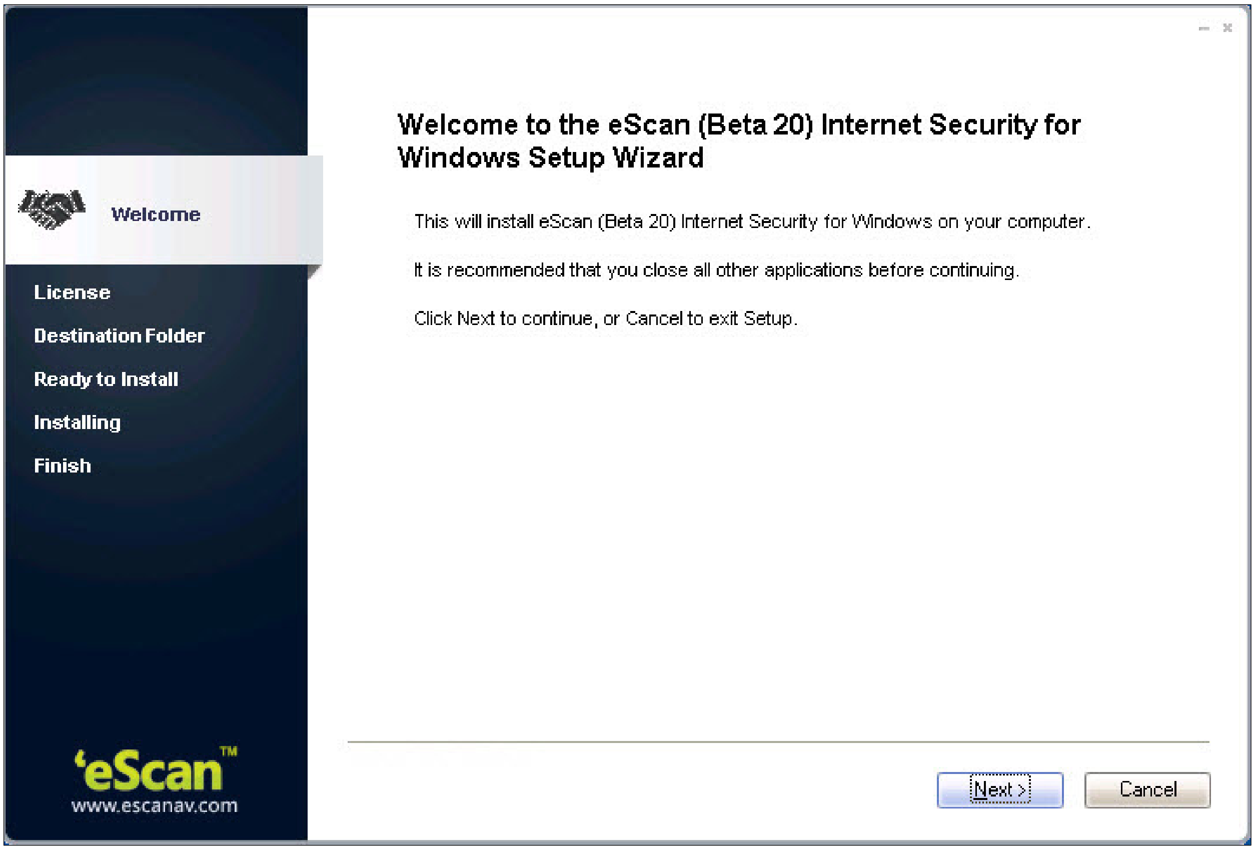
English

Figure 10

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

STEP 2 - Installation Wizard Welcome Screen

The welcome screen helps you decide whether you want to proceed with the installation of eScan. Refer Figure 11.



Welcome to the eScan (Beta 20) Internet Security for Windows Setup Wizard

This will install eScan (Beta 20) Internet Security for Windows on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 11

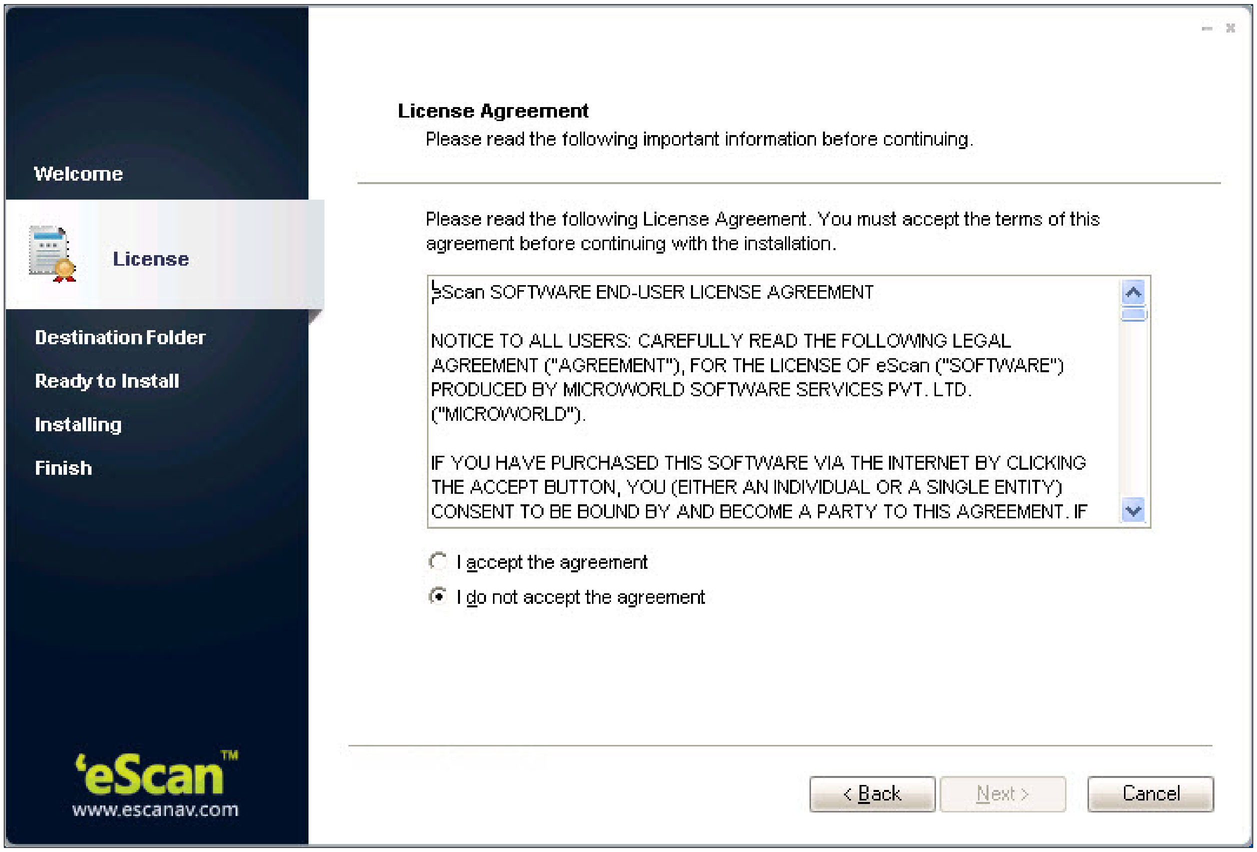
To proceed with the installation, click **Next**. This will display the **License Agreement** screen.

Alternatively, if you do not wish to proceed, you can click **Cancel**. This will cancel the installation and close the wizard.

STEP 3 - License Agreement

This screen displays the EULA for eScan. Please read it carefully.

To accept the EULA, on the **License Agreement** screen, click **I accept the agreement**, and then click **Next**. This will display the **Select Destination Location** screen. Refer Figure 12.



License Agreement
Please read the following important information before continuing.

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. ("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

○ I accept the agreement
● I do not accept the agreement

Figure 12

Alternatively, if you do not wish to accept the EULA, you can click **Cancel**. This will cancel the installation and close the wizard.

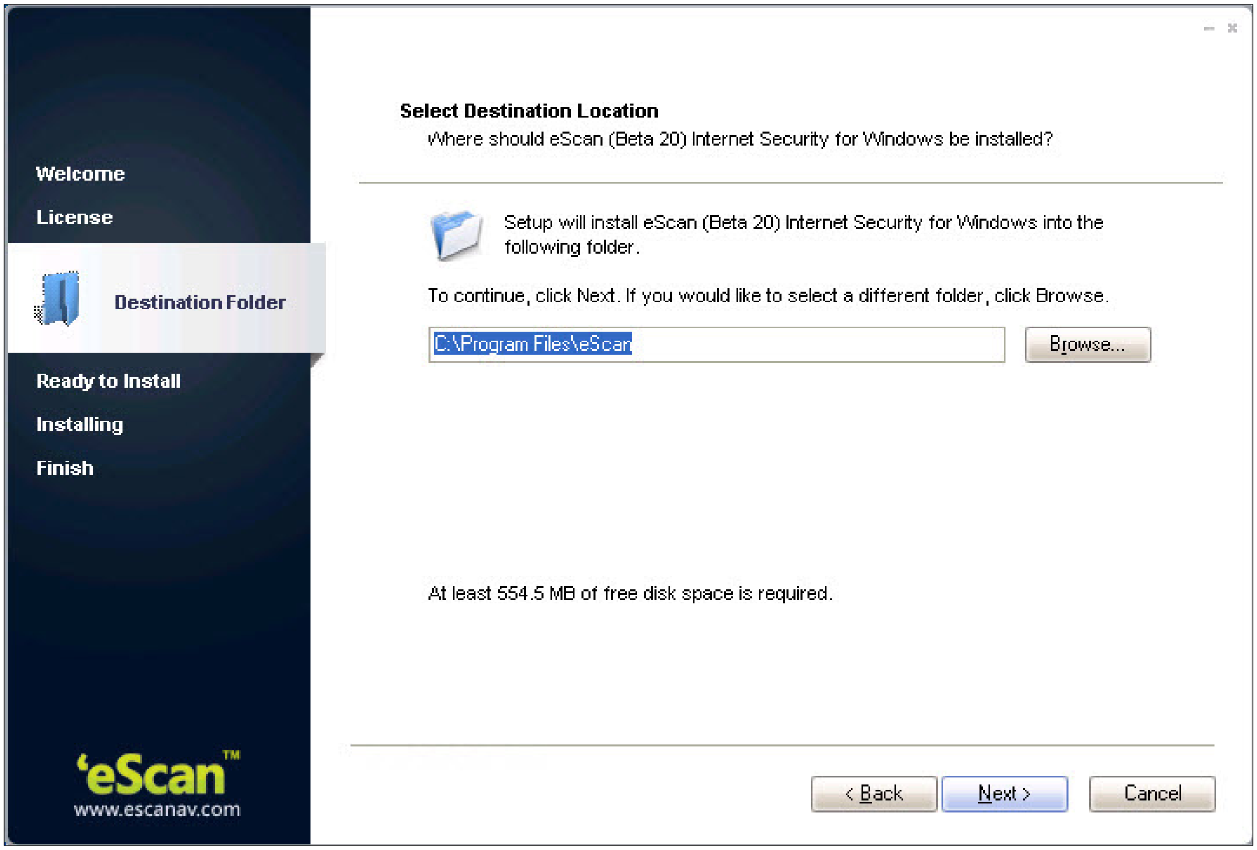
STEP 4 - Selecting the Installation Folder

In this step, you can select the drive and folder in which you want to install eScan.

To select the eScan installation folder on your computer, on the **Select Destination Location** screen, in the box, either type the path of the folder or click **Browse** to browse to the folder, and then click **Next**. Refer Figure 13.

✍ The default path for 32-bit computer: ***[Disk Drive]*\Program Files\eScan**

✍ The default path for 64-bit computers: ***[Disk Drive]*\Program Files (x86)\eScan**



Select Destination Location

Where should eScan (Beta 20) Internet Security for Windows be installed?

Setup will install eScan (Beta 20) Internet Security for Windows into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\eScan

At least 554.5 MB of free disk space is required.

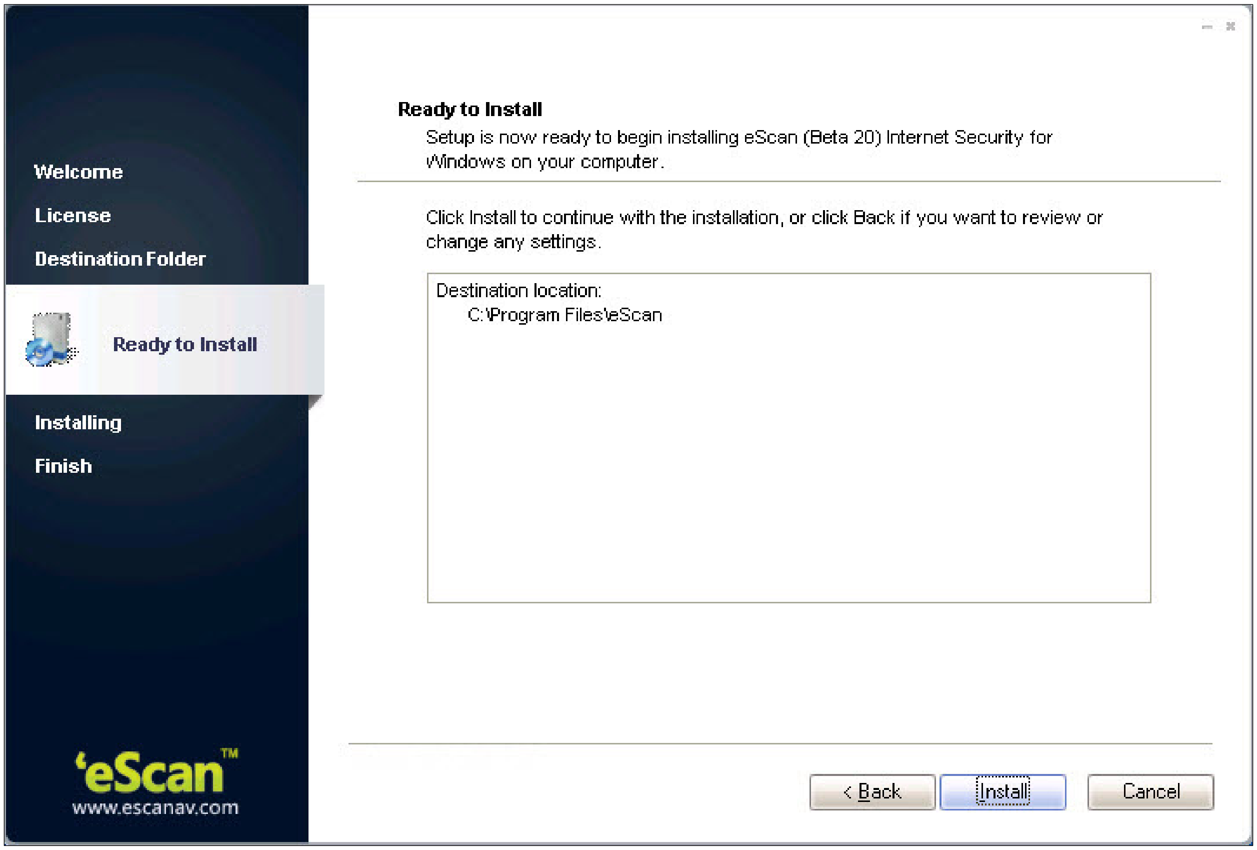
Figure 13

Alternatively, if you need to view the EULA, you can click **Back** to navigate to the **License Agreement** screen.

However, if you do not wish to proceed, you can click **Cancel**. This will cancel the installation and close the wizard.

STEP 5 – Viewing the Summary Report Before Installation

This window displays a summary of the options that you have selected on the previous screens of the wizard. This step completes the preparation for installing the application on your computer. You can click the **Back** button to review or change the settings that you have made on the previous screens. Refer Figure 14.



Ready to Install

Setup is now ready to begin installing eScan (Beta 20) Internet Security for Windows on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\eScan

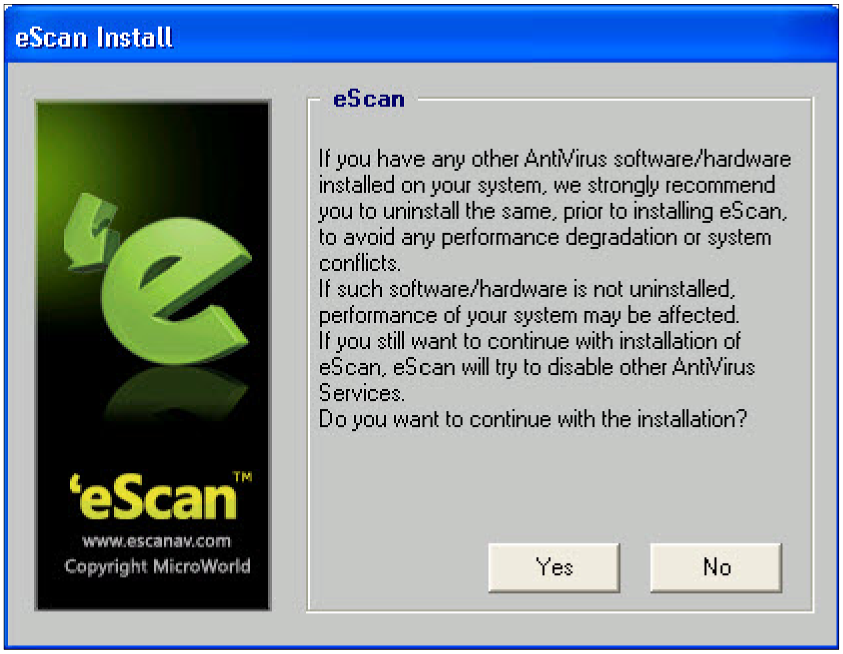
Figure 14

To proceed with the installation, click **Install**. When you click Install, the wizard should start installing eScan on the computer.

However, if you do not wish to proceed, you can cancel the installation by clicking **Cancel**.

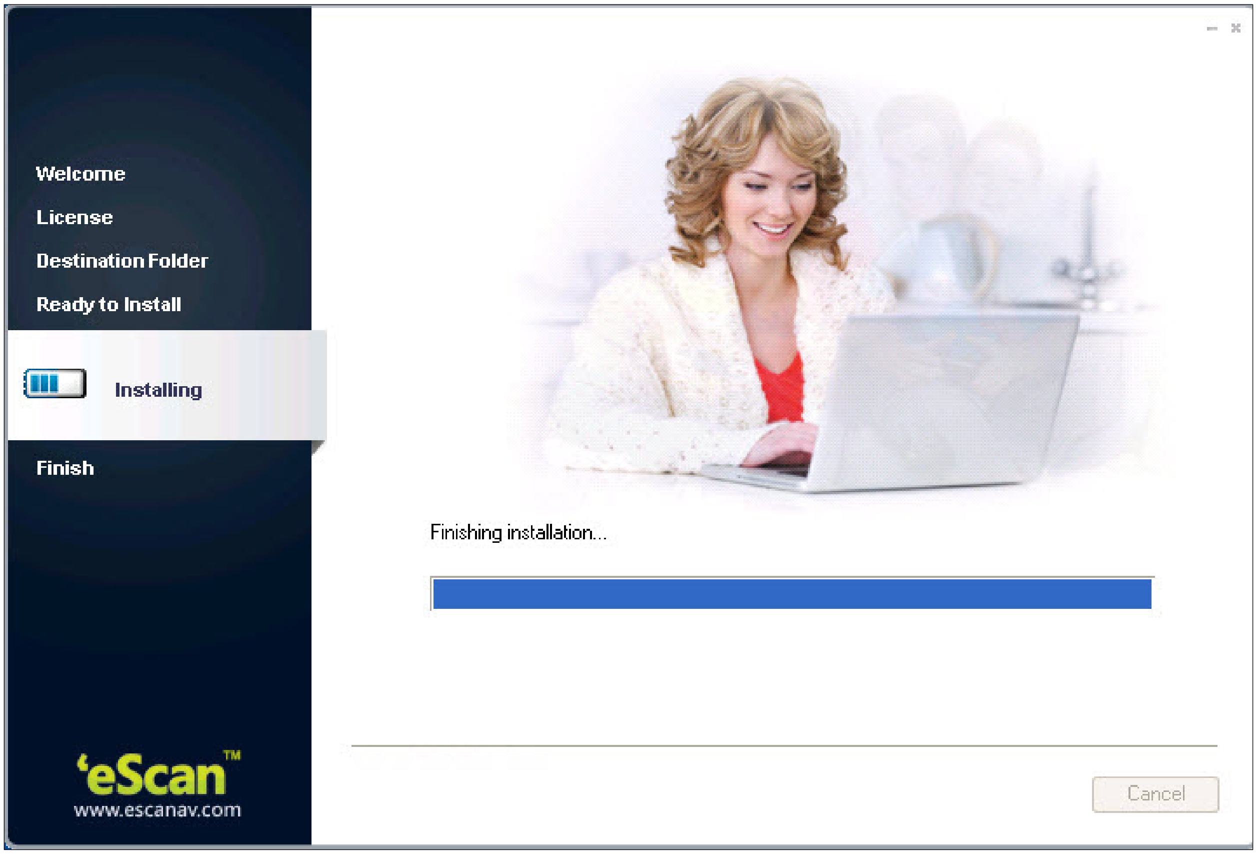
STEP 6 – Install eScan

During the installation process, the wizard searches your computer for other Anti-Virus programs that may conflict with the eScan installation and prompts you to remove them. If there are no conflicting programs, the wizard proceeds with the installation. Refer Figure 15, Figure 16, Figure 17, Figure 18, and Figure 19.



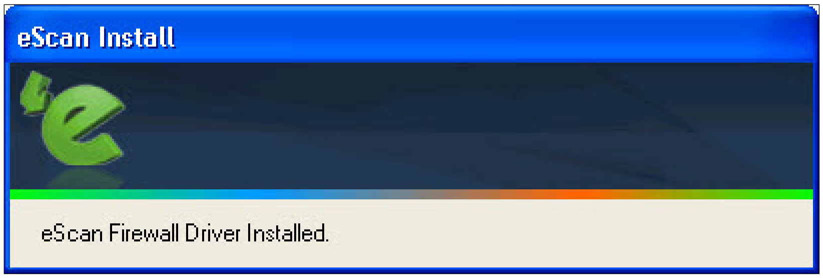
If you have any other AntiVirus software/hardware installed on your system, we strongly recommend you to uninstall the same, prior to installing eScan, to avoid any performance degradation or system conflicts.
If such software/hardware is not uninstalled, performance of your system may be affected.
If you still want to continue with installation of eScan, eScan will try to disable other AntiVirus Services.
Do you want to continue with the installation?

Figure 15



Finishing installation...

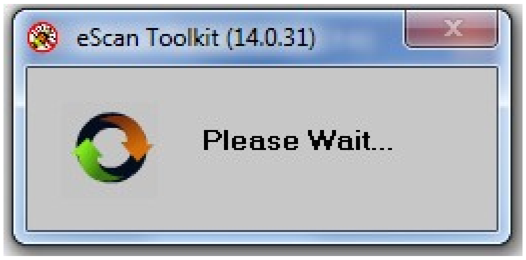
Figure 16



eScan Firewall Driver Installed.

Figure 17

If you do not wish to proceed, you can cancel the installation by clicking **Cancel**. Refer Figure 18.

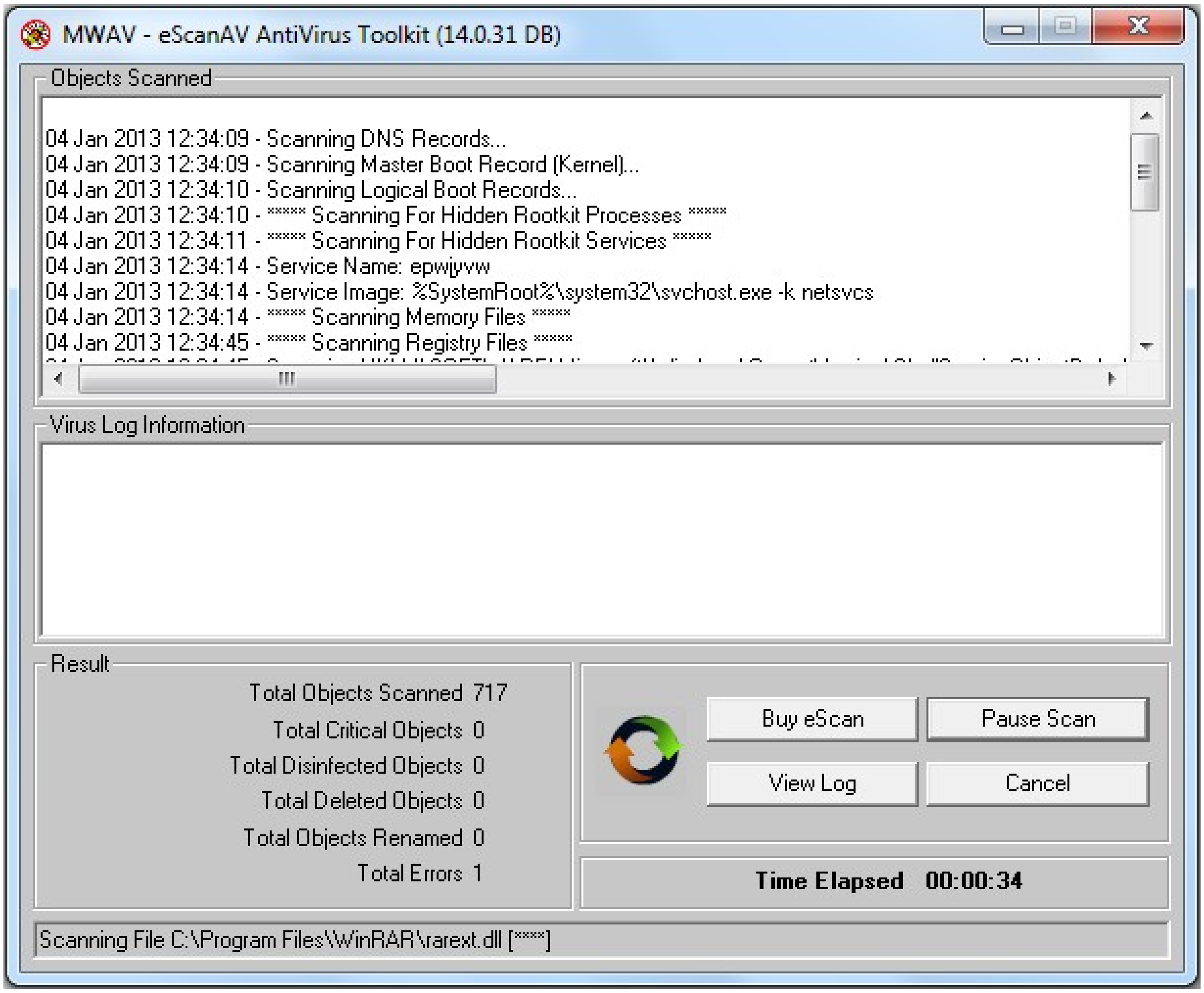


eScan Toolkit (14.0.31)

Please Wait...

Figure 18

The eScan setup also runs eScan Anti-Virus Toolkit. This tool scans and removes the viruses and spyware found on your computer. Refer Figure 19.



MWAV - eScanAV AntiVirus Toolkit (14.0.31 DB)

Objects Scanned

```
04 Jan 2013 12:34:09 - Scanning DNS Records...
04 Jan 2013 12:34:09 - Scanning Master Boot Record (Kernel)...
04 Jan 2013 12:34:10 - Scanning Logical Boot Records...
04 Jan 2013 12:34:10 - ***** Scanning For Hidden Rootkit Processes *****
04 Jan 2013 12:34:11 - ***** Scanning For Hidden Rootkit Services *****
04 Jan 2013 12:34:14 - Service Name: epwjyvw
04 Jan 2013 12:34:14 - Service Image: %SystemRoot%\system32\svchost.exe -k netsvcs
04 Jan 2013 12:34:14 - ***** Scanning Memory Files *****
04 Jan 2013 12:34:45 - ***** Scanning Registry Files *****
```

Virus Log Information

Result

Total Objects Scanned 717
Total Critical Objects 0
Total Disinfected Objects 0
Total Deleted Objects 0
Total Objects Renamed 0
Total Errors 1

Time Elapsed 00:00:34

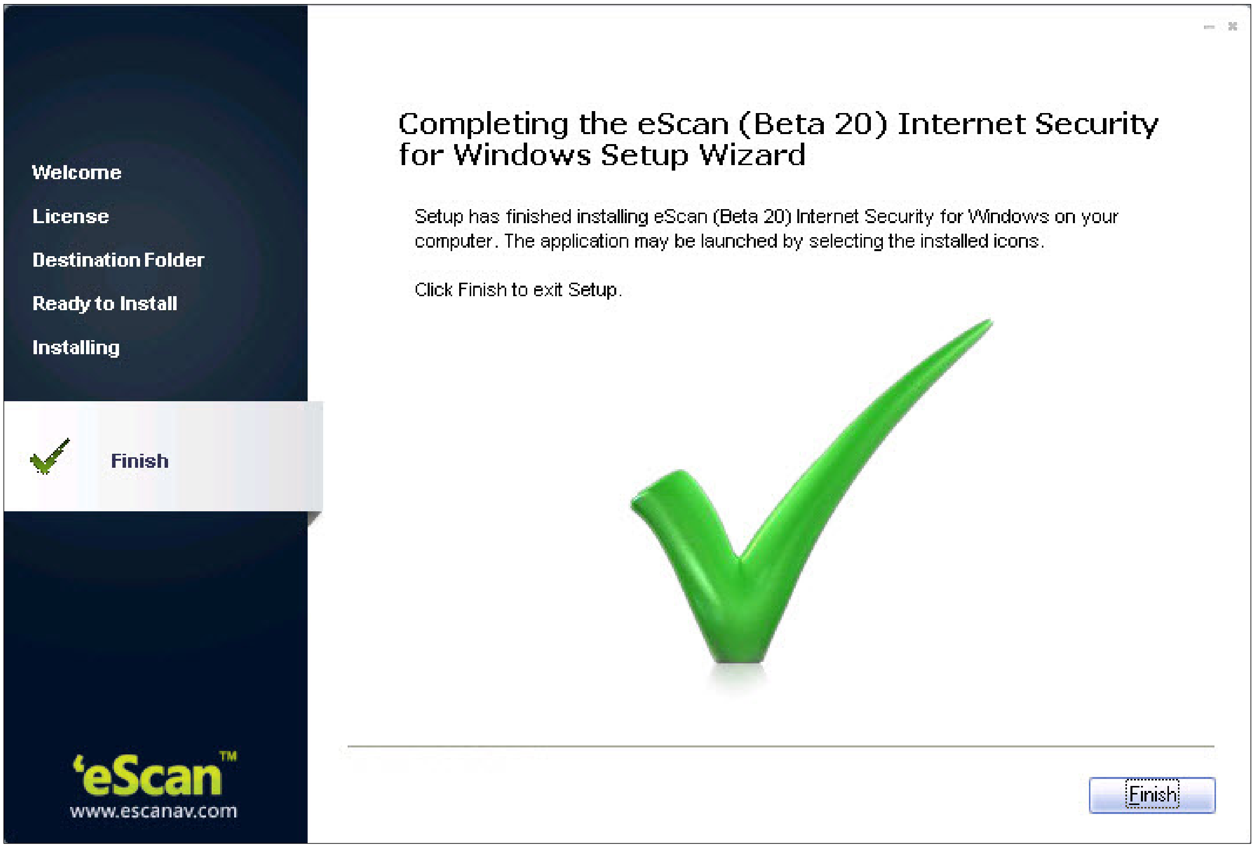
Scanning File C:\Program Files\WinRAR\rarext.dll [****]

Figure 19

STEP 7 - Completing the Installation

After completing all the tasks, the eScan gets installed on your computer. Refer Figure 20.

✍ After eScan installation, an option for rebooting the system appears, incase if eScan Firewall driver requires rebooting to apply settings.



Completing the eScan (Beta 20) Internet Security for Windows Setup Wizard

Setup has finished installing eScan (Beta 20) Internet Security for Windows on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

Figure 20

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. Refer Figure 21.

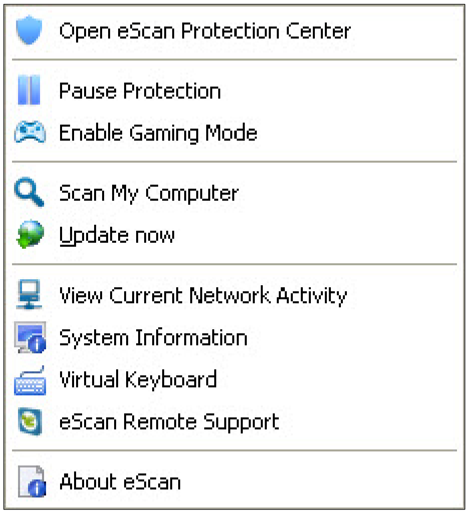


Figure 21

You can access eScan for ISS 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 Internet Security Suite for Home and Small Office product comes with a 30 days trial period. You should purchase the product license key before the trial period expires, wherein you receive a license key for registration. You can also renew the product, as per your requirement.

To know information on registration and renewing your eScan product, visit the below link

http://www.escanav.com/register

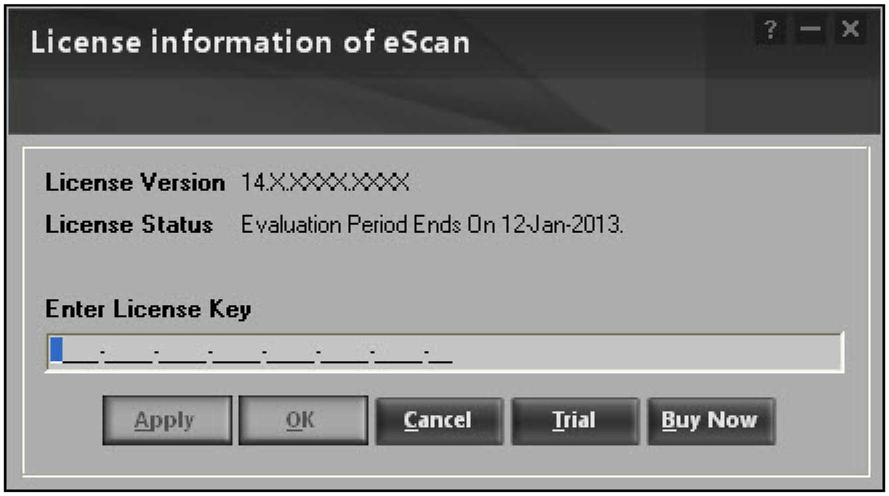
Contents

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. Refer Figure 22.



License information of eScan

License Version 14.X.XXXX.XXXX

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

Enter License Key

Figure 22

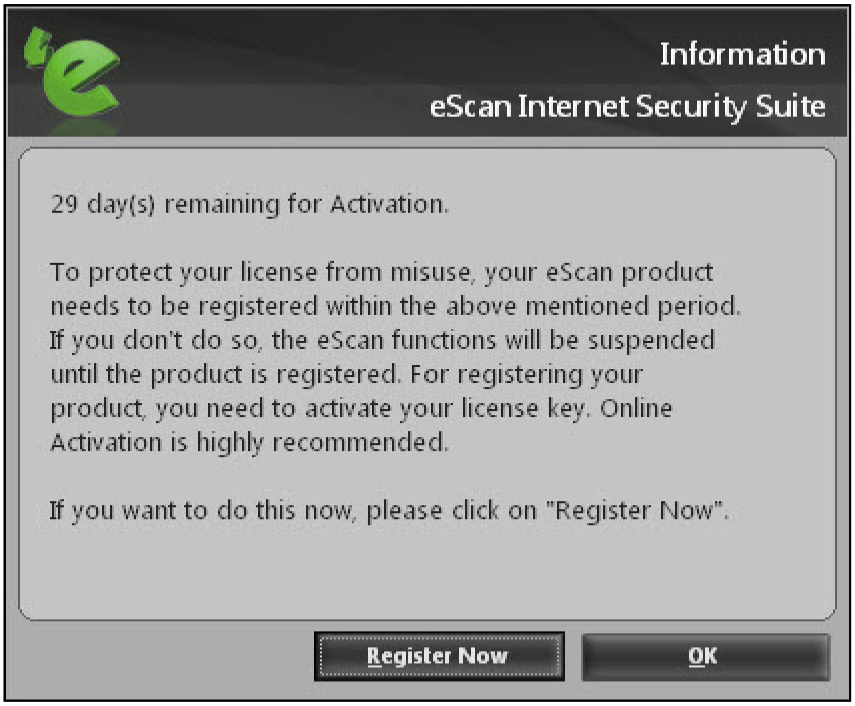
1. Type the 30-character valid license key in the **Enter License Key** field.

✍ 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.

✍ 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.

2. Click the **Apply** button, and then click the **OK** button.
   The **Information** dialog box appears. Refer Figure 23.



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 23

3. Click the **OK** button.
   The license information gets updated.

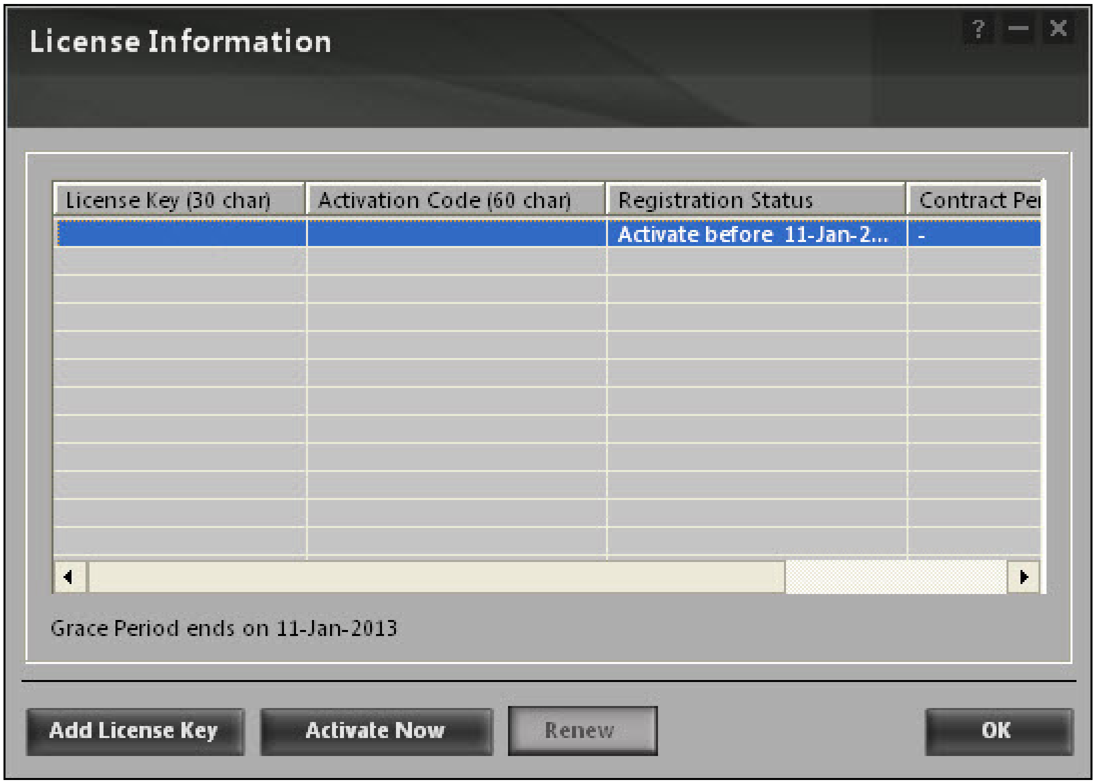
Activating the License Key

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 23.
   - **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. Refer Figure 24.



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

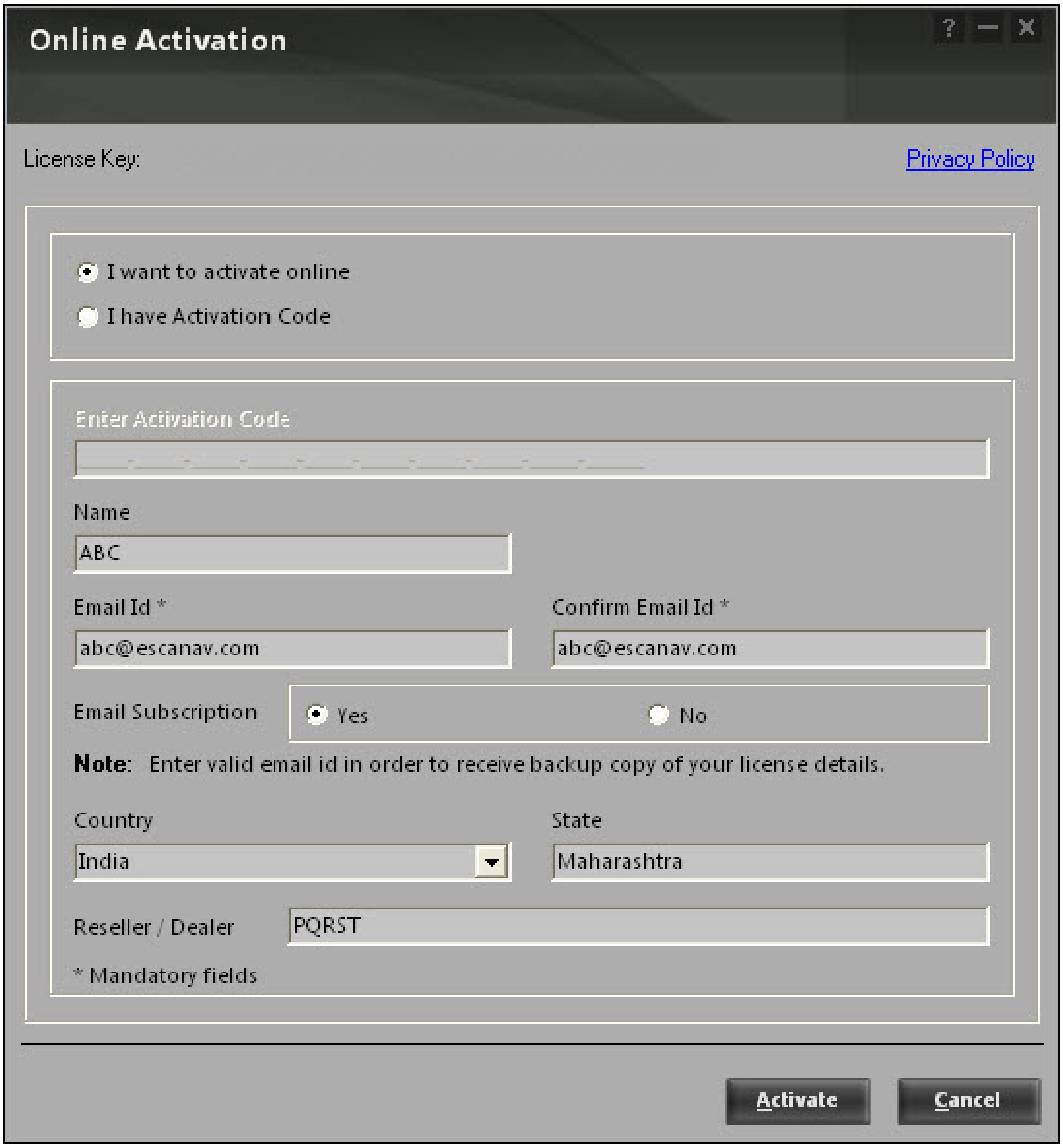
Grace Period ends on 11-Jan-2013

Figure 24

4. 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. Refer Figure 25.



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

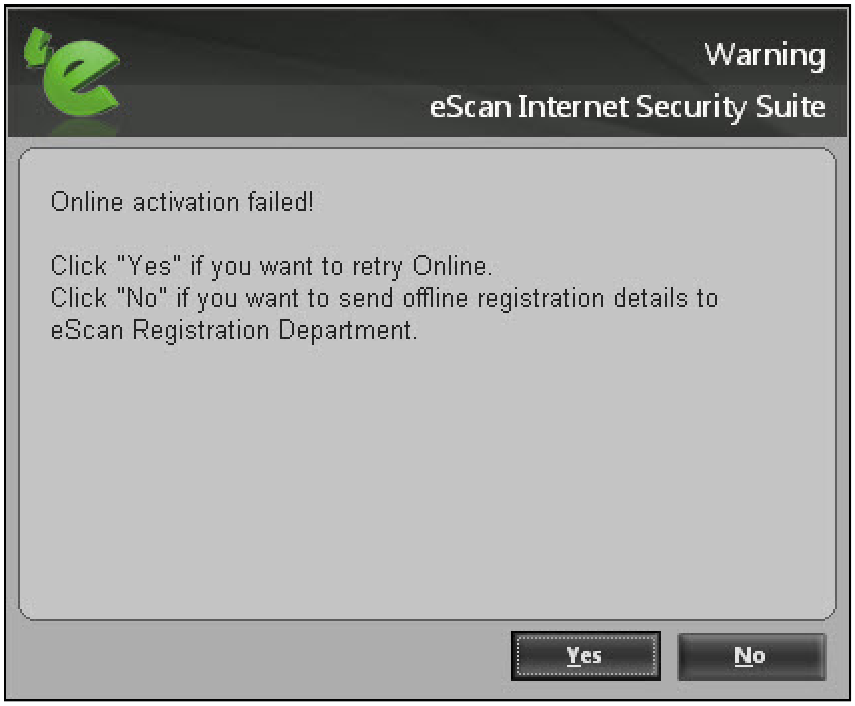
State: Maharashtra

Reseller / Dealer: PQRST

* Mandatory fields

Figure 25

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. 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.  Online activation failed! Click "Yes" if you want to retry Online. Click "No" if you want to send offline registration details to eScan Registration Department. **Figure 26** Click the **No** button, an OnlineRegister.TXT file gets generated with registration details, You have to send the OnlineRegister.TXT file to register@escanav.com, wherein you receive an activation code to the specified e-mail ID.
I have Activation Code	When you click this option only **Enter Activation Code** field is available. Click this option, if you already have activation code received through an e-mail from register@escanav.com. In the **Enter Activation Code** field, type or copy and paste the activation

Field	Description
	code. This enables you to activate the eScan product immediately.
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 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. 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. Click an appropriate option. ● **Yes:** Click this option if you want to subscribe for e-mails. ● **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.

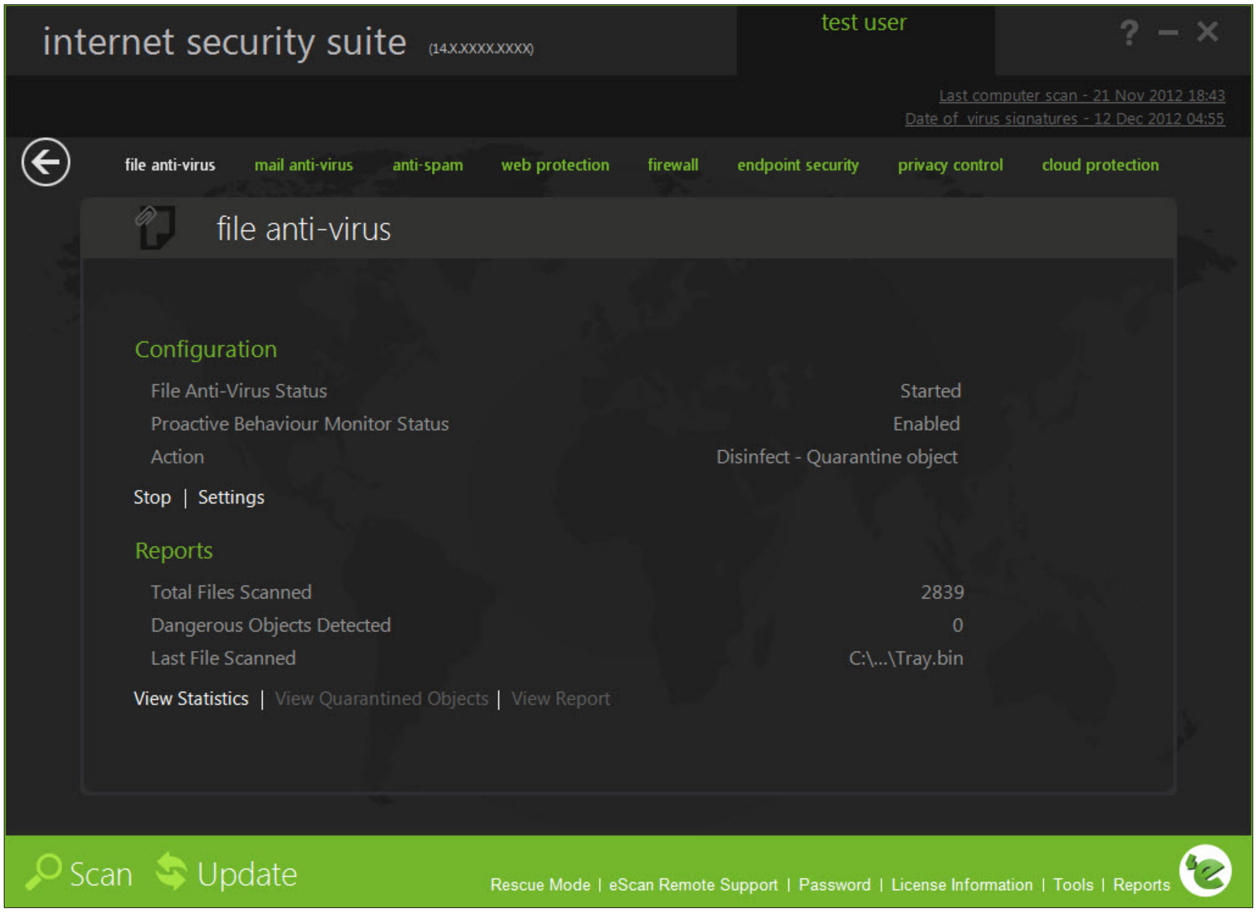
7. Click the **Activate** button.
   The license key gets activated.

eScan for ISS Features

The eScan Internet Security Suite for Home and Small Office contains eight comprehensive modules — **File Anti-Virus**, **Mail Anti-Virus**, **Anti-Spam**, **Web Protection**, **Firewall**, **Endpoint Security**, **Privacy Control**, and **Cloud Protection** and two additional options for Scan and Update.

File Anti-Virus

File Anti-Virus is the first module of the eScan for ISS. 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. Refer Figure 27.



Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55

Configuration

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

Stop | Settings

Reports

Total Files Scanned: 2839
Dangerous Objects Detected: 0
Last File Scanned: C:\...\Tray.bin

View Statistics | View Quarantined Objects | View Report

Figure 27

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 to be 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:

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

Default: Click this button to apply the default settings.

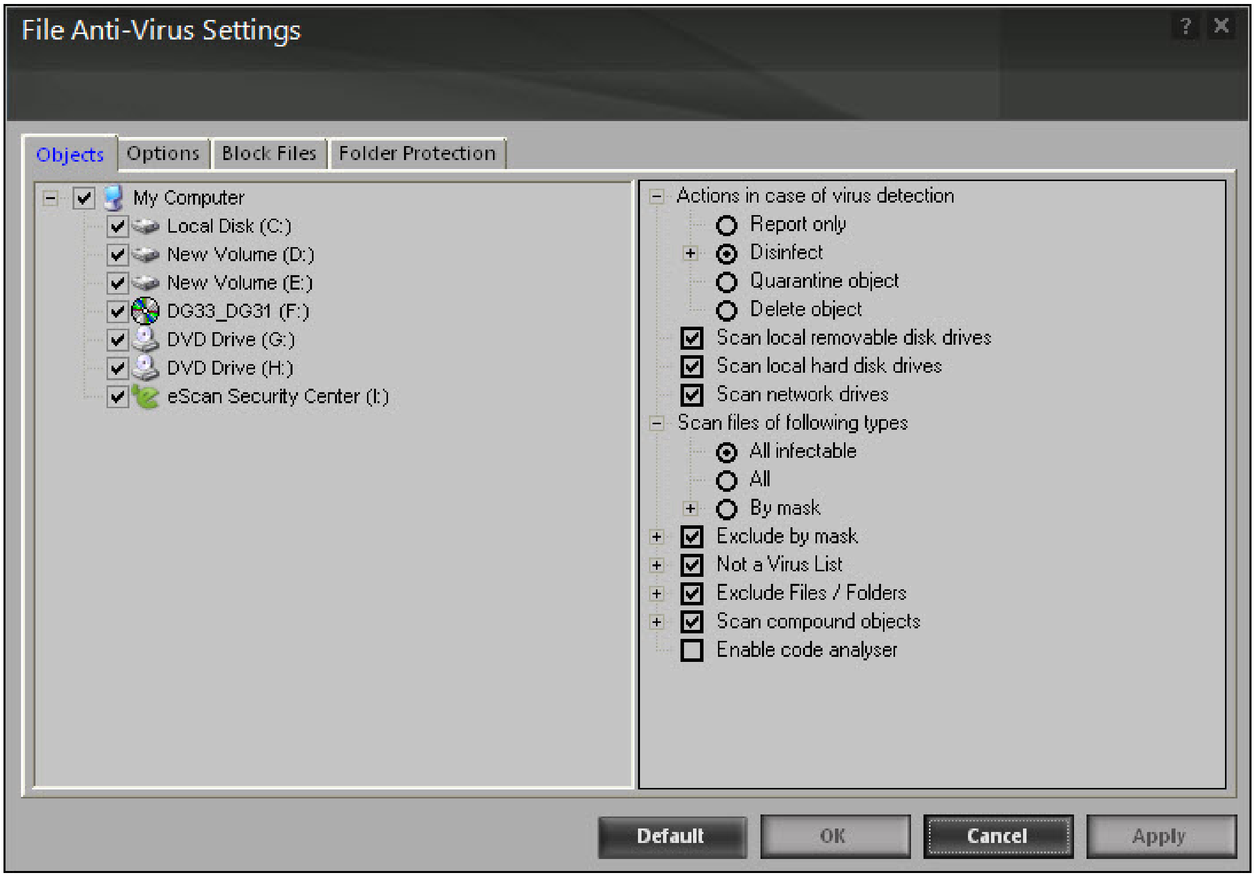
OK: Click this button after you click the **Apply** button to apply the configured settings.

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

Apply: Click this button to apply the configured settings.

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. Refer Figure 28.



- ☑ 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 28

- **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 infected, 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.

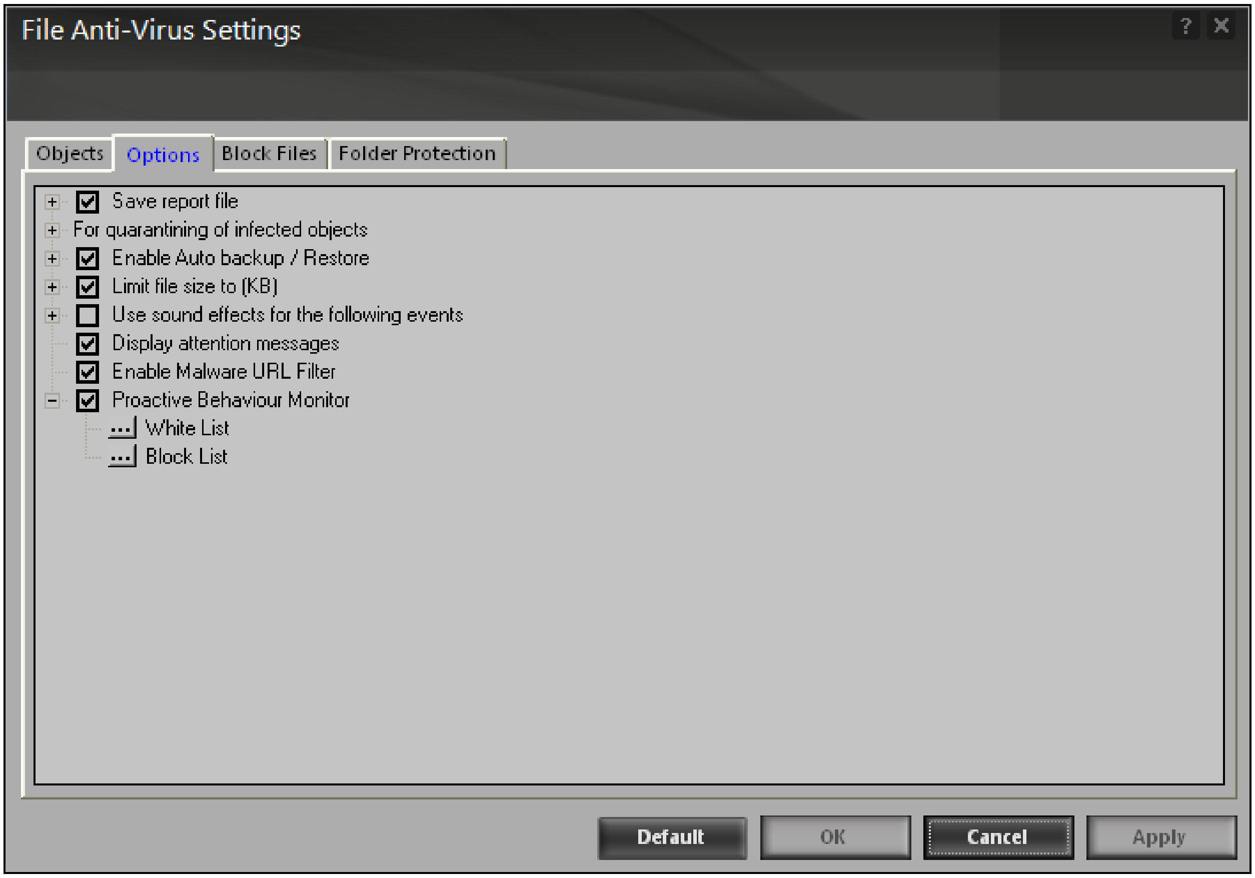
- **Exclude Files/Folders:** [Default] Select this check box if you want File Anti-Virus to exclude all the listed files, folders, and sub-folders, while it is monitoring or scanning folders. You can add or delete folders from the existing list of folders by double-clicking the **Add / Delete** option.

- **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. Refer Figure 29.



- ☑ Save report file
- For quarantining of infected objects
- ☑ Enable Auto backup / Restore
- ☑ Limit file size to (KB)
- ☐ Use sound effects for the following events
- ☑ Display attention messages
- ☑ Enable Malware URL Filter
- ☑ Proactive Behaviour Monitor
  - White List
  - Block List

Figure 29

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

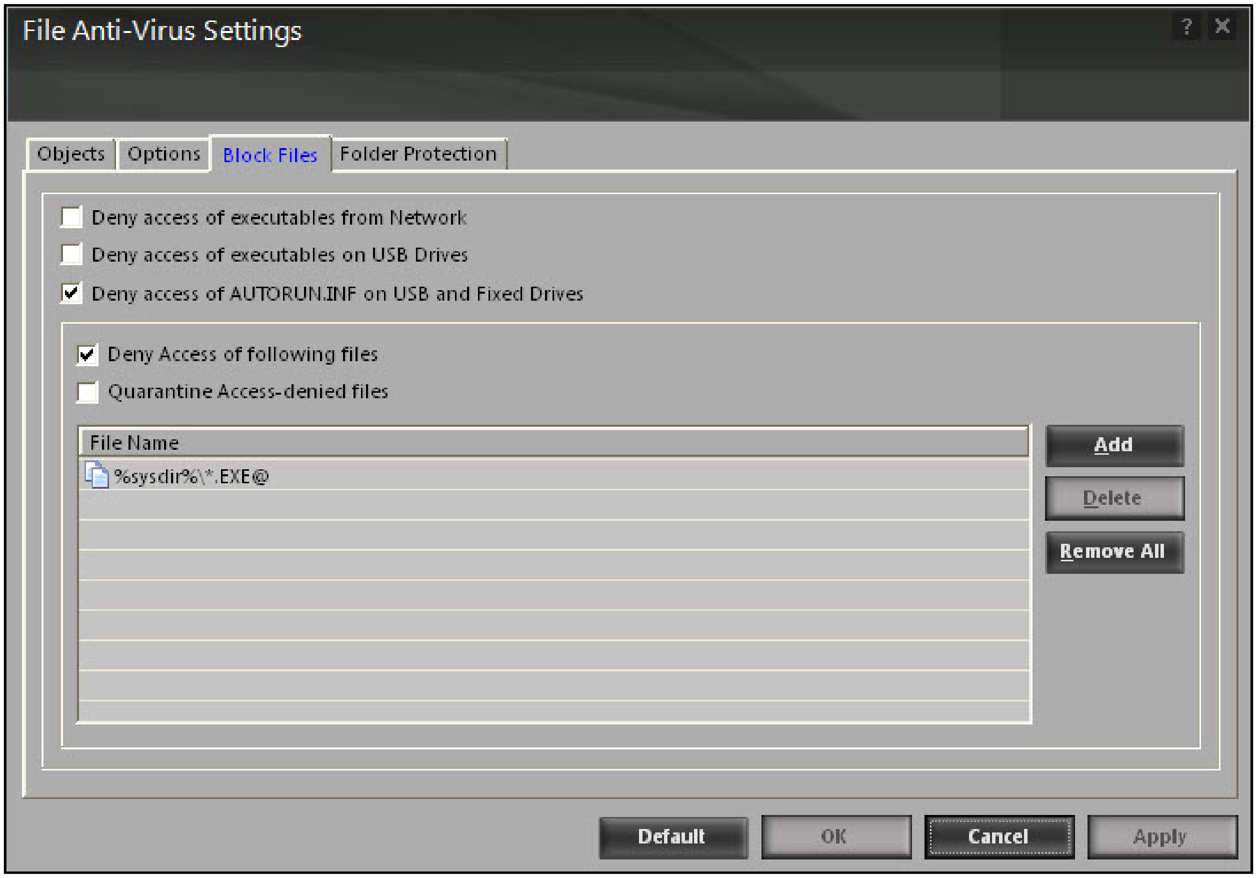
- **For quarantining of infected objects:** This option helps you specify the destination for storing quarantined objects. By default, the quarantined objects are stored in the C:\Program Files\eScan\Infected folder. You can change the location of the destination folder if required.
- **Enable Auto backup / 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:** eScan backs up uninfected objects and store them in a given folder. By default, these objects are stored in a folder named Fbackup on the drive that has maximum free space. You can change the path of the destination folder if desired.
  - **Do not backup files above size (KB):** [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** MB, 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 Behaviour 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.

  It also allows you to view the list of files that are blocked from executing on the system. You can add a File to White list or Block List through options present on Right Click in Generated Report table .

- ### Block Files

This tab helps you configure settings for preventing executables and files, such as autorun.inf, on network drives, USB drives, and fixed drives from accessing your computer. Refer Figure 30.



File Anti-Virus Settings

☐ 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

File Name
%sysdir%*.EXE@

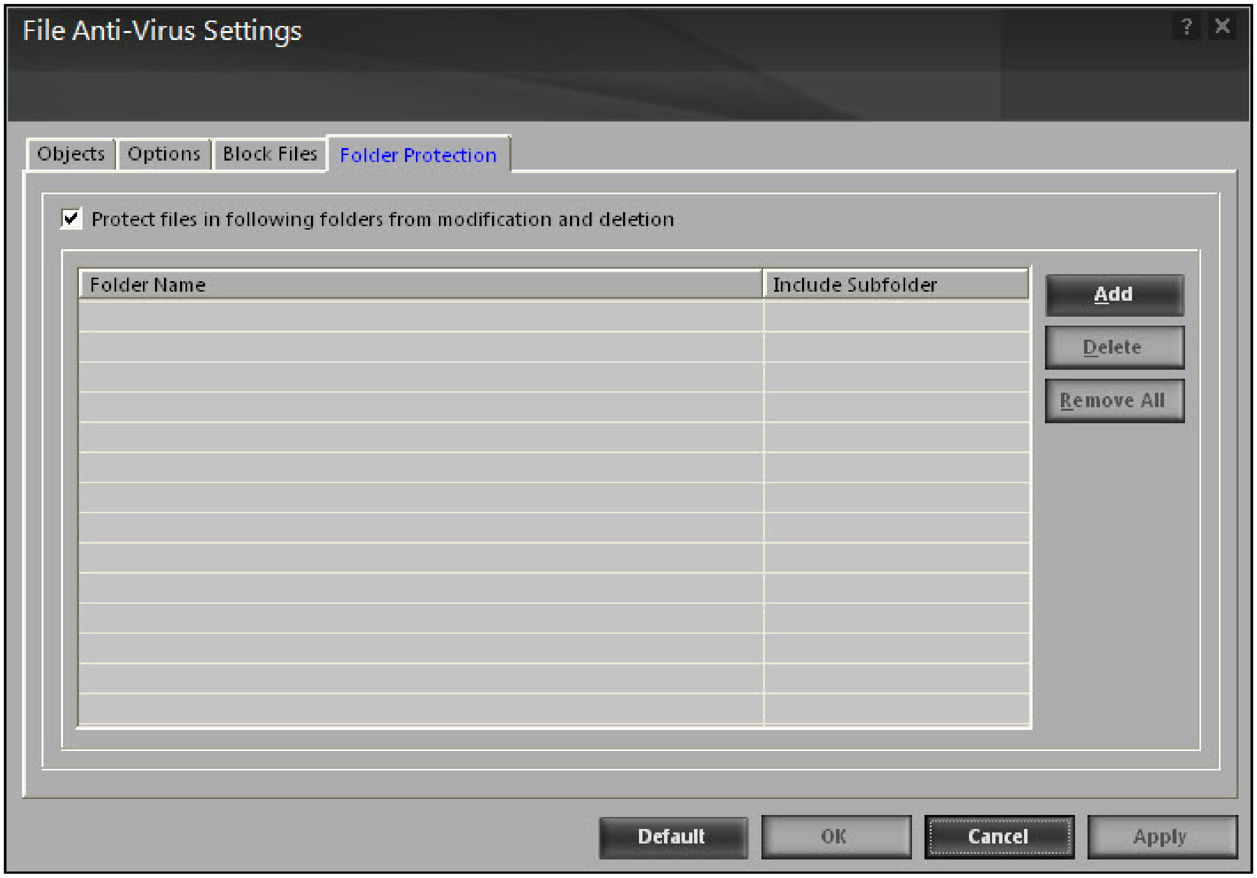
Figure 30

You can configure the following settings:

- **Deny access of executable from Network:** Select this check box if you want to prevent executables from network from being executed on your computer.
- **Deny access of executables on USB Drives:** Select this check box if you want to prevent executables stored on USB drives from being executed.
- **Deny access of AUTORUN.INF on USB and Fixed Drives:** [Default] Select this check box if you want to prevent Autorun.inf from execution.
- **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. Refer Figure 31.



☑ Protect files in following folders from modification and deletion

Figure 31

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

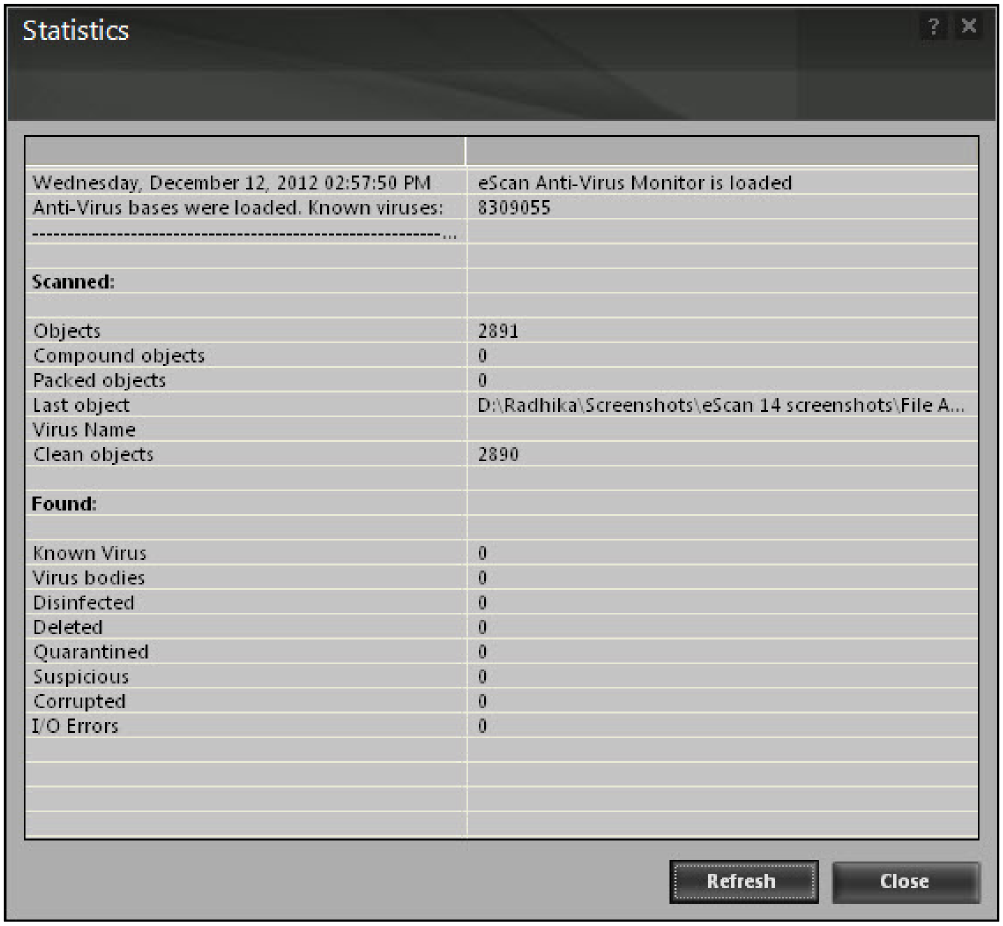
This section displays the following information. Refer Figure 27.

- **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. Refer Figure 32.



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

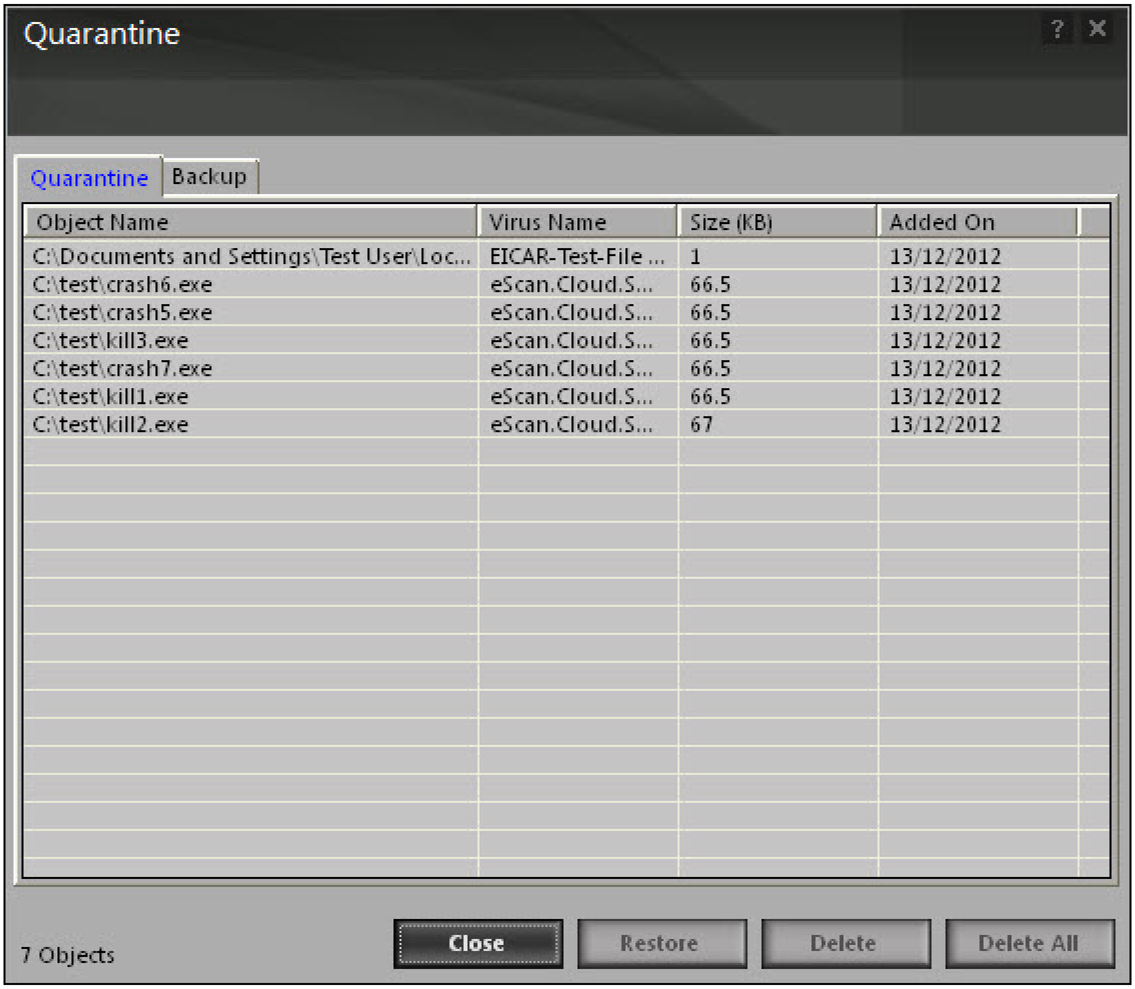
Figure 32

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: Refer Figure 33.



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

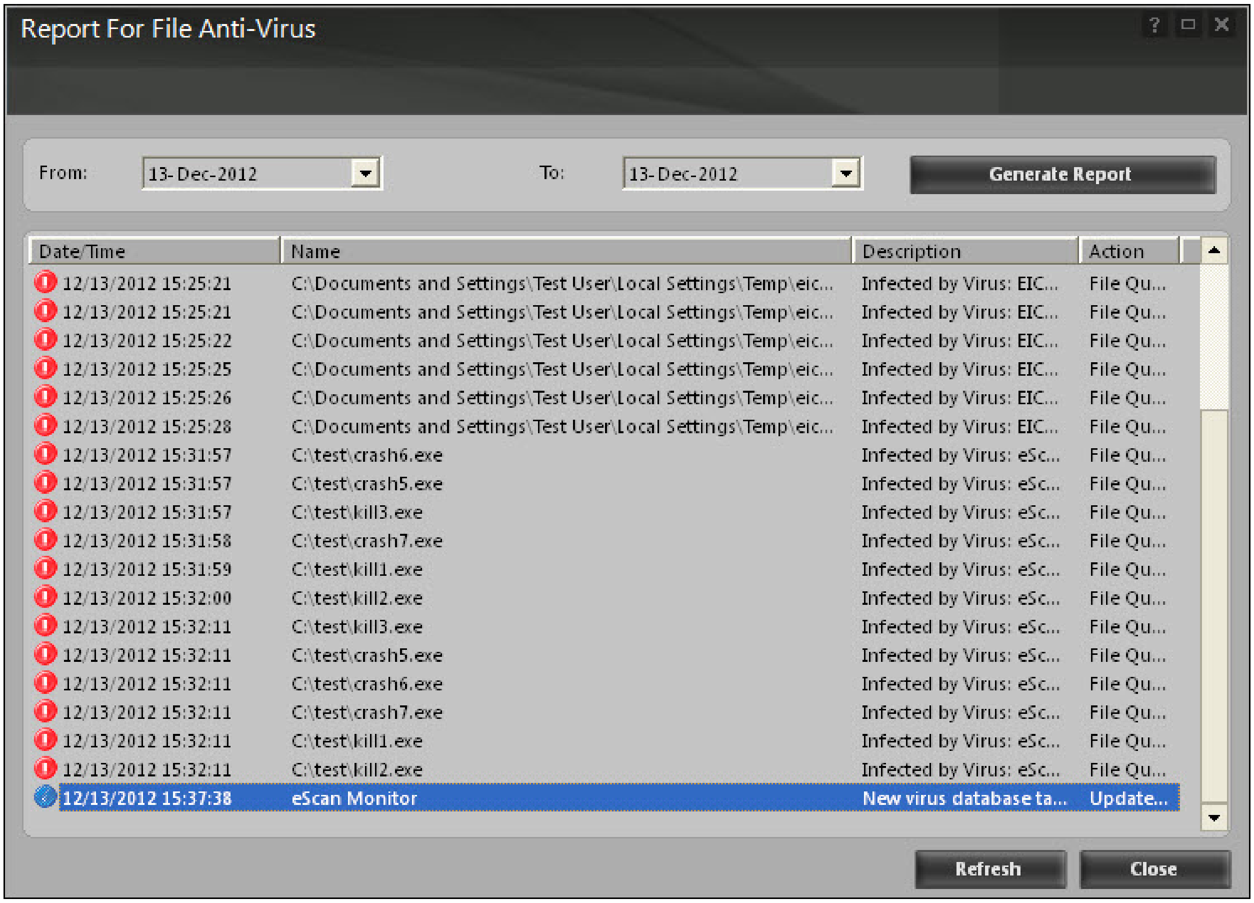
7 Objects

Figure 33

- 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. Refer Figure 34.



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

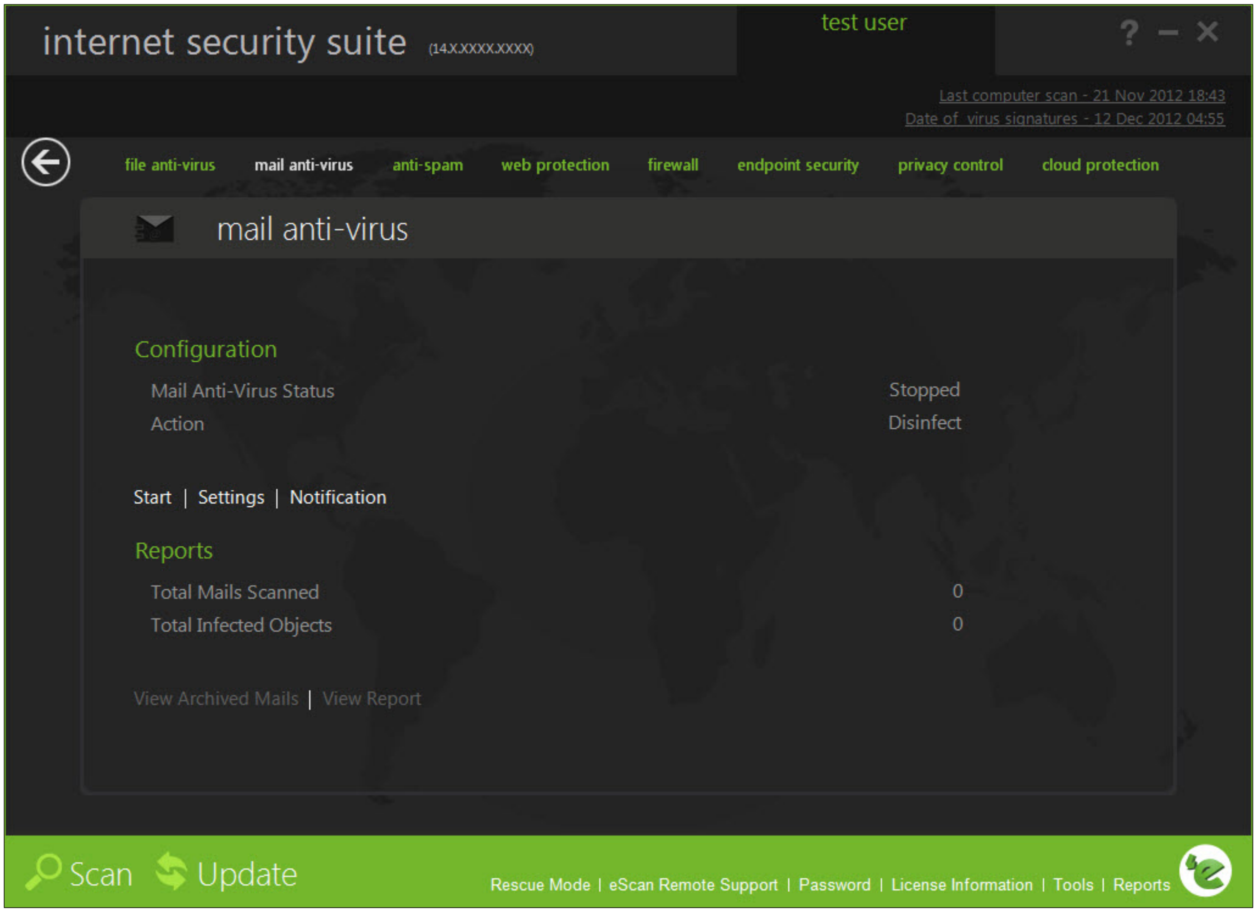
Date/Time	Name	Description	Action
12/13/2012 15:25:21	C:\Documents and Settings\Test User\Local Settings\Temp\eic...	Infected by Virus: EIC...	File Qu...
12/13/2012 15:25:21	C:\Documents and Settings\Test User\Local Settings\Temp\eic...	Infected by Virus: EIC...	File Qu...
12/13/2012 15:25:22	C:\Documents 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 34

- **Add to White List**: This option is present on Right Click of any populated row in the Report Table, use this option to Add any exe to the White List, it will always be considered as a trusted exe file.
- **Add to Block List**: This option is present on Right Click of any populated row, use this option to Add any exe to the block list, it will always be considered as a suspicious file and will be prevented from executing on the system.

Mail Anti-Virus

Mail Anti-Virus is the second module of the eScan for ISS. This module scans all incoming and outgoing e-mails for viruses, spyware, adware, and other malicious objects. 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. Refer Figure 35.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
mail anti-virus
Start | Settings | Notification
View Archived Mails | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

Mail Anti-Virus Status	Stopped
Action	Disinfect

Reports

Total Mails Scanned	0
Total Infected Objects	0

Figure 35

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:

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

Default: Click this button to apply the default settings.

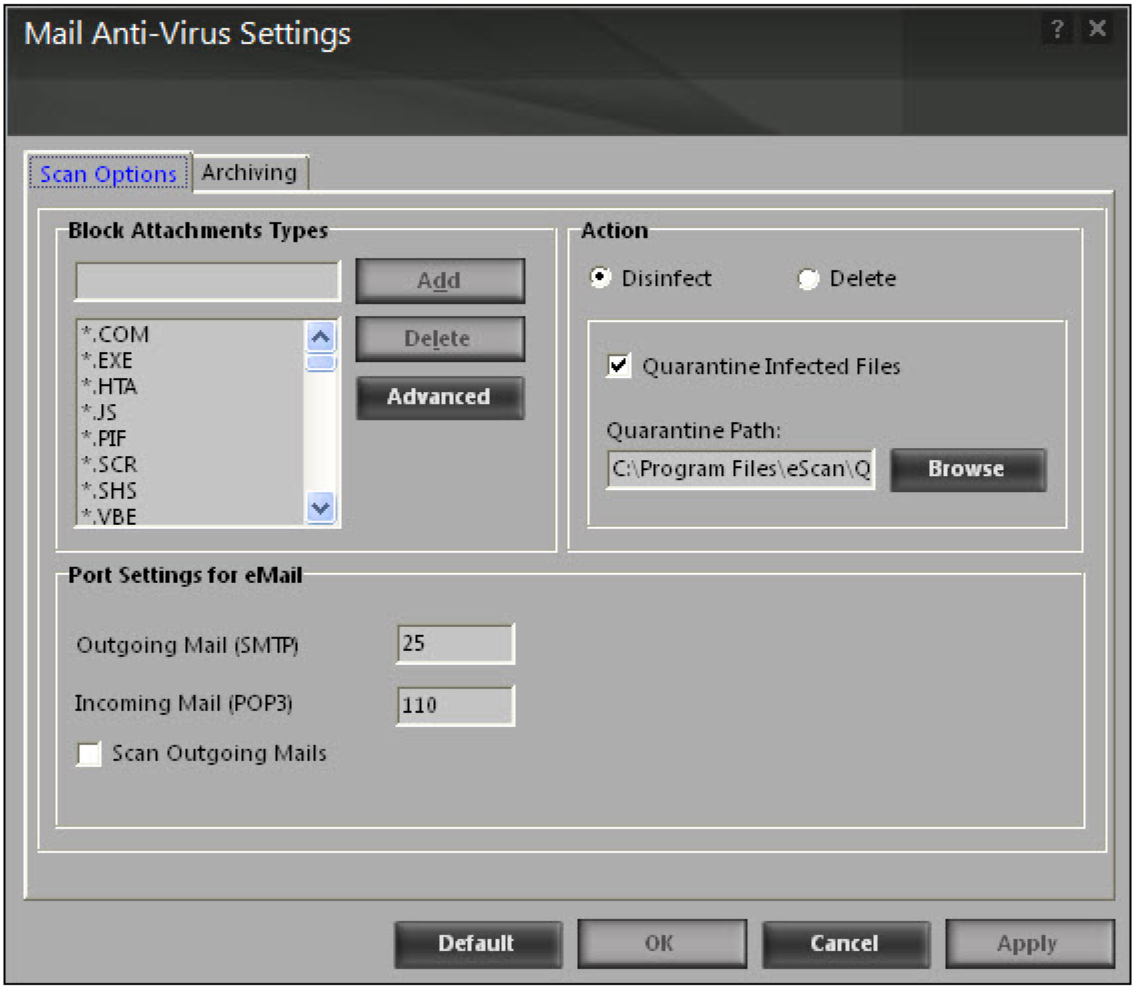
OK: Click this button after you click the **Apply** button to apply the configured settings.

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

Apply: Click this button to apply the configured settings.

- ### 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. Refer Figure 36.



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 36

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 host level. You can add file extensions to this list as per your requirement. As a best practice, you should avoid deleting the file extensions that are present in the Block Attachments Types list by default. You can also configure advanced settings required to scan 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:

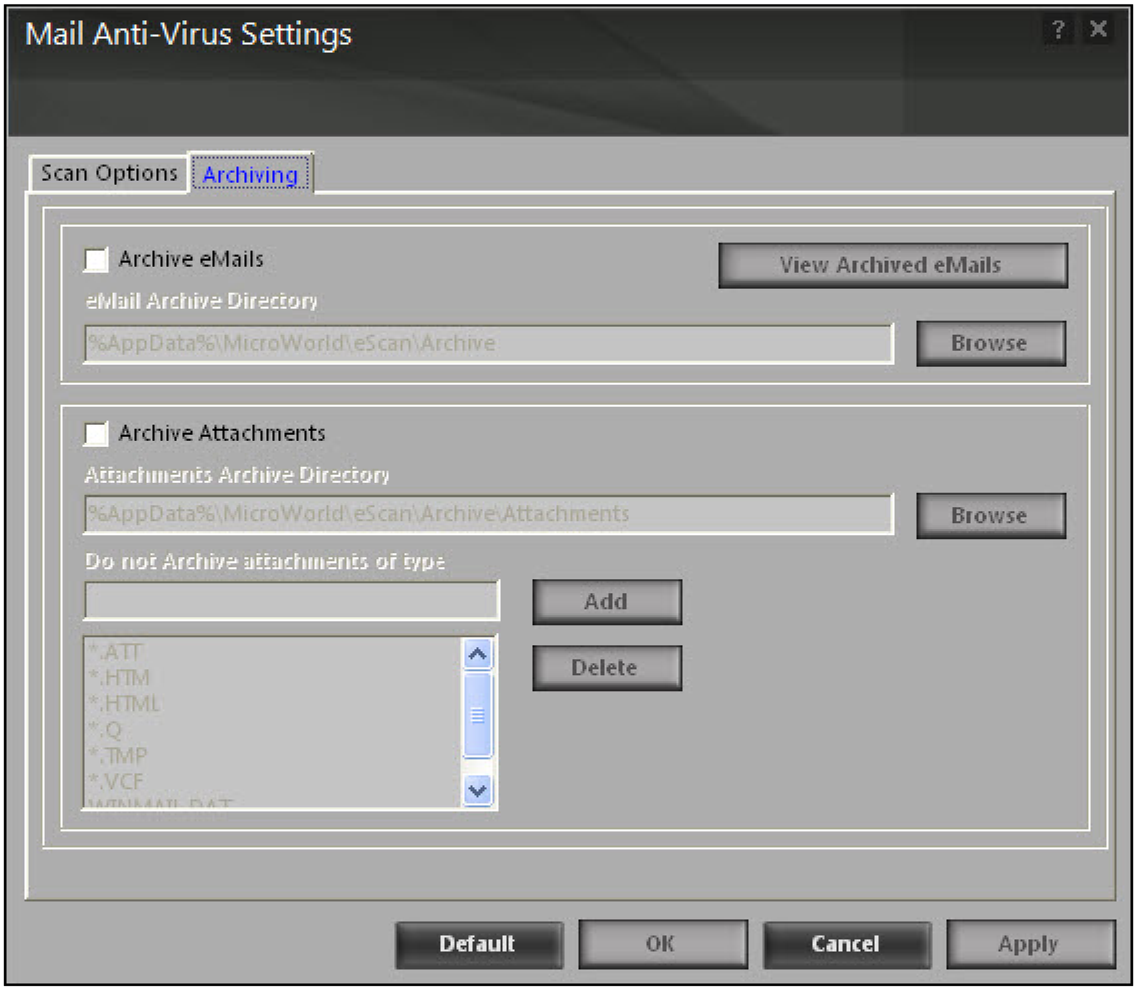
- **Delete all Attachment in eMail if disinfection is not possible:** Select this check box if you want to delete all the e-mail attachments that cannot be cleaned.
- **Delete entire eMail if disinfection is not possible:** [Default] Select this check box if you want to delete the entire e-mail if any 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. Refer Figure 37.



Mail Anti-Virus Settings

Scan Options | Archiving

□ 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 37

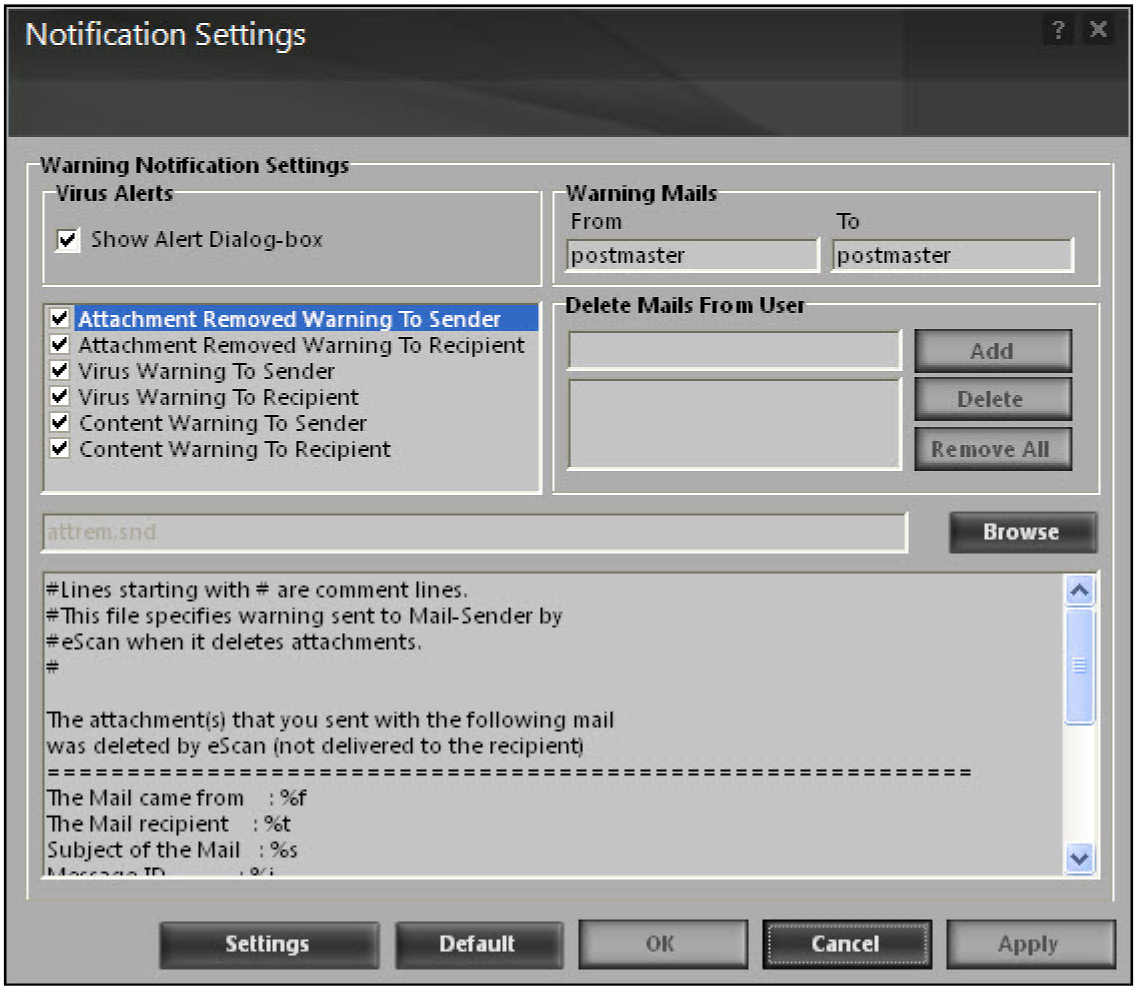
The following configuration options are available on this screen:

- 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 exclude certain file types, such as *.VCF, *.HTM, and *.HTML, from being archived by adding them to the Do not Archive attachments of type list.

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. Refer Figure 38.



☑ Show Alert Dialog-box

From: postmaster
To: postmaster

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

attrem.snd

```
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#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 38

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:** [Default] 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: Refer Figure 35.

- 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. Refer Figure 39.

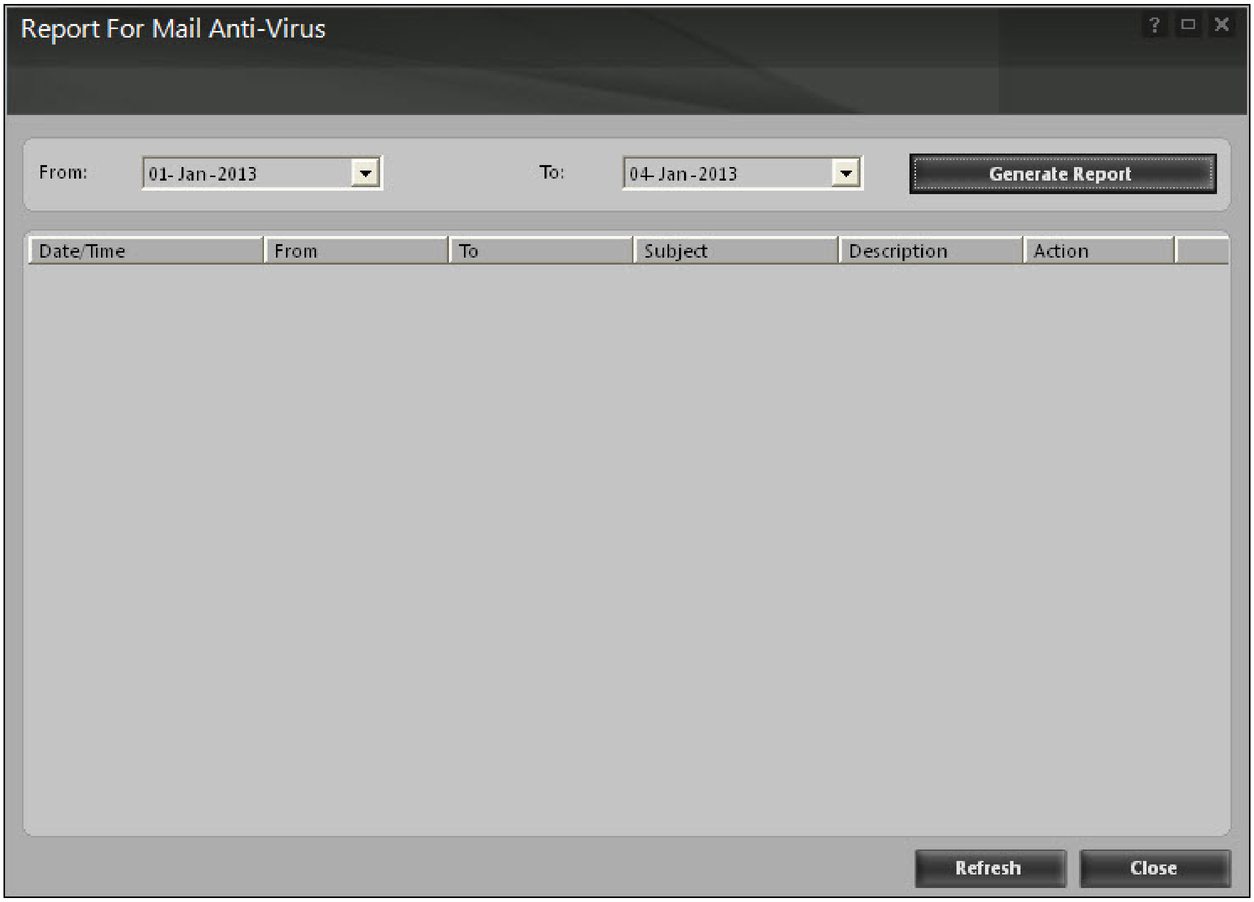
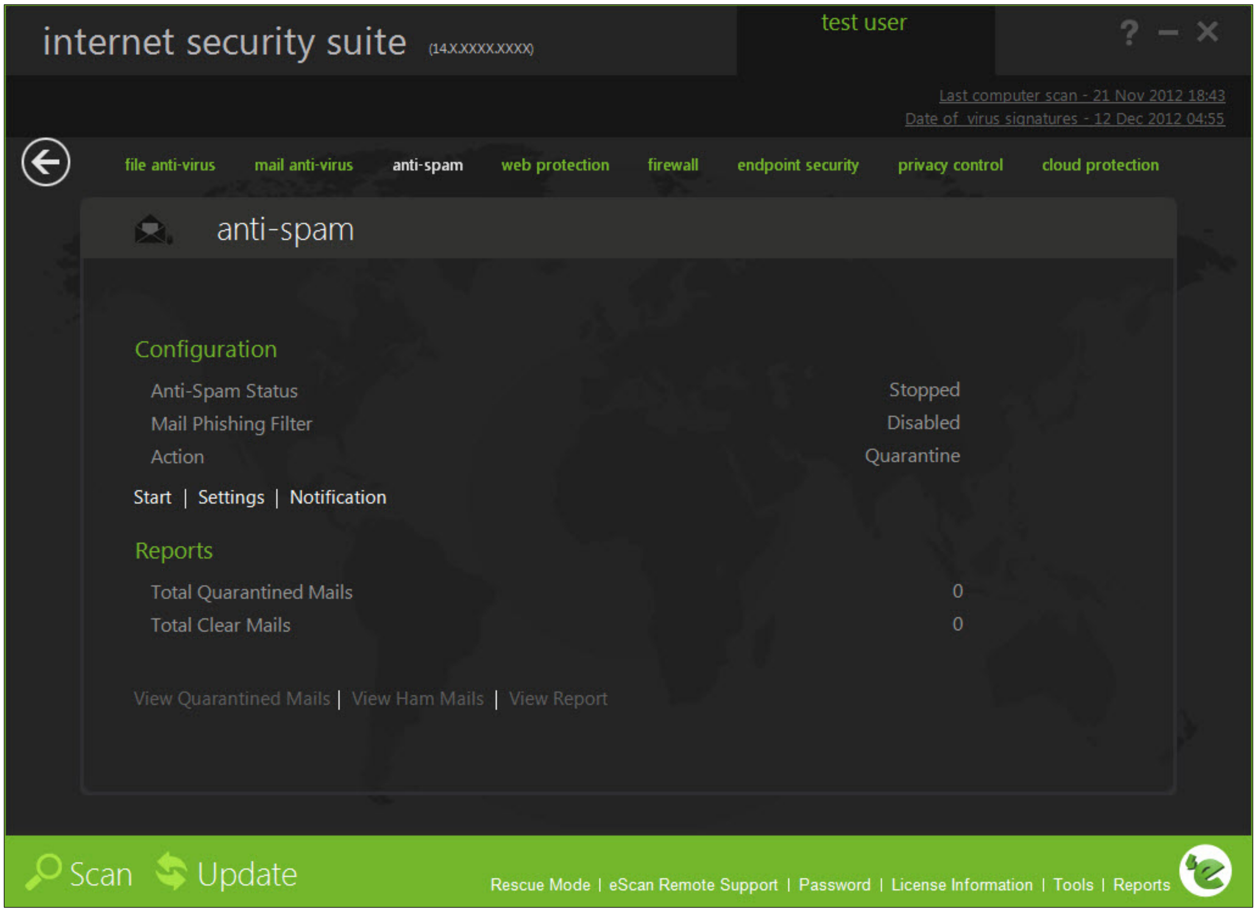


Figure 39

Anti-Spam

Anti-Spam is the third module of the eScan for ISS. This module filters all your junk and spam e-mails by using the NILP technology and sends content warnings to specified recipients. Refer Figure 40.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
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 40

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 this 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:

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

Default: Click this button to apply the default settings.

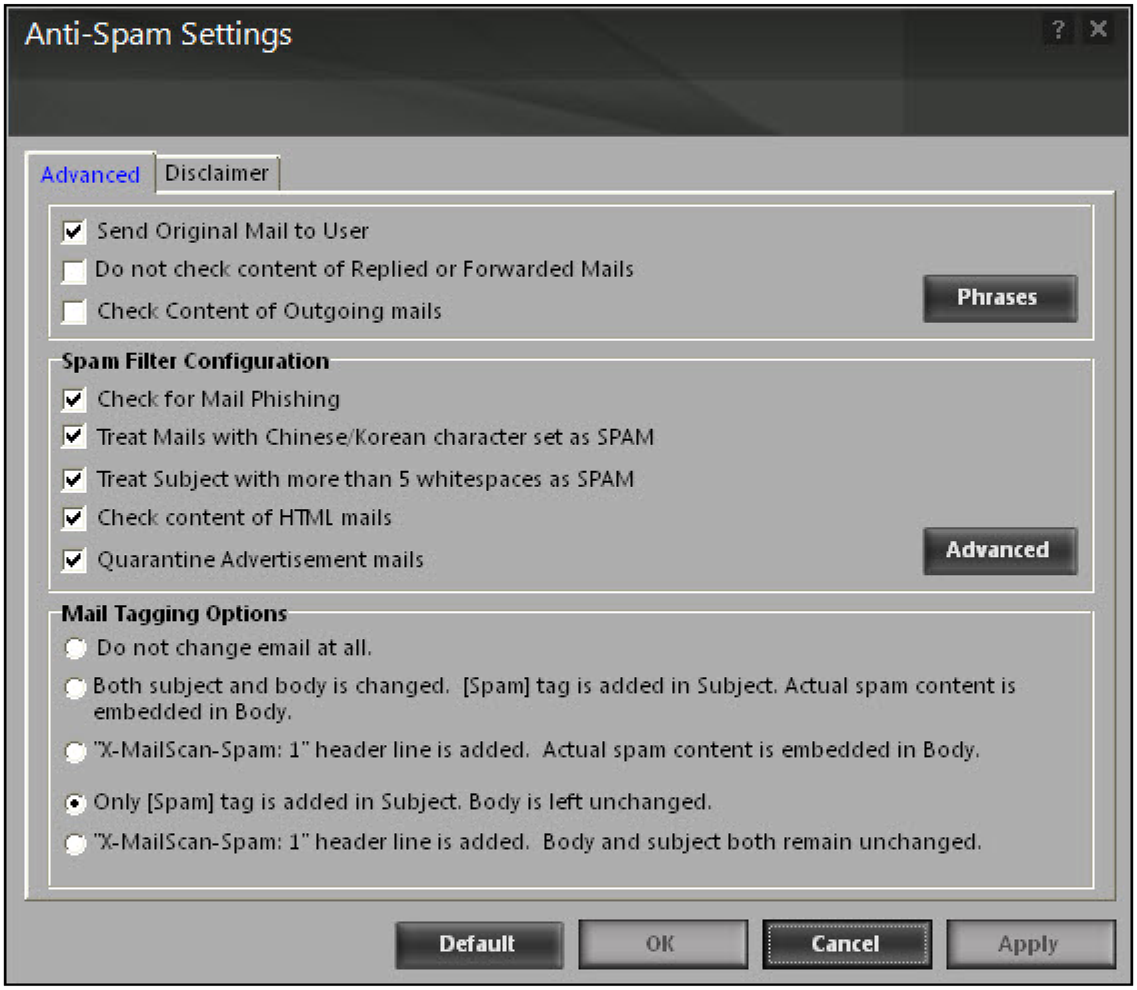
OK: Click this button after you click the **Apply** button to apply the configured settings.

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

Apply: Click this button to apply the configured settings.

Advanced

This section provides you with options for configuring the general e-mail options, spam filter configuration, and tagging e-mails in Anti-Spam. Refer Figure 41.



☑ 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 41

- Send Original Mail to User: [Default] This check box is selected by default. eScan creates Spam folder within the e-mail client depending upon the email client configured. 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 you can either allow or block. This list is called the **whitelist**. Similarly, you can specify certain words or phrases, so that mails containing those words or phrases in the subject, header, or body part of an email are recognized as spam and are quarantined or deleted, as defined by you. 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 select the starting row of Whitelisted words or phrases. A phrase that is added to the whitelist cannot be edited, enabled, or disabled.
- **User specified List of Blocked words/phrases:** (Color Code: **RED**) Click this option to select the starting row of the words or phrases that are defined in block list.
- **User specified words/phrases disabled:** (Color Code: **GRAY**) Click this option to select the starting row of words or phrases that are defined to be excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

- 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 URL 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:

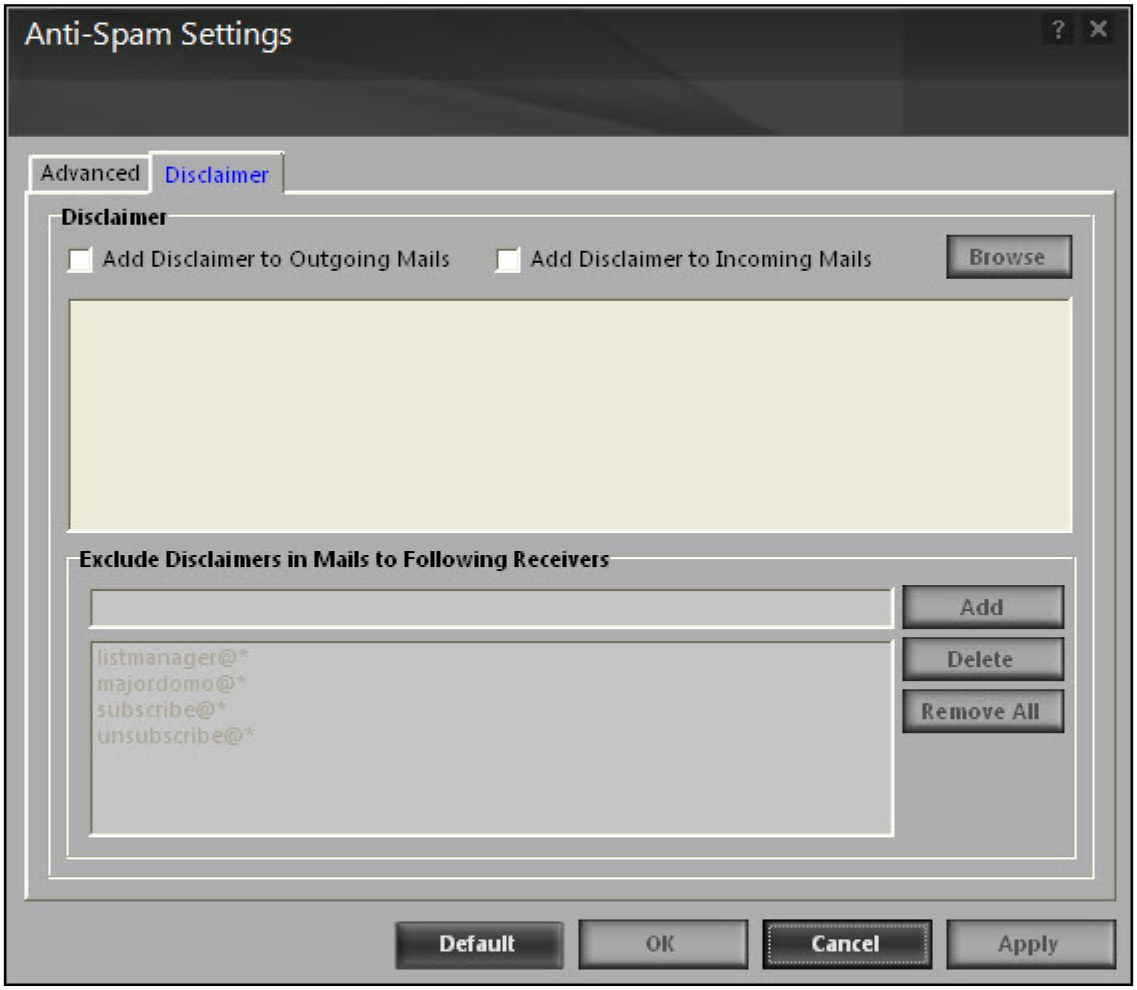
  - ▪ **Do not change email at all:** Click this option if you want to prevent Anti-Spam from adding the [Spam] tag to e-mails that have been identified as spam.

  - ▪ **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 part 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 part 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. Refer Figure 42.


Anti-Spam Settings

Disclaimer

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

Exclude Disclaimers in Mails to Following Receivers

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

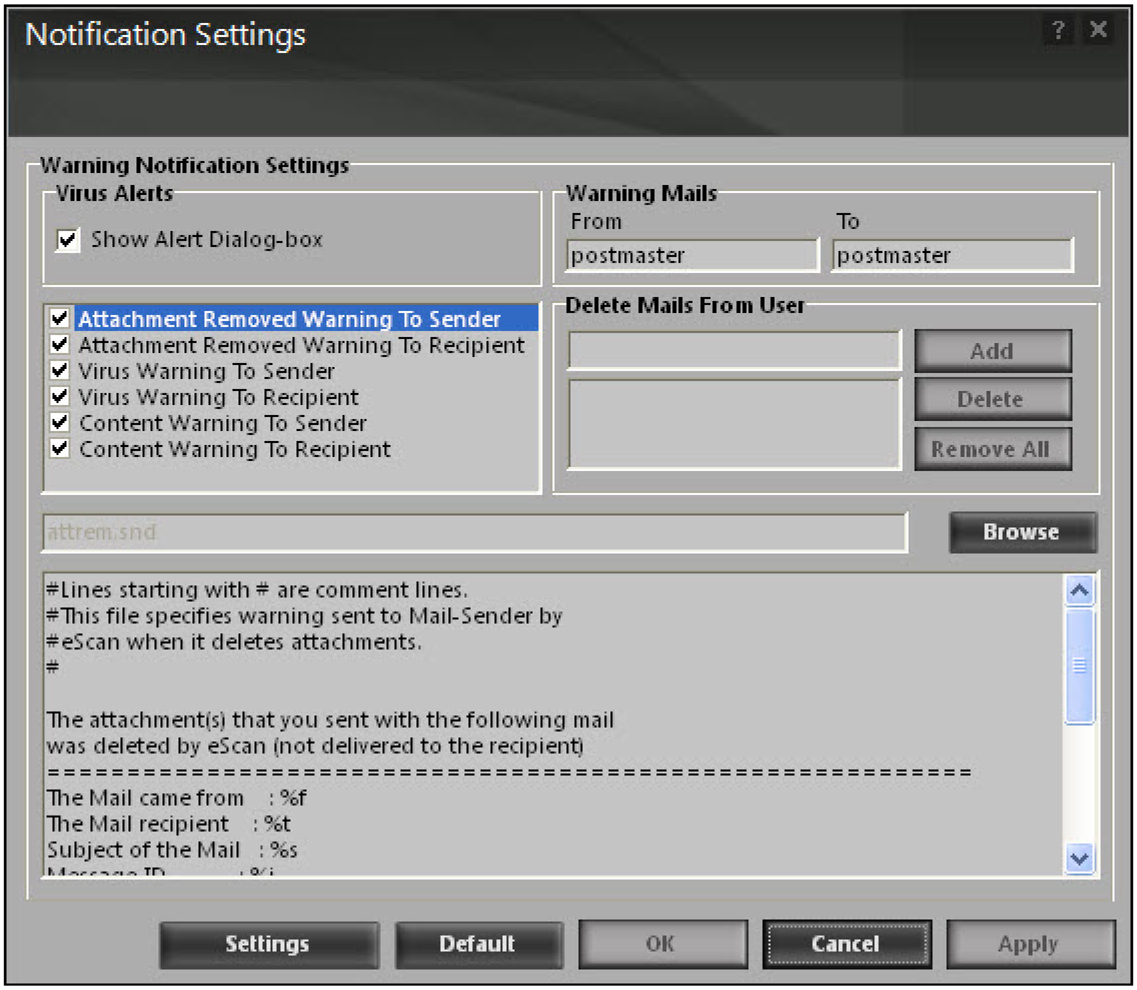
Figure 42

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 dim; 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. Refer Figure 43.



☑ Show Alert Dialog-box

From: postmaster
To: postmaster

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

attrem.snd

```
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#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 43

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:** [Default] 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

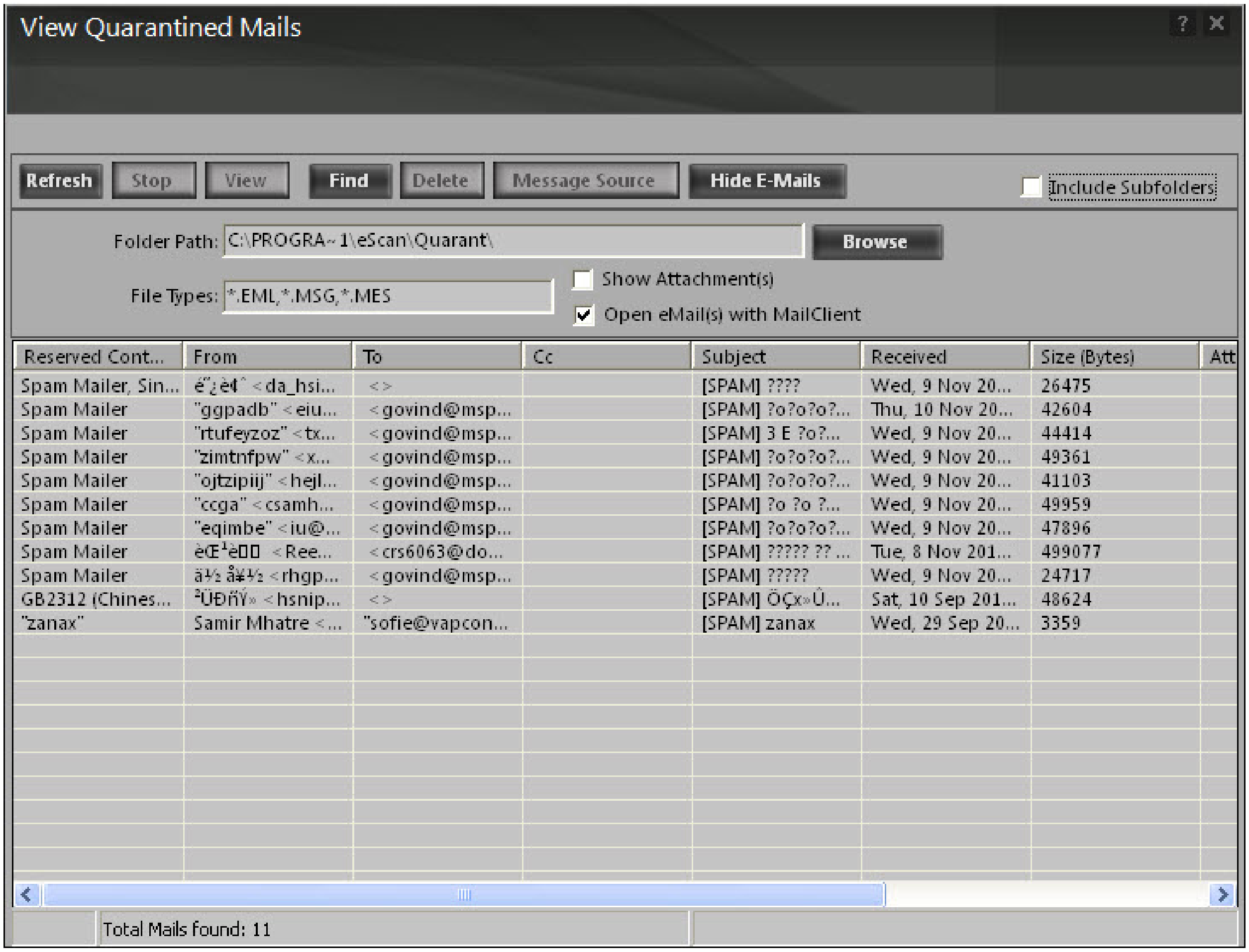
This section displays the following information: Refer Figure 40.

- 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. Refer Figure 44.



□ Include Subfolders

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

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

□ Show Attachment(s)

☑ Open eMail(s) with MailClient

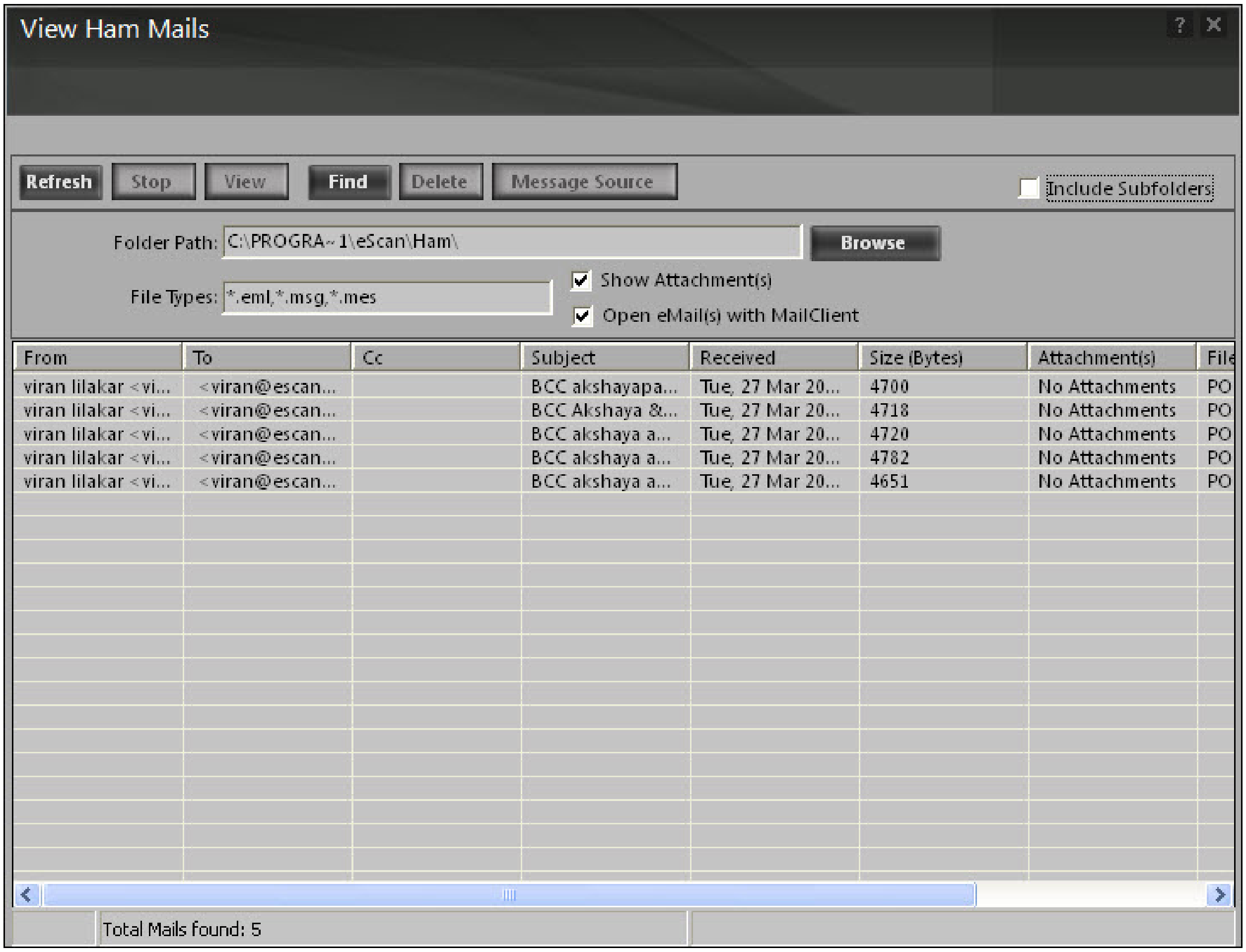
Reserved Cont...	From	To	Cc	Subject	Received	Size (Bytes)	Att
Spam Mailer, Sin...	é˝¿è¢ˆ <da_hsi...	<>		[SPAM] ????	Wed, 9 Nov 20...	26475	
Spam Mailer	"ggpadb" <eiu...	<govind@msp...		[SPAM] ?o?o?o?...	Thu, 10 Nov 20...	42604	
Spam Mailer	"rtufeyzoz" <tx...	<govind@msp...		[SPAM] 3 E ?o?...	Wed, 9 Nov 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 44

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 Refer Figure 45.



□ Include Subfolders

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

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

☑ Show Attachment(s)

☑ Open eMail(s) with MailClient

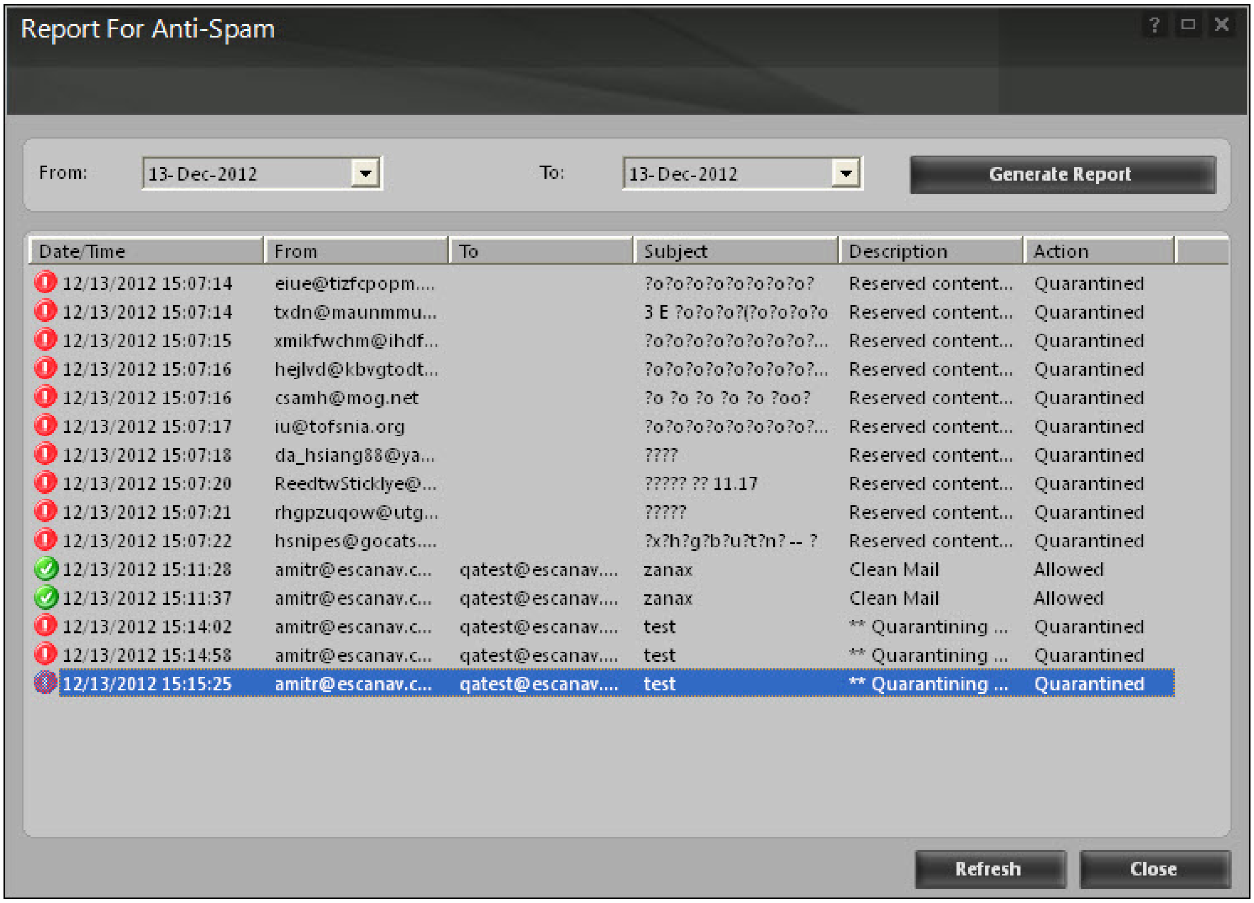
From	To	Cc	Subject	Received	Size (Bytes)	Attachment(s)	File
viran lilakar <vi...	<viran@escan...		BCC akshayapa...	Tue, 27 Mar 20...	4700	No Attachments	PO
viran lilakar <vi...	<viran@escan...		BCC Akshaya &...	Tue, 27 Mar 20...	4718	No Attachments	PO
viran lilakar <vi...	<viran@escan...		BCC akshaya 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 45

View Report:

This section displays the **Report for the Anti-Spam** window. This window displays report for the Anti-Spam module between the desired range of dates in a tabular format when you click the **Generate Report** button. Refer Figure 46.



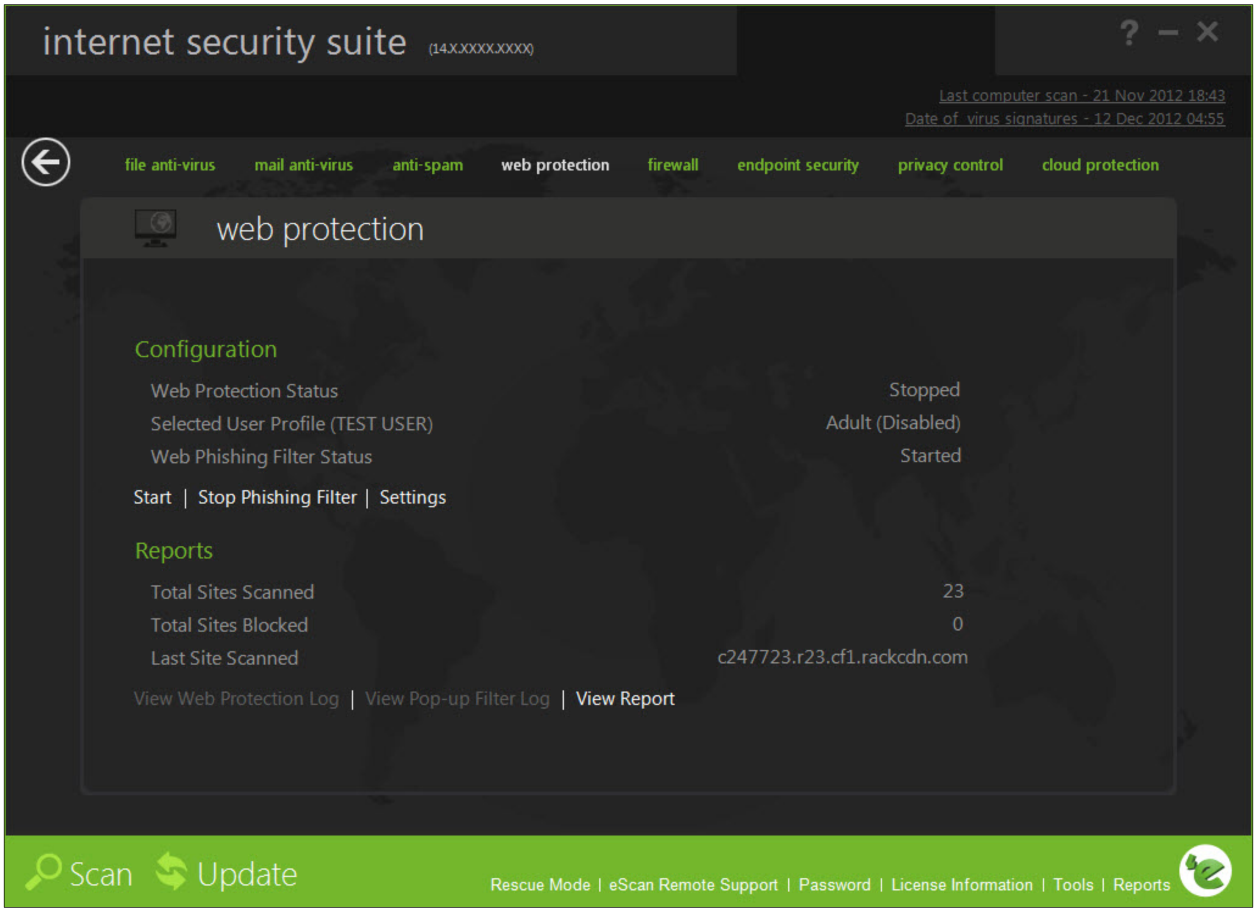
From: 13-Dec-2012 To: 13-Dec-2012

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?o?...	Reserved content...	Quarantined
12/13/2012 15:07:16	hejlvd@kbvgtodt...		?o?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?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 46

Web Protection

Web Protection is the fourth module of the eScan for ISS. This module uses highly advanced algorithms to block access of websites, based on the occurrence of specific words or phrases in the site and to block Web sites containing pornographic or offensive material. This feature is extremely beneficial to parents because it prevents kids from accessing Web sites containing vulgar or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related web sites during work hours. Refer Figure 47.


internet security suite (14.X.XXXX.XXXX)
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
web protection

Configuration

Web Protection Status	Stopped
Selected User Profile (TEST USER)	Adult (Disabled)
Web Phishing Filter Status	Started

Start | Stop Phishing Filter | Settings

Reports

Total Sites Scanned	23
Total Sites Blocked	0
Last Site Scanned	c247723.r23.cf1.rackcdn.com

View Web Protection Log | View Pop-up Filter Log | View Report

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

Figure 47

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:

- Web Protection Status: It displays the status of whether Web Protection module is started or stopped.
- Selected User Profile: It displays the selected user profile with its status.
- Web Phishing Filter Status: It displays the status of Web phishing filter.

Start/Stop:

Click on this option to enable or disable Web-Protection module.

> ✍ If you want to apply the web protection settings to the selected user profile, You have to make sure that web protection status is enabled on both the windows – on the eScan main window, under **Configuration** section, **Start/Stop** option and on the **Web Protection Settings** window, **enable/Disable** button on upper-left corner of the window.

Start/Stop Phishing Filter:

Click this option to start or stop the phishing filter.

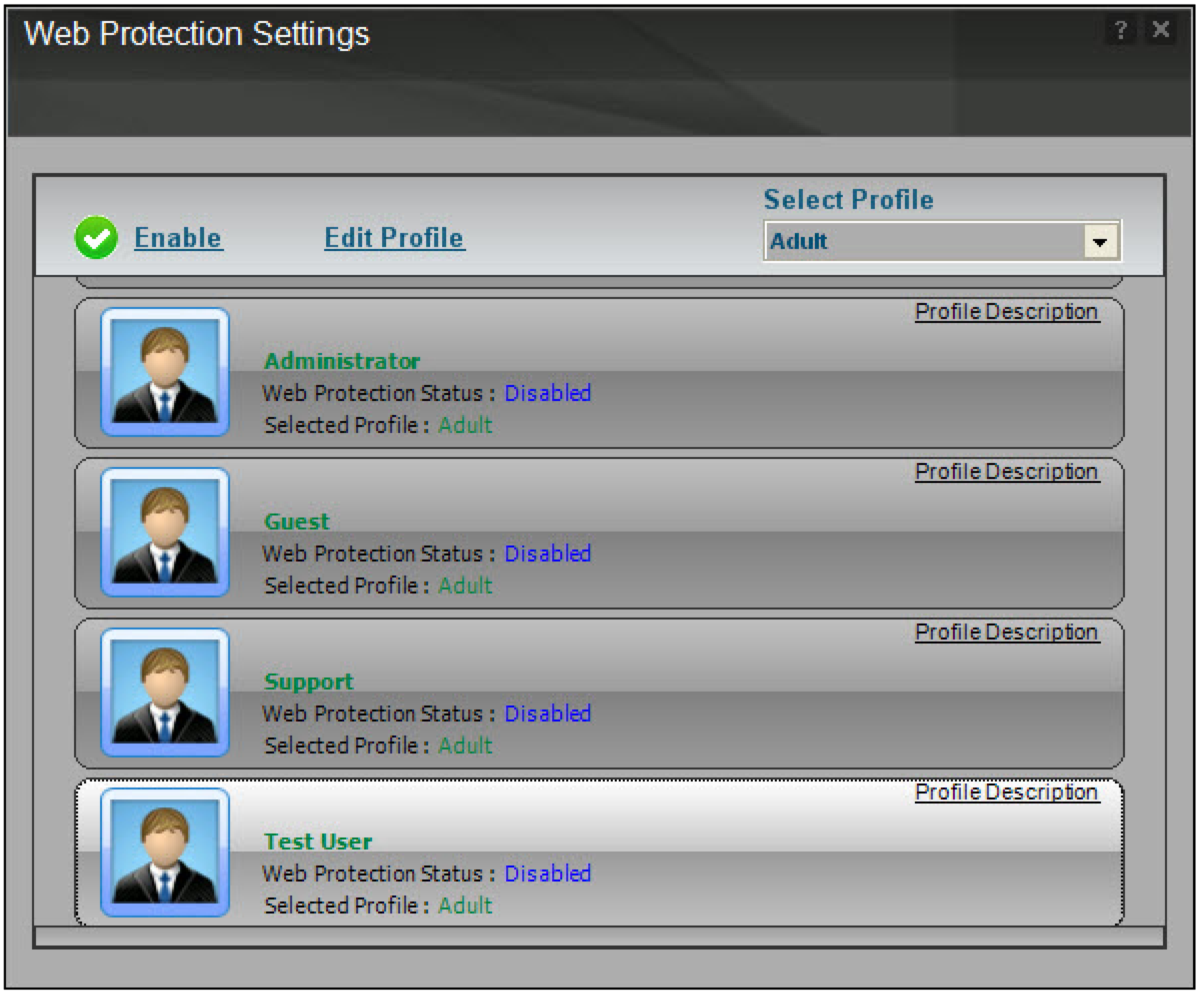
Settings:

When you click this button, the **Web Protection Settings** window appears. On the **Web Protection Settings** window, you have four different profiles – Walled Garden, Teenager, Adolescent, and Adult. You can change the web protection status of the selected user profile and you can edit the settings of the selected profile.

> ✍ At the bottom of the screen of all the tabs — Default, OK, Cancel, and Apply buttons are present that you can use after configuring the settings based on your requirement.
>
> **Default:** Click this button to apply the default settings.
>
> **OK:** Click this button after you click the **Apply** button to apply the configured settings.
>
> **Cancel:** Click this button to cancel the configured settings or to close the window.
>
> **Apply:** Click this button to apply the configured settings.

Perform the following steps to edit the settings of a profile:

1. Click the **Settings** button.
   The **Web Protection Settings** window appears. Refer Figure 48.



Select Profile: Adult

Administrator
Web Protection Status : Disabled
Selected Profile : Adult

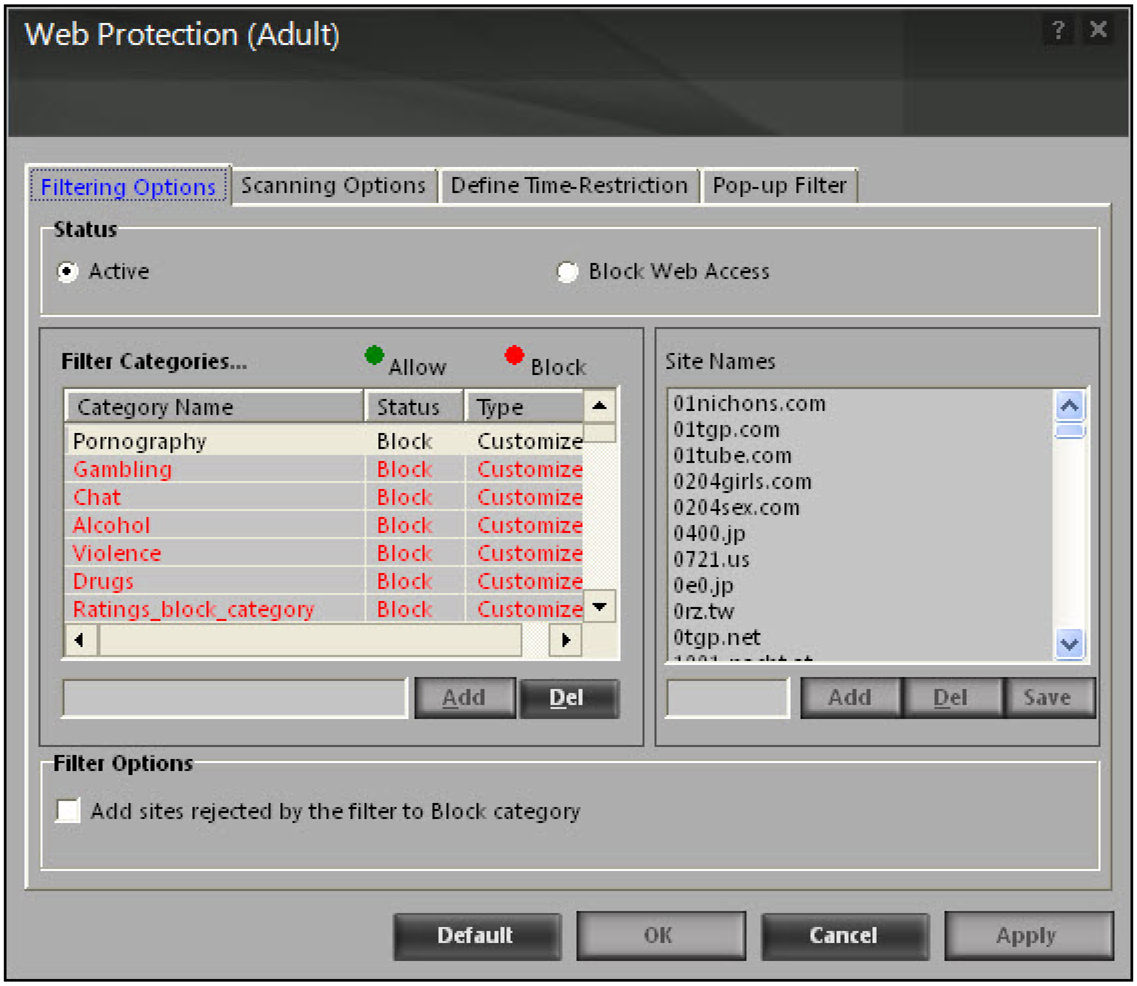
Guest
Web Protection Status : Disabled
Selected Profile : Adult

Support
Web Protection Status : Disabled
Selected Profile : Adult

Test User
Web Protection Status : Disabled
Selected Profile : Adult

Figure 48

8. Select an appropriate profile for which you want to change the settings from the **Select Profile** drop-down list, and if you want to change the web protection status of a profile, click **Enable/Disable** button on upper-left corner of the window, and then click the **Edit Profile** button.
   The **Web Protection (Adult)** window appears. Refer Figure 49.



Status

● Active ○ Block Web Access

Filter Categories... ● Allow ● Block

Category Name	Status	Type
Pornography	Block	Customize
Gambling	Block	Customize
Chat	Block	Customize
Alcohol	Block	Customize
Violence	Block	Customize
Drugs	Block	Customize
Ratings_block_category	Block	Customize

Site Names

01nichons.com
01tgp.com
01tube.com
0204girls.com
0204sex.com
0400.jp
0721.us
0e0.jp
0rz.tw
0tgp.net

Filter Options

□ Add sites rejected by the filter to Block category

Figure 49

9. Click the **Filtering Options** tab.
   The **Web Protection (Adult)** window appears. Refer Figure 49.

Filtering Options

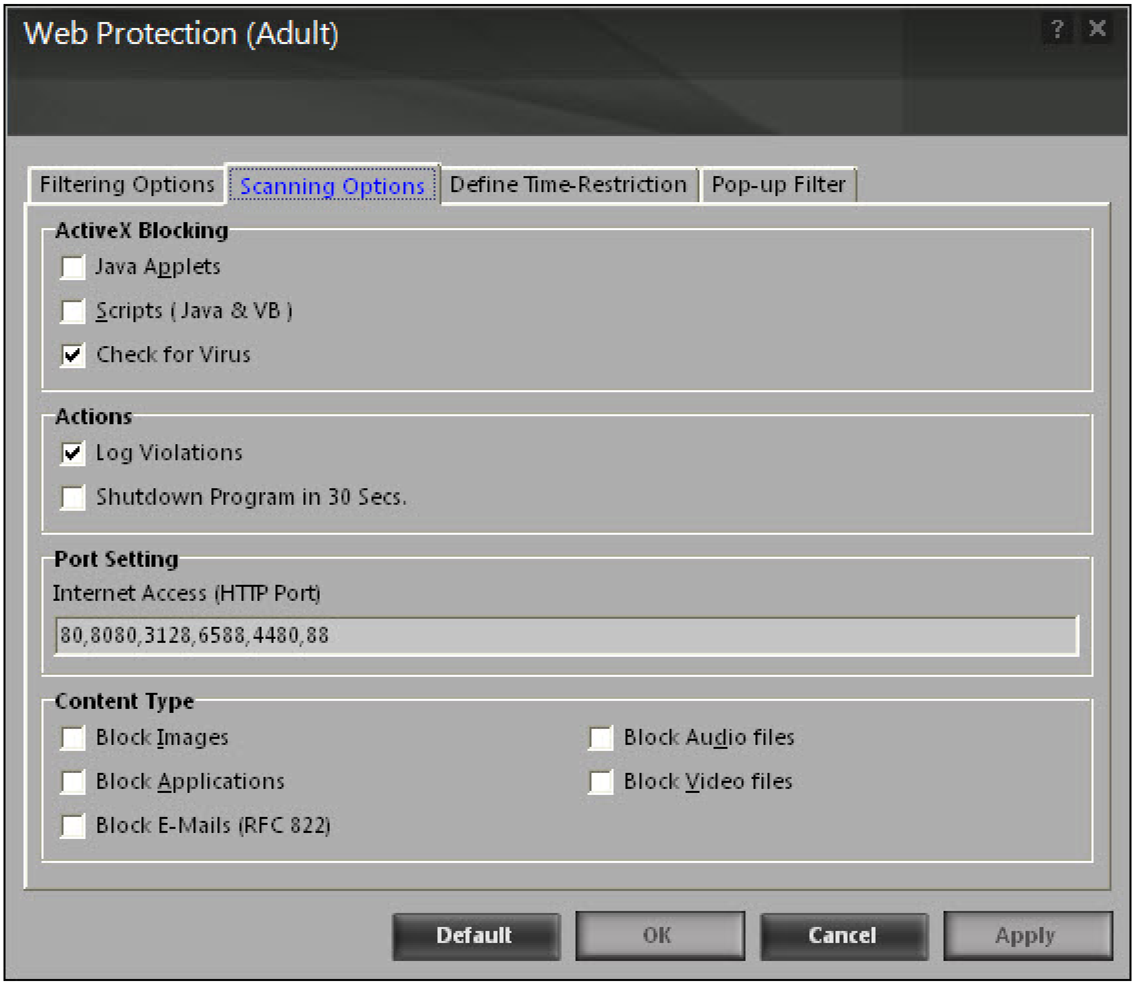
This section provides you with options for filtering the websites based on various categories. You can either allow or block websites depending on certain words/phrases that are found in the web sites.

- Status: This section helps you to allow or block access to specific Web site based on Filter Categories. You can set the status as Active or Block Web Access. Select the Block Web Access option, if you want to block all the web sites except the ones that have been listed in the Filter Categories. When you select this option, only Filtering Options and Pop-up Filter tabs are available.
  - **Filter Categories:** This section uses the following color codes for allowed and blocked Web sites.
    - **Green:** It represents an allowed Web site.
    - **Red:** It represents a blocked Web site.

    The filter categories used in this section include Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings_block_category, Websites_Allowed, and so on. You can also add or delete filter categories depending on your requirement.
  - **Category:** [Category name]: This section shows the **Words / Phrases** list, which lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the Web sites belonging to the selected category. You can also add or delete filter categories depending on your requirement.
  - **Filter Options:** This section includes the **Add sites rejected by the filter to Block category** check box. Select this check box if you want eScan to add Web sites that are denied access to the Block category database automatically.

Scanning Options

This tab helps to block images, ActiveX controls, media components, and applications from appearing within the browser. Refer Figure 50.



Web Protection (Adult)

ActiveX Blocking

□ Java Applets

□ Scripts (Java & VB)

☑ Check for Virus

Actions

☑ Log Violations

□ Shutdown Program in 30 Secs.

Port Setting

Internet Access (HTTP Port)

80,8080,3128,6588,4480,88

Content Type

□ Block Images

□ Block Applications

□ Block E-Mails (RFC 822)

□ Block Audio files

□ Block Video files

Figure 50

- ActiveX Blocking: An ActiveX control is a component program that can be automatically downloaded and executed by a Web browser. It is similar to a Java applet. ActiveX controls may include malicious code and therefore may pose as a security hazard.
  - **Java Applets:** Java Applets are programs that are written in the Java programming language. These applets can be embedded in an HTML page and can be viewed from a Java-enabled Web browser. Applets enhance the interactivity in Web pages and provide users with an enhanced Web experience. However, some applets contain malicious code that may either disrupt the processes running on your computer or steal sensitive information. Select this check box to block applets from being downloaded to your computer.

  - **Scripts (Java & VB):** Scripts are usually written in scripting languages such as JavaScript and VBScript. A script is a list of commands that can execute without user input. With the help of scripts, you can automate certain tasks within an application to work in a particular computing scenario. Hackers often use malicious script to steal information about the victims. When you select the **Scripts (Java & VB)** check box, eScan blocks scripts from being downloaded to your computer from the Internet.
  - **Check for Virus:** [Default] This check box is selected by default. Select this check box if you want eScan to scan and block all Web sites that contain malicious code.

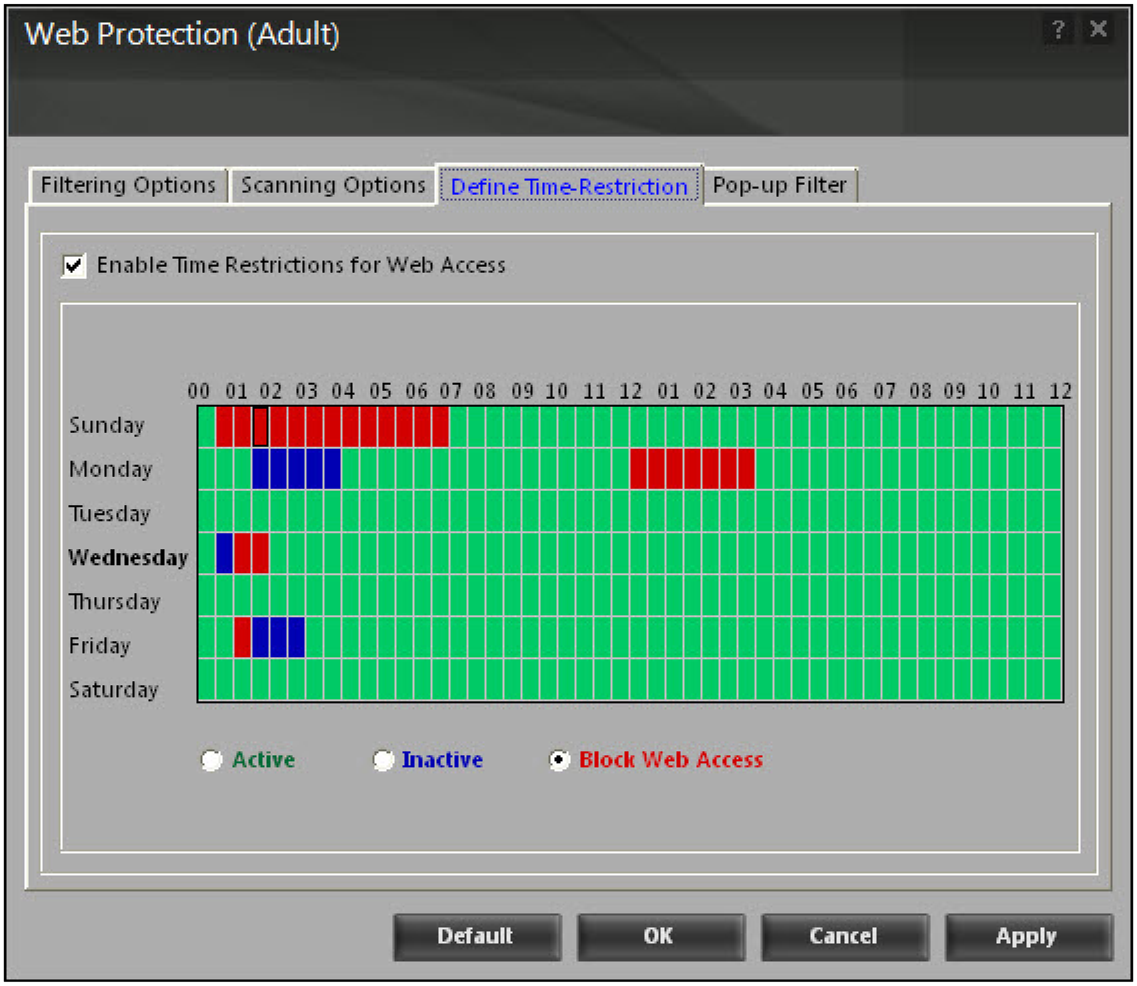
- **Actions:** This section helps you select the actions that eScan should perform when it detects a security violation.
  - **Log Violations:** [Default] This check box is selected by default. Select this check box if you want Web Protection to log all security violations for your future reference.
  - **Shutdown Program in 30 Secs:** Select this check box if you want Web Protection to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.

- **Port Setting:** This section helps you specify the port numbers that eScan should monitor for suspicious traffic.
  - **Internet Access (HTTP Port):** Web browsers commonly use the port numbers 80, 8080, 3128, 6588, 4480, and 88 for accessing the Internet. You can add port numbers to the **Internet Access (HTTP Port)** box to monitor the traffic on those ports.

- Content Type: This section helps you block content based on their type, such as images, applications, e-mails (RFC 822), audio files, and video files.

Define Time Restriction

This section helps you define policies to restrict access to the Internet. Refer Figure 51.



☑ Enable Time Restrictions for Web Access

00 01 02 03 04 05 06 07 08 09 10 11 12 01 02 03 04 05 06 07 08 09 10 11 12

Sunday	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Monday	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Tuesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Wednesday	🟩	🟦	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Thursday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Friday	🟩	🟩	🟥	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Saturday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

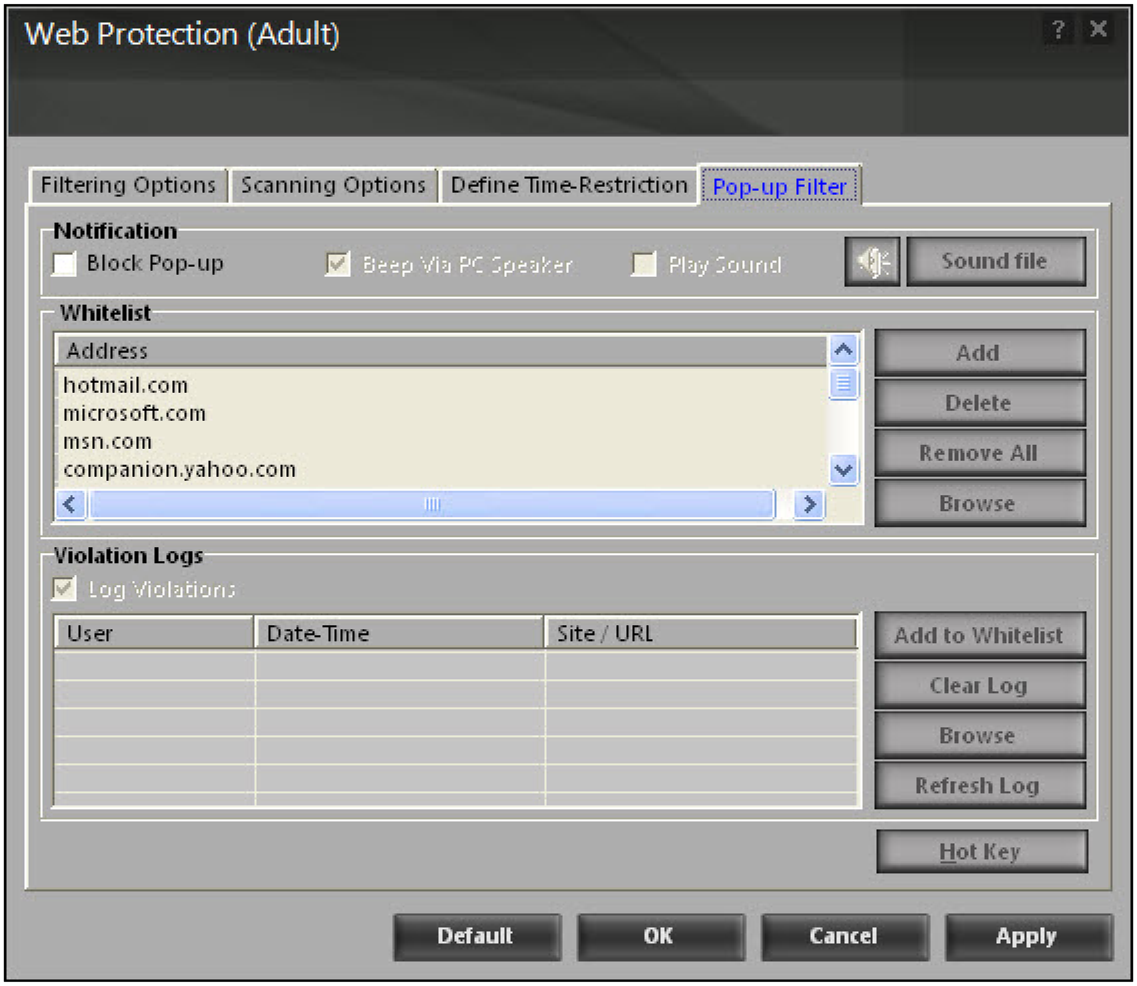
○ Active ○ Inactive ● Block Web Access

Figure 51

- Enable Time Restrictions for Web Access: Select this check box if you want to set restrictions on when a user can access the internet. By default, all the fields appear dimmed. The fields are available only when you select this check box.
  You also have an option to select and schedule the days in a week, and time on which you want to allow or restrict the web access.
  - **Active:** Click this option if you want to keep web protection active on certain days at specific time.
  - **Inactive:** Click this option if you want to keep web access inactive on certain days at specific time.
  - **Block Web Access:** Click this option if you want to block web access on certain days at specific time.

Pop-up Filter

This section includes options for customizing notification alerts, whitelist, and violation logs for pop-ups. Refer Figure 52.



Notification

☐ Block Pop-up ☑ Beep Via PC Speaker ☐ Play Sound

Whitelist

Address
hotmail.com
microsoft.com
msn.com
companion.yahoo.com

Violation Logs

☑ Log Violations

User	Date-Time	Site / URL

Figure 52

- Notification: In this section, you can configure the settings for receiving notification alerts. Select the Block Pop – up check box to block popup windows to open while you are browsing, click on Beep Via PC Speaker to hear a beep from your speaker whenever a pop up is blocked, you can add your sound file that you wish to hear whenever a pop up is blocked using the play sound option.
- White List: This section helps you customize the list of Web sites whose pop-ups will not be blocked by the Pop-up Filter.
- Violation Logs: You can also log all violations by selecting Log Violations check box, add the web sites to the whitelist for which a pop-up was blocked by the pop-up filter, clear the log, browse the web sites listed in the log, and refresh the log. In addition, you can assign a key to allow pop-ups temporarily for the Web site being accessed.

- Reports

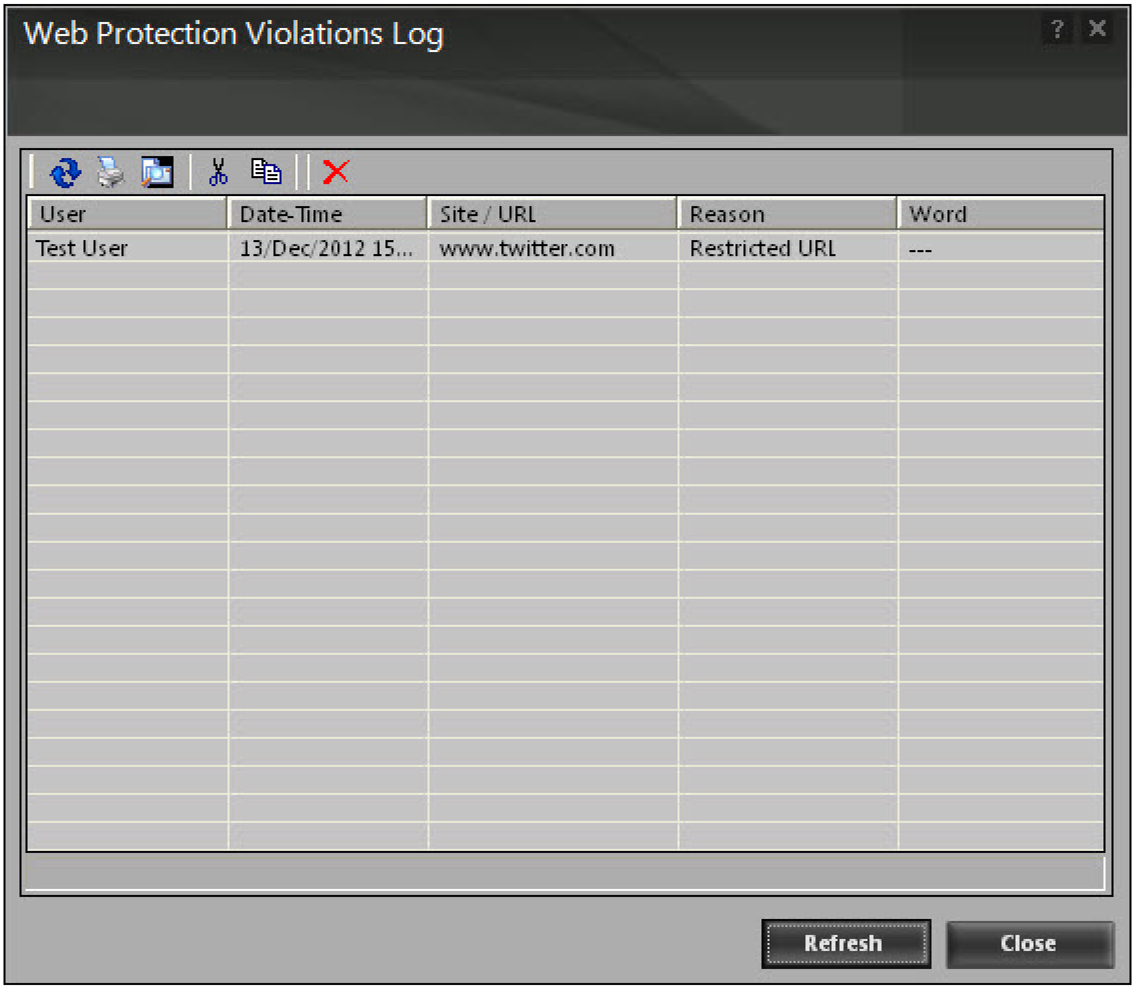
This section displays the following information. Refer Figure 47.

- Total Sites Scanned: It shows the total number of Web sites scanned by Web Protection.
- Total Sites Blocked: It shows the total number of Web sites blocked by Web Protection.
- Last Site Scanned: It shows the name of the last Web site scanned by Web Protection.

In addition, you can view the following reports.

View Web Protection Log:

This button opens the Web Protection Violations Log window, which displays information such as the user name, date and time when the violation occurred, the URL of the Web site, the reason for the violation, and the word or phrase that triggered the violation event. Refer Figure 53.

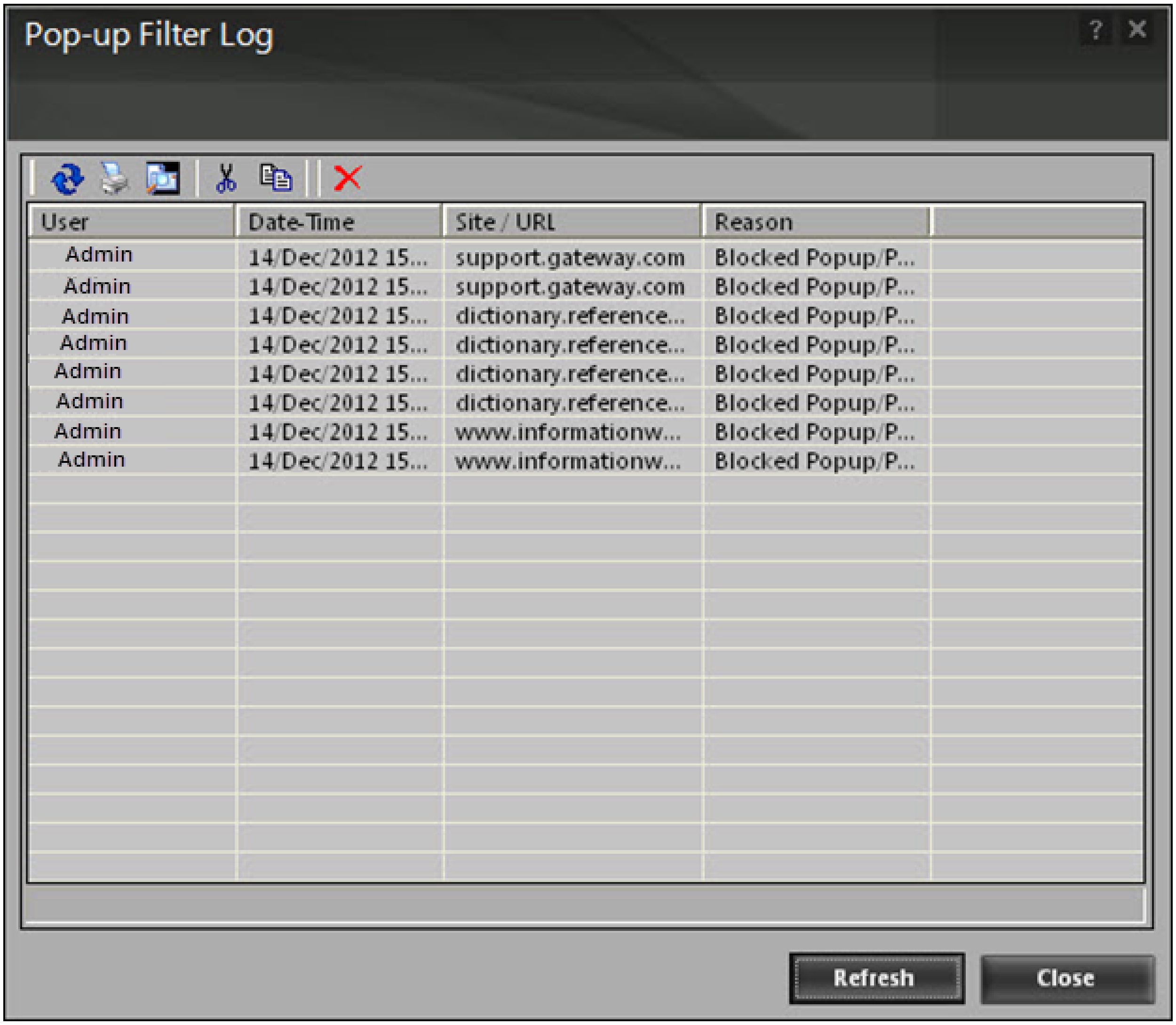


User	Date-Time	Site / URL	Reason	Word
Test User	13/Dec/2012 15...	www.twitter.com	Restricted URL	---

Figure 53

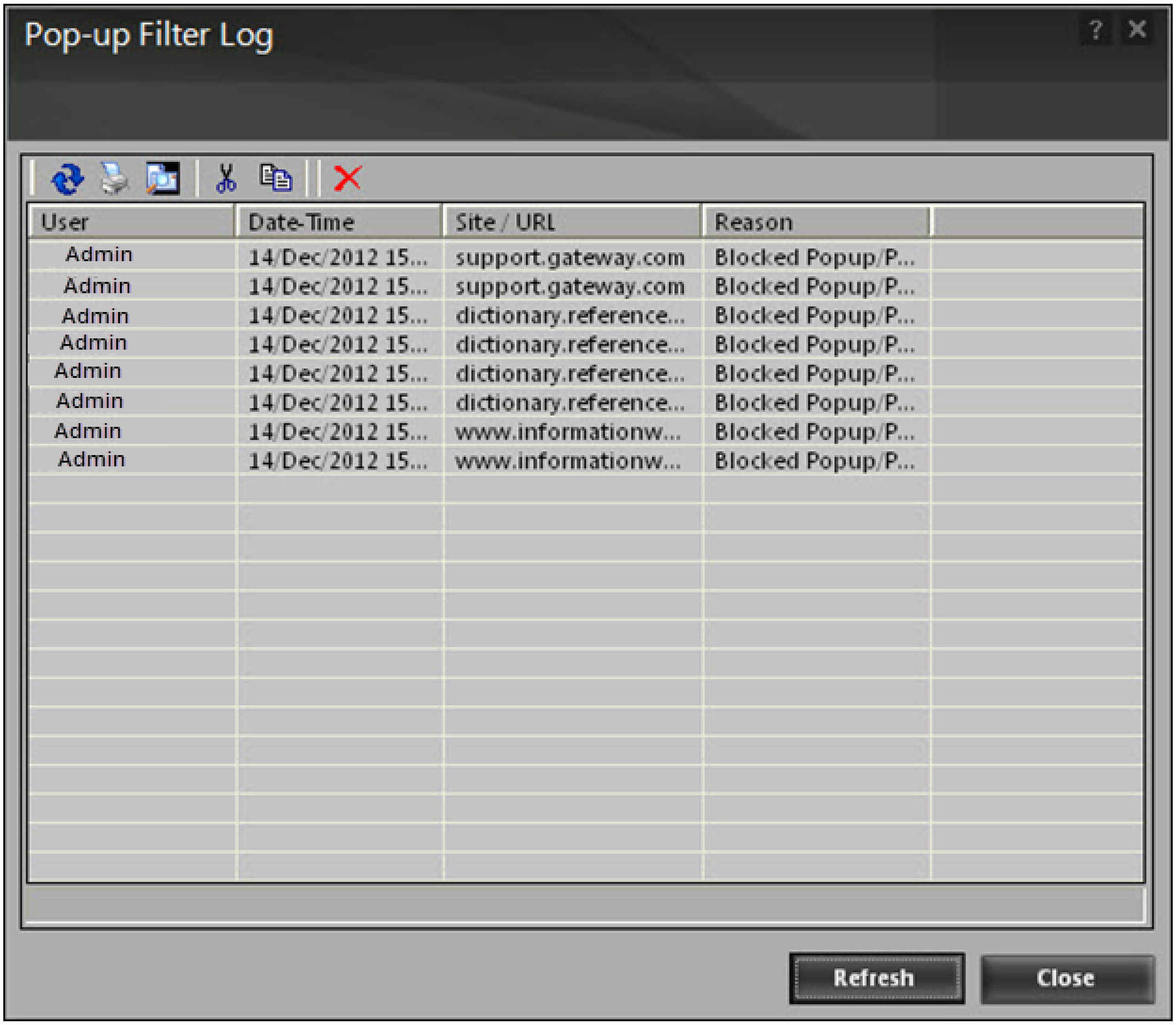
View Pop-up Filter Log:

This button opens the View Popup Filter Log window, which displays the details of the pop-up windows that were blocked while you were browsing websites. This window displays information such as the user name, date and time when the pop-up window was displayed, the URL of the Web site. Refer



User	Date-Time	Site / URL	Reason
Admin	14/Dec/2012 15...	support.gateway.com	Blocked Popup/P...
Admin	14/Dec/2012 15...	support.gateway.com	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	www.informationw...	Blocked Popup/P...
Admin	14/Dec/2012 15...	www.informationw...	Blocked Popup/P...

Figure 54.

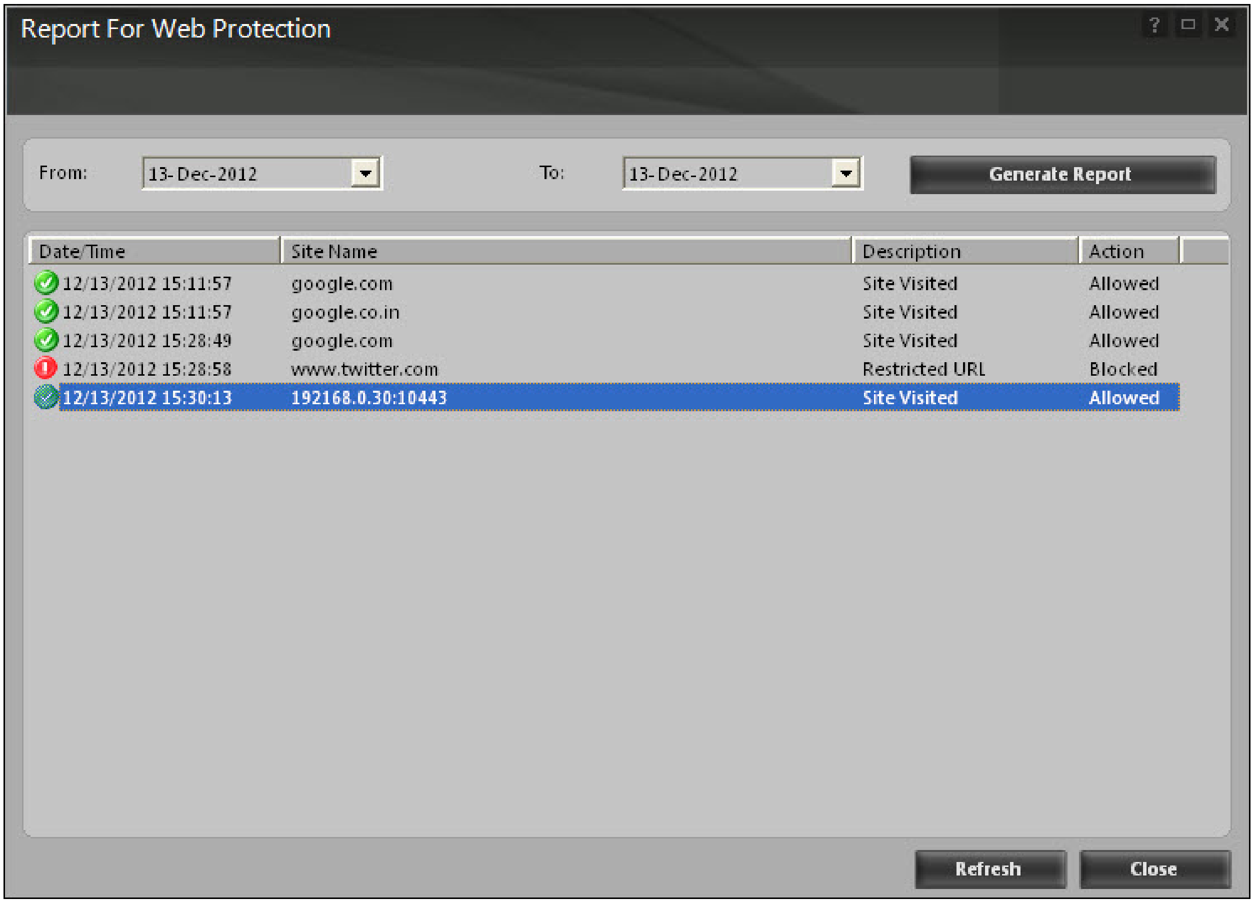


User	Date-Time	Site / URL	Reason
Admin	14/Dec/2012 15...	support.gateway.com	Blocked Popup/P...
Admin	14/Dec/2012 15...	support.gateway.com	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	dictionary.reference...	Blocked Popup/P...
Admin	14/Dec/2012 15...	www.informationw...	Blocked Popup/P...
Admin	14/Dec/2012 15...	www.informationw...	Blocked Popup/P...

Figure 54

View Report:

This button displays the **Report for Web Protection** window. This window displays the report for the Web Protection module for a given range of dates in a tabular format when you click the **Generate Report** button. Refer Figure 55.



Report For Web Protection

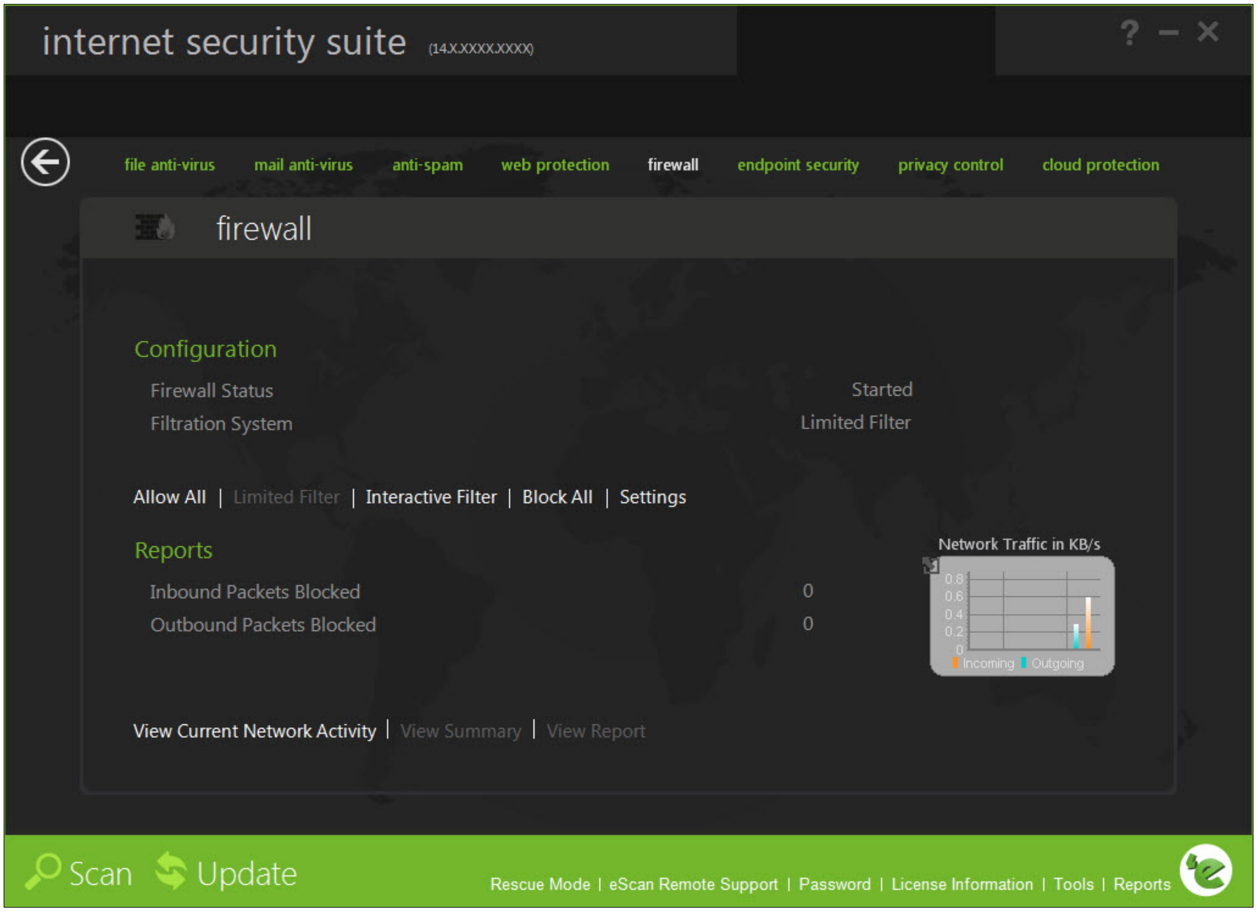
From: 13-Dec-2012 To: 13-Dec-2012

Date/Time	Site Name	Description	Action
✓ 12/13/2012 15:11:57	google.com	Site Visited	Allowed
✓ 12/13/2012 15:11:57	google.co.in	Site Visited	Allowed
✓ 12/13/2012 15:28:49	google.com	Site Visited	Allowed
! 12/13/2012 15:28:58	www.twitter.com	Restricted URL	Blocked
✓ 12/13/2012 15:30:13	192168.0.30:10443	Site Visited	Allowed

Figure 55

Firewall

Firewall is the fifth module of the eScan for ISS. 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. Refer Figure 56.


internet security suite (14.X.XXXX.XXXX)
? – ✕
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
firewall
Allow All | Limited Filter | Interactive Filter | Block All | Settings
Network Traffic in KB/s
0.8
0.6
0.4
0.2
0
Incoming
Outgoing
View Current Network Activity | View Summary | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

Firewall Status Started

Filtration System Limited Filter

Reports

Inbound Packets Blocked 0

Outbound Packets Blocked 0

Figure 56

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.

Available Modes:

- **Allow All -** It will filter all incoming as well as outgoing traffic.
- **Limited Filter** - It will filter all Incoming traffic.
- **Interactive Filter** – It will filter Incoming as well as outgoing traffic but will give you an alert message whenever user input is required. .
- **Block All** – It will block all network connections.

✍ By default, the firewall operates in the **Limited Filter** mode.

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.

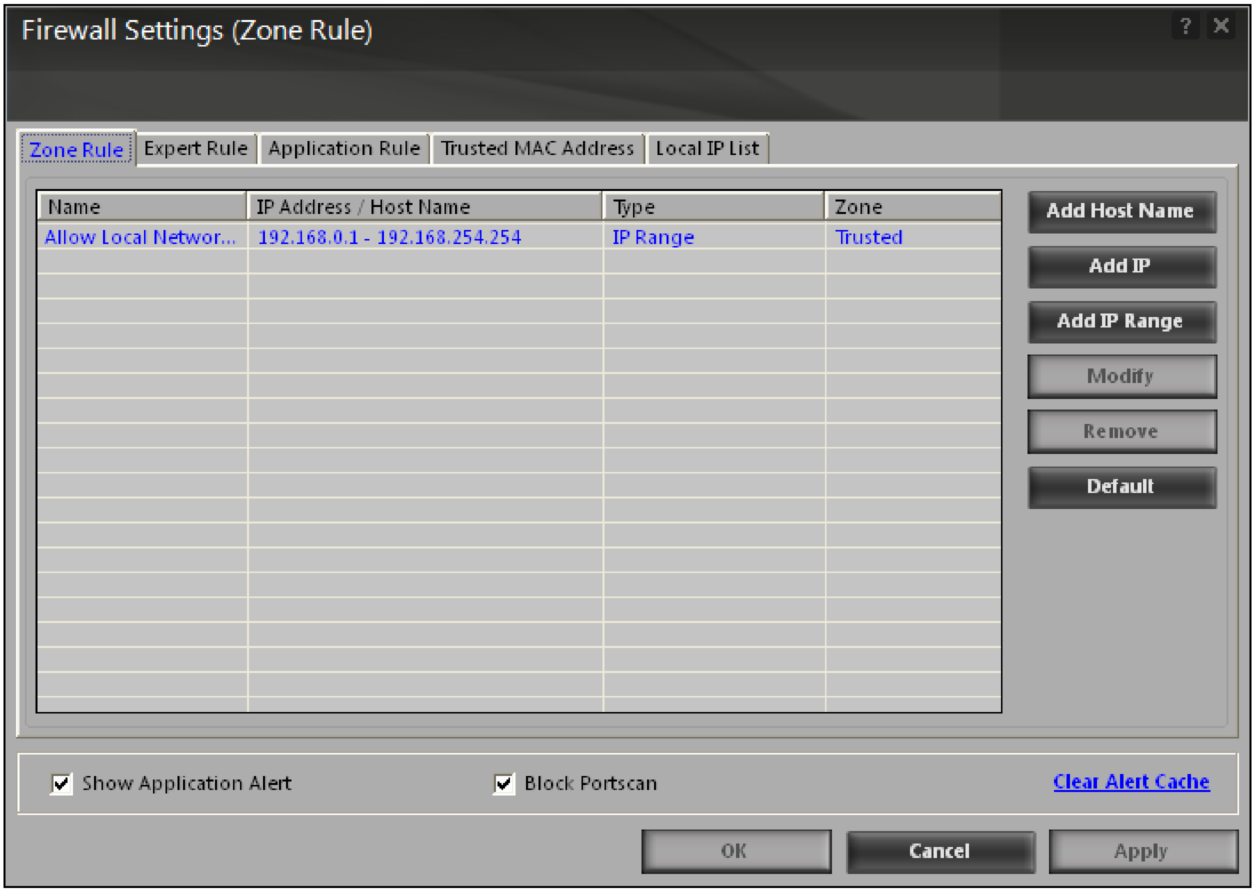
Settings:

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:

> At the bottom of the screen of all the tabs — Default, OK, Cancel, and Apply buttons are present that you can use after configuring the settings based on your requirement.
>
> **Default:** Click this button to apply the default settings.
>
> **OK:** Click this button after you click the **Apply** button to apply the configured settings.
>
> **Cancel:** Click this button to cancel the configured settings or to close the window.
>
> **Apply:** Click this button to apply the configured settings.

- ## 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. Refer Figure 57.



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

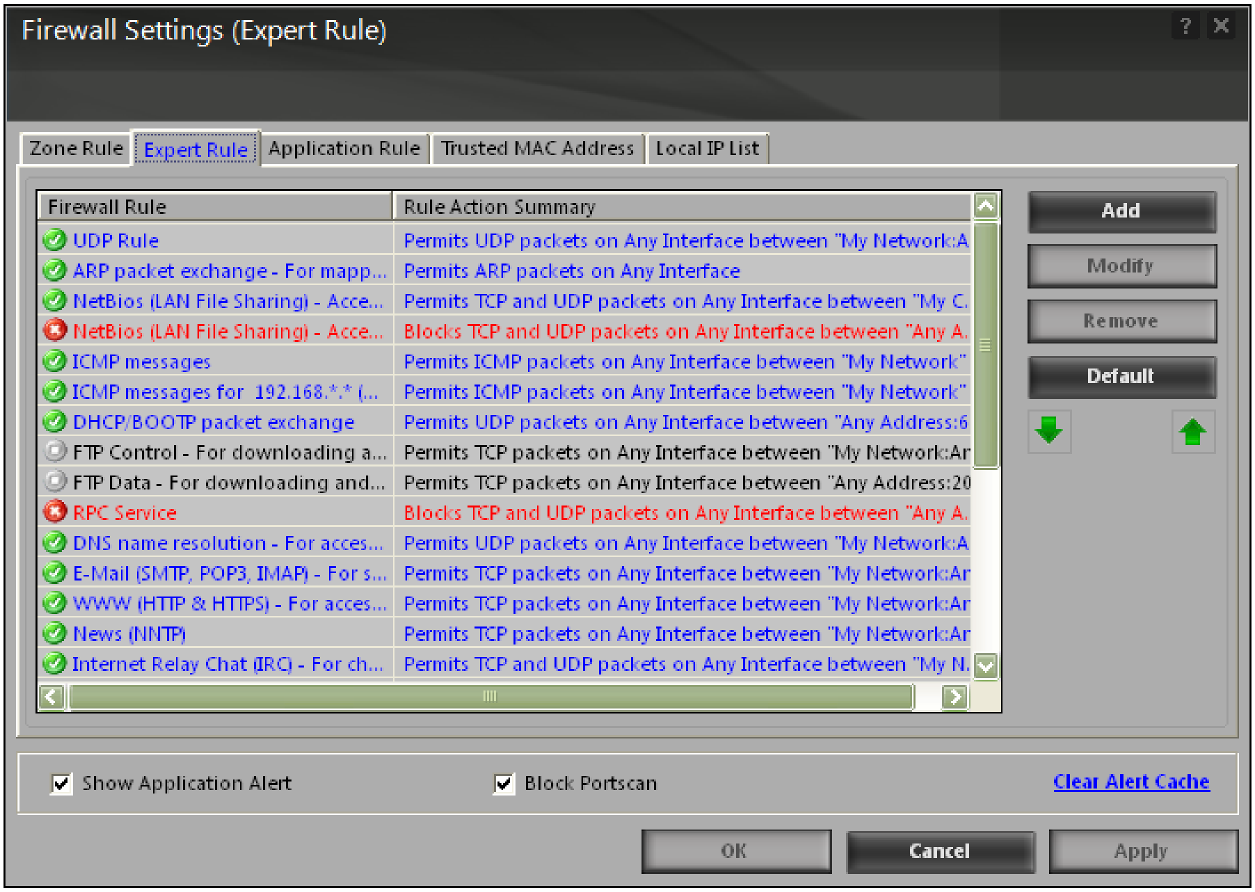
Figure 57

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. Refer Figure 58.

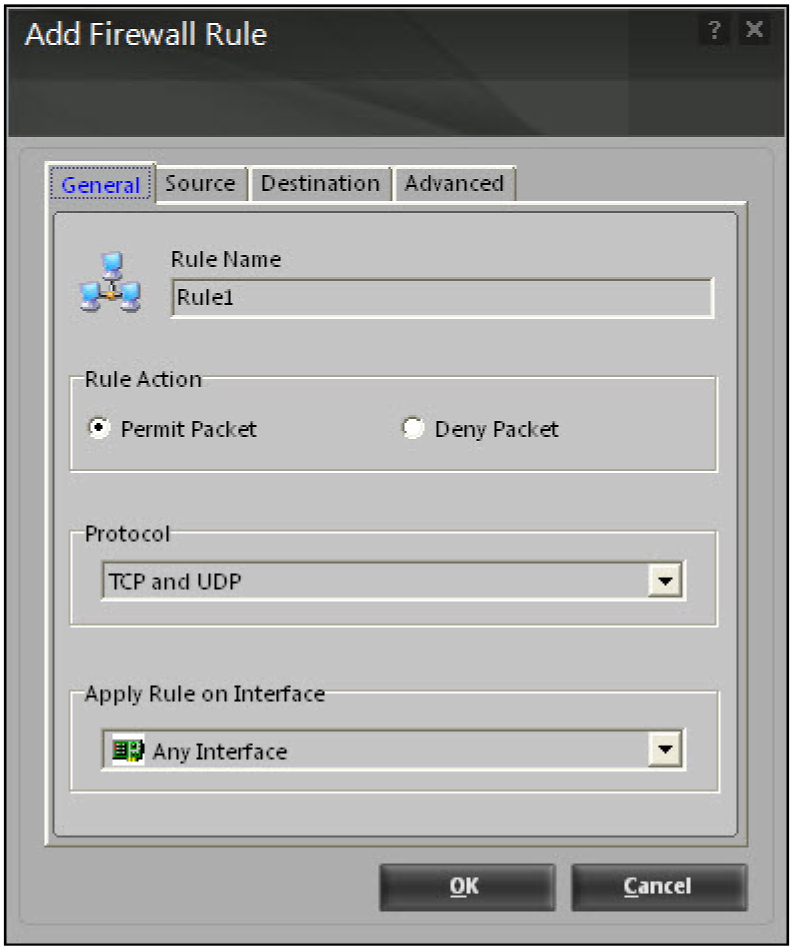


Firewall Rule	Rule Action Summary
✓ UDP Rule	Permits UDP packets on Any Interface between "My Network:A
✓ ARP packet exchange - For mapp...	Permits ARP packets on Any Interface
✓ NetBios (LAN File Sharing) - Acce...	Permits TCP and UDP packets on Any Interface between "My C.
✗ NetBios (LAN File Sharing) - 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 58

- Click the Add button to add new rules.
  The Add Firewall Rule window appears. Refer Figure 59.



Rule Name: Rule1

Rule Action: ● Permit Packet ○ Deny Packet

Protocol: TCP and UDP

Apply Rule on Interface: Any Interface

Figure 59

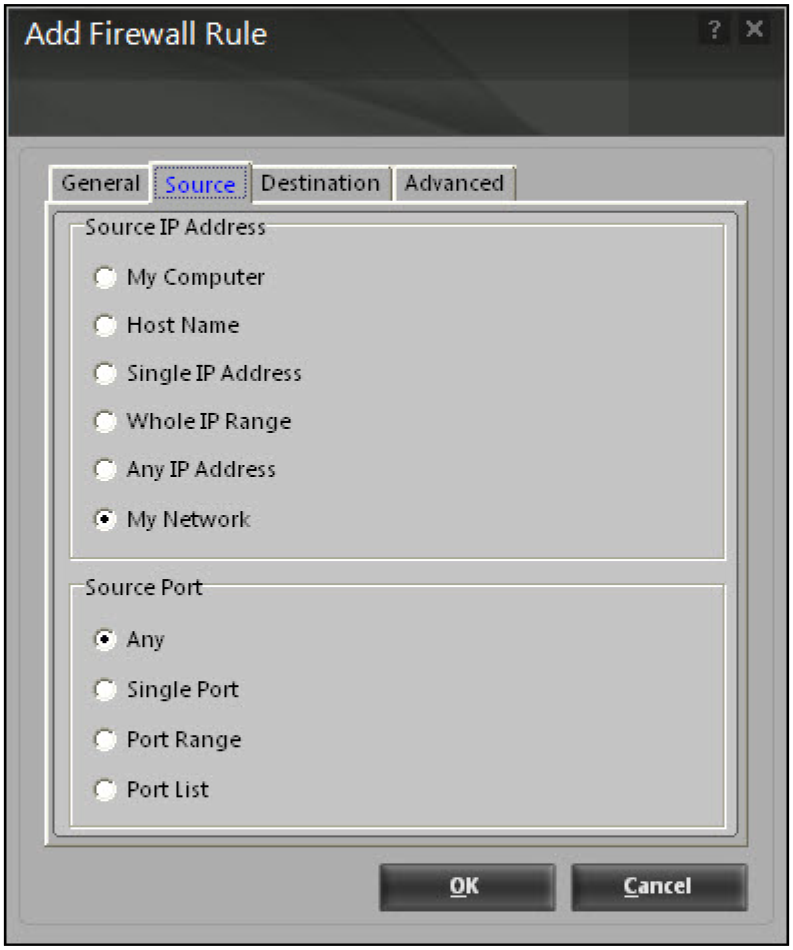
- **General**

This tab enables you to define rules and its actions. Specify the following field details – Refer Figure 59.

- **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:** Click on this option to select Interface to apply the rule. By default, **Any Interface** is selected.

- **Source**

This tab enables you to type the source IP address and port wherever applicable. Click an appropriate option. By default, **My Network** under **Source IP Address** section and **Any** under **Source Port** section are selected. Refer Figure 60.



Source IP Address

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

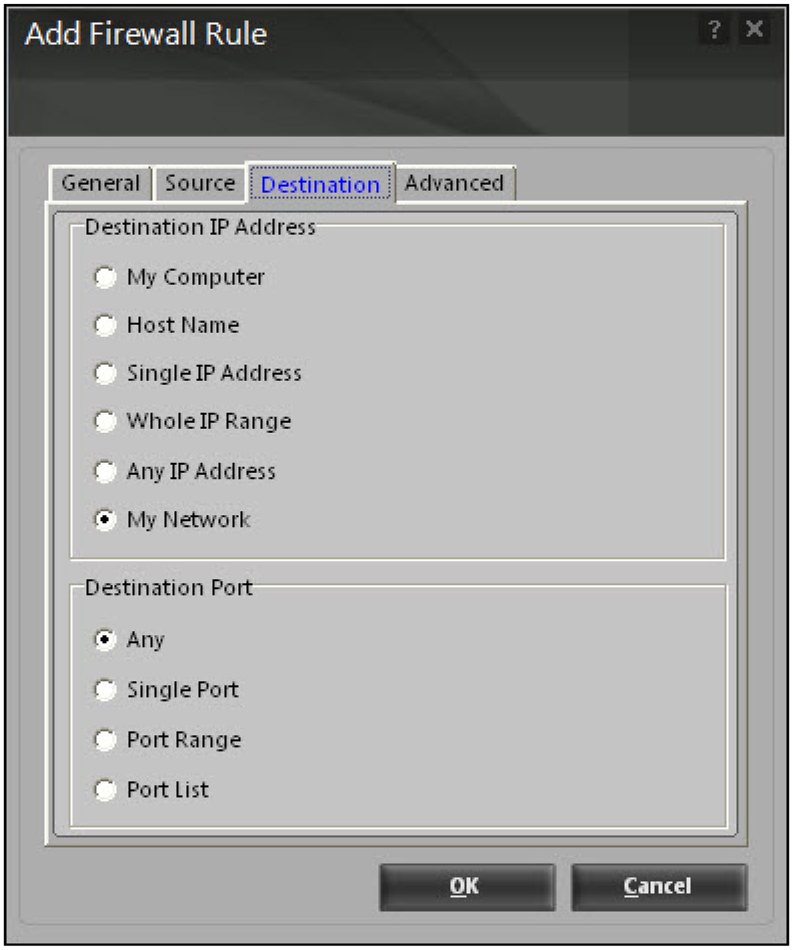
Source Port

● Any
○ Single Port
○ Port Range
○ Port List

Figure 60

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. Refer Figure 61.



Destination IP Address

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

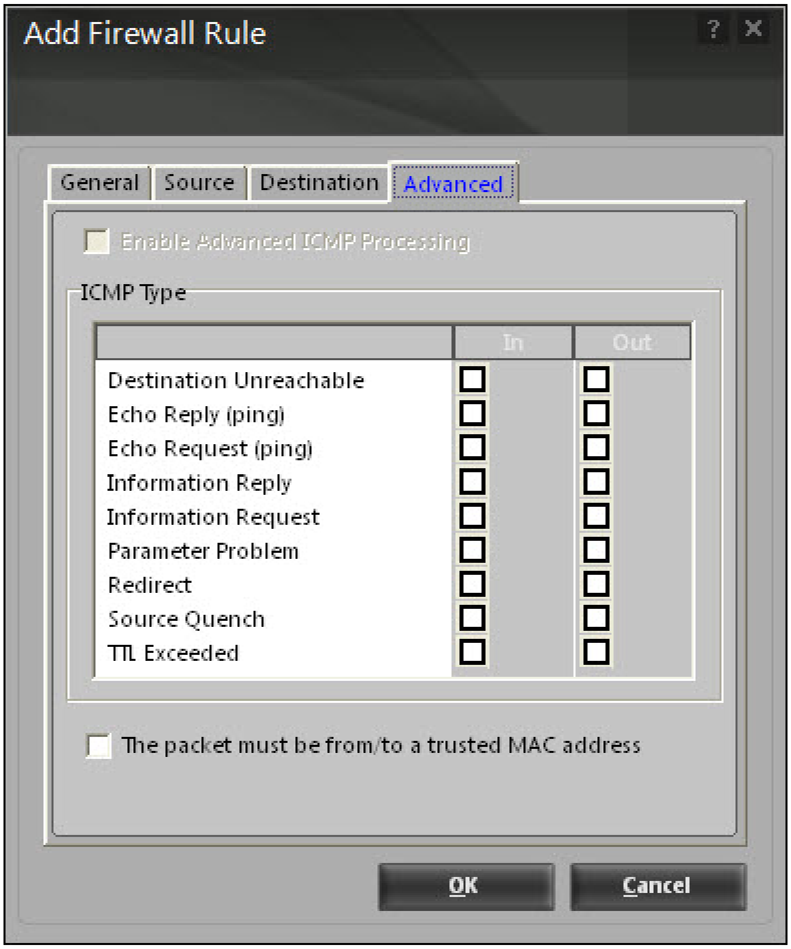
Destination Port

● Any
○ Single Port
○ Port Range
○ Port List

Figure 61

- ### 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. Refer Figure 62.



□ Enable Advanced ICMP Processing

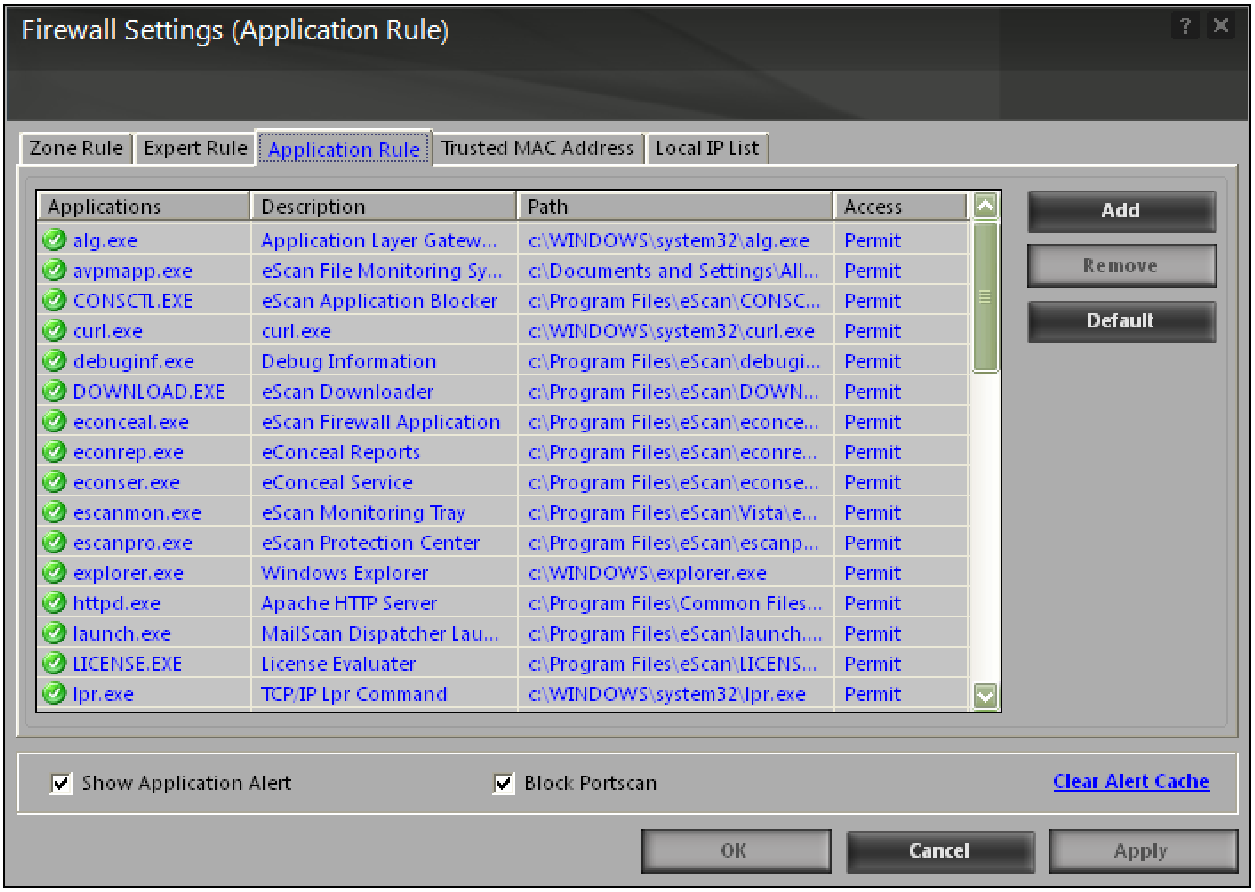
	In	Out
Destination Unreachable	□	□
Echo Reply (ping)	□	□
Echo Request (ping)	□	□
Information Reply	□	□
Information Request	□	□
Parameter Problem	□	□
Redirect	□	□
Source Quench	□	□
TTL Exceeded	□	□

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

Figure 62

▪ 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.



Firewall Settings (Application Rule)

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 Clear Alert Cache

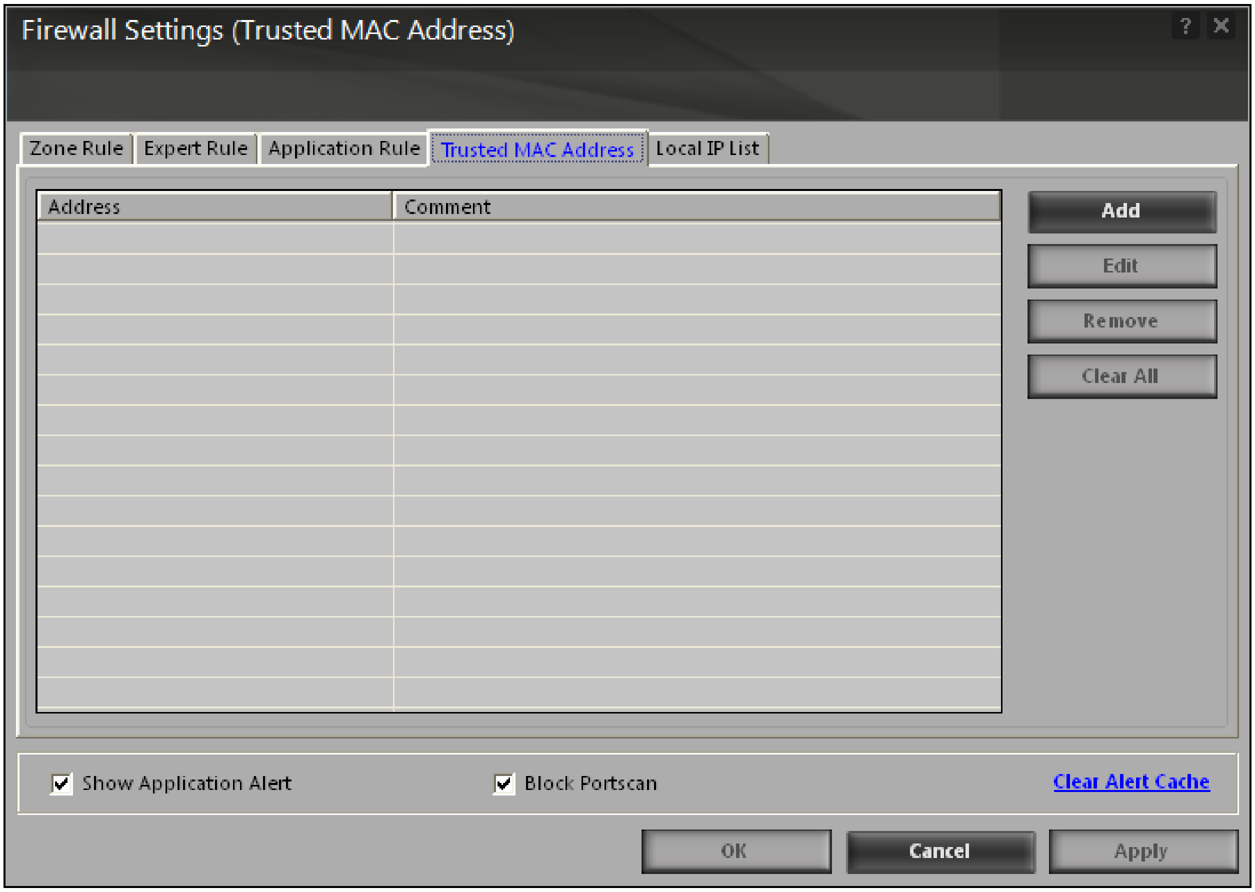
Figure 63

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

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

Trusted MAC Address

This section contains a list of Trusted Mac Addresses. A MAC address is a hardware address that uniquely identifies each node of a network. 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. Refer Figure 64.



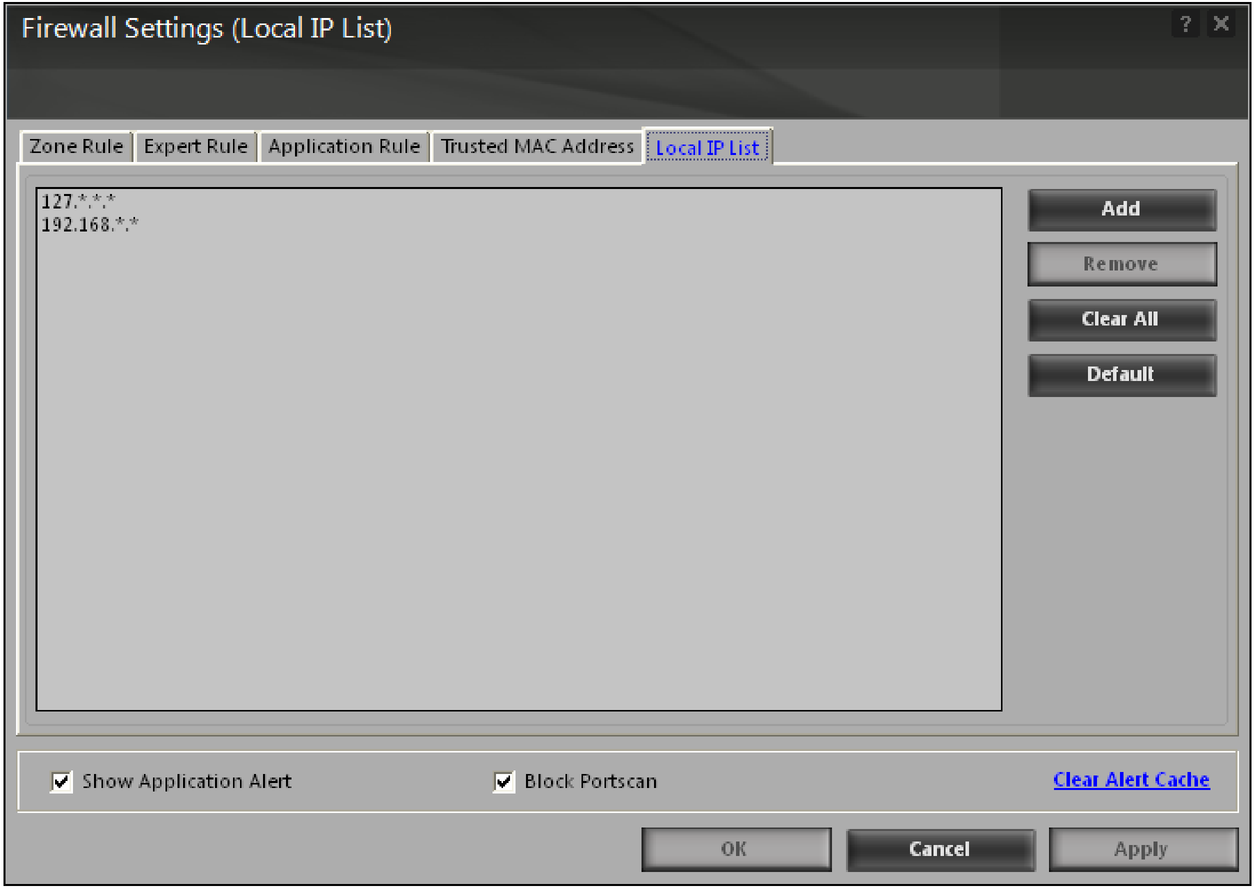
☑ Show Application Alert

☑ Block Portscan

Figure 64

- ### Local IP List

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

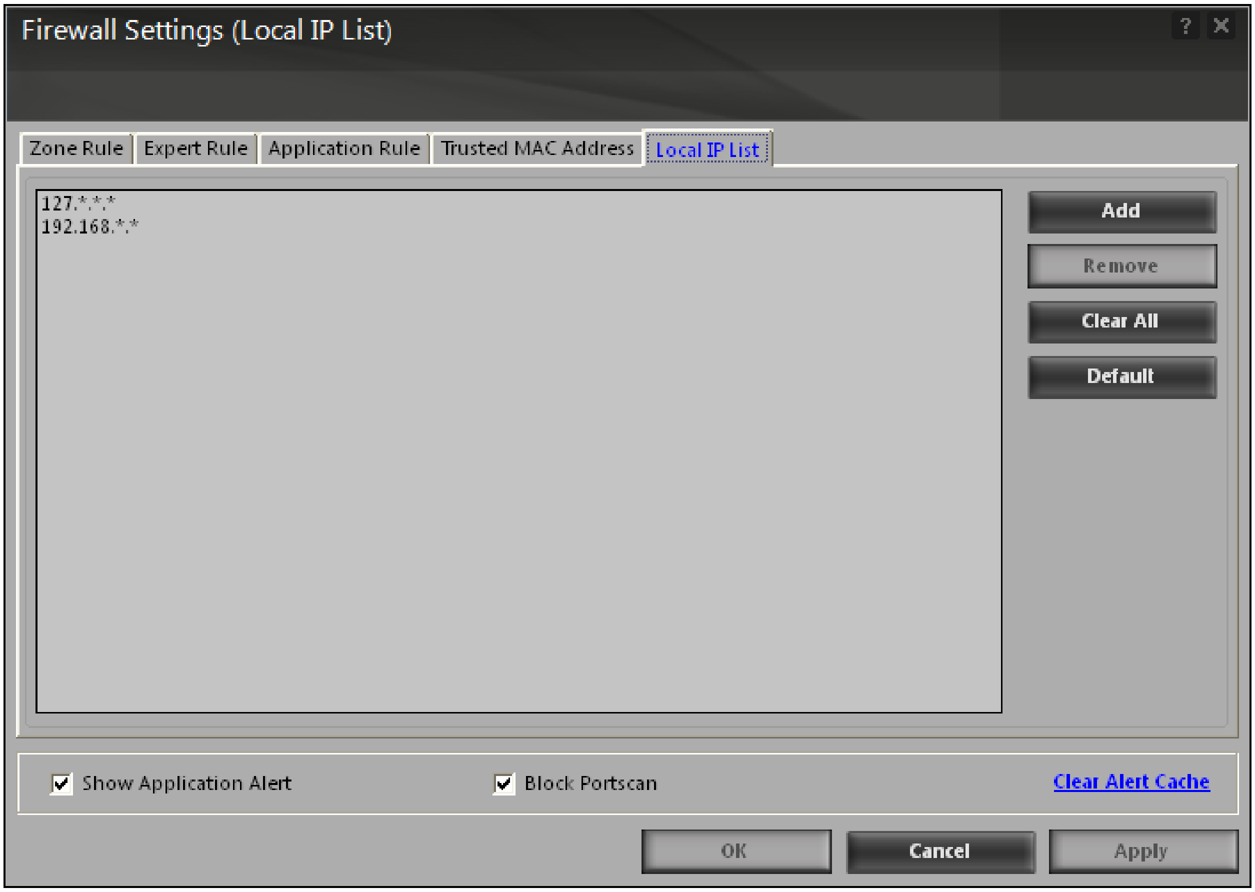


```
127.*.*.*
192.168.*.*
```

☑ Show Application Alert

☑ Block Portscan

Figure 65.



Firewall Settings (Local IP List)

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

☑ Show Application Alert ☑ Block Portscan

Figure 65

- **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.
- **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 checkbox, if you wish to block all Portscan attempts made by Hackers.
- Reports

This section displays the following information: Refer Figure 56.

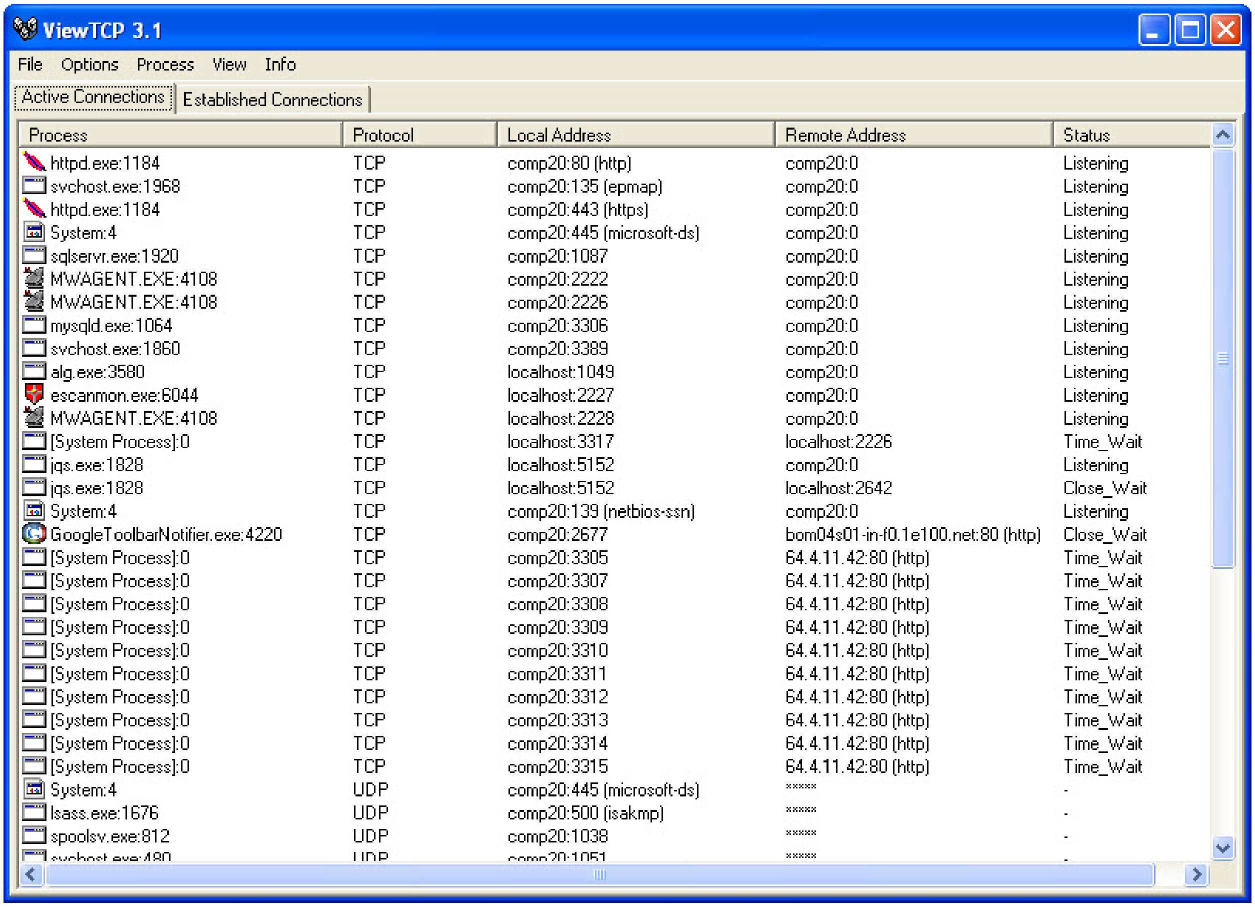
- **Inbound Packets Blocked:** It shows the total number of inbound packets that were blocked by the firewall.
- **Outbound Packets Blocked:** It shows the total number of outbound packets that were blocked by the firewall.

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. Refer Figure 66.



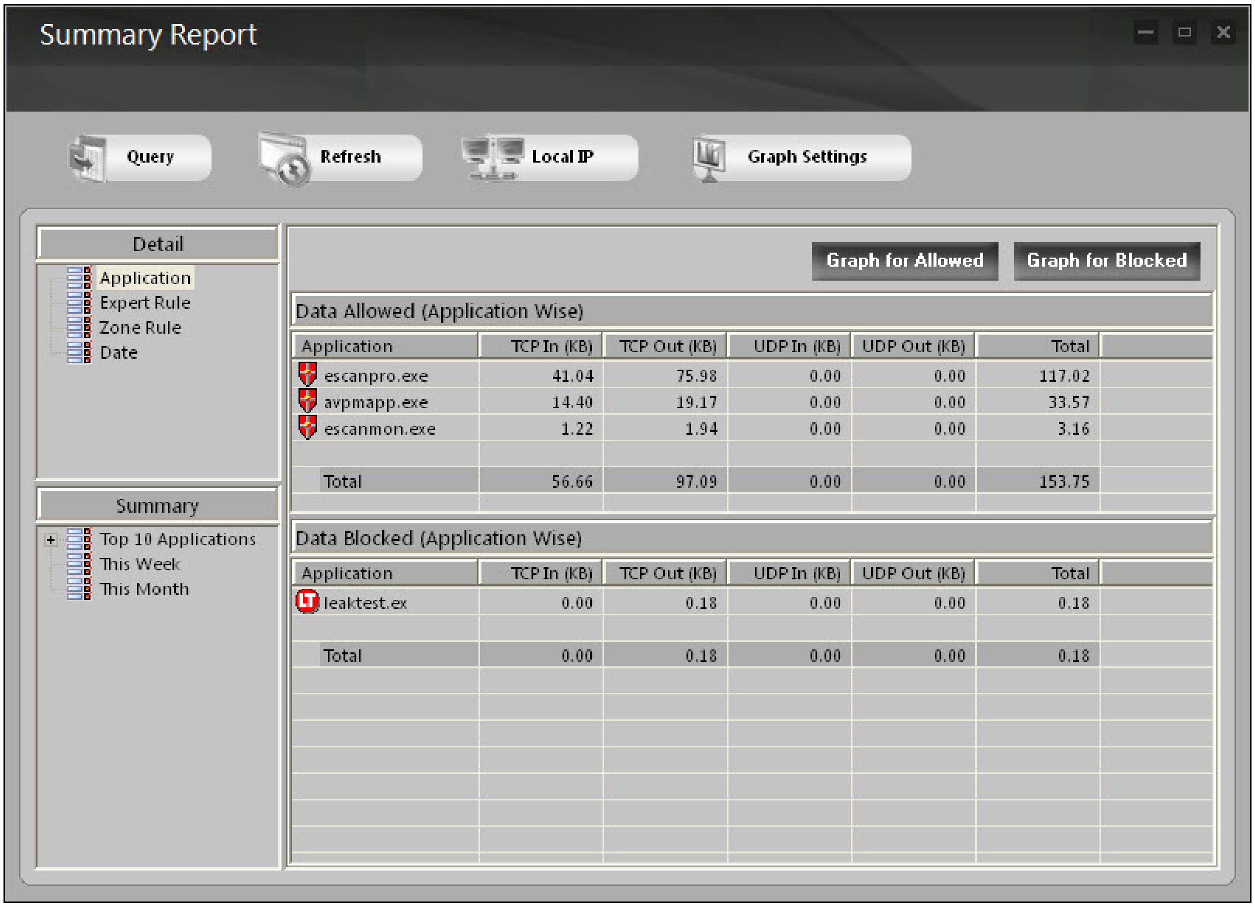
Process	Protocol	Local Address	Remote Address	Status
httpd.exe:1184	TCP	comp20:80 (http)	comp20:0	Listening
svchost.exe:1968	TCP	comp20:135 (epmap)	comp20:0	Listening
httpd.exe:1184	TCP	comp20:443 (https)	comp20:0	Listening
System:4	TCP	comp20:445 (microsoft-ds)	comp20:0	Listening
sqlservr.exe:1920	TCP	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 66

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. Refer Figure 67.



Data Allowed (Application Wise)

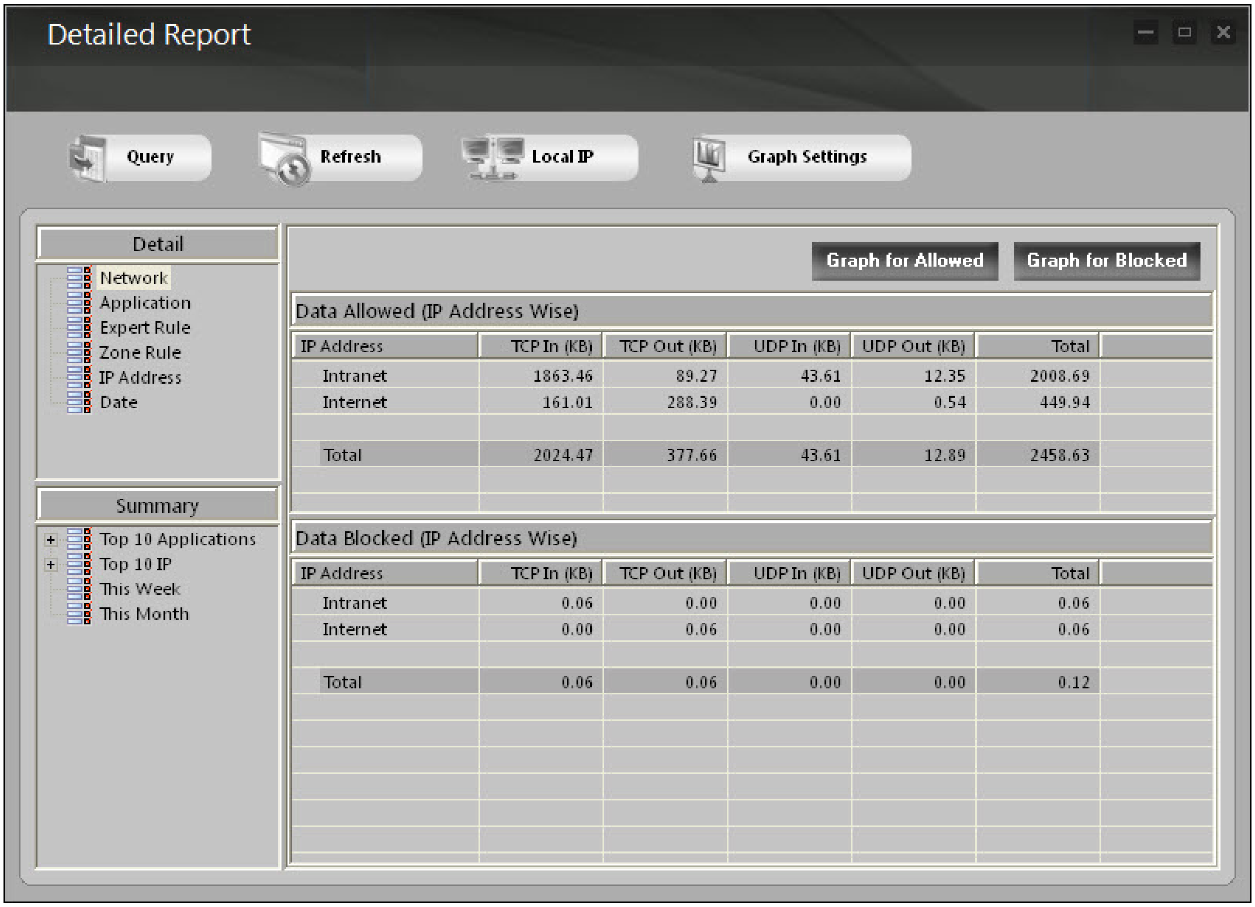
Application	TCP In (KB)	TCP Out (KB)	UDP In (KB)	UDP Out (KB)	Total
escanpro.exe	41.04	75.98	0.00	0.00	117.02
avpmapp.exe	14.40	19.17	0.00	0.00	33.57
escanmon.exe	1.22	1.94	0.00	0.00	3.16
Total	56.66	97.09	0.00	0.00	153.75

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 67

A detailed report includes information about the rules regarding network activities and shows data in the form of graphs and charts. Refer Figure 68.



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

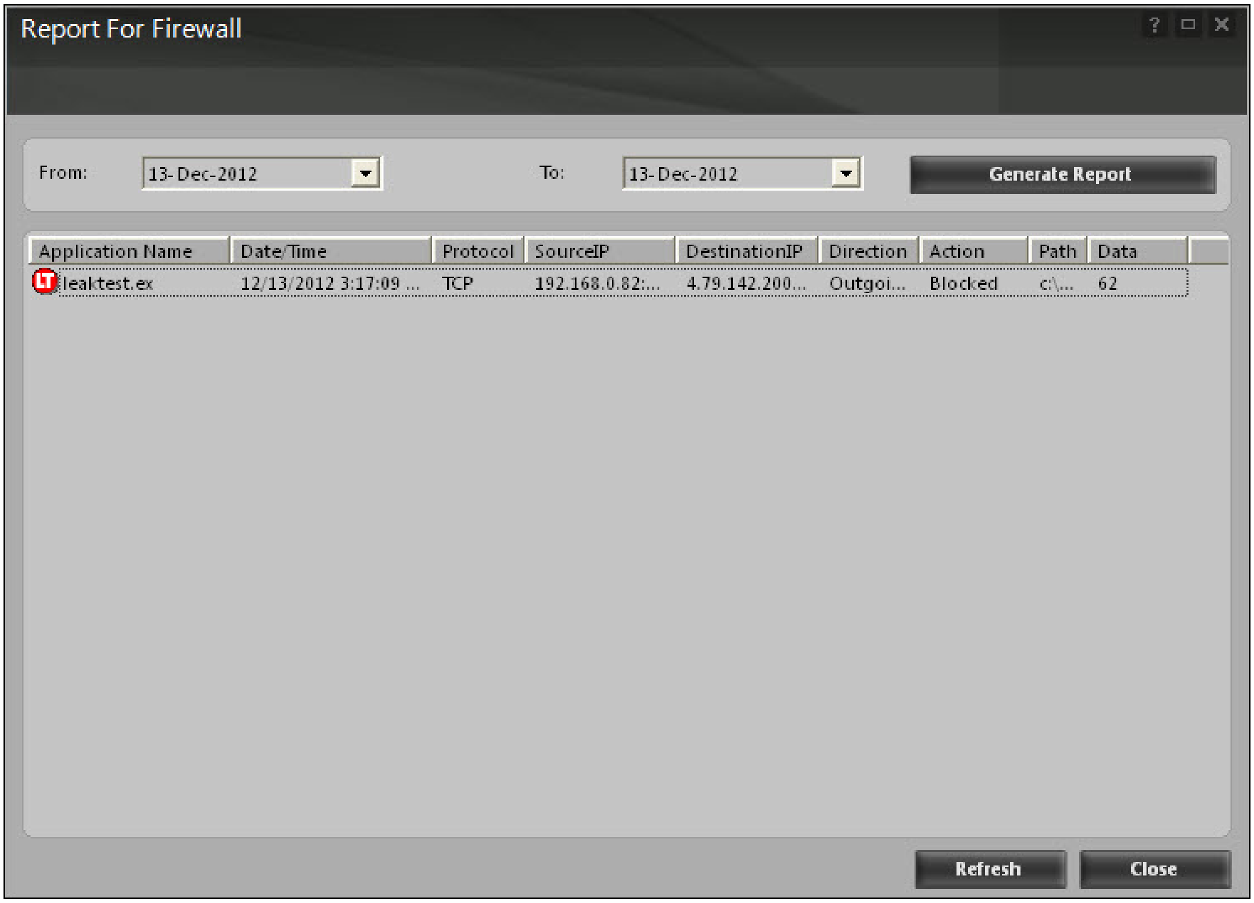
Data Blocked (IP Address Wise)

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 68

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. Refer Figure 69.



From: 13-Dec-2012

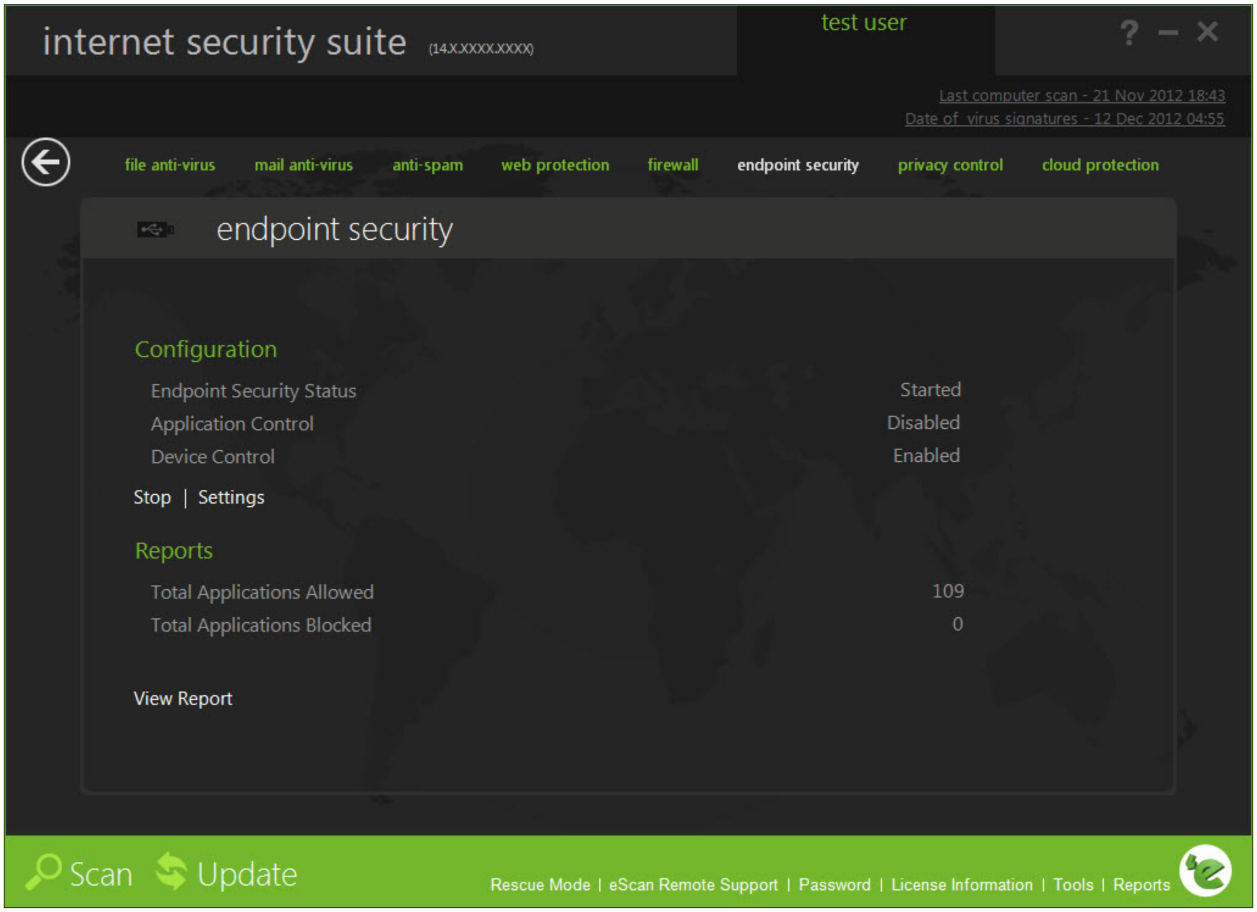
To: 13-Dec-2012

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 69

Endpoint Security

Endpoint Security is the sixth module of the eScan for ISS. This module protects your computer or Endpoints from data thefts and security threats through USB or FireWire®-based portable devices. It comes with an Application control feature, which helps you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that helps you determine which applications and portable devices are allowed or blocked by eScan. Refer Figure 70.



endpoint security

Configuration

Endpoint Security Status Started
Application Control Disabled
Device Control Enabled

Stop | Settings

Reports

Total Applications Allowed 109
Total Applications Blocked 0

View Report

internet security suite (14.X.XXXX.XXXX)
test user
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Figure 70

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:

- **Endpoint Security Status:** It displays the status of whether Endpoint Security module is started or stopped.
- **Application Control:** It displays the status of Application Control.
- **Device Control:** It displays the status of Device Control.

Start/Stop:

Click on this option to enable or disable Endpoint Security module.

Settings:

When you click this button, the **Endpoint Security Settings** window appears. On the **Endpoint Security Settings** window, you have two main tabs — Application Control and Device Control, and under Application Control, you have three sub-tabs — Block list, White list, and Define time-restriction.

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

Default: Click this button to apply the default settings.

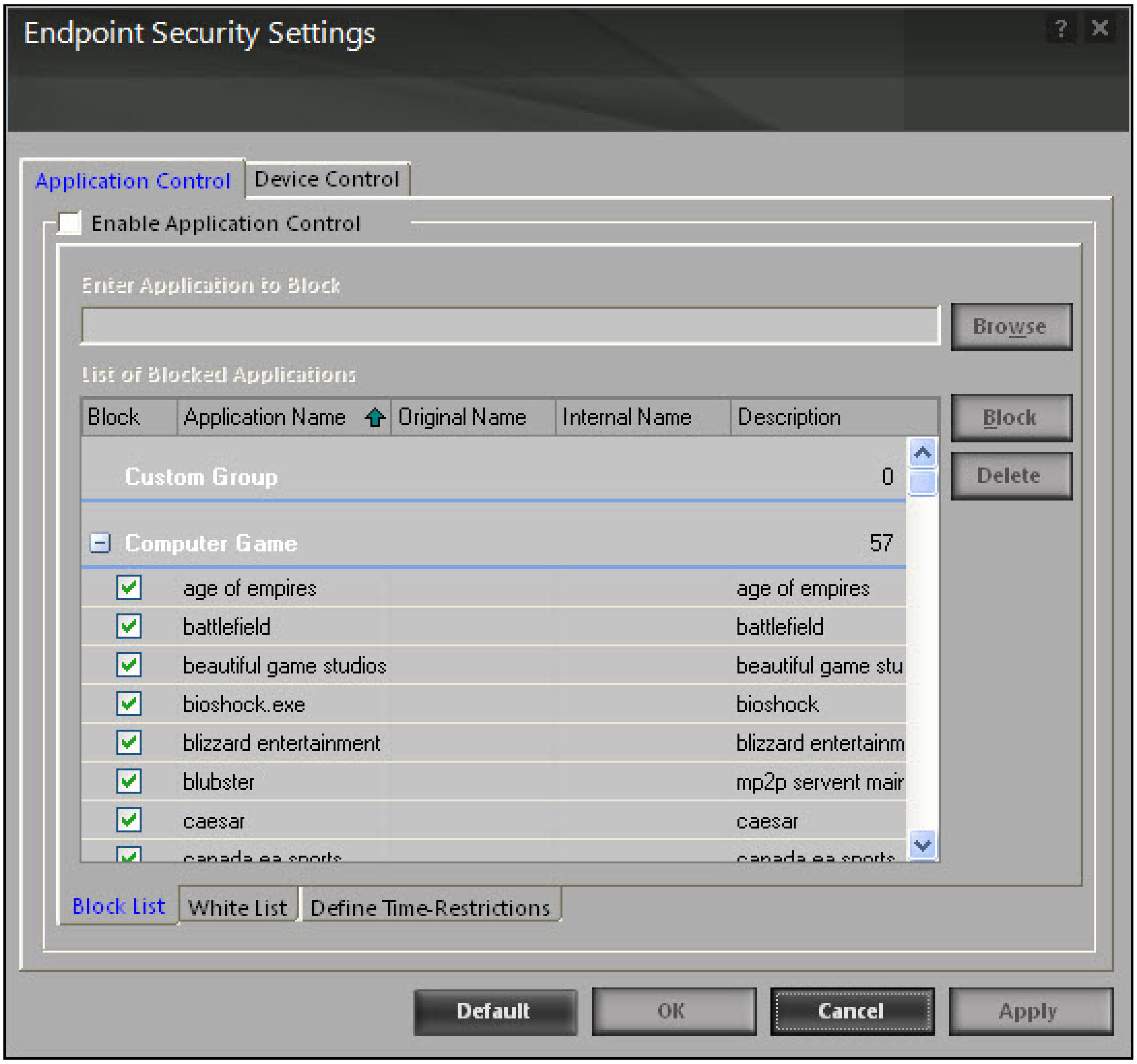
OK: Click this button after you click the **Apply** button to apply the configured settings.

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

Apply: Click this button to apply the configured settings.

Application Control

This tab helps you control execution of applications on the computer. By default, all the options are unavailable, except Block List and White list tab. The following are two types of list which helps you control applications: Refer Figure 71.



□ Enable Application Control

Block	Application Name	Original Name	Internal Name	Description
Custom Group				0
⊟ Computer Game				57
☑	age of empires			age of empires
☑	battlefield			battlefield
☑	beautiful game studios			beautiful game stu
☑	bioshock.exe			bioshock
☑	blizzard entertainment			blizzard entertainm
☑	blubster			mp2p servent mair
☑	caesar			caesar
☑	canada ea sports			canada ea sports

Figure 71

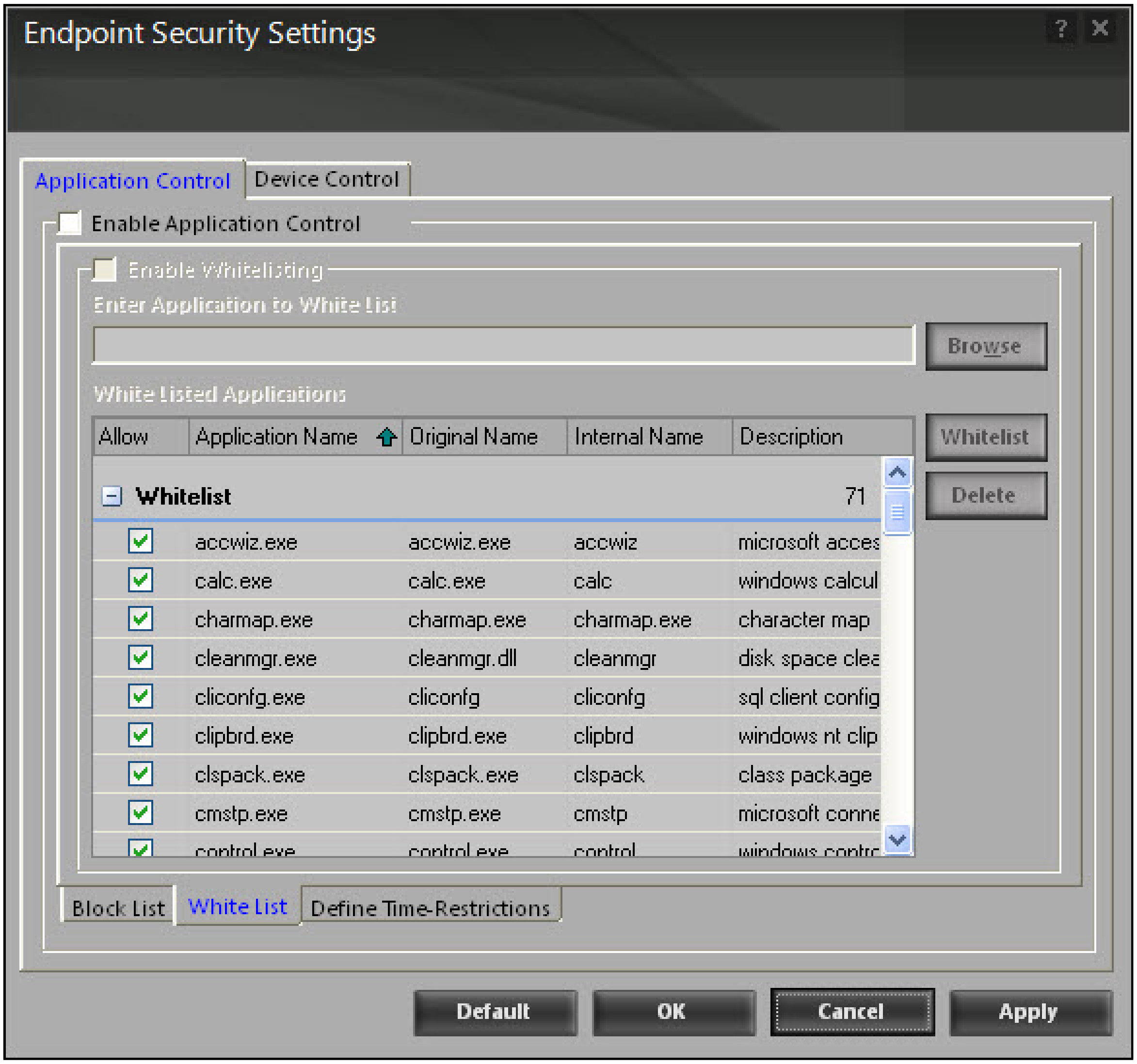
- **Block list:** Click this tab, if you want to configure settings for blocking the unwanted applications.

  You can configure the following settings:

  - **Enable Application Control:** Select this check box, if you want to enable Application Control feature, which helps you to block application.

- **Enter Application to Block:** This field and **Browse** button is available only when you select **Enable Application Control** check box.
  Type or click the **Browse** button to select name of the application that you want to block, and then click the **Block** button. If you want to delete an application, click an appropriate application from the group that you want to delete, and then click the **Delete** button.
- **List of Blocked Applications:** It contains the list of blocked executables of applications that are pre-defined by MicroWorld. By default, all the applications listed in pre-defined category are blocked. You can also add application that you want to block, but only to the **Custom Group** category. Select an appropriate application checkbox, and then click **Block** button. If you want to unblock any application, click to clear the application checkbox. The predefined categories include computer game, instant messengers, music video players, and P2P applications.
  In addition, you can also allow or block the pre-defined categories of group or an application in a group. You have to right-click the group or an application, and then click **Allow This Group** or **Block This Group** option accordingly.

- **Whitelist:** Click this tab, if you want to configure settings for whitelisting the known good applications of your choice. This feature helps you to allow access only to the whitelisted applications and block all other third-party applications. Apart from the listed whitelisted applications, all other Microsoft signed exe files also won’t be blocked. Refer Figure 72.



☐ Enable Application Control

☐ Enable Whitelisting

Enter Application to White List

White Listed Applications

⊟ **Whitelist** 71

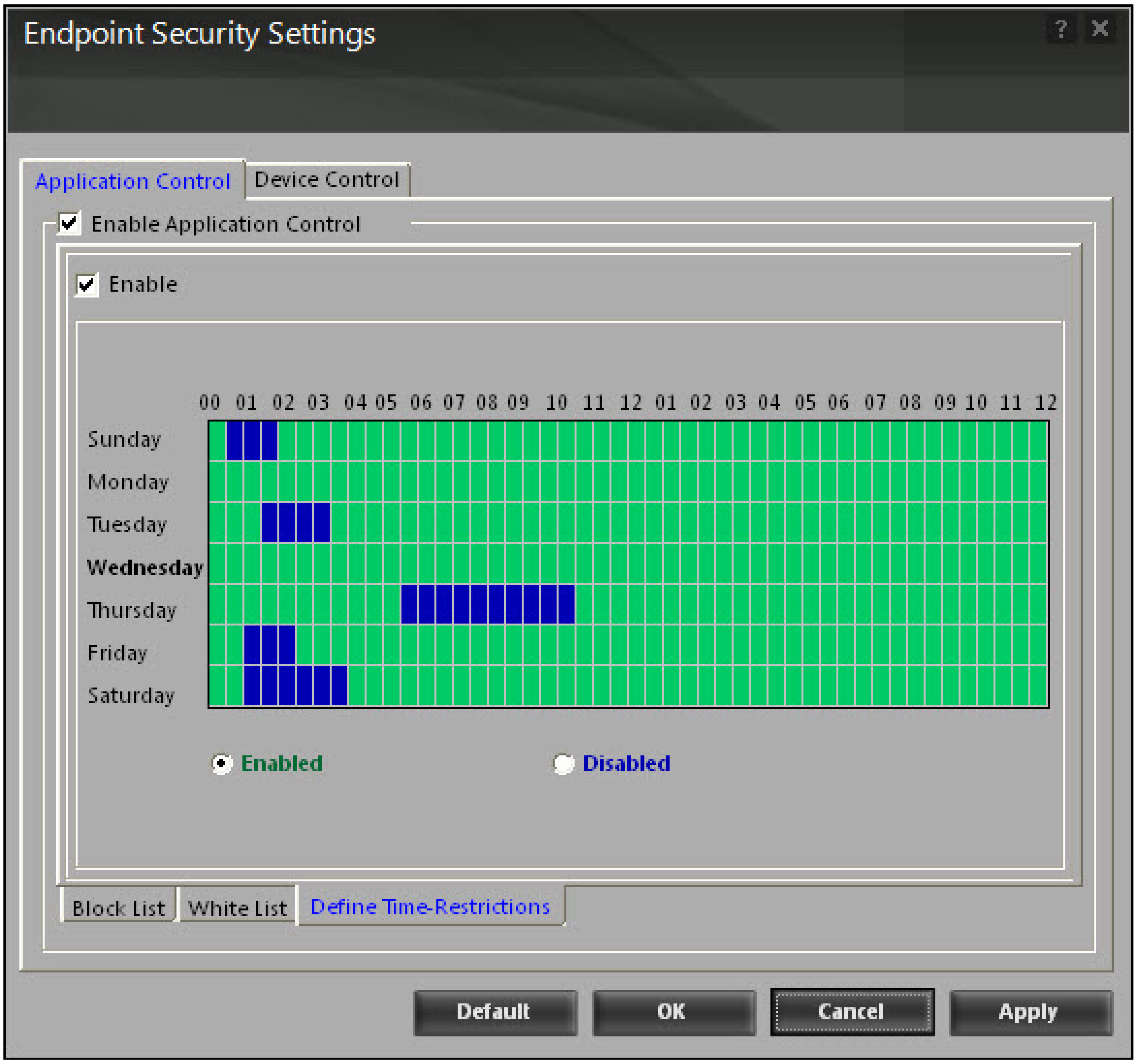
Allow	Application Name	Original Name	Internal Name	Description
☑	accwiz.exe	accwiz.exe	accwiz	microsoft acces
☑	calc.exe	calc.exe	calc	windows calcul
☑	charmap.exe	charmap.exe	charmap.exe	character map
☑	cleanmgr.exe	cleanmgr.dll	cleanmgr	disk space clea
☑	cliconfg.exe	cliconfg	cliconfg	sql client config
☑	clipbrd.exe	clipbrd.exe	clipbrd	windows nt clip
☑	clspack.exe	clspack.exe	clspack	class package
☑	cmstp.exe	cmstp.exe	cmstp	microsoft conne
☑	control.exe	control.exe	control	windows contro

Figure 72

You can configure the following settings:

- **Enable Application Control:** [Default] Select this check box, if you want to enable Application Control feature, which helps you to whitelist an application.
- **Enable Whitelisting:** This field is available only when you select Enable Application Control check box. Select this checkbox if you want to whitelist an application.
- **Enter Application to White List:** This field and **Browse** button is available only when you select **Enable Application Control** and **Enable Whitelisting** check box.
  Type or click the **Browse** button to select name of an application that you want to whitelist, and then click the **Whitelist** button. If you want to delete an application, click an appropriate application from the list that you want to delete, and then click the **Delete** button.
- **White Listed Applications:** It contains the list of whitelisted applications.

- **Define Time-Restrictions:** Click this tab, if you want to disable application control feature. This feature helps you define time restriction on when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day. Refer Figure 73.



Endpoint Security Settings

Application Control | Device Control

☑ Enable Application Control

☑ Enable

● Enabled ○ Disabled

Figure 73

- **Enable:** By default, this check box appears dimmed. It is available only if you select the **Enable Application Control** check box. Select this check box if you want to define time restriction.
  - **Enabled:** [Default] This option is available only when you select **Enable** check box. Click this option if you want to allow access to the applications on certain days at specific time, and then select the days and time by clicking the appropriate boxes from the matrix.

  - **Disabled:** This option is available only when you select **Enable** check box. Click this option if you want to block access to the applications on certain days at specific time, and then select the days and time by clicking the appropriate boxes in the matrix.

- ### Device Control

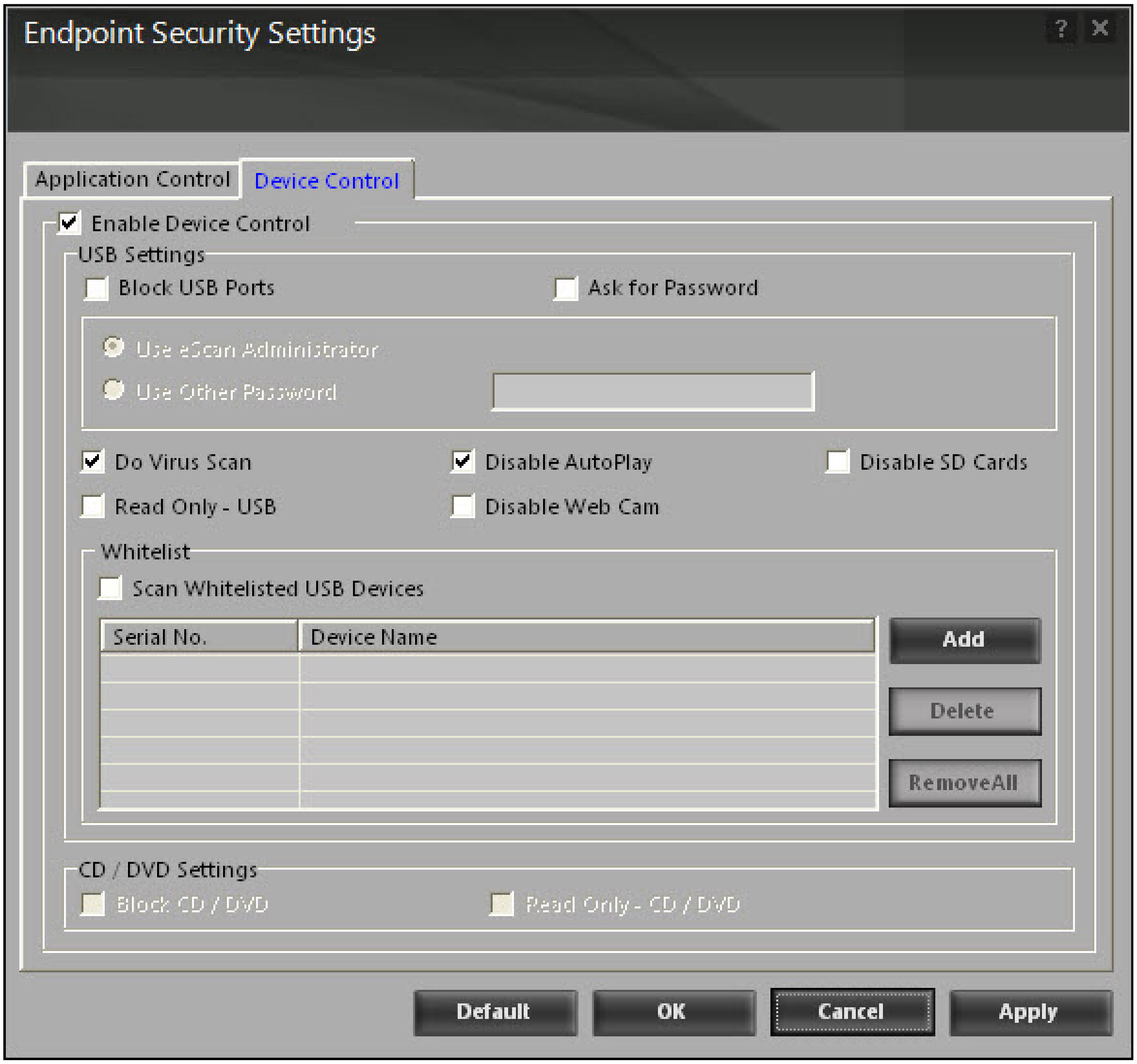
This tab helps you to protect your computer from unauthorized portable storage devices like USBs, SD cards, Webcams, CDs, and DVDs. As most of the viruses spread through external devices, it is essential that you provide proper protection.

The Enable Device Control feature enables you to keep monitor on devices that are connected to the computer. You can block or password protect the USB device, wherein unauthorized device cannot access your computer unless a valid password is entered.

The device control feature helps you to block, disable, or keep devices in read-only mode as per your requirement. Whenever required, you can perform a virus scan on the connected devices.

With the help of whitelisting feature you can whitelist USB devices, and if required you can also set an automatic scan on those devices. Refer Figure 74.

Figure 74



☑ Enable Device Control

USB Settings

□ Block USB Ports □ Ask for Password

○ Use eScan Administrator

○ Use Other Password

☑ Do Virus Scan ☑ Disable AutoPlay □ Disable SD Cards

□ Read Only - USB □ Disable Web Cam

Whitelist

□ Scan Whitelisted USB Devices

Serial No.	Device Name

CD / DVD Settings

□ Block CD / DVD □ Read Only - CD / DVD

You can configure the following settings:

- **Enable Device Control:** [Default] Select this check box, if you want to monitor the devices connected to your computer. When you select this check box, all the fields become available.
- **USB Settings:** This section helps you to customize the settings for controlling access to USB storage devices.
  - **Block USB Ports:** This field is available only when you select **Enable Device Control** check box. Select this check box if you want to block all USB ports.

    When you select this check box, **Ask for Password**, **Do Virus Scan**, **Disable AutoPlay**, **Disable SD Cards**, **Read Only- USB**, **Disable Web Cam**, **Scan Whitelisted USB Devices** fields, and **Add** button becomes unavailable.

- **Ask for Password:** This field is available only when you select **Enable Device Control** check box. Select this check box, if you want eScan to prompt for a password, whenever a USB storage device is connected to the computer. Do any one of the following:
  - **Use eScan Administrator Password:** This option is available only when you select the **Ask for Password** check box. Click this option, if you want to use eScan ISS password for accessing USB device.
  - **Use Other Password:** This option is available only when you select the **Ask for Password** check box. Click this option, if you want to assign a unique password for accessing USB storage device. Type the password.
- **Do Virus Scan:** [Default] This field is available only when you select **Enable Device Control** check box.
  Select this check box, if you want to run a virus scan whenever a USB Device is plugged in, It is recommended that you always keep this check box selected.
- **Disable AutoPlay:** [Default] This field is available only when you select **Enable Device Control** check box.
  When you select this check box, eScan disables the automatic execution of any program stored on a USB storage device when you connect the device.
- **Disable SD Cards:** This field is available only when you select **Enable Device Control** check box.
  Select this check box, if you do not want to give the access to SD cards. This feature is applicable only for laptops.
- **Read Only - USB:** This field is available only when you select **Enable Device Control** check box.
  Select this check box, if you want to allow access to the USB device in a read-only mode.
- **Disable Web Cam:** This field is available only when you select **Enable Device Control** check box.
  Select this check box, if you do not want to give the access to webcam.

- **Whitelist:** eScan provides a greater level of endpoint security by prompting you for a password, whenever you connect a USB drive. To disable password protection for a specific device, you can add it to the whitelist along with its name and serial number. Due to which, next time when you connect the device it does not prompt you for a password for accessing the device. This section displays the serial number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking the **Add** button.
  - **Scan Whitelisted USB Devices:** This field is available only when you select **Enable Device Control** check box.
    Select this check box, if you want to scan all USB devices that are added to the whitelist.
  - **CD/DVD Settings:** This section helps you to customize the settings for controlling access to CD and DVD device.
    - **Block CD/DVD:** Select this check box if you want to block access to CD/DVD devices.
    - **Read Only - CD/DVD:** Select this check box, if you want to access the CD/DVD devices in a read-only mode.

- Reports

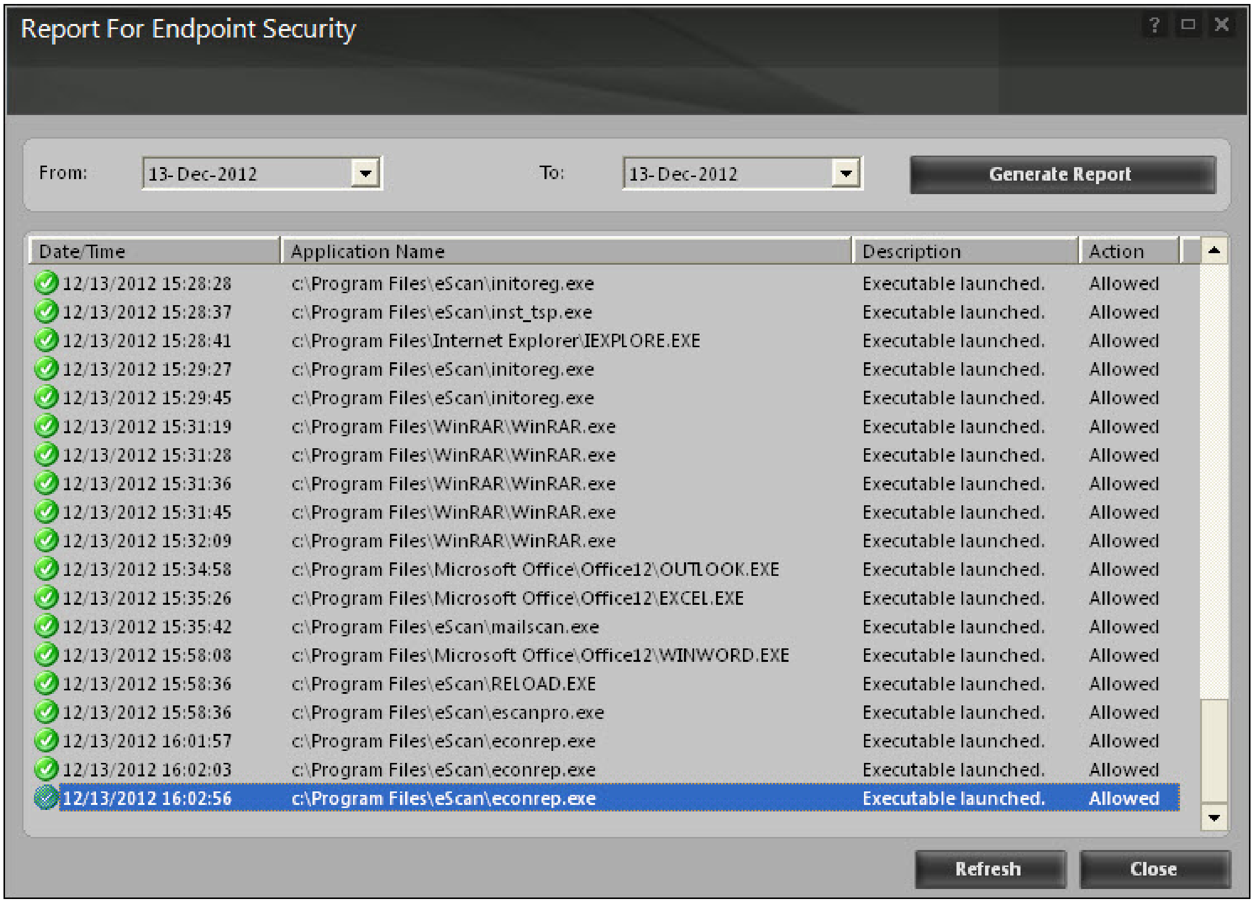
This section displays the following information: Refer Figure 70.

- **Total Applications Allowed:** It shows the total number of applications allowed by the Application Control module.
- **Total Applications Blocked:** It shows the total number of applications blocked by the Application Control module.

In addition, you can view the following reports:

View Report:

You can click this button to open the **Report For Endpoint Security** window. This window includes the **Generate Report** button, which displays the report for the Endpoint Security module for a given range of dates in a tabular format. Refer Figure 75.



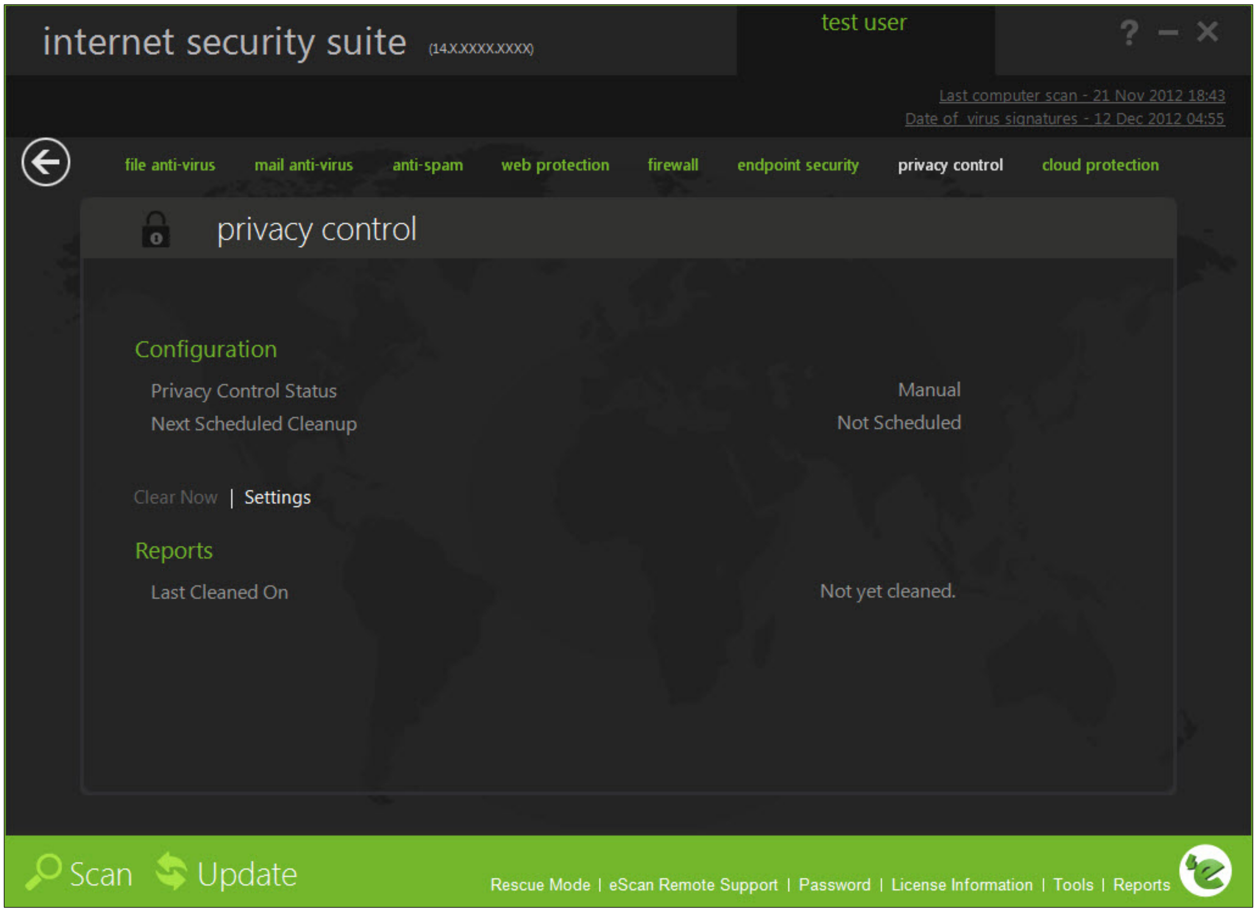
From: 13-Dec-2012 To: 13-Dec-2012

Date/Time	Application Name	Description	Action
✓ 12/13/2012 15:28:28	c:\Program Files\eScan\initoreg.exe	Executable launched.	Allowed
✓ 12/13/2012 15:28:37	c:\Program Files\eScan\inst_tsp.exe	Executable launched.	Allowed
✓ 12/13/2012 15:28:41	c:\Program Files\Internet Explorer\IEXPLORE.EXE	Executable launched.	Allowed
✓ 12/13/2012 15:29:27	c:\Program Files\eScan\initoreg.exe	Executable launched.	Allowed
✓ 12/13/2012 15:29:45	c:\Program Files\eScan\initoreg.exe	Executable launched.	Allowed
✓ 12/13/2012 15:31:19	c:\Program Files\WinRAR\WinRAR.exe	Executable launched.	Allowed
✓ 12/13/2012 15:31:28	c:\Program Files\WinRAR\WinRAR.exe	Executable launched.	Allowed
✓ 12/13/2012 15:31:36	c:\Program Files\WinRAR\WinRAR.exe	Executable launched.	Allowed
✓ 12/13/2012 15:31:45	c:\Program Files\WinRAR\WinRAR.exe	Executable launched.	Allowed
✓ 12/13/2012 15:32:09	c:\Program Files\WinRAR\WinRAR.exe	Executable launched.	Allowed
✓ 12/13/2012 15:34:58	c:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE	Executable launched.	Allowed
✓ 12/13/2012 15:35:26	c:\Program Files\Microsoft Office\Office12\EXCEL.EXE	Executable launched.	Allowed
✓ 12/13/2012 15:35:42	c:\Program Files\eScan\mailscan.exe	Executable launched.	Allowed
✓ 12/13/2012 15:58:08	c:\Program Files\Microsoft Office\Office12\WINWORD.EXE	Executable launched.	Allowed
✓ 12/13/2012 15:58:36	c:\Program Files\eScan\RELOAD.EXE	Executable launched.	Allowed
✓ 12/13/2012 15:58:36	c:\Program Files\eScan\escanpro.exe	Executable launched.	Allowed
✓ 12/13/2012 16:01:57	c:\Program Files\eScan\econrep.exe	Executable launched.	Allowed
✓ 12/13/2012 16:02:03	c:\Program Files\eScan\econrep.exe	Executable launched.	Allowed
✓ 12/13/2012 16:02:56	c:\Program Files\eScan\econrep.exe	Executable launched.	Allowed

Figure 75

Privacy Control

Privacy Control is the seventh module of the eScan for ISS. It protects your confidential information from theft by deleting all the temporary information stored on your computer. This module comes with the eScan Browser Cleanup feature, which allows you to use the Internet without leaving any history or residual data on your hard drive by erasing details of sites and Web pages you have accessed while browsing. Refer Figure 76.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
privacy control
Clear Now | Settings
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

Privacy Control Status	Manual
Next Scheduled Cleanup	Not Scheduled

Reports

Last Cleaned On	Not yet cleaned.

Figure 76

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.

- **Privacy Control Status:** It shows the mode in which the Privacy Control module is running. This mode can be either Manual or Scheduled mode.
- **Next Scheduled Cleanup:** It displays when Privacy Control will run next.

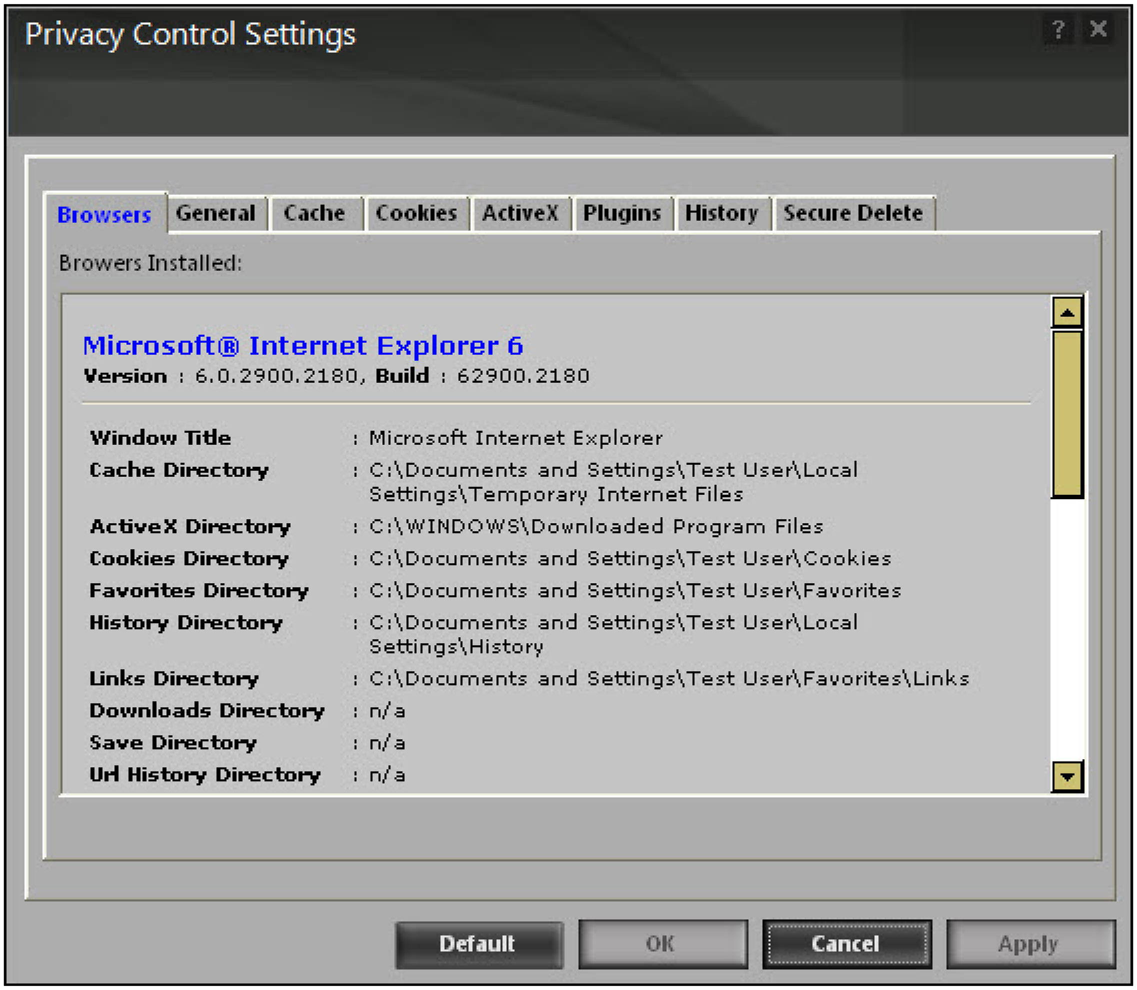
In addition, you can perform the following tasks:

Clear Now:

You can click this button to clear the information specified under Options in the Browser Clean up dialog box.

- **Browsers**

This tab displays information regarding all the browsers installed on your computer. Refer Figure 77.



Browers Installed:

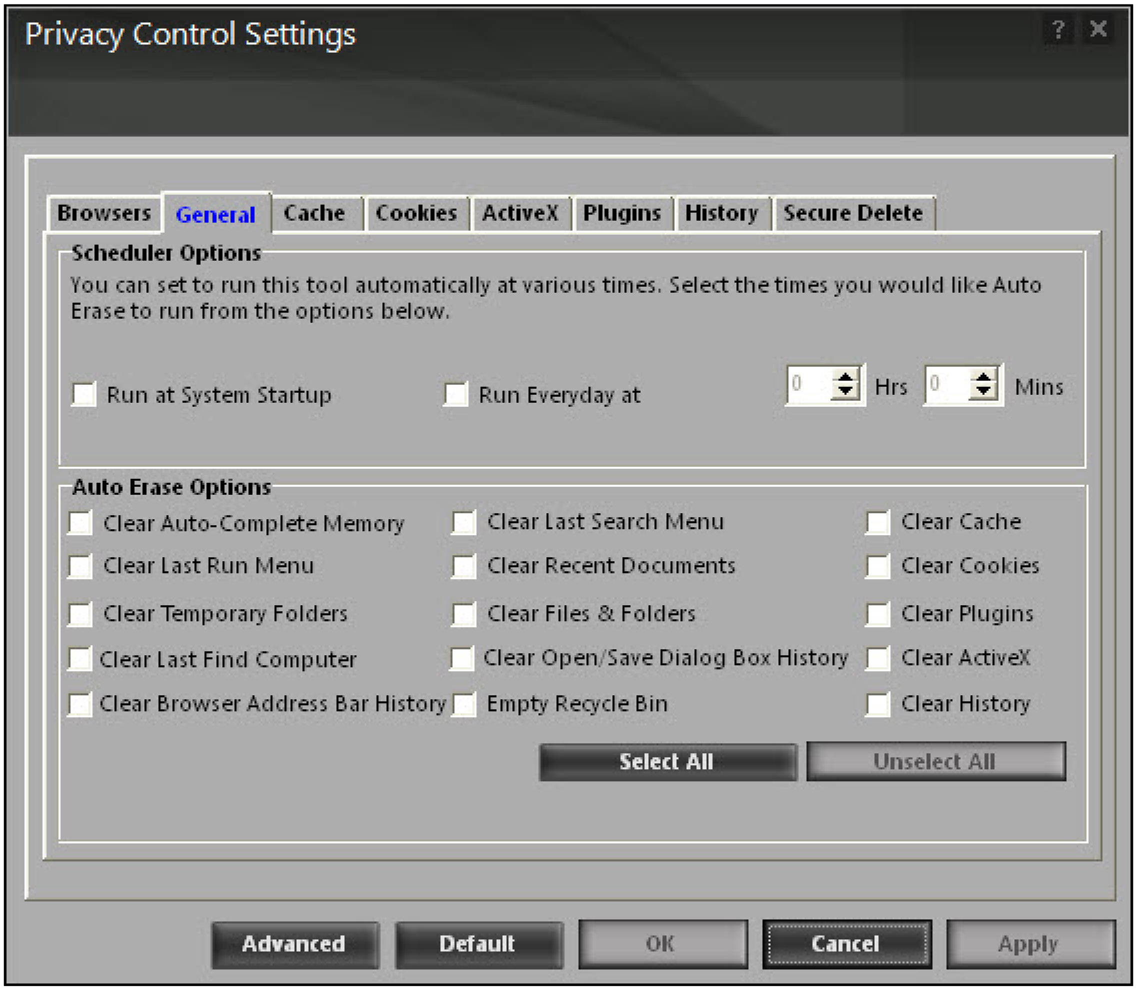
Microsoft® Internet Explorer 6
Version : 6.0.2900.2180, **Build** : 62900.2180

Window Title	: Microsoft Internet Explorer
Cache Directory	: C:\Documents and Settings\Test User\Local Settings\Temporary Internet Files
ActiveX Directory	: C:\WINDOWS\Downloaded Program Files
Cookies Directory	: C:\Documents and Settings\Test User\Cookies
Favorites Directory	: C:\Documents and Settings\Test User\Favorites
History Directory	: C:\Documents and Settings\Test User\Local Settings\History
Links Directory	: C:\Documents and Settings\Test User\Favorites\Links
Downloads Directory	: n/a
Save Directory	: n/a
Url History Directory	: n/a

Figure 77

- **General**

This tab helps you specify the unwanted files created by Web browsers or by other installed software that should be deleted. Refer Figure 78.



Scheduler Options

You can set to run this tool automatically at various times. Select the times you would like Auto Erase to run from the options below.

□ Run at System Startup □ Run Everyday at 0 Hrs 0 Mins

Auto Erase Options

□ Clear Auto-Complete Memory □ Clear Last Search Menu □ Clear Cache
□ Clear Last Run Menu □ Clear Recent Documents □ Clear Cookies
□ Clear Temporary Folders □ Clear Files & Folders □ Clear Plugins
□ Clear Last Find Computer □ Clear Open/Save Dialog Box History □ Clear ActiveX
□ Clear Browser Address Bar History □ Empty Recycle Bin □ Clear History

Figure 78

You can configure the following settings.

- **Scheduler Options:** You can set the scheduler to run at specific time and erase private information, such as your browsing history from your computer. You can perform the following settings:
  - **Run at System Startup:** Select this check box if you want to run auto erase tool at system startup. It auto executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.
  - **Run Everyday at:** Select this check box if you want to specify the time at which you want auto erase tool to run. It auto-executes the Privacy Control module at a specified time and performs the desired auto erase functions.
    The **Hrs** and **Mins** field is available only when you select **Run Everyday at** check box. Type the time in hours and minutes in appropriate boxes.

- **Auto Erase Options:** The browser stores traceable information of the web sites that you have visited in certain folders. This information can be viewed by others. eScan allows you to remove all traces of web sites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. Select the following options based on your requirement:
    - **Clear Auto-Complete Memory:** Auto-Complete Memory refers to the suggested matches that appear when you type text in the Address bar, the Run dialog box, or forms in Web pages. Hackers can use this information to monitor your surfing habits. When you select this check box, Privacy Control clears all this information from the computer.
    - **Clear Last Run Menu:** When you select this check box, Privacy Control clears this information in the Run dialog box.
    - **Clear Temporary Folders:** When you select this check box, Privacy Control clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive of the computer and boosts the performance of the computer.
    - **Clear Last Find Computer:** When you select this check box, Privacy Control clears name of the computer for which you searched last.
    - **Clear Browser Address Bar History:** When you select this check box, Privacy Control clears Web sites from the browser's address bar history.
    - **Clear Last Search Menu:** When you select this check box, Privacy Control clears name of the objects that you last searched for by using the Search Menu.
    - **Clear Recent Documents:** When you select this check box, Privacy Control clears names of the objects found in Recent Documents.
    - **Clear Files & Folders:** When you select this check box, Privacy Control deletes selected Files and Folders. You should use this option with caution because it permanently deletes mentioned files and folders from the computer.
    - **Clear Open/Save Dialog Box History:** When you select this check box, Privacy Control clears the links of all the opened and saved files.
    - **Empty Recycle Bin:** When you select this check box, Privacy Control clears the Recycle Bin. You should use this option with caution because it permanently clears the recycle bin.
    - **Clear Cache:** When you select this check box, Privacy Control clears the Temporary Internet Files.
    - **Clear Cookies:** When you select this check box, Privacy Control clears the Cookies stored by Web sites in the browser's cache.
    - **Clear Plugins:** When you select this check box, Privacy Control removes the browser plug-in.
    - **Clear ActiveX:** When you select this check box, Privacy Control clears the ActiveX controls.
    - **Clear History:** When you select this check box, Privacy Control clears the history of all the Web sites that you have visited.

In addition to these options, the **Auto Erase Options** section has two buttons:

- **Select All:** You can click this button to select all the auto erase options.
- **Unselect All:** You can click this button to clear all the selected auto erase options. You can either schedule the auto erase tasks to run automatically or remove the traces manually.

- **Advanced**

This tab helps you to clear unwanted or sensitive information stored in the browser's cache under **MS Office**, **Windows**, **Others**, and **Internet Explorer** categories.

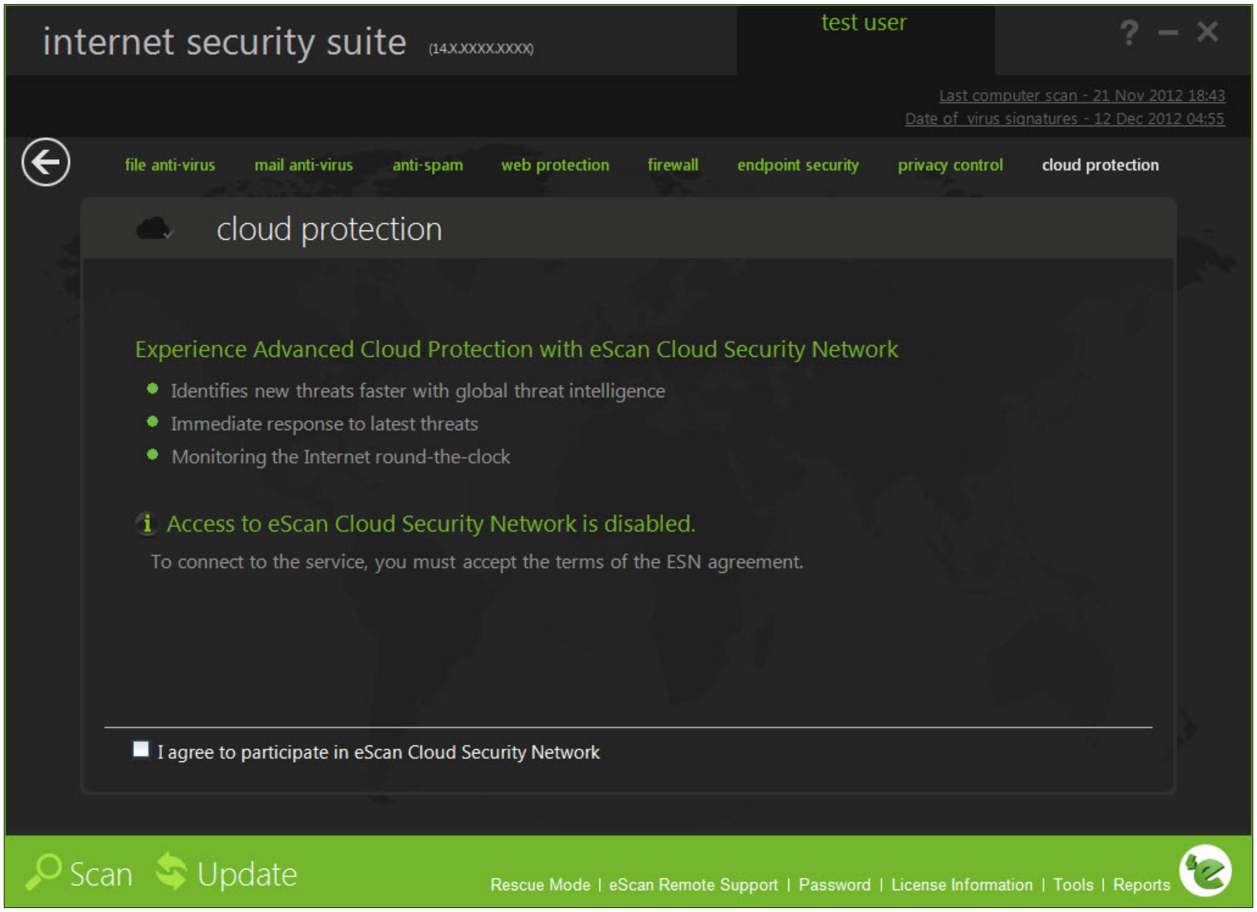
Cloud Protection

The cloud protection is the eight module of the eScan for ISS. 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. Refer Figure 79.

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.


internet security suite (14.X.XXXX.XXXX)
test user
?
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
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

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

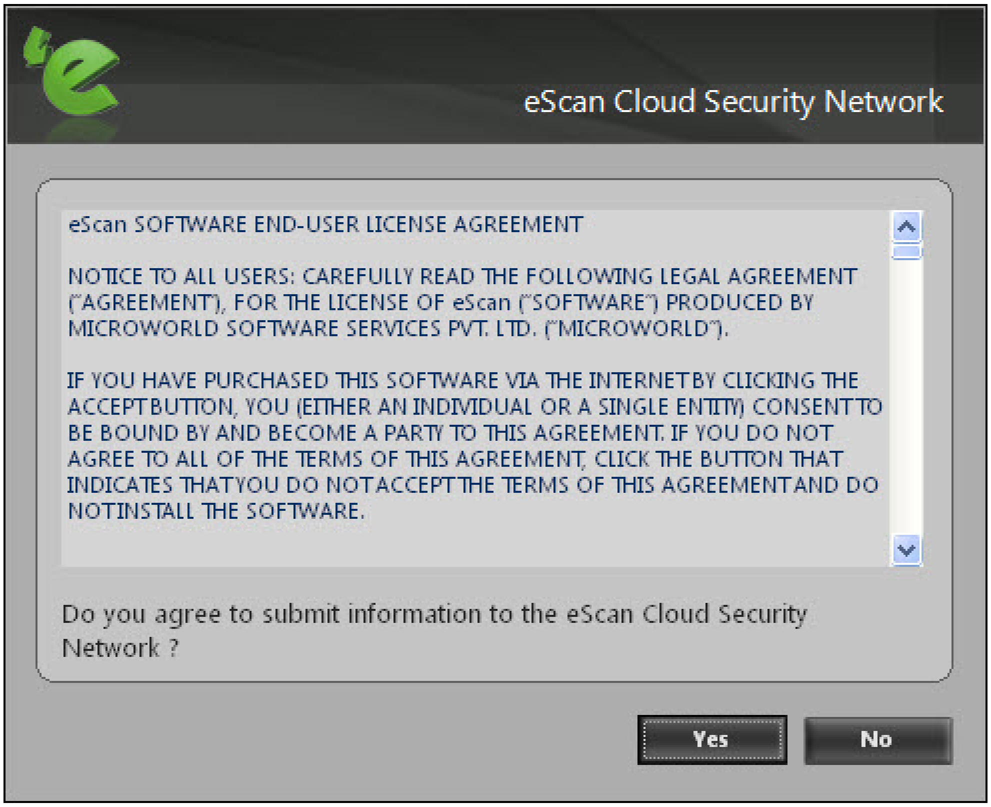
Figure 79

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. Refer Figure 80.



eScan SOFTWARE END-USER LICENSE AGREEMENT

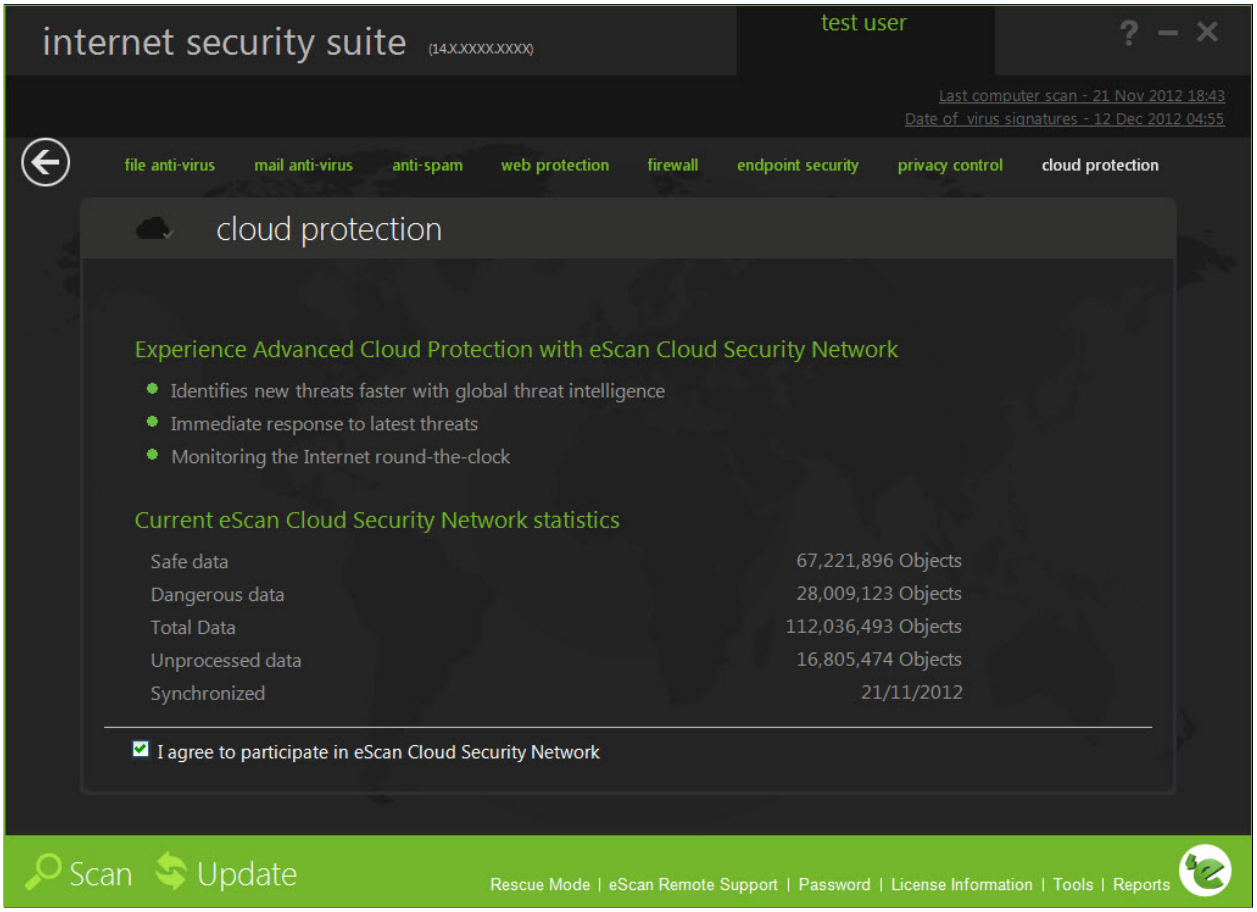
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF eScan ("SOFTWARE") PRODUCED BY MICROWORLD SOFTWARE SERVICES PVT. LTD. ("MICROWORLD").

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 80

2. Click the **Yes** button.
   The eScan Security Network starts functioning and displays the current eScan Security Network statistics. Refer Figure 81.


internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
cloud protection
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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	67,221,896 Objects
Dangerous data	28,009,123 Objects
Total Data	112,036,493 Objects
Unprocessed data	16,805,474 Objects
Synchronized	21/11/2012

☑ I agree to participate in eScan Cloud Security Network

Figure 81

Scan

The Scan module helps you perform on-demand scans on files, folders, storage devices, and the registry and schedule automatic scans. It checks your computer for security threats, such as viruses, spyware, and other malicious software and creates logs of all scan operations. Refer Figure 82.

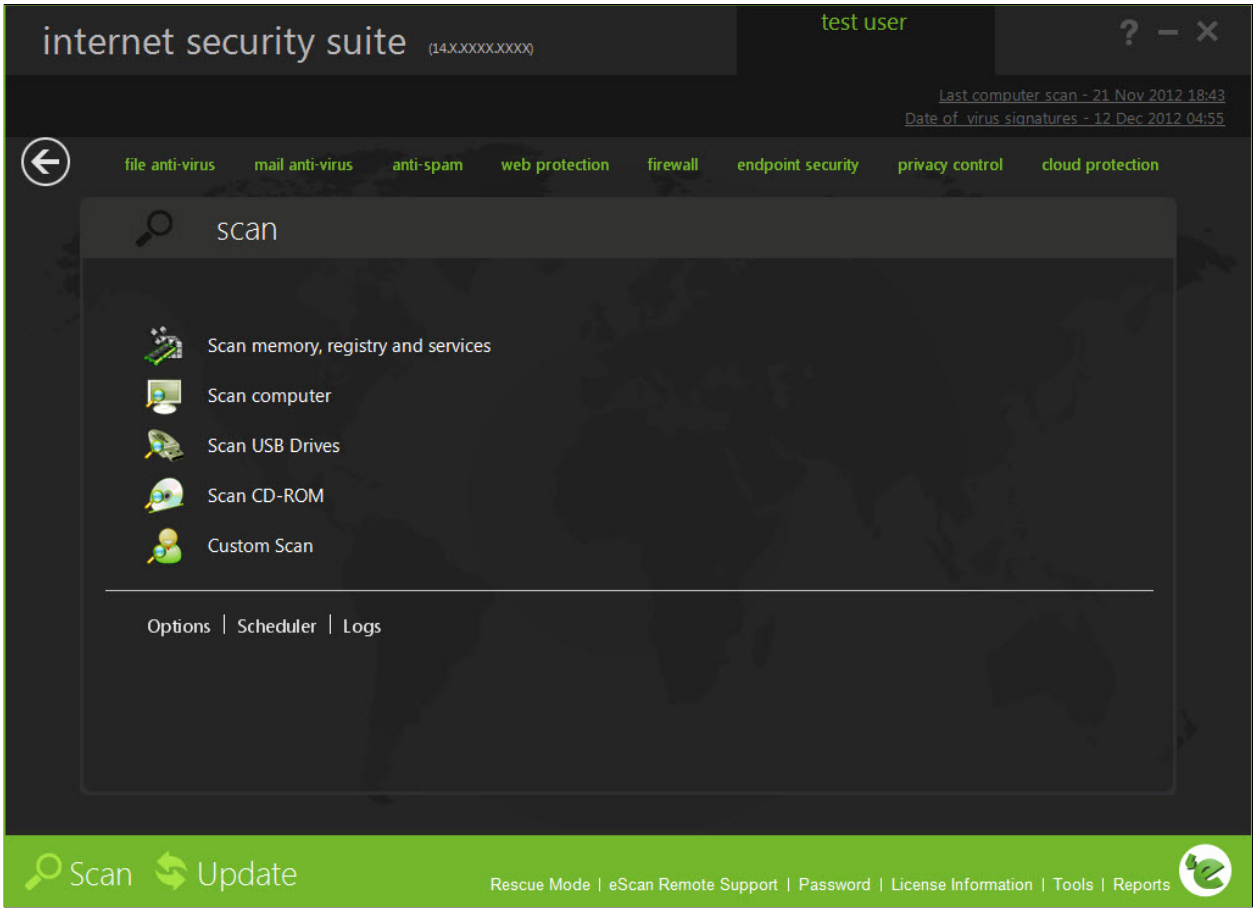
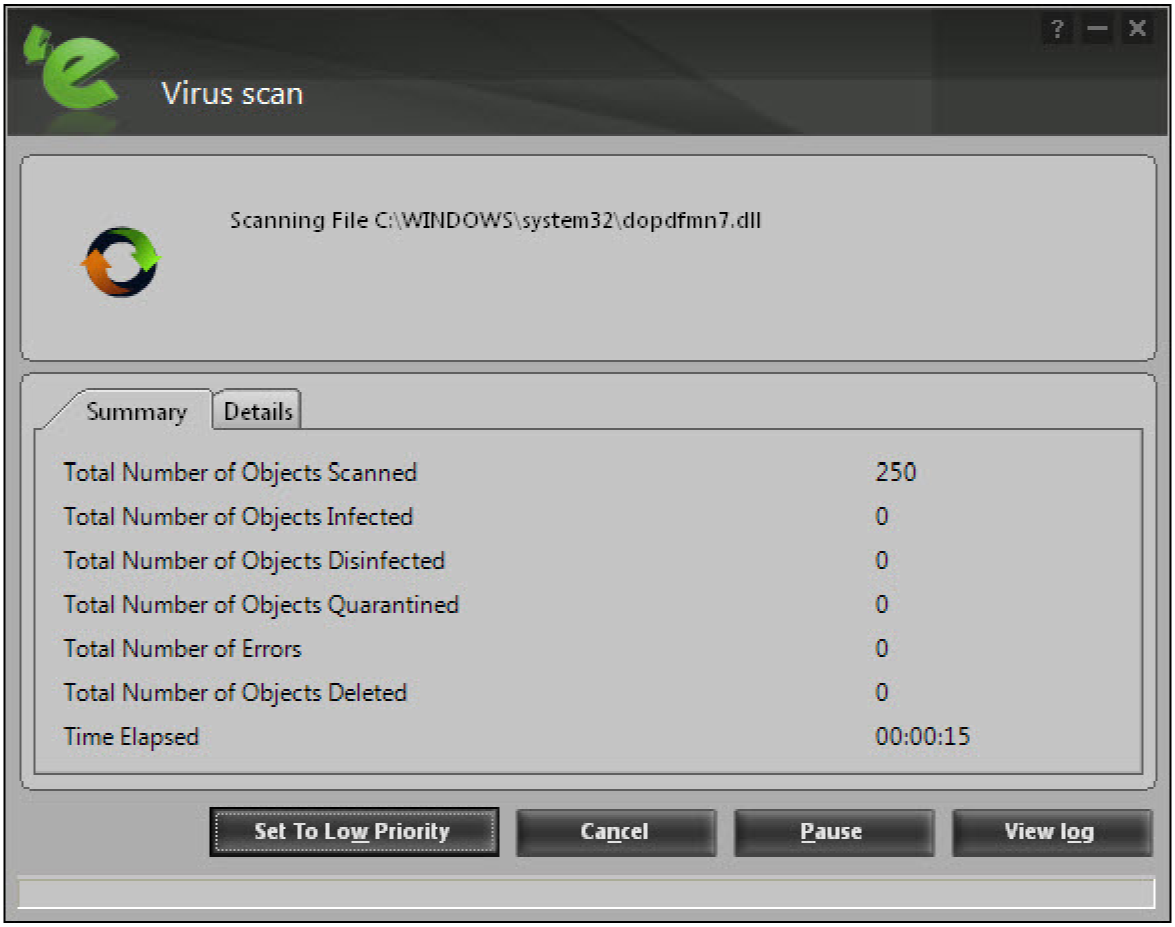

internet security suite (14.X.XXXX.XXXX)
test user
? – ✕
Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55
file anti-virus
mail anti-virus
anti-spam
web protection
firewall
endpoint security
privacy control
cloud protection
scan
Scan memory, registry and services
Scan 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 82

When you click the **Scan** button on the eScan for ISS, the **Scan** tabbed page is displayed. This page provides you with options for scanning the computer and peripheral storage devices, configuring the Scan module, 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 mode 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. Refer Figure 83.



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 83

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:

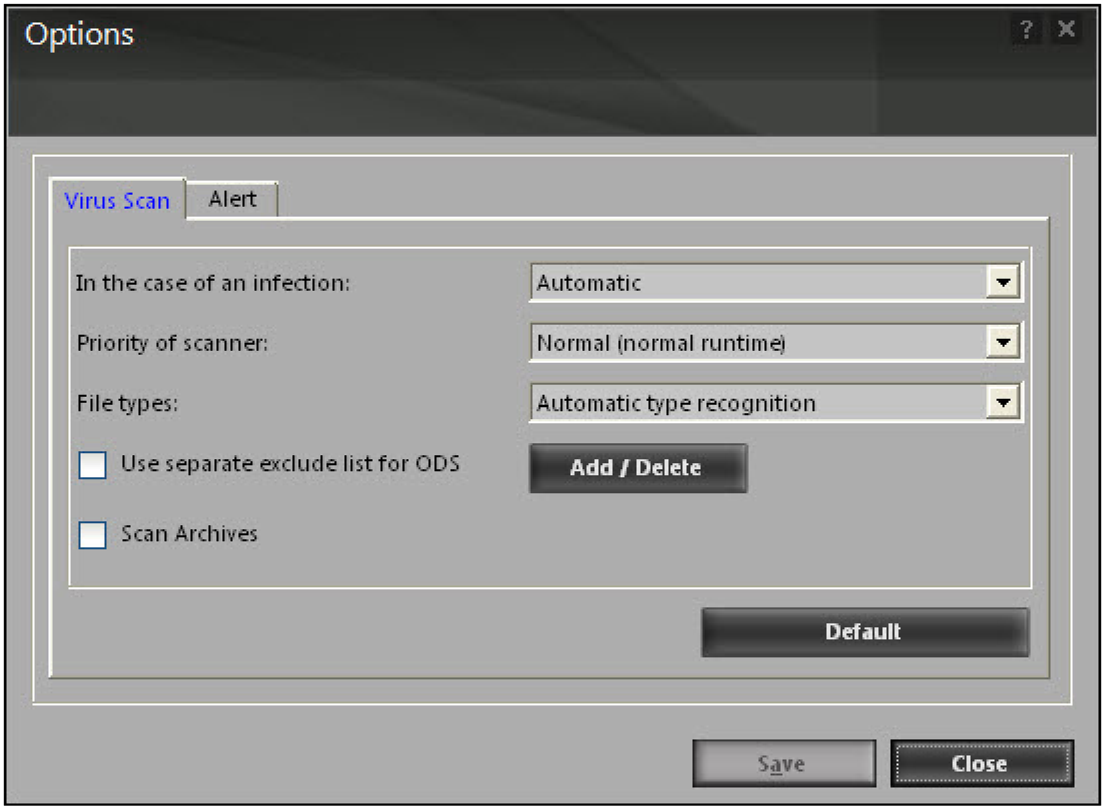
Options

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 module. 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. Refer Figure 84.



Options

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 84

- **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 executables stored on your computer.

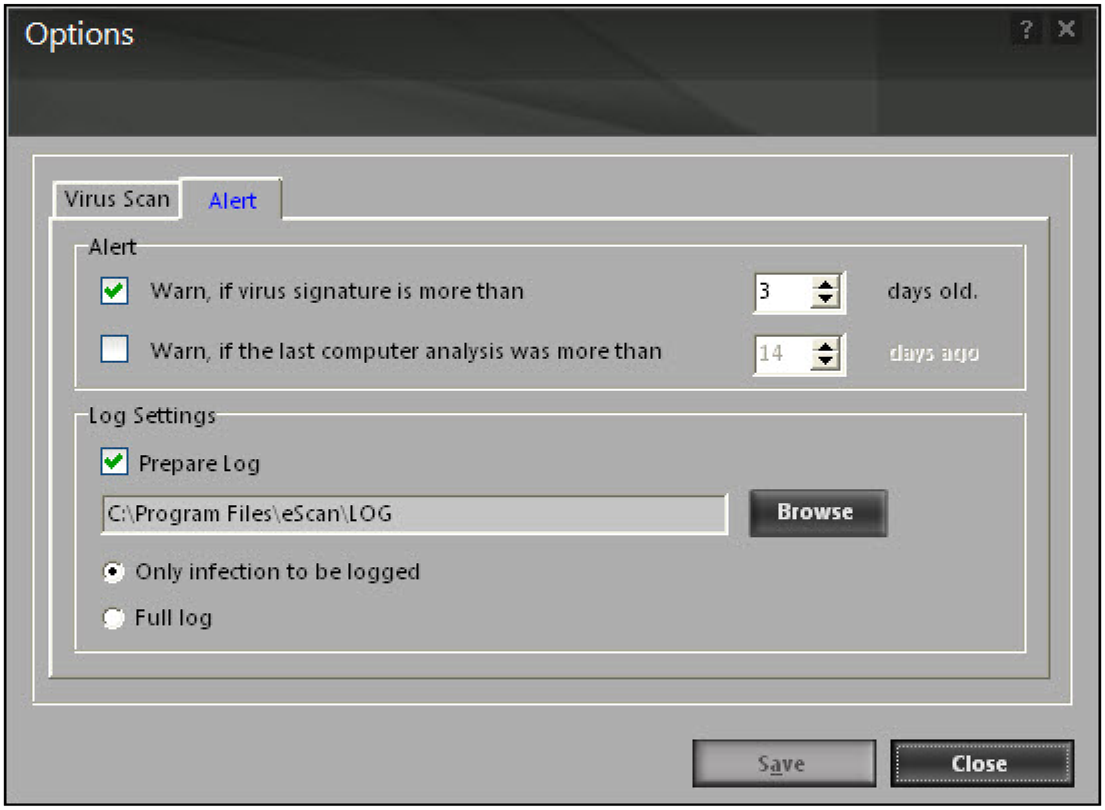
- **Use separate exclude list for ODS:** [Default] Select this check box, if you want eScan to exclude all the listed files, folders, and sub folders from monitoring during the on-demand scan.
  This option helps eScan to separate the exclude list of on-demand scanning from real-time scanning exclude 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. Refer Figure 85.



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

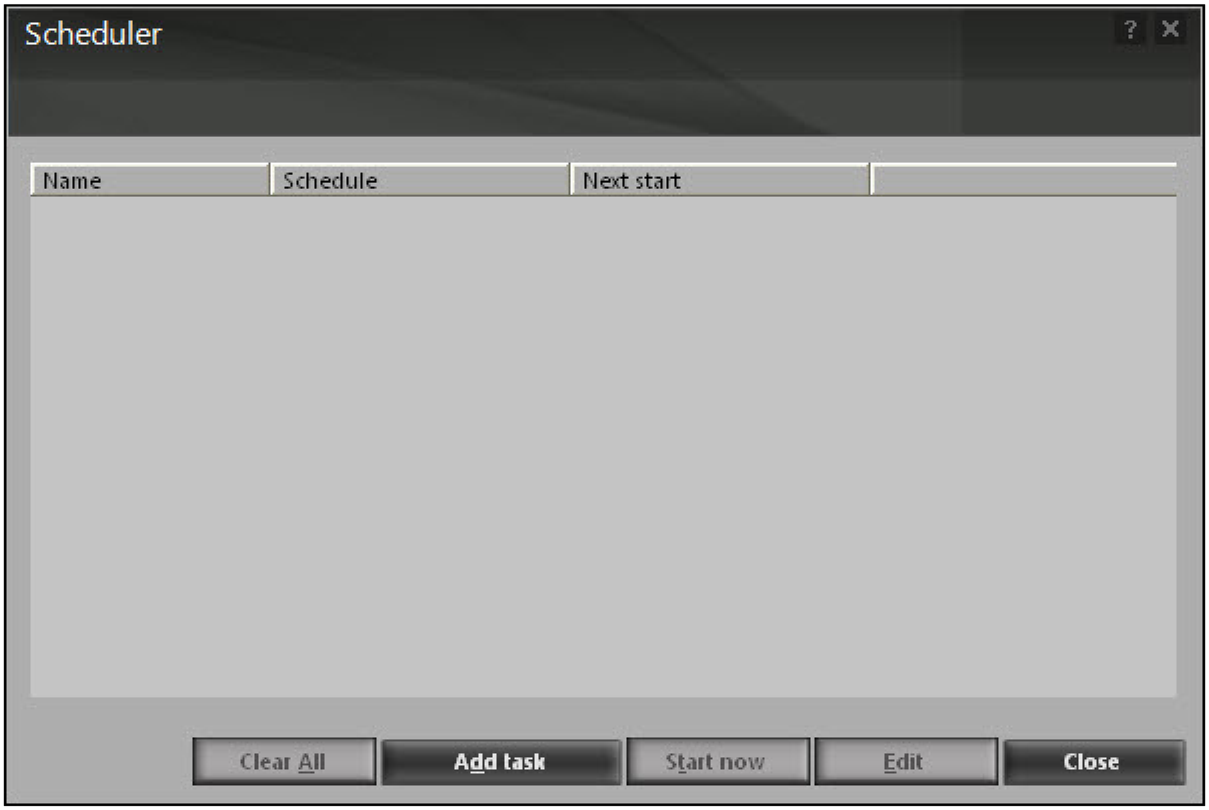
Figure 85

- **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 module.
  - **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. Refer Figure 86.



Scheduler

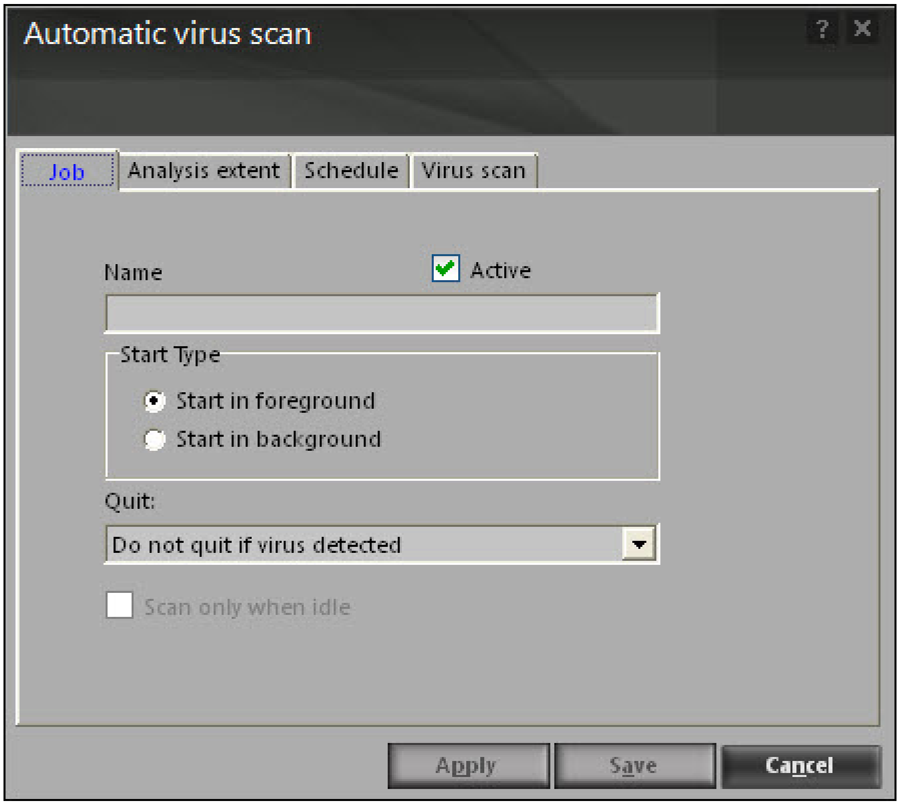
Name	Schedule	Next start

Figure 86

- **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. Refer Figure 87.



Automatic virus scan

Name ☑ Active

Start Type

● Start in foreground

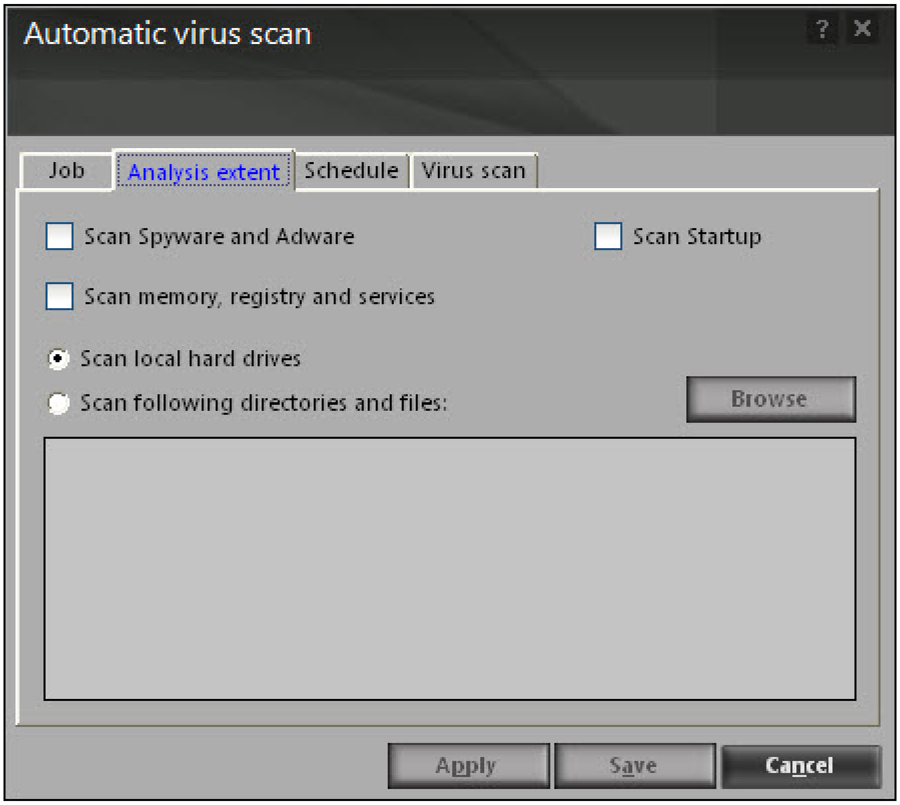
○ Start in background

Quit: Do not quit if virus detected

□ Scan only when idle

Figure 87

- **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. Refer Figure 88.



Automatic virus scan

Job | Analysis extent | Schedule | Virus scan

□ Scan Spyware and Adware

□ Scan Startup

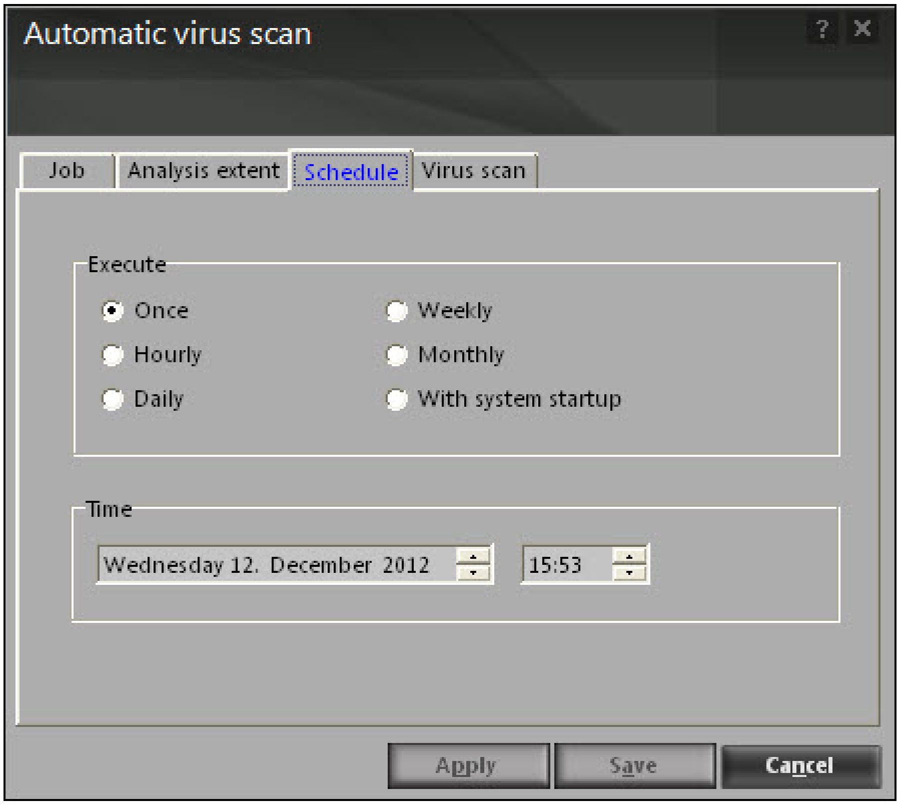
□ Scan memory, registry and services

● Scan local hard drives

○ Scan following directories and files:

Figure 88

- **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. Refer Figure 89.



Execute

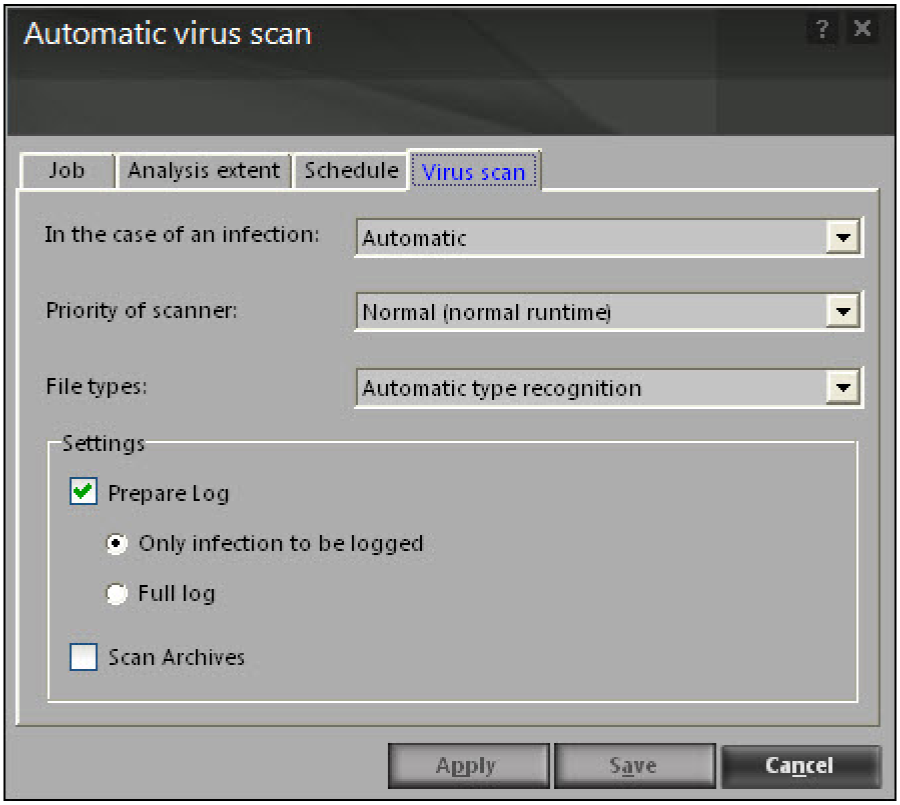
● Once ○ Weekly
○ Hourly ○ Monthly
○ Daily ○ With system startup

Time

Wednesday 12. December 2012 15:53

Figure 89

- **Virus scan:** This tab provides you with the same options as the ones present on the **Virus scan** tab of the Scan module. You can configure On-demand Scan to perform a specific action when a virus infection is detected. You can also set the priority of the eScan scanner in relation to other processes running on the computer. The priority level can be high, normal, or low. By default, the scanner runs with low priority. In addition, you can configure On-demand Scan to scan only program files or executable files. Refer Figure 90.



Automatic virus scan

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

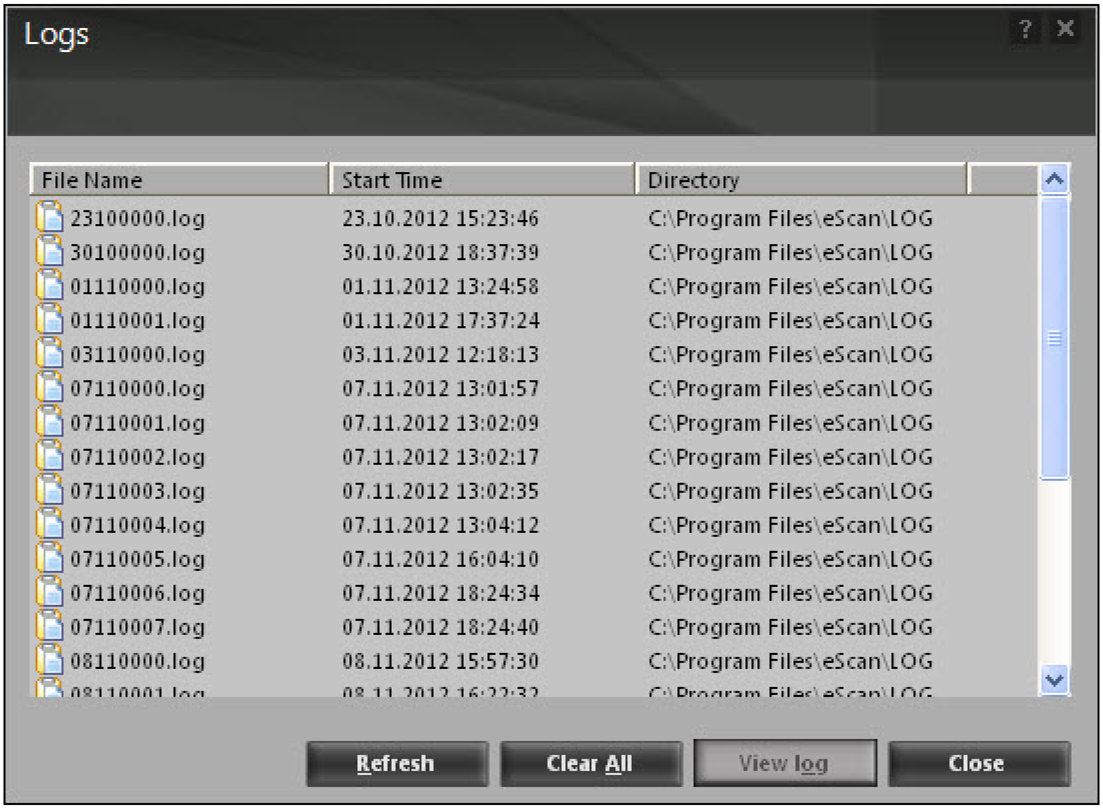
○ Full log

☐ Scan Archives

Figure 90

Logs:

You can view reports of the scheduled On-demand scans performed on your computer and storage devices in the **Logs** dialog box. Refer Figure 91.

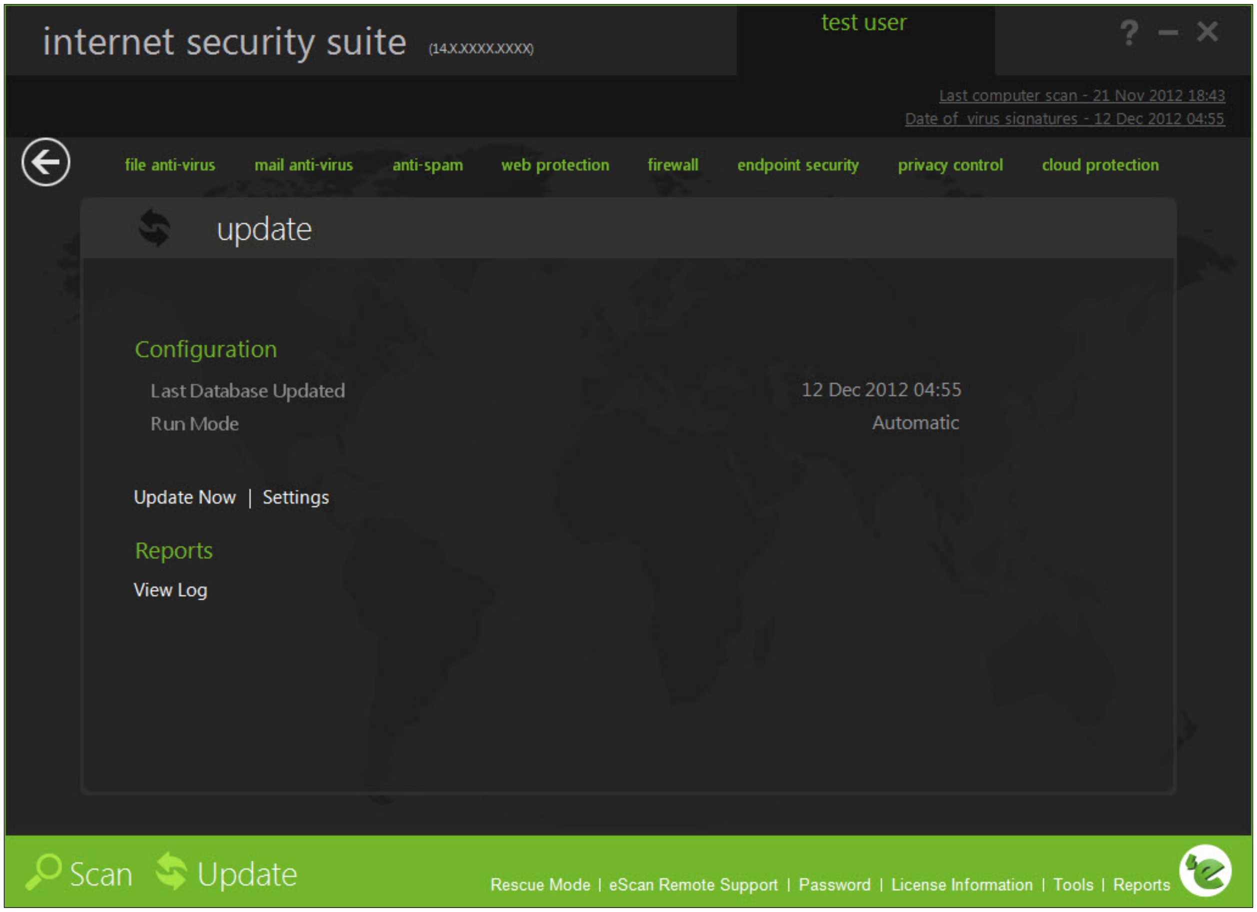


File Name	Start Time	Directory
23100000.log	23.10.2012 15:23:46	C:\Program Files\eScan\LOG
30100000.log	30.10.2012 18:37:39	C:\Program Files\eScan\LOG
01110000.log	01.11.2012 13:24:58	C:\Program Files\eScan\LOG
01110001.log	01.11.2012 17:37:24	C:\Program Files\eScan\LOG
03110000.log	03.11.2012 12:18:13	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 91

Update

The Update module automatically keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. You can configure eScan to download updates automatically either from eScan update servers or from local network by using FTP or HTTP. Figure 92.



internet security suite (14.X.XXXX.XXXX)

test user

Last computer scan - 21 Nov 2012 18:43
Date of virus signatures - 12 Dec 2012 04:55

update

Configuration

Last Database Updated	12 Dec 2012 04:55
Run Mode	Automatic

Reports

Figure 92

You can access tabbed page for the Update module from eScan for ISS 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 below:

- Configuration

This section displays the following information:

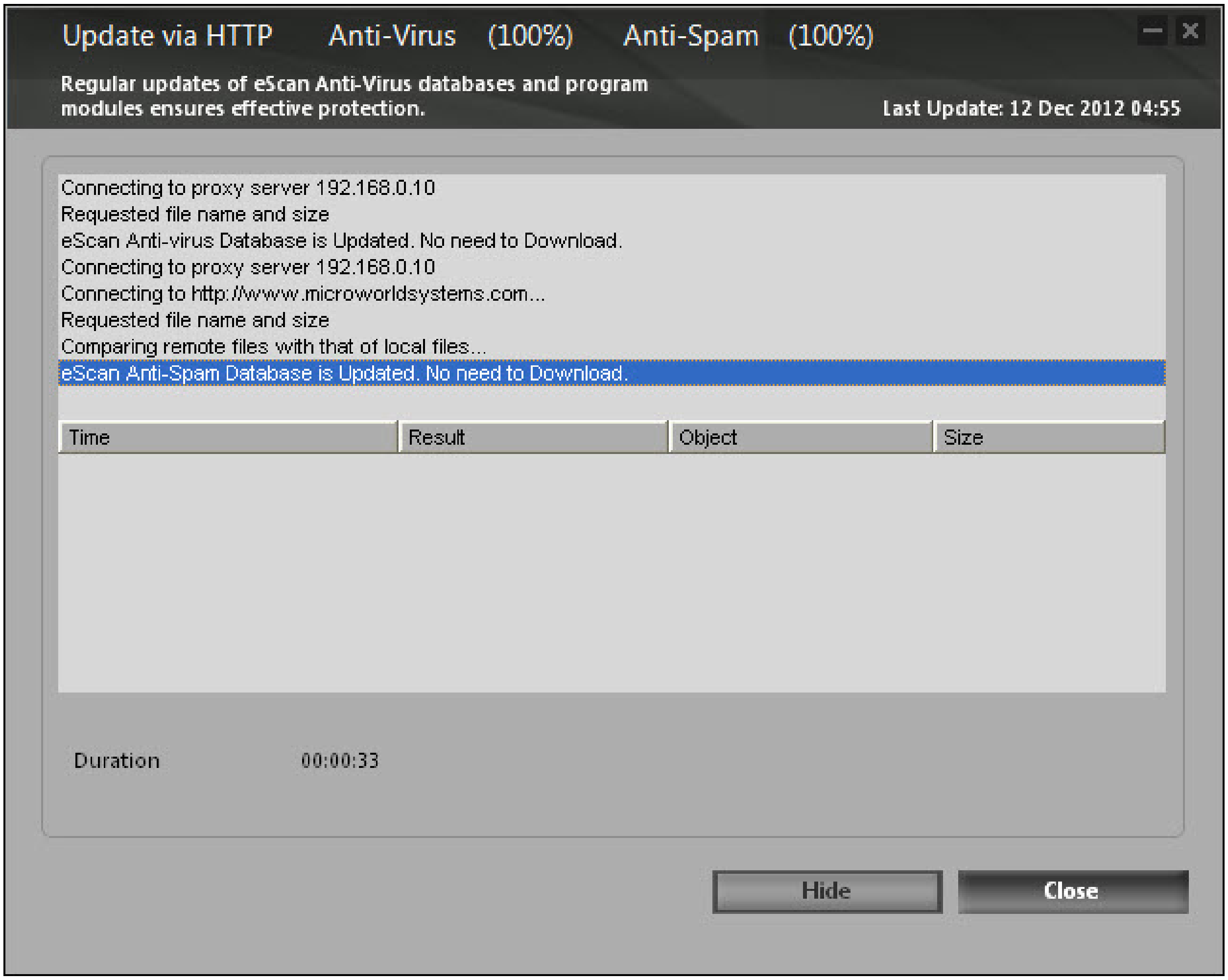
- **Last Database Updated:** It shows when the eScan database was last updated.

- **Run Mode:** It displays the type of update mode used by eScan. The run mode can be either Automatic or Scheduled.

Click on **View Logs** option present under **Reports** to view Update Logs of eScan ISS on your system.

Update Now:

You can click this button to update the Anti-Virus and Anti-Spam definitions through HTTP or FTP.


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.
```

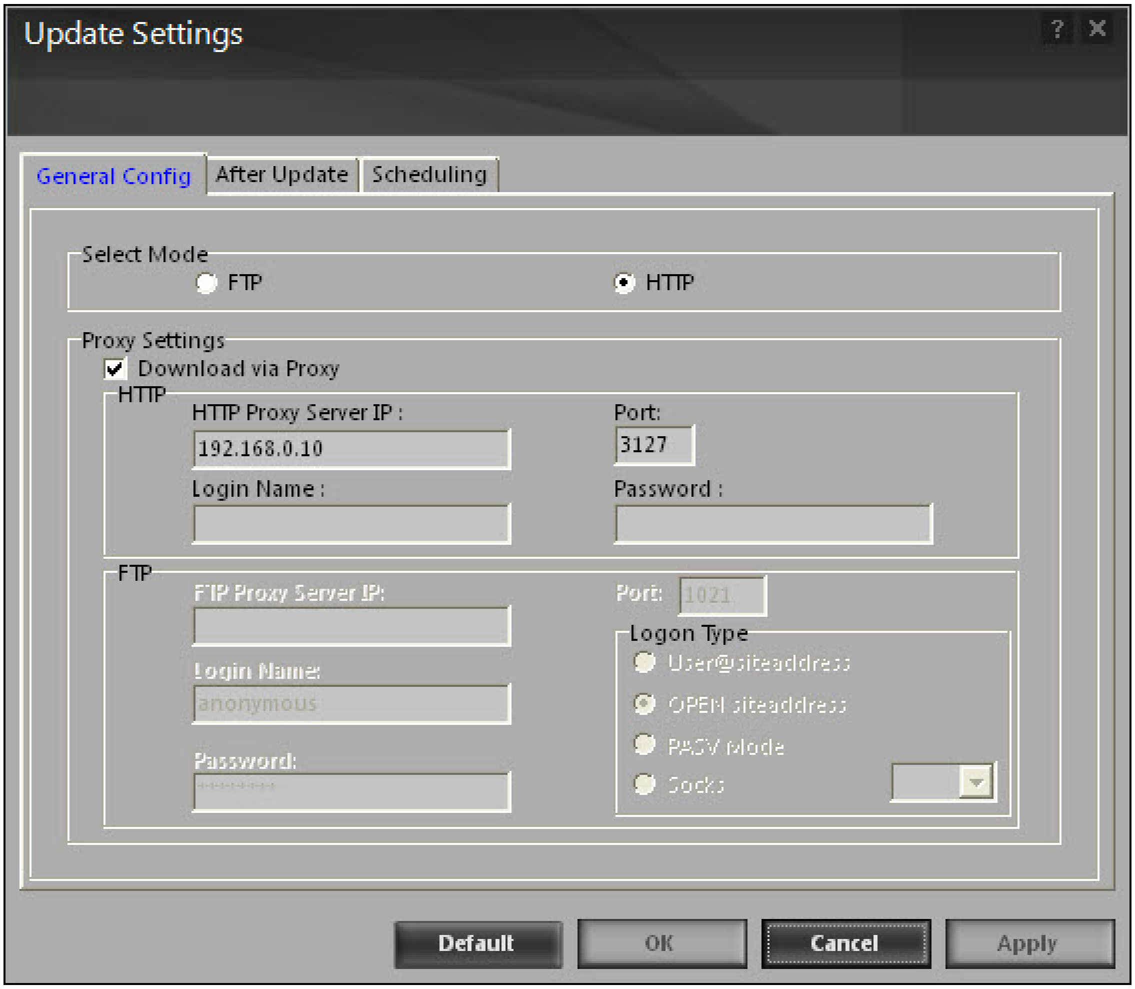
Figure 93

Settings:

You can click this button to open the **Update Settings** dialog box, which helps you configure the Update module to download updates automatically. This dialog box has the following tabs.

- **General Config**

This tab provides you with general options for configuring the Update module. Refer Figure 94.



Select Mode
○ FTP ● HTTP

Proxy Settings
☑ Download via Proxy

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

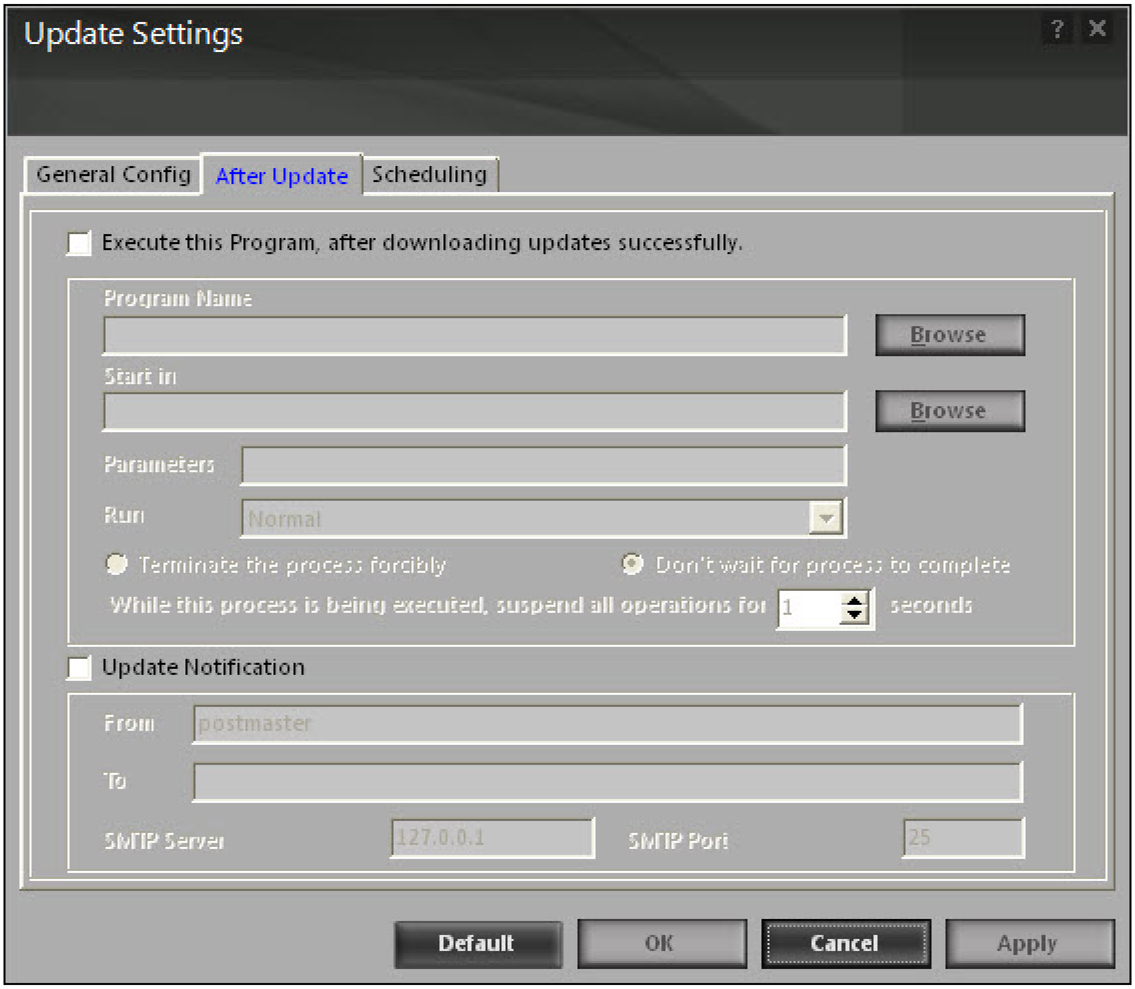
FTP
FTP Proxy Server IP:
Port: 1021
Login Name: anonymous
Password: ********
Logon Type
○ User@siteaddress
● OPEN siteaddress
○ PASV Mode
○ Socks

Figure 94

- **Select Mode:** It indicates the mode for downloading updates from eScan update servers. The available modes are **FTP** and HTTP. 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. Refer Figure 95.



□ 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 95

- **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.

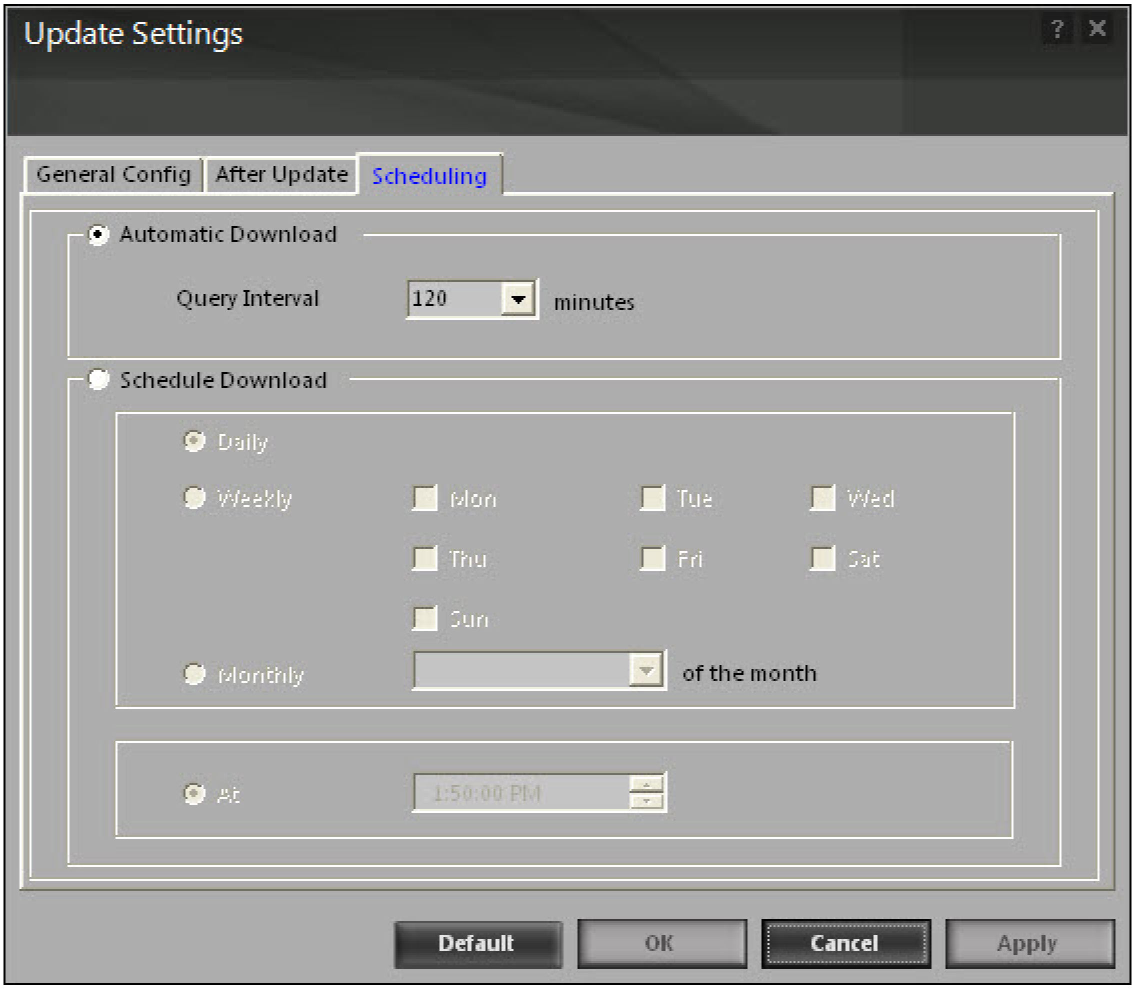
- **Start In:** You can also specify the program to execute from a given location. You can either specify the location in the **Start In** box or use the **Browse** button to navigate to the folder where the program should execute.
- **Parameters:** Some programs require additional parameters to execute. 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. Refer Figure 96.



● 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 96

- **Automatic Download:** [Default] You can configure the Update module 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.

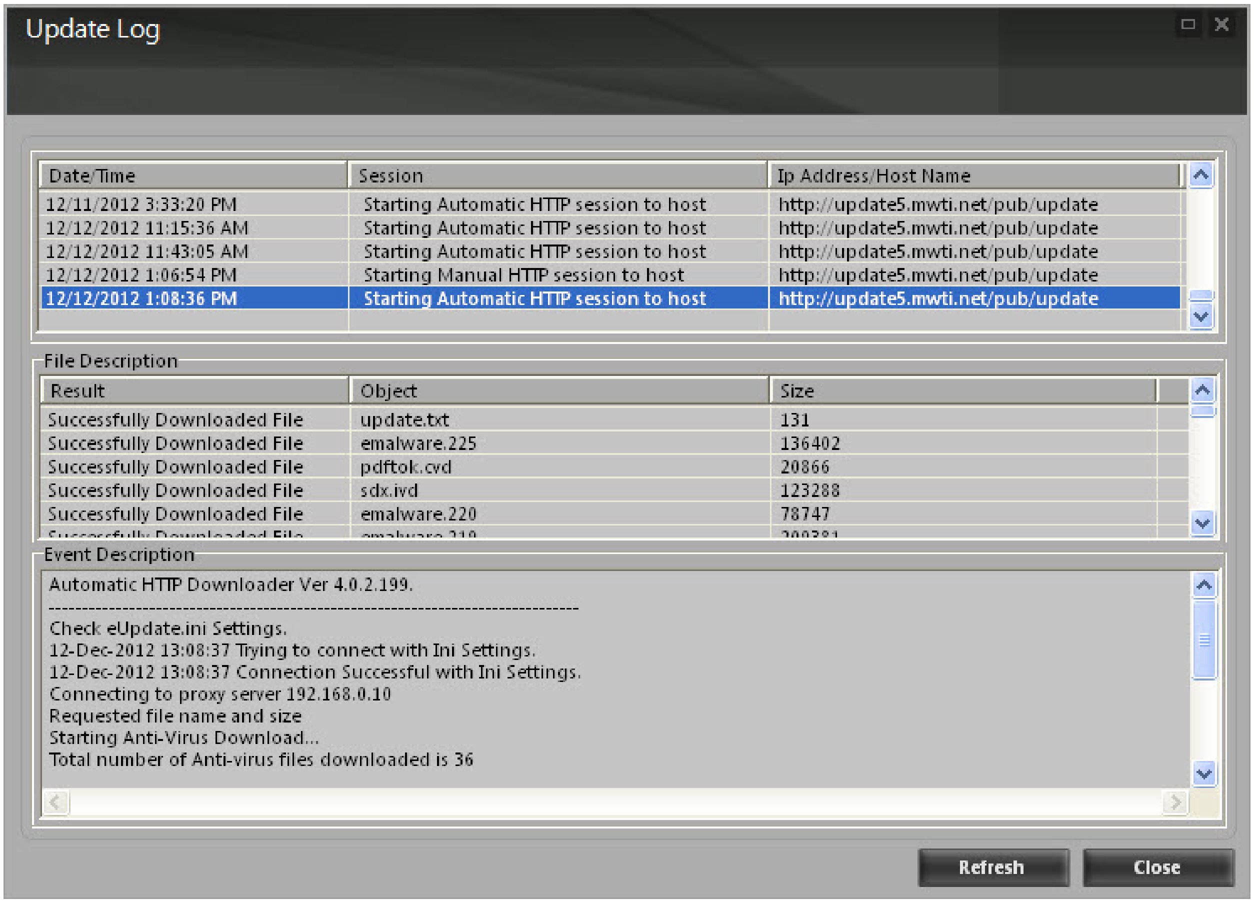
  Type or select the time at which you want eScan to download updates, by clicking the ▴▾

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.

- 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 module. Refer Figure 97.



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 97

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 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 Contacts and URLS

- 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
Fax: (91) (22) 2830-4750
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 or (603) 2333-8910
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, Randburg, Gauteng, South Africa
Tel : Local 08610 eScan (37226)
Fax: (086) 502 0482
International : (27) (11) 781-4235
E-mail : sales@microworld.co.za
Web site: http://www.microworld.co.za

USA

MicroWorld Technologies Inc.

31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334
USA

Tel : +1 248 855 2020 / +1 248 855 2021

Fax: +1 248 855 2024

E-mail : sales@escanav.com

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

Germany

MicroWorld Technologies GmbH

Drosselweg 1,
76327 Pfinztal,
Germany.

Tel : +49 7240 944909 20

Fax: +49 7240 944909 92 E-mail : sales@escanav.de

Web site: http://www.escanav.de

Mexico

Manzana 3, SuperManzana 505, Lote 13,
Fraccionamiento Pehaltun, C.P. 77533,
Cancun, Quintana Roo,
Mexico.

Tel: 52 998 9893157

Email: ventas-la@escanav.com

Website: http://www.escanav.com.mxm