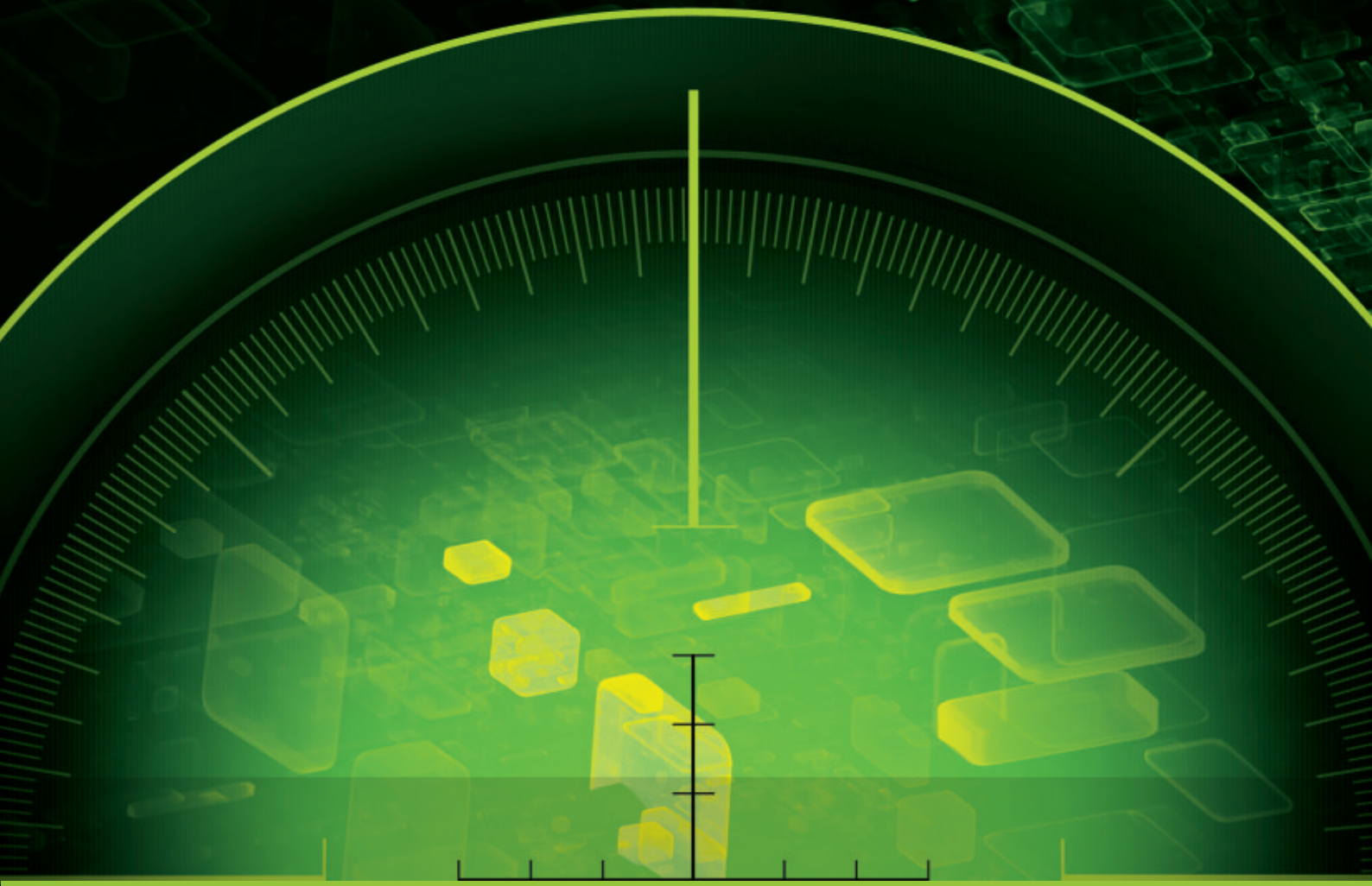
eScan™

Anti-Virus & Content Security

eScan Total Security Suite
User Guide



www.escanav.com sales@escanav.com

Table of Contents

Welcome

MicroWorld's **eScan 14** is an 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 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

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

Document Number: 5BUG/02.05.2014/14.1

Current Software Version: 14.1

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: December, 2015

eScan Total Security Suite

eScan Total Security Suite with Cloud Security offers protection from computer viruses and also provides security from evolving cyber-threats such as Adware, Spyware, Trojans, Spam and Phishing. It provides complete security solution by improving your PC performance, protecting your children online, and keeping your important data and privacy safe.

Pre-Requisites

Pre- requisites for installing eScan

Please check the following pre-requisites before installing eScan Total Security Suite on your system.

First Time Installation

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

Renewal and Upgrade

- ***Renewal*** **–**You need to have a License Key for Renewing eScan, you can purchase the license key from any dealer nearby your place or you can purchase online from eScan at www.escanav.com.

- ***Upgrade*** **–** If a newer version is available, eScan can be upgraded by downloading and installing eScan from our website.

System Requirements

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

Operating System

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

Note:
eScan 14 SOHO products do not support Server Operating systems.

Minimum Hardware Requirements

CPU: 1 GHz recommended

Memory (RAM): 1 GB recommended

Disk Space: 1 GB Recommended

CPU: 1 GHz recommended

Installing eScan

Installing eScan from CD/DVD

Installing Total Security Suite from the CD/DVD is very simple, just insert the CD/DVD in the ROM and wait for few seconds for auto run to start the installation process and follow the instructions on screen. In case if installation does not start on its own, click **Install** option on the CD ROM, this will open the one click installation wizard setup of Total Security Suite on your computer.

Downloading and installing Total Security Suite from the internet

You can also download the setup file from **www.escanav.com**

For installing Total Security Suite from the setup file downloaded from Internet, just double click on the Twnxxxxxx.exe and follow the instructions on screen to complete the installation process.

Note:
· Click the QRG link present on the eScan TSS installation screen to view a Quick Reference Guide for using eScan Total Security Suite.
· In case, if Auto run is disabled on your system, use windows explorer and run the EXE (Twnxxxxx.exe) present in eScan folder on the Installation Disk and follow the instructions on screen.

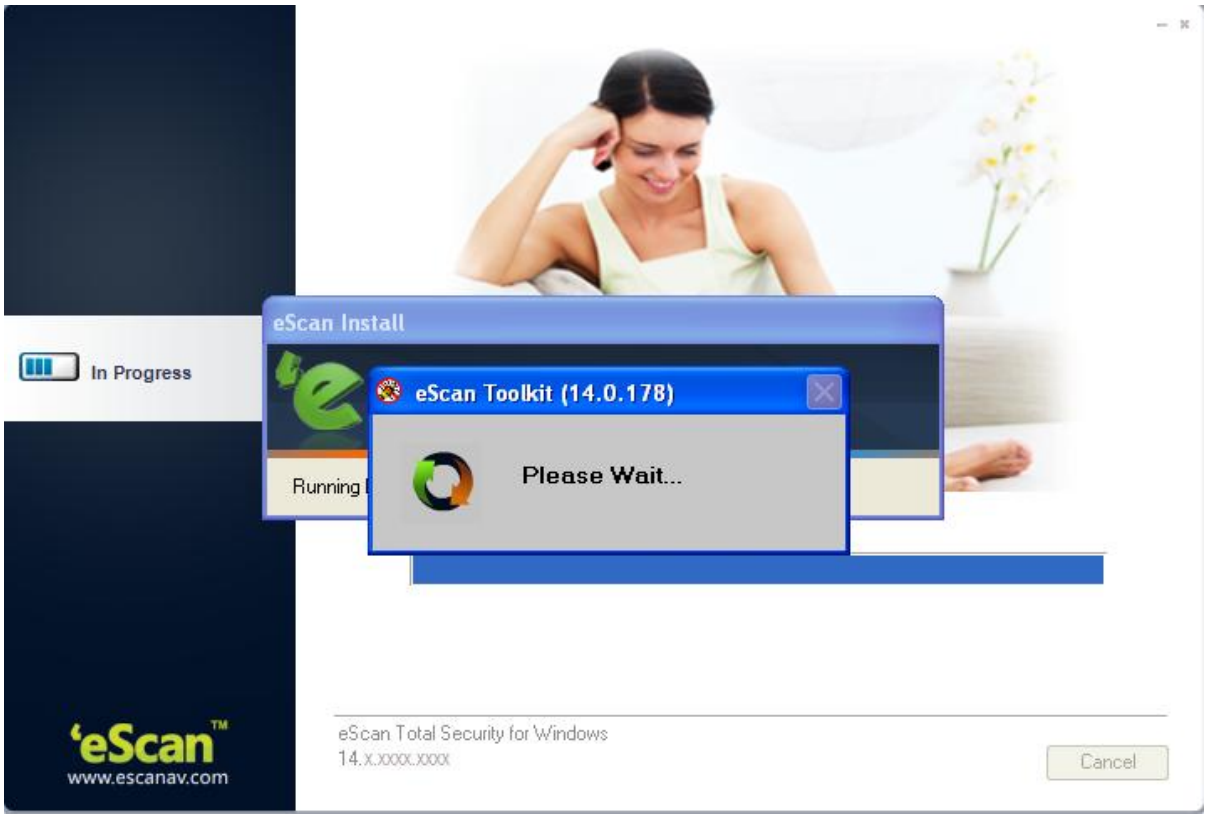
Special Instruction for Windows Vista Users with User Access Control (UAC) enabled on them –

Double click on setup file for installing eScan TSS. A **User Access Control** dialog box appears asking you for permission to run Twn2[xxxx].tmp file. This is a valid eScan file, to proceed with the installation, click **Continue.**

Installation Process

eScan uses the auto- installation wizard that facilitates installation in just one step. Please uninstall any other anti-virus software from your system before installing eScan.

Click the setup file and the installation process will start by itself.



Note:
1. *If there are no conflicting programs, the wizard proceeds with the installation.*
2. *The eScan setup also runs eScan Anti-Virus Toolkit. This tool scans and removes the viruses and spyware found on your computer. It is recommended that you run this toolkit to remove any malware from your system and keep your system clean.*
3. *The default path for 32-bit operating system: [Disk Drive]\Program Files\eScan.*
4. *The default path for 64-bit operating system: [Disk Drive]\Program Files (x86)\eScan.*
5. *It is recommended to **Restart** the System to apply the settings for eScan Total Security.*
6. *Installation CD can also be used as a Rescue Disk when you are unable to boot your system in Normal mode. To use the installation CD a Rescue Disk, insert the CD at the time of booting and boot the system using eScan Rescue Mode.*
7. *eScan Web Safe is automatically installed along with eScan Total Security Suite. This helps in identifying the websites you can trust for safe surfing and shopping based on the experience of millions of users across the world.*
8. *It is recommended to reboot the system after the completion of installation.*

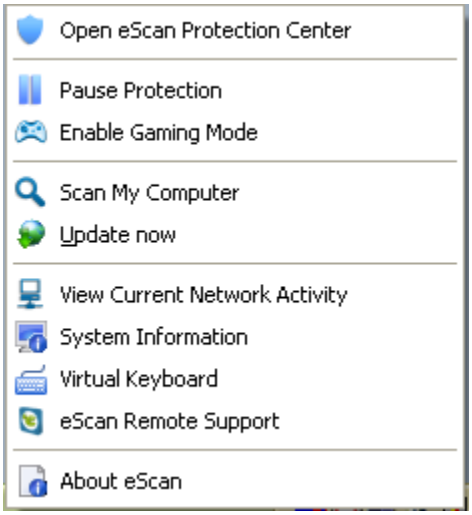
Verifying the Installation

Check for a **Red Shield Icon** in the System Tray. It indicates the protection status of the computer.

Option	Description
	It indicates that the eScan's real-time protection is active.
	It indicates that the eScan's real-time protection is either paused or disabled.

User Interface

All major functions can be performed using the options present on the **Right Click** Menu of **eScan Red Shield** (System tray).



Sr. No.	Option	Description
1.	Open eScan Protection Center	Click this option to open main window of eScan Total Security Suite.
2.	Pause Protection	Click this option to Pause Protection for a specific time period. It is recommended to not use this option more frequently.
3.	Resume Protection	This option will be displayed only if the protection has been disabled on the system. Click this option to resume the protection of your system.
4.	Enable Gaming Mode	On enabling this option you will not receive any pop ups or notification while your game or any application is running in full screen.
5.	Scan My Computer	Click this option to initiate the scanning of the computer instantly.
6.	Update Now	Click this option to download and install latest Updates from our Update Server. It is mandatory to have an active internet connection to download the latest updates.
7.	View Current Network Activity	Click this option to View the list of applications installed on your system that are communicating actively on the internet.
8.	System Information	Click this option to view detailed System Information of your Computer.

9.	Virtual Keyboard	Click this option to use Virtual Keyboard; this can be used to reduce key logging.
10.	eScan Remote Support	Click this option to get Remote Help from our Support Center, the Technical Support Executive will take control of your system for resolving the issue; this requires internet connection.
11.	About eScan	Click this option to view information about eScan version installed on your system.

System Tray Menu

User Interface of eScan

The User Interface of eScan is logically designed and gives you an easy access to all the features and modules of the software. eScan opens with a Dashboard interface that gives you easy access to all the modules as well as informs you about the product, version number, real-time protection status, last date when the computer was scanned, date of virus signature update, and quick access links.

eScan Dashboard

- **File Antivirus** - This module provides real-time protection to the files and folders existing on your computer.

- **Mail Antivirus -** This module prevents infected emails and attachments from reaching your inbox, and thus protects your computer from malicious programs that propagate through emails.
- **Anti – Spam** - This module helps you filter emails based on keywords and phrases that appear within e-mails. This filter can be created and configured as per your requirement.
- **Web Protection -** This module helps you prevent offensive or pornographic content from appearing within a web browser.
- **Firewall -** This module helps you apply various rules for blocking specific ports, programs, or services on your computer.
- **Endpoint Security -** This module helps you to protect your computer from infected devices such as USBs, SD cards, Web cams, and CD/DVD ROMs' and it will also allow you to control the access to various applications by blocking or whitelisting.
- **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.

  Click the individual modules present on the interface to view status or configure settings for the respective modules.

Note:
The modules that are started will be green on the interface and will also indicate as started under the module name. The modules that are stopped will appear in red on the interface and will also display as stopped under the module name.

Quick Access Links

1. Quick Access Links are present at the bottom of the eScan interface providing you with various options to work smooth and fast with eScan.
2. Please go through the following table for a brief functional overview on options present in the Quick Access Links.

License Management

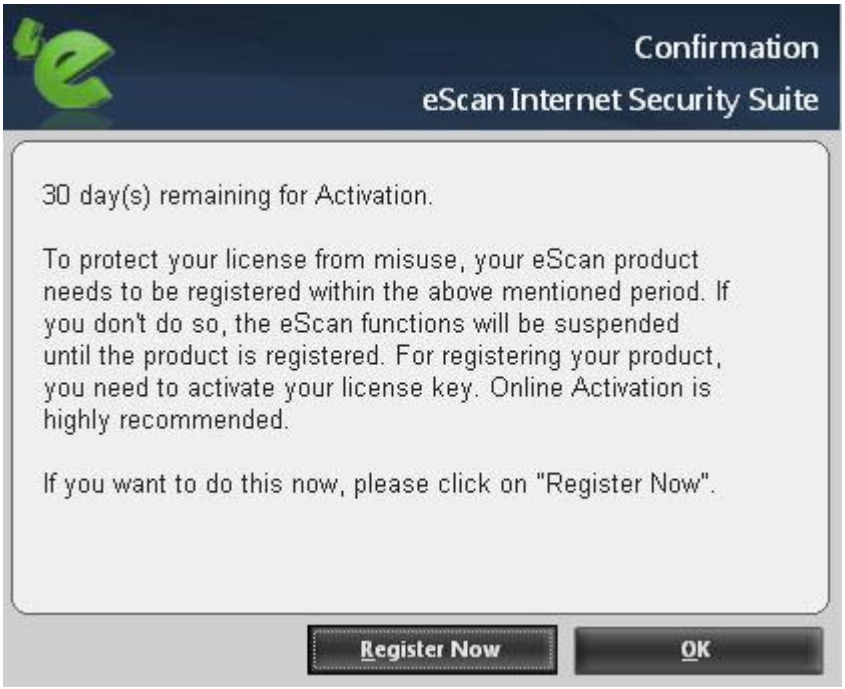
eScan comes with a pre-activated evaluation period of one month; you can activate the License for one year using the License key that you received with the CD or if you have downloaded the .exe file from internet. You can also purchase the License Key on clicking the buy now option present in the license information window.

Option	Description
Scan	Click this option to manually start scanning of Drives, ROM, Boot Sector, Registry and Services, as desired. Using this section you can schedule scanning as well as view Logs of earlier scans whenever desired. For more details **click here.**
Update	Click this option to Update eScan with the latest virus signatures available on our update servers. Using this section, you can schedule next update or view logs for previous updates installed on your system. You can also configure Update settings, as desired. For more details **click here**.
Rescue Mode	Use this option to restart your system in Rescue Mode; it is beneficial to boot your system in Rescue Mode when the Antivirus is not able to clean the infection. eScan will disinfect the system in rescue Mode. For more details **click here**.
eScan Remote Support	Click this option for troubleshooting and product assistance. It allows the eScan technical support representative to remotely take control and troubleshoot eScan related issues on your computer. For more details **click here**.
Password	Set the Administrator password for accessing eScan and its various modules. System Users can configure or change Module Settings for eScan only if they have Administrator password. For more details **click here**.
License Information	Click this option to View/ Enter /Buy Registration Key for eScan after expiry of Trial Version (1 Month after installation). You can Register eScan during trial period also. For more details **click here**.
Tools	Click this option to Create eScan Rescue ISO Image File, Download Latest Hotfix (eScan), Download Latest Hotfix (Microsoft Windows OS), Send Debug Information, Restore Windows Default Settings, Upload Samples, and USB Vaccination. For more details **click here**.
Reports	Click this option to Generate Reports for desired Modules between specific dates. For more details **click here**.

Online Activation

Steps for Activating the License Key through Online Registration –

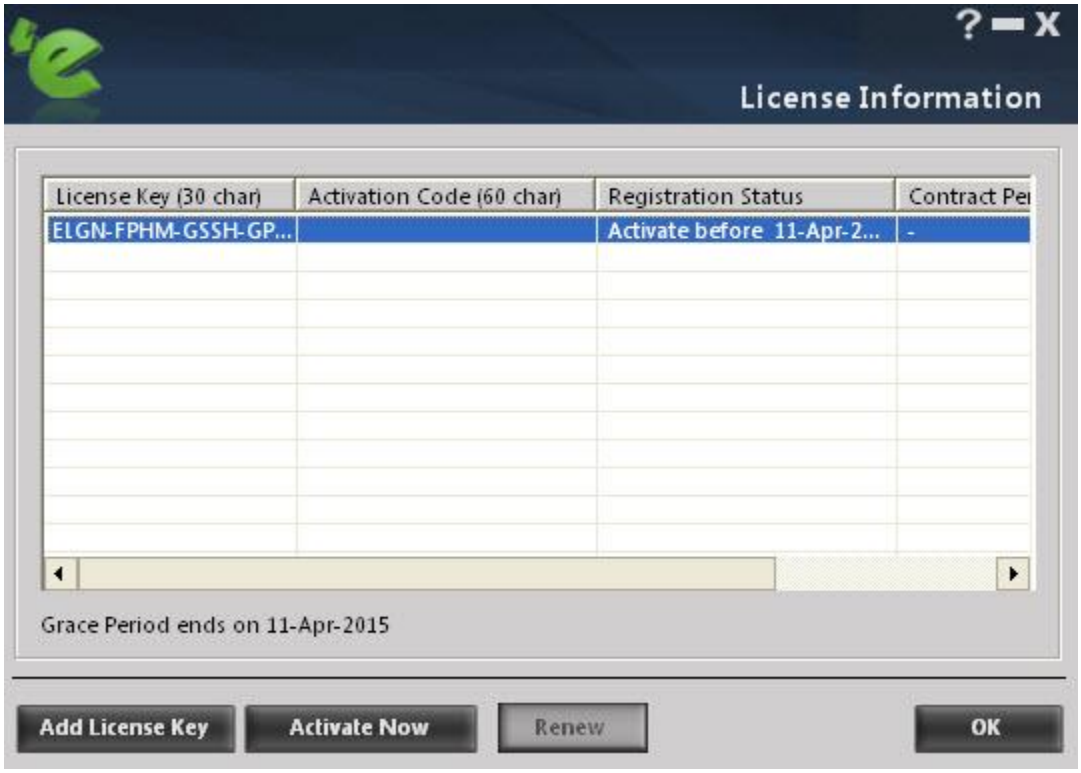
1. Open eScan.
2. Click the **License Information** link present in **Quick Access Links** at the bottom of eScan Interface.
3. Enter the 30 digit License key in the space provided on the interface and click **Apply**. A popup message will appear displaying the number of days remaining to register the license.



Note:
· The license key should be entered without any space in between the characters, for example: ABCD-EFGH-ABCD-EFGH-ABCD-EFGH-ABCD-EF.
· Apply button will be activated only after entering the key.

4. Click **Register Now** to proceed with the registration. The key will be Added to the License Information window.

5. Select the Key and click **Activate Now**, this will forward you to the online activation window.



6. For first time registration, select the option "**I want to activate online**" and fill up all the details.

7. Click **Activate** at the bottom of the Window.

8. eScan will be activated for the purchased duration and the date of expiry will be informed to you on a pop up message.

Note:
· If you type an invalid key, a warning message appears after verification from our database "Key not present in our database".
· "I want to activate online" option requires internet connection at the time of activation.

Offline Activation

Follow these steps for offline activation

1. Open eScan.

2. Click the **License Information** link present in Quick Links at the bottom of eScan Interface.

3. Enter the 30 digit License key in the space provided on the interface and click Apply. This will forward you to the **Online Activation** window. Select I want to activate online and fill in the details.

4. Click Activate, your online activation will fail as you are offline and No key will be generated for activating eScan on your machine. You will get the message as in below Figure

5. Click No, eScan will generate a text file (OnlineRegister.txt) with your personal details.

6. For getting the activation key and activating your product, send all the details present in this file to register@escanav.com.

7. eScan will send you the activation Key that you can use to register / activate your product even if you are not connected to internet.
8. Go to License Information window and enter the license key and click Apply and you will be redirected to another license information window.
9. Select the license key on this window and click Activate Now.
10. On the next License information window select I have Activation Code option and type the activation code that you received on your mail along with your personal details and click Activate. Your product will be registered instantly without Internet connection.

Renewing eScan

For Renewing **eScan** before the expiry of your License Period, click Renew on the License Information window and follow the instructions on screen.

Getting Started

Working with eScan

Opening eScan

Double click the icon on your desktop or click the icon in your system tray. You can also open eScan for windows from **All programs**.

Configure eScan Modules

You can configure all Modules of eScan to suite all your security needs by simply clicking on the desired Modules and then configure settings through the **Settings** option present under **Configuration** of that module.

As per your preferences you can turn **On** or **Off** any module of eScan by clicking on **Start**/ or **Stop** option present under configuration section in every Module.

Generating Reports

eScan generates reports of all its modules. You can **View**/ **Generate** a report of any module through **View Report** link present in every module.

USB Vaccination

This feature is very useful to prevent Auto run Viruses that are generally spread through USB drives that are used on multiple systems and are prone to spread infection.

Help

Click on this icon for a Live Chat with our Technical Support Representative, access Online Help, Visit and Join our Online Forums or get Remote support from our Technical support team, you can also send your feedback to 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

Information Bar

eScan displays important information/ links for Updates, Scans and system protection status at the top right on the interface.

Status and Links	Description
System is Secured	eScan displays this message on top Left Corner of the interface when eScan protection is enabled and active.
System is not Secured	eScan displays this message on top Left Corner of the interface when eScan protection is disabled or Paused.
Date of Virus Signatures	The last date when the Virus signatures were downloaded and updated on your system, eScan displays Date of Virus Signatures on the top right corner of the interface; you can click on this link to download the latest Virus signatures from our servers to protect your system for recent Virus threats and infections.
Last Computer Scan	eScan displays date of Last Computer Scan at the top right corner of the interface, you can click on this link to start the scanning of your system instantly.
Module Activity and Logs	eScan displays **Activity Logs** and **Status** below the tabs of the respective modules.

Configuring Settings

The "**Settings**" option is available under the configuration section in every module. The following is an overview of settings for every Module –

- **File Antivirus** – Using this section, you can define settings for the following:
  - Scanning drives for infections
  - Actions to be taken when any infection is detected
  - Save reports
  - Manage the quarantined files
  - Define settings for Backup and Restore
  - Access permissions for specific .exe and certain file types
  - Define settings for Folder Protection

  For more details **click here**

- **Mail Antivirus – Using this section, you can define the following settings:**
  - Scan or block mails with attachment having certain pre-defined extensions
  - Add new extension types
  - Define port settings along with action to be taken when an infected attachment is detected
  - Define path for storing Quarantined Files
  - Define settings for archiving mails and also to not archive email attachments with pre-defined extensions

  For more details **click here**

- **Anti - Spam -** Using this section, you can define the following settings**:**
  - Add Phrases to include/exclude (Whitelist) in Spam List
  - Configure detailed settings for filtering and tagging mails
  - Add disclaimer to Incoming or Outgoing Mails
  - Exclude disclaimers in mails to pre-defined list (you can create a list of your own) of receivers

  For more details **click here**

- **Web & Parental Control -** Using this section, you can define the following settings:
  - Create different user profiles, categorize (as Adult, Walled Garden, Teenager, and Adolescent) and also define settings for Web access permissions for restricted access to internet.
  - It will allow you to define the settings for identifying the phishing sites and block them.

- It will allow you to define the settings for identifying the malicious URLs and block them.

  For more details **click here**

- **Firewall –** You can define the following settings under Firewall

  - Monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks.
  - Pre-define 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.

    For more details **click here**

- **Endpoint Security** – You can define the settings under Endpoint Security:

  - Block unwanted applications from running on your computer
  - Define time restrictions for blocking applications
  - Block USB ports, Virus scan of USB devices, read only USB, Record the files copied for USB, Disable Auto play
  - Define password for accessing USB ports/ devices
  - Whitelist USB devices
  - Block CD/ DVD settings or Read only CD/ DVD
  - Disable SD cards, Imaging devices, USB Modem, Print Screens, Wi-Fi Network, Web Cams, Composite USB, Bluetooth, attachments, Network Printer
  - Define Allowed Wi-Fi SSID and allowed Printers list
  - Control of the applications and portable devices are allowed or blocked by eScan

    For more details **click here**

- **Privacy Control –** You can define the following settings under Privacy control:

  - Delete all the temporary information stored on your computer such as History, cache, cookies, temporary folders etc.
  - Schedule an auto-erase for the set options

    For more details **click here**

- **Cloud Protection –** You can define the following settings under Cloud Protection.

  - It will allow you to identify any new threats faster with global threat intelligence engine
  - It will allow you to receive immediate response to latest threats.
  - Monitor the internet round the dock. Agree to the terms and conditions and cloud protection will be activated on your system.
    For more details **click here**

- **Identity Protection –** You can define the following settings under Identity Protection
  - It will allow you to prevent data theft.
  - It will protect your sensitive information by detecting any attempt to send across the information to the internet and it will block the transmission immediately.

    For more details **click here**

- **Update -** You can define the following settings under update
  - Configure FTP or HTTP settings for downloading eScan Updates from our servers
  - Define application that you wish to automatically run after updates
  - Schedule your updates for automatic download and install on your system.

    For more details **click here**

Managing Notifications

Notifications Settings

Configuring notification settings will allow you to send emails to specific recipients when malicious code is detected in an e-mail or e-mail attachment or a Spam Classified mail is received or sent through the mail server. You can configure settings for following Notifications -

Virus Alerts for Infected Mails and Spams

- **Show Alert Dialog-box:** [Default] Select this check box if you want eScan to alert you through a display message when it detects a malicious object in an email or a virus infection.
- **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 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.

Notification Mails, Actions and Server Settings

- **Warning Mails -** You can configure this setting if you want eScan to send warning e-mails and alerts to a pre-defined sender or recipient.
- **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 fields are in disabled state, it is enabled only when you add mail addresses in the Delete Mails From User field.
- **Defining Settings for Mail Server –** For sending and receiving Notification Mails, you need to define settings for the Mail server that includes defining Mail Server address (SMTP) and SMTP Port number (Mandatory) and setting User Authentication and Password (if desired).

eScan provides pre-defined notification messages for warnings to both senders and receivers, you can always define your own warning mail using the following steps –

- Write the Warning Mail in a Notepad file(.txt extension) and save it on your system
- Select the Notification Alert in the List and click **browse** on the screen
- Browse the notepad File created by you on your machine and click **OK**.
- The content of that file will be visible in the text area on the Notification Settings Window.
- This text will be sent on mails for the Selected Notification mail.

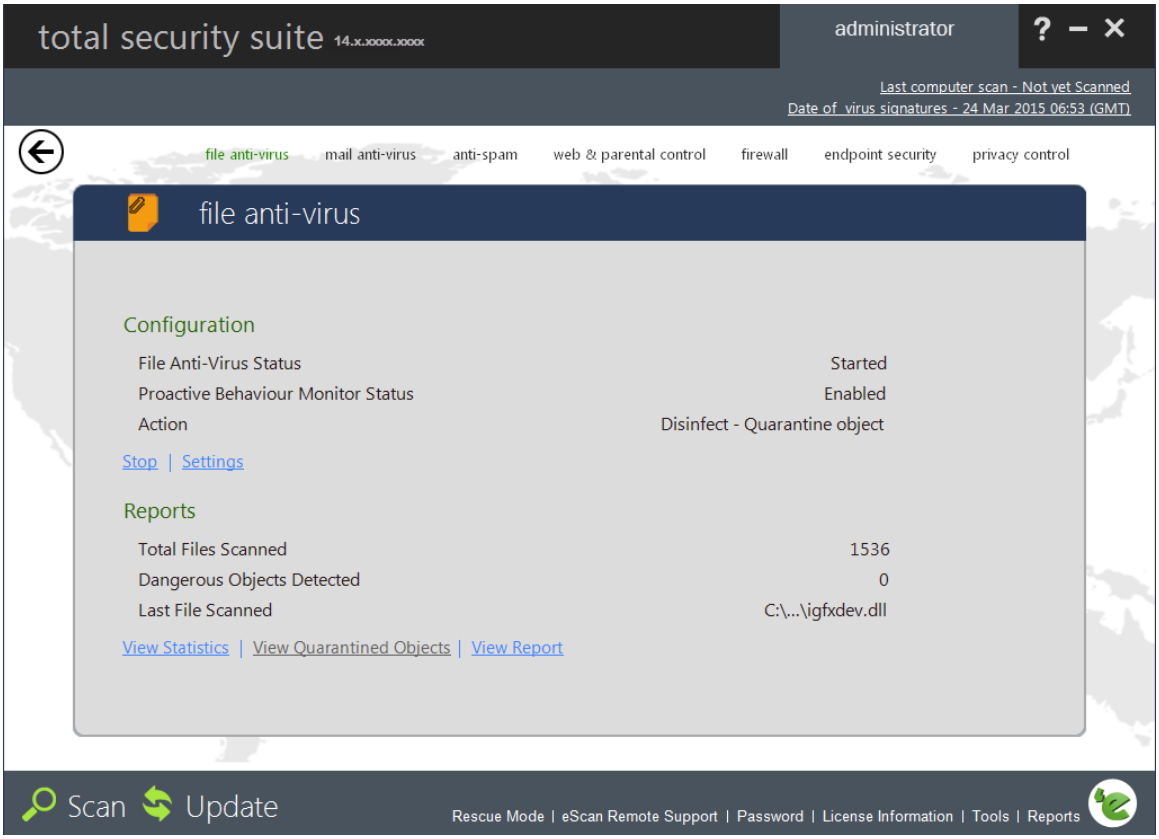
Update Notifications

Notification mails are sent to the users whenever eScan is updated, you can configure settings for sending/receiving mails using the Settings option present in the Update section of eScan.

File Antivirus

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 has a Proactive Behavior Monitoring system that blocks any application that is malicious or functions suspiciously. Based on the severity of the infection you can define what action should be taken by eScan when any infection or threat is detected.

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; this prevents users from creating, deleting, or updating files or sub-folders within specified folder list.



Turning on/off File Protection

- Open eScan Protection Center
- Click File Anti-Virus module on the interface
- Now click Start/ Stop option to enable or disable File Protection, as desired

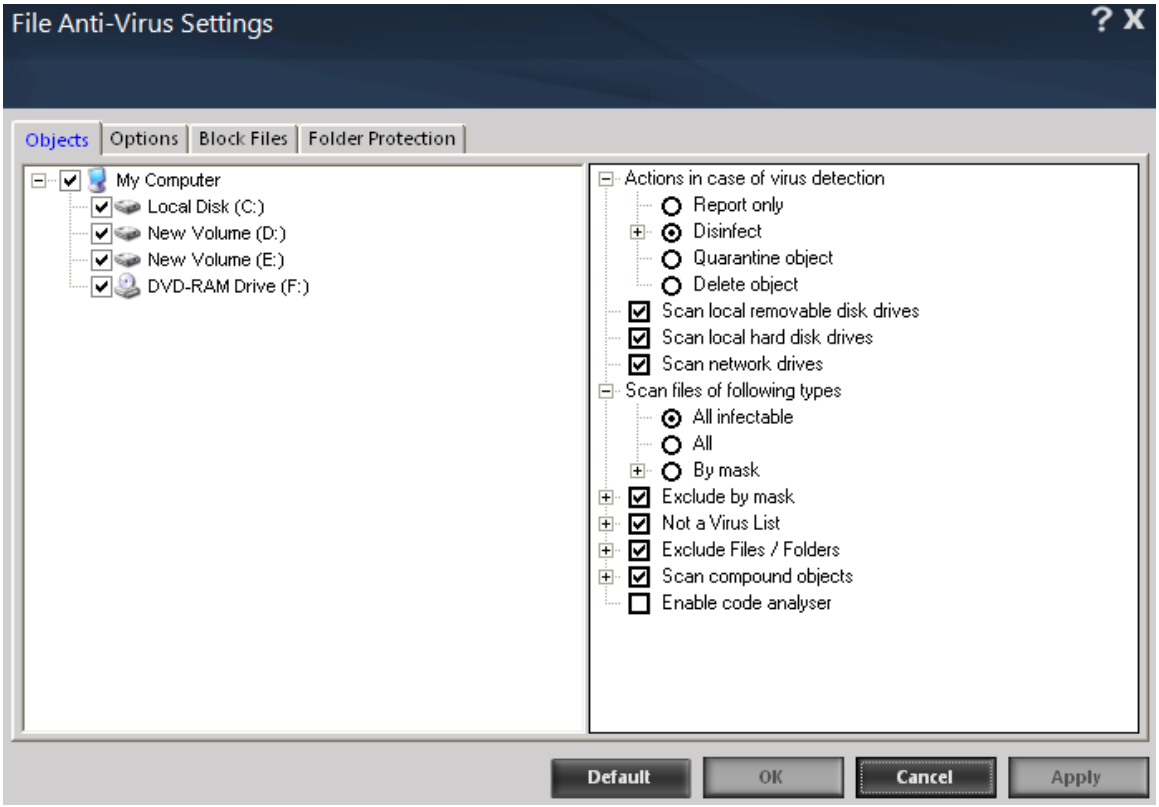
Note:
Please do not turn off protection for longer time as it will disable protection against viruses and malware infections.

Configuring Settings for File Anti -Virus

You can configure settings for File Antivirus using the settings option present under configuration in File Anti-Virus module of eScan. This module allows you to configure following settings –

File Anti-Virus > Settings > Objects

Scanning Drives and Actions on Virus detection - You can selectively scan any partition of your hard drive or a ROM connected to your system. Additionally, it also allows you to define action to take whenever a virus is detected. For this just Click Settings > Select the Drive for scanning on the left Panel > Option to Define Actions to be taken in case of Virus detection using the right Panel. (By Default Objects tab opens on the Settings window.)



- **Actions in case of virus detection -** It lists the different actions that File Anti-Virus can perform when it detects a virus infection. These actions are -
- **Report only** – Detection of an infected file is reported to you on a Pop up without taking any action on the file.

- **Disinfect -** eScan will automatically disinfect any infected file on detection. You can take a backup of the original file before disinfecting, click check box "Make backup file before disinfection". In this case eScan will automatically take a backup of the infected file before disinfecting it. The backup will be in an encrypted file format hence will not be harmful for your system. In case the file is damaged during disinfection you can anytime restore the original file.
  - **If disinfection is not Possible:** On detection of a virus escan will try to disinfect the virus, in case if disinfection is not possible, it will do the following:
  - **Report:** Select this option to report in case escan is not able to disinfect a particular virus.
  - **Quarantine Object:** Select this option to quarantine the infected object wherever eScan is not able to disinfect a virus**.**
  - **Delete Object:** Select this option to delete the object in case eScan is not able to disinfect the virus.
- **Quarantine Object** - eScan will quarantine the file whenever an infection is detected.
  - Restoring the Quarantine / Backup File

    You can restore the backup of the infected file using the following steps –
  - Click View Quarantine Objects option present on the main interface of eScan
  - You will be forwarded to the Quarantine Window, Click object name that you wish to restore Now click restore button to restore
  - File will be restored instantly

Note:
▪ *For restoring Backup File navigate to the objects tab on the window and click the object name that wish to restore and then click restore. The selected file will be restored instantly.*
▪ *By default, the quarantined files are saved in C:\Program Files\eScan\Infected folder*

- **Delete object** – If you have selected this option, eScan will automatically delete the file whenever an infected file is detected.
- **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 three 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 Selected]**
  Select this check box if you want eScan to exclude certain file names, types or extensions from being scanned, you can create a list by using the Add/ Delete option present under it. You can use filenames, Extensions, Special characters for listing. For example: *.pdf, grey*.tmp

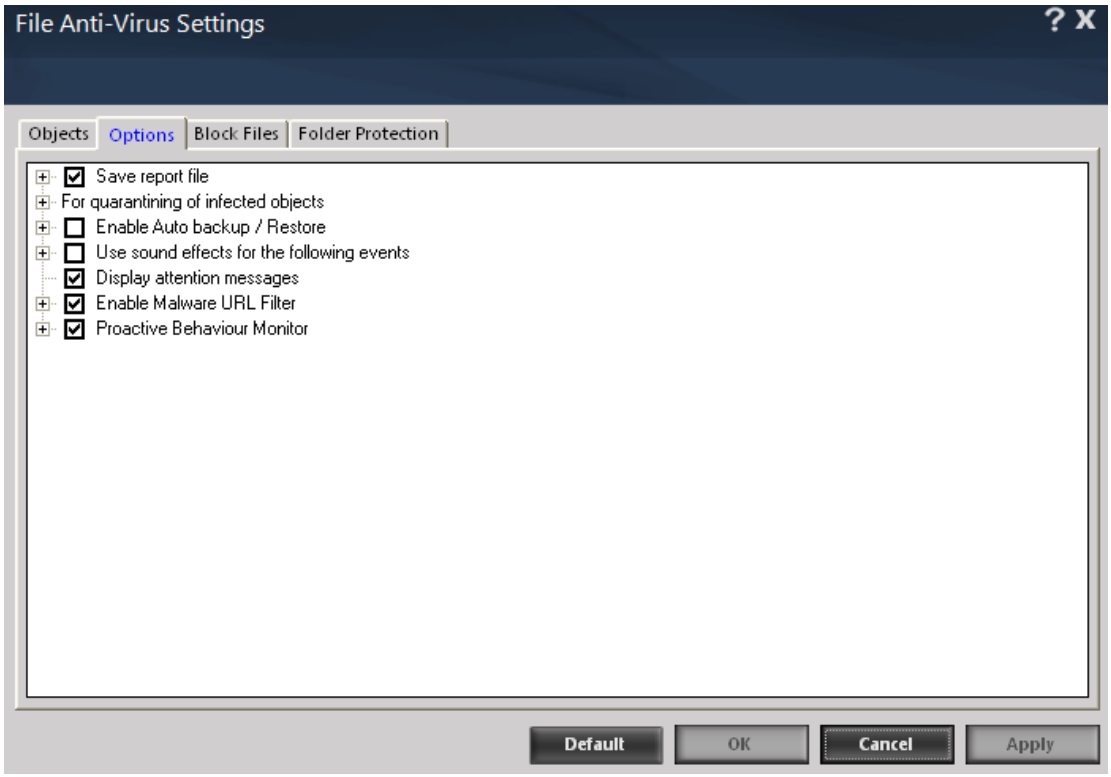
- **Not A Virus List - [Default Selected]**
  File Anti-Virus is capable of detecting riskware. Riskware refers to software that is originally not intended to be malicious, but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote 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. For this you just need to add Virus Name to the list with which it has been detected as Malicious by eScan.

- **Exclude Files/Folders - [Default Selected]**
  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 -**
  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. It will also allow you to define the depth level up to which an archived file is to be scanned. 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 analyzer**
  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.

File Anti-Virus > Settings > Options



- **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 the files that 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**

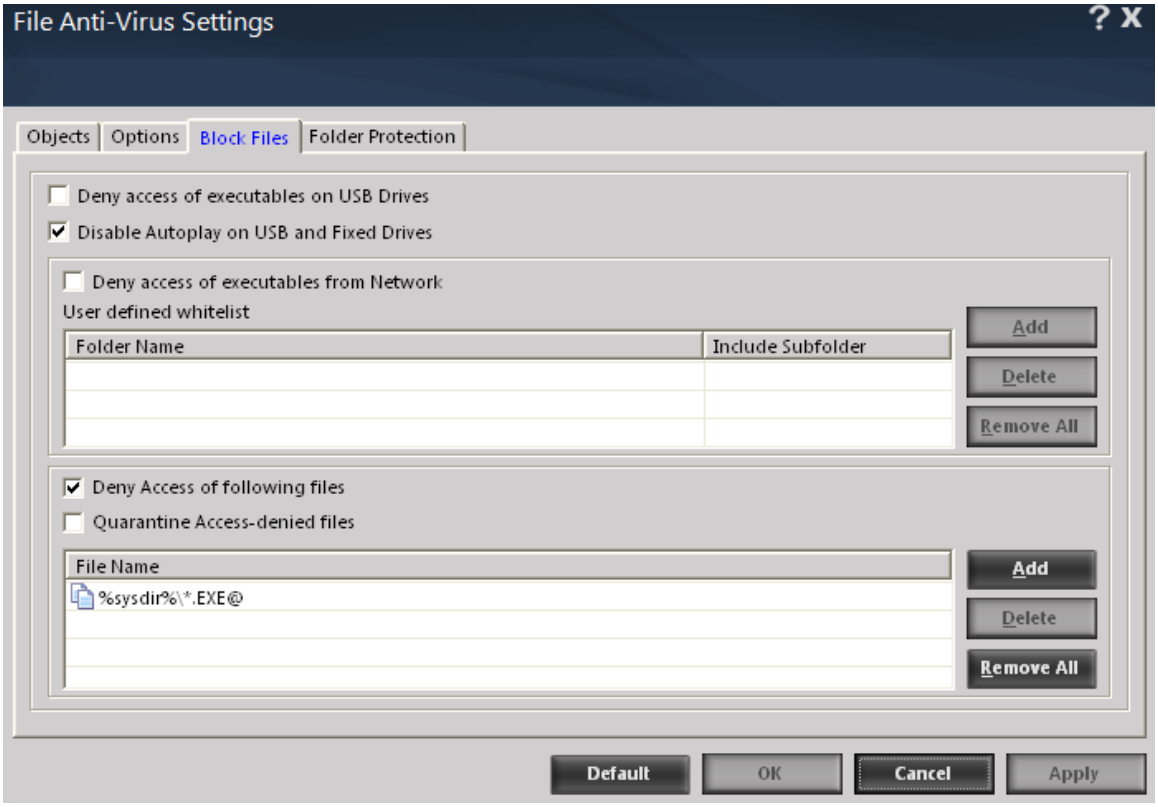
  This option helps you specify the destination for storing quarantined objects. By default, the quarantined objects are stored in

  C:\Program Files\eScan\Infected folder.

You can change the location of the destination folder if desired.

- **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 that cannot be disinfected. You can do the following settings:
- **For backup of clean objects -** eScan does a backup 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 up to which you want eScan to take backup of files. By default, value is 1 MB, but you can change it by double-clicking the  icon, and then type value in the size box.
- **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 -**Select this option to browse and play a sound file whenever an infection is detected on your system. Please ensure that the computer speakers are switched on.
- **Display attention messages [Default] –** Select this option to display an alert message with the path and name of the infected object and the action taken by the File Anti-Virus module.
- **Proactive Behavior Monitor [Default**] -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.

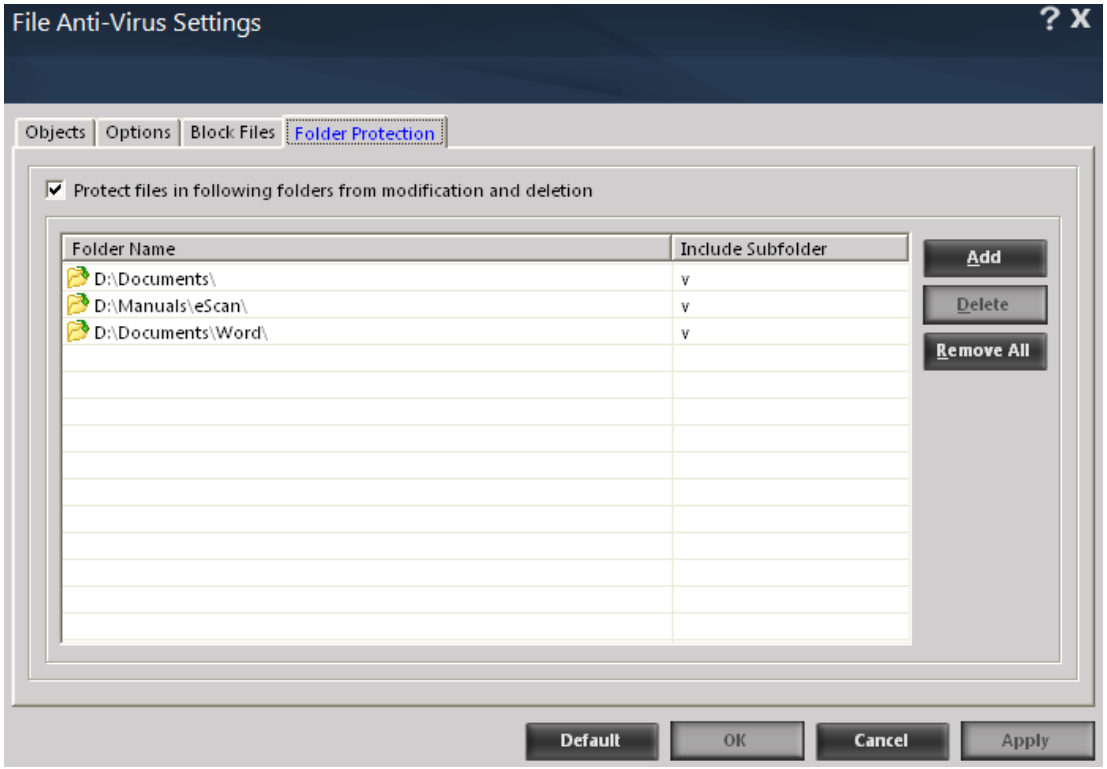
File Anti-Virus > Settings > Block Files



- **Deny access of executable from Network** - Select this check box if you want to prevent any executable controlled or downloaded 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 Selected] Select this check box if you want to prevent Autorun.inf from execution.
- **Deny Access of following files [Default Selected] -** Select this check box if you want to prevent the files in the list from running on your computer. You can Add a file as well as remove any or all files present in the list.
- **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@.

File Anti-Virus > Setting > Folder Protection

This tab helps you protect specific folders from being modified or deleted by adding them to the Folder Protection list. You can Add desired folder in the list by clicking on Add button present on the interface, for deleting a folder name from the list of protected folders click Delete. You can delete the entire folder list by clicking on Remove All option.

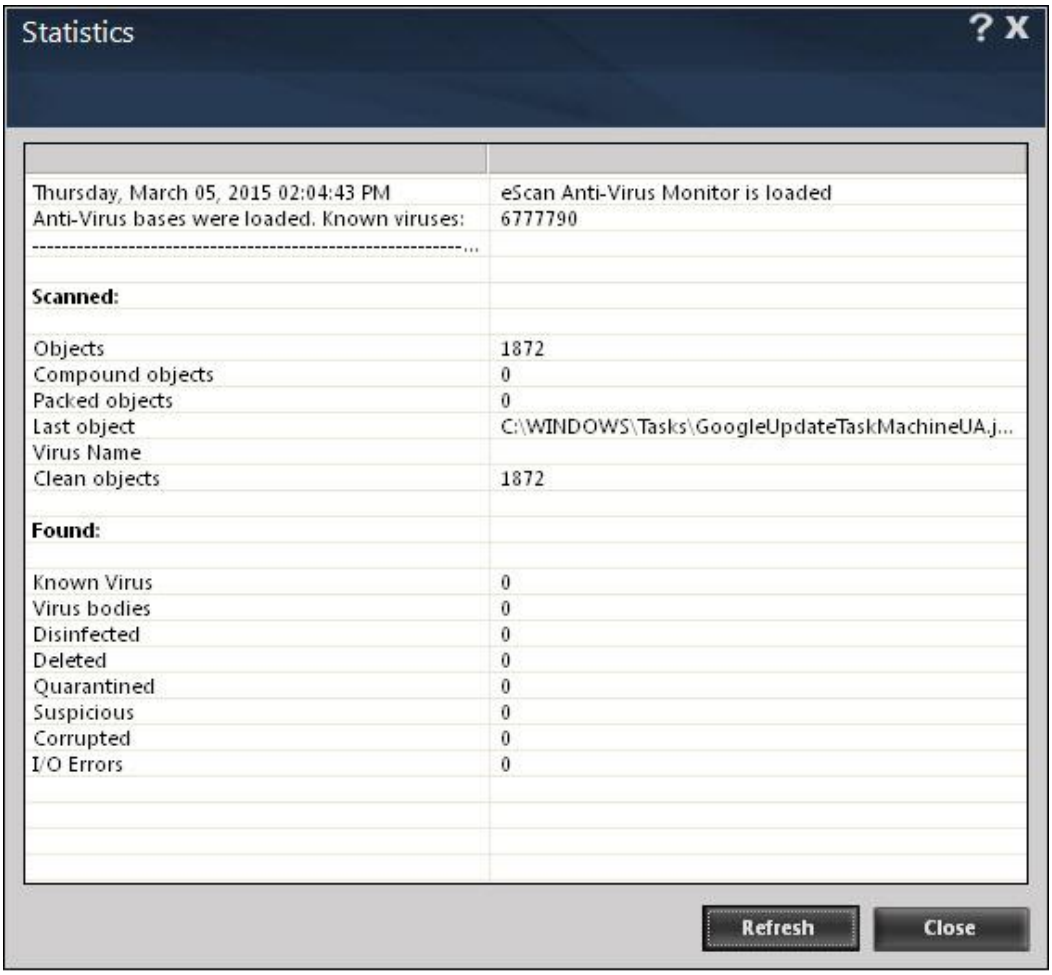


Note:
▪ *At the bottom of the screen of all the tabs-Default, OK, Cancel, and Apply buttons that you can use after configuring the settings based on your requirement.*
▪ ***Default:*** *Click this button to apply the default settings. It will ensure protection against viruses and malware infection with less impact on system performance.*
▪ ***OK:*** *Click this button after configuring desired settings. The settings will be applied and the settings window will close instantly.*
▪ ***Cancel:*** *Click this to cancel the configured settings or to close the window without changing any settings.*
▪ ***Apply:*** *Click this button to apply the configured settings. You can continue configuring other settings present on the Settings Window. Click OK to apply the settings and close the settings window.*

File Anti-Virus > Reports

This section displays the following information.

- **Total Files Scanned:** It shows the total number of files scanned by real-time File Anti-Virus monitor.
- **Dangerous Objects Detected:** It shows the total number of viruses or malicious software detected by 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:** This will display the latest activity report of the real-time monitor. The information is divided in to two sections Scanned and Found. The Scanned section includes , the number of scanned objects, compound objects, packed objects, last object, virus name clean objects, and so on are displayed, and under Found, the count of known virus, virus bodies, disinfected, deleted, quarantined, suspicious, Corrupted and I/O errors are displayed.

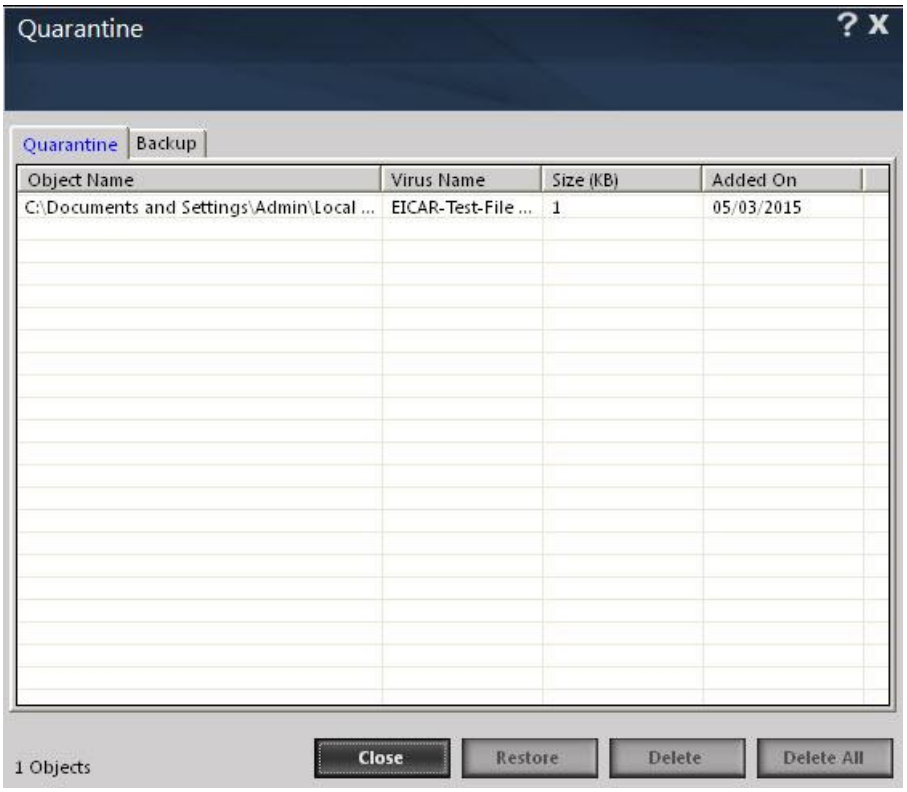


In addition, it displays the following information:

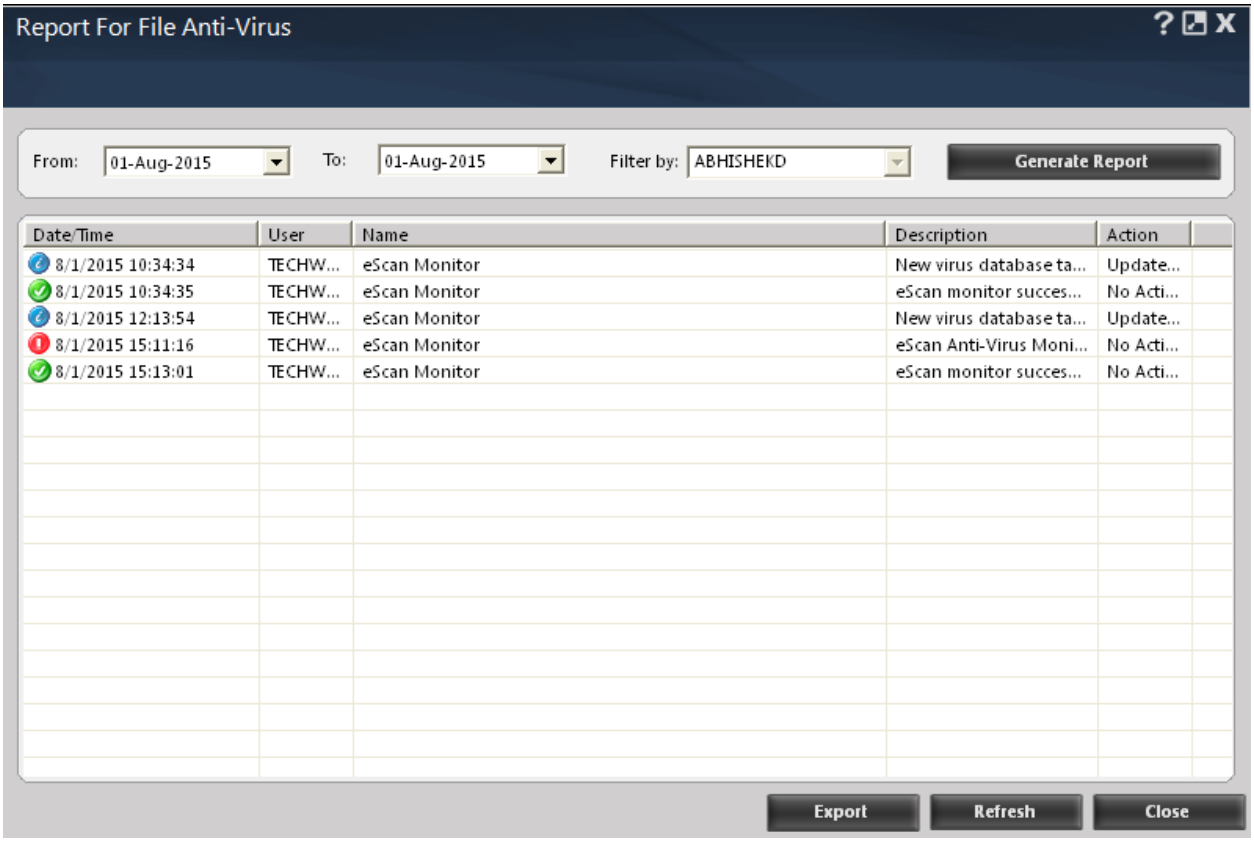
- The current details of the system date, time, and whether the eScan Anti-Virus monitor is running or not.
- The number of viruses detected.
- The results of most recent scan, such as the last object scanned and name of the virus detected.

View Quarantined Objects: This will display the quarantined files and backup files in two different tabs:

- **Quarantine:** This tab displays the files that have been quarantined. You can restore or delete the quarantined objects by a right-click on the object, and then click 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 a right-click on the object, and then click on an appropriate option. Before clicking any of these options, you should ensure that you have selected an appropriate row in the table for which you need to perform the action.

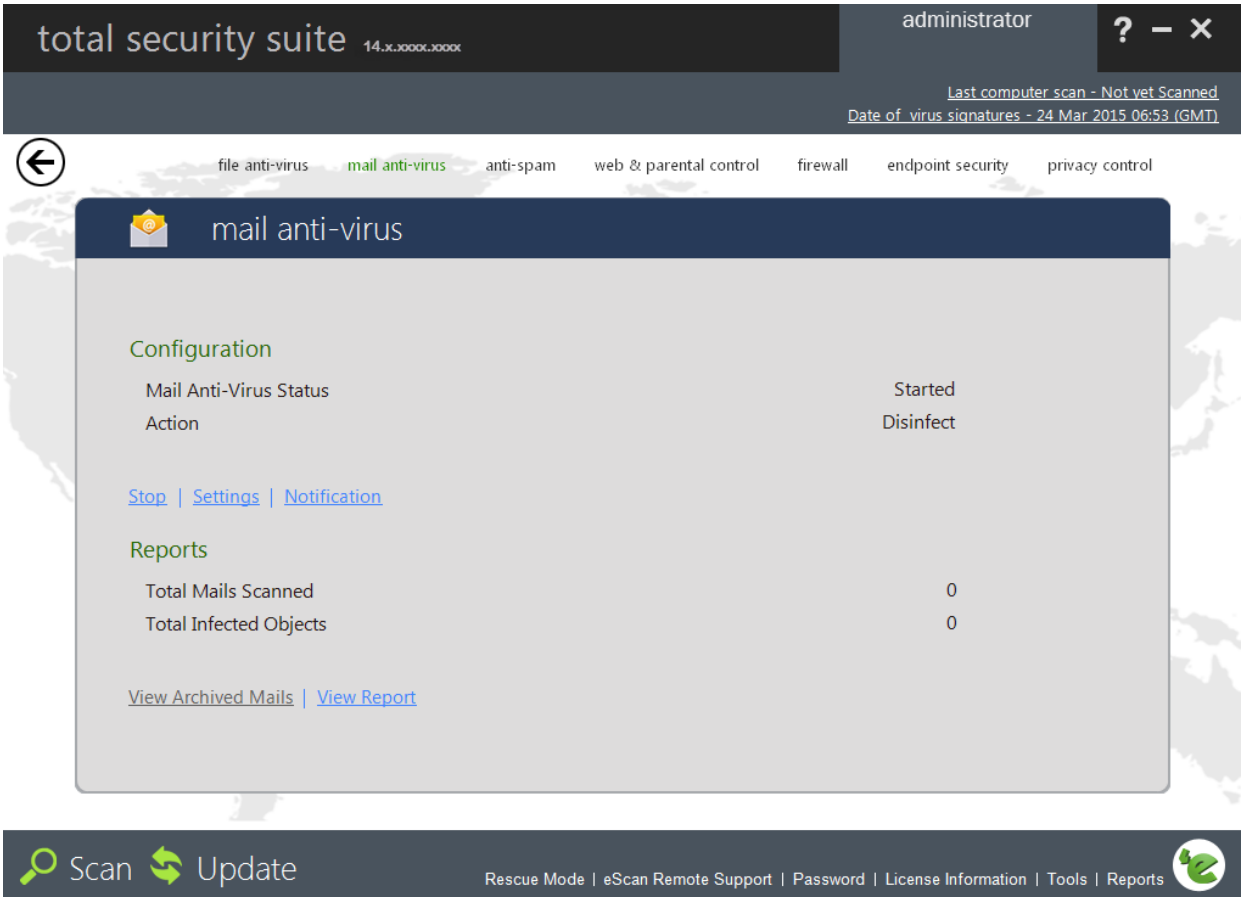


- **View Report:** This window displays the report for the File Anti-Virus module for a given range of dates in a tabular format on clicking the Generate Report button.



Mail Anti-Virus

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 emails 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 email or attachment.



Turning on/off Mail Scanning

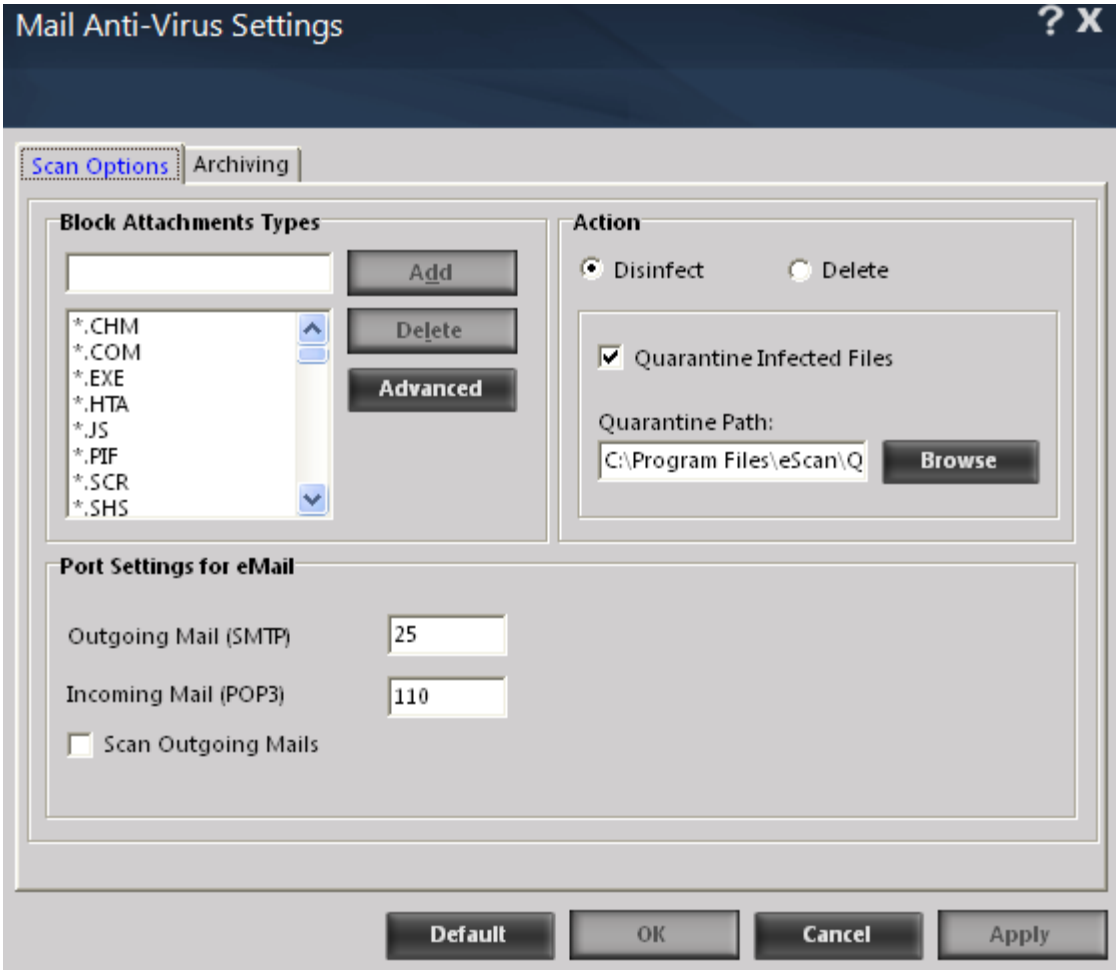
- Open eScan Protection Center
- Click Mail Anti-Virus option present on the interface
- Now click Start/ Stop option to enable or disable Mail Protection, as desired

Configuring Settings for Mail Anti -Virus

You can configure settings for Mail Anti-Virus using the Settings option present under configuration in Mail Anti-Virus section of eScan. This Section allows you to configure following settings –

Mail Anti-Virus > Settings > Scan Options

Block Attachment Types



This section provides you with a pre-defined list of file types that are often used by virus writers to embed viruses. Any email with 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. You should avoid deleting the file extensions that are present in the Block Attachments Types list by default. You can also configure advanced options required to scan emails for malicious code.

Defining Actions when an infection is detected

- **Disinfect -** [Default] Click this option if you want Mail Anti-Virus to disinfect infected emails or attachments.
- **Delete -** Click this option if you want Mail Anti-Virus to delete infected emails or attachments.
- **Quarantine Infected Files - [Default]** Select this check box if you want Mail Anti-Virus to quarantine infected emails or attachments.
  The default path for storing quarantined emails or attachments is C:\Program Files\eScan\QUARANT.
  However, you can specify a different path for storing quarantined files, if required.

Configuring Port Settings for emails

You need to define Port number for incoming as well as outgoing mails so that eScan can scan emails sent or received through those ports for Viruses.

Configure Settings for Archiving emails and email attachments

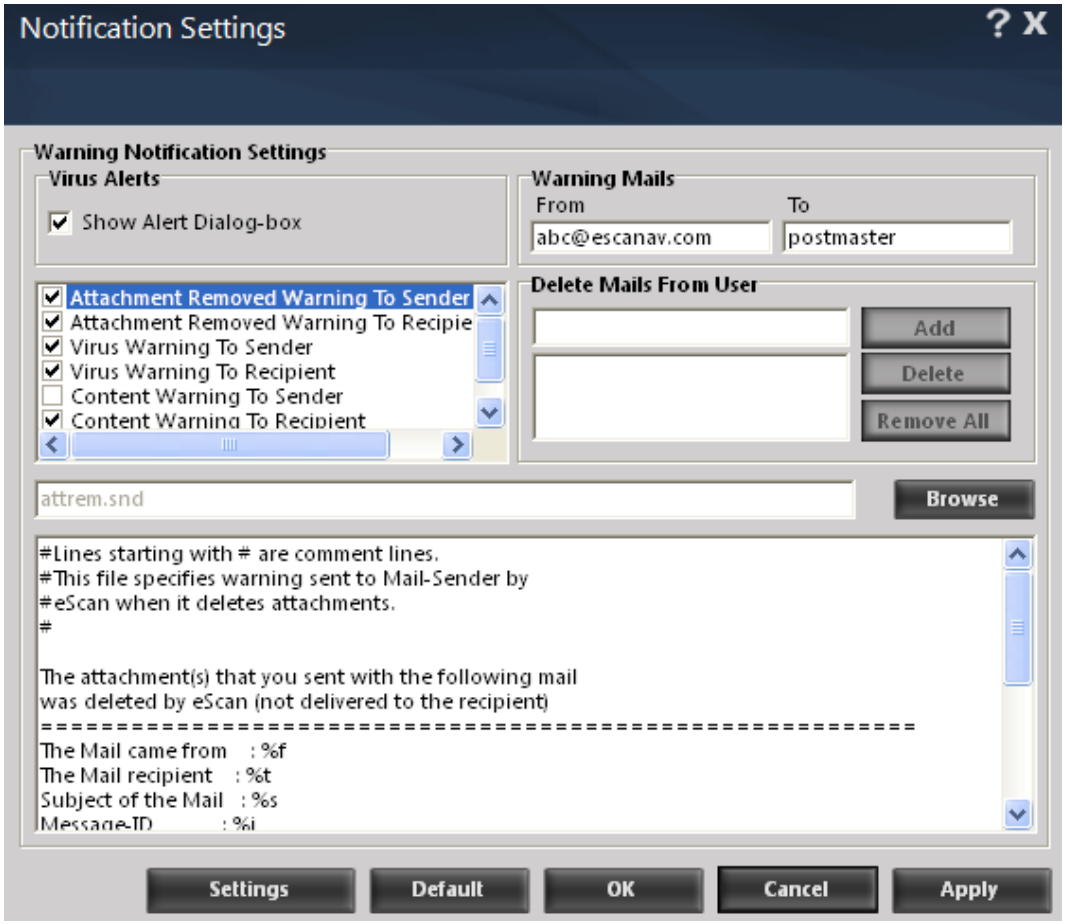
The following configuration options are available on this screen:

- **Archive emails:** This option helps you archive or back up all scanned emails that you have sent or received. Mail Anti-Virus provides you with the facility of backing up your emails to a given folder. The default path for storing archived emails is %appdata%\MicroWorld\eScan\Archive. By default, the email Archive Directory field, View Archived email button, and Browse button is disabled. It is enabled only when you select the Archive email check box. Select the Archive email 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 email 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 email attachments to a 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 is disabled. These fields are enabled 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.

Note:
▪ Mail Antivirus does not provide protection for email accounts that you access through a web- based email service.
▪ 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. It will ensure protection against viruses and malware infection with less impact on system performance.
▪ **OK**: Click this button after configuring desired settings. The settings will be applied and the settings windows will close instantly.
▪ **Cancel**: Click this button to cancel the configured settings or to close the window without changing any settings.
▪ **Apply**: Click this button to apply the configured settings. You can continue configuring other settings present on the settings window.

Notifications

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 emails to specific recipients when malicious code is detected in an email or email 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.



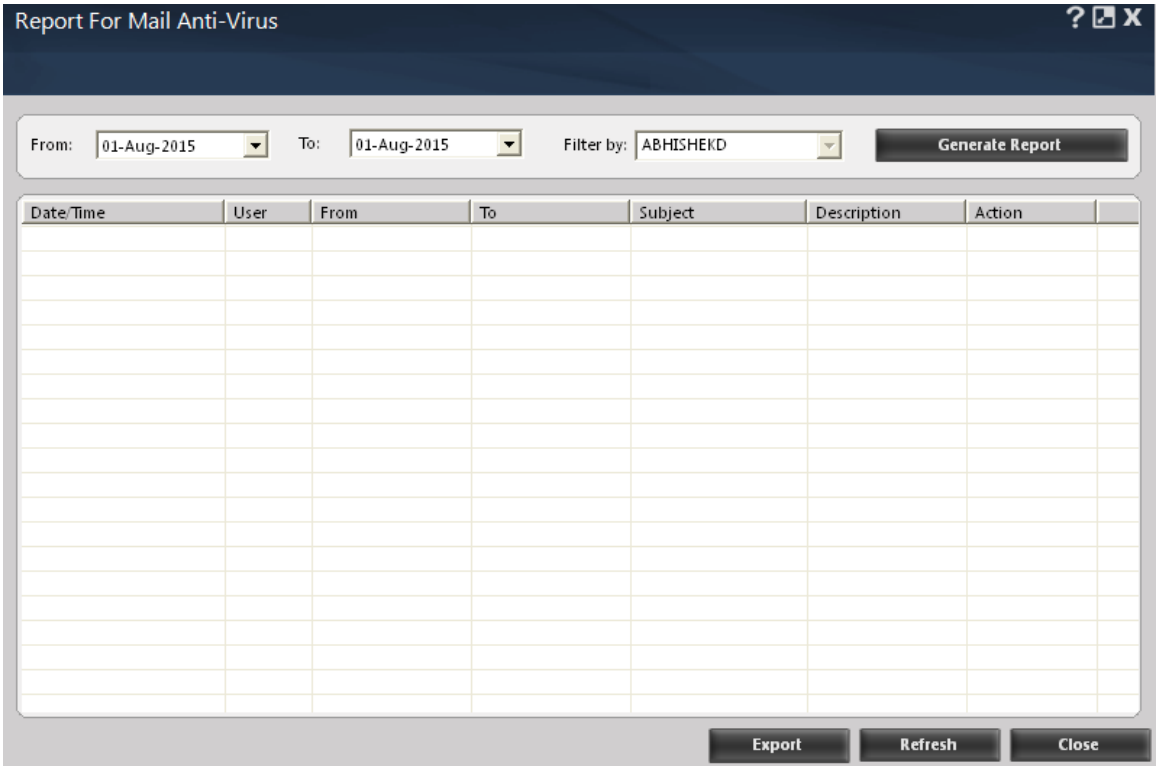
Mail Anti-Virus > Settings > Archiving

Using this tab you can define settings for archiving mails as well as attachments received on your mail. It also allows you to exclude attachments with desired extensions. You can also define the path for storing Archived mails and attachment on your computer.

Note:
▪ *Mail Antivirus does not provide protection for email accounts that you access through a web- based email service.*
▪ *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. It will ensure protection against viruses and malware infection with less impact on system performance.*
▪ ***OK:*** *Click this button after configuring desired settings. The settings will be applied and the settings windows will close instantly.*
▪ ***Cancel:*** *Click this button to cancel the configured settings or to close the window without changing any settings.*
▪ ***Apply:*** *Click this button to apply the configured settings. You can continue configuring other settings present on the settings window.*

Reports

This section gives you a report for total Mails scanned and total infected files during a specific period, as selected by you.



Anti-Spam

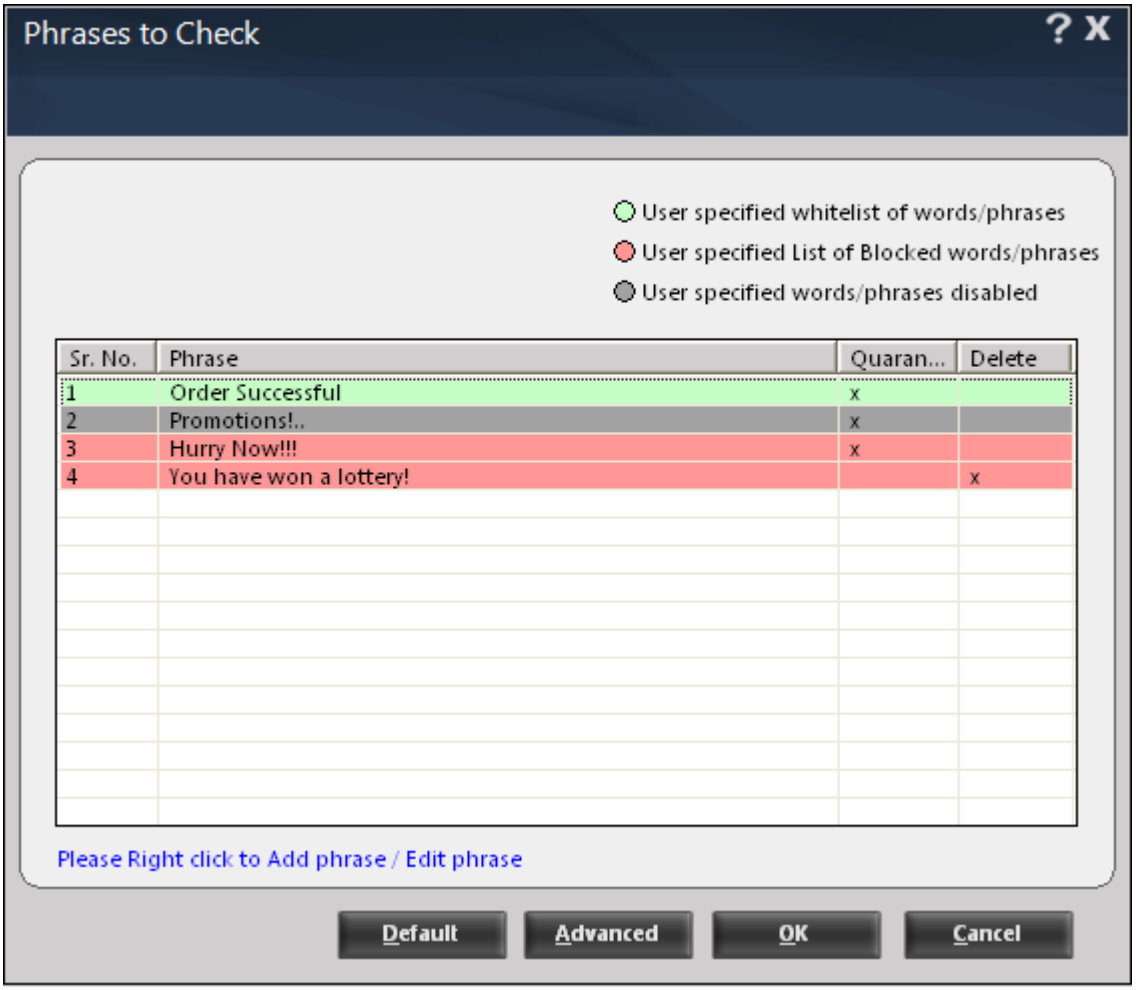
This module filters all your junk and spam emails by using the advanced NILP technology and sends content warnings to specified recipients.

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

Configuring Settings for Anti-Spam

Anti-Spam > Settings

Define settings for anti-spam such as whitelisting words or phrases received or set over mail. It also allows you to block specific words/ phrases or block words or phrases for specific users.

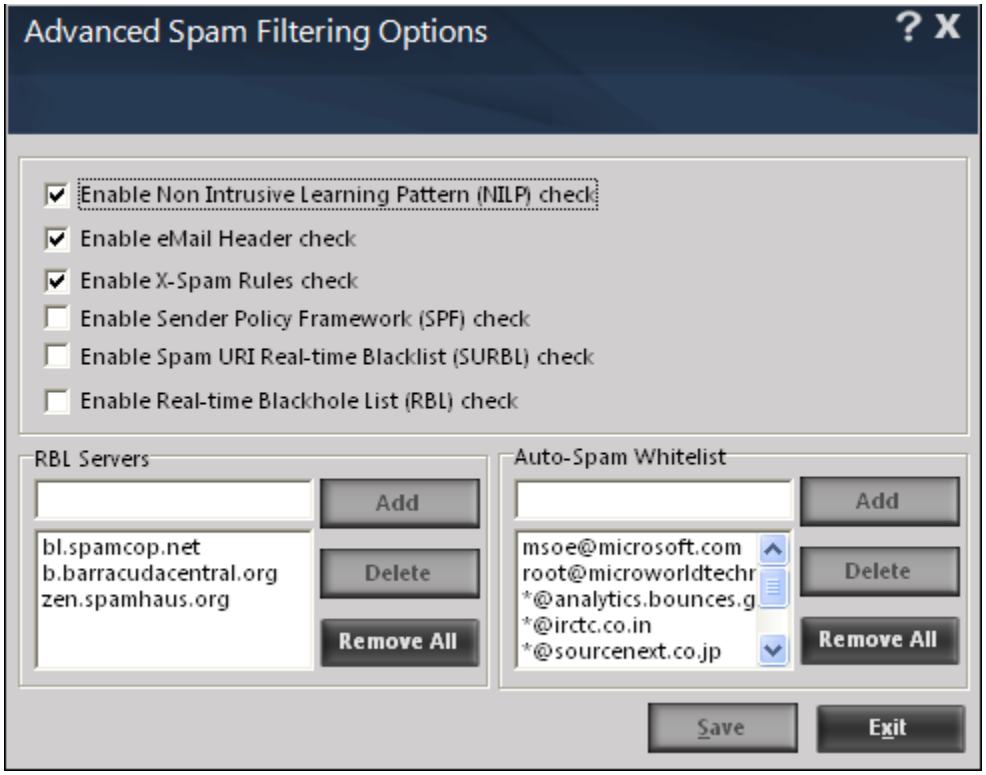


- **Adding Phrases to Blacklist or White List** –It will allow you to specify certain words or phrases, so that mails containing those words or phrases in the subject, header, or body part of an email are recognized as spam and are quarantined or deleted, as defined by you. Do right click to specify a list of words that you can either allow (**Whitelist**) or block (**Blocklist**) or to disable the checking of specified phrases **(Disabled)**. The whitelisted/ blocked/ disabled phrases are differentiated with the following color codes.
  - User specified whitelist of words/phrases are color coded in GREEN
  - User specified List of Blocked words/phrases are color coded in RED

Note:
You can disable a rule defined for whitelisting or blacklisting by using the disable phrase option.

Advanced Spam Filter Configuration

Using Advanced Spam Filter Configuration options you can configure the following 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 email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user. Select this check box if you want to enable NILP check.
- **Enable email Header check:** [Default] Select this check box if you want to check the validity of certain generic fields, such as From, To, and CC in an email and marks it as spam if any of the headers are invalid.
- **Enable X-Spam Rules check:** [Default] X-Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The X-Spam Rules Check technology matches X-Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.

- **Enable Sender Policy Framework (SPF) check:** SPF is a world standard framework that is adopted by eScan to prevent hackers from forging sender addresses. It acts a powerful mechanism for controlling phishing mails. Select this check box if you want Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.
- **Enable Spam URL Real-time 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 Real-time 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.
- **AutoSpam Whitelist:** Unlike normal RBLs, SURBL scans emails for names or URLs of spam Web sites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid 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.

Notifications

You can configure the notification settings for the Anti-Spam module by using this dialog box. By configuring this module, you can send emails to specific recipients when a particular event occurs. For more details **click here**

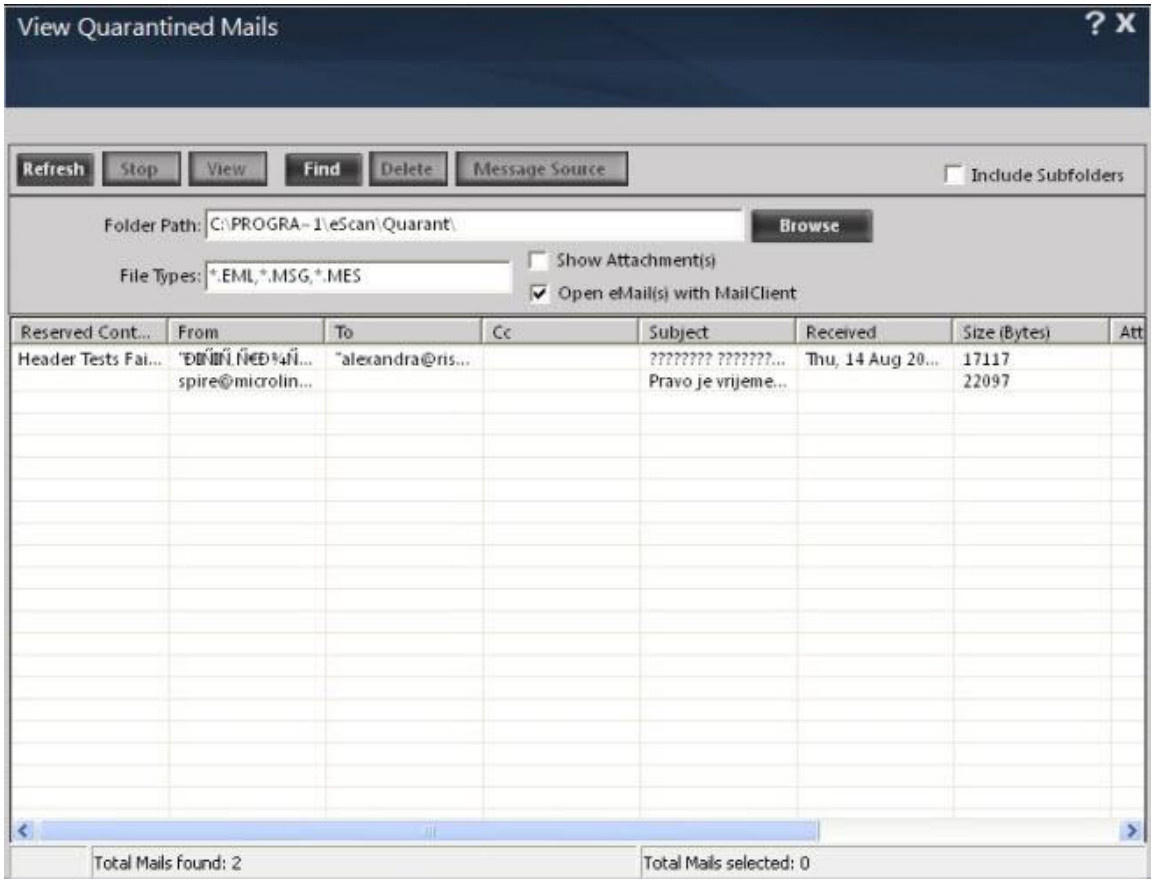
Reports

This section gives you detailed report for total number of Quarantined Mails and total number of Clear Mails received. If any mail is wrongly or mistakenly reported as Blocked you can easily add it to white list using the options present on right click in the Report for Anti - Spam table. Henceforth, that mail will not be marked as a Spam. This section also displays count of Quarantined mails as well as Clear Mails on the main interface of eScan in Anti -Spam module.

- **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 mails that are free from any virus or malware infection.

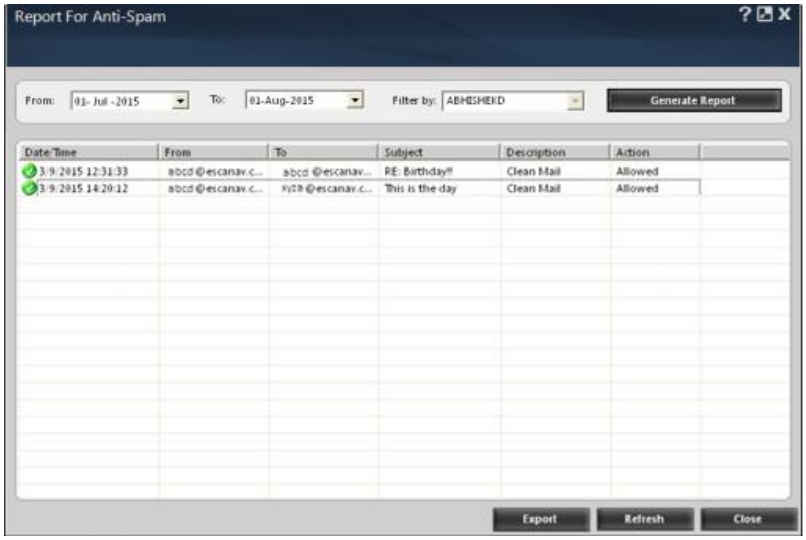
In addition, you can view the following reports:

- **View Quarantined Mails:** This will display the list of e-mails that have been quarantined by Anti-Spam. With the help of this window, you can configure the settings by specifying the path of the folder where you need to store the archived e-mails and specifying the format for storing e-mails. In addition, you can view the contents of e-mails, add sender's email id to the white list or add reserve content of the selected e-mail to the Hide email List.



- **View Ham Mails:** This will display the report of all ham e mails identified by eScan and have been archived by Mail Anti-Virus. As in the case of quarantined mails, you can specify the path of the folder where you need to store the archived e-mails and can also specify the format for storing emails.

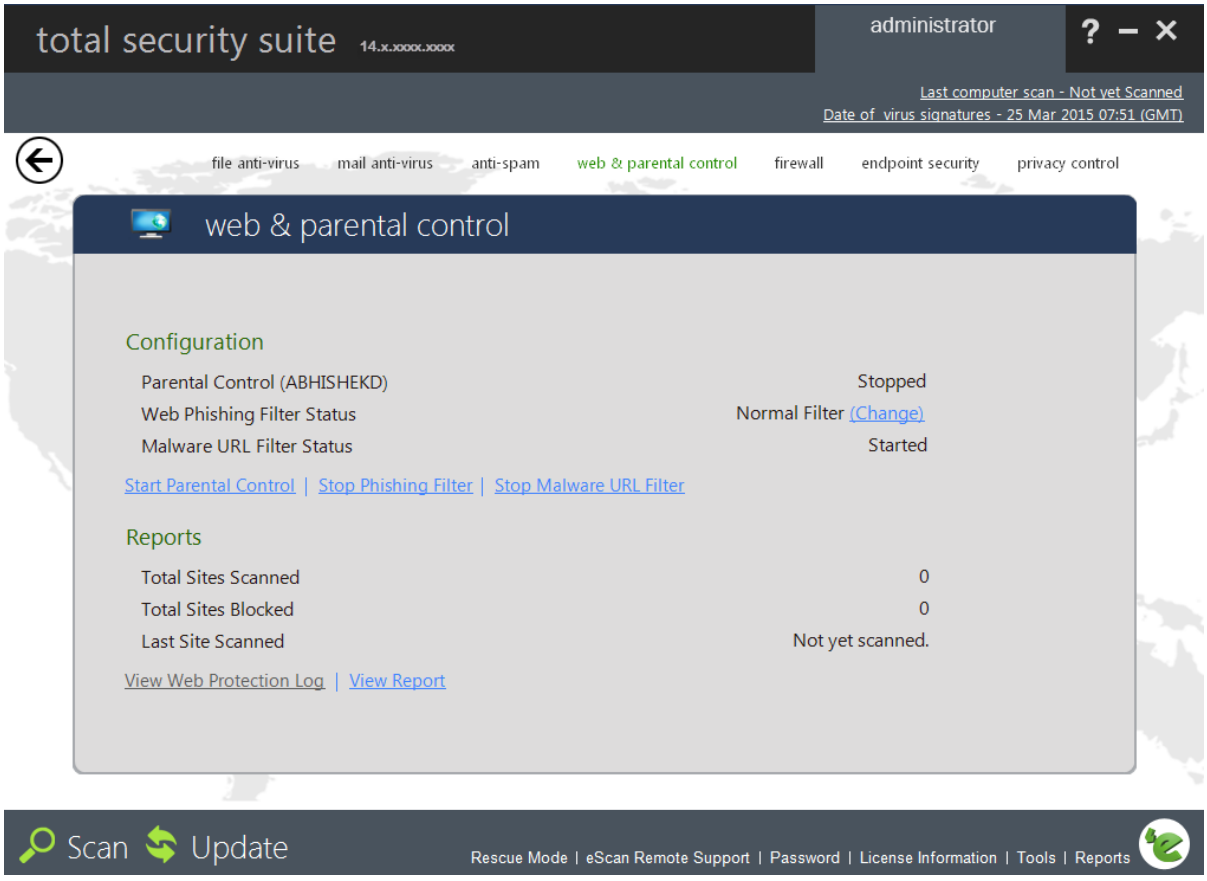
- **View Report:** This will display the Report for the Anti-Spam window. This window displays report for the Anti-Spam module for a given range of dates in a tabular format when you click the Generate Report button.



Note:
▪ Quarantined Mails are the mails that have been found carrying malicious content marked as Spam and are stored by eScan in an isolated folder so that it cannot harm your system or spread infection.
▪ Ham Mails are all Clean mails that have been scanned and are not carrying any malware infection or virus that can harm your system or spread infection in other files on your system.

Web & Parental Control

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. It can also be to prevent employees from accessing non-work-related web sites during work hours.



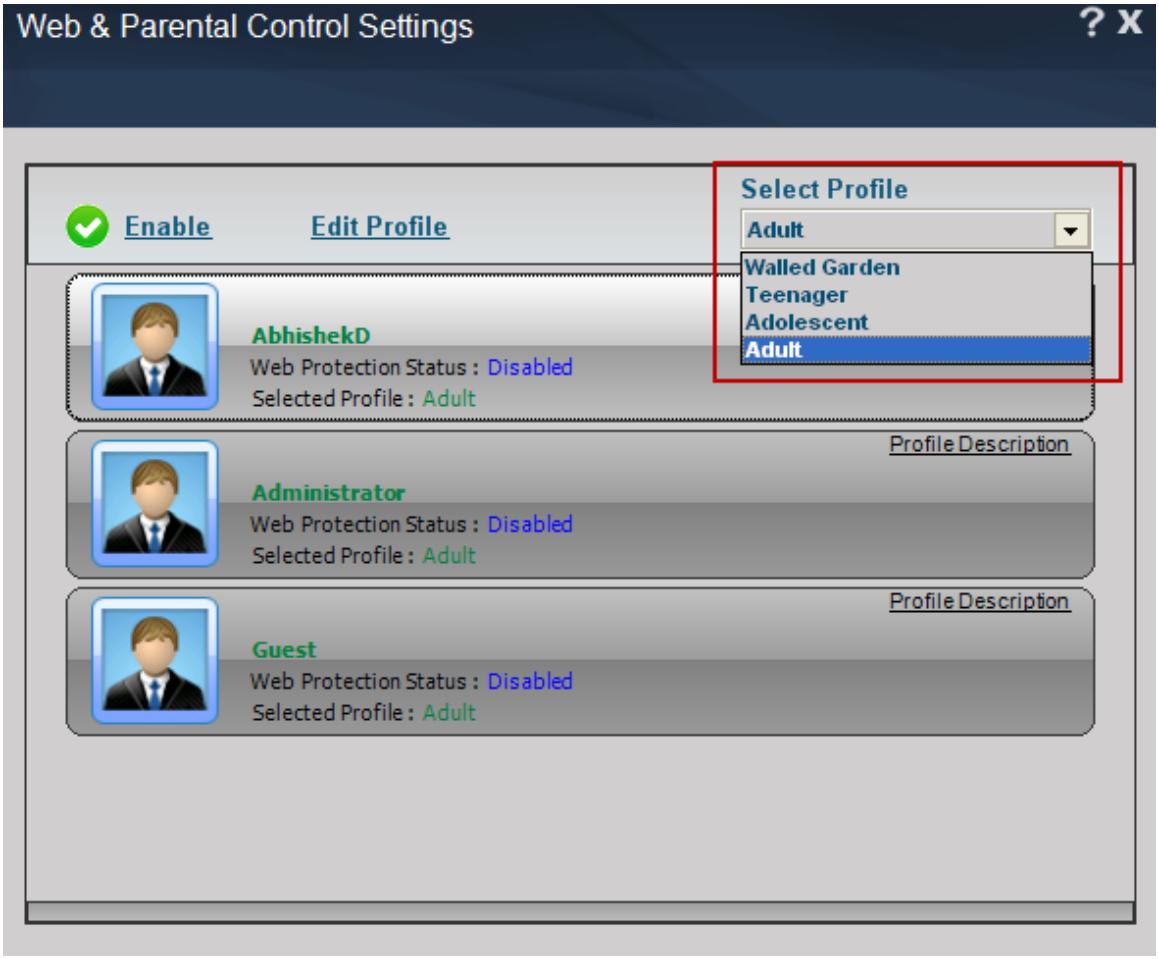
Turning on/off Web Protection

- Open eScan Protection Center.
- Click Web Protection option present on the interface.
- Now click Start/ Stop option to enable or disable Web Protection, as desired.

Configuring Settings for Web Protection

Using the Web Protection Module you can create Profiles for various types of users; you can categorize them in different categories that have variable permissions for net usage and

website access. For your convenience four profiles have already been defined in eScan with different access rights and web Access control levels.



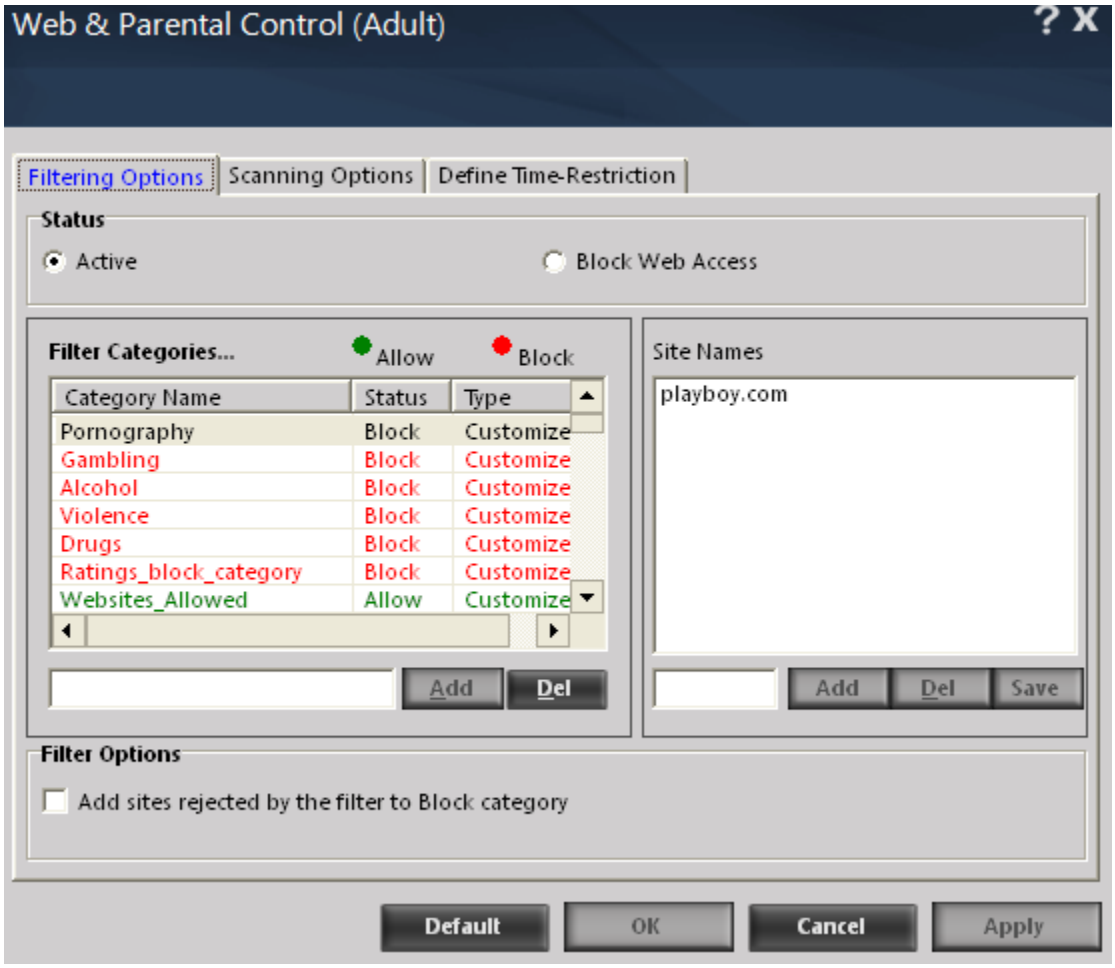
A brief description of Profiles

- **Walled Garden** – Recommended for children up to the age of 10. This profile blocks all access to the internet.
- **Teenager -** Recommended for the kids in age group 11 – 15. This profile activates the following filters –
  - Blacklists
  - Web Page filter
  - Domain name filter
  - Page title filter
  - Reserved word threshold of 3
  - Blocks all Java applets and Active X scripts except from predefined site list
- **Adolescent** – Recommended for kids in age group of 16 to 18. This profile activates the following filters –

- Blacklists
- Web Page filter
- Domain name filter
- Page title filter
- Reserved word threshold of 5

- **Adult –** Recommended for Adults (age more than 18). This profile allows all traffic except for the websites in black lists No reserved word threshold value is used.

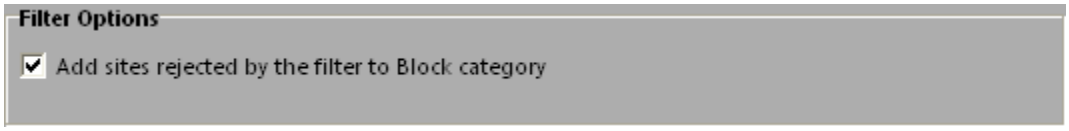
Editing a Profile



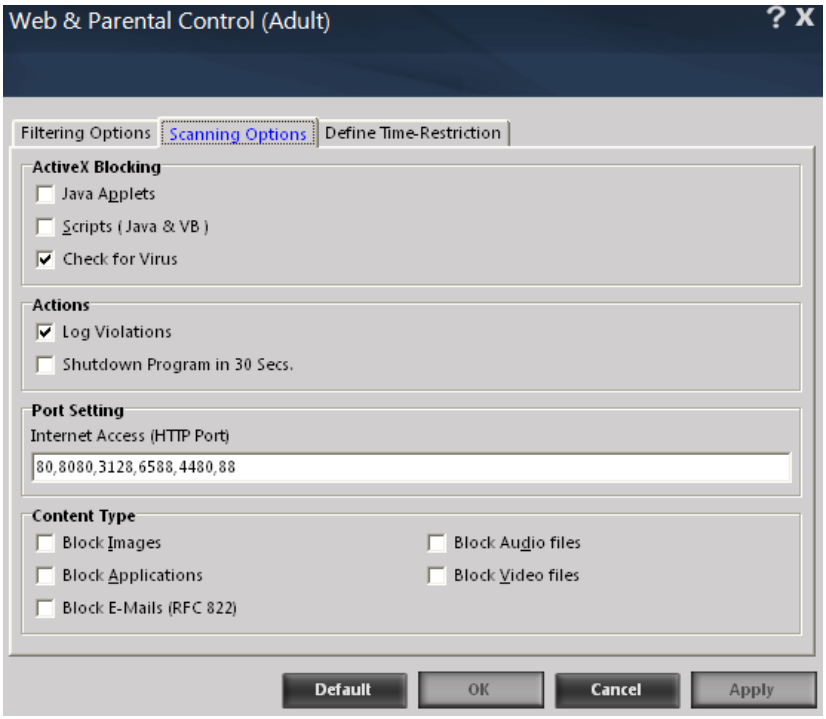
You can edit the selected profile using the following simple steps –

Filter Options

1. Select the desired profile using the drop down present on the Web Protection Settings Window.
2. Now click Edit Profile option present on the interface. This will forward you to the Web Protection Window. Filtering options Tab will open on the Window.
3. Categories listed in Red are Blocked whereas Categories listed in Green are allowed.
4. You can Block or Allow any category either by clicking on it once or right click and block or allow a Category.
5. For adding a site name to any of the Categories just type the name of the website that you wish to Add in field present under Site Names and click Add button present beside it.
6. You can create your own new category of Blocked or Allowed sites using the Add option present under Filter Categories list. Similarly you can delete any category from the list using the Del option present below the filter categories list.
7. If you wish to Add sites that are rejected by the filter to Block list, tick on the check box present under Filter Options.



Scanning Options



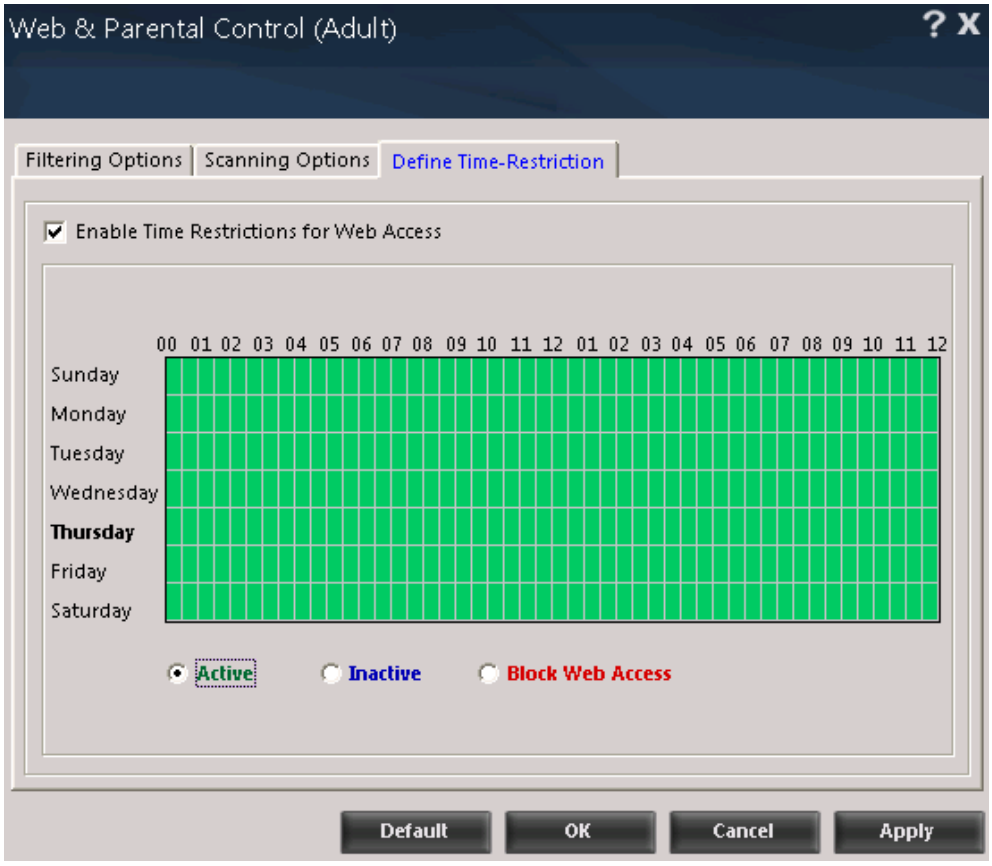
Using this tab you can define settings for Active X blocking, check for Viruses and Actions to be taken on detection. Port settings and content blocking as desired.

Define Time Restriction

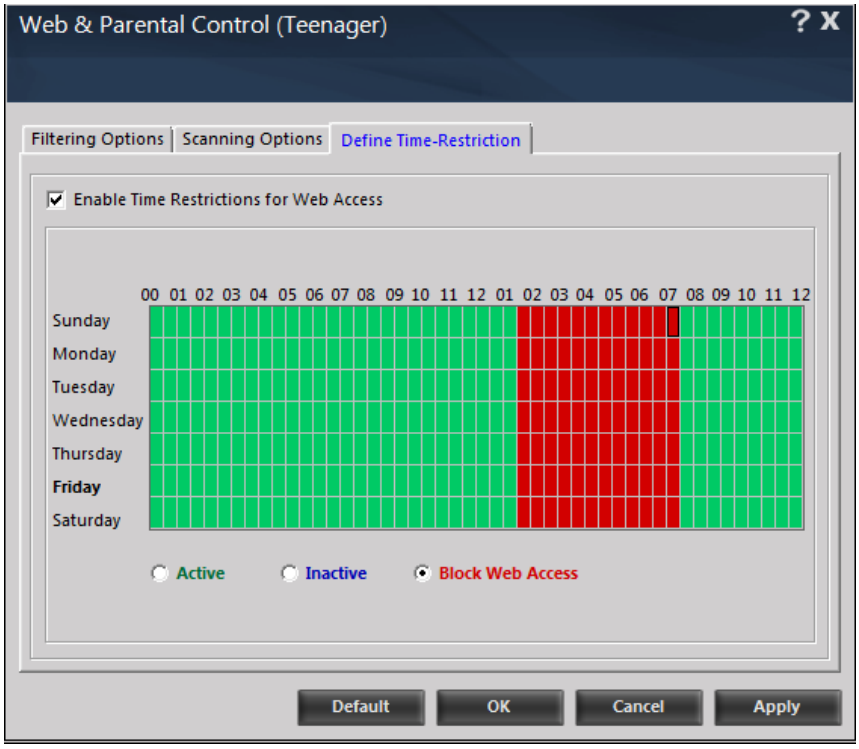
I. Multiple User Logins

You can define the settings for web access based on the different user logins created on your system.
For example: Suppose you have a parent and child login. The parent can act as an administrator and define different settings for both the user logins.

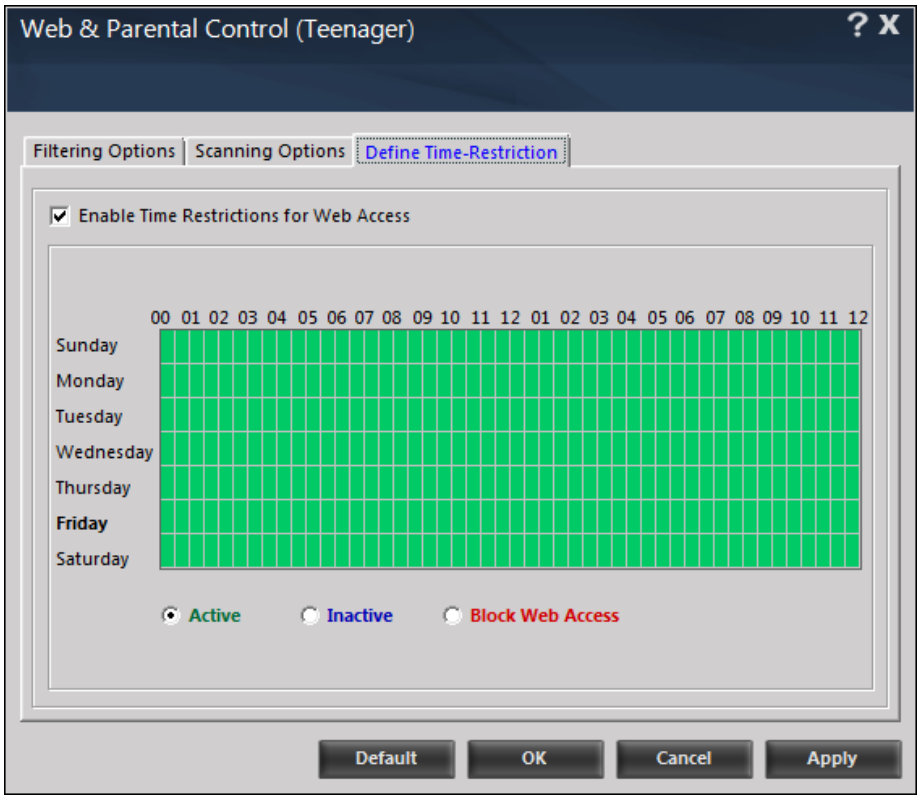
The Parent users (Adult) can have restricted web access throughout the day (See below figure)



- Allow restricted web access for children or block web access during study time (see below figure)



- Allow restricted web access throughout for children (See below figure)

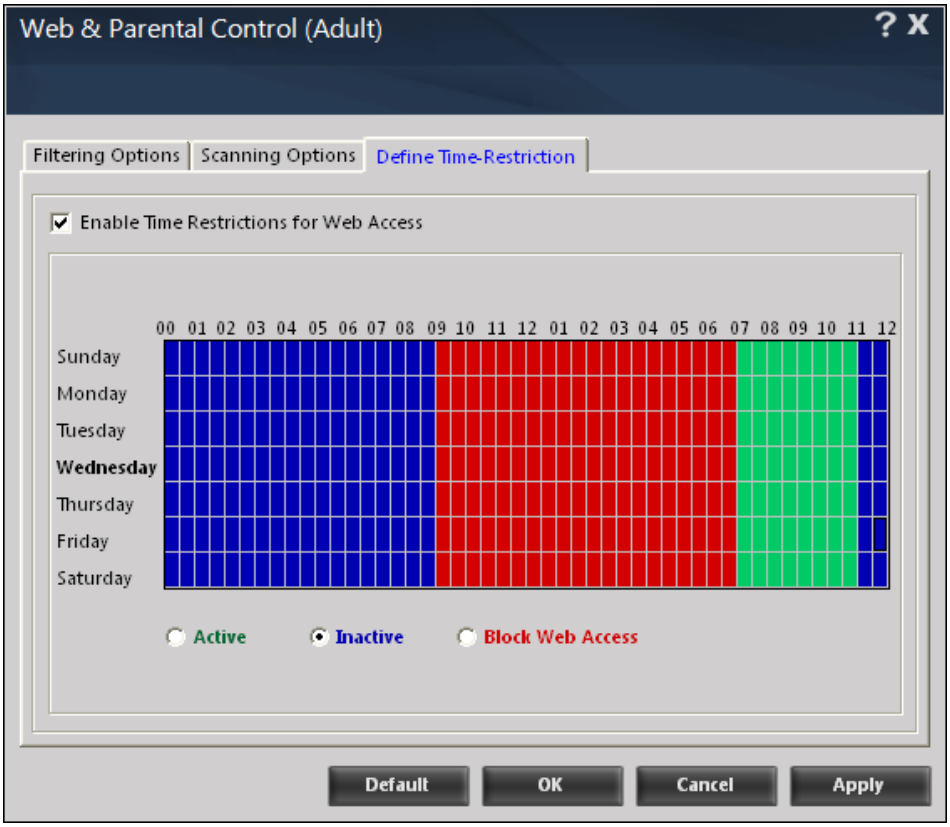


You can define the settings as per your personal requirements; the above example and images are for illustrational purpose only. Each profile can have a customized setting of web Protection.

II. Single User Login

If you have only a single login on your computer/laptop then you can do the following

- Block web access during DAY when only caretakers are at home or only children are at home (For example between 9 am to 7 pm); you can allow restricted web access when you are home i.e. 7 PM to 11 PM or you can inactivate the module between 11 PM to 9 AM when you want unrestricted web access for yourself, as shown in the following figure -



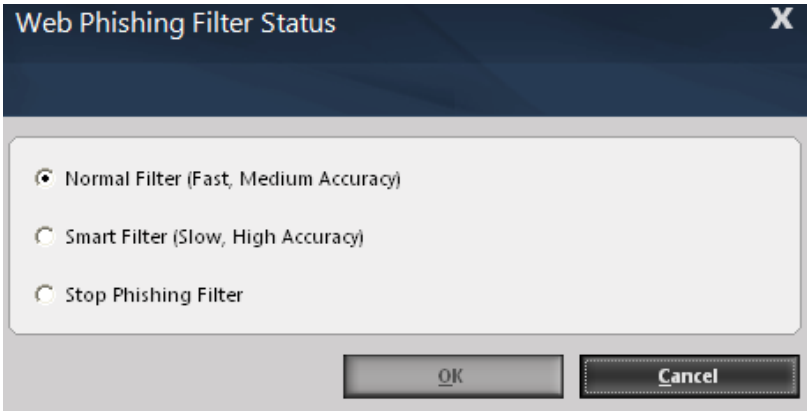
In the above figure:

- **Block Web access: 9 AM to 7 PM**
- **Active (Allowed Restricted Access): 7PM to 11 PM**
- **Inactive (Full Access): 11 PM to 9 AM**

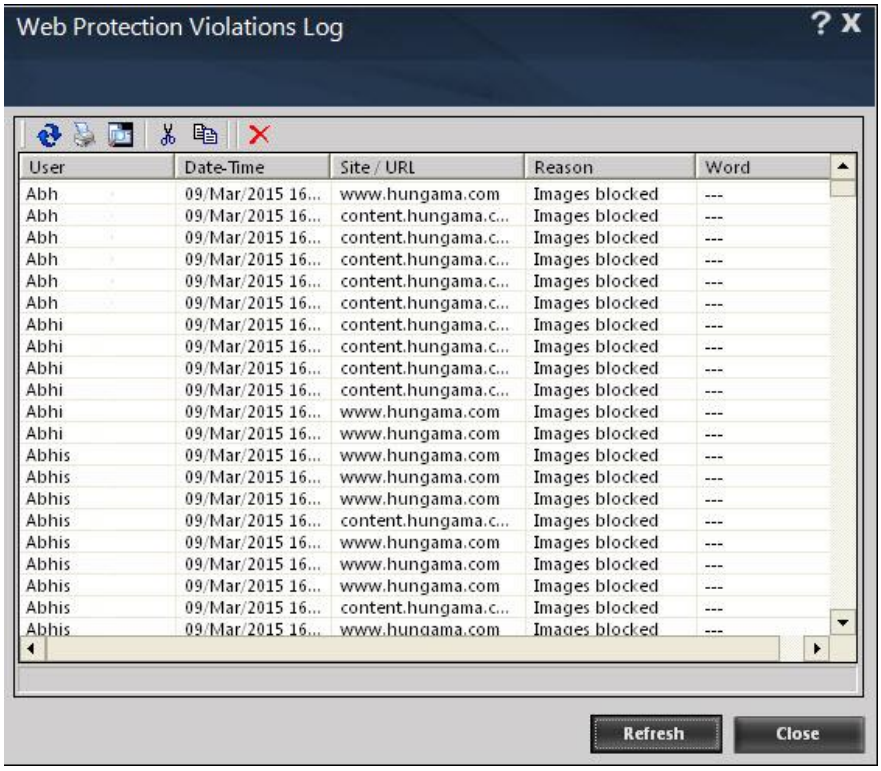
Note:
▪ You can change the settings as per your convenience.

Phishing Filter

You can turn on or turn off the Phishing filter using the Start / stop Phishing filter option present under Web Protection on the main interface of eScan. While turning it on you can set the parameter to Normal Filter that is Fast with medium level of accuracy or Smart Filter that is slow but has higher level of accuracy.



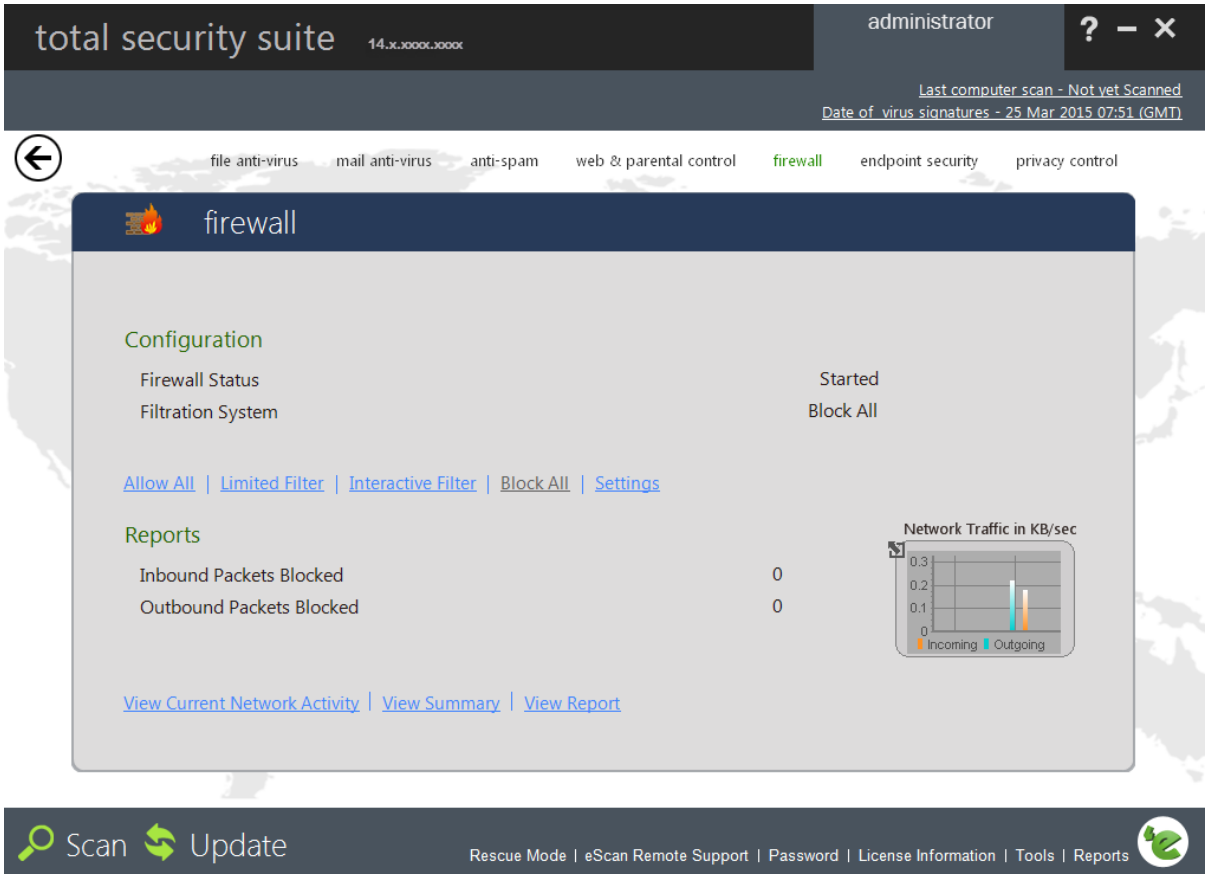
Logs and Reports



Web Protection Module of eScan also maintains a Log of Web Access Violations, Pop ups Blocked as well as a detailed report of Web Protection activity. This can be accessed by clicking on the desired links present on eScan interface under Web Protection Module.

Firewall

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.



Available Modes:

- **Allow All** - It will filter all incoming as well as outgoing traffic
- **Limited Filter** – [**Default**] 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

Benefits of the Firewall feature

You expose your computer to various security threats on connecting to the internet. 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 email

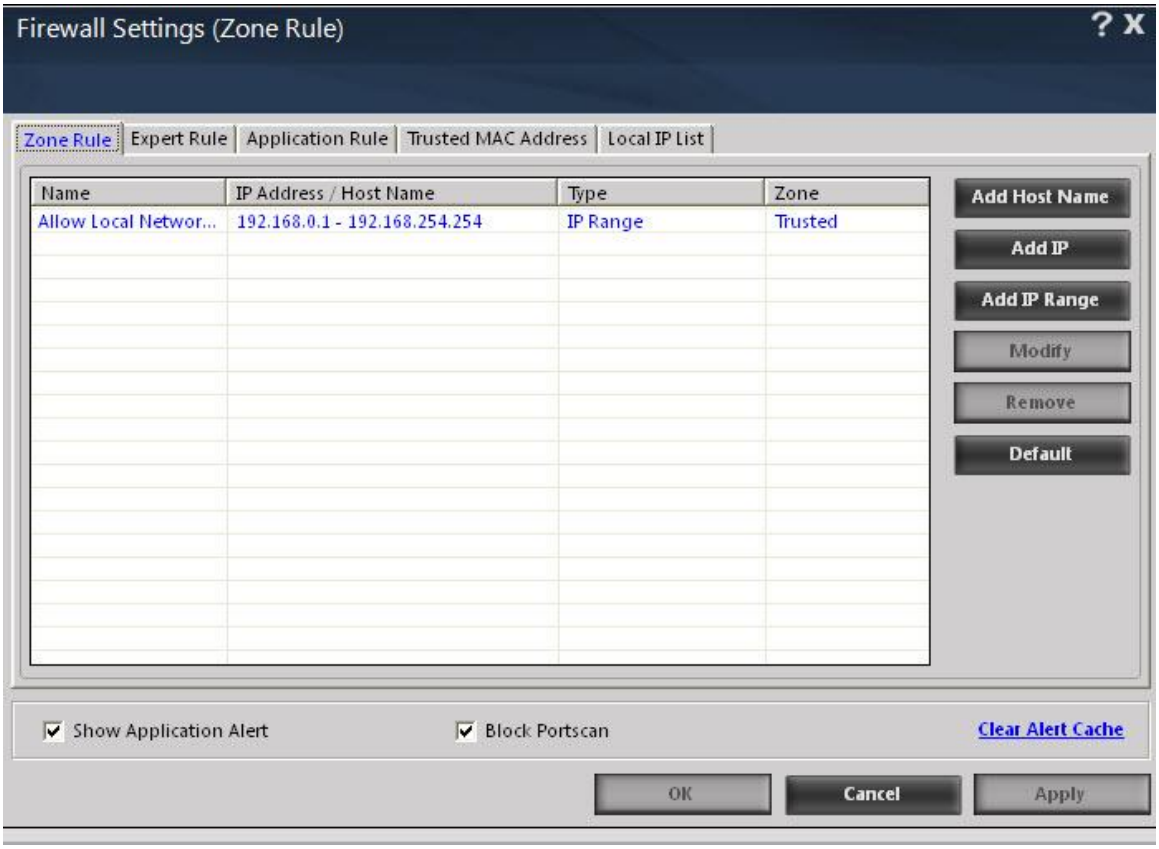
Configuring Settings for Firewall

Firewall protects your system from inbound or outbound un-authorized connection attempts, it can happen through a local network or through internet. It keeps a track of connection attempts and decides which to allow and which to block.

eScan uses a set of rules for allowing or blocking access to your computer. These rules are categorized into **Zone Rule**, **Expert Rule**, **Application Rule**; you can also define a list of Mac addresses that are trusted. It also allows you define Local IP list.

Defining Zone Rule

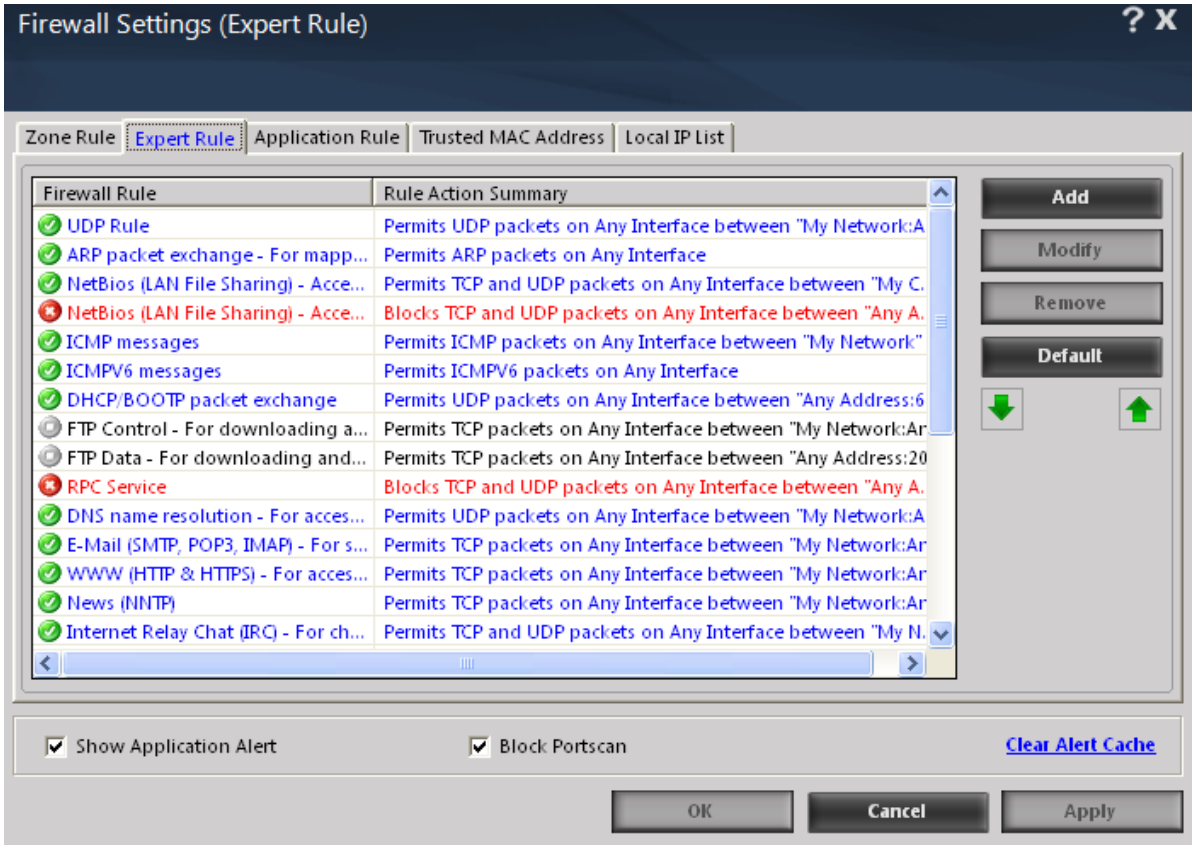
Using this tab you can configure network access rules that specify which IP address, host name, or IP range of computers can access your computer.



This tab gives you following options

- **Add Host Name -** Click this option to define a zone rule for a specific host. Provide a name of the host to add the zone rule; the type of zone, whether it is **Trusted** or **Blocked** and specify a name for the zone rule. Click **OK**.
- **Add IP-** Click this option to add a zone rule for a specific IP address. Provide the IP address for which you wish to add the Zone rule, the type of Zone, whether it is **Trusted or Blocked** and specify a name for the Zone rule, click ok.
- **Add IP Range-** Click this option to add a zone rule for a range of IP addresses. Provide the range of IP address to be added to the Zone rule, also provide the starting IP address to ending IP address; the type of Zone, whether it is **Trusted** or **Blocked** and specify a name for the Zone rule. click **OK.**
- **Modify-** Click this option to modify or make changes in any of the rules created by you. To do so first click on the rule and then click on the Modify button on the interface, you will be forwarded to the Modify Zone window. Make desired changes and click OK. All changes made will be saved in the Rule.

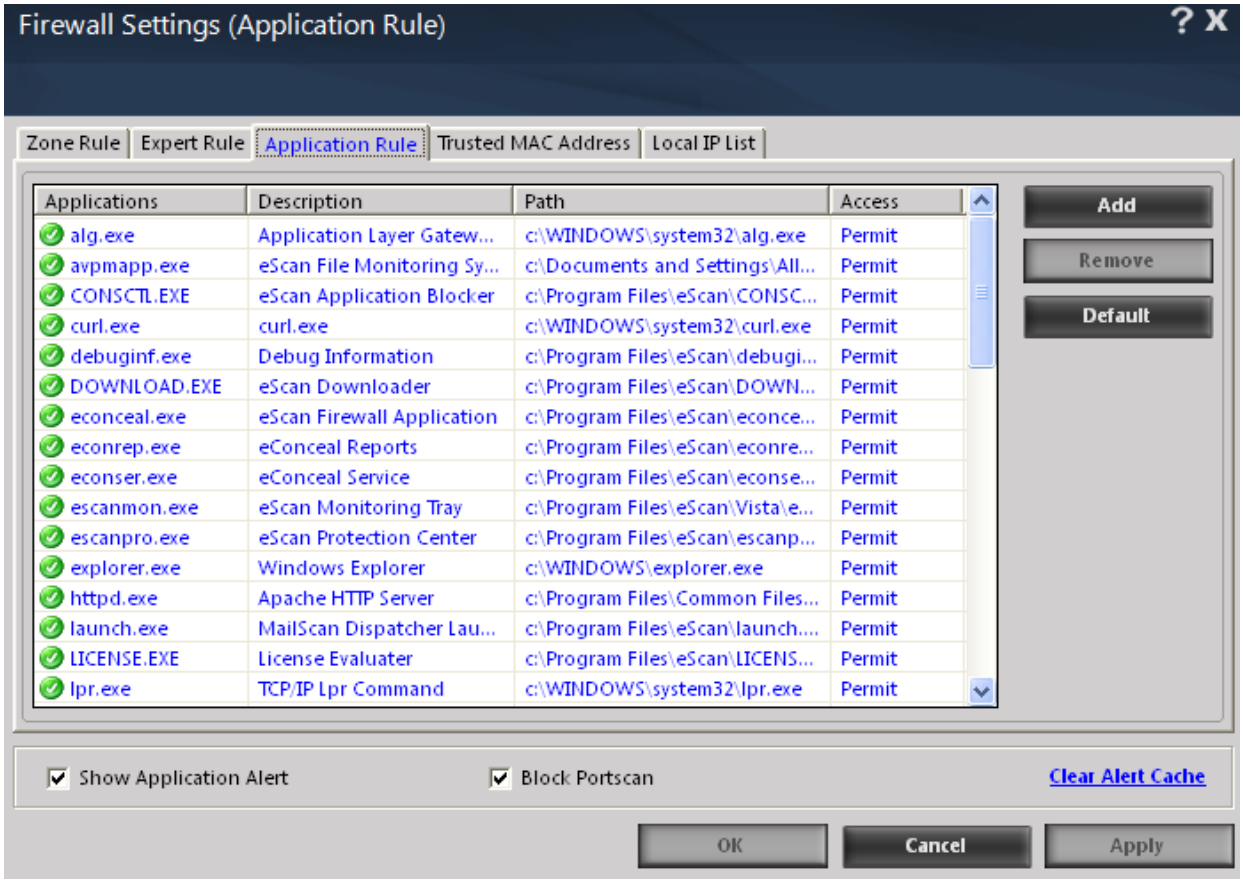
Defining Expert Rule



Using this tab you can specify advanced rules and settings for the eScan firewall. Here you can permit or block traffic based on protocols used by them, its origination be it LAN or WAN, source IP Address, the port number or range from where it originated, the destination where it is routed to i.e. – the destination IP address / range or the destination port number/ range. You can also define **Advanced** settings for ICMP type. You can also **Modify, Delete** or **Disable** any existing Expert by doing a right click on the selected rule.

Defining 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. This tab provides you with a default list of rules and options for configuring application rules. For defining or redefining an Application rule you can use the following options –



- **Add -** Use this option to define a rule for any application. You can do so by browsing the EXE of the application and select the desired permissions to Permit, Deny or Ask on any kind of network or internet access by this application. The rule will be added instantly.
- **Remove –** For removing any rule present in the Application Rule list, select the rule and then click Remove button present on the interface. The selected rule will be deleted instantly from the list.
- **Loading Default Application Rule Settings** - Click the Default option present on the screen to load Default Application Rule settings that were pre –defined before any changes were made by you in the rules.

Options present on Right Click on any rule

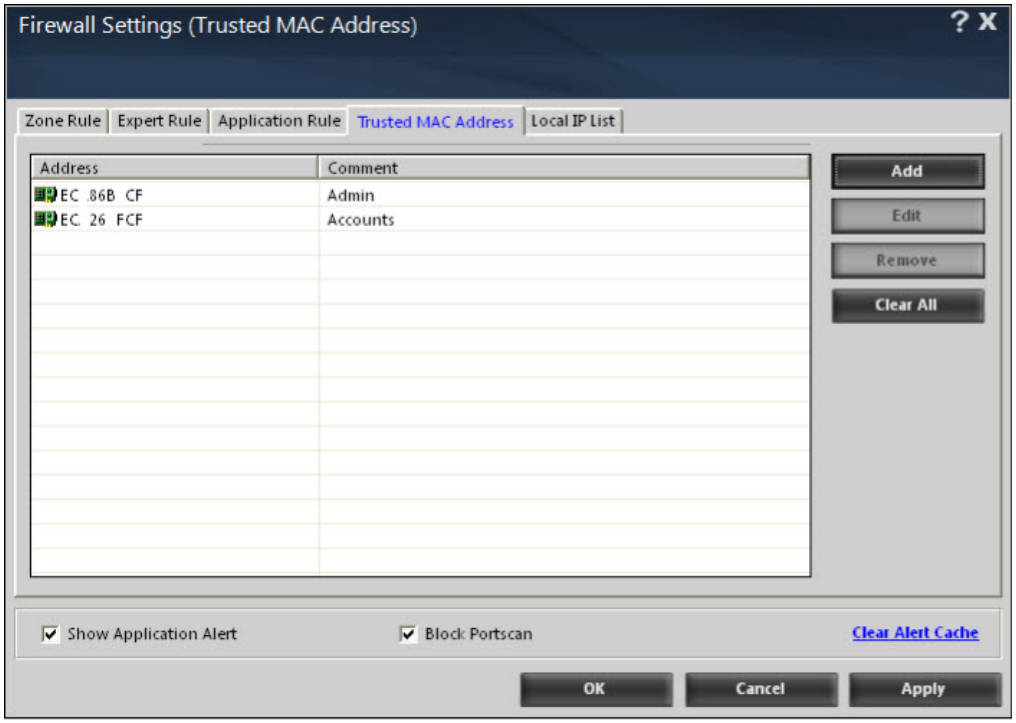
- **Add:** Use this option to Add Application to the Application Rule list
- **Remove:** Use this option to remove any application from the Application Rule list
- **Ask:** Use this option to ask for your permission to permit or deny network access
- **Permit:** Use this option to permit any added Application 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

Additional Options

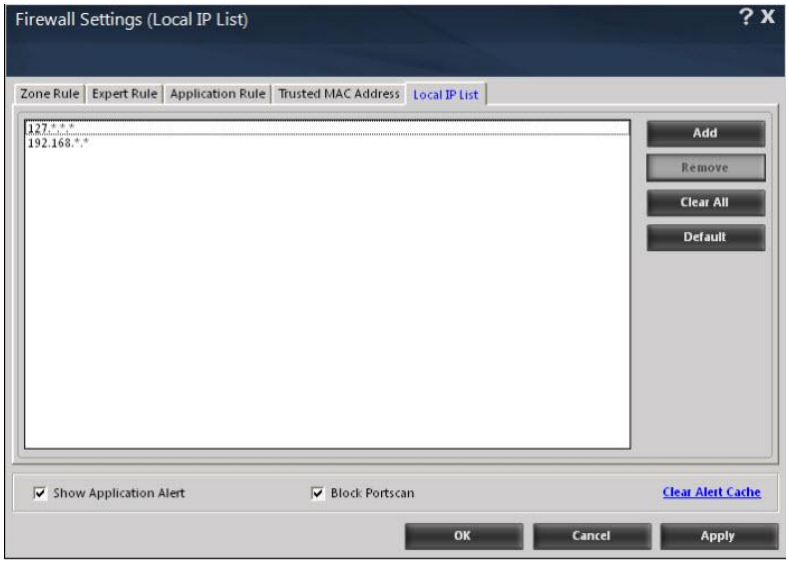
- **Show Application Alert**: [Default] Select this check box, if you want to receive firewall alert when an application is blocked as per an application rule.
- **Block Portscan**: [Default] Select this checkbox, if you wish to block all Portscan attempts made by Hackers.

Adding Trusted MAC Addresses



Using this option, you can create a list of Trusted MAC addresses that will be allowed access of your computer or any application installed on it through internal network or internet. If you have selected / checked "The packet must be from/to a trusted MAC address " at the time of defining Expert Rule then any kind of access will be allowed from or to the trusted MAC addresses only.

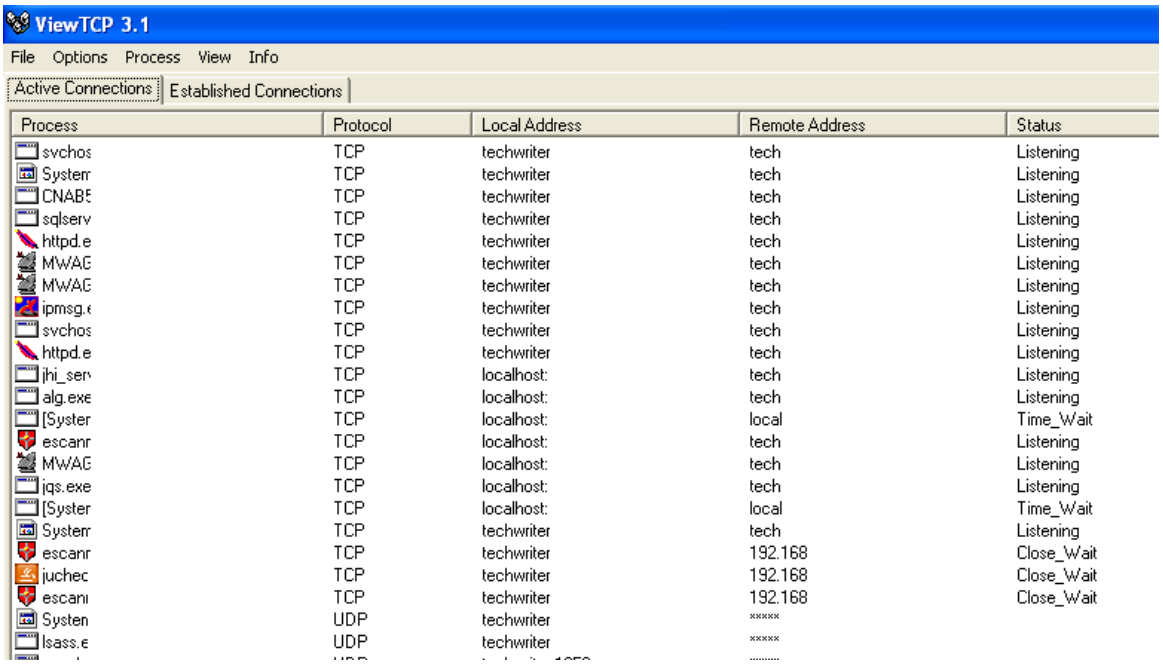
Creating Local IP List



You can create a List of IP Addresses that will be trusted for any kind of access of your system through network or internet. At any time you can Add a new IP Address, Remove an already present IP Address or Clear All IP Addresses present in the List. You can also load the default IP address list using the **Default** option present on the interface.

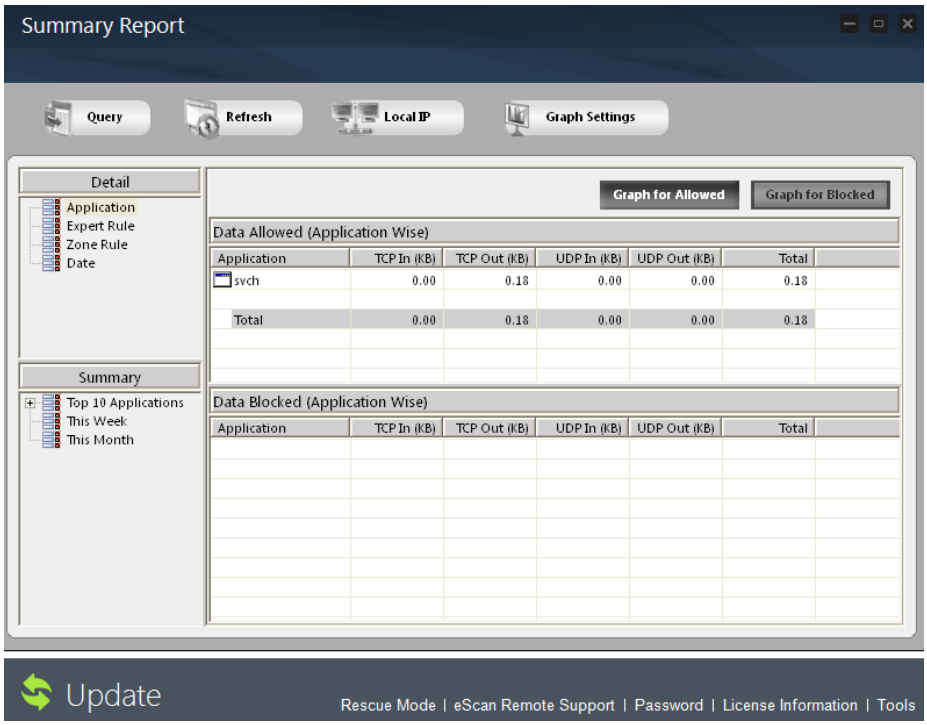
Click **Apply** button after defining the settings for firewall.

Viewing Current Network Activity



Click View Current Network Activity option to open the View TCP tool, it 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.

Viewing Summary

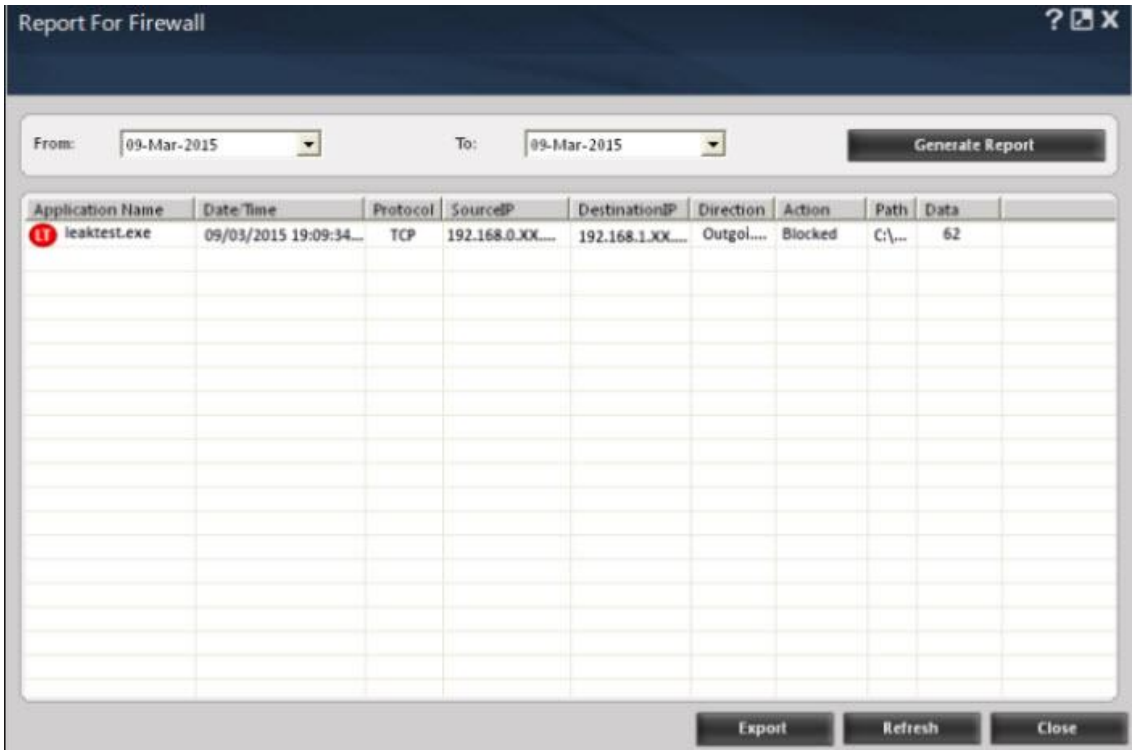


Click this option to view the firewall report either in the form of detailed report or a summary report.

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.

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

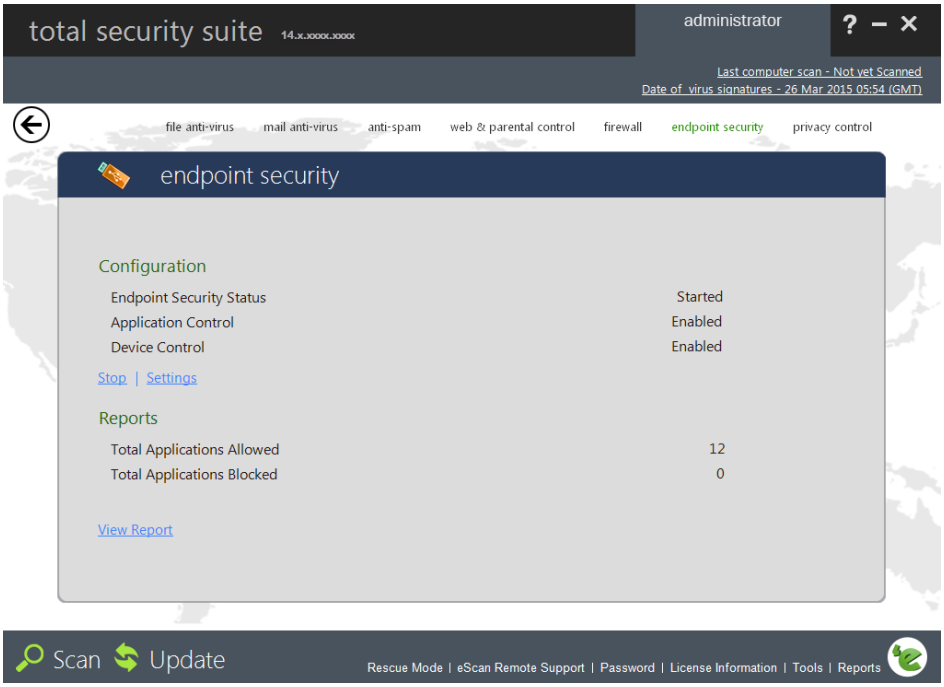
View Report



A detailed report is generated for tracking the Firewall activity that can be accessed by clicking on the **View Report** option present on the interface. The report can be viewed between any two desired dates.

Endpoint Security

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.



Turning on/off Endpoint Security

- Open eScan Protection Center
- Click **Endpoint Security** option present on the interface
- Now click **Start/ Stop** option to enable or disable Endpoint Security, as desired

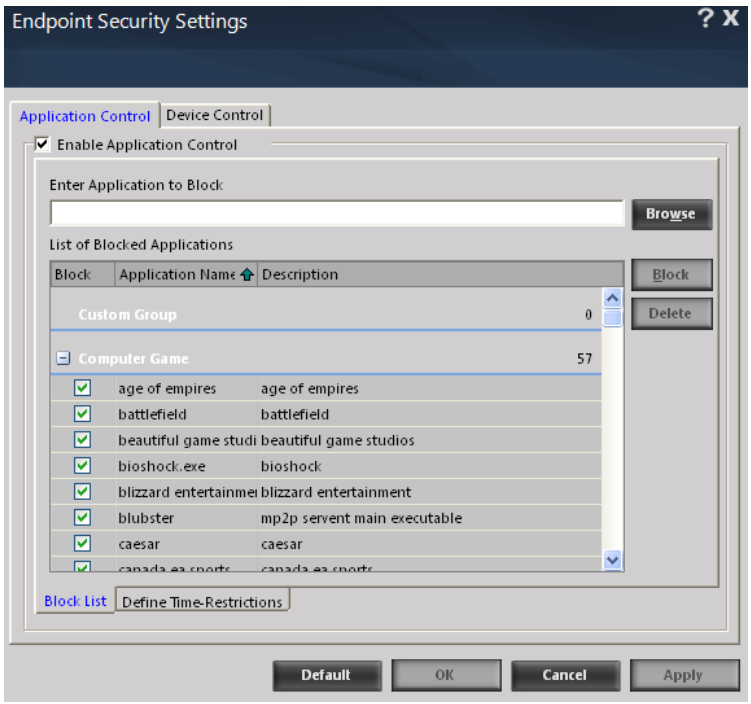
Configuring Settings for Endpoint Security

You can configure following settings for Endpoint Security.

Configuring Application Control

- Click the settings option present under Endpoint Security Module on the main interface of eScan. You will be forwarded to the Application Control on Endpoint Security Settings Window.

- Click "Enable Application Control" option to configure and start Endpoint Security to control/ Monitor execution of desired files on your computer. Using this tab you can Add / Modify a list of block listed executable files or Add / Modify a list of whitelisted executable files for your computer. It also allows defining timeline to allow running or blocking of listed executables during certain time period only.



Steps to Configure Application Control

Click Settings option present on eScan interface under Endpoint Security Module. You will be forwarded to Application Control tab of Endpoint Security Settings window. Using this window you can perform following activities.

This tab helps you configure the following settings.

- **Enable Application Control Section** - 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** - This list contains blocked executables under categories that are predefined by MicroWorld. Each of the applications listed in the predefined categories are blocked by default. In addition, you can also add executables that you need to block to

the Custom Group category. You can unblock an executable by clearing the check box next to it. The predefined categories include the following:

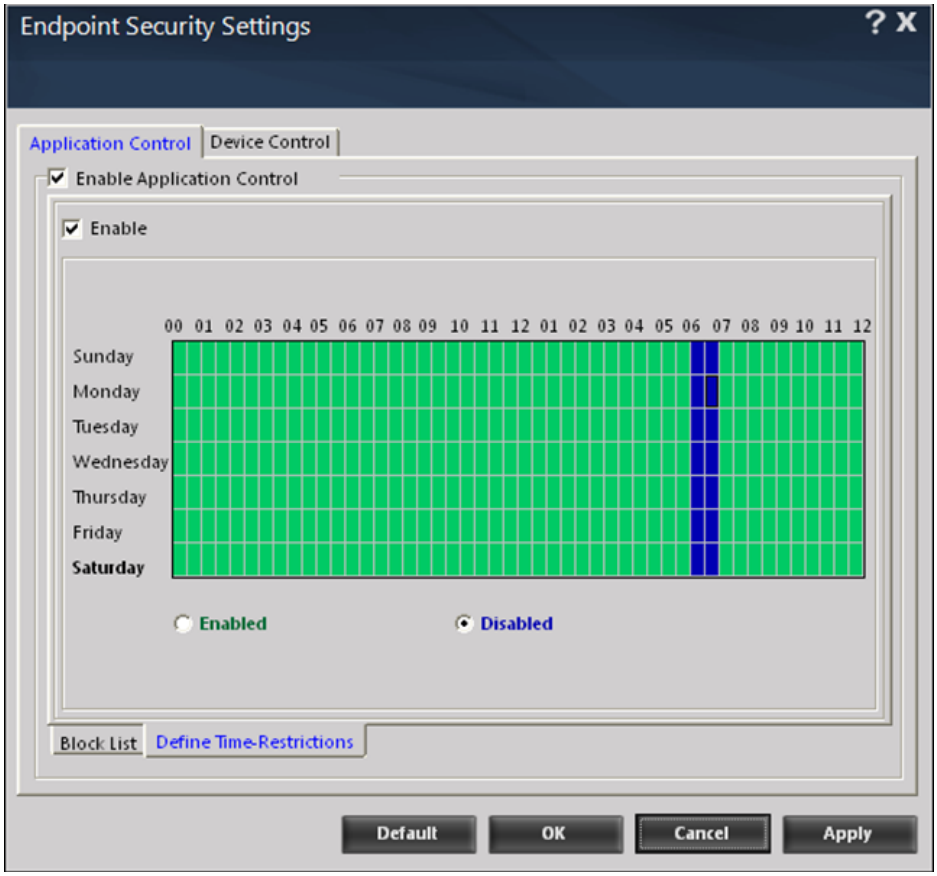
- **Computer Game:** This category contains the list of computer games, which are locked by default.
- **Instant Messengers**: This category contains the list of instant messenger programs like Yahoo!® Messenger, MSN® Messenger, which are blocked by default.
- **Music Video Players:** This category contains the list of music video players programs, which are blocked by default.
- **P2P Applications:** This category contains the list of P2P applications, which are blocked by default.

Note:
eScan will detect and block harmful or blocked applications even if they are renamed and given another extension.

The Endpoint Security Settings dialog box also shows these buttons.

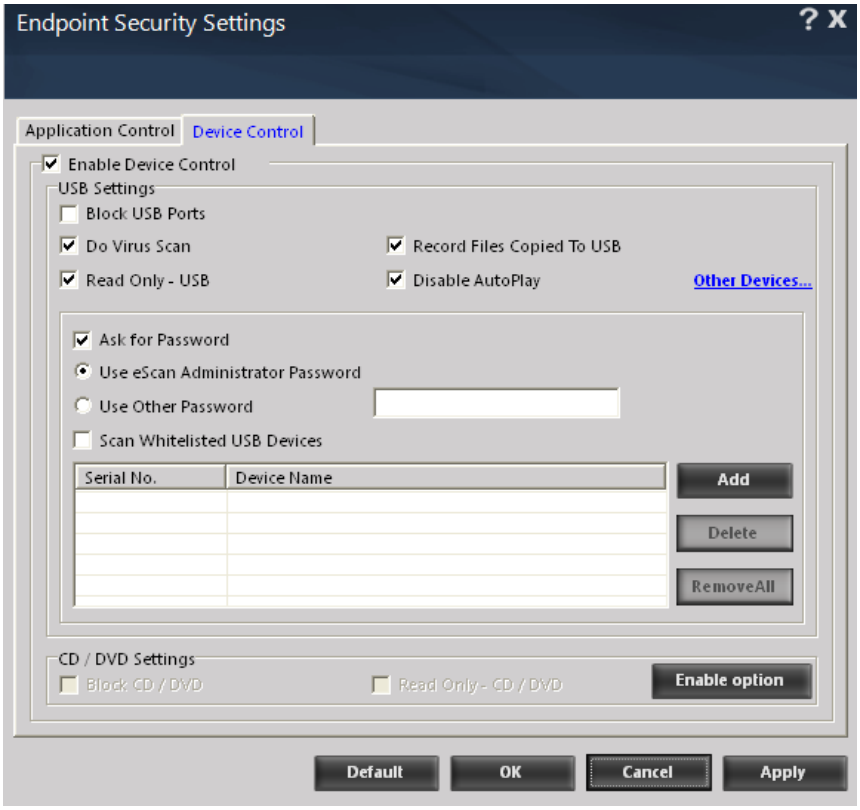
- **Block:** This button blocks the selected application in the Custom Group from running.
- **Delete:** This button deletes the selection application from the Custom Group.

Define Time Restriction: This option will allow you to Enable / Disable application control feature. This feature helps you define time restriction when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day. For example - You can allow your kids to play computer games between 6 - 7 pm without violating the Application Control Policies defined by you, by disabling the module during 6 - 7 PM through Define Time Restriction feature.as shown below.



II. Device Control

The Endpoint Security feature of eScan protects your computer from malicious software that may enter your computer via USB storage devices. It does this by asking you for the password whenever you plug in a USB storage device.



The Device Control tab of the Endpoint Security Settings dialog box helps you configure the following settings.

- **Enable Device Control –** You should select this check box if you need to monitor all the USB storages devices connected to your computer.
- **USB Settings -**This section helps you customize the settings for controlling access to USB storage devices.
- **Block USB Ports -** You should select this check box if you need to block all the USB ports.
- **Do Virus Scan:** Select this checkbox to scan for viruses whenever a USB device is connected to the computer.
- **Record Files Copied to USB:** Select this check box to keep a log of the files that are being copied to the USB.
- **Read only USB-** Select this check box to make the USB read only. If this check box is selected, it will not allow you to edit the files on the USB and you will not be able to copy any files to the USB.

- **Disable AutoPlay:** Select this option to disable the auto play of the USB device. In case of USB devices it will not display the folder structure.
- **Ask for Password** - Select this check box to prompt for a password whenever a USB storage device is connected to the computer. You will not be able to access the USB storage device until you enter the correct password. As a best practice, you should always keep this check box selected.
- **Use eScan Administrator Password:** Select this check box to prompt you to enter the PC password whenever you try to access a USB storage device.
- **Use Other Password -** Select this check box to prompt for a password whenever a USB storage device is accessed. It will allow you to specify a unique password for accessing USB Storage devices.
- **Scan Whitelisted USB Devices:** Select this option to add USB devices to whitelist.
    - **Process to add USB devices to whitelist:**
        - Click **Add** the USB Whitelist window will open**.**
        - Click **Custom** and **add** the **USB device serial numbers** and click **ok.**

          It will also allow you to delete/ remove all the whitelisted USB drives.
- **CD/DVD Settings:** Click on the enable option to enable the CD/ DVD settings. This will restart the system, once restarted the option will be enabled.
- **Block CD/DVD:** Select this checkbox to block any CD/DVD on your system.
- **Read only CD/ DVD:** Select this check box so that any CD/ DVD on the system would be read only.
- **Other Device Settings**
    - **Disable SD Cards:** Select this check box to disable all SD cards accessed through your system.
    - **Disable Imaging Device:** Select this check box to disable all Imaging Devices accessed through your system.
    - **Disable USB Modem:** Select this check box to disable all USB modems connected through your system.
    - **Disable Print Screen:** Select this check box to disable the Print Screen function on your system.

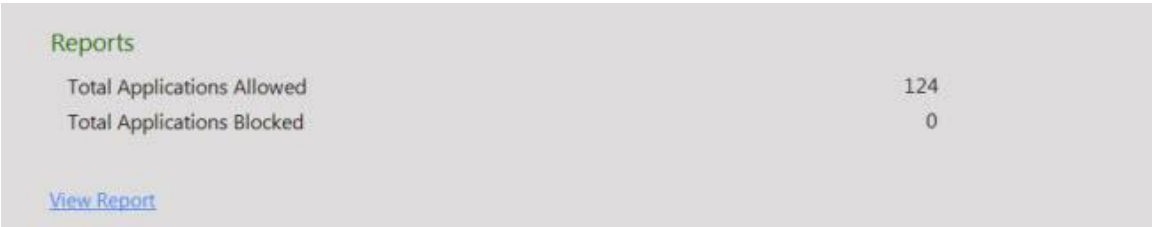
- **Disable Web Cam:** Select this check box to disable all Web Cams connected to your system.
- **Disable Composite USB:** Select this check box to disable all the functions of a composite USB on your system**.**
- **Disable Bluetooth:** Select this check box to disable Bluetooth access on your system.
- **Block Attachments:** Select this check box to block all attachments from opening on your system.
- **Disable WiFi Network:** Select this check box to disable all SD cards accessed through your system.
- **WiFi SSID allowed:** Add the WiFi SSIDs that are to be allowed. Only these WiFi will be allowed and the rest of them will be blocked.
- **Disable Network Printer:** Select this check box to disable the network printers accessed through your system**.**
- **Allowed Printers List:** Add the list of network printers allowed access through your system.

- **Generating Reports**

  eScan generates a report of Applications allowed as well as Applications blocked. This information is displayed under Reports section in Endpoint Security module. You can generate report between two desired dates by clicking on the View Reports option present on the interface. Select the desired dates and click Generate Report button present on the Report for Endpoint Security Window.

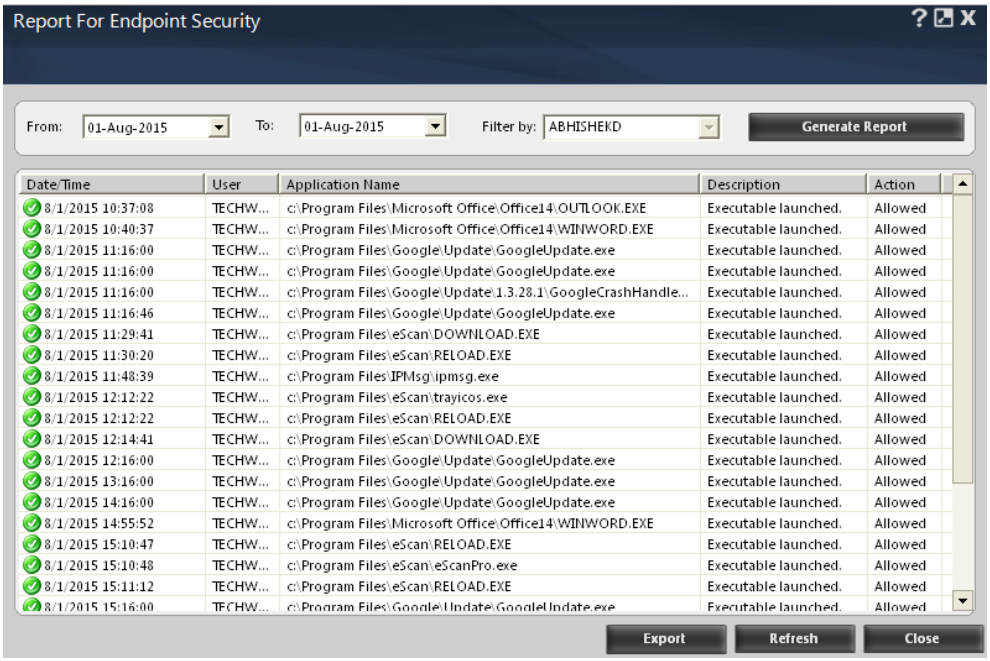
  This section displays the following information.

  - **Total Applications Allowed** - It shows the total number of applications allowed by the Endpoint Security module.
  - **Total Applications Blocked** - It shows the total number of applications blocked by the Endpoint Security module.



In addition, you can view the following reports.

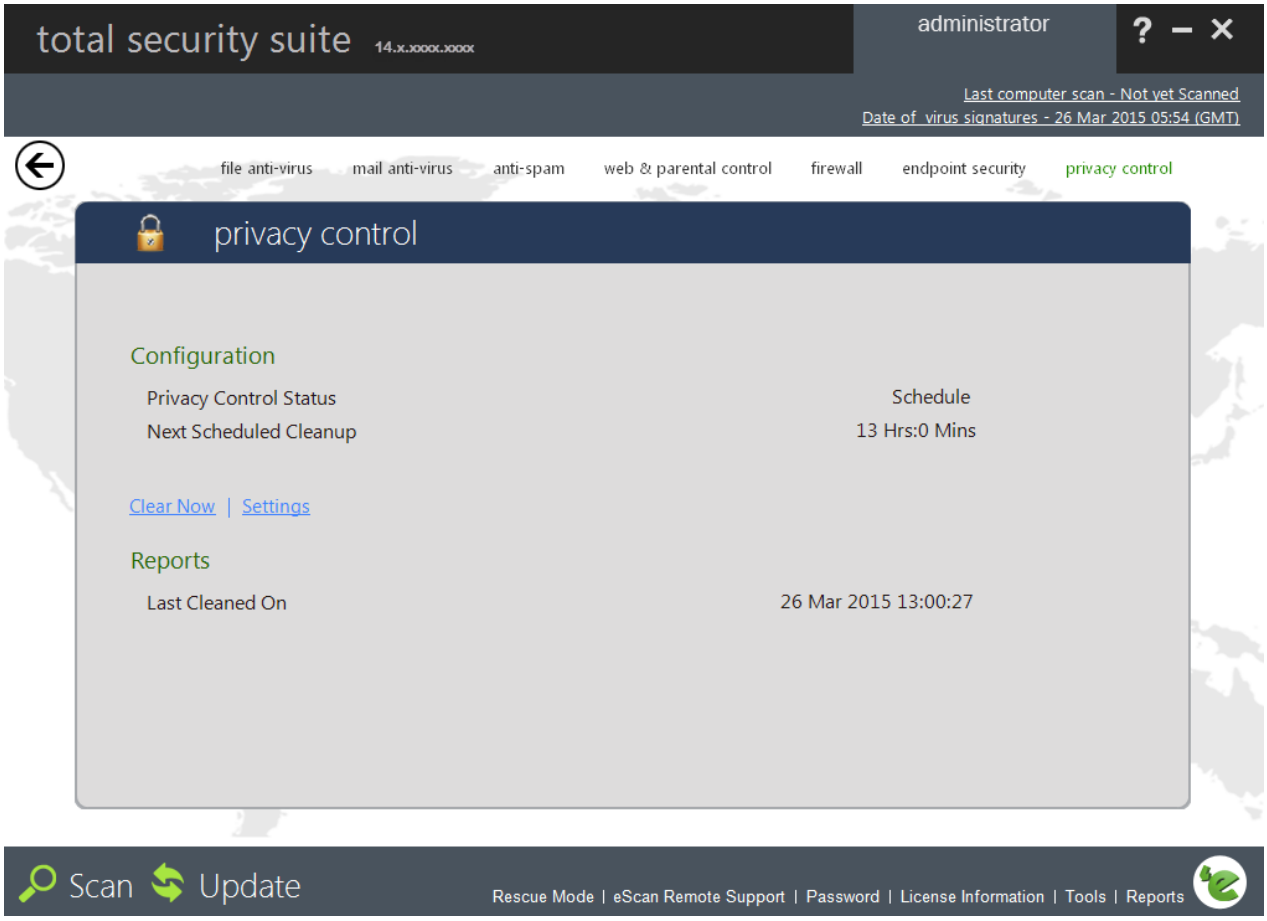
- **View Report** – It will display the report for the Endpoint Security module for a given range of dates in a tabular format when you click the Generate Report button.



Date/Time	User	Application Name	Description	Action
8/1/2015 10:37:08	TECHW...	c:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE	Executable launched.	Allowed
8/1/2015 10:40:37	TECHW...	c:\Program Files\Microsoft Office\Office14\WINWORD.EXE	Executable launched.	Allowed
8/1/2015 11:16:00	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed
8/1/2015 11:16:00	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed
8/1/2015 11:16:00	TECHW...	c:\Program Files\Google\Update\1.3.28.1\GoogleCrashHandle...	Executable launched.	Allowed
8/1/2015 11:16:46	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed
8/1/2015 11:29:41	TECHW...	c:\Program Files\eScan\DOWNLOAD.EXE	Executable launched.	Allowed
8/1/2015 11:30:20	TECHW...	c:\Program Files\eScan\RELOAD.EXE	Executable launched.	Allowed
8/1/2015 11:48:39	TECHW...	c:\Program Files\IPMsg\ipmsg.exe	Executable launched.	Allowed
8/1/2015 12:12:22	TECHW...	c:\Program Files\eScan\trayicos.exe	Executable launched.	Allowed
8/1/2015 12:12:22	TECHW...	c:\Program Files\eScan\RELOAD.EXE	Executable launched.	Allowed
8/1/2015 12:14:41	TECHW...	c:\Program Files\eScan\DOWNLOAD.EXE	Executable launched.	Allowed
8/1/2015 12:16:00	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed
8/1/2015 13:16:00	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed
8/1/2015 14:16:00	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed
8/1/2015 14:55:52	TECHW...	c:\Program Files\Microsoft Office\Office14\WINWORD.EXE	Executable launched.	Allowed
8/1/2015 15:10:47	TECHW...	c:\Program Files\eScan\RELOAD.EXE	Executable launched.	Allowed
8/1/2015 15:10:48	TECHW...	c:\Program Files\eScan\eScanPro.exe	Executable launched.	Allowed
8/1/2015 15:11:12	TECHW...	c:\Program Files\eScan\RELOAD.EXE	Executable launched.	Allowed
8/1/2015 15:16:00	TECHW...	c:\Program Files\Google\Update\GoogleUpdate.exe	Executable launched.	Allowed

Privacy Control

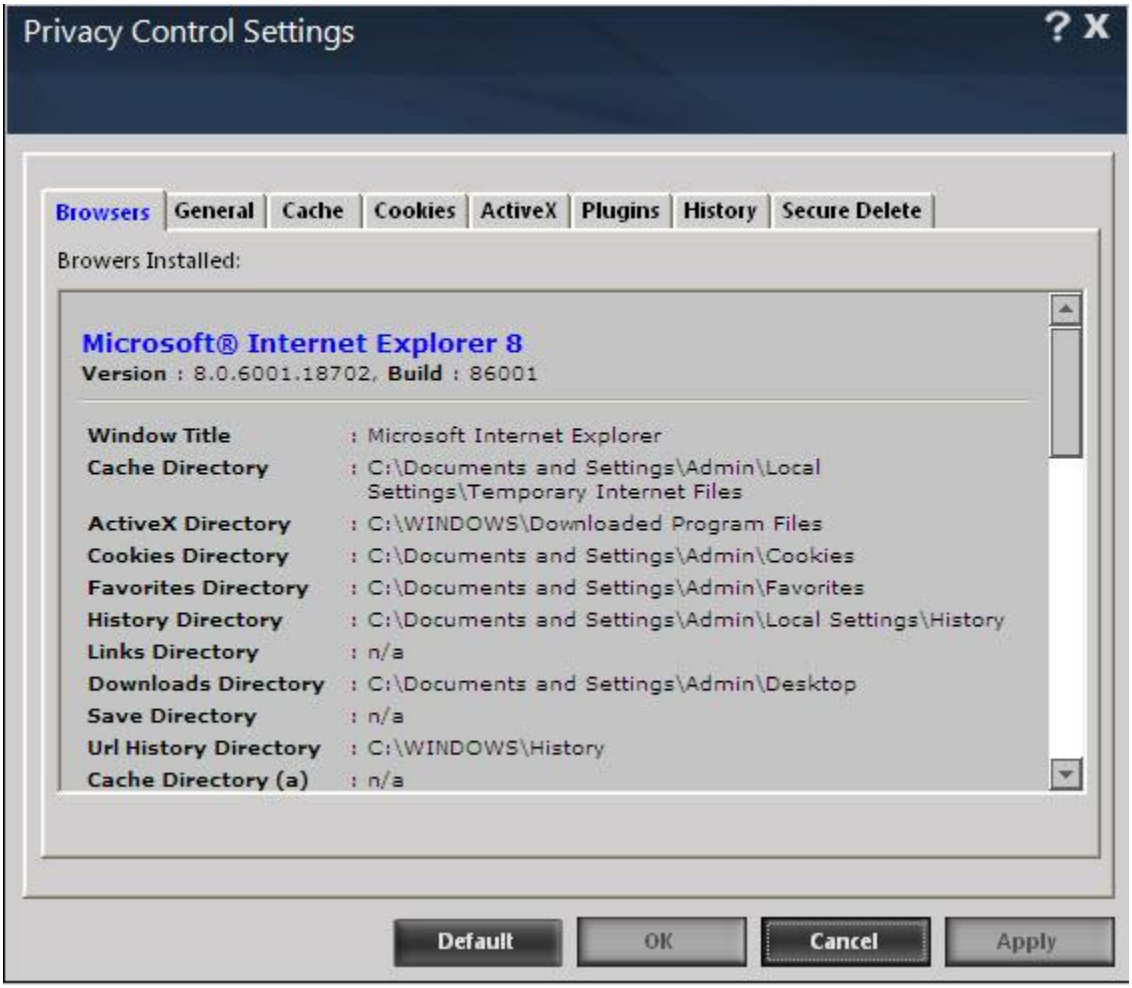
Privacy Control protects your private information from various threats by deleting all temporarily stored information. This module comes with the Browser Cleanup feature that allows you to use the Internet without leaving any history or residual data on your hard drive by erasing details of sites and Web pages you have visited while browsing.



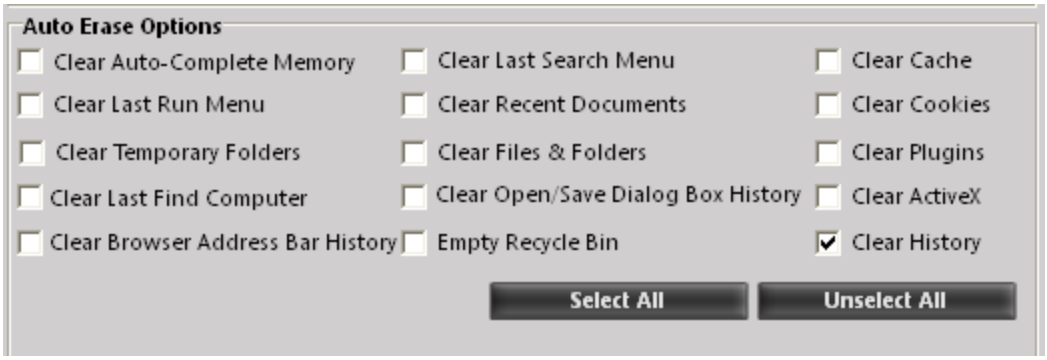
Using Privacy Control

Privacy control options can be run manually or scheduled at a desired time of the day or on system start up. The scheduling can be done using the **General** tab present on the Privacy Control Window. The Privacy Control settings window shows following –

- **Browsers:** It will display the list of Browsers installed on Computer. The browser stores all the traceable information of the websites that you have visited. This option displays the entire traceable component and the path where these temporary data is stored on your computer.



- **General:** The general tab will display the Auto-Erase options and will also allow you to set the time as to when you want to run the auto-erase options. The browser stores traceable information of the web sites that you have visited on your computer. This information can be viewed by others. eScan allows you to remove all traces of web sites that you have visited through the auto-erase option.



Using the Auto Erase options you can perform the following tasks –

- **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:** Select this check box to clear the information in the Run dialog box.
- **Clear Temporary Folders:** Select this check box to clear 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:** Select this check box to clear name of the computer that you searched last.
- **Clear Browser Address Bar History:** Select this check box to clear Web sites from the browser's address bar history.
- **Clear Last Search Menu:** Select this check box to clear name of the objects that you last searched for by using the Search Menu.
- **Clear Recent Documents:** Select this check box to clear names of the objects found in Recent Documents.
- **Clear Files & Folders:** Select this check box to delete 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:** Select this check box to clear the links of all the opened and saved files.
- **Empty Recycle Bin:** Select this check box to clear the Recycle Bin. You should use this option with caution because it permanently clears the recycle bin.
- **Clear Cache:** Select this check box to clear the Temporary Internet Files.
- **Clear Cookies:** Select this check box to clear the Cookies stored by Web sites in the browser's cache.
- **Clear Plugins:** Select this check box to remove the browser plug-in.
- **Clear ActiveX:** Select this check box to clear the ActiveX controls.
- **Clear History:** Select this check box to clear the history of all the Web sites that you have visited. You can choose to run these options on system start-up or you can choose to run these options every day at a particular time of your choice.
- **Advanced:** This option is displayed in the general tab and using this option you can clean up history of MS Office Files, Windows Files or Media Player files. You can also Add desired cookies to exclusion list stored on your computer for Internet Explorer.

Similarly you can also remove desired cookies from the exclusion list if required. All cookies in the exclusion list will not be deleted / cleaned during system clean up using eScan.

- **Cache:** This tab displays the list of files stored in the Temporary Internet Files folders in a tabular form. The table displays information such as the URL of the Web page, number of hits, size of the Web page, date of creation, date of modification, date of access, and the path where the page is downloaded and stored on the computer.

- **Cookies:** This tab displays the list of cookies installed on your computer. The table displays information such as the name, number of hits, size, date of modification, date of access, date of expiry, and full path of the cookie file.

- **ActiveX:** This tab displays the list of ActiveX controls installed on your computer. The table displays information such as the name, size, date of creation, date of modification, date of access, full path, version, description, company, and comments.

- **Plugins:** This tab displays the list of plug-in installed on your browser. The table displays information such as the name, size, date of creation, date of modification, date of access, full path, version, description, company, and comments.

- **History:** This tab displays the list of Web sites that you have visited and the files that you have opened. The table displays information such as the name, size, date of creation, date of modification, date of access, and full path of each file.

- **Secure Delete:** You can use this option to prevent misuse or recovery of the files that were deleted by you. For this, Add the files that you wish to permanently delete from your computer to the deletion list by browsing the file using the options present on the window. You can also use Add files or Add Folder option when you right click on the deletion list area. After Adding desired Files/ Folders for deletion click Delete Files /Folders option present on the right click menu and confirm by clicking Yes button on the window that pops up on the screen.

Cloud Protection

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. In case of new malwares, it makes a prompt response with an advanced level of detection that provides superior protection.

Basics of cloud-based eScan Security Network

- Continuous global monitoring of threats on real-time basis and immediate delivery of collected data to eScan host servers.
- Analysis of collected data and the creation of protection measures against new threats, and the fast distribution of those measures to users.
- 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.

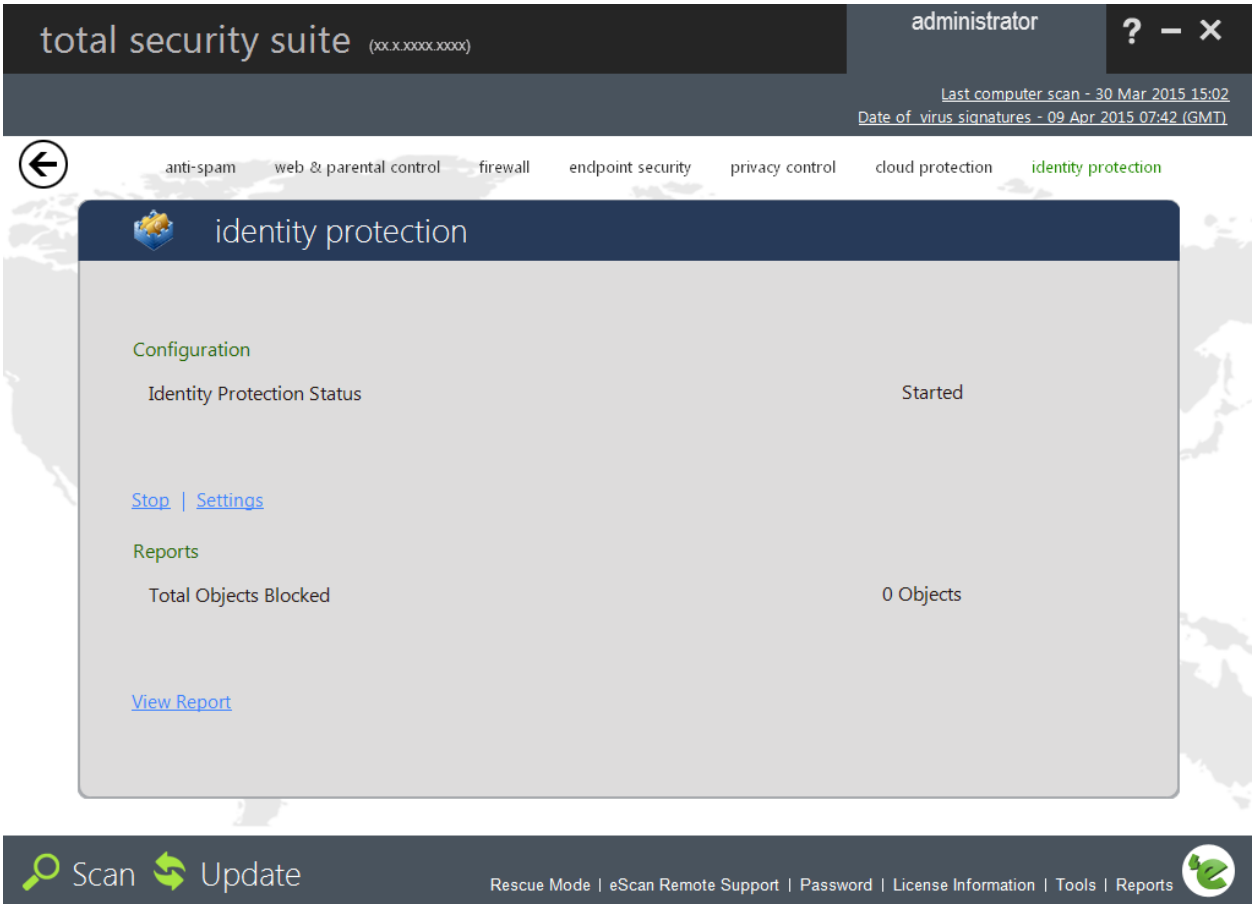
Note:
The user of any one of eScan SOHO products has to agree to participate in the system and this is done strictly voluntarily and confidentially. In any case, strict confidentiality is maintained and no personal information, such as user names, passwords, or any other personal details are collected.

- The decision on the safety of a program is made based on internal algorithms like the file is having a valid digital signature or not and number of other factors.
- As soon as a program is declared malicious or unsafe, the information becomes available to eScan product users even before the signature for that piece of malware is created and updated on their computers.

  Thus, eScan clients receive prompt information about new and unknown threats minutes after the launch of a cyber-attack, compared to hours for traditional signature database update. You need to have internet connection, to access Cloud Protection.

Identity Protection

Identity Protection will prevent data theft. It will protect sensitive personal information, such as credit card numbers or passwords for online services. Upon detecting any attempt to send protected information to the Internet, whether to a web page, by email or through an instant message, the transmission can be blocked automatically.



Data Theft Prevention monitors HTTP traffic (ports 80, 81, 8080, and any proxy server port you configure in your Microsoft® Internet Explorer® settings), but not HTTPS traffic (encrypted information cannot be filtered).

Supported Software

Data Theft Prevention works with the following software:

- Microsoft® Internet Explorer® 7.0 or 8.0
- Mozilla® Firefox® 3.0 or above
- Google Chrome 3.0 or above

- AOL® Instant Messenger™ (AIM®) 6.8 or 6.9, Windows Live™ Messenger 8.1 or 9.0, Yahoo!® Messenger 8.0, 9.0 or 10.0
- Microsoft Outlook and other SMTP email programs

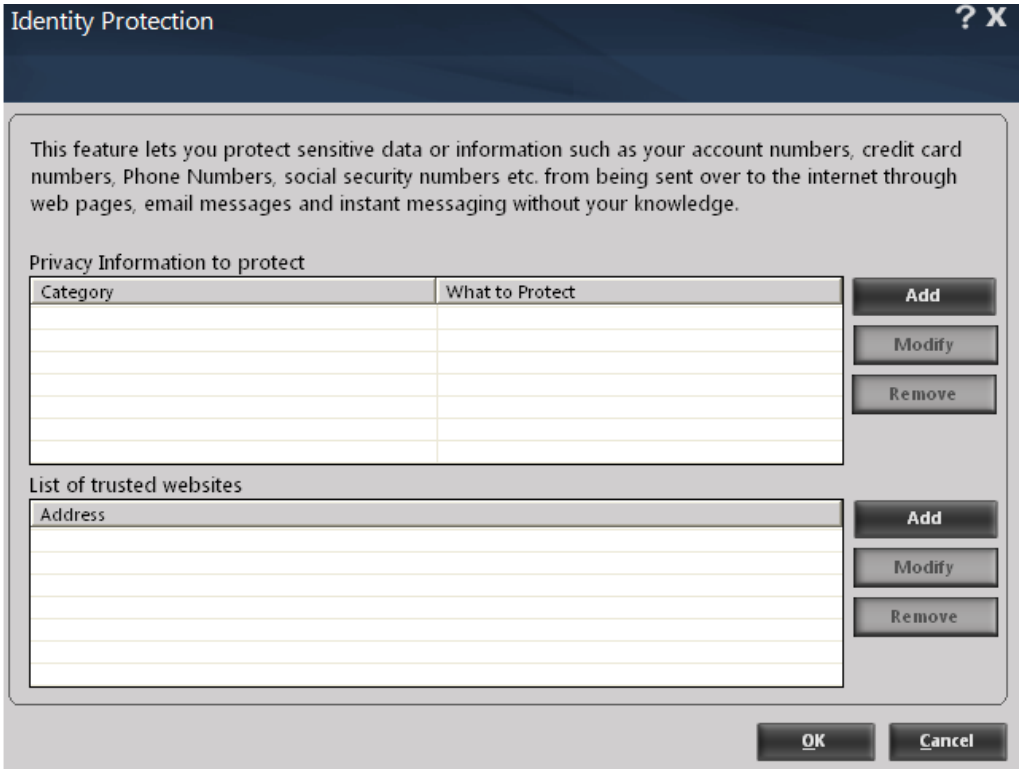
Using Data Theft Prevention

This feature can only protect information that you have defined. However, you do not need to enter a complete credit card, bank account, or Social Security number to gain this protection. As few as four of the digits entered in the correct order can stand for and effectively protect the entire sequence.

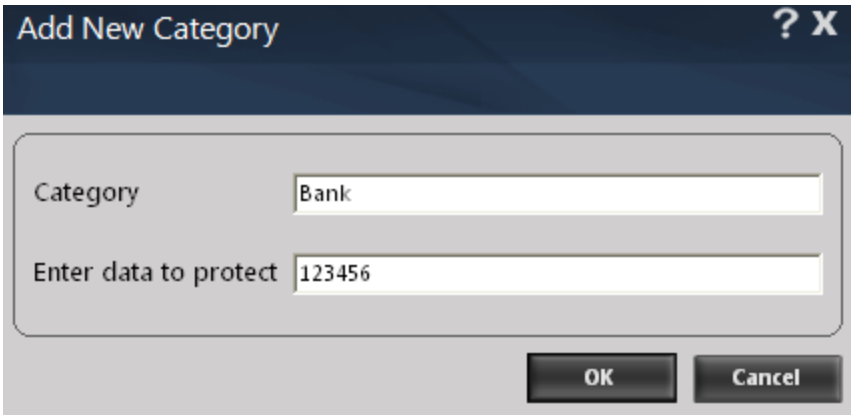
This module helps you protect your confidential data / information from being sent from your system. It can be your bank information (Account number) or your social security number that you have saved on your system in a text format.

Steps for Adding information to be protected –

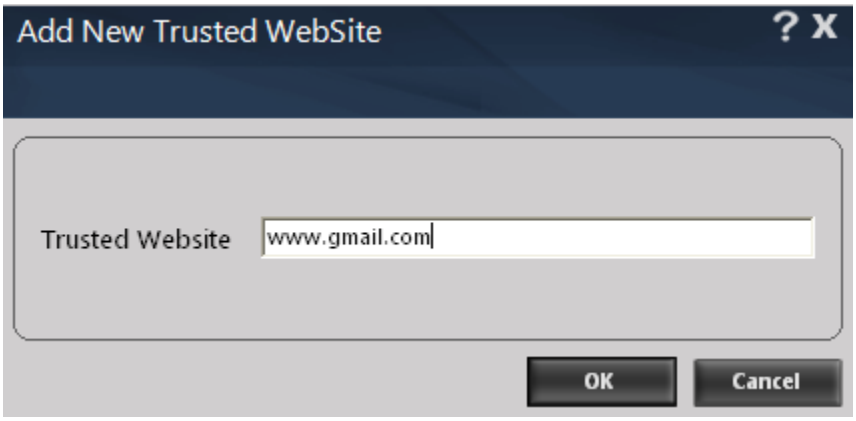
1. Click the Setting option present on the Identity Protection window. A new window will open as shown below.



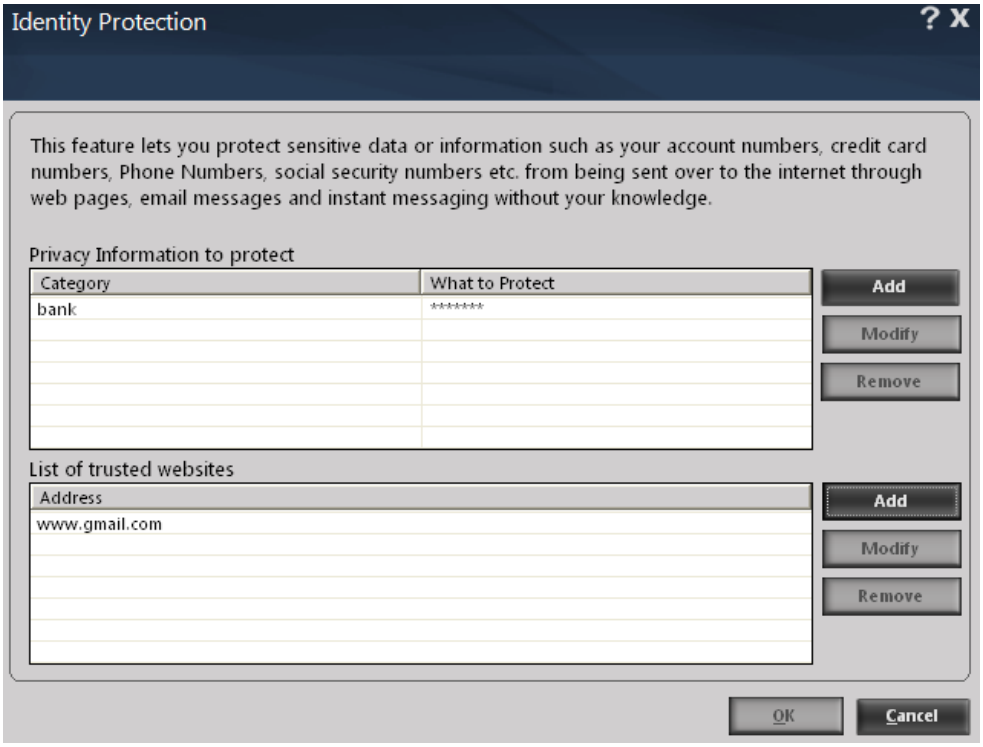
2. To save some category of information, click Add on the category section and a new window will be opened as shown below.



3. Enter the category of the data and the data to be protected. The category will be created and the information to be protection will be encrypted.
4. Click Ok; the entered information cannot be sent over internet through any means from your computer. It will be blocked and a report will be generated.
5. To add a list of trusted websites, Click Add and a new window will be opened as below.

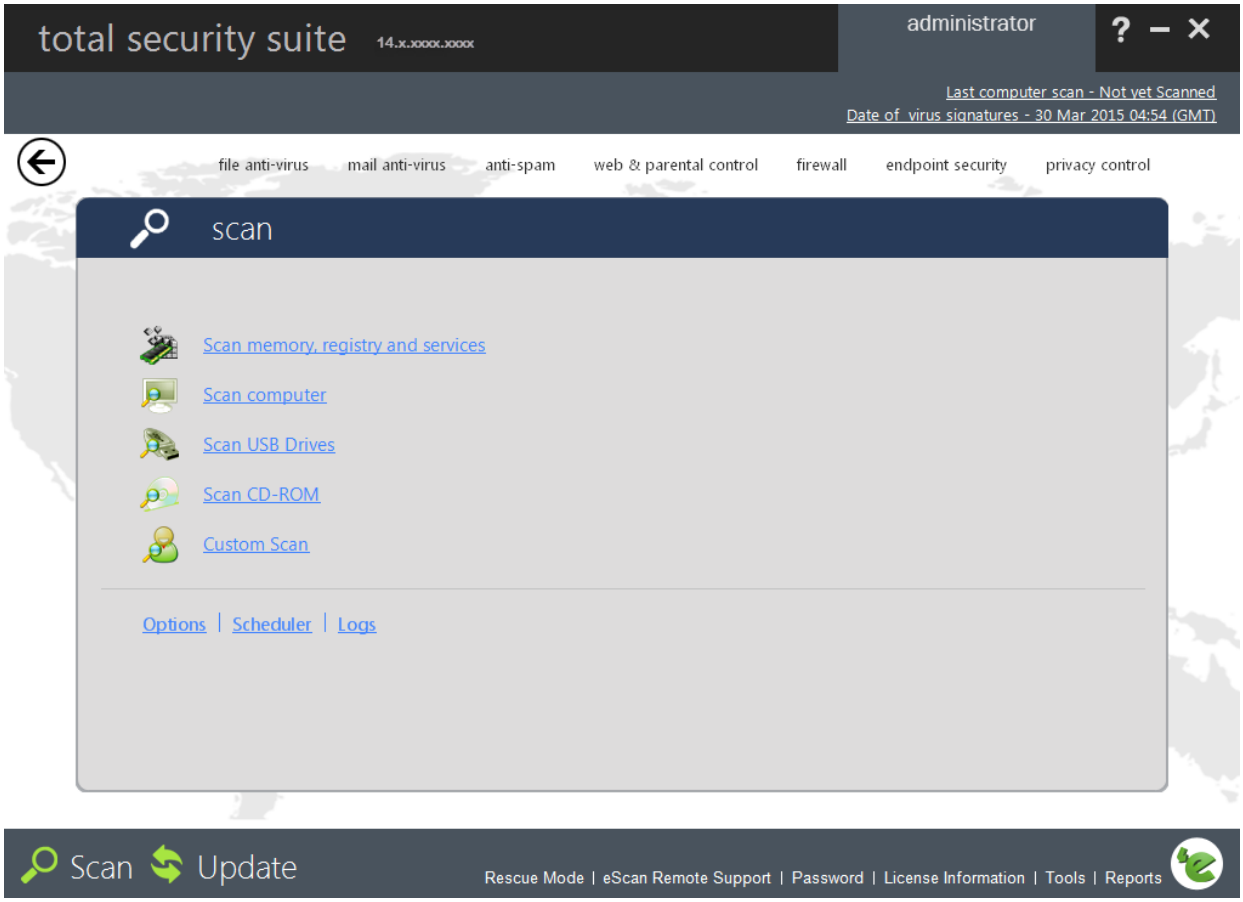


6. Enter the website address. This website will be added to your list of trusted websites.
7. Click **ok**. In case you want to send these details to anyone, you can send it only through one of the trusted websites added by you.


Identity Protection
? X
This feature lets you protect sensitive data or information such as your account numbers, credit card numbers, Phone Numbers, social security numbers etc. from being sent over to the internet through web pages, email messages and instant messaging without your knowledge.
Privacy Information to protect
Category
What to Protect
bank
****
Add
Modify
Remove
List of trusted websites
Address
www.gmail.com
Add
Modify
Remove
OK
Cancel

Scan

You can manually scan your computer for any kind of virus or malware infection using the **Scan** option present at the bottom of the eScan Window. It gives you a set of Customized options for scanning. You can do an on demand scan or a scheduled scan along with this. It also gives options to define **Actions**, **Alerts** and **Priority** of the defined task of scanning.



On Demand Scan

Scanning Memory Registry and Services

1. Click Scan option present at the bottom of eScan Interface.
2. Now click "*Scanning Memory Registry and Services*" option present on the interface.
3. Scanning will start instantly, eScan shows the Summary of the scanning in progress on a real time basis on the Virus Scan Window that will pop up on the screen. It will also display the details of the infected file along with the Virus name and its cleanup status.

4. You can also prioritize the scanning in Progress to Low or Normal using the options present on the Virus Scan Window.

Scan Computer

- Click Scan Computer option for Scanning all drives attached to the computer and Partitions of the Hard Disk.

Scan USB Drives

- Click Scan USB Drives to scan USB cards or drives attached to the computer.

Scan CD - ROM

- Click Scan CD - ROM option if you wish to scan CD ROM inserted in the CD ROM drive of the computer

Custom Scan

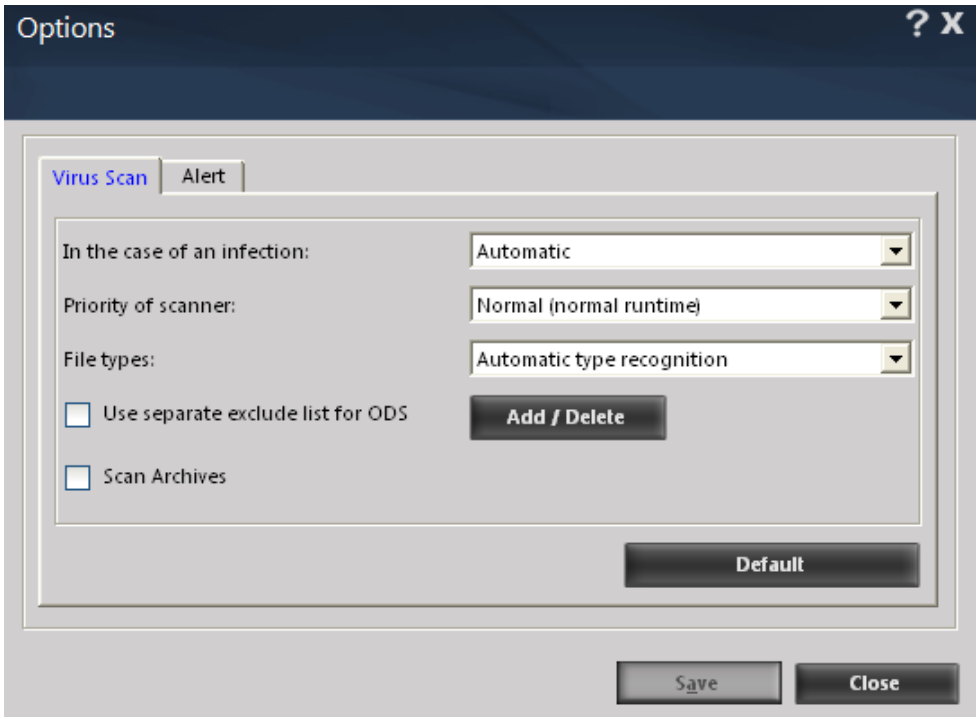
- Click Custom scan for a customized scan of your computer. It will allow you to do the following:
  - Scan CD-ROM
  - Scan Spyware and Adware
  - Scan memory, registry and service
  - Scan local hard drives
  - Scan USB Drives
  - Scan Startup
  - Scan specific directories and files

Options

You can configure **Scan** options by clicking the **Options** button. This will display the **Options** dialog box that provides you with options for configuring the Scan module. This dialog box has two panes: Virus Scan and Alert.

Virus Scan

This will help 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.



- **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.

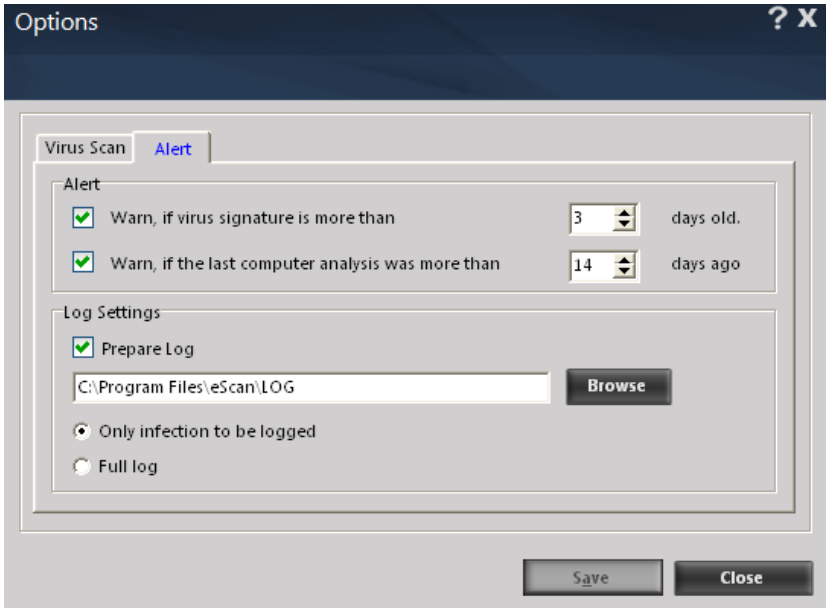
This option helps eScan to separate the exclude list of on-demand scanning from real-time scanning exclude list.

- **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.



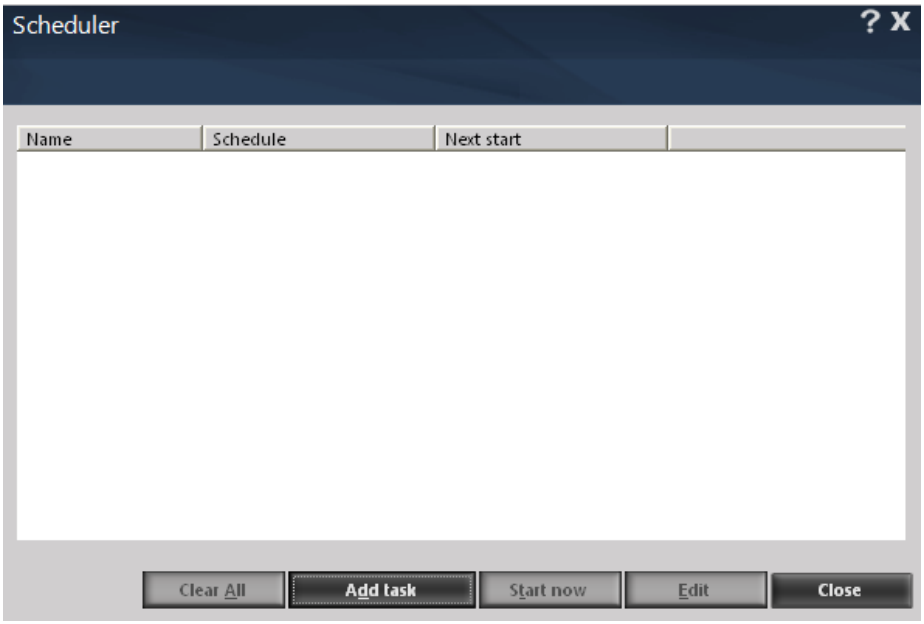
- **Alert:** In this section, you can configure when eScan should notify you when the virus definitions are outdated or when a specified number of days have elapsed since you have last scanned your computer.

  - **Warn, if virus signature is more than:** [Default] 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:** Select this check box, eScan will notify you when a specified number of days have elapsed since the computer was last analyzed. By default, the value is 14.
- **Log Settings:** In this section, you can configure the log settings for the Scan module.
- **Prepare log: [Default] S**elect 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]** 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:** This option is selected; the On-demand Scan log will contain information about all the files scanned by eScan.

Scheduler

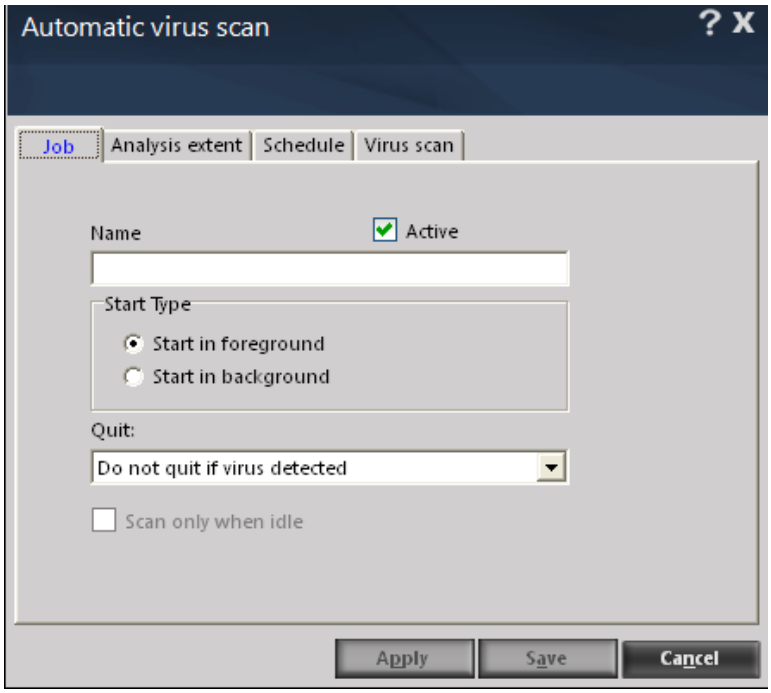
You can schedule on-demand Scan to scan your computer and storage devices for malicious objects. It contains a table, which displays name of the schedule, frequency of occurrence, and the next time it will be run. This dialog box includes an **Add task** button that helps you add a new scan task to the schedule.



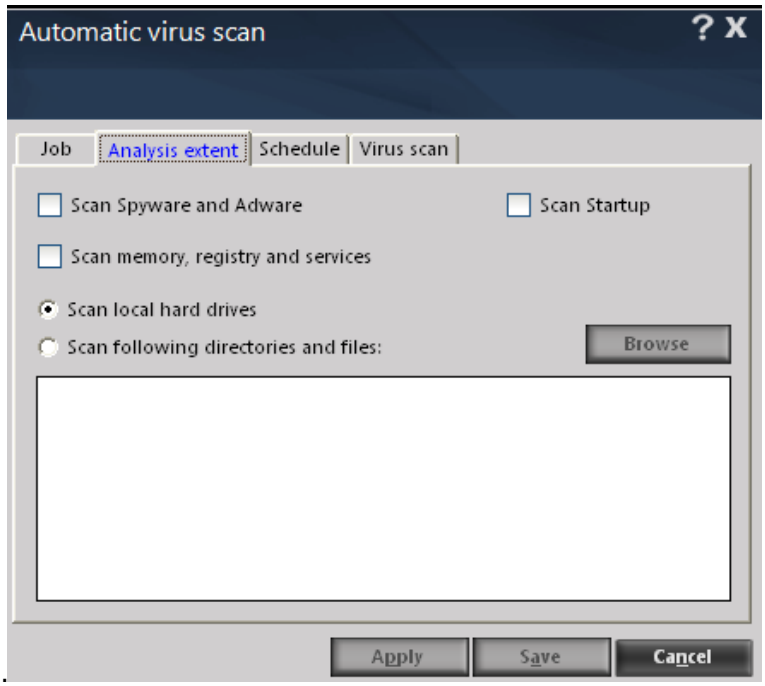
After configuring all the required settings on the **Automatic virus scan** dialog box, click the **Apply** button and then **Save** button to save the settings and click the **Cancel** button to cancel the configured settings or to close the dialog box.

- **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

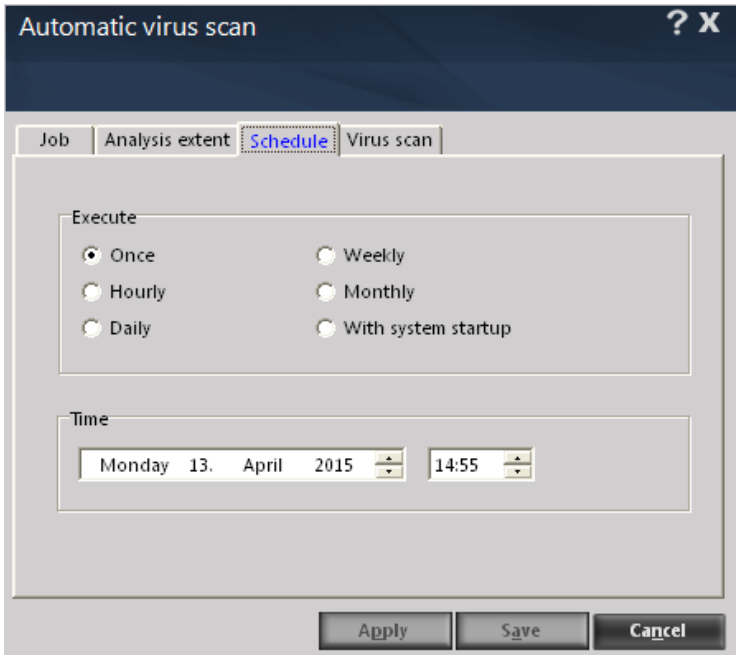
select the termination condition for the task. For example, you can specify that the On-demand Scan should always quit automatically after it has finished scanning.



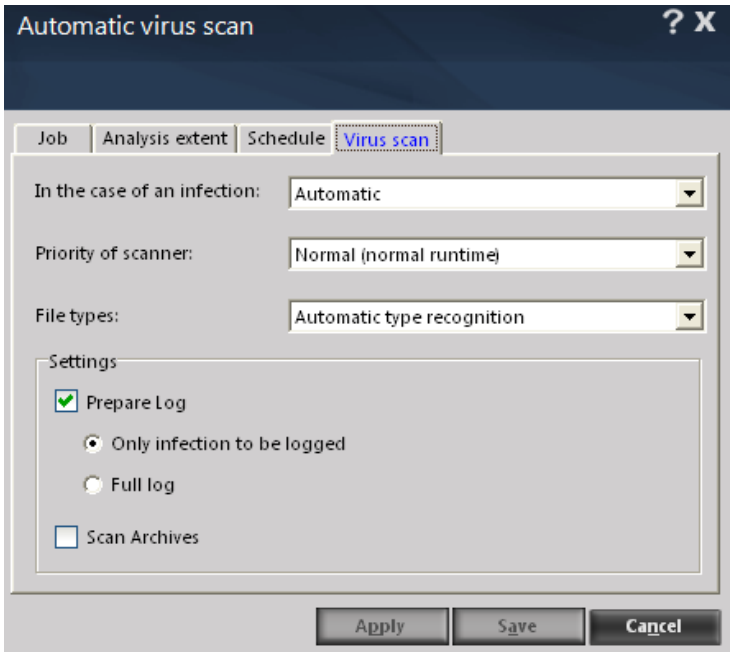
- **Analysis extent:** This tab presents you with options that help you select the type of scanning, and the list of directories, folders, or local hard drives to be scanned



- **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.

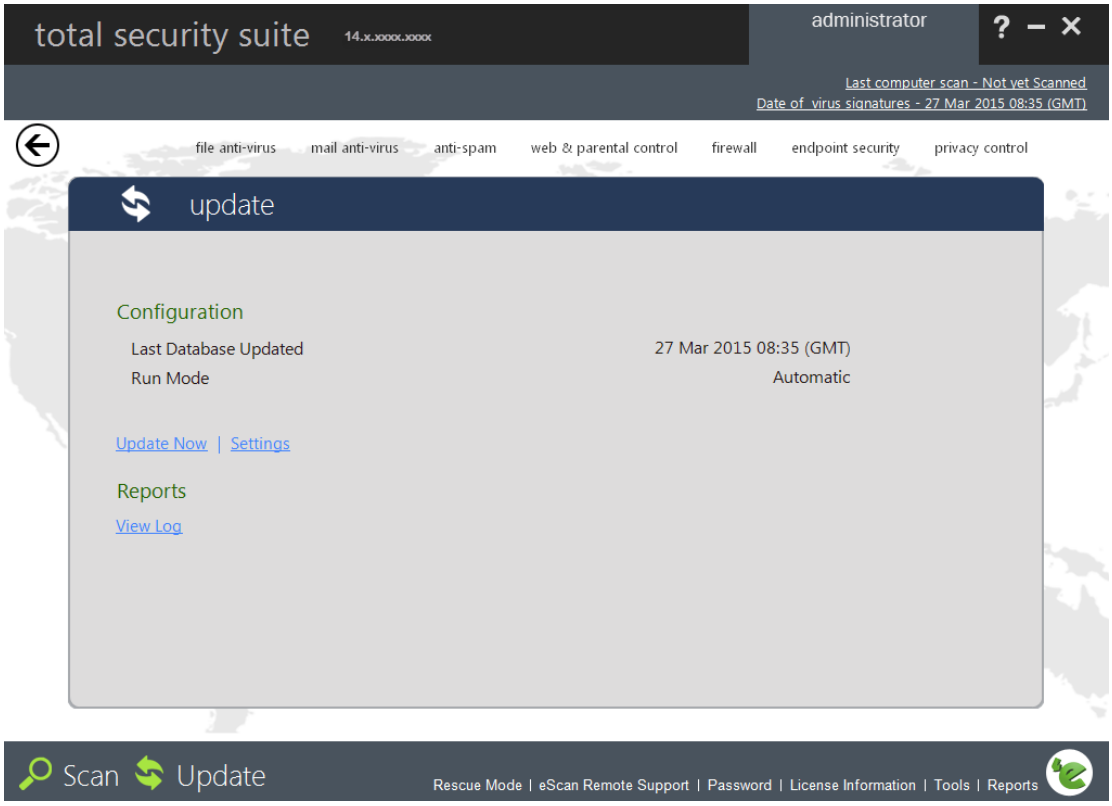


- **Virus scan:** This tab provides you with the same options as the ones present on the **Virus scan** tab of the Scan module. You can configure On-demand Scan to perform a specific action when a virus infection is detected. You can also set the priority of the eScan scanner in relation to other processes 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.


Automatic virus scan
? X
Job
Analysis extent
Schedule
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
Apply
Save
Cancel

Update

If you are connected to the Internet, eScan updates are automatically downloaded and installed on your system frequently or as defined by you in Update Settings. This prevents your system against attacks from recently detected viruses or infections.



Note:
To be protected against latest threats and infections keep "**Automatic download**" on.

Configuring Settings for Proxy Server

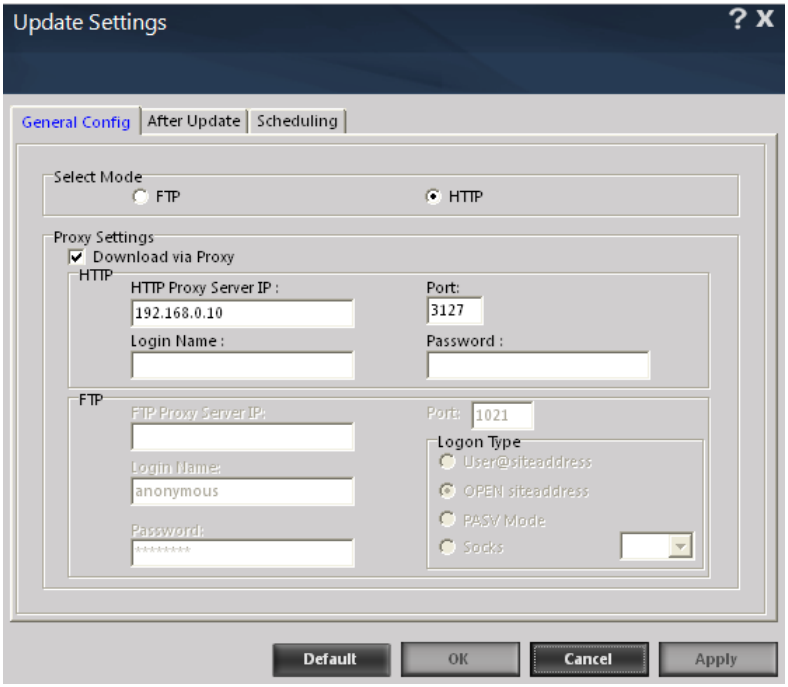
General Configurations

You can configure Proxy settings using the following steps –

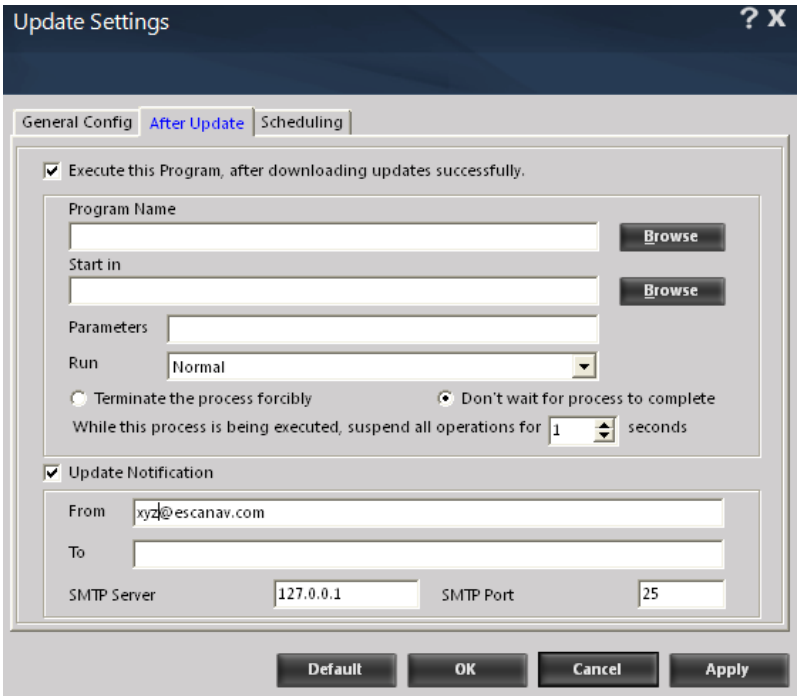
1. Click Update option present in the Quick links at the bottom of the eScan Interface.
2. Click settings link present under Configuration.
3. Checkmark "Download via Proxy option".

4. Now write the HTTP proxy server IP and Port number in the respective fields; also enter Login Name and Password, if applicable.

5. Click **OK** on the Update Settings window. Proxy settings will be applied instantly.



After Update



Managing Notification Messages after Update

As an Admin you can define customized update Messages for informing the user that the Update is complete using the following simple steps –

- Click **After Update** Tab in Update Settings window.
- Now the select the check box "Execute this Program after downloading updates successfully". This will activate the fields present under it.
- Now click browse button and browse MSG.EXE file present in eScan folder.
- Define the Start in Path (system path on the network where the message will pop up).

  Write the message in the Parameters field and define the running status of the window by selecting from Minimized, Maximized, Hidden, or Normal. The message runs on a window that can be in the maximized, minimized, normal, or hidden state, as defined by you. The default state of the window is normal.

- **Terminate the Process Forcibly** - Select this option if you want to forcibly terminate running of download.exe that download eScan updates automatically after the Update is over.

- **Don't wait for process to complete** - Select this option to push the message on user's system anytime during the update process. During the update process, you can suspend all operations for the time set by you. By fault it will appear as one second.
- **Update Notification** – Configure the settings for sending / receiving mail notification after every update.
- **From:** [Default: escanuser@escanav.com] Specify the sender's e-mail address in the notification mail in this box.
- **To:** Specify the recipient's e-mail address in the notification mail in this box.
- **SMTP Server:** [Default:] Specify the IP address of the SMTP server in this box.
- **SMTP Port:** [Default:] Specify the port number of the SMTP port in this box.

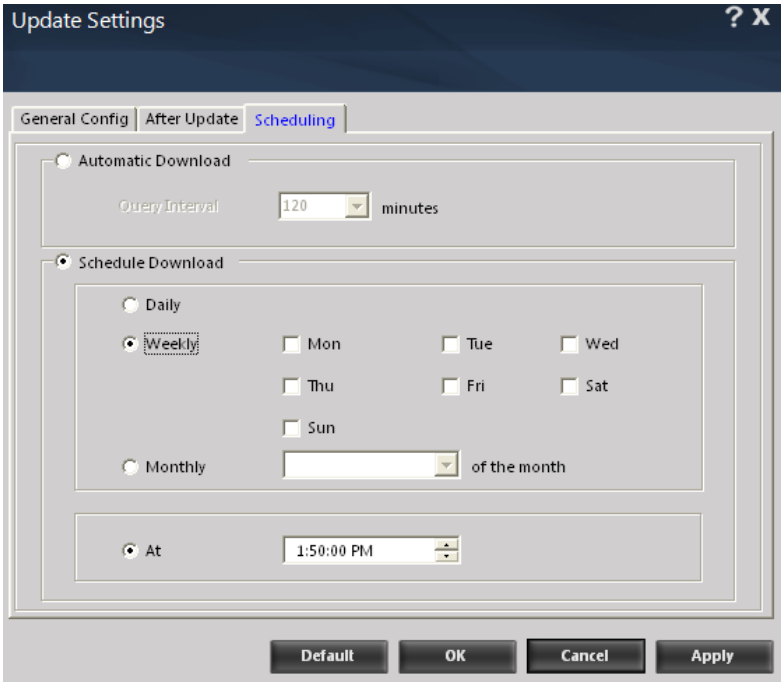
Note:
Using this Tab, you can **run hotfixes** that you wish to run after every eScan update download.

Scheduling

Scheduling the Updates

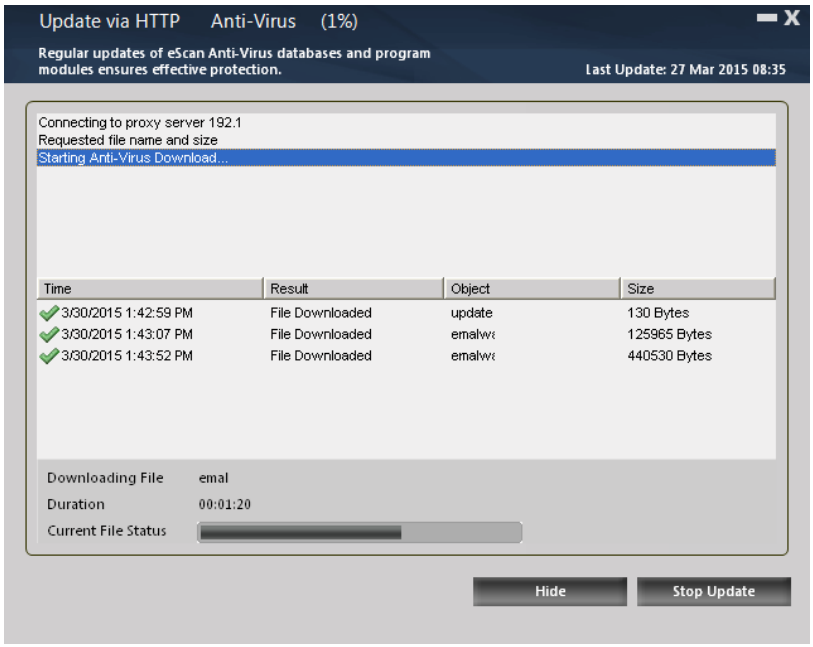
Using this tab you can schedule the download of Update Patches as per your convenience, using this tab you can schedule the Updates to be downloaded **Daily** or check for updates on eScan server at **fixed time intervals**. You can also schedule Update patches to be

downloaded on desired **days** or **dates** of the month as well as at fixed **time** of the day. When you click **OK** button or **Apply** button the defined settings will be applied instantly.

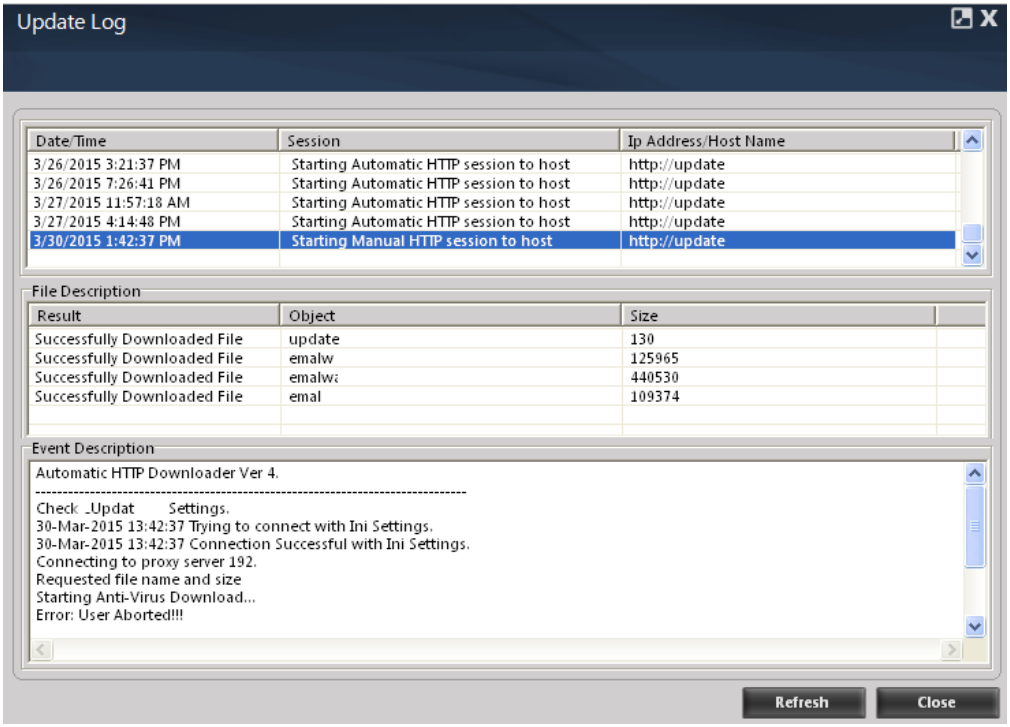


Update Now

Click this option to Update eScan instantly. Ensure that you are connected to internet to download the latest patches from our Update Servers.



Viewing Logs



eScan maintains a log of all the recent updates downloaded and installed on the system, you can view them by clicking View Logs option under Reports in the Update section. These logs include the following –

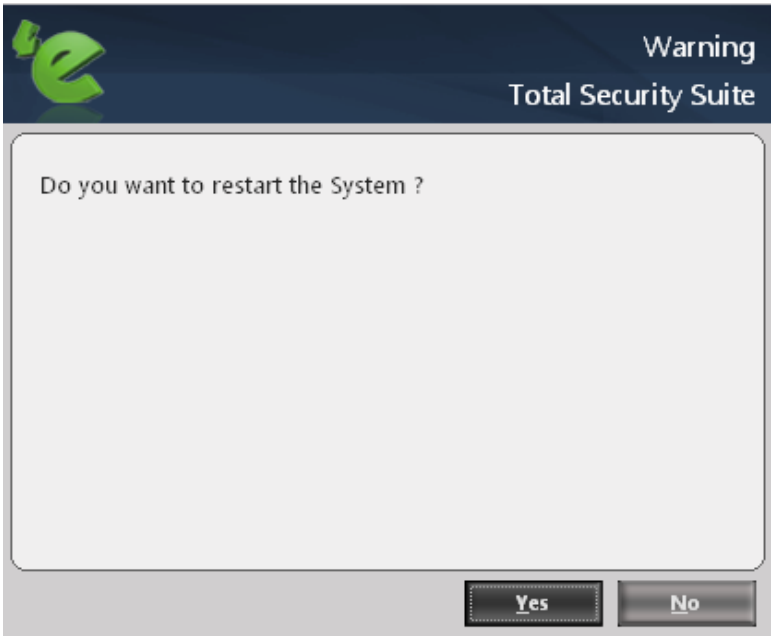
- The timestamp, session description, and host name or IP address
- The description of file, such as result of the download, name of the object, and its size
- The description of event, such as the number of files downloaded, time at which the connection was established or terminated, and the errors,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

Quick Access Links

Rescue Mode

Rescue mode is specifically designed to scan and clean your 32 and 64 bit operating systems that 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 into the memory, it can also update its database, if system is connected to internet. It will disable the task manager and registry editor.

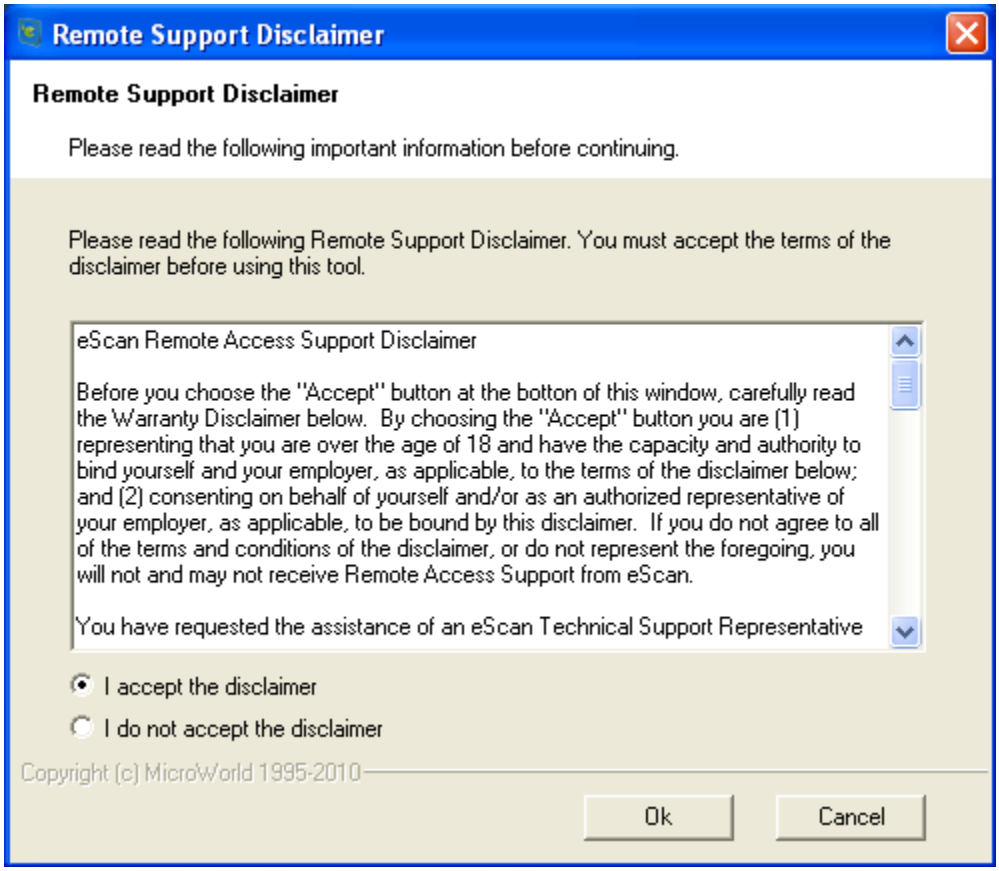


eScan Remote Support

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

Steps for availing remote support –

1. Click on eScan remote support link at the bottom of the interface. A new window will be opened as in the below figure.



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

Password

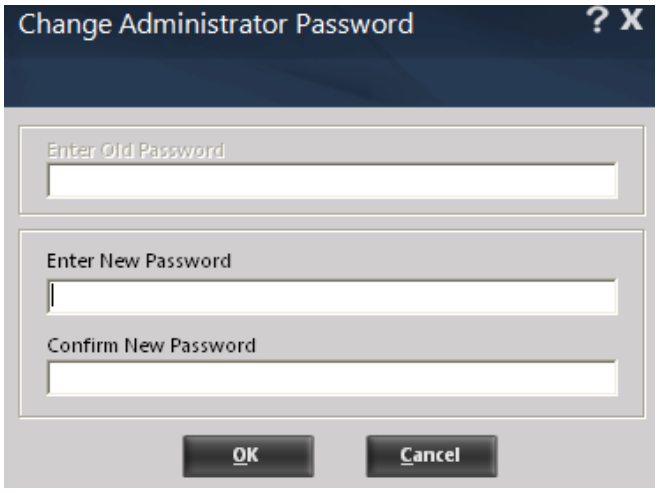
Password will secure your system from making any unauthorized changes to the settings and configurations defined by you.

Using Password Protection for opening eScan

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

1. Open eScan Window.
2. Click Password link at the bottom of the interface.
3. Type a Password in the Enter New Password field.
4. Re-enter the Password in Confirm New Password field and click OK.

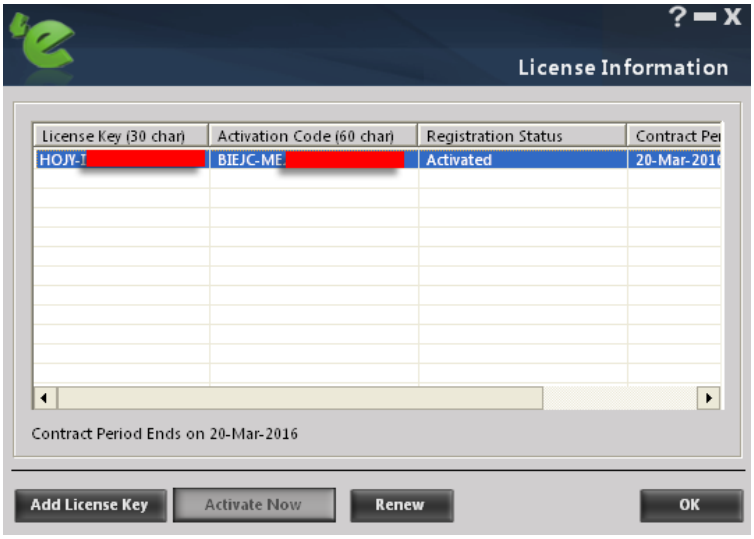
You will have to enter this password to change any settings and also to open eScan.



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

License Information

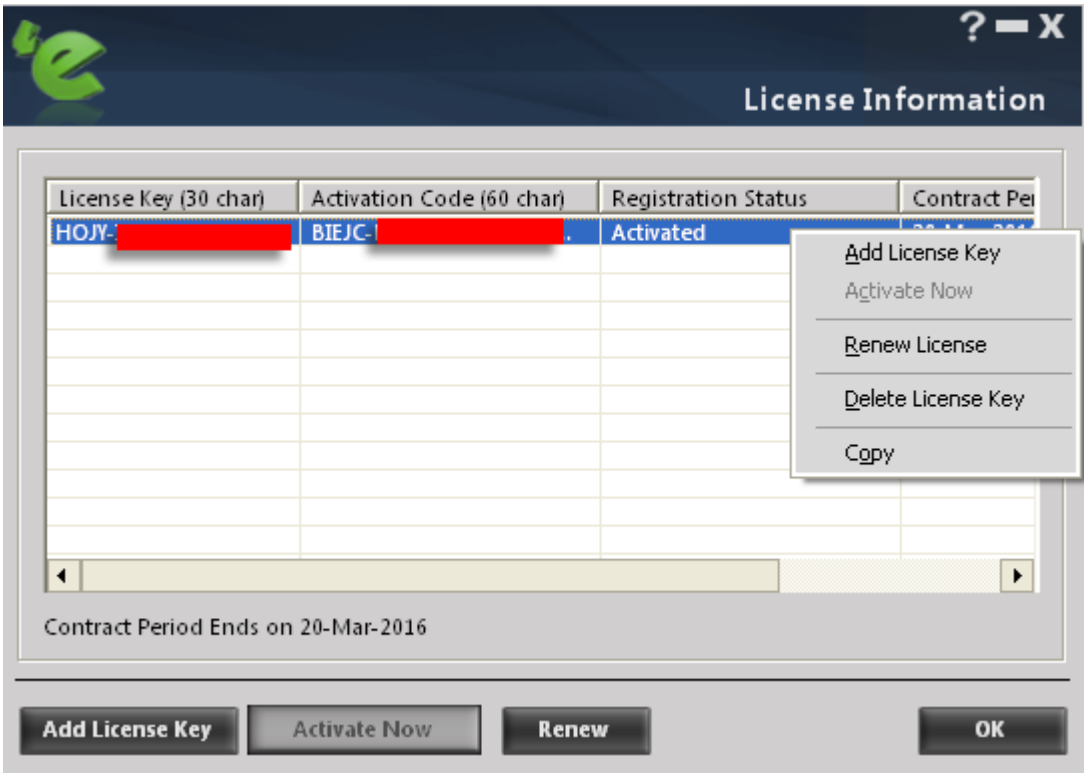
Click License Information link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to License information window, it displays following important information –



- License Key
- Activation Code

- Registration Status
- Contract Period
- Software Version

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



- Add License Key
- Activate already added key
- Renew a license key
- Delete License Key

Tools

The tools link provides you with the options for easy and quick access to various tools for eScan and each tool will have its own functions. To mention a few eScan Rescue disk, windows essential updates, disk defragmenter, vulnerability scanner, ebackup, registry cleaner are some of the tools.

Tools will allow you to perform the following actions:

- **eScan Rescue Disk Creation:** eScan Rescue wizard will allow you to create the eScan Rescue ISO image file. You will have to burn the Image on to a CD/DVD ROM/ USB device before using it to repair/clean infected or damaged systems.

Follow these steps to create a rescue disk:

- Click eScan Rescue Disk creation link, the eScan Rescue File creation interactive wizard will open and follow the instructions on screen.
- **Restore Windows Default Settings:** You can restore the Windows® operating system settings, such as desktop and background settings, to eliminate all the modifications made by a virus attack by using this button. eScan automatically scans your computer for viruses when you click this button and sets the system variables to their default values.
- **Upload Samples:** It will allow you to post your queries on the website (Clicking on this link will take you to our website). You can also upload sample files here to support your question.
- **Windows essential updates:** It will update your system with the latest windows patch updates. eScan maintains a list of critical Windows Update patches on every computer that are available for free, whenever the user clicks on "Download Latest Hotfix (Microsoft Windows OS)" option, it checks the computer for missing patches on the OS by matching the installed patches with the released patch list in the database. The missing critical Windows update patches are then downloaded and installed on the computer where eScan is running. The database list is categorized on the basis of the operating system.
- **Disk Defragmenter:** Disk Defragmenter is a system utility for analyzing local volumes and locating and consolidating fragmented files and folders.
- **Vulnerability Scanner:** This option will check the vulnerability of the softwares installed on your computer for any kind of weakness that can be used by the attacker to gain access to the information stored on your computer without your permission.

Using the options present in Vulnerability Scanner module of eScan, you can easily update the listed softwares with the more secured version of the same.

- **Download eScan Service Pack:** eScan opens the MicroWorld Download Manager and starts downloading the latest critical hotfix for the Windows® operating system from the Microsoft® Web site.

- **Import/ export Settings:** This option to Export the settings configured by you in eScan. These settings can be imported and implemented automatically in eScan whenever the drive is formatted and eScan is freshly installed. These settings can also be used on other computers with eScan.

- **USB Vaccination:** eScan will vaccinate USB based storage devices that will protect your computer from Malware that spread through USB devices as the eScan Vaccinated devices cannot get infected even when they are used on infected systems. For preventing spread of auto run -based malware infection eScan provides an advanced USB Vaccination feature that replaces the autorun.inf file present on any USB Drive with its own autorun.inf file that cannot be modified or deleted manually or by any malicious program. This file is created in such a way that it does not allow malicious program to execute on any system to which the USB Drive is mounted on, irrespective whether the system is protected by AV or not. The vaccinated drive can be used normally for copying and transferring files from one computer to other without any concern for malware spreading through USB drives even if the PCs are not protected by any antivirus. The drive will remain vaccinated till it is formatted by the user or de-vaccinated using eScan.

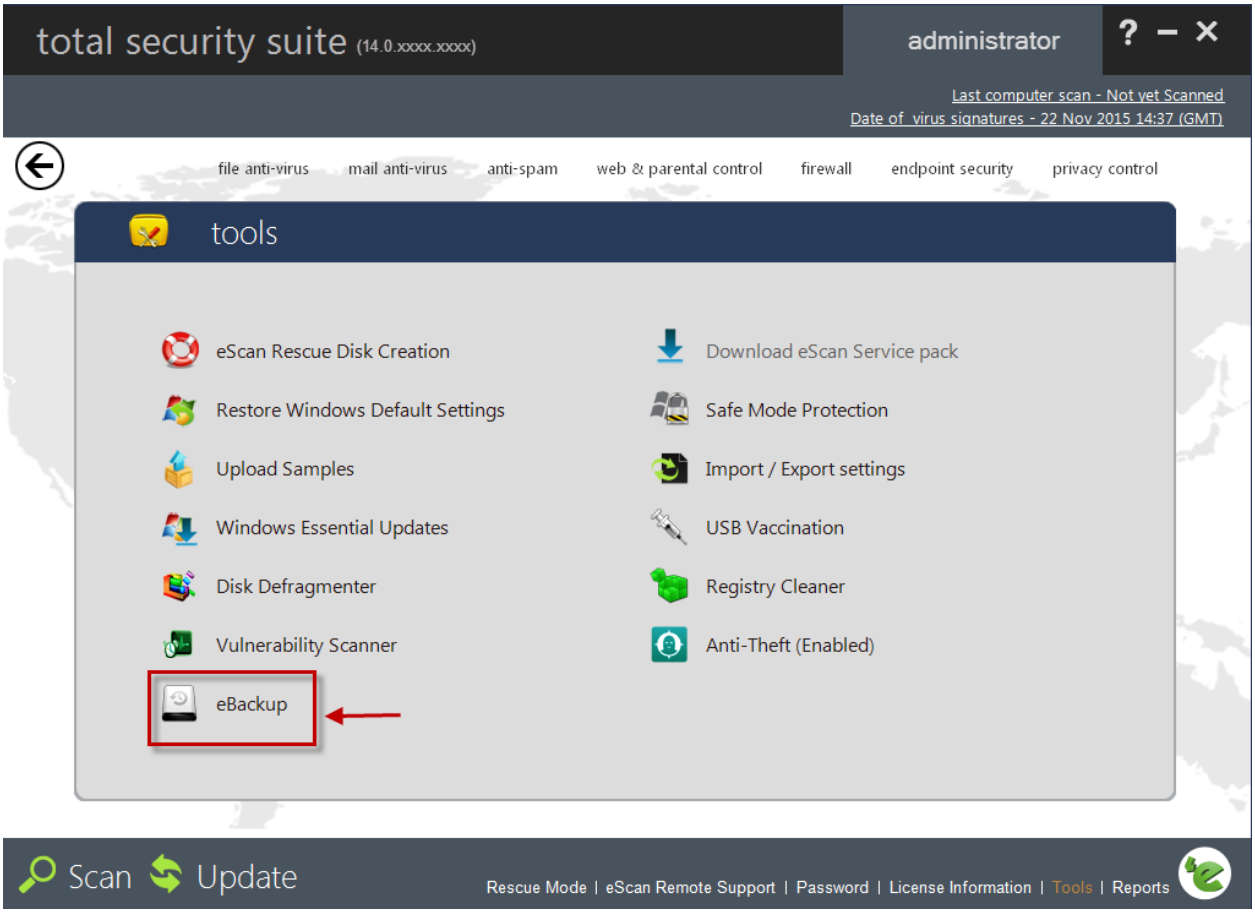
- **Registry Cleaner:** eScan will scan for issues in the selected registry entries, all issues found will be displayed in the Panel on the right. You can select / unselect the issues found by eScan and fix selected issues button to fix the issues. eScan will fix the selected issues instantly.

- **eBackup:** Taking regular backup of your critical files stored on your computer is very important, as it can be lost or damaged due to issues such as virus outbreak, modification by a ransomware or another user. This feature of eScan total security suite allows you to take backup of your important files stored on your computer such as documents, Photos, media files, music files, contacts and so on. You can define the path to store the backed up data either on your computer, CD/DVD or USB Drive. It allows you to schedule the backup process by creating tasks. The backed up data is stored in an encrypted format in a folder secured by eScan's real-time protection. You can create Backup jobs by adding files, folders to take backup either manually or schedule the backup at a defined time or day.

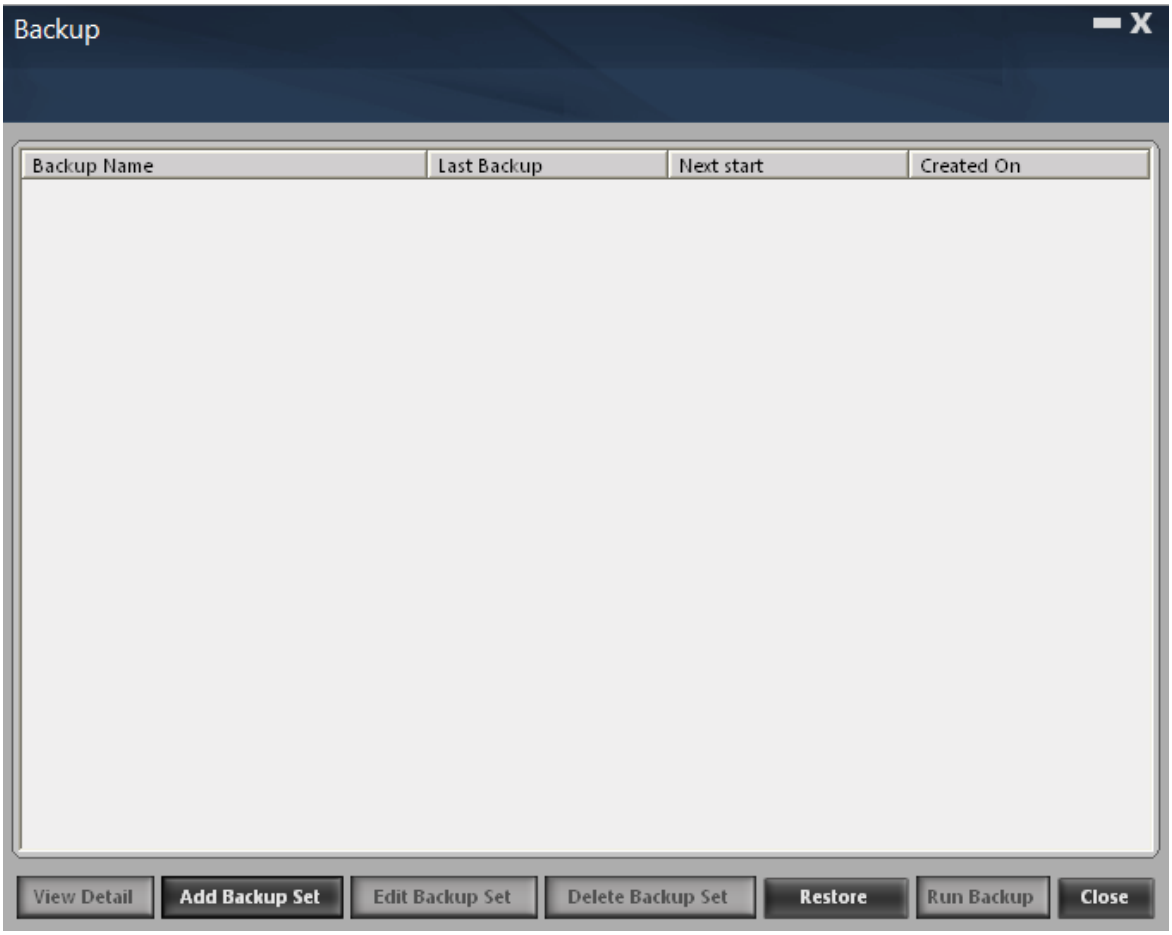
How to Access eBackup

Use the following simple steps to use eBackup feature of eScan Total Security Suite:

1. Click on the Red shield of eScan Total Security present in the task bar to open eScan Protection Center.
2. Click on Tools option present at the bottom of the eScan Protection Center, you will be forwarded to the tools Module of eScan Total Security, as shown below -

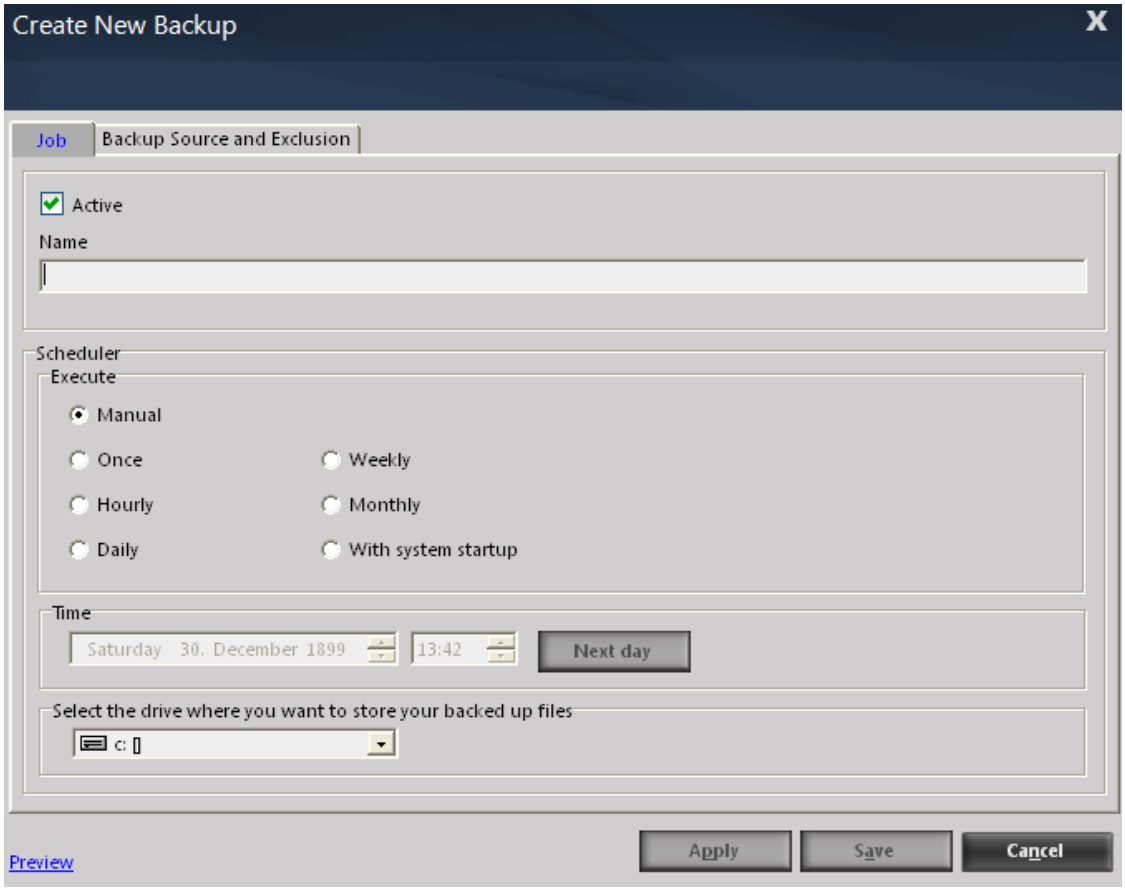


3. Click on eBackup to take backup of your important files and folders.



Adding Backup Set

Click **Add Backup Set** option to create a new backup job, it allows you to take backup either manually or schedule a backup at a desired time; it also allows you to add files and folder for taking backup.



Creating New Backup Job

- **Job:** This tab will allow you to create a new back up job for your important files /folders. The following options are available in this tab:
- **Active:** Select this check box to activate a backup schedule. The backup process will be run only for active backup jobs. Inactive Backup Set is displayed in Red.
- **Name:** Enter a name in this field; this will be name of the backup schedule created by you. For example: You name this schedule "Backup080515" and all your files and folders containing Backup080515 can be added to this particular schedule.

Scheduling a Backup Job

Scheduler will allow you to schedule the backup jobs. You can schedule the backup jobs to be executed manually or schedule it just for once or on a daily/hourly/ weekly/monthly or with system start up.

- **Manual:** Select this option to manually run the backup. You cannot create a schedule for a manual backup. This option will allow you to take a backup on an external device as well.
- **Once:** Select this option to schedule the backup for only once. On selecting this option the date and time field will be activated. You can set the date and time to schedule the backup.

Note:
At the time of **Editing Backup Set** - Active option cannot be un-ticked for the Backup Jobs that have been scheduled to run only once by the user.

- **Hourly:** Select this option to schedule the backup on an hourly basis. This option allows you to take a backup of the defined backup job on an hourly basis.
- **Daily:** Select this option to schedule the backup on a daily basis. You will have to define a particular time at which the backup has to be taken, the backup will take place every day at the same time.
- **Weekly:** Select this option to schedule the backup once in a week. It will allow you to set the day and time for the backup to be scheduled at.
- **Monthly:** Select this option to schedule the backup on a monthly basis. t will allow you to set the time and day of the month+ when you want the backup to take place.
- **With System Startup**: Select this option to take back up of all the selected files and folders every time the system is started. You should be selected the drive where you want the back up files and folders to be placed.

Note:
Scheduled Job will be executed only if the Laptop is connected to a Power Source. In case at the scheduled time the Laptop is on Battery mode the Scheduled backup job will start only when it is connected to a power source next time.

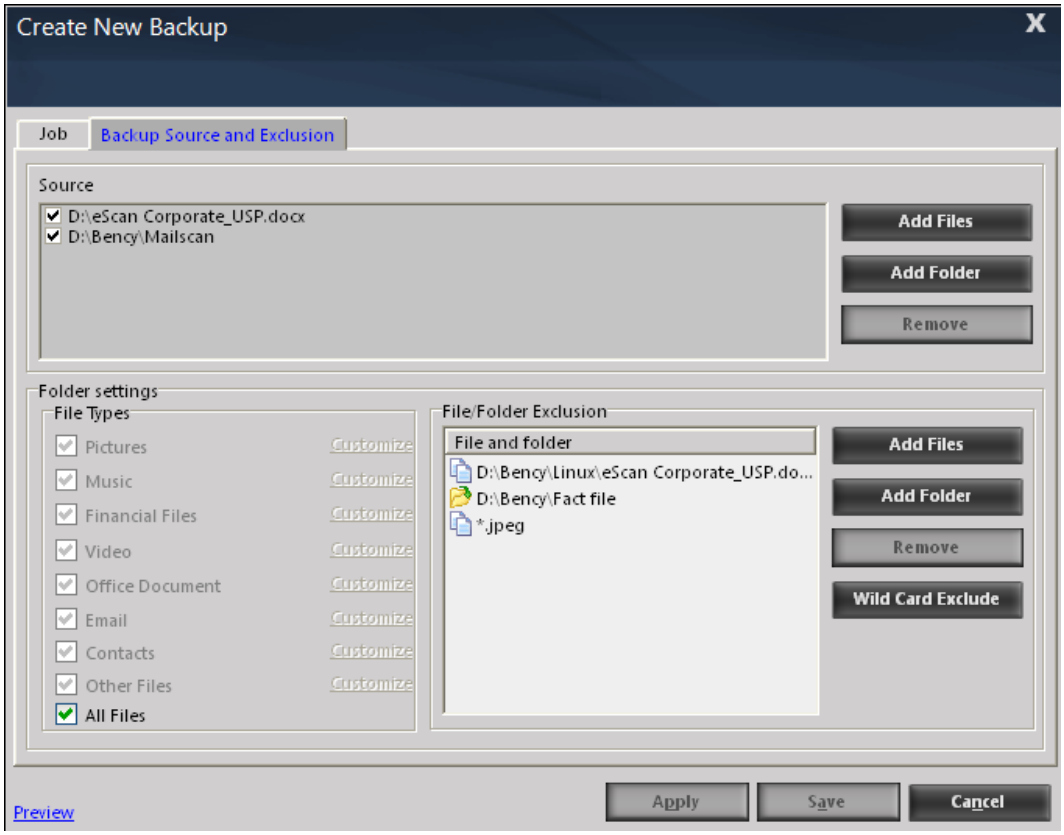
Selecting the destination folder for Storing backed up Data

- **Select the drive where you want to store your backed up Files**

  This option allows you to select the drive where you wish to store the backed up files. You can select either the hard drive partitions or you can write the data on CD/DVD or store it on a USB Drive. In case if the space is less than the Backup set size on the selected drive, you will be informed through the following popup message.

Backup Source and Exclusion

In this section you will add the source files and folders for which the backup has to be taken. It will also allow you to exclude some files and folders from the backup process. It will also allow you to customize the file types for the backup or you can also include all types of files for the backup.



Source

In this section you will add the files and folders to backup**.** It has the following options:

- **Add Files:** Click this option to browse and add files to backup.
- **Add Folder:** Click this option to browse and add folders to backup.
- **Remove:** Select a file or folder and click **Remove** to remove it from the backup process

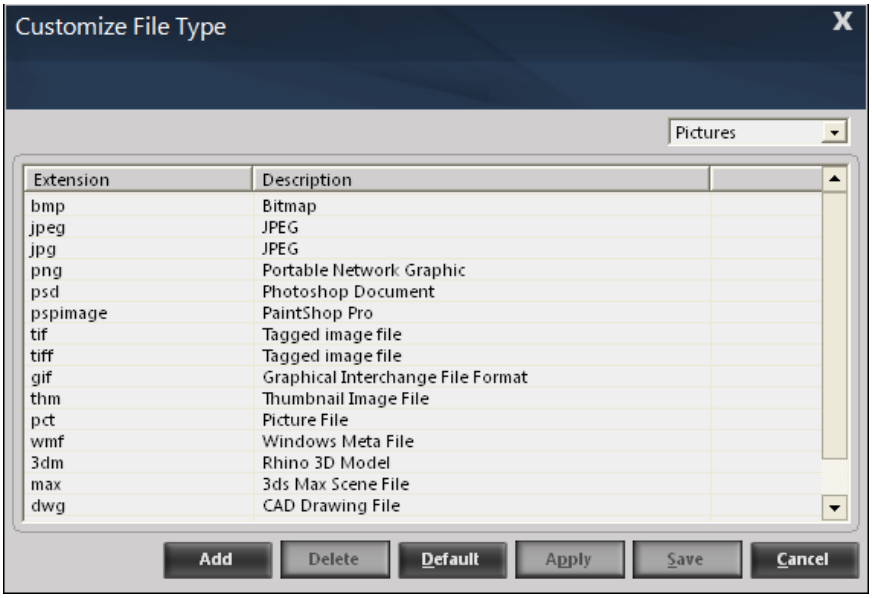
Folder Settings

This section will allow you to define the type of files that you want to backup. Select **All Files** to include all types of files. In case if you want to include only certain types of files, it will allow you to customize the file types as per your requirement.

- **File and Folder Exclusion –** This option allows you to add Files or Folders that you wish to be excluded from the selected Backup set.
  - **Add Files** – Click on this option to Add desired files to the exclusion list from the selected backup set. No backup will be taken of the selected file whenever a backup is run.
  - **Add Folder** – Click on Add Folder to add a sub folder to the exclusion list from the selected backup set. No backup will be taken of the selected sub folder whenever a back is run.
  - Wild Card Exclude - This option allows you to exclude files by adding their extensions to the File and Folder Exclusion list. For example – If you wish to exclude all notepad files from the backup set, you can simply add *.txt in the File and Folder Exclusion list. No backup will be taken of the files having extension *.txt whenever a backup is run.
- **Preview –** Click on this option to view the Files included in the backup set

How to add customized file types?

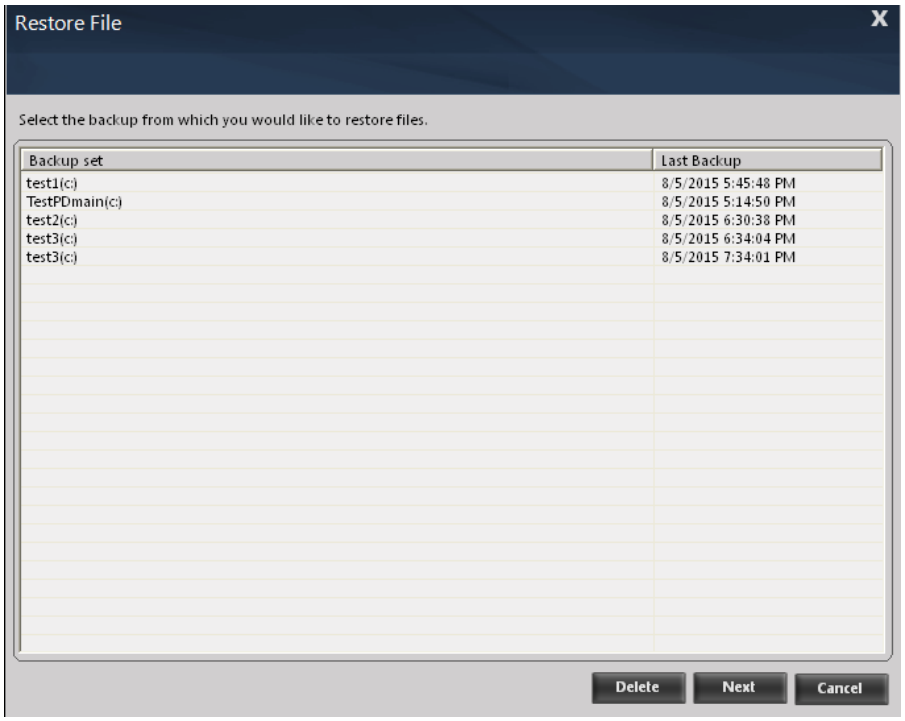
1. Select the check box next to file types option and click customize. A new window Customize File Type will open.



2. Click Add option on this window, another window Add Extension will open.
3. Enter the extension type and also give a brief description about the extension type and click Add.
4. The file type will be added to the customized list.

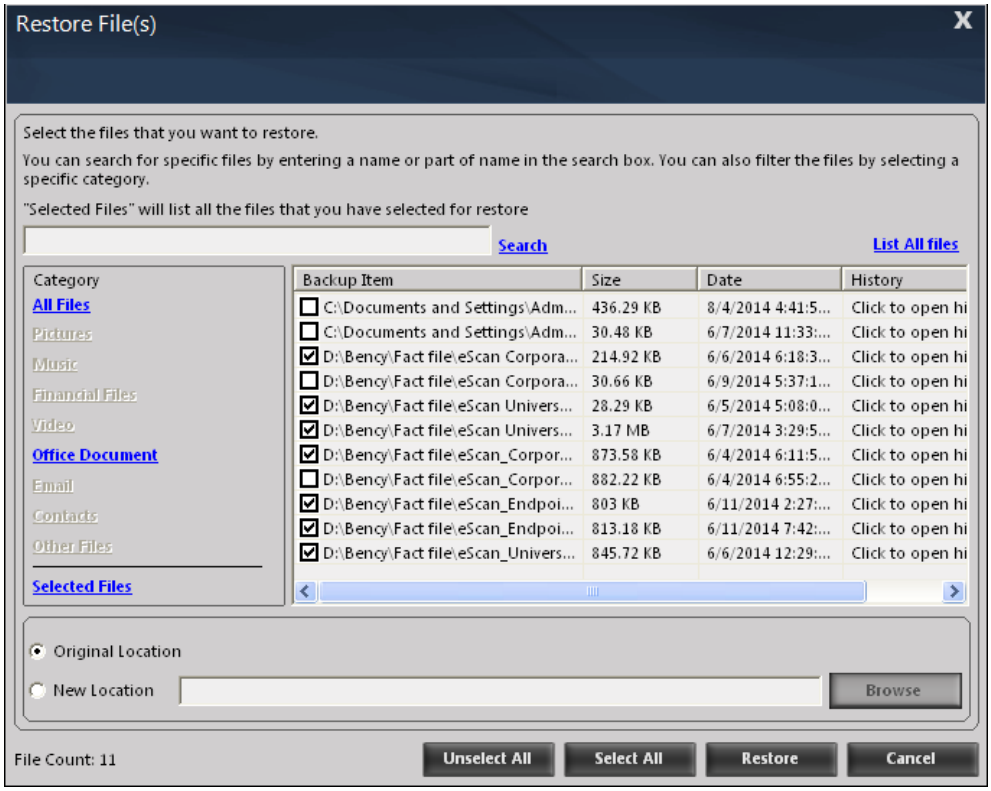
Editing Backup

- Edit Backup will allow you to edit an existing backup job. Select an existing backup job and click Edit Backup. The Create New Backup window will open. You can make the required changes to the existing backup job.
- **Delete Backup set:** It will allow you to delete an existing backup job, Select an existing backup job and click delete, this will delete the selected backup job.
- **Restore:** It will allow you to restore the backup files and folders.



Procedure to Restore Files

1. **C**lick **Restore,** the **Restore File** window will open**, Click Next** on this window.
2. Search for the specific file to be restored by entering a name or part of the file name in the search box OR click on **List All Files** link to display the list of all the files.



3. By default all the files will be selected, select only those files that you want to restore and click Selected Files. All the unselected files will be removed from the list.

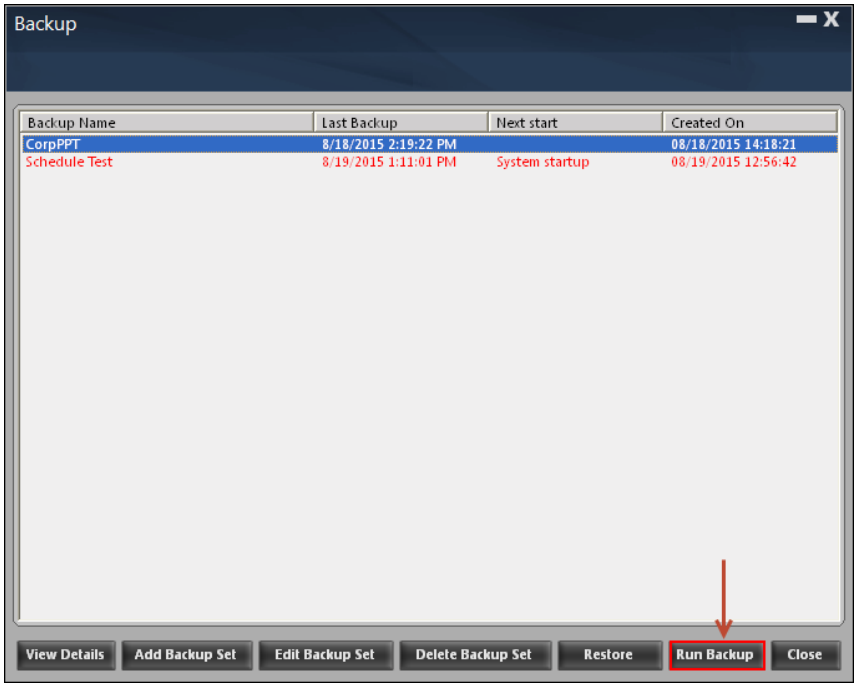
4. Select the option Original Location to restore the files to the original location (The selected backup set will be restored at the original path of the backed up file or Folder) Or Select the option New Location and Click Browse to restore the files to a new location.

5. Click Restore, this will restore the selected backup set and you will be informed through a message Backup Successfully Restored will be displayed. The restored files can be accessed either from original path(Where the Backed up files were stored) the pre-defined path

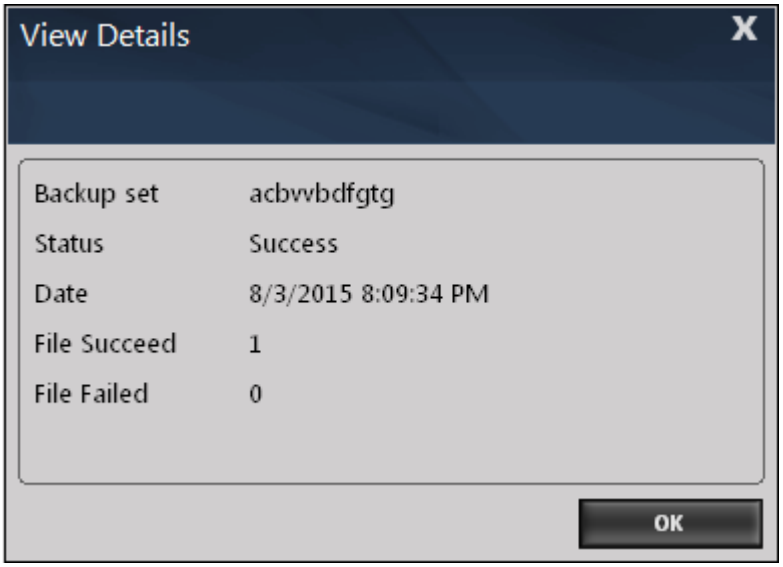
- **Run Backup:** Click **Run backup** to take a manual backup of the selected backup job.

Procedure to Run Backup

- Select an existing backup job and click **Run Backup**, the message **Backup completed successfully** will be displayed.



- **View Details:** It will display the details of the selected backup job schedules, it also displays the status of the backups that have failed / succeeded, along with the date and time stamp. It also displays the total number of files that have been backed up successfully and the files for which the backup has failed.



- Restoring Data in case of System format or re-installing eScan Total Security Suite on the system

You can easily restore the data that has been backed up earlier before the format if you have saved the backed up folder on a USB Drive or a CD /DVD.

Procedure - Restoring Data in case of System format

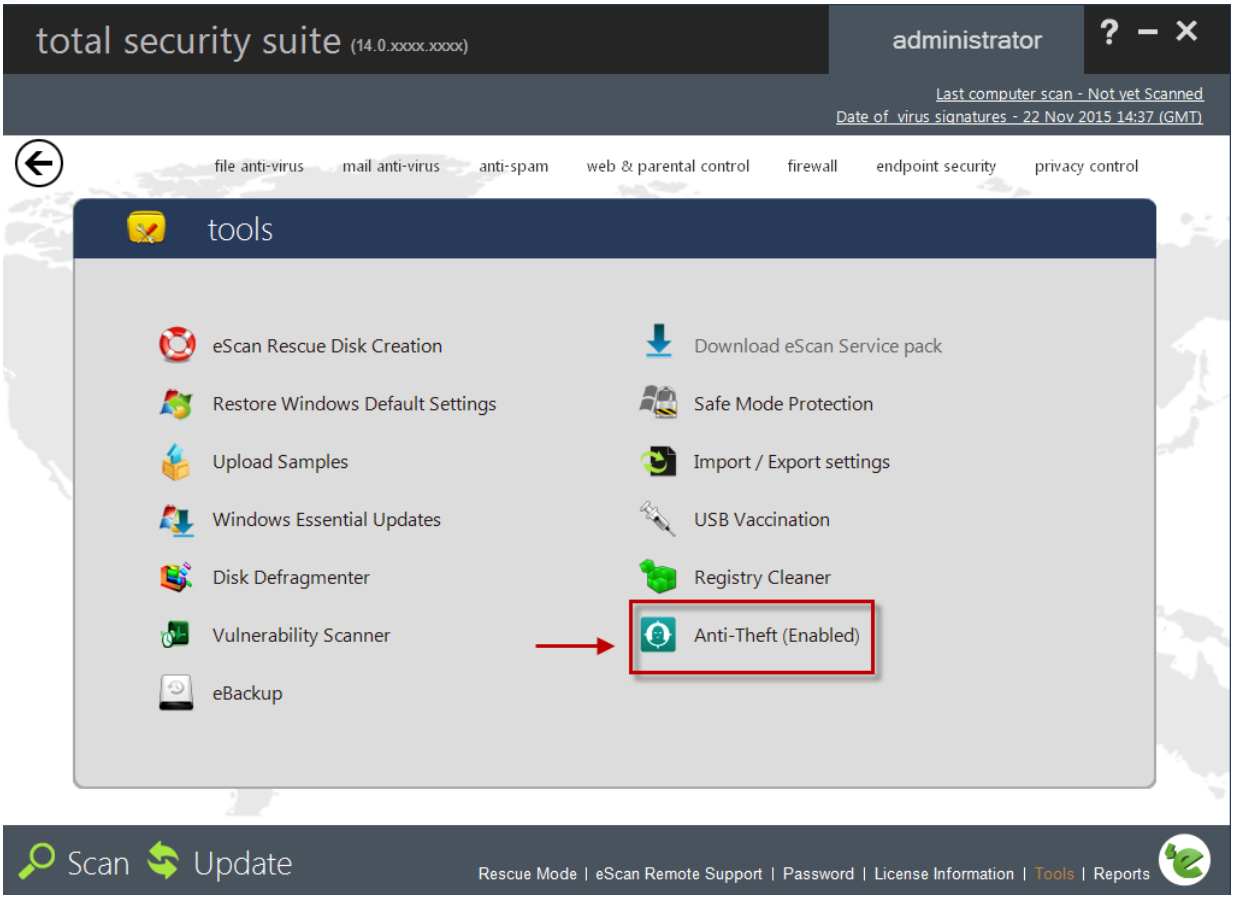
- Install Total Security Suite on your computer
- Copy the **eBackup** Folder in the path where you have saved the backup before the format.
- Now open **eBackup** option present under **Tools** in Total Security Suite.
- All saved backup jobs will be displayed in the backup list, select and restore the desired backup job using Restore option present at the bottom of the window.

Anti-Theft

Our personal devices are constantly at risk of being lost or stolen. If your device is ever lost or stolen, eScan Anti-Theft lets you track your missing device using localization by IP address, helping you retrieve your device and protect personal data.

eScan Anti-Theft is a new feature introduced in eScan Total Security Suite Version 1802 and above that increases user-level security in the case of a lost or stolen device.

Using advanced technologies such as IP address lookup, image capture, screenshots, lock down of device, Alerts, scream, and Data wipe. These wide varieties of techniques ease down the process of tracking the device in case of lost or stolen.



How to activate the anti-theft feature?

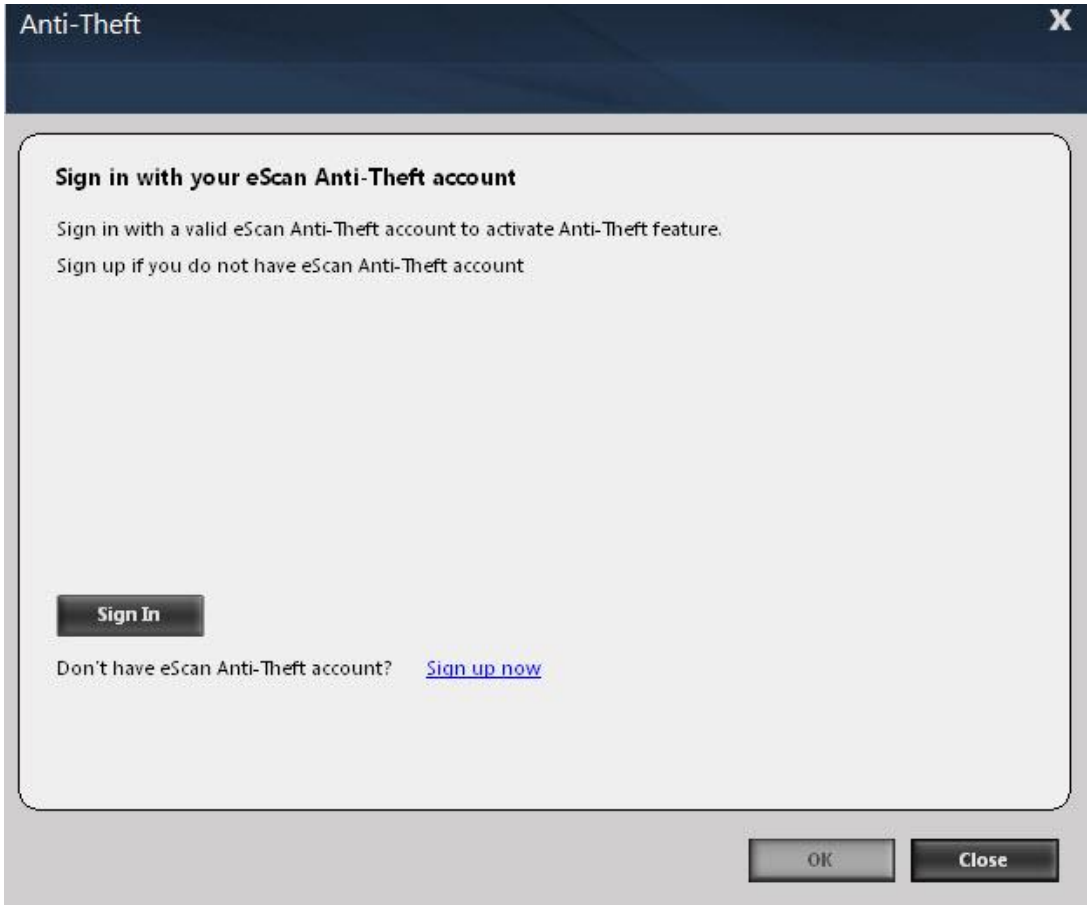
To activate the anti-theft feature on your system, you need to register and add your system on to the anti-theft portal. The first time ever you open the feature on your windows system, it will ask you to create an account on the anti-theft portal and login with the same credentials on your system.

Note:

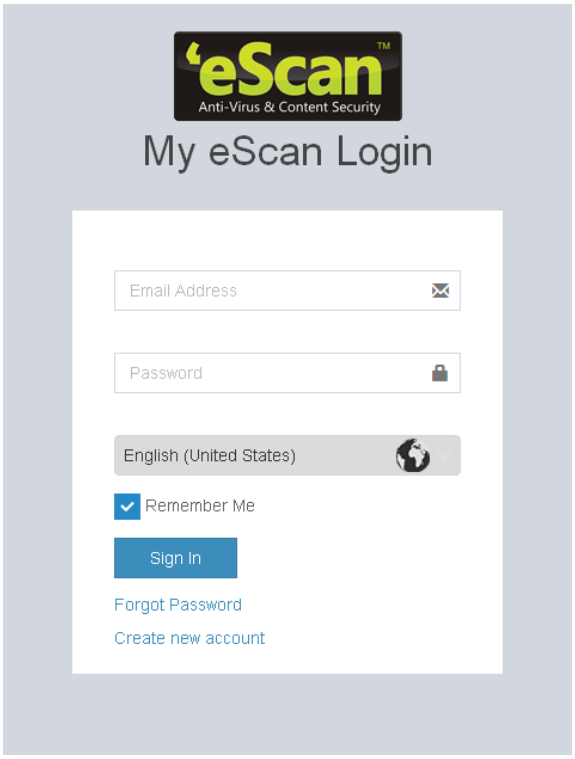
- If you already have anti-theft portal login details for Android or iOS, you can use the same user details for windows system as well.
- If you already have an account refer step 7

Steps for Creating New Account

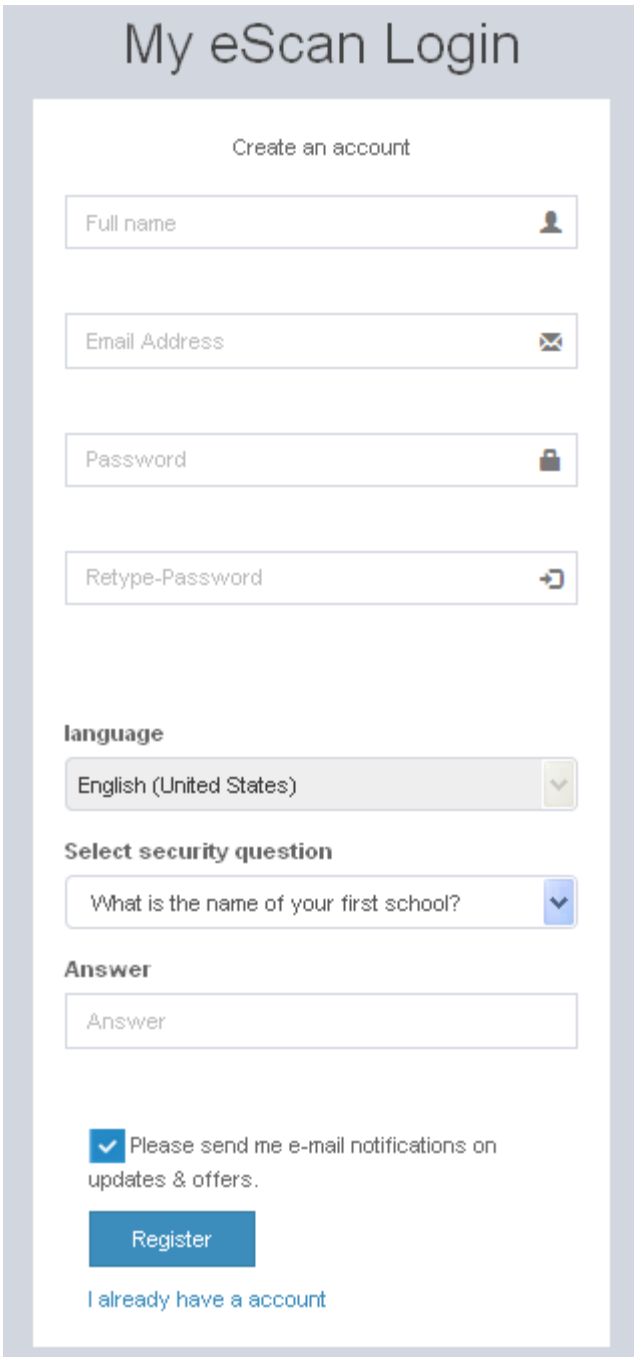
1. Click **Anti-Theft** from the Tools option on the Quick Access Link and a window Anti-Theft will open as shown in below figure.



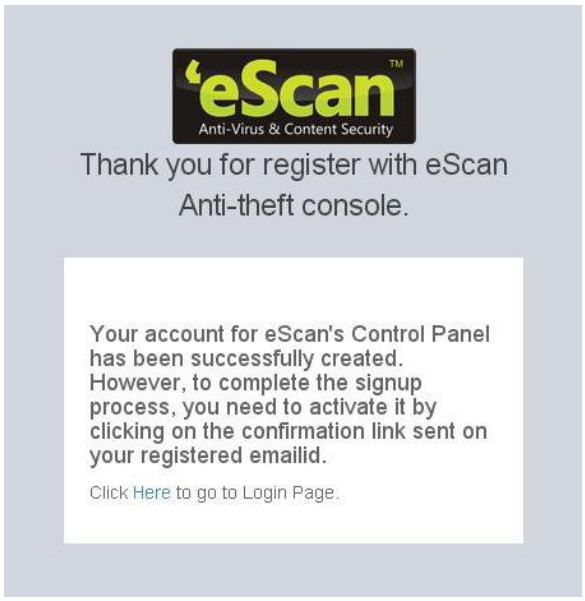
2. Click **Sign In** and enter your login details if you already have an account or Click the **Sign up now** to create a account; you will be redirected to My eScan login page as shown in the below figure



3. Click **Create new account** link on this page and enter your details and click **Register**;



4. The following message will be displayed on screen.



5. You will receive an email on your registered email address with the following message; Click on the **conifrm account** link or copy paste the link in your browser.

Congratulations on choosing eScan for your security needs.

The email-address was used to register with eScan. Please click on the below link to confirm your registration
Confirm Account

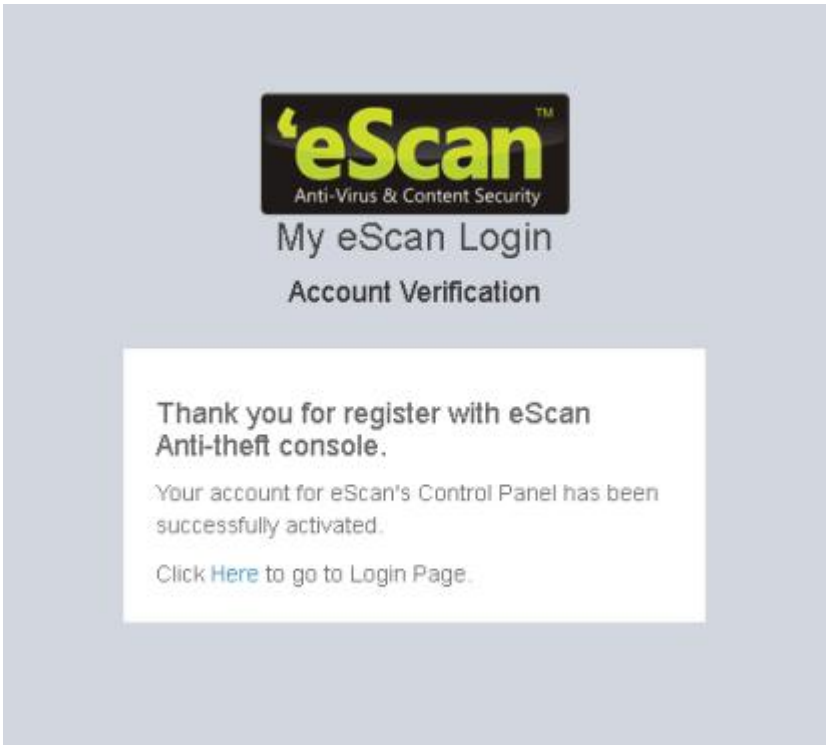
OR

copy and paste the below link in your browser to complete the regis tration process
http://ios.escanav.com/contentpage/reconfirmation.aspx?Id=EDGH HNAHHNHHHNNHHNHHHNKHANHHENCHENLHENAHE NOHLNNHHNAHHNFHGNMHENKHENGHENOHENJHENL HANAHENEGENKHENKHANCHENLHENLHLNCHFNAHF NDJ

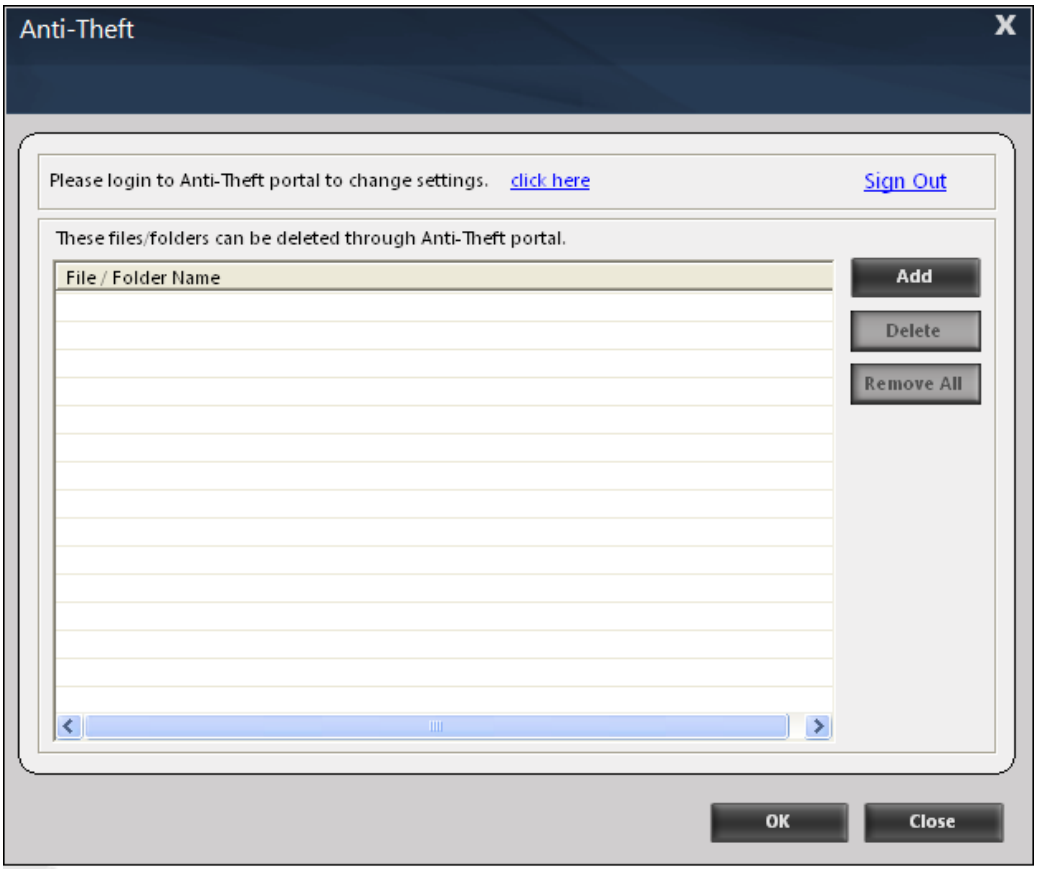
Please contact us on support@escanav.com for assistance

Warm Regards,
eScan Anti-Theft

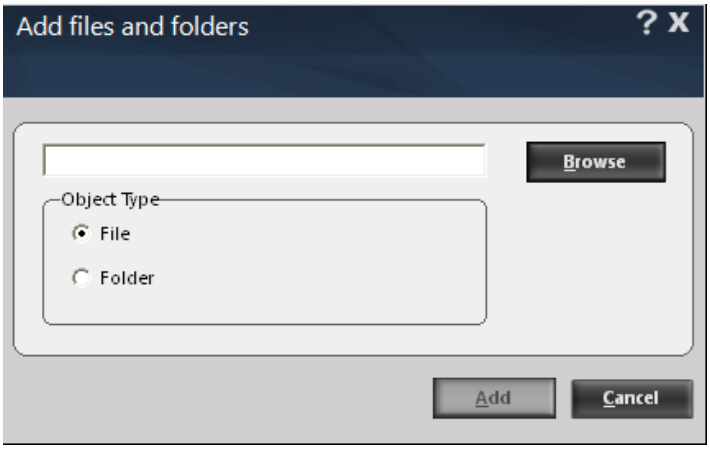
6. A confirmation as in the below image will be dispalyed on screen. Click on the Here link to go back to the login page.



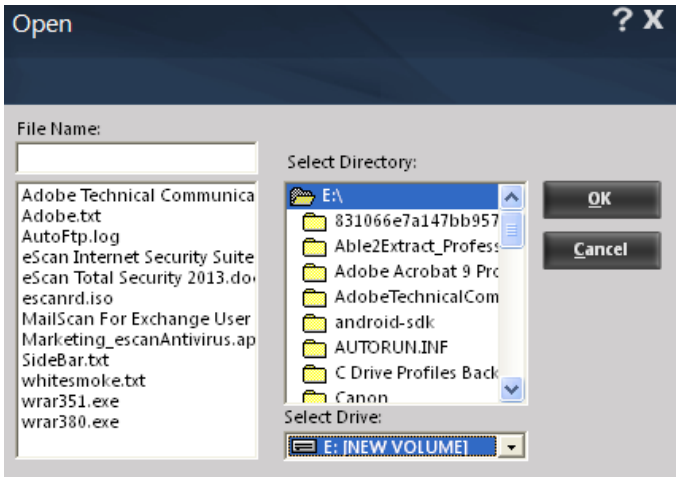
7. Now login on the system with the same credentials. Anti-Theft window will be displayed as shown in the below figure.



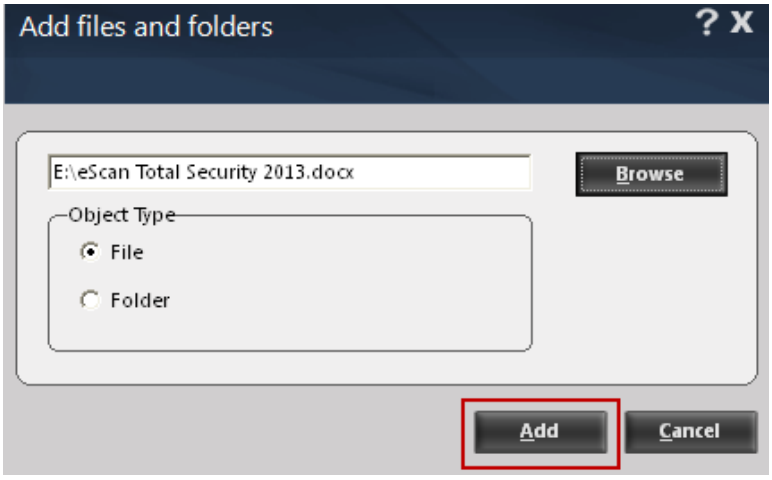
8. Click **Add** option on this page, a new window "**Add files and folders"** will open, Select the object type (whether you want to add files or folders)on this window and Click **Browse**.



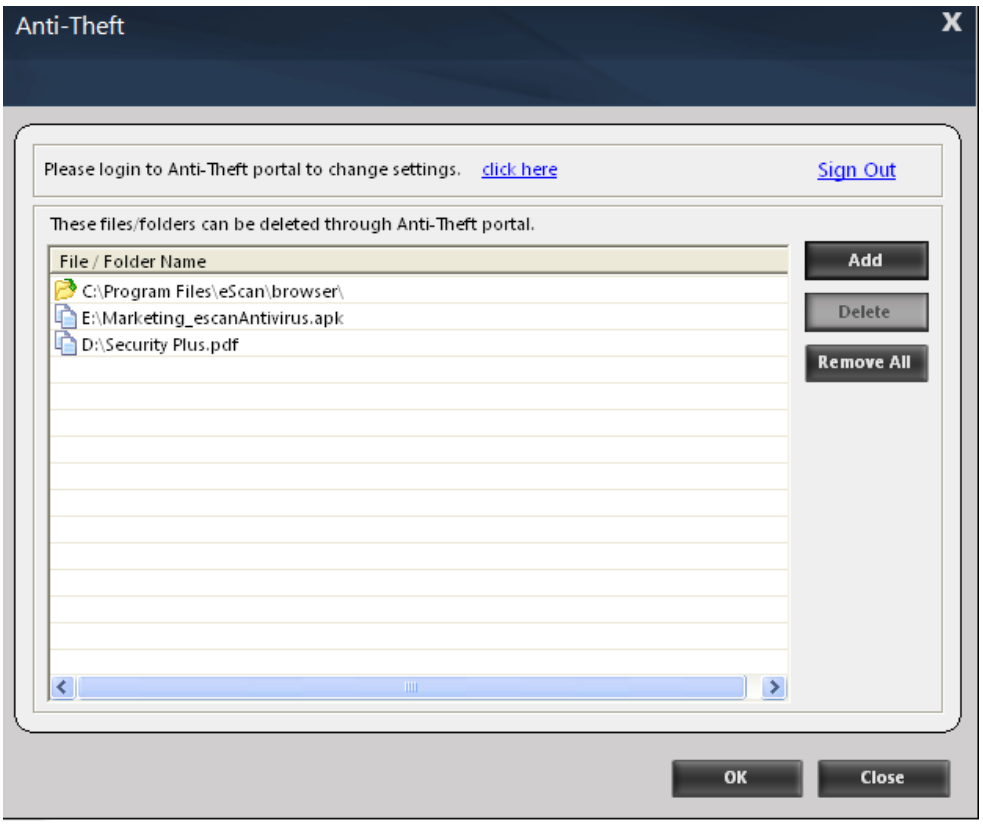
9. On the **Open** window, you can select the drive, directory and files and folders and click **ok**.



10. You will be redirected to Add files and folders window, click **Add** on this window to add the files and folders to the list.



The files / folders added to the list will be displayed as in the figure below. You will have to add the files and folders that have any kind of confidential information, these files and folders will be remotely deleted from the anti-theft portal incase of loss or theft.


Anti-Theft
Please login to Anti-Theft portal to change settings.
click here
Sign Out
These files/folders can be deleted through Anti-Theft portal.
File / Folder Name
C:\Program Files\eScan\browser\
E:\Marketing_escanAntivirus.apk
D:\Security Plus.pdf
Add
Delete
Remove All
OK
Close

Anti-Theft Portal

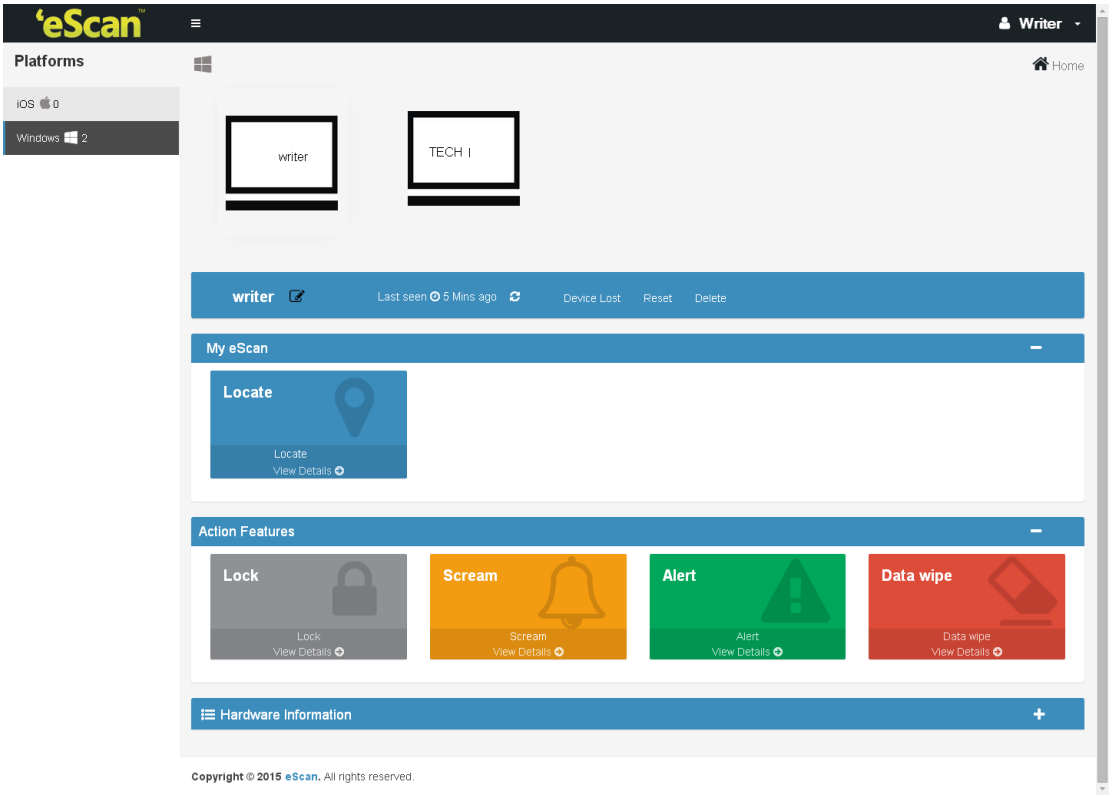
Anti-Theft portal is an online portal that can be accessed through any computer, laptop, tablet or phone at www.escanav.com. From the anti-theft portal you can trace the last location of your lost or stolen system through this portal. The first time you login to the system, you will have to register on the ant-theft portal. This will help you in tracing your system in case of loss or theft. You can use the scream option to check if the phone is in the vicinity, if you still can't find the system, set the system as lost / stolen on the anti-theft portal and the Locate, Scream, Camera and Alert features will be activated and will be performed on the system.

Note: The lost/stolen system should be connected to the internet for efficient functioning of all the features.

You can remotely execute the following commands through the Anti-Theft portal on to your lost Windows system already added to it.

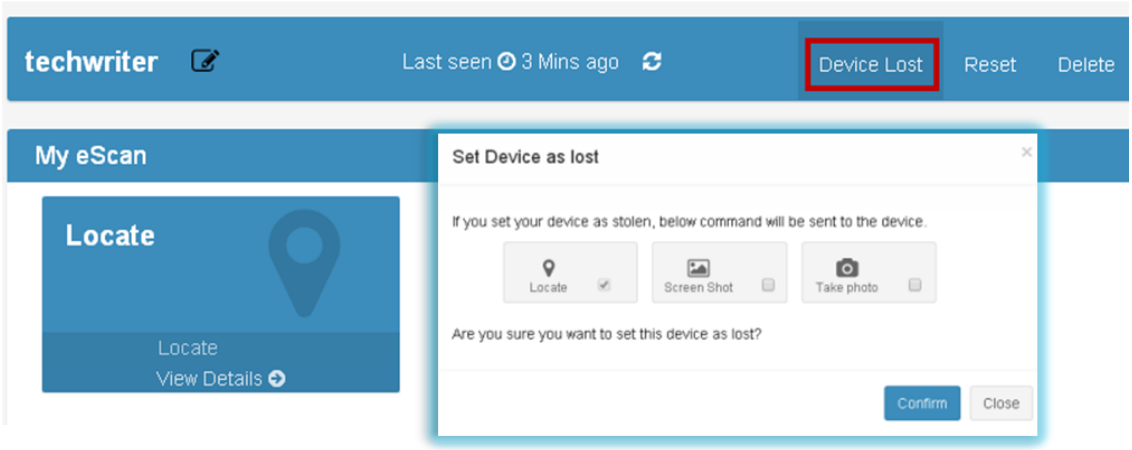
On the anti-theft portal it will display all your Windows, Android and iOS devices that are added to the portal.

1. Select Windows from the menu and click your system name, it will display the anti-theft features that you can activate in case your system is lost or stolen.



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

3. Click **Device Lost** and this will allow you to enable the features Locate, ScreenShot and Camera.



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

- **Locate**

  This option will allow you to locate the system in case of loss/ theft. Click on the Locate option on the anti-theft portal and the last known location of the system will be displayed on the map.

  Procedure to Locate the system

  1. Click **Locate**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to locate the system is in progress.
  2. View Details displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.

- **Screen Shot**

  This option will take a screen shot of the system whenever it is synced to the server.

  1. Click **Screenshot**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a screenshot is in progress.
  2. View Details displays the last two screenshots from the successful execution of the screenshot command.

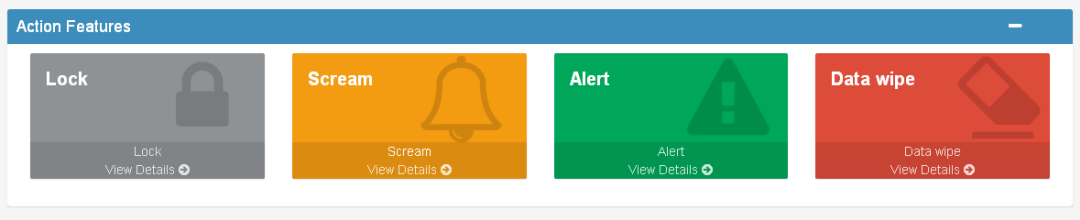
- **Camera**

  This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the camera option on the anti-theft portal.

  1. Click **Camera**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a snapshot is in progress.
  2. View Details displays the last two snapshots taken from your system.

RESET

Click Reset to reset the **"Action features"** on the system; these actions can be performed on the system when it has been lost or stolen.



Lock

The Lock feature will block the system from any further access. You will have to unblock the system by entering the pin provided on the anti-theft portal.

- On the anti-theft portal, select your System Alias name and then click **Lock** to remotely block your system, to unblock your system you will have to enter the Secret Code provided at the time of executing the lock command.

Scream

Scream will allow you to raise a loud alarm on the system; this will allow you to trace the system if it is in the vicinity.

- Click **Scream** option to remotely raise a loud alarm on your system.

Alert

This option will allow you to send an alert message (up to 200 characters) to the lost system. This alert message will be displayed on the screen; you can write and send any message for example: Request a call back or send your address or any kind of message to the current holder of your system. With this option there will be higher chance of your lost system being returned.

- Click **Alert** option to remotely send a message to your lost system. Type in your message in the send message section and click confirm.

Data Wipe

The Data Wipe feature will delete all the selected files and folders that have been added to the list to be deleted from the portal.

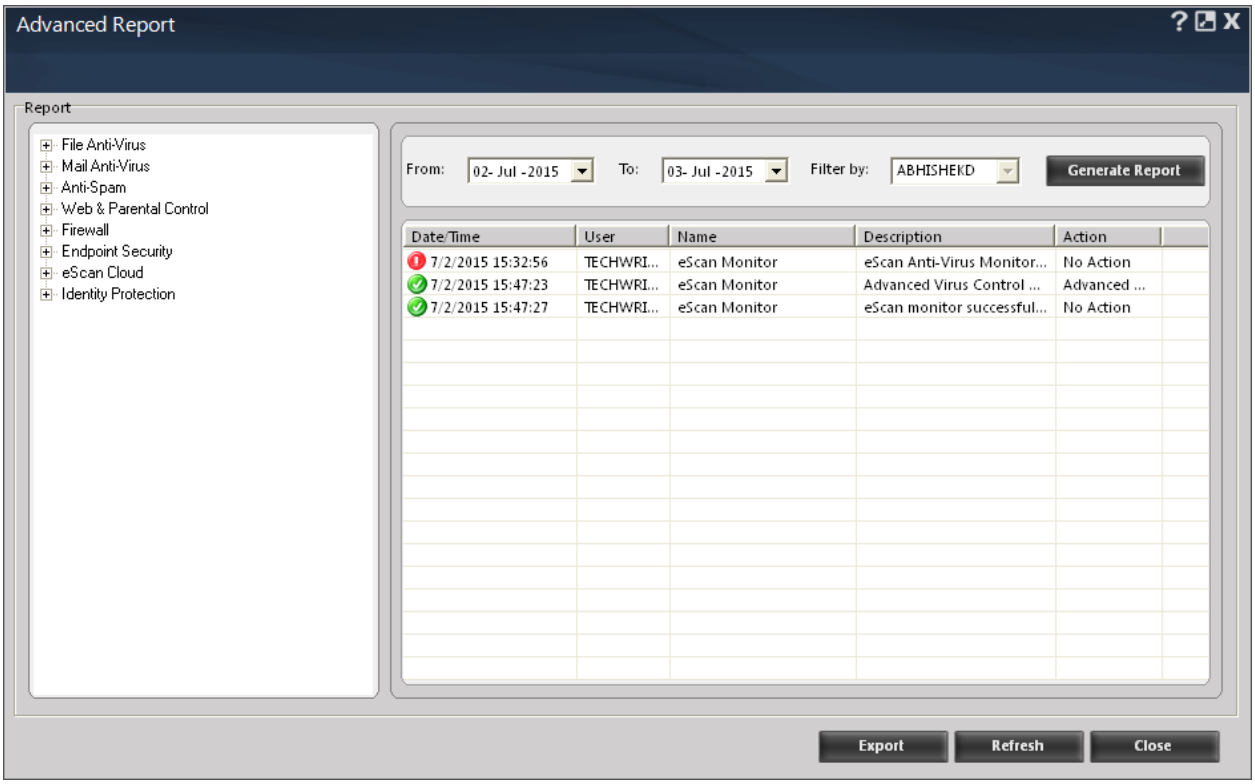
- Click **Data Wipe** option to remotely wipe all the selected files and folders or only delete the cookies and click confirm.

Points to remember
• Successful execution of all the features is completely dependent on the internet connection on the lost / stolen laptop.
• If the device is set as lost, the time taken for the device to sync with the anti-theft portal is five minutes.
• The Status for all the features and actions will remain as “Request Pending” till the lost or stolen laptop is synced with the eScan anti-theft portal.
• If the device is not set as lost, it will take ten minutes to sync with the anti-theft portal if the system is connected to internet.
• The camera and Screenshot feature will save only the last two successful executions on the anti-theft portal.
• Once you have recovered your system, click on “I recovered device” to deactivate all the features.

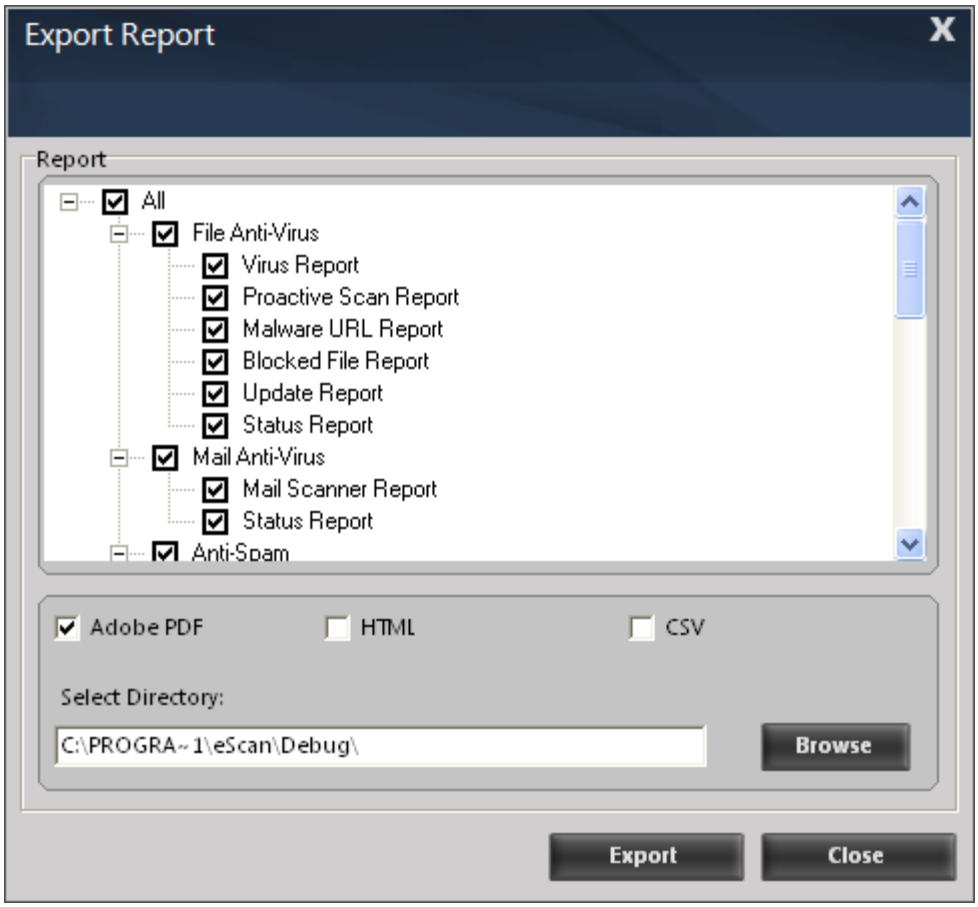
Reports

eScan will generate reports for File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Firewall, Endpoint Security, and eScan Cloud modules.

Click Reports link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to Advance Report window; it displays the report for all the modules of eScan Total security Suite.



- eScan generates reports of all its modules; You can View/Generate a report of any module through Reports link present in every module.
- eScan maintains a log of all the recent activities; it includes the date and timestamp, the user details, description and the action taken.
- It will also allow you to export the particular report as per your requirement or all the existing reports in .pdf/ HTML/CSV format; it will also allow you to choose the path to save these files on to your computer.



Procedure to export the report files:

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

Contact Us

We offer 24x7 FREE Online+ Technical Support to our customers through email and Live Chat. We also provide FREE Telephonic Support to our customers during business hours.

Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries. You can contact our support team via Live Chat by visiting the following link.
http://www.escanav.com/english/livechat.asp

Forums Support

You can even join the MicroWorld Forum at **http://forums.escanav.com** to discuss all your eScan related problems with eScan experts.

Email Support

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

For sales enquiry, please write to: sales@escanav.com
For support enquiry, please write to: support@escanav.com
For knowledgebase, please visit: http://forums.escanav.com
For Wikipedia/Help, please visit: http://www.escanav.com/wiki

Regional Offices

Asia Pacific
MicroWorld Software Services Pvt. Ltd.
CIN No.: U72200MH2000PTC127055
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**

USA
MicroWorld Technologies Inc. 31700 W 13 Mile Rd, Ste 98, Farmington Hills, MI 48334, USA.
Tel: +1 248 855 2020/2021
Fax: +1 248 855 2024

Germany
MicroWorld Technologies GmbH Drosselweg 1,
76327 Pfinztal,
Germany.
Tel: +49 72 40 94 49 0920
Fax: +49 72 40 94 49 0992

Malaysia
MicroWorld Technologies Sdn Bhd (722338-A)
E-8-6, Megan Avenue 1, 189, Jalan Tun Razak, 50400
Kuala Lumpur, Malaysia.
Tel: +603 2333 8909/8910
Fax: +603 2333 8911

South Africa:
MicroWorld Technologies South Africa (Pty) Ltd.
376 Oak Avenue, Block C (Entrance at 372 Oak Avenue) Ferndale,
Randburg, Gauteng, South Africa.
Tel: Local: 08610 eScan (37226), International: +27 11 781 4235
Fax: +086 502 0482

For sales enquiry, please write to: sales@escanav.com
For support enquiry, please write to: support@escanav.com
For knowledgebase, please visit: http://forums.escanav.com
For Wikipedia/Help, please visit: http://www.escanav.com/wiki