eScan™

Internet Security Suite

(Cyber Vaccine Edition)

User Guide

NEW

- Two Factor Authentication (OTP)

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

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

Document Number: 5BUG/21.07.2021/22.0
Current Software Version: 22.0.xxxx.xxxx
Copyright Notice: Copyright © 2021. All rights reserved.

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

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

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

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

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

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

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

Welcome

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

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

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

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

MicroWorld designs its security solutions with an aim of providing 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 22.

Thank you for choosing eScan.

The eScan Team

Contents

Overview

eScan Internet Security Suite (Cyber Vaccine Edition) protects the home network against online threats without slowing down the system. Being powerful and lightweight eScan defend the personal sensitive data by blocking the latest malware, phishing, and cyber-attacks. The eScan's real-time protection monitors the computer continuously to determine where and what is safe online.

eScan ISS is equipped latest innovative technologies like malware detection, heuristic scan, and many more. Parental control is designed to protect children and teenagers by blocking access to websites based on categories such as hate, violence, and porn. It also consists of advanced two-way firewall, spam filter, gaming mode, and several other techniques that will keep the system safe, clean and optimized.

Key Features

Real-time Protection

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

Optimized Performance

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

Two-Factor Authentication

eScan provides an extra layer of protection to the Windows login process that authenticates and prevent any hackers from accessing the computer and personal data. This offers an additional step of security as cyberthieves require more than a username and password for authentication.

Powerful Anti-Ransomware

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

Smart Parental Control

eScan has designed Smart Parental Control to protect children and teenagers from latest cyberthreats. It allows to set time restriction on access the websites and applications for different users based on their age. Different users have different profile and access/web control rights.

Windows Essential Updates

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

Two-way Firewall

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

eBackup

eBackup helps in taking regular backup of the system/files/folder as it can be lost or damaged due to various issues such as virus outbreak, ransomware attack, or cloud-based disaster. eScan allows you to schedule and store the backup file according to the user requirements.

Effective Endpoint Security

eScan provides protection from the known and unknown threats that can spread through USB or Firewire-based portable storage device, such as Flash drive, Webcam, SD Card, and more. It offers an advanced Application Control that allows you to block/permit applications and prevent the critical threats.

Advanced Anti-Phishing

eScan uses proactive detection technique that detects phisinglinks, emails, and attachment based on the malicious behavior and blocks automatically every time when they try to reach the email boxes.

What's new

eScan ISS (Cyber Vaccine Edition) has introduces following new features:

- Advanced Malware Detection
- Two-Factor Authentication
- Highly Optimized Performance
- Heuristic Scan
- Sophisticated Threat-Detection Mechanism
- Powerful And Layered Anti-Ransomware Technology
- Smart Parental Control

Pre-requisites for installing eScan

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

First Time Installation

- Ensure that you have Administrator Rights on the system where you wish to install eScan Internet Security Suite.

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

Renewal and Upgrade

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

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

System Requirements

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

Operating System

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

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

Minimum Hardware Requirements

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

Installation Steps

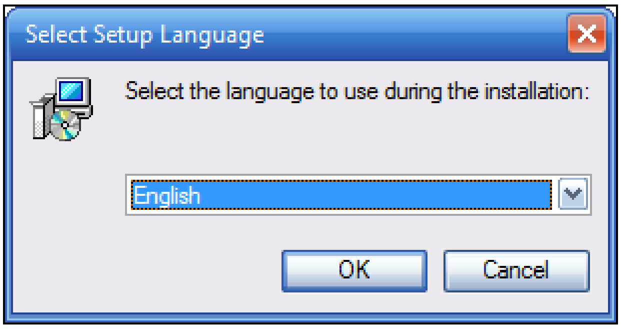
Install eScan Internet Security Suite (ISS) either by using the eScan setup file or using the eScan product installation CD/DVD. To download the eScan setup file, visit the following link: https://www.escanav.com/en/windows-antivirus/internet-security-suite.asp

Installing Internet 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 of installation does not start on its own, click Install option on the CD ROM, this will open the one click installation wizard setup of Internet Security Suite on your computer.

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

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

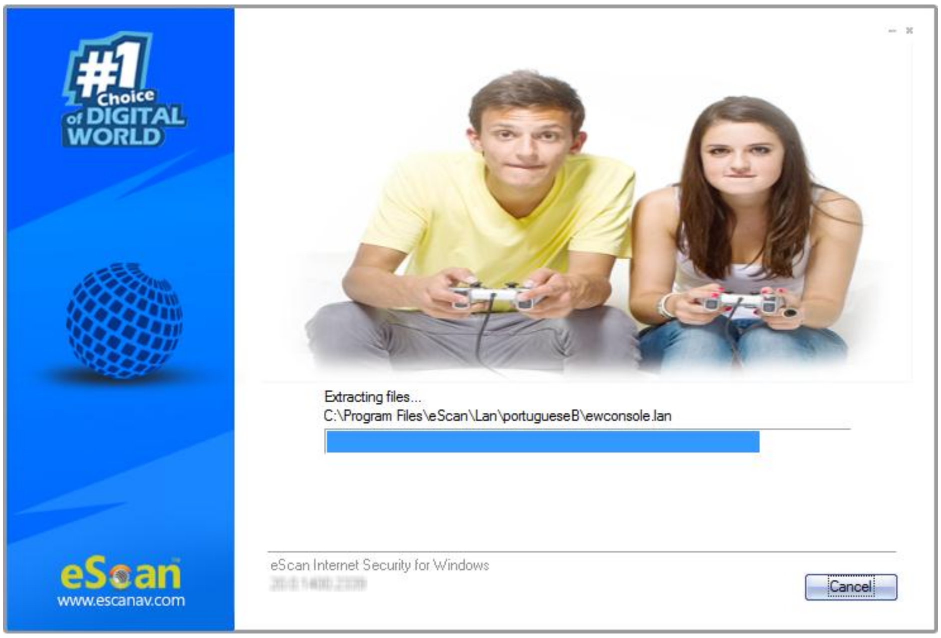
   Use the drop-down menu to select Product language in which your eScan ISS will be installed.



Select the language to use during the installation:

English

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

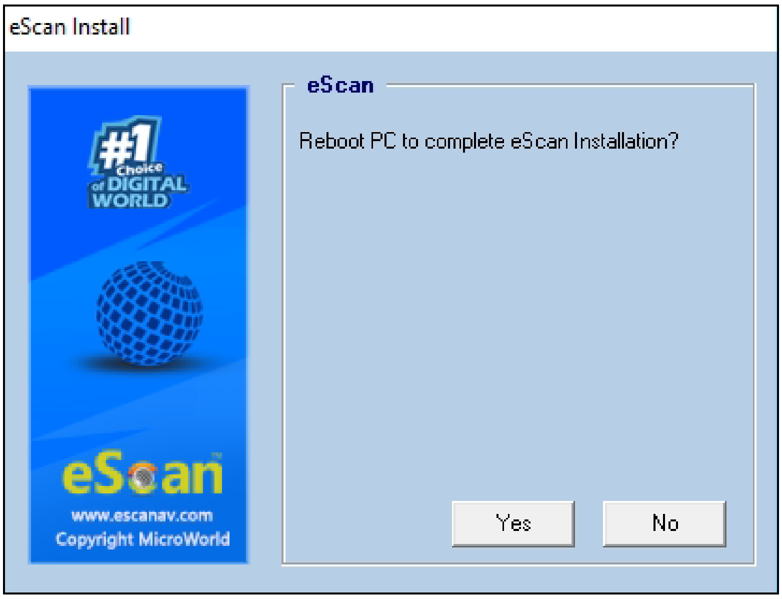


Extracting files...
C:\Program Files\eScan\Lan\portugueseB\ewconsole.lan

eScan Internet Security for Windows

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

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



eScan Install

eScan

Reboot PC to complete eScan Installation?

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

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

Product Activation

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

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

You can use any of the following methods to activate the eScan Internet Security Suite.

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

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

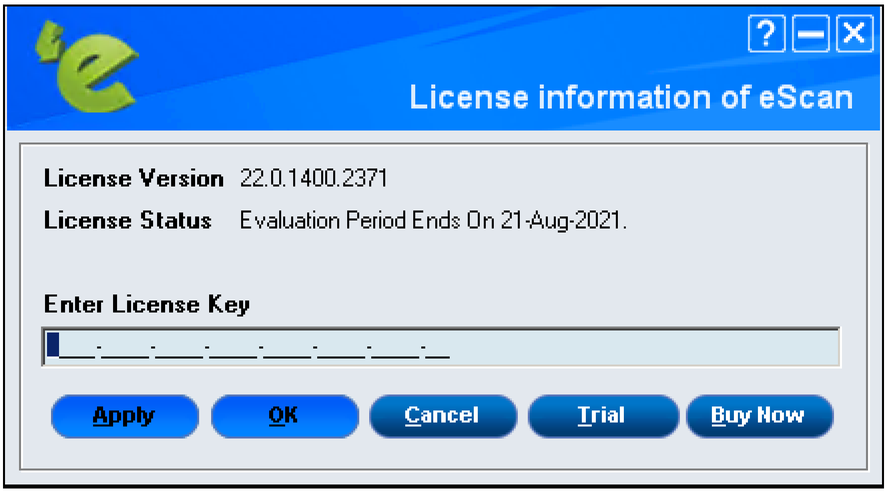
To use this feature, you need to install the eScan TPN for Android devices from Play Store or for iOS devices from App Store on your smart device.

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

Adding and Activating the License Key

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

1. Click **Start**, point to **All Programs**, point to **eScan for Windows**, and then click **eScan Registration**. The License information of eScan window appears.



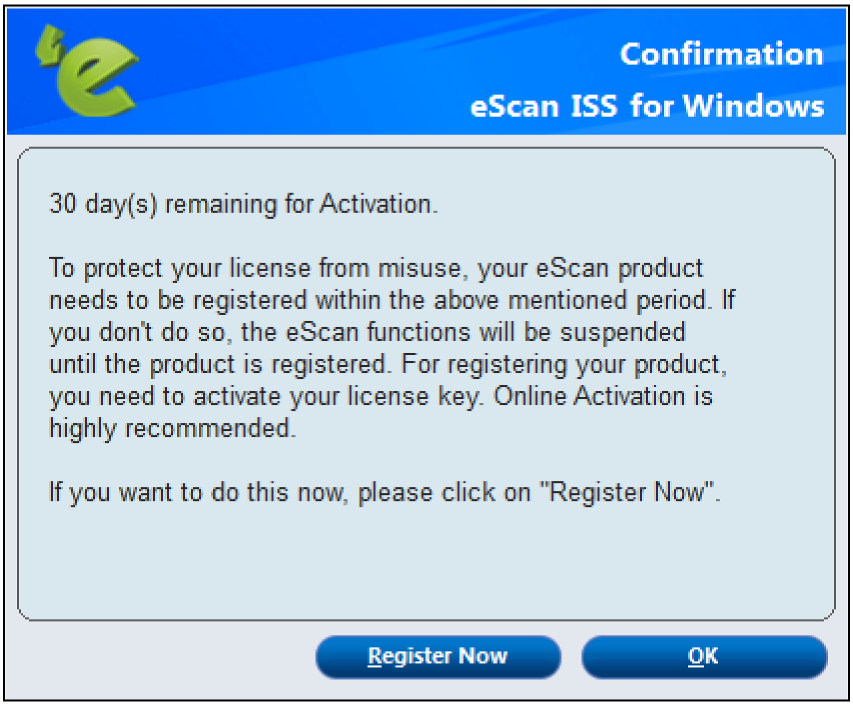
License information of eScan

License Version 22.0.1400.2371

License Status Evaluation Period Ends On 21-Aug-2021.

Enter License Key

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



Confirmation
eScan ISS for Windows

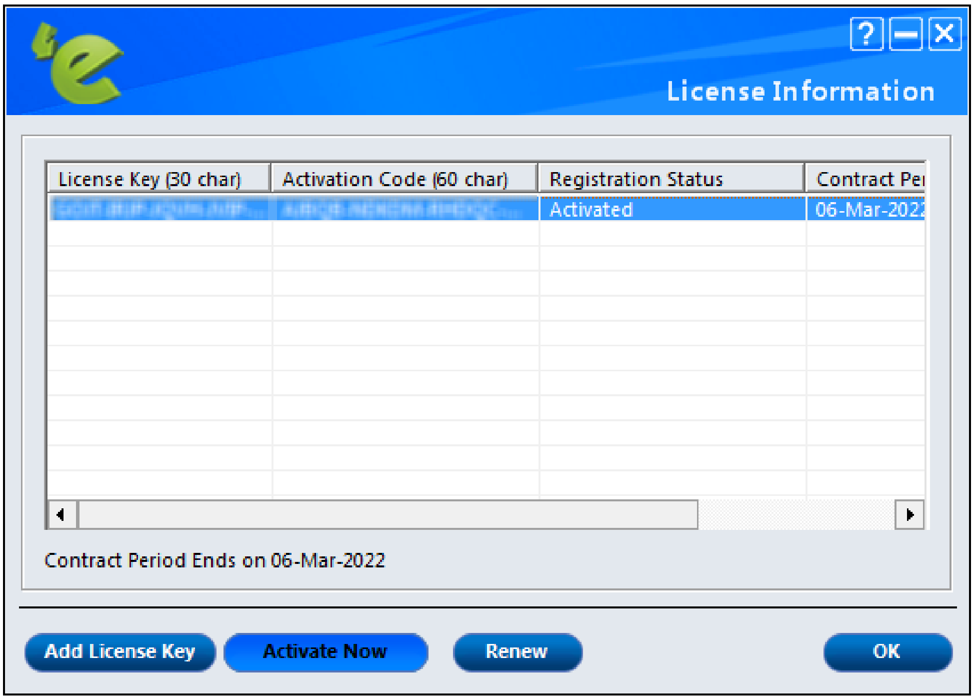
30 day(s) remaining for Activation.

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

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

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

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



License Information

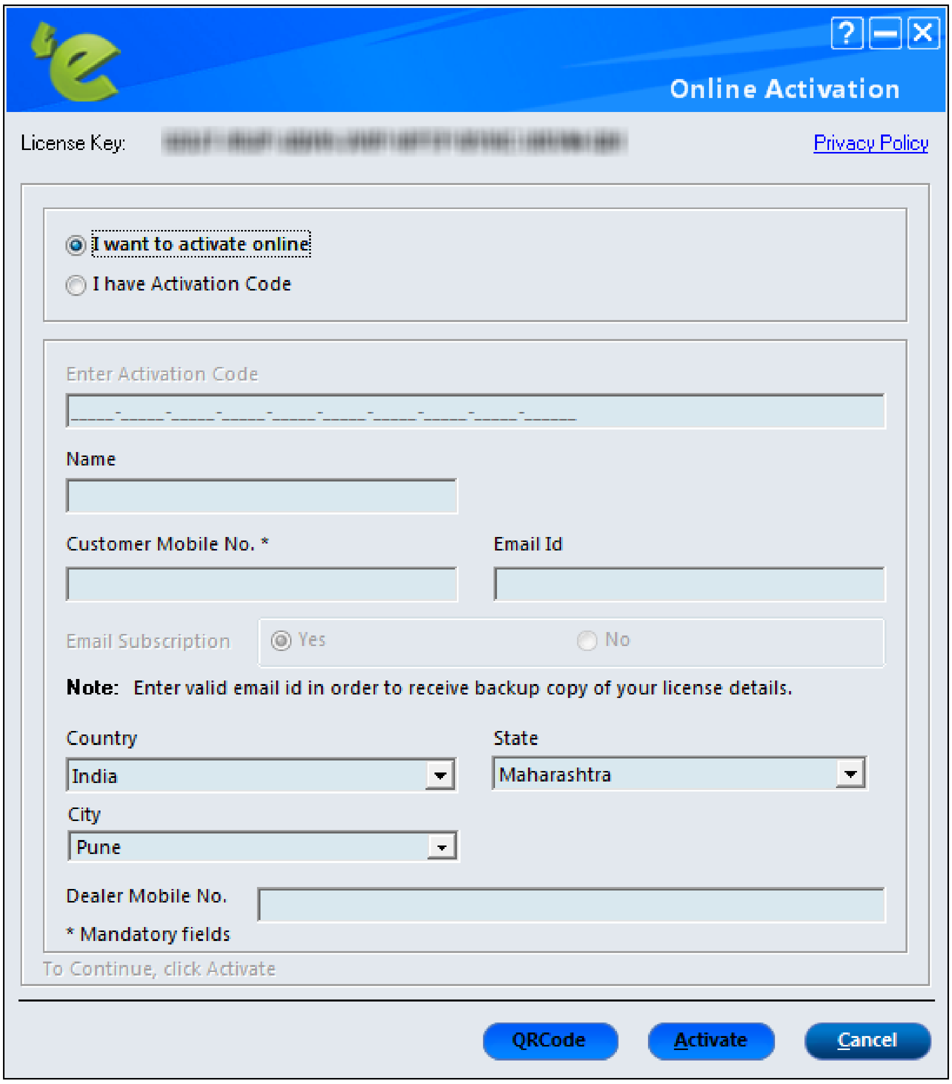
License Key (30 char)	Activation Code (60 char)	Registration Status	Contract Pe
[redacted]	[redacted]	Activated	06-Mar-202

Contract Period Ends on 06-Mar-2022

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

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

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



Online Activation

License Key: [redacted]

Privacy Policy

● I want to activate online

○ I have Activation Code

Enter Activation Code: _____-_____-_____-_____-_____-_____-_____-_____-_____-______

Name:

Customer Mobile No. *:

Email Id:

Email Subscription: ● Yes ○ No

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

Country: India

State: Maharashtra

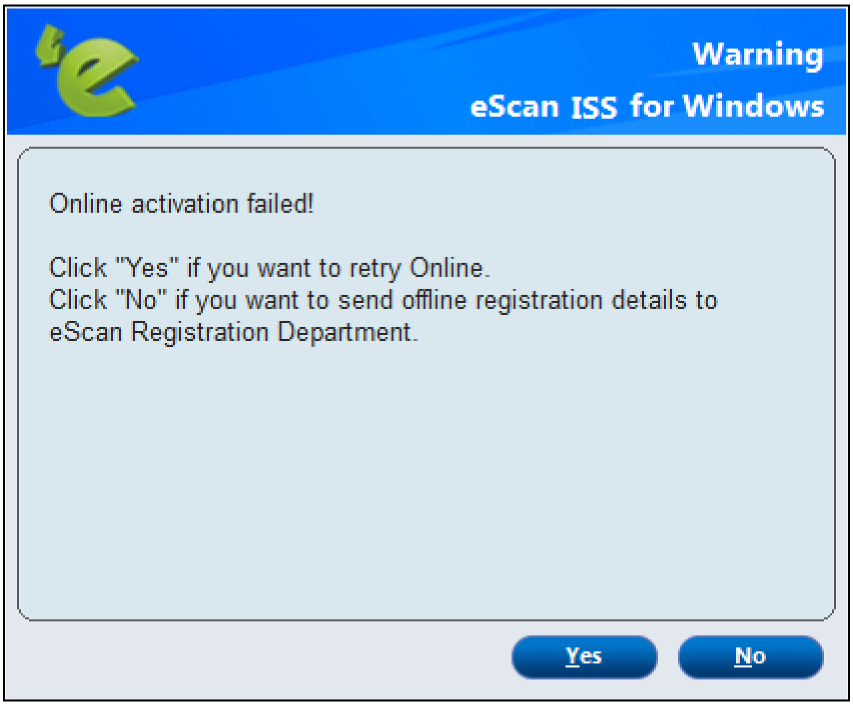
City: Pune

Dealer Mobile No.:

* Mandatory fields

To Continue, click Activate

5. Specify the details of the following fields:
    - **I want to activate online**: By default, this option is selected. When you click this option Name, Email Id *, Confirm Email Id*, Email Subscription, Country, State, and Dealer Mobile Number* fields are available.
    Click this button to activate the eScan product online. You need to have active internet connection to activate online. In case, if you do not have internet connection the online activation fails and displays the following dialog box.



Online activation failed!

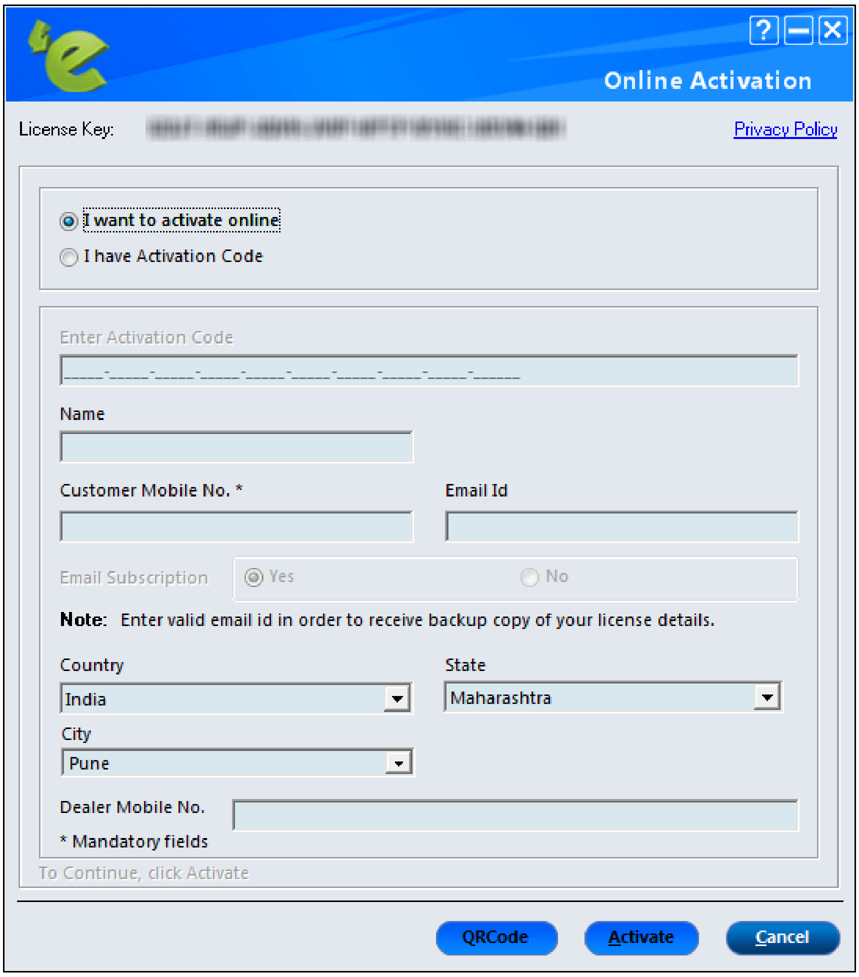
Click "Yes" if you want to retry Online.
Click "No" if you want to send offline registration details to eScan Registration Department.

    Click **No**, an **OnlineRegister.TXT** file gets generated with registration details. You have to send the **OnlineRegister.TXT** file to register@escanav.com, wherein you receive an activation code to the specified email ID.
    - **I have Activation Code**: When you click this option only **Enter Activation Code** field is available. To learn more click here.
    Click this option, if you already have activation code received through an email from register@escanav.com.
    In the **Enter Activation Code** field, type or copy and paste the activation code. This enables you to activate the eScan product immediately.
6. Click **Activate**.
    The license key gets activated.

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

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

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



Online Activation

License Key: [redacted] Privacy Policy

● I want to activate online

○ I have Activation Code

Enter Activation Code

_____-_____-_____-_____-_____-_____-_____-_____-_____-_____-______

Name

Customer Mobile No. *

Email Id

Email Subscription ● Yes ○ No

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

Country: India

State: Maharashtra

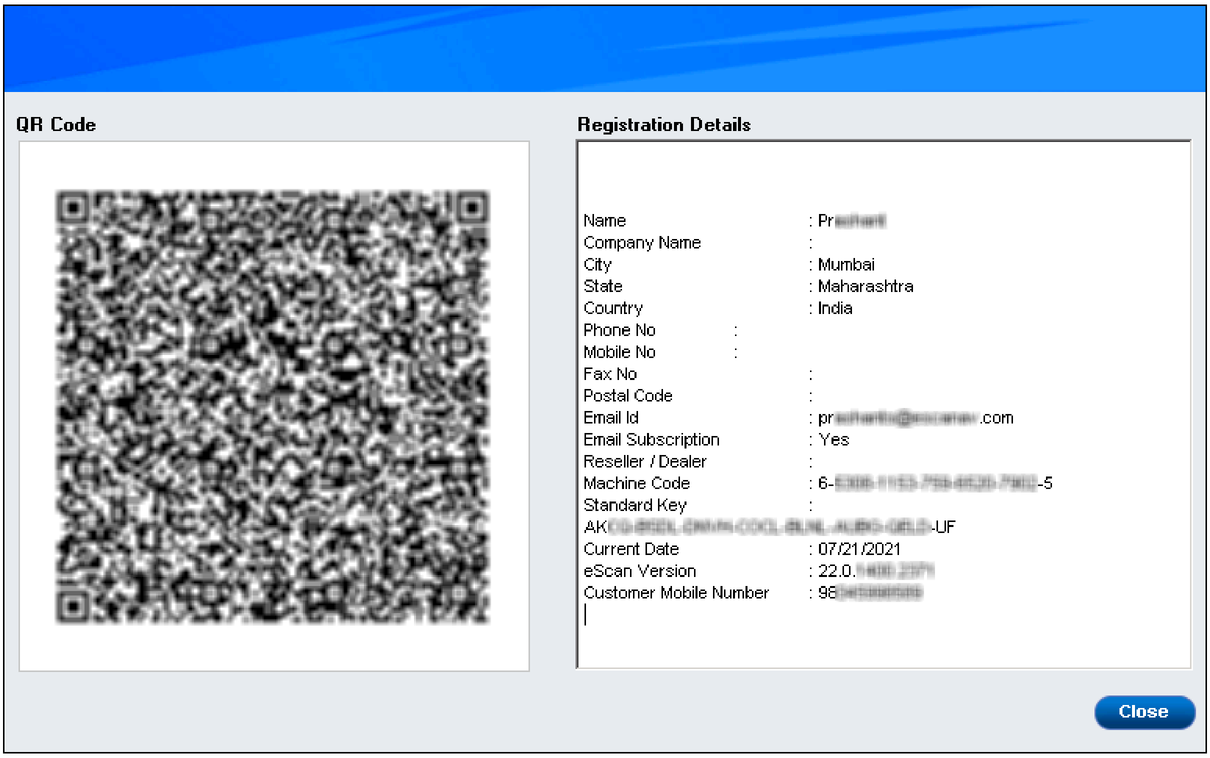
City: Pune

Dealer Mobile No.

* Mandatory fields

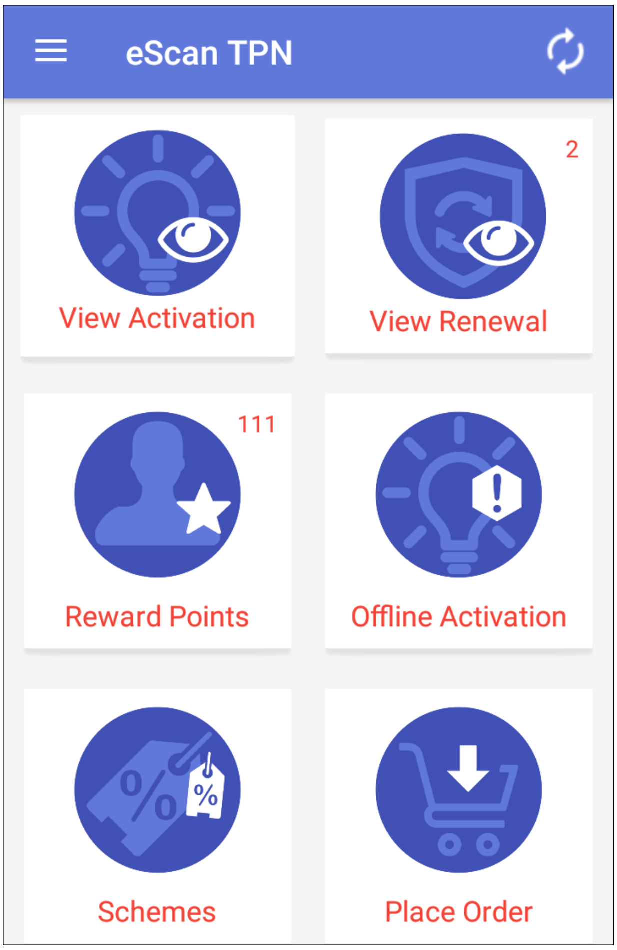
To Continue, click Activate

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

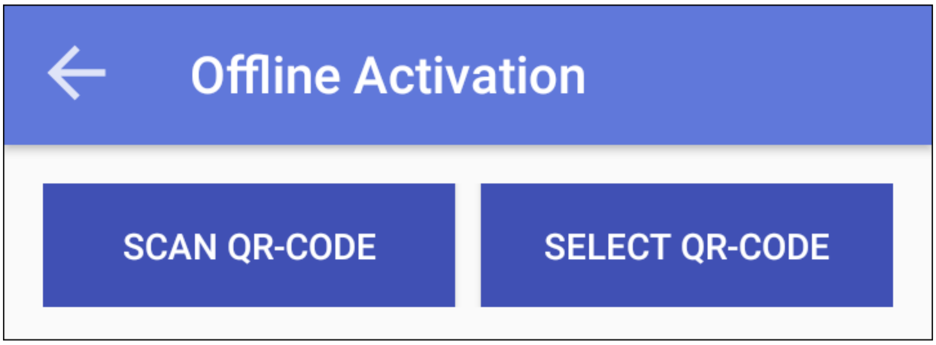


Name : Pr[redacted]
Company Name :
City : Mumbai
State : Maharashtra
Country : India
Phone No :
Mobile No :
Fax No :
Postal Code :
Email Id : pr[redacted].com
Email Subscription : Yes
Reseller / Dealer :
Machine Code : 6-[redacted]-5
Standard Key :
AK[redacted]-UF
Current Date : 07/21/2021
eScan Version : 22.0.[redacted]
Customer Mobile Number : 98[redacted]

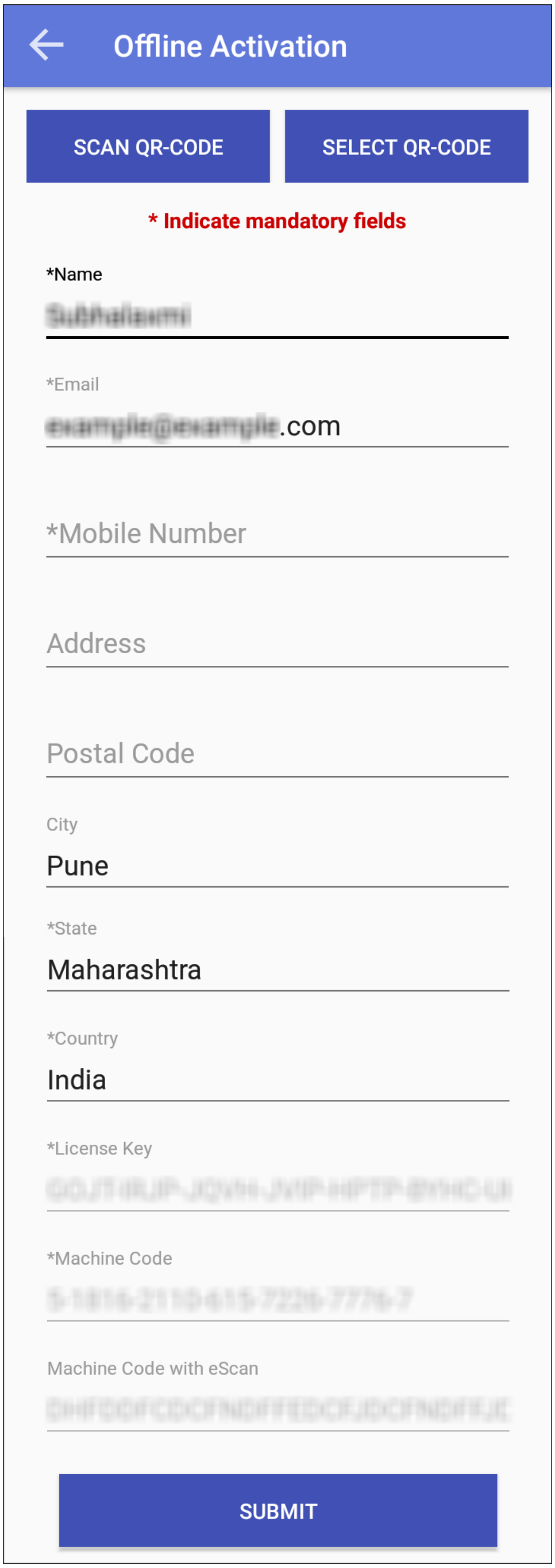
3. In the eScan TPN app, tap **Offline Activation**.



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



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



* Indicate mandatory fields

*Name
[redacted]

*Email
[redacted].com

*Mobile Number

Address

Postal Code

City
Pune

*State
Maharashtra

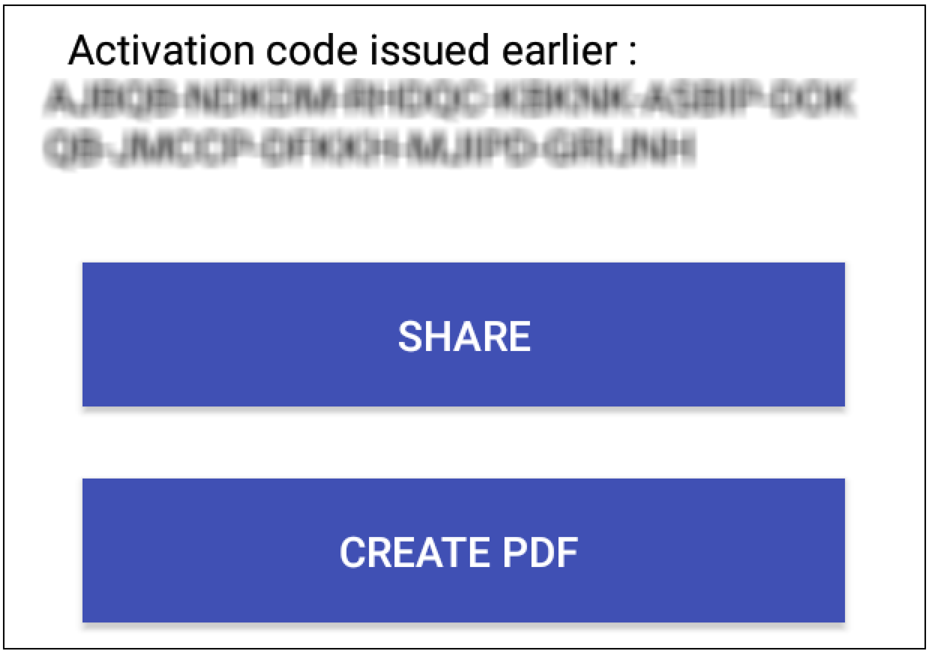
*Country
India

*License Key
[redacted]

*Machine Code
[redacted]

Machine Code with eScan
[redacted]

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



Activation code issued earlier :
[redacted]

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

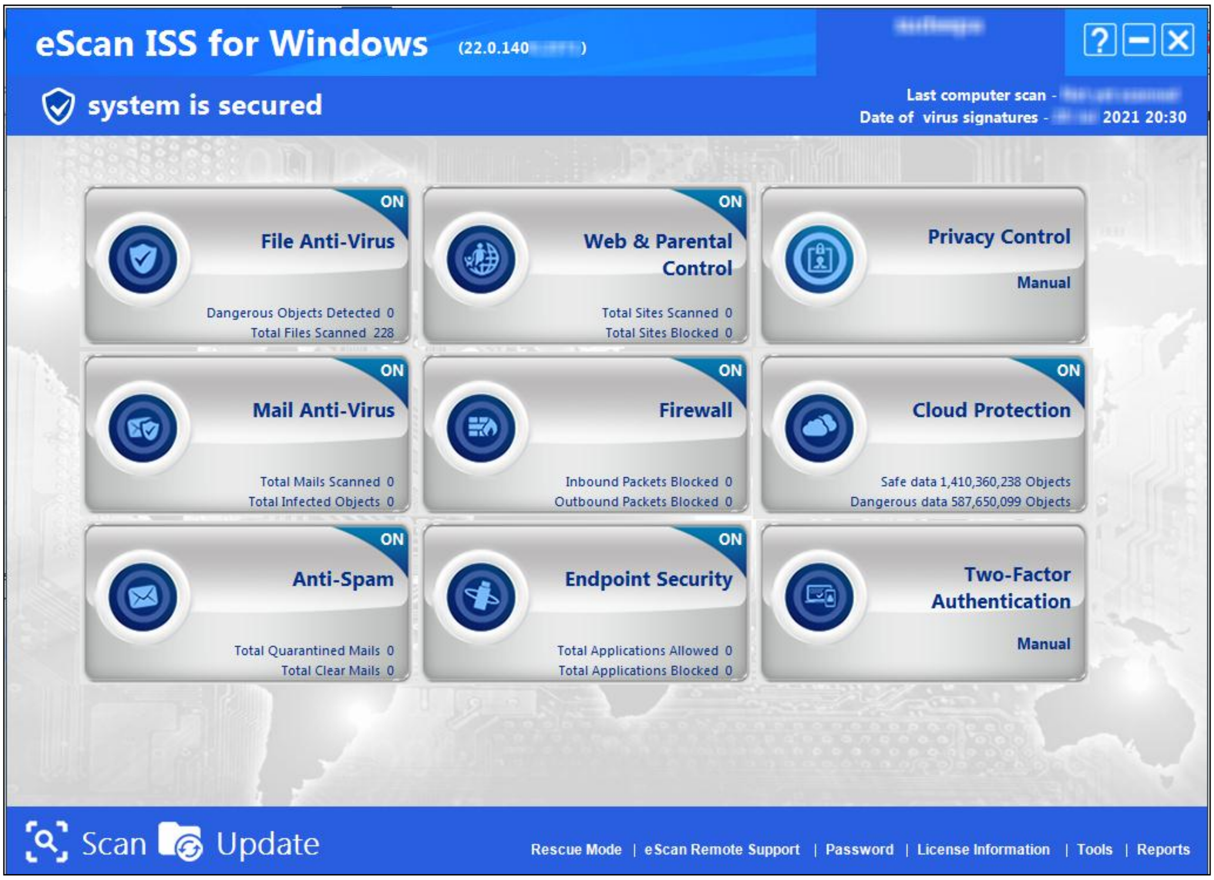
Getting Started

The following sections will be give you the detailed description and configuration procedure of all the eScan GUI and Modules presents in the eScan Internet Security Suite.

Graphical User Interface (GUI)

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

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



eScan ISS for Windows (22.0.140[redacted])

[redacted]

system is secured

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 20:30

File Anti-Virus — ON
Dangerous Objects Detected 0
Total Files Scanned 228

Web & Parental Control — ON
Total Sites Scanned 0
Total Sites Blocked 0

Privacy Control
Manual

Mail Anti-Virus — ON
Total Mails Scanned 0
Total Infected Objects 0

Firewall — ON
Inbound Packets Blocked 0
Outbound Packets Blocked 0

Cloud Protection — ON
Safe data 1,410,360,238 Objects
Dangerous data 587,650,099 Objects

Anti-Spam — ON
Total Quarantined Mails 0
Total Clear Mails 0

Endpoint Security — ON
Total Applications Allowed 0
Total Applications Blocked 0

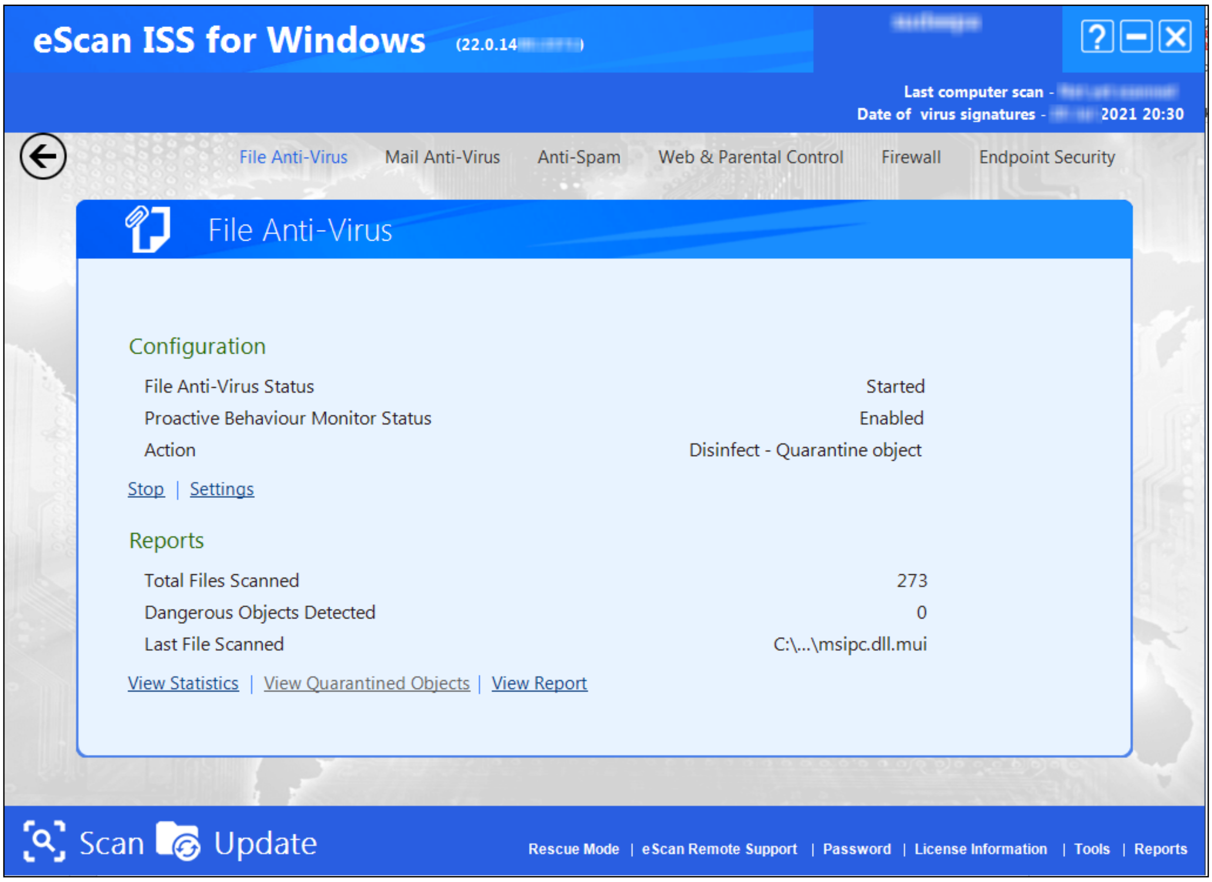
Two-Factor Authentication
Manual

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

File Anti-Virus

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

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


eScan ISS for Windows (22.0.14[redacted])
[redacted]
File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
File Anti-Virus
Stop | Settings
View Statistics | View Quarantined Objects | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 20:30

Configuration

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

Reports

Total Files Scanned	273
Dangerous Objects Detected	0
Last File Scanned	C:\...\msipc.dll.mui

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

- Configuration
- Reports

Configuration

This section displays the following information:

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

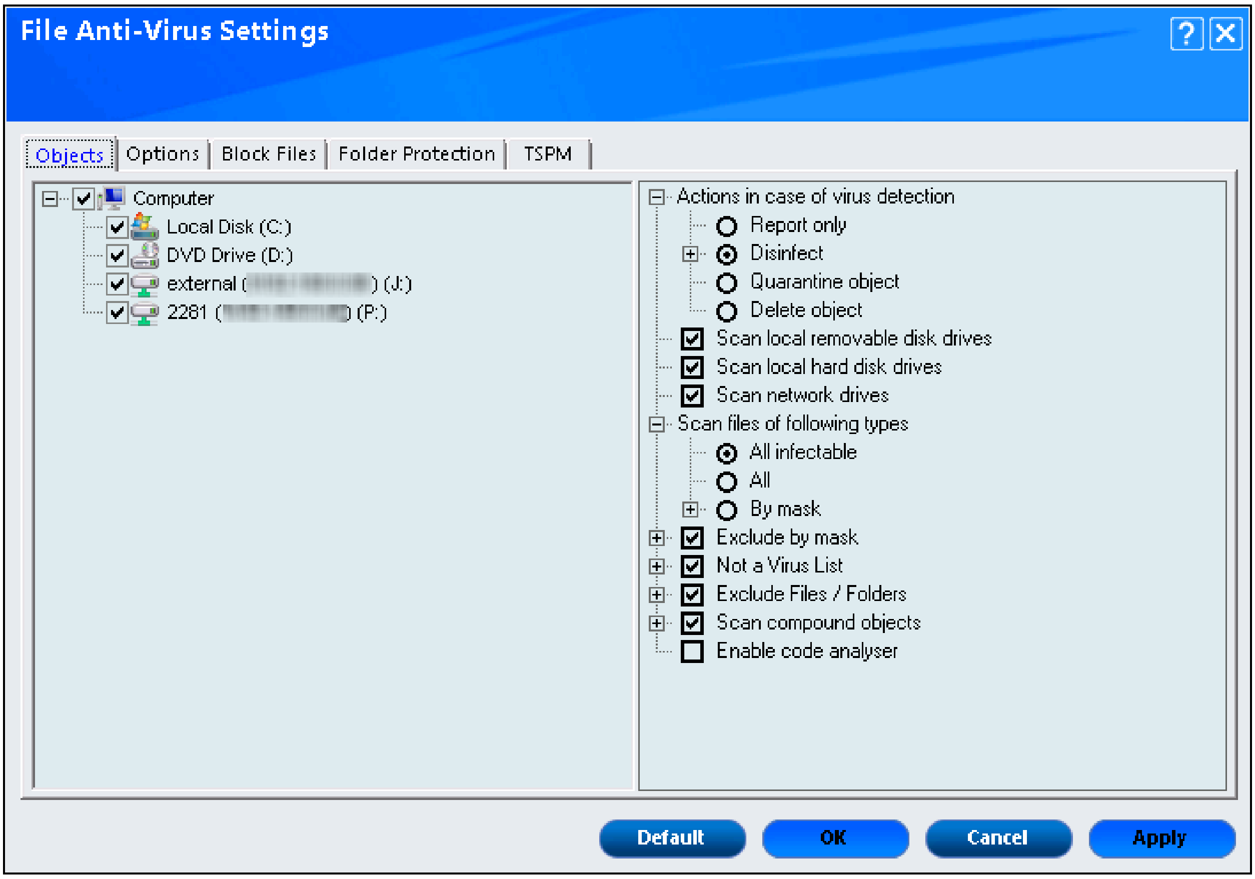
Settings

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

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

Objects

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



File Anti-Virus Settings

- ☑ Computer
  - ☑ Local Disk (C:)
  - ☑ DVD Drive (D:)
  - ☑ external ([redacted]) (J:)
  - ☑ 2281 ([redacted]) (P:)

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

Actions in case of virus definition

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

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

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

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

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

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

Scan files of following types

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

Exclude by mask

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

Not a Virus List

File Anti-Virus is able to detect the riskware. Riskware are legitimate program that are not strictly malicious, but pose some sort of risk for the user in another way. You can add the names of riskware, such as remote admin software to the riskware list in the **Not a Virus List** dialog box by double-clicking the **Add / Delete** option, if you are certain that they are not malicious. This option is enabled by default and the riskware list is empty by default.

Exclude Files/Folders

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

Scan compound objects

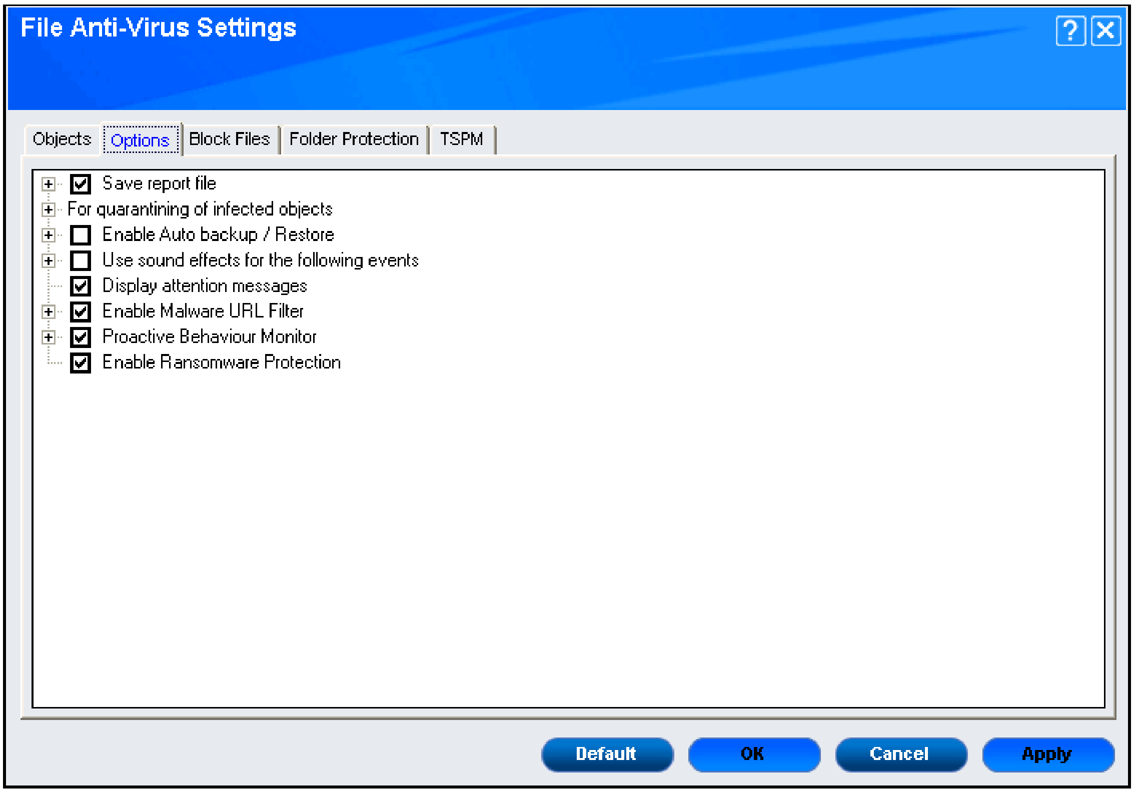
This option allows to scan the archives and packed files during the scan. The **Archive** check box allows to scan archive files. The depth level of an archived file up to which you want to scan can be defined in **Archive Depth Level** field. By default, value is 16, but you can change it by double-clicking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

Enable code analyser

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

Options

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



☑ Save report file
For quarantining of infected objects
□ Enable Auto backup / Restore
□ Use sound effects for the following events
☑ Display attention messages
☑ Enable Malware URL Filter
☑ Proactive Behaviour Monitor
☑ Enable Ransomware Protection

It provides the following options for configuration:

Save report file

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

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

For quarantining of infected objects

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

Enable Auto backup / Restore

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

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

Use sound effects for the following events

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

Display attention messages

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

Enable Malware URL Filter

This option is blocks the access to malicious websites/URL.

Proactive Behaviour Monitor

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

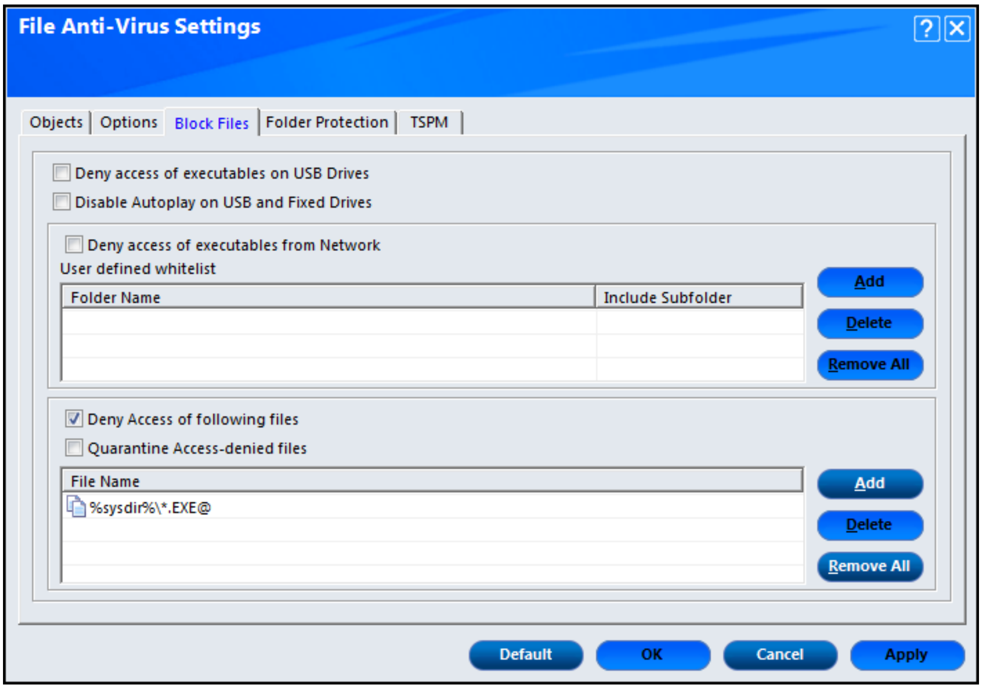
It also allows to view the list of files that are blocked from executing on the system. You can add a File to White list or Block List using this option.

Enable Ransomware Protection

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

Block Files

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



File Anti-Virus Settings

□ Deny access of executables on USB Drives

□ Disable Autoplay on USB and Fixed Drives

□ Deny access of executables from Network

User defined whitelist

Folder Name	Include Subfolder

☑ Deny Access of following files

□ Quarantine Access-denied files

File Name
%sysdir%*.EXE@

It provides the following options for configuration:

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

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

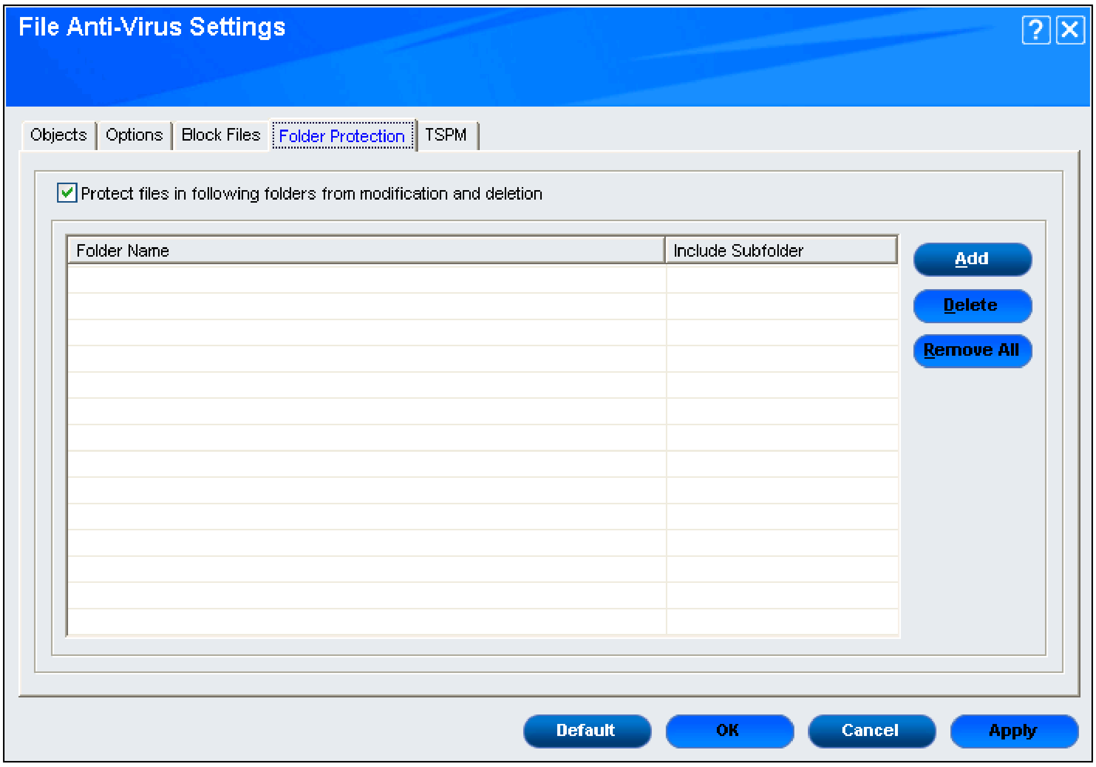
Deny access of executables from Network
This check box option helps to prevent executables from network from being executed on the computer. This option also allows to whitelist the folder/subfolder on the network as per the requirement. The whitelisted folder/subfolder can be access the executable from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

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

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

Folder Protection

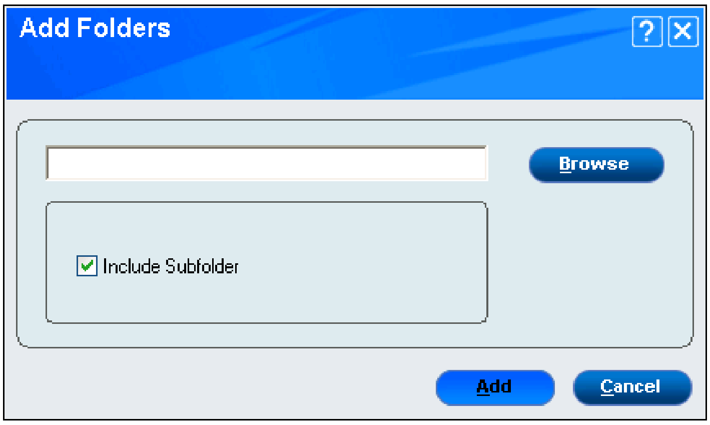
This tab helps to protect specific folders from being modified or deleted by adding them to the **Folder Protection list**.



☑ Protect files in following folders from modification and deletion

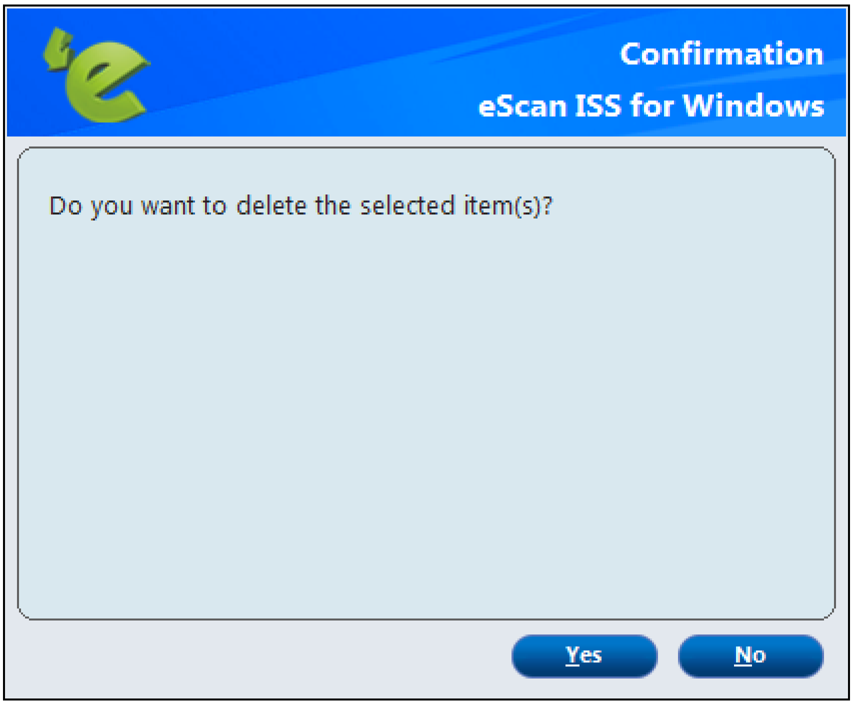
It provides the following options for configuration:

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



☑ Include Subfolder

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



Confirmation

eScan ISS for Windows

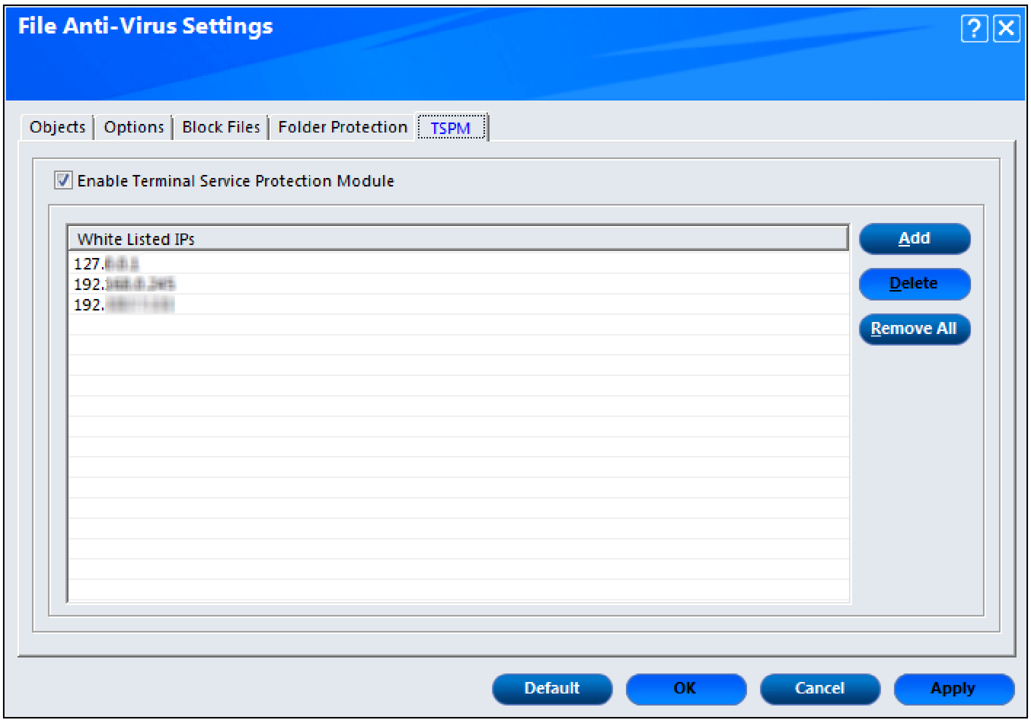
Do you want to delete the selected item(s)?

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

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

TSPM

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

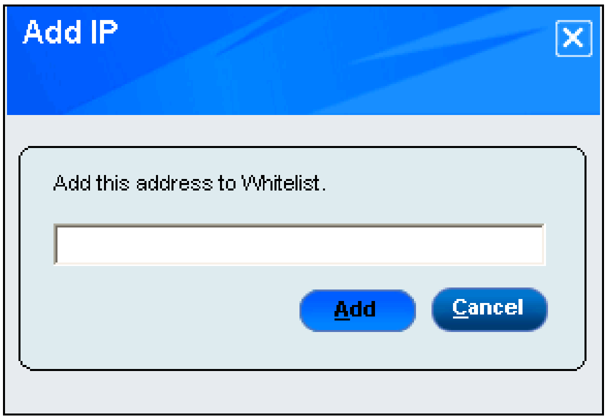


☑ Enable Terminal Service Protection Module

White Listed IPs
127.[redacted]
192.[redacted]
192.[redacted]

Enable Terminal Service Protection Module

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



Add this address to Whitelist.

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

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

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

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

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

Reports

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

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

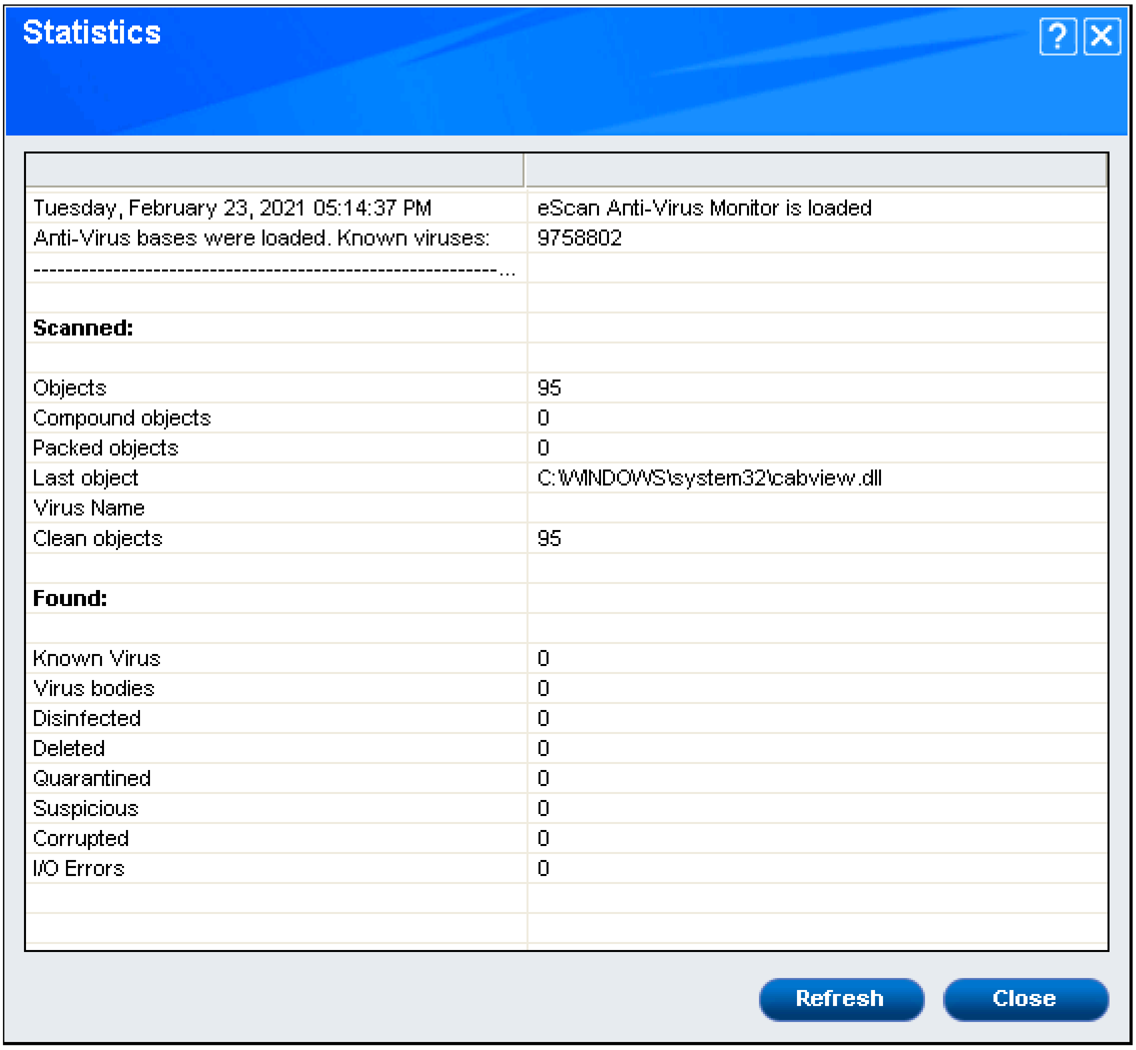
Dangerous Objects Detected
It shows the total number of viruses or malicious software detected by the File Anti-Virus monitor on a real-time basis.

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

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

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

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

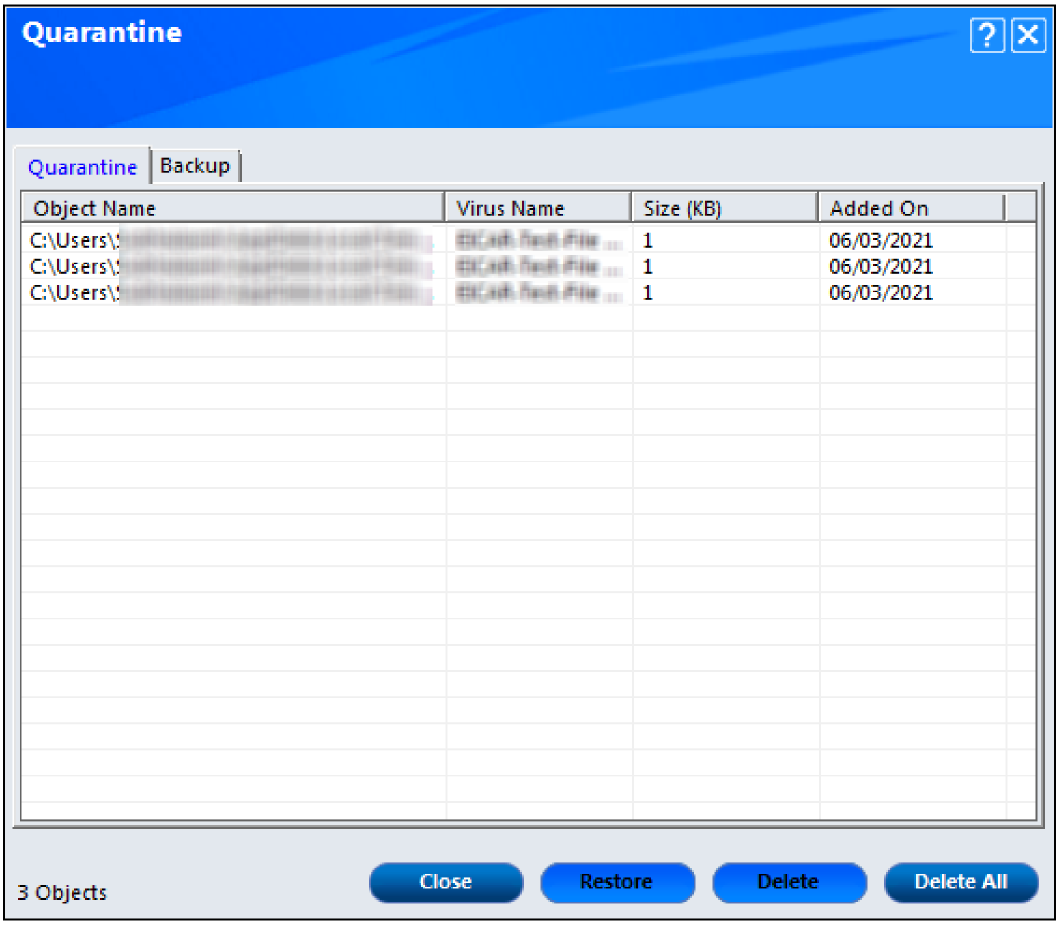


Tuesday, February 23, 2021 05:14:37 PM	eScan Anti-Virus Monitor is loaded
Anti-Virus bases were loaded. Known viruses:	9758802
--...	
Scanned:	
Objects	95
Compound objects	0
Packed objects	0
Last object	C:\WINDOWS\system32\cabview.dll
Virus Name	
Clean objects	95
Found:	
Known Virus	0
Virus bodies	0
Disinfected	0
Deleted	0
Quarantined	0
Suspicious	0
Corrupted	0
I/O Errors	0

View Quarantined Objects

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

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

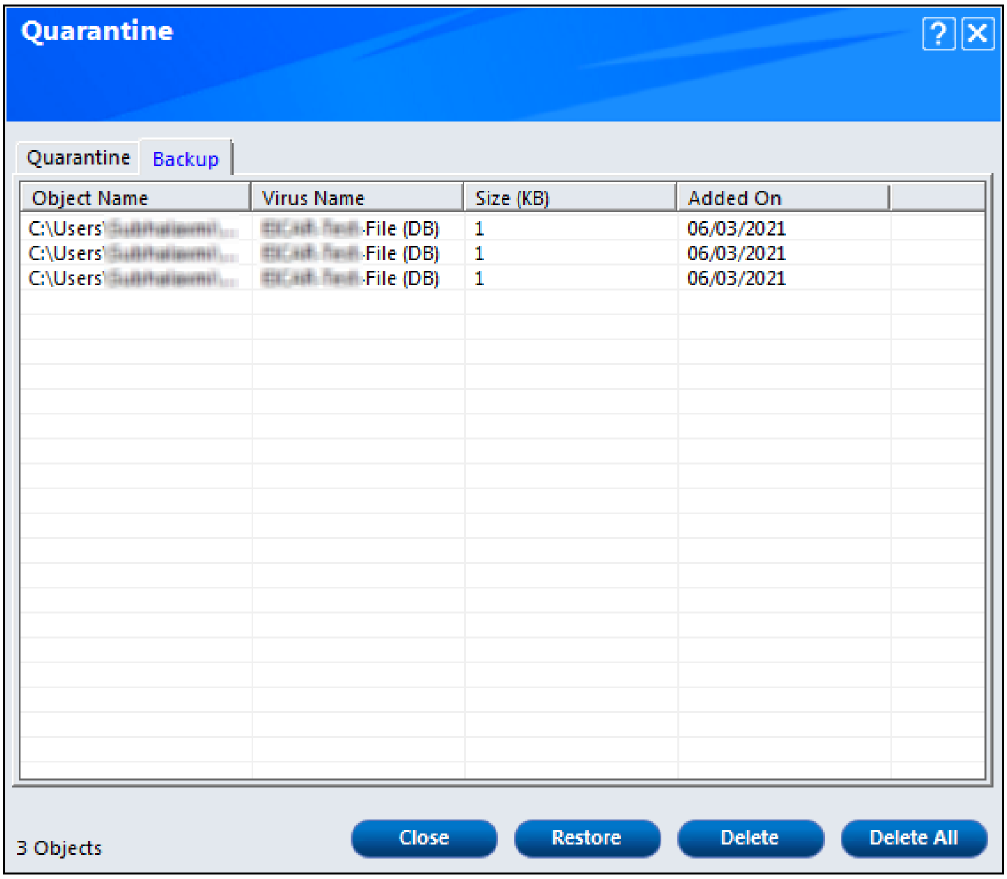


Object Name	Virus Name	Size (KB)	Added On
C:\Users\[redacted]	[redacted]	1	06/03/2021
C:\Users\[redacted]	[redacted]	1	06/03/2021
C:\Users\[redacted]	[redacted]	1	06/03/2021

3 Objects

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

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



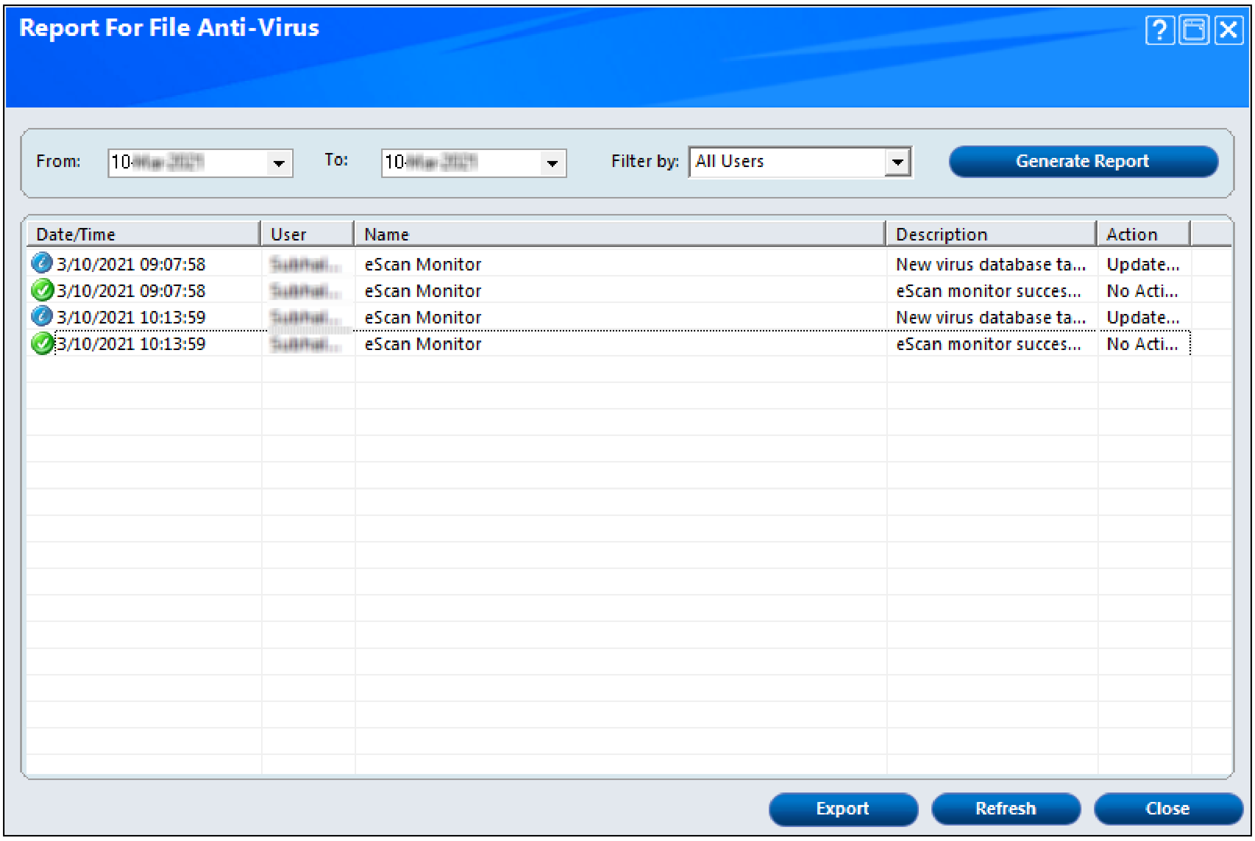
Object Name	Virus Name	Size (KB)	Added On
C:\Users\[redacted]	[redacted]-File (DB)	1	06/03/2021
C:\Users\[redacted]	[redacted]-File (DB)	1	06/03/2021
C:\Users\[redacted]	[redacted]-File (DB)	1	06/03/2021

3 Objects

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

View Report

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



From: 10[redacted] To: 10[redacted] Filter by: All Users

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

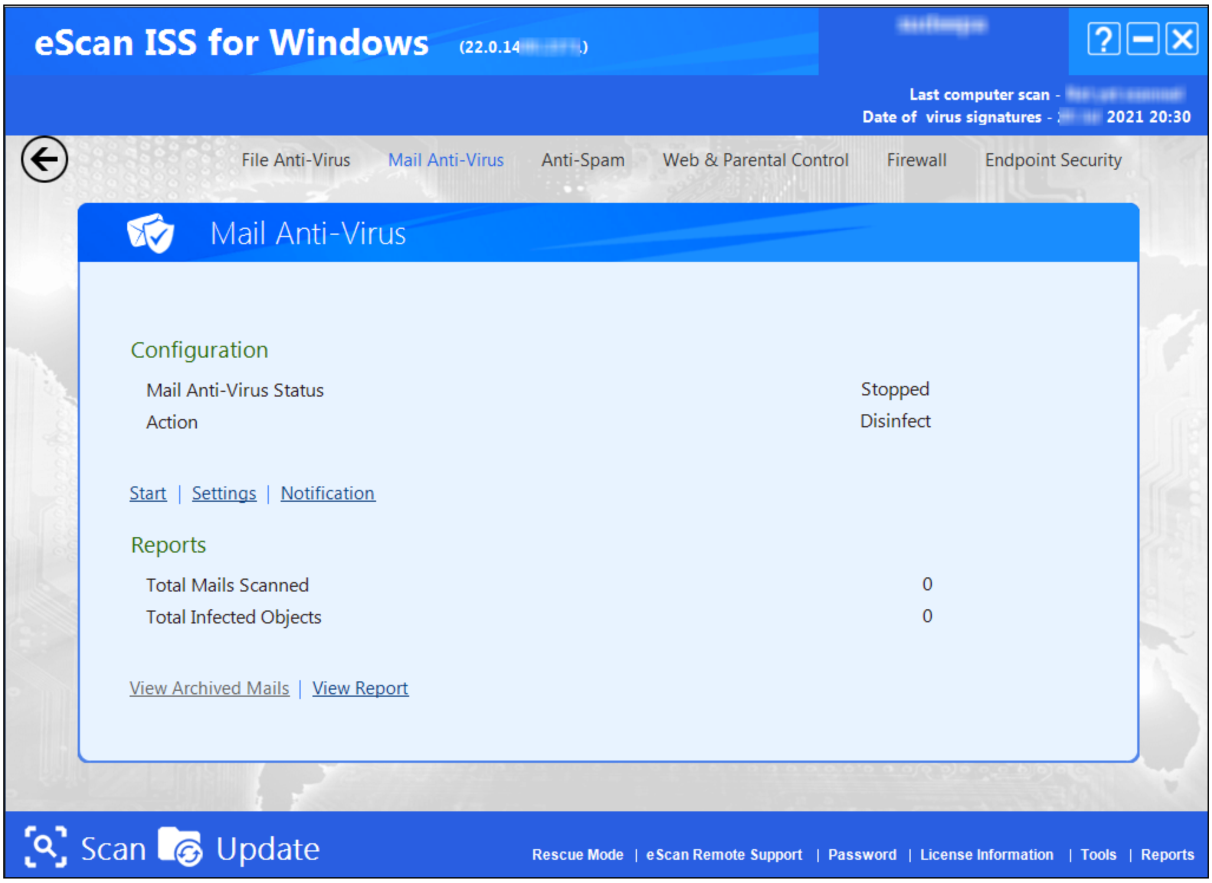
To refresh the generated report, click **Refresh** button. Click **Close,** to close report window. You can export the generated report using **Export** button.

You can export reports in the following formats:

- PDF
- HTML
- CSV

Mail Anti-virus

Mail Anti-Virus scans all incoming and outgoing emails for viruses, spyware, adware, and other malicious objects. It helps you send virus warnings to client computers on the Mail Anti-Virus activities. By default, Mail Anti-Virus scans only the incoming emails and attachments, but you can configure it to scan outgoing emails and attachments as well. Moreover, it helps you notify the sender or system administrator, whenever you receive an infected email or attachment.



eScan ISS for Windows (22.0.14[redacted])

[redacted]

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 20:30

Mail Anti-Virus

Configuration

Mail Anti-Virus Status: Stopped
Action: Disinfect

Start | Settings | Notification

Reports

Total Mails Scanned: 0
Total Infected Objects: 0

View Archived Mails | View Report

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

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

Configuration

This section displays the following information:

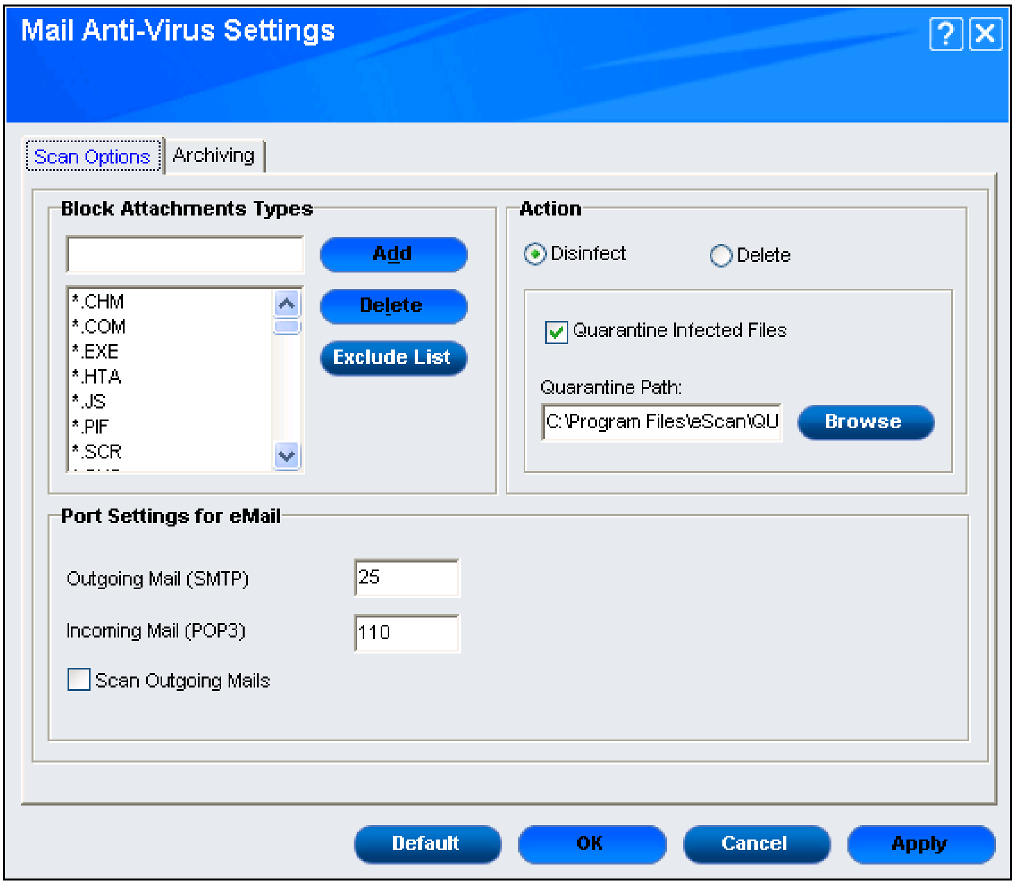
- **Mail Anti-Virus Status**: It displays the status of whether Mail Anti-Virus module is started or stopped.
- **Action**: It displays the type of action set in the Mail Anti-Virus module.
- **Start/Stop**: Click an appropriate option to start/stop or enable/disable Mail Anti-Virus module.
- **Settings**: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

Settings

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

Scan Options

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



Mail Anti-Virus Settings

Scan Options | Archiving

Block Attachments Types

*.CHM
*.COM
*.EXE
*.HTA
*.JS
*.PIF
*.SCR

Action

● Disinfect ○ Delete

☑ Quarantine Infected Files

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

Port Settings for eMail

Outgoing Mail (SMTP): 25

Incoming Mail (POP3): 110

□ Scan Outgoing Mails

This tab helps you to configure the following setting:

Block Attachments Types

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

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

Action

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

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

In both of the above cases you can **Quarantine Infected Files** which is selected by default. Select this check box if you want Mail Anti-Virus to quarantine infected emails or attachments. The default path for storing quarantined emails or attachments is **C:\Program Files\eScan\QUARANT** which you can specify in **Quarantine Path**. However, you can specify a different path for storing quarantined files, if required.

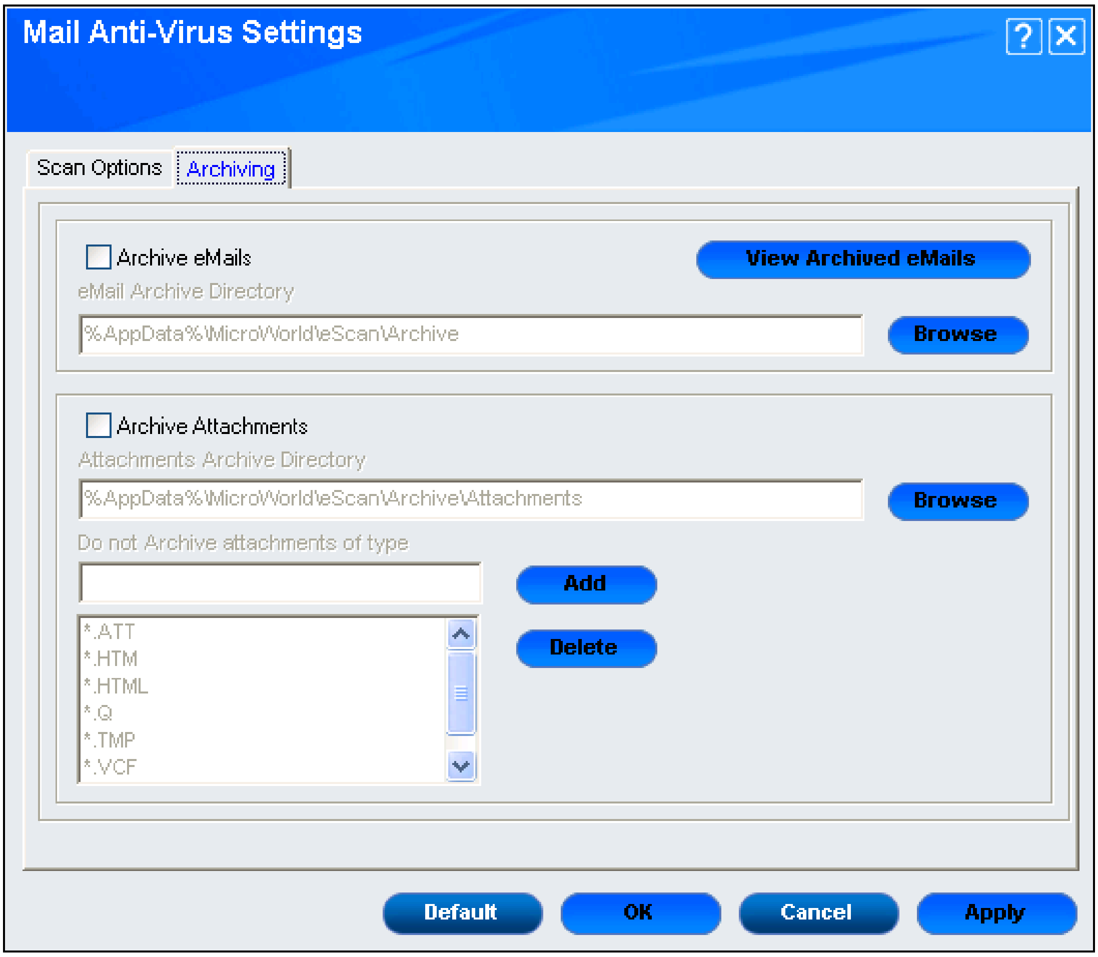
Port Settings for eMail

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

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

Archiving

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



Mail Anti-Virus Settings

□ Archive eMails

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

□ Archive Attachments

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

Do not Archive attachments of type

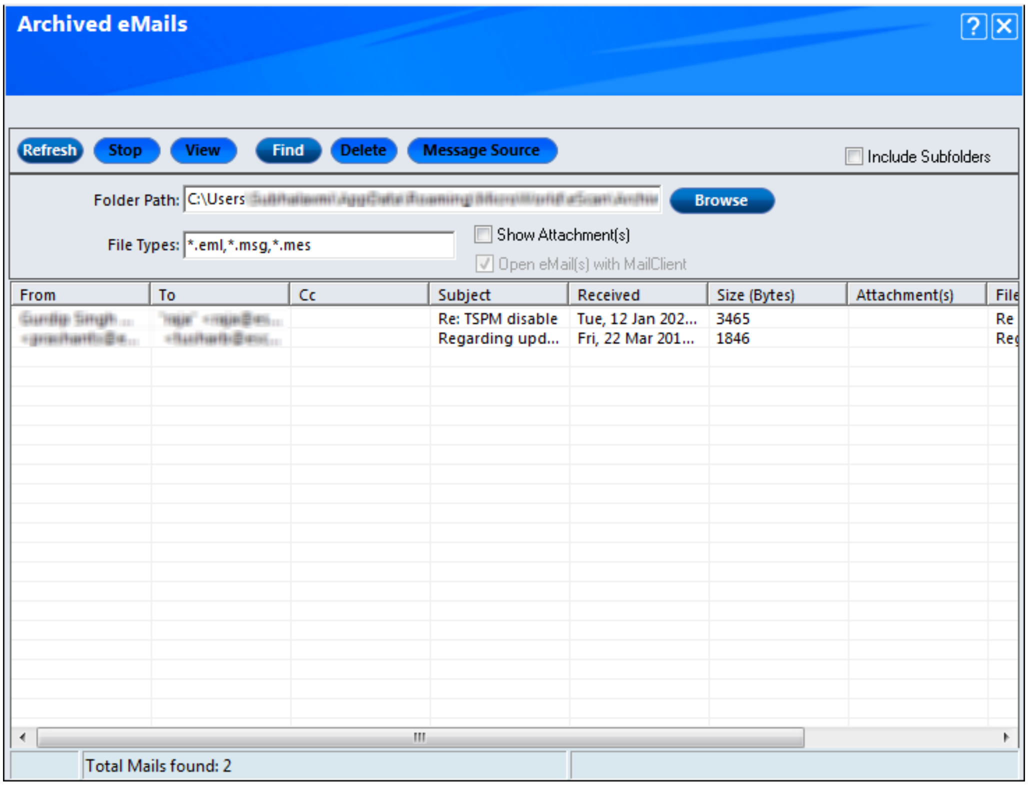
*.ATT
*.HTM
*.HTML
*.Q
*.TMP
*.VCF

The following configuration options are available:

Archive eMails

This check box option helps you archive or back up all scanned emails that you have sent or received. Mail Anti-Virus provides you with the facility of backing up your emails to a given folder. The default path for storing archived emails is **%appdata%\MicroWorld\eScan\Archive**. You can also change the default path by clicking on **Browse** button and provide the path.

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



□ Include Subfolders

Folder Path: C:\Users [redacted]

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

□ Show Attachment(s)

☑ Open eMail(s) with MailClient

From	To	Cc	Subject	Received	Size (Bytes)	Attachment(s)	File
[redacted]	[redacted]		Re: TSPM disable	Tue, 12 Jan 202...	3465		Re
[redacted]	[redacted]		Regarding upd...	Fri, 22 Mar 201...	1846		Re

Total Mails found: 2

Following are the options to configure archived emails:

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

It has the following fields:

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

Archive Attachments

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

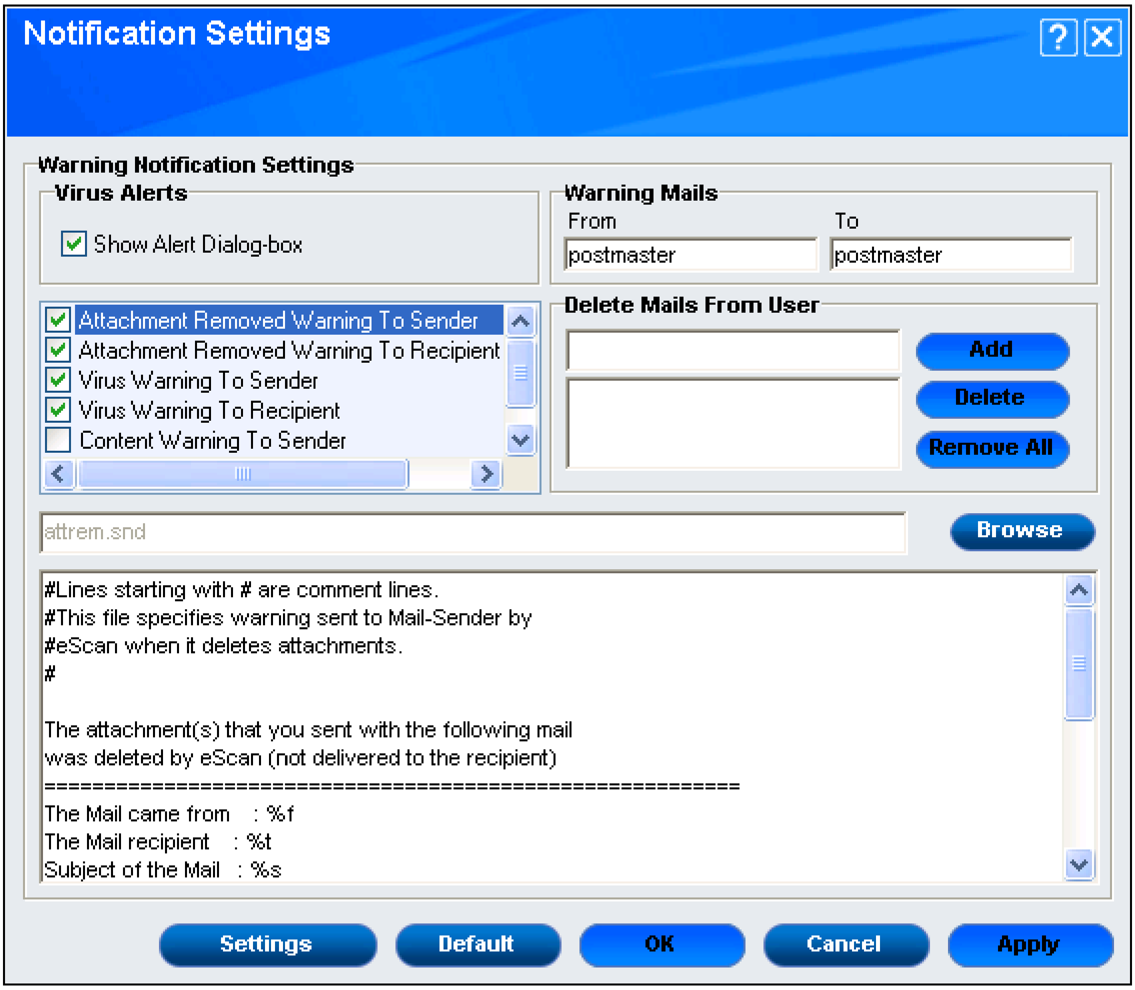
- **Add**: You can add extension that you want to exclude from being archived.
- **Delete**: You can delete the extension that you want to remove from the exclude list.

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

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

Notification

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



Notification Settings

Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

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

Warning Mails
From: postmaster
To: postmaster

Delete Mails From User

attrem.snd

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

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

You can configure the Warning Notification Settings:

Virus Alerts

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

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

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

Warning Mails

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

Delete emails From User

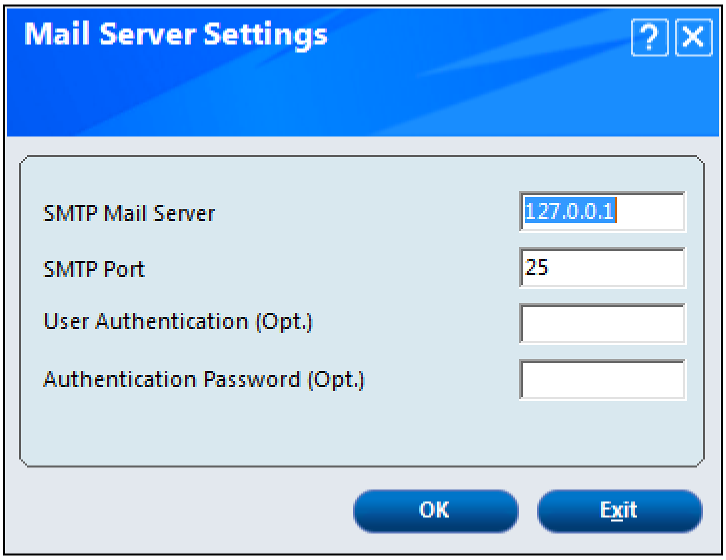
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the mail addresses of such users to the **Delete Mails From User** list. By default, the **Delete Mails From User** section fields are unavailable; it is available only when you type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

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

Settings

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

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



Mail Server Settings

SMTP Mail Server: 127.0.0.1

SMTP Port: 25

User Authentication (Opt.):

Authentication Password (Opt.):

This dialogue box has two buttons:

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

Default

Click this button to apply the default settings.

OK

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

Cancel

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

Apply

Click this button to apply the configured settings.

Reports

This section displays the following information along with the reports:

Total Mails Scanned

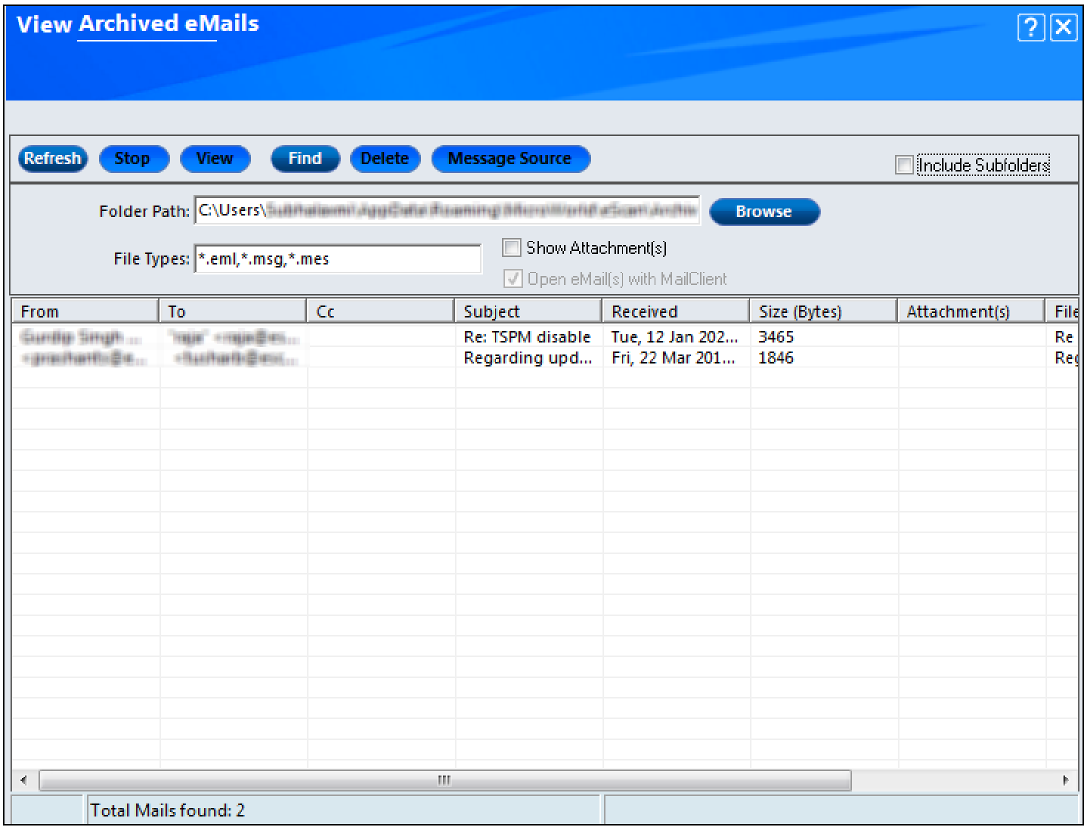
It displays total emails scanned by Mail Anti-Virus module on a real-time basis.

Total Infected Objects

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

View Archived Mails

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



☐ Include Subfolders

Folder Path: C:\Users\[redacted]

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

☐ Show Attachment(s)

☑ Open eMail(s) with MailClient

From	To	Cc	Subject	Received	Size (Bytes)	Attachment(s)	File
[redacted]	[redacted]		Re: TSPM disable	Tue, 12 Jan 202...	3465		Re
[redacted]	[redacted]		Regarding upd...	Fri, 22 Mar 201...	1846		Re

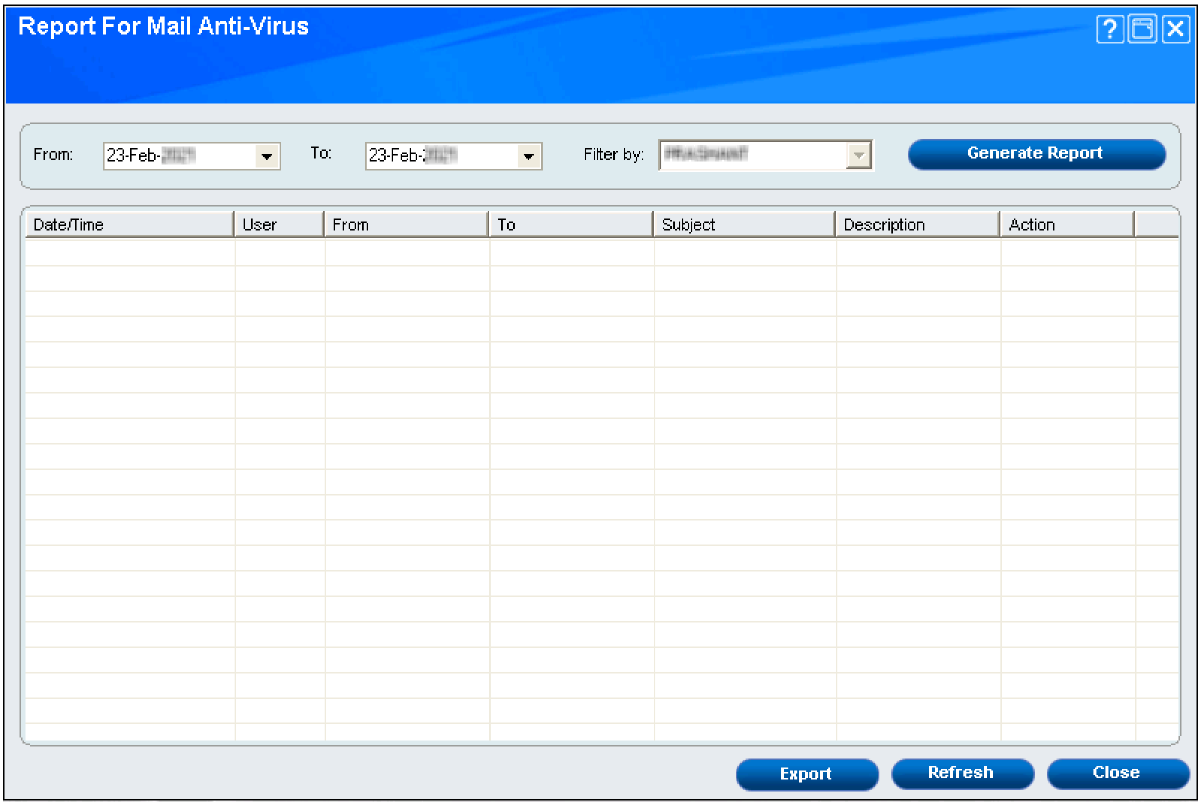
Total Mails found: 2

Following are the options to configure archived emails:

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

View Report

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



From: 23-Feb-[redacted]

To: 23-Feb-[redacted]

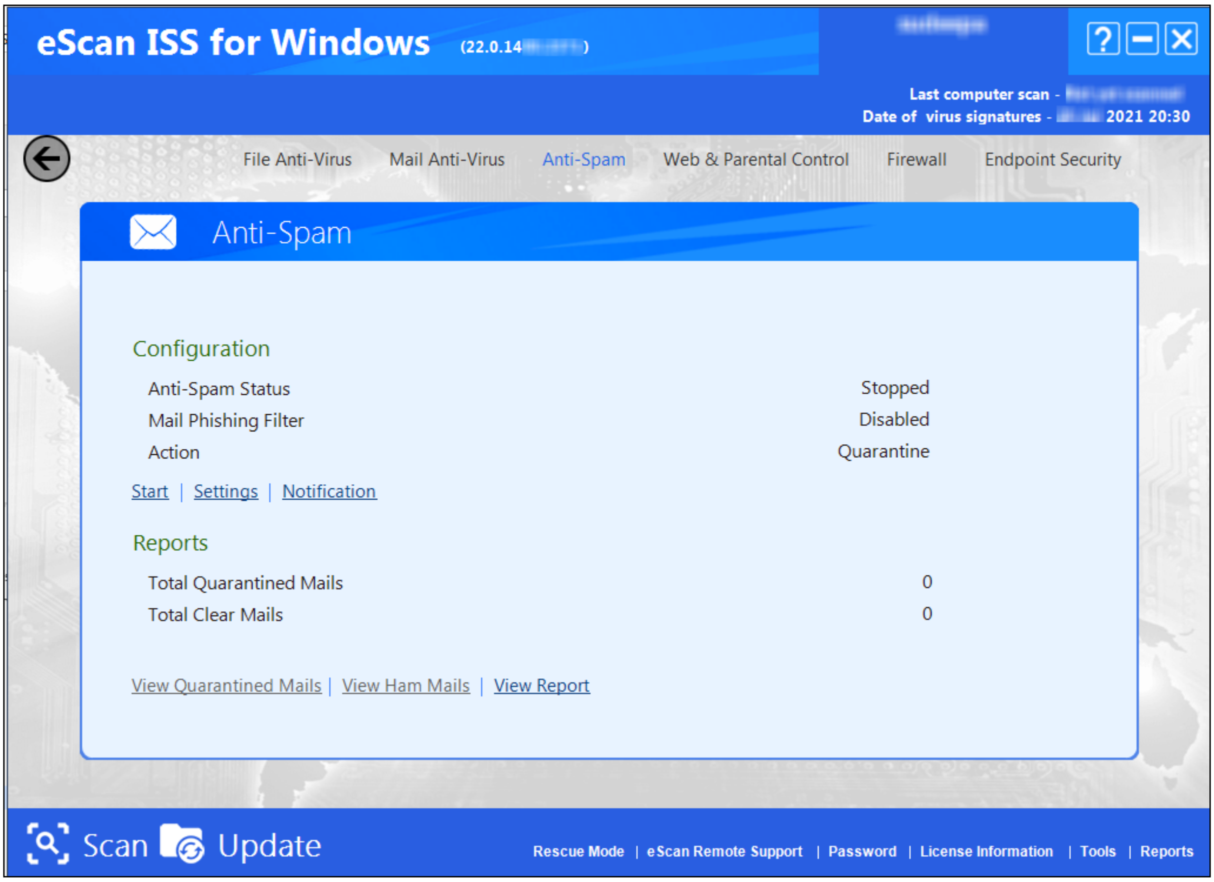
Filter by: [redacted]

You can export the reports in the following format:

- PDF
- HTML
- CSV

Anti-spam

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



eScan ISS for Windows (22.0.14[redacted]) [redacted]

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 20:30

File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security

Anti-Spam

Configuration

Anti-Spam Status	Stopped
Mail Phishing Filter	Disabled
Action	Quarantine

Start | Settings | Notification

Reports

Total Quarantined Mails	0
Total Clear Mails	0

View Quarantined Mails | View Ham Mails | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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

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

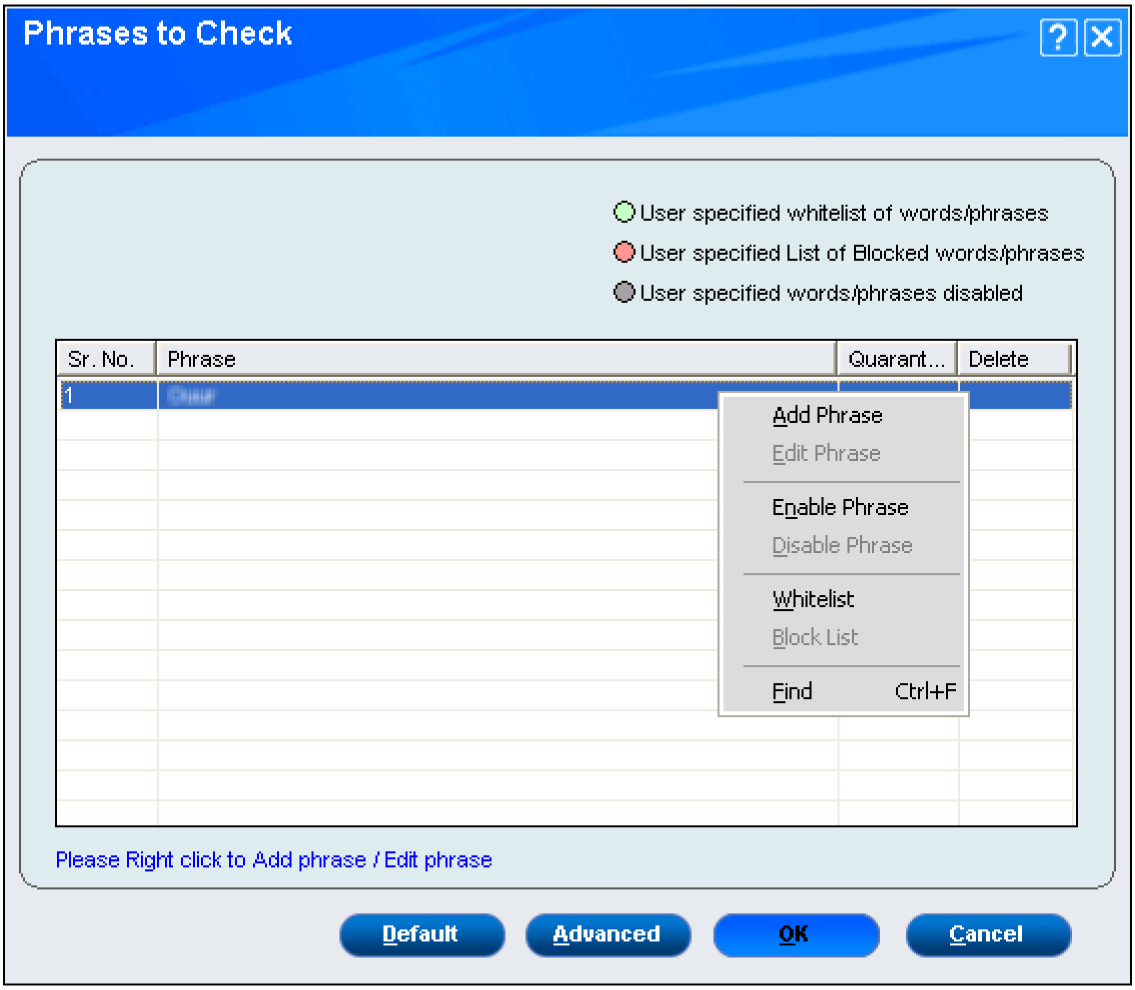
Configuration

This section displays the following information:

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

Settings

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



Phrases to Check

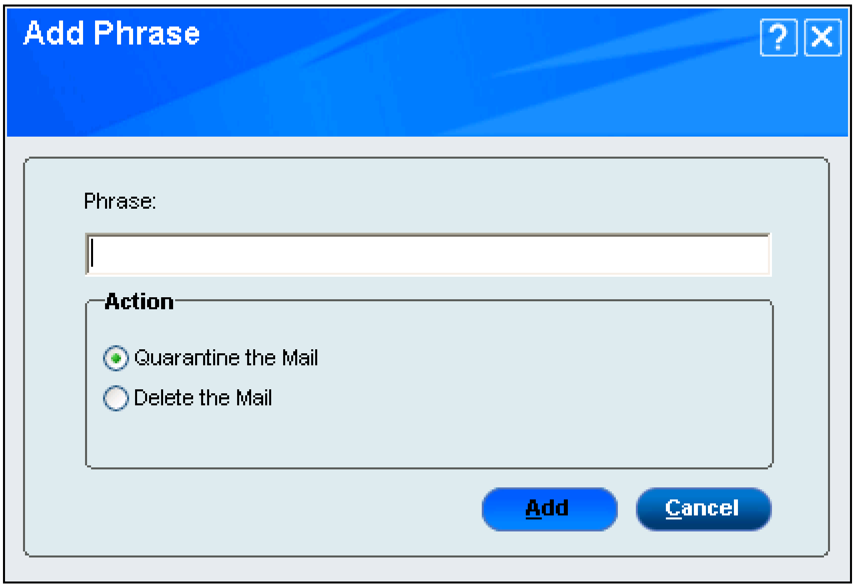
🟢 User specified whitelist of words/phrases
🔴 User specified List of Blocked words/phrases
⚫ User specified words/phrases disabled

Sr. No.	Phrase	Quarant...	Delete
1	[illegible]		

Please Right click to Add phrase / Edit phrase

You can configure the following settings:

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

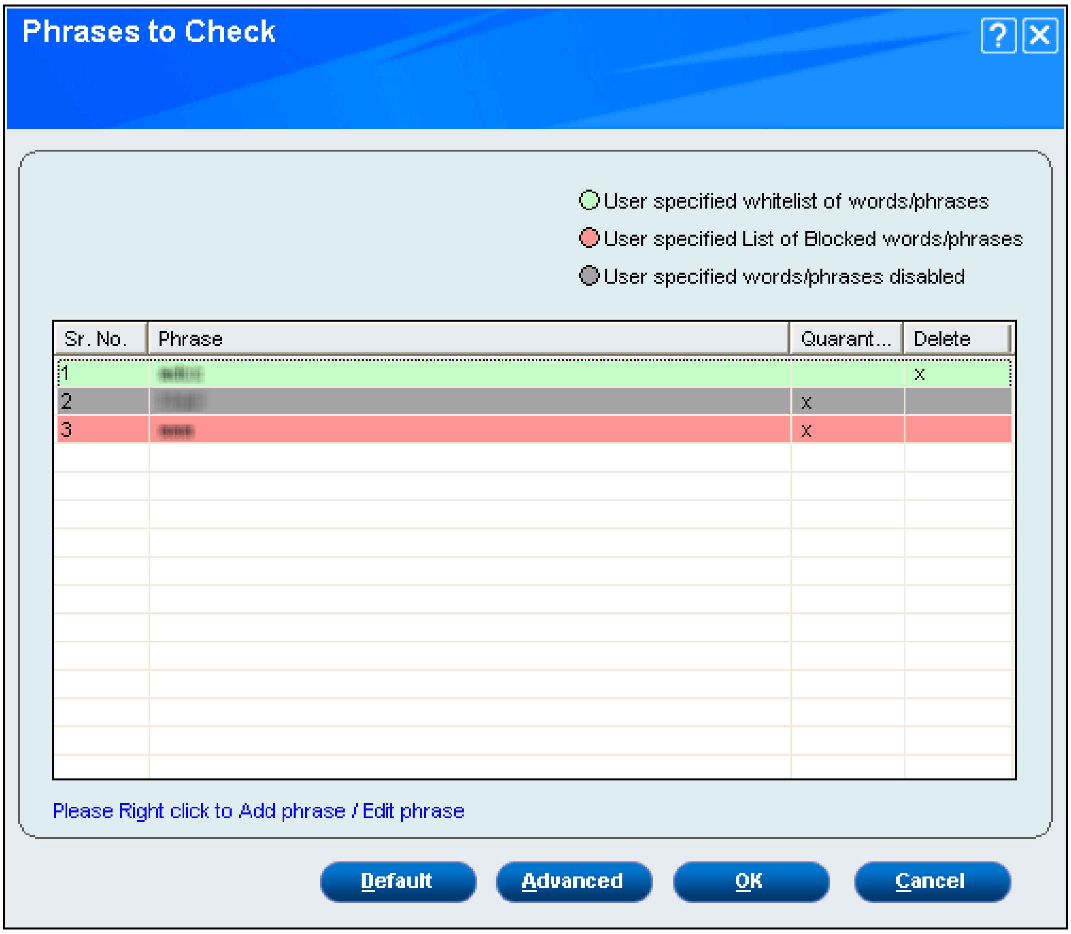


Phrase: You can add certain words or phrases, so that mails containing those words or phrases in the subject, header, or body part of an email are recognized as spam. Once you add the phrase you can edit the phrase along with the actions defined by you, which are as follows:

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

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

- ✓ **User specified whitelist of words/phrases:** (Color Code: **GREEN**) Click this option to select the starting row of Whitelisted words or phrases. A phrase that is added to the whitelist cannot be edited, enabled, or disabled.
- ✓ **User specified List of Blocked words/phrases:** (Color Code: **RED**) Click this option to select the starting row of the words or phrases that are defined in block list.
- ✓ **User specified words/phrases disabled:** (Color Code: **GRAY**) Click this option to select the starting row of words or phrases that are defined to be excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.



Phrases to Check

🟢 User specified whitelist of words/phrases
🔴 User specified List of Blocked words/phrases
⚫ User specified words/phrases disabled

Sr. No.	Phrase	Quarant...	Delete
1	[redacted]		x
2	[redacted]	x	
3	[redacted]	x	

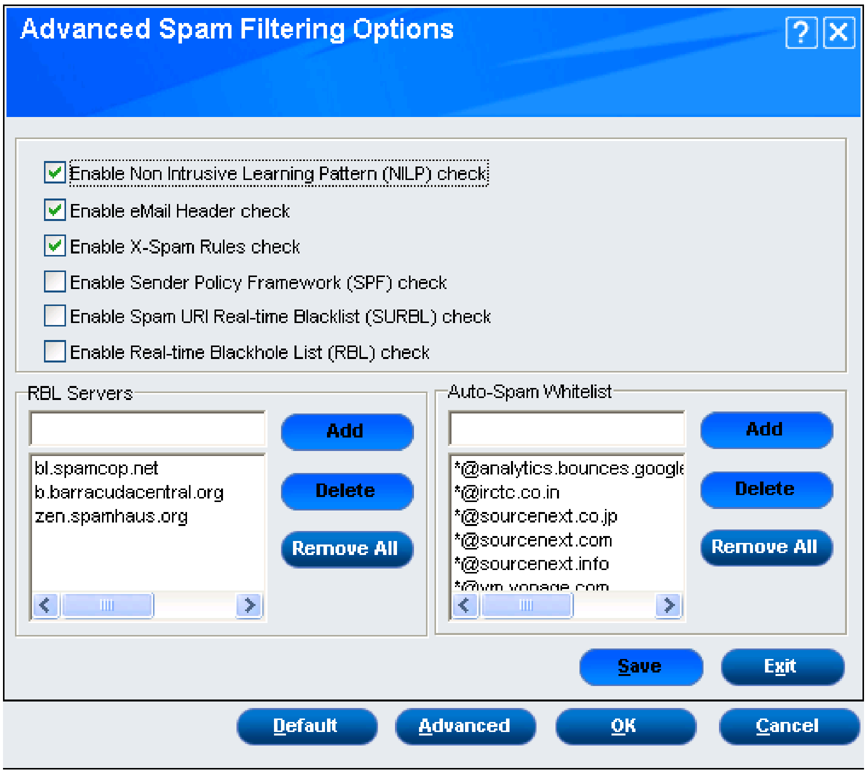
Please Right click to Add phrase / Edit phrase

Default

Click this button to apply the default settings.

Advanced

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



Advanced Spam Filtering Options

☑ Enable Non Intrusive Learning Pattern (NILP) check
☑ Enable eMail Header check
☑ Enable X-Spam Rules check
□ Enable Sender Policy Framework (SPF) check
□ Enable Spam URI Real-time Blacklist (SURBL) check
□ Enable Real-time Blackhole List (RBL) check

RBL Servers
bl.spamcop.net
b.barracudacentral.org
zen.spamhaus.org

Auto-Spam Whitelist
*@analytics.bounces.google
*@irctc.co.in
*@sourcenext.co.jp
*@sourcenext.com
*@sourcenext.info
*@vm.vonage.com

- **Enable Non Intrusive Learning Pattern (NILP) check:** This option is selected by default. NILP is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user. Select this check box if you want to enable NILP check.
- **Enable eMail Header check:** This option is selected by default. Select this check box if you want to check the validity of certain generic fields, such as From, To, and CC in an email and marks it as spam if any of the headers are invalid.
- **Enable X-Spam Rules check:** This option is selected by default. X-Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The X-Spam Rules Check technology matches X-Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.
- **Enable Sender Policy Framework (SPF) check:** SPF is a world-standard framework that is adopted by eScan to prevent hackers from forging sender addresses. It acts a powerful mechanism for controlling phishing mails. Select this check box if you want Anti-Spam to

check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.

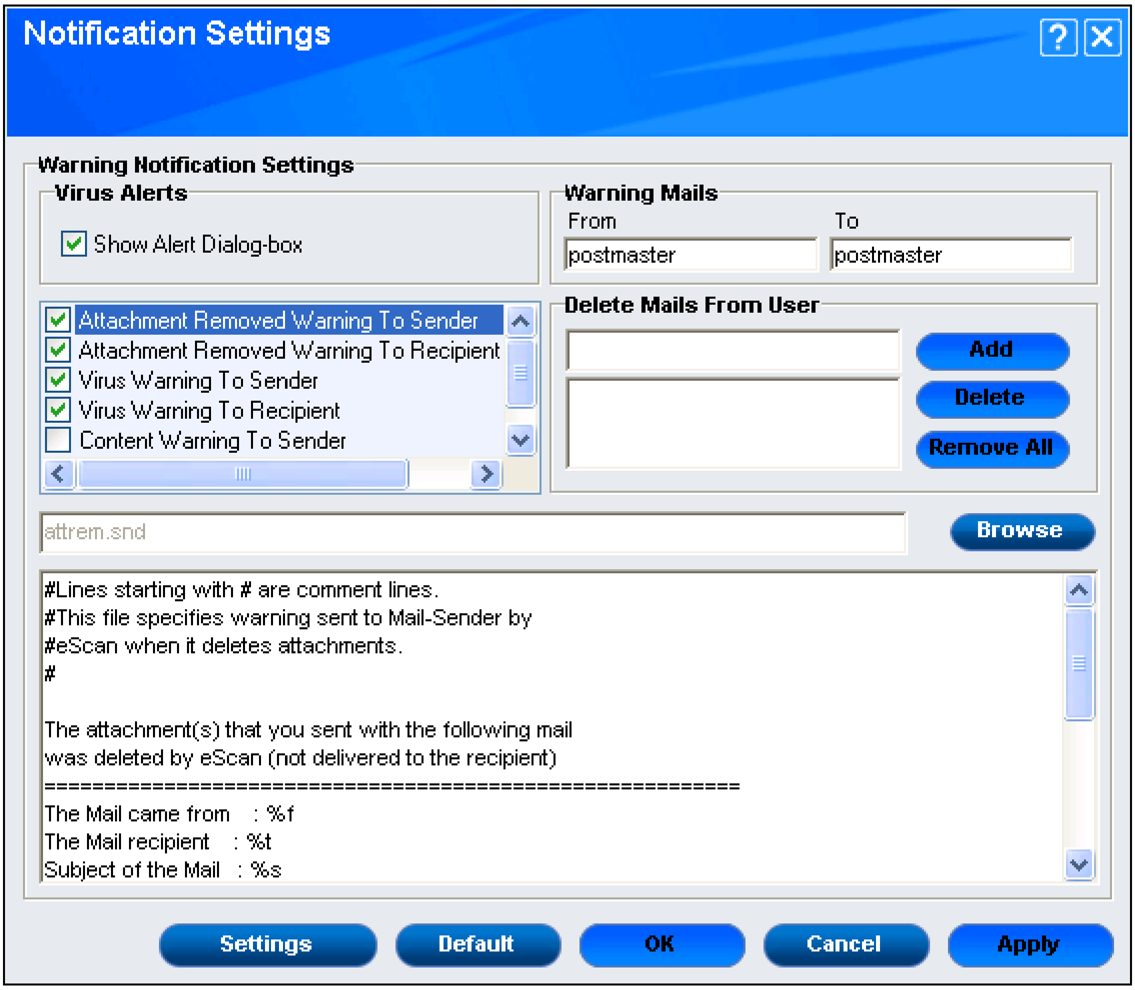
- **Enable Spam URL Realtime Blacklist (SURBL) check:** Select this check box if you want Anti-Spam to check the URLs in the message body of an email. If the URL is listed in the SURBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **Enable Realtime Blackhole List (RBL) check:** Select this check box if you want Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **RBL Servers:** RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.
    - **Add**: You can add servers and sites that contain information of spammers.
    - **Delete**: You can delete a specific server or site from the list.
    - **Remove All**: You can remove all the servers and sites from list all at once.
- **Auto-Spam Whitelist:** Unlike normal RBLs, SURBL scans emails for names or URLs of spam Web sites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid email addresses that can bypass the above Spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.
    - **Add**: You can add valid email addresses that can bypass the above spam filtering.
    - **Delete**: You can delete the specific email address from the list.
    - **Remove All**: You can remove all the email addresses from list all at once.
- **Save**: You can save the configuration by clicking on this button.
- **Exit**: You can exit the **Advanced Spam Filtering Options** without saving the configuration.

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

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

Notification

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



☑ Show Alert Dialog-box

From: postmaster

To: postmaster

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

attrem.snd

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

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

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

Virus Alerts

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

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

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

Warning Mails

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

Delete emails From User

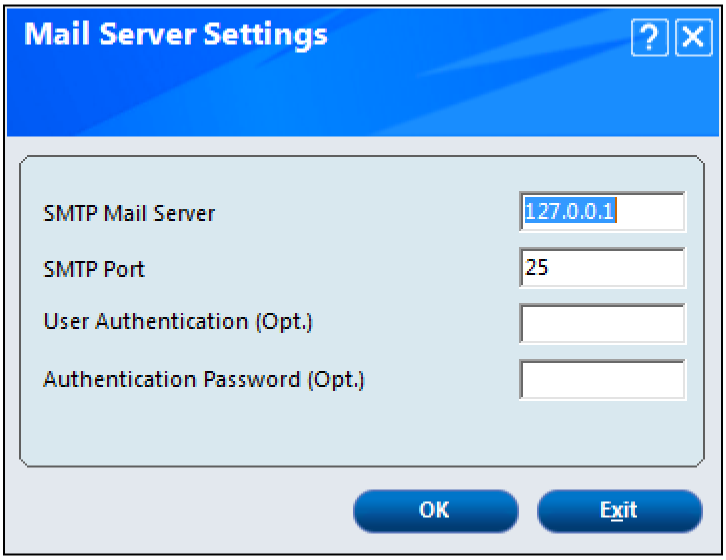
This option is used to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete emails From User** list. By default, the **Delete emails From User** section fields are unavailable, it is available only when you type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

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

Settings

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

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



SMTP Mail Server: 127.0.0.1
SMTP Port: 25
User Authentication (Opt.):
Authentication Password (Opt.):

This dialogue box has two buttons:

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

Default

Click this button to apply the default settings.

OK

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

Cancel

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

Apply

Click this button to apply the configured settings.

Reports

Total Quarantined Mails

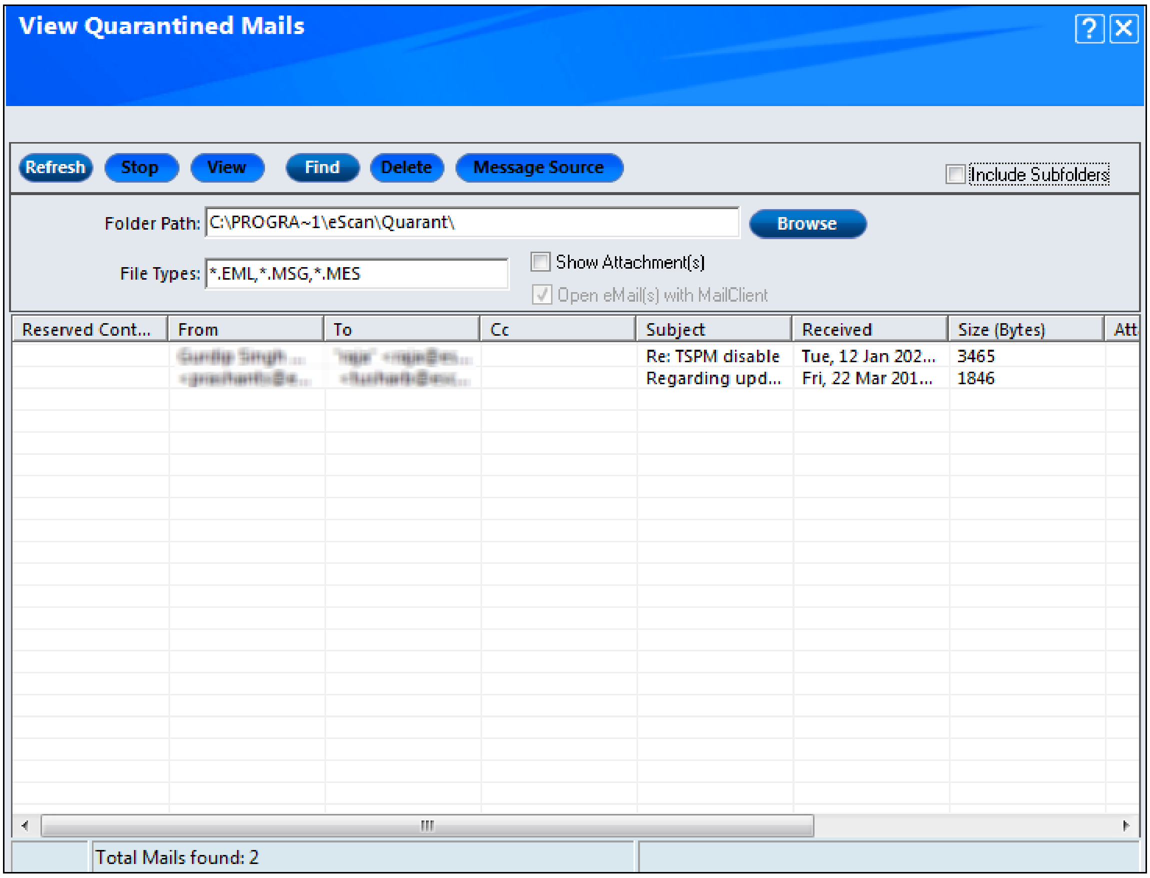
It shows the total number of quarantined mails monitored by Real-Time scanning.

Total Clear Mails

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

View Quarantined Mails

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



□ Include Subfolders

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

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

□ Show Attachment(s)

☑ Open eMail(s) with MailClient

Reserved Cont...	From	To	Cc	Subject	Received	Size (Bytes)	Att
	[redacted]	[redacted]		Re: TSPM disable	Tue, 12 Jan 202...	3465	
	[redacted]	[redacted]		Regarding upd...	Fri, 22 Mar 201...	1846	

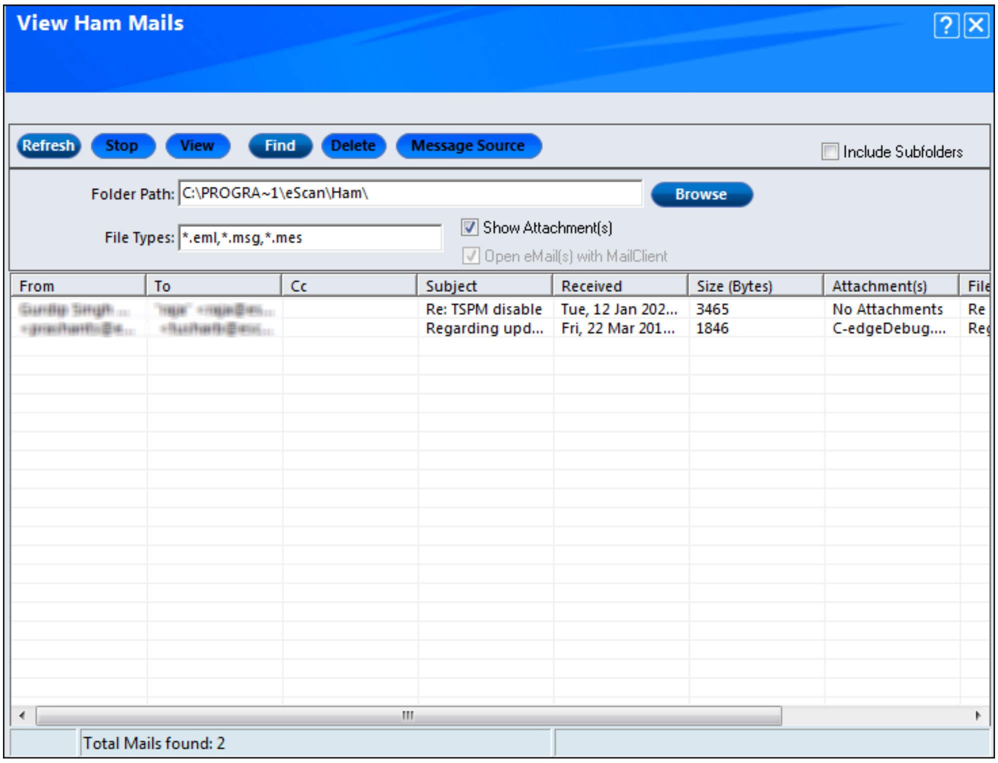
Total Mails found: 2

Following are the options to configure quarantined emails:

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

View Ham Mails

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



□ Include Subfolders

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

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

☑ Show Attachment(s)

☑ Open eMail(s) with MailClient

From	To	Cc	Subject	Received	Size (Bytes)	Attachment(s)	File
[redacted]	[redacted]		Re: TSPM disable	Tue, 12 Jan 202...	3465	No Attachments	Re
[redacted]	[redacted]		Regarding upd...	Fri, 22 Mar 201...	1846	C-edgeDebug....	Re(

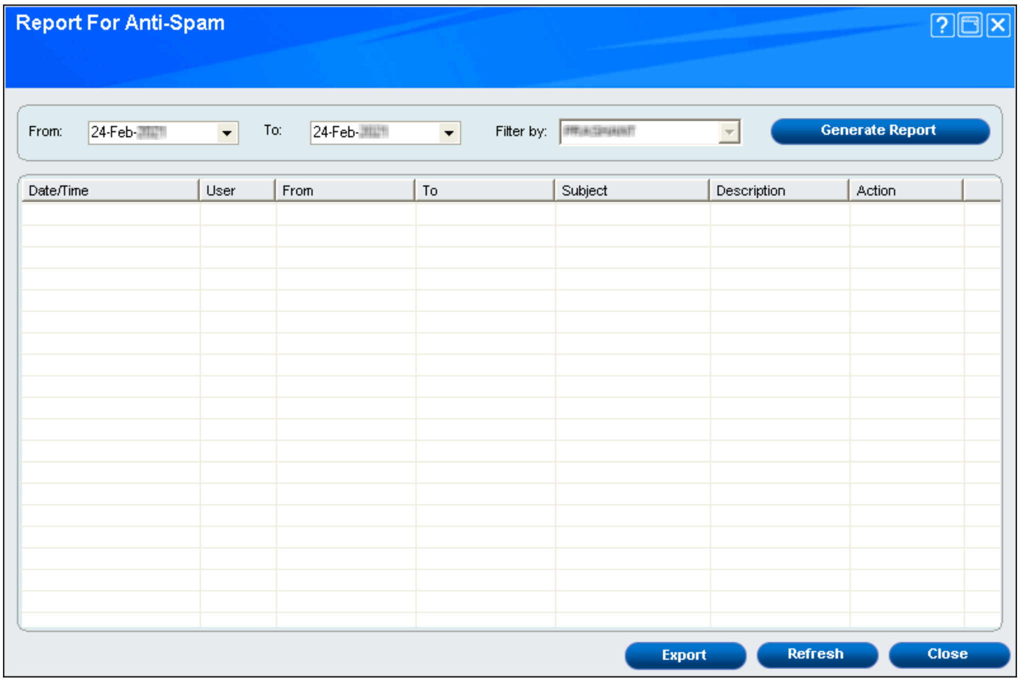
Total Mails found: 2

Following are the options to configure ham emails:

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

View Report

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



From: 24-Feb-[redacted] To: 24-Feb-[redacted] Filter by: [redacted]

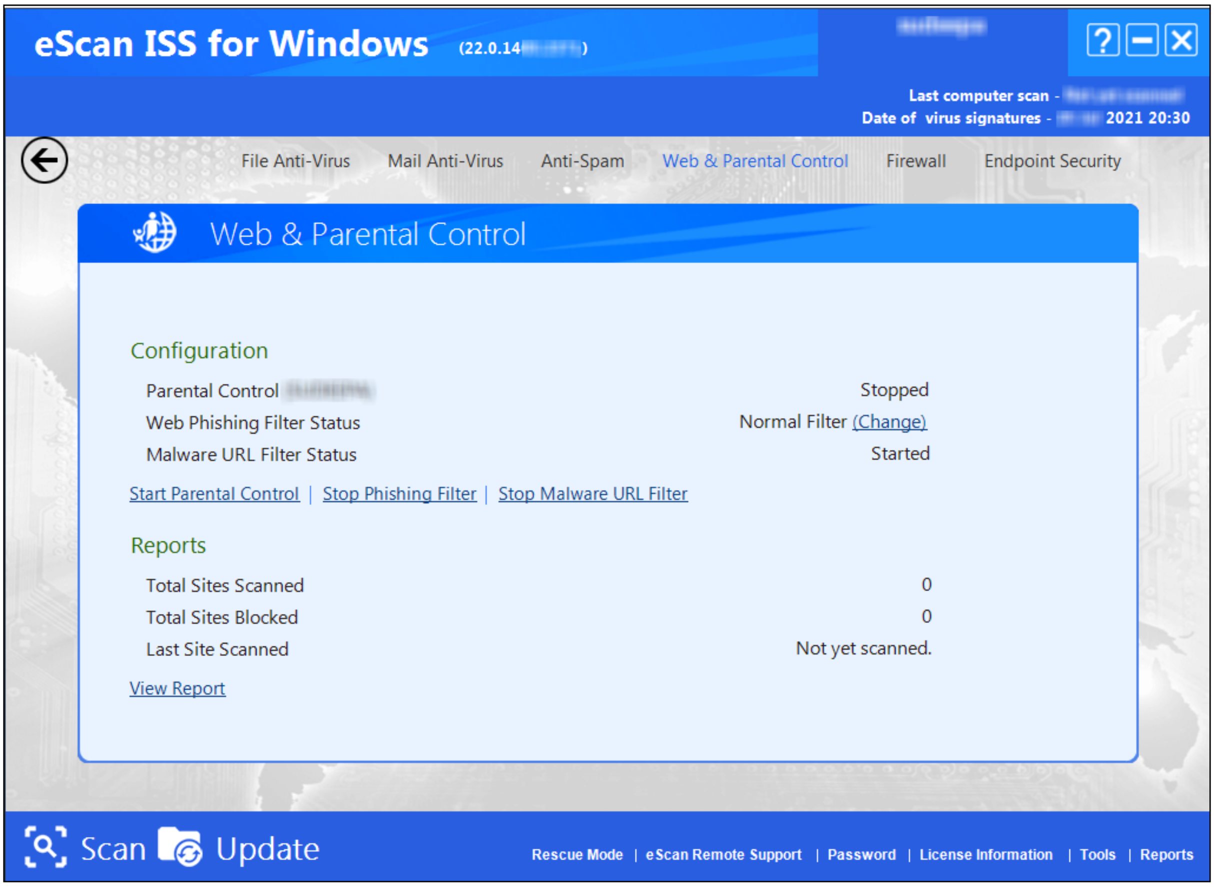
Date/Time	User	From	To	Subject	Description	Action

You can export the reports in the following format:

- PDF
- HTML
- CSV

Web & Parental Control

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



Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 20:30

Configuration

Parental Control [redacted] Stopped
Web Phishing Filter Status Normal Filter (Change)
Malware URL Filter Status Started

Start Parental Control | Stop Phishing Filter | Stop Malware URL Filter

Reports

Total Sites Scanned 0
Total Sites Blocked 0
Last Site Scanned Not yet scanned.

View Report

This page has provides you following sections to configure this module.

Configuration

This section displays the following information:

Parental Control
To learn more, click here.

Web Phishing Filter Status
It displays the type of filter for web phishing.

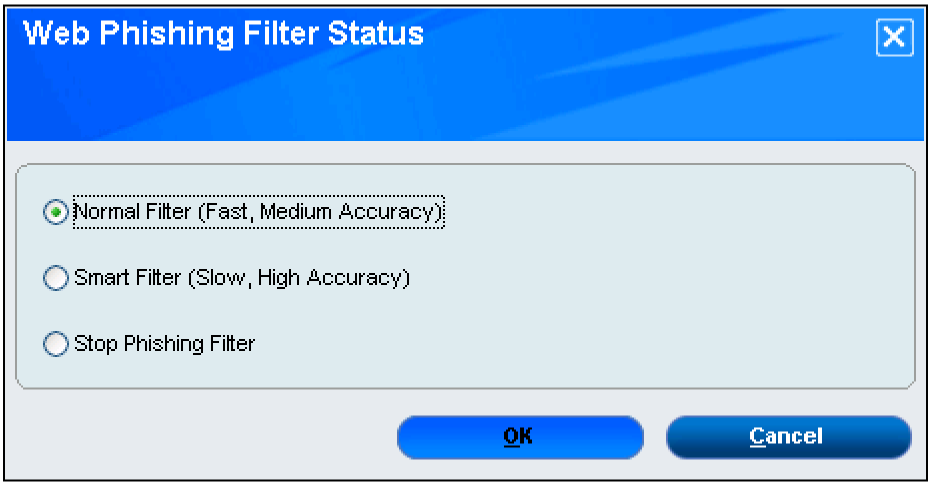
Malware URL Filter Status

It displays the status of Malware URL filter.

Stop/Start Parental Control

This option is used to enable or disable Web & Parental Control module.

Stop/Start Phishing Filter: This button is used to display the alert, you can select **Normal Filter** or **Smart Filter**.



Web Phishing Filter Status

● Normal Filter (Fast, Medium Accuracy)

○ Smart Filter (Slow, High Accuracy)

○ Stop Phishing Filter

- **Normal Filter**: Select Normal Filter to activate Normal Filter.
- **Smart Filter**: Select Smart Filter to activate Smart Filter.

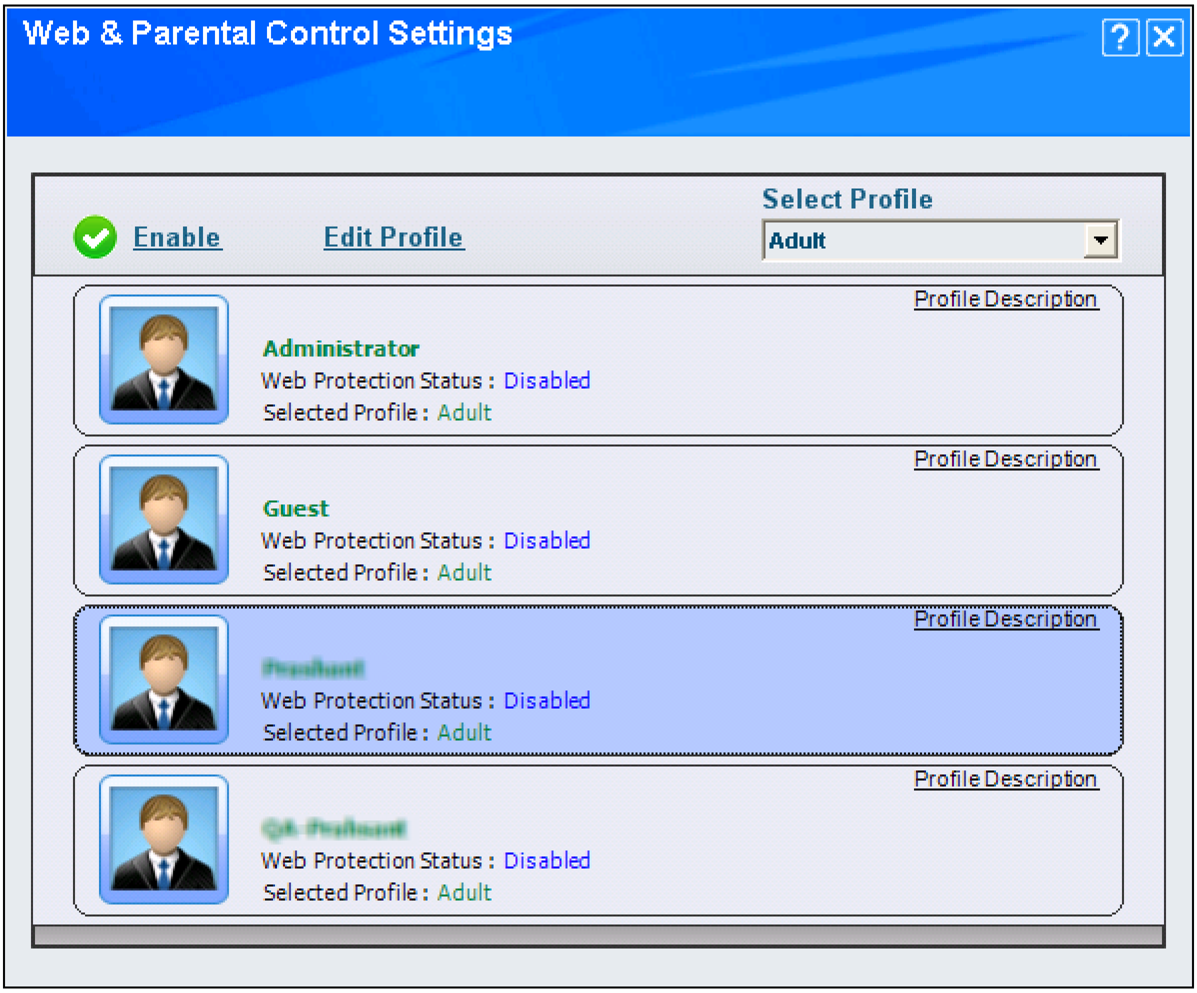
Start Malware URL Filter

This option is used to start Malware URL filter.

Parental Control

It displays whether Web & Parental Control module is in Start or Stop mode. You can configure this option according to the **Profile**.

It provides you the Filtering options.



Web & Parental Control Settings

✓ Enable   Edit Profile

Select Profile: Adult ▾

Administrator
Web Protection Status : Disabled
Selected Profile : Adult
Profile Description

Guest
Web Protection Status : Disabled
Selected Profile : Adult
Profile Description

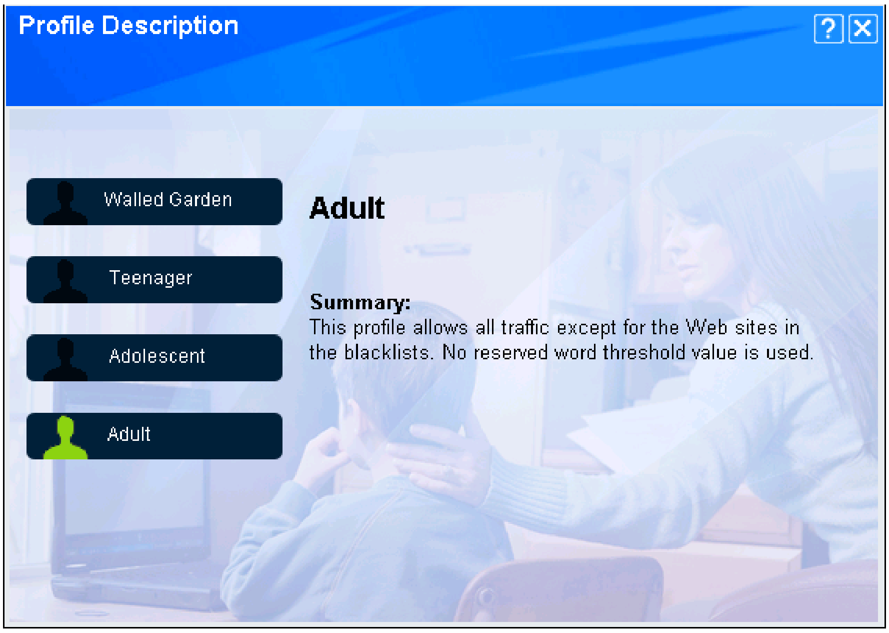
[redacted]
Web Protection Status : Disabled
Selected Profile : Adult
Profile Description

[redacted]
Web Protection Status : Disabled
Selected Profile : Adult
Profile Description

There are following settings to configure the options available in the parental control:

- **Enable**: This option is used to enable the selected user profile for web filtering from the Web & Parental Control Settings.
- **Edit Profile**: You can edit the default setting for each of the option available according to your need. To learn more click here.
- **Select Profile**: You can select the Profile you want to set from the dropdown menu. By default it is selected as **Adult**.

- **Profile Description**: This link will give you the brief description about the selected profile.



Profile Description

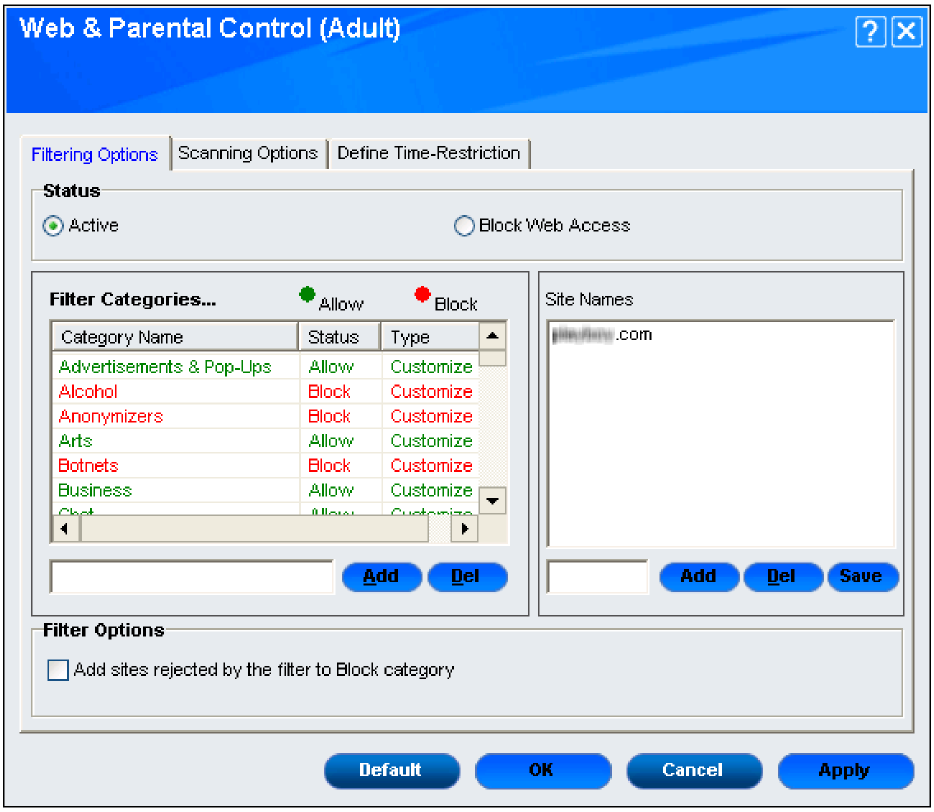
Adult

Summary:
This profile allows all traffic except for the Web sites in the blacklists. No reserved word threshold value is used.

How to Configure Profile?

Filtering Options

This tab helps to block certain categories of sites.



Web & Parental Control (Adult)

Status

● Active ○ Block Web Access

Filter Categories... ● Allow ● Block

Category Name	Status	Type
Advertisements & Pop-Ups	Allow	Customize
Alcohol	Block	Customize
Anonymizers	Block	Customize
Arts	Allow	Customize
Botnets	Block	Customize
Business	Allow	Customize
Chat	Allow	Customize

Site Names

[redacted].com

Filter Options

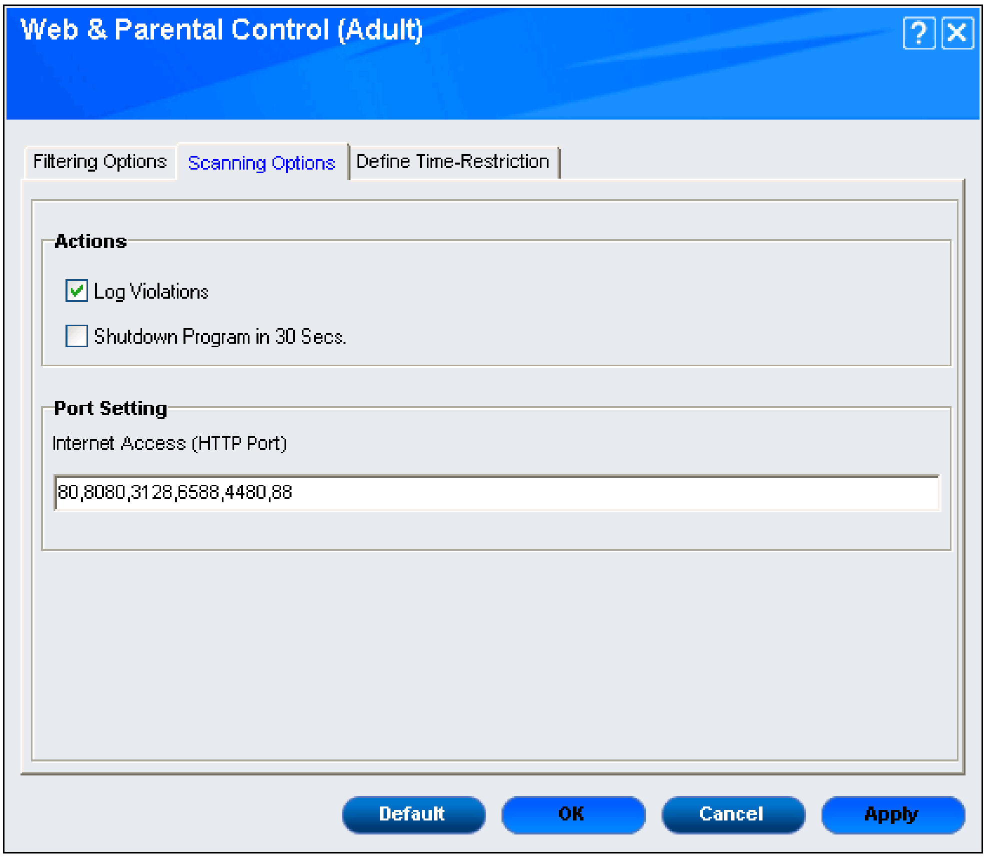
□ Add sites rejected by the filter to Block category

It has following options for configuring the filter:

- **Status**: This option gives you the status of the filtering option, namely,

  - **Active**
  - **Block Web Access**
- **Filter Categories**: This option provides you to filter the web access according to the category such as business, botnets, advertisements, and more. Here **GREEN** indicates that access is allowed while **RED** indicated that access is blocked. Here you can add or delete the category according to your need using **Add** and **Del** button present in that box.
- **Site Names**: You can block specific site by adding the site names in this option. It has 3 buttons:
  - **Add**: You can add the site name to the list.
  - **Del**: you can delete the site name from the existing list.
  - **Save**: Once the site name is added you can use this button to save the changes.
- **Filter Options**: There is check box called **Add sites rejected by the filter** to **Block category** which is used to add all the rejected sites to the block category.

Scanning Options
This tab lets you enable log violations and shutdown program if it violates the filtering options. It also lets you specify ports that need monitoring.


Web & Parental Control (Adult)

Filtering Options | Scanning Options | Define Time-Restriction

Actions

☑ Log Violations

□ Shutdown Program in 30 Secs.

Port Setting

Internet Access (HTTP Port)

80,8080,3128,6588,4480,88

- **Actions**: This section helps you select the actions that eScan should perform when it detects a security violation.
  - **Log Violations**: This check box is selected by default and used to log all security violations for your future reference.

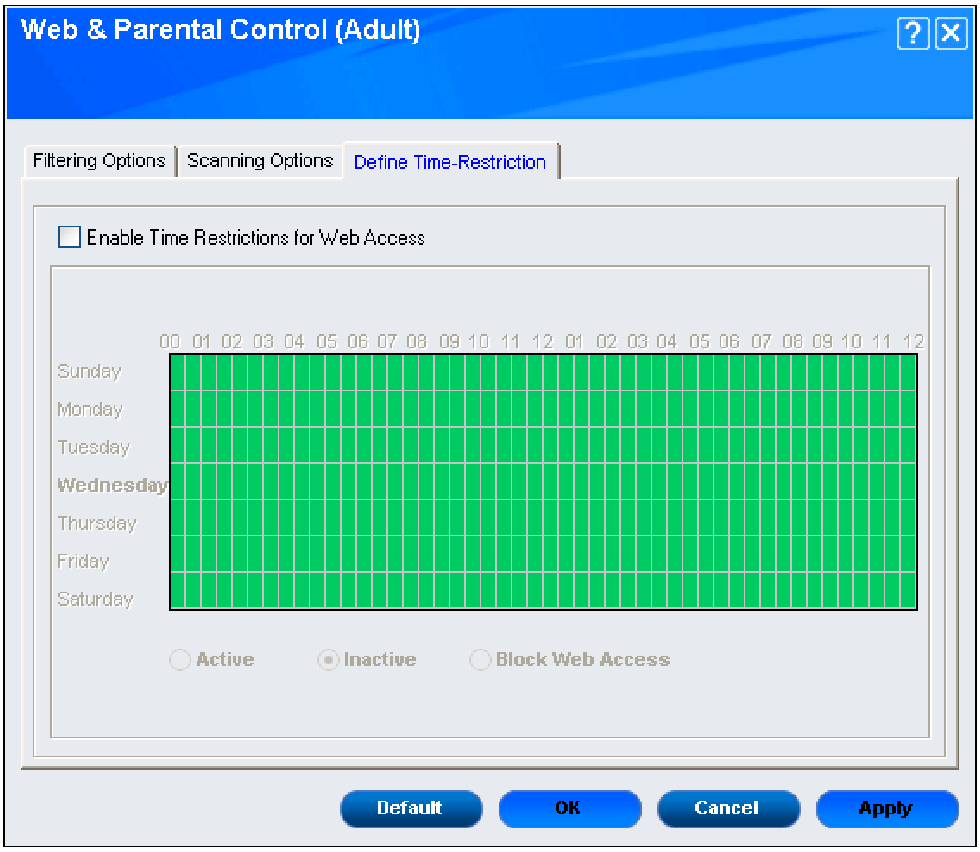
    - **Shutdown Program in 30 Secs**: This check box is used if you want to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.
- **Port Setting**: This section helps you specify the port numbers that you want to monitor for suspicious traffic.
- **Internet Access (HTTP Port)**: Web browsers commonly use the port numbers 80, 8080, 3128, 6588, 4480, and 88 for accessing the Internet. You can add port numbers to the **Internet Access (HTTP Port)** box to monitor the traffic on those ports.

Define Time Restriction

This section helps you define policies to restrict access to the internet based on time.

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

- ○ **Block Web Access:** This option blocks web access on certain days at specific time.

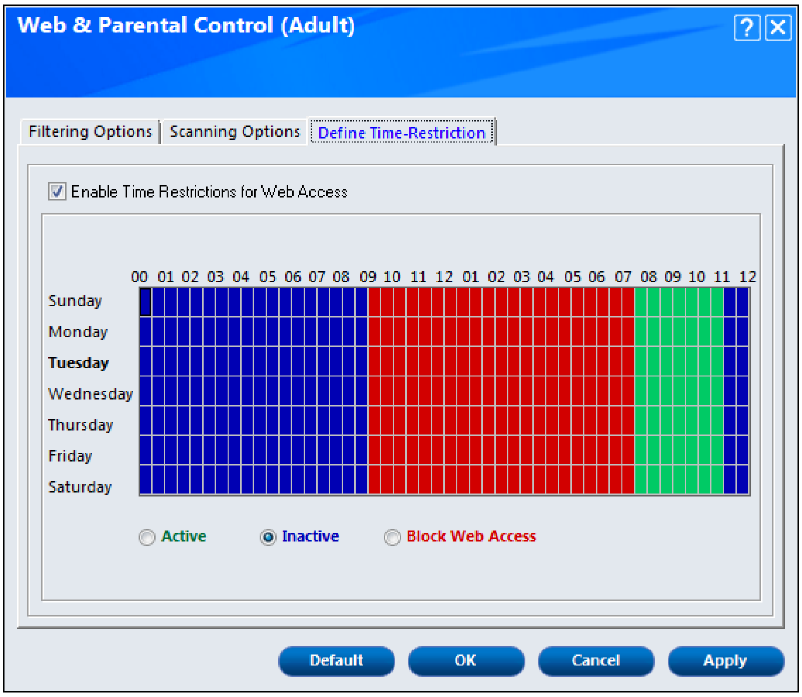


☐ Enable Time Restrictions for Web Access

○ Active ● Inactive ○ Block Web Access

You can assign settings for single and multiple users.

- **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.
  Allow restricted web access for children or block web access during study time.
  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.
- **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.



☑ Enable Time Restrictions for Web Access

	00	01	02	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06	07	08	09	10	11
Sunday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦
Monday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦
Tuesday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦
Wednesday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦
Thursday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦
Friday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦
Saturday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟦

○ Active ● Inactive ○ Block Web Access

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.

Default
Click this button to apply the default settings.

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

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

Apply
Click this button to apply the configured settings.

Reports

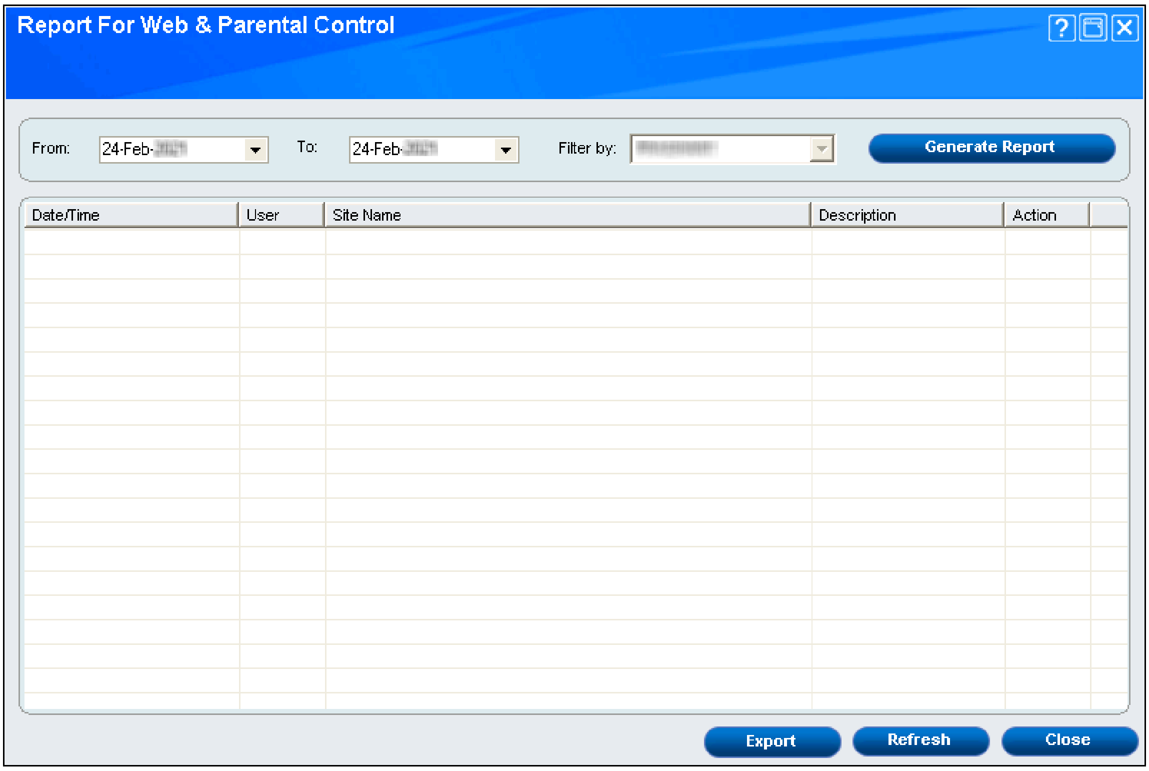
This section displays the following information:

Total Sites Scanned
It displays Total Sites Scanned.

Total Sites Blocked
It displays Total Sites Blocked.

Last Site Scanned
It displays the last site which was scanned**.**

View Report
This button is used to view Reports for Web & Parental Control.



Report For Web & Parental Control

From: 24-Feb-[redacted] To: 24-Feb-[redacted] Filter by: [redacted]

Date/Time	User	Site Name	Description	Action

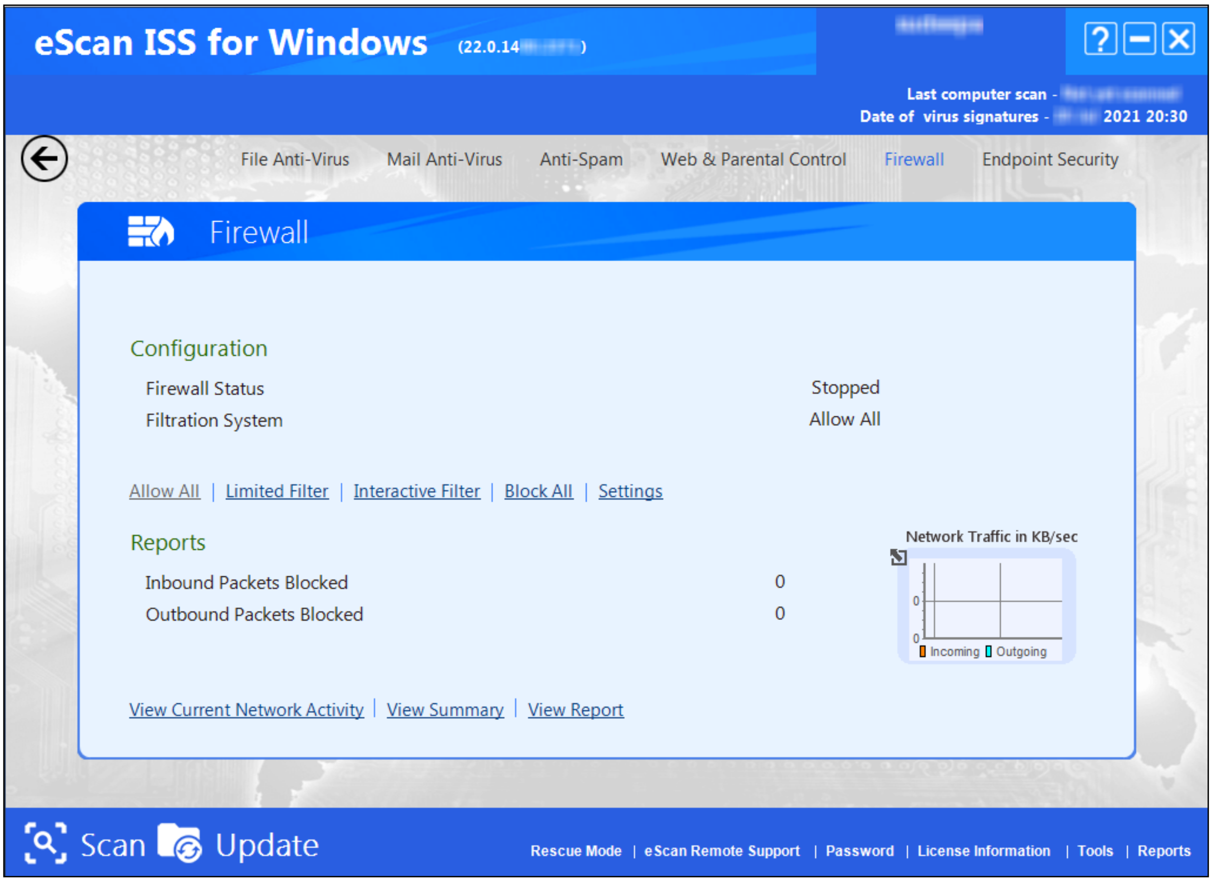
You can export reports in the following formats:

- PDF
- HTML
- CSV

Firewall

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

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



eScan ISS for Windows (22.0.14[redacted])

[redacted]

Last computer scan - [redacted]

Date of virus signatures - [redacted] 2021 20:30

File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Firewall

Configuration

Firewall Status: Stopped

Filtration System: Allow All

Allow All | Limited Filter | Interactive Filter | Block All | Settings

Reports

Inbound Packets Blocked: 0

Outbound Packets Blocked: 0

Network Traffic in KB/sec
0
0
Incoming
Outgoing
View Current Network Activity | View Summary | View Report
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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

Configuration

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

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

Modes that are available are as follows:

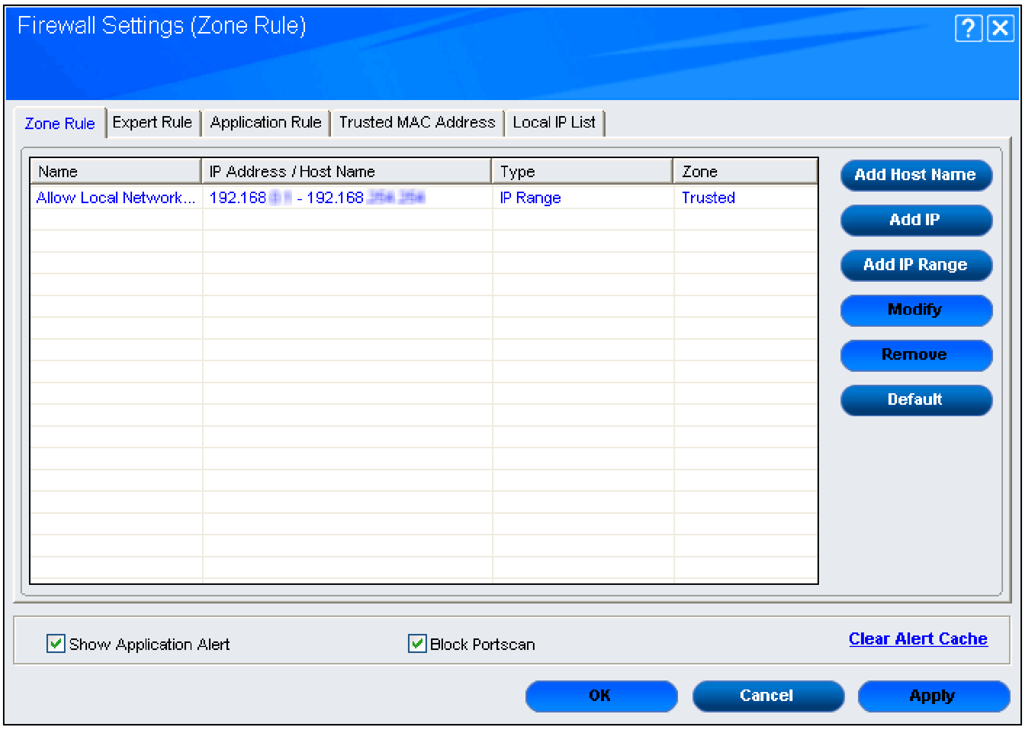
- **Allow All**: This option is turned on by default and you can disable Firewall if you want to.
- **Limited Filter**: This option enables the **Limited Filter** mode. When this mode is enabled, it monitors all incoming traffic and helps you allow or block traffic as per the defined conditions or rules.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

Settings

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

Zone Rule

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

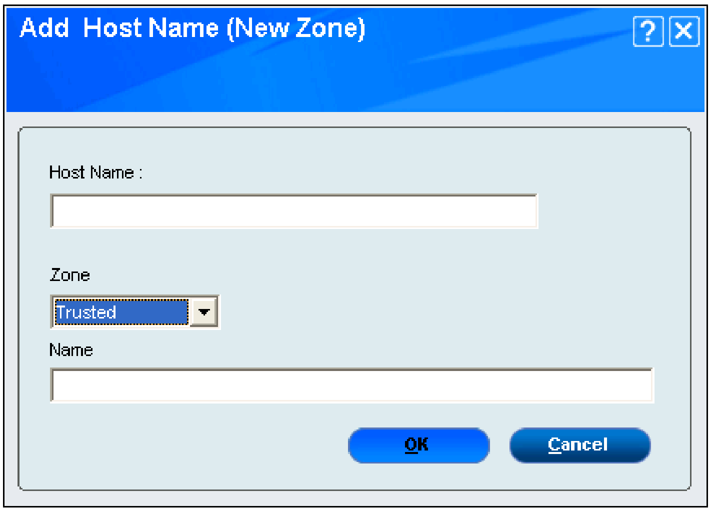


Name	IP Address / Host Name	Type	Zone
Allow Local Network...	192.168[redacted] - 192.168[redacted]	IP Range	Trusted

☑ Show Application Alert ☑ Block Portscan

This tab includes the following buttons:

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

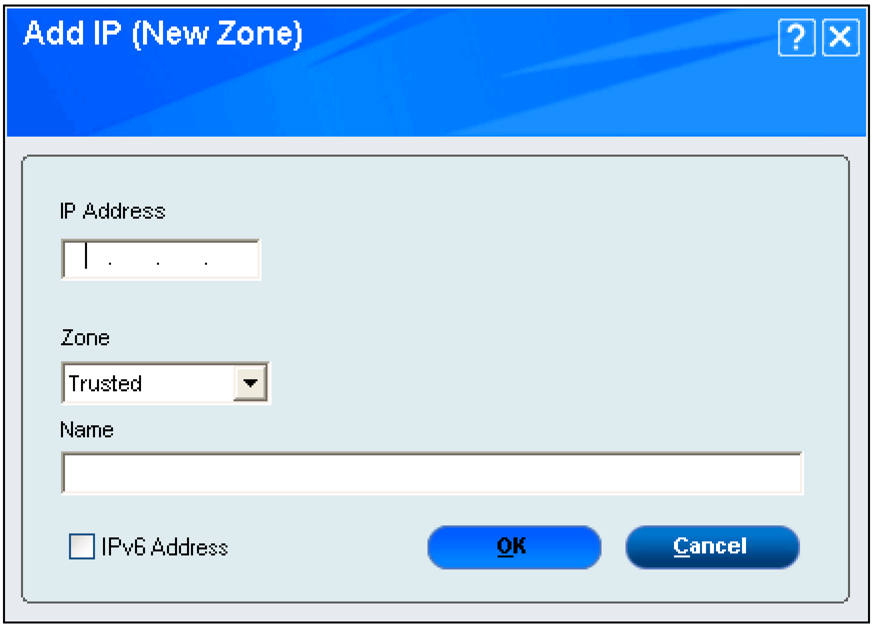


Host Name :

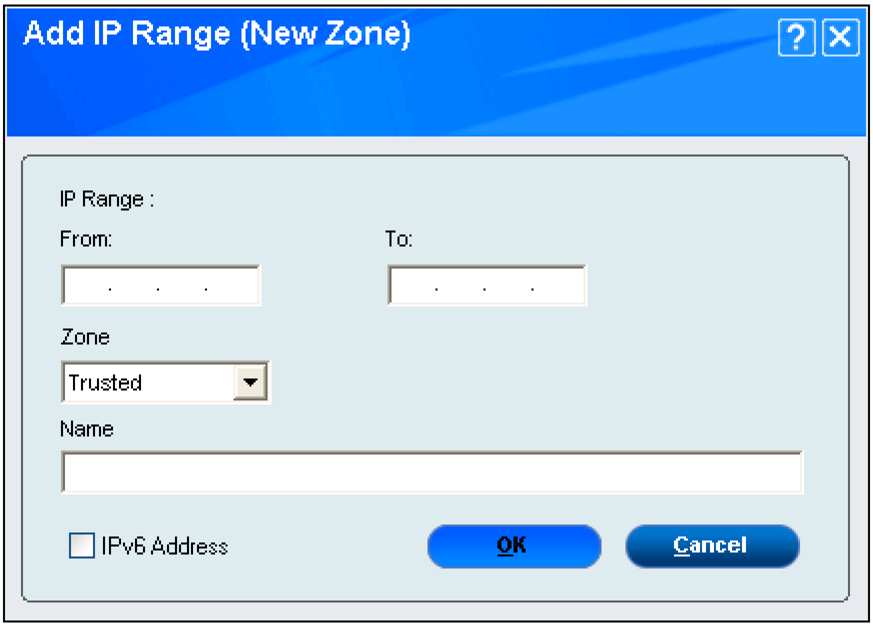
Zone: Trusted

Name

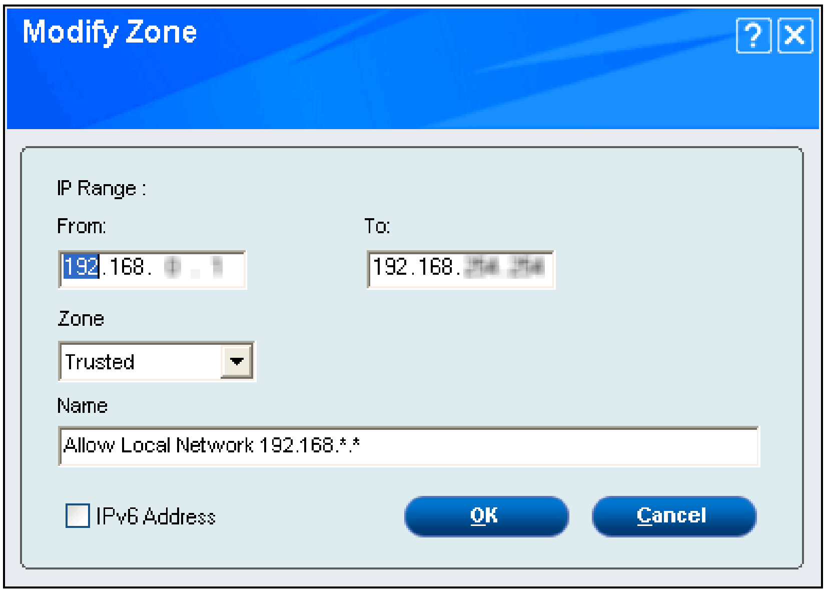
- **Add IP**: This button is used to add a zone rule for a given IP address. To add the zone rule, you must provide the IP address for which you are adding the zone rule, the type of zone, whether it is **Trusted** or **Blocked** and specify a name for the zone rule. By selecting **IPv6 Address** check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



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



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



IP Range :

From: 192.168.[redacted]

To: 192.168.[redacted]

Zone: Trusted

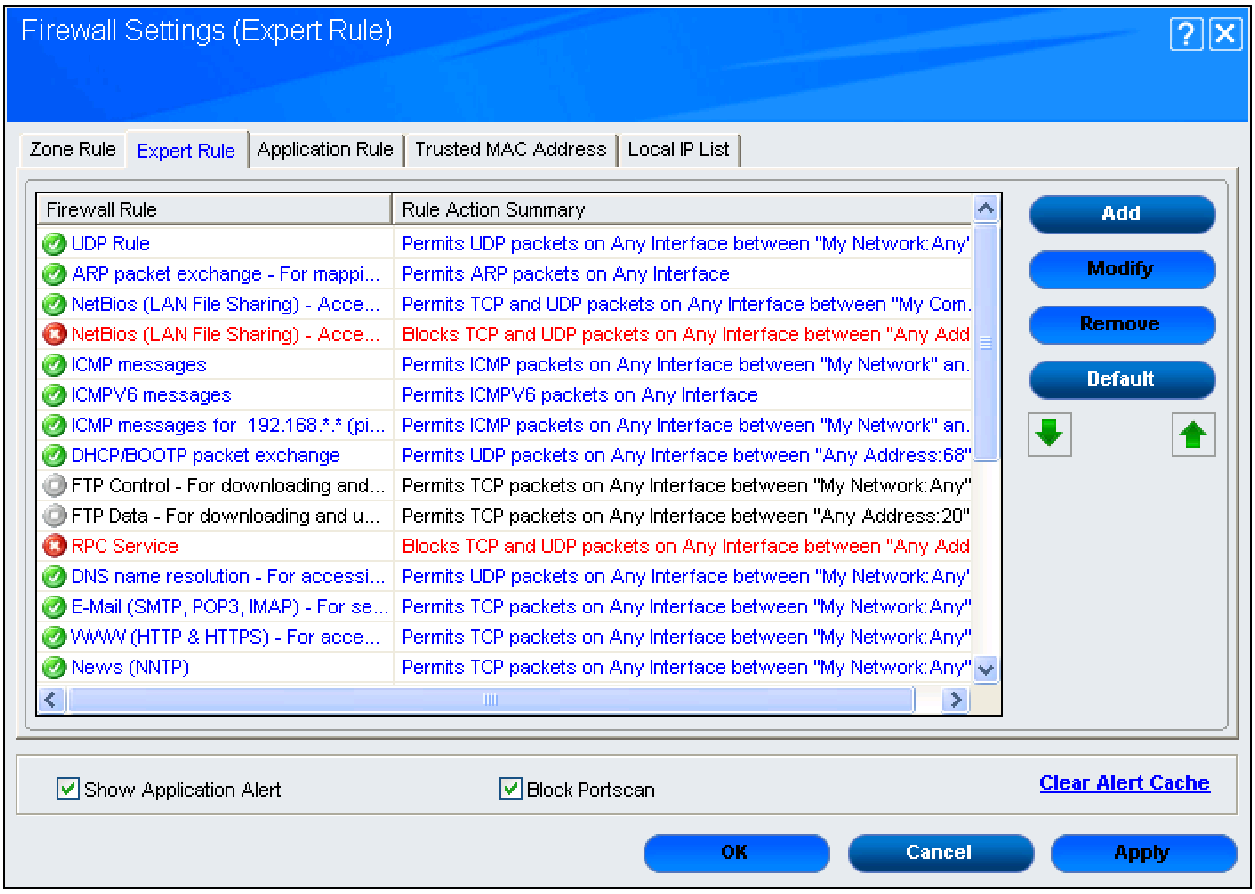
Name: Allow Local Network 192.168.*.*

☐ IPv6 Address

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

Expert Rule

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



Firewall Settings (Expert Rule)

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

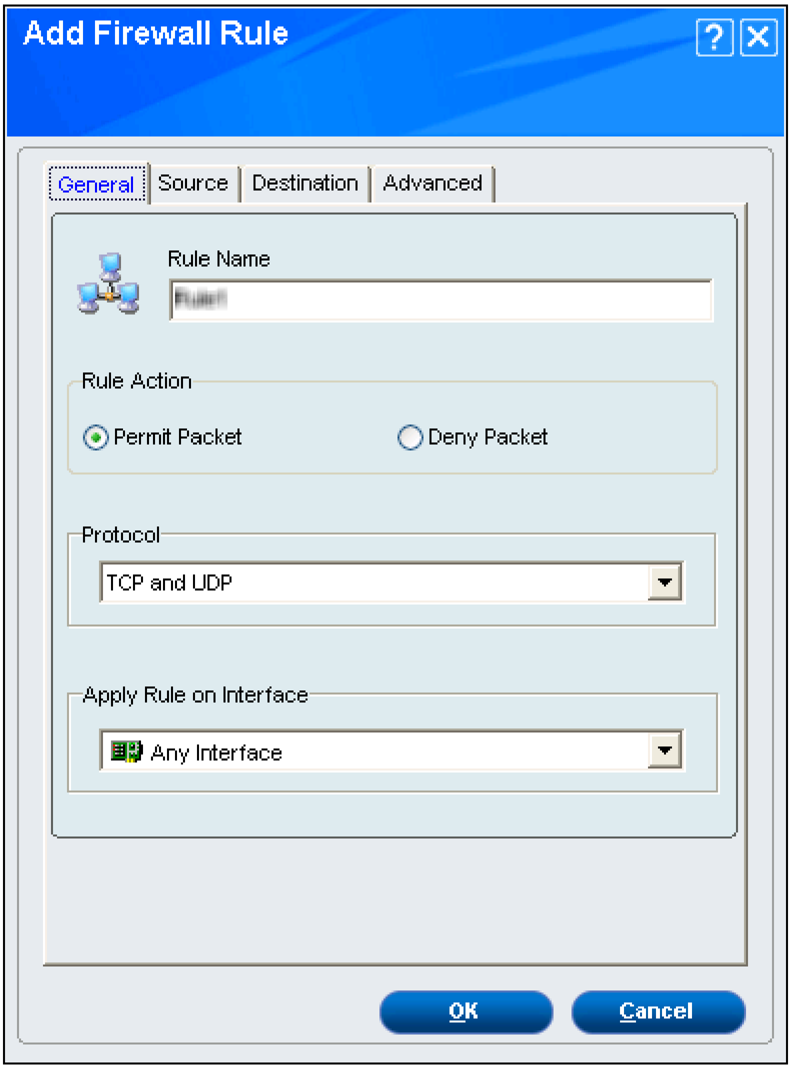
☑ Show Application Alert ☑ Block Portscan

This tab has various button and settings:

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

Adding new rule

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



Add Firewall Rule

General | Source | Destination | Advanced

Rule Name

Rule Action

● Permit Packet ○ Deny Packet

Protocol: TCP and UDP

Apply Rule on Interface: Any Interface

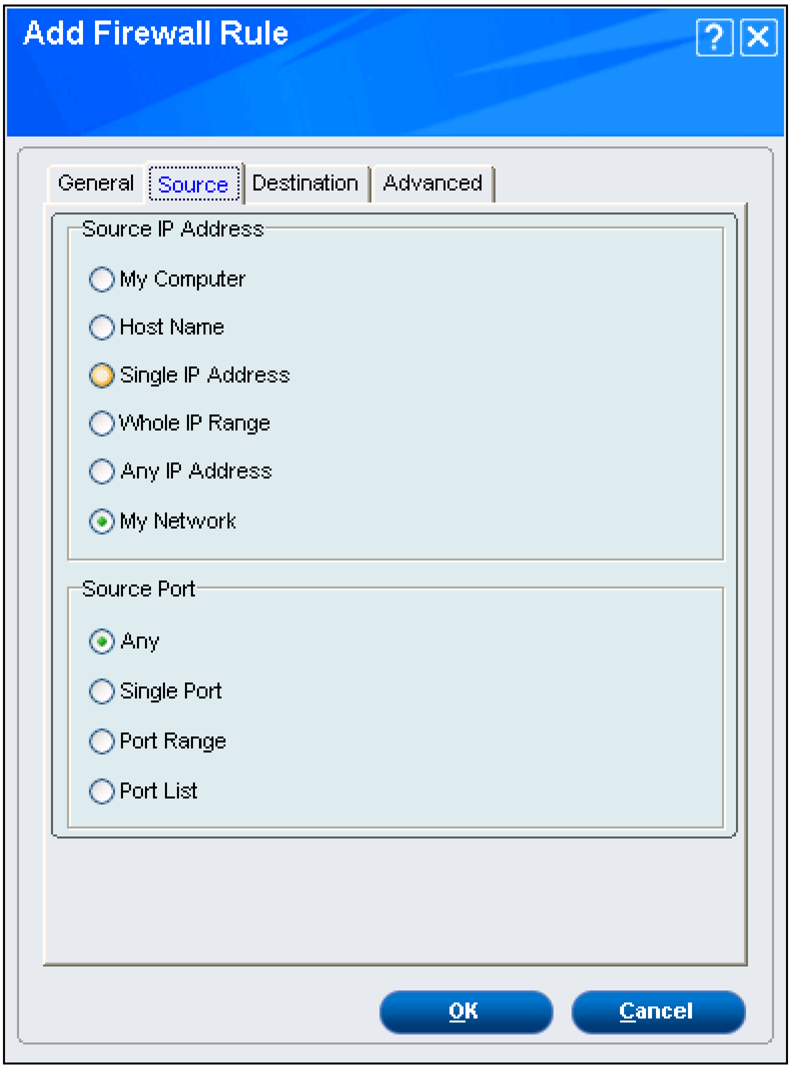
General

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

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

Source

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



Add Firewall Rule

General | Source | Destination | Advanced

Source IP Address

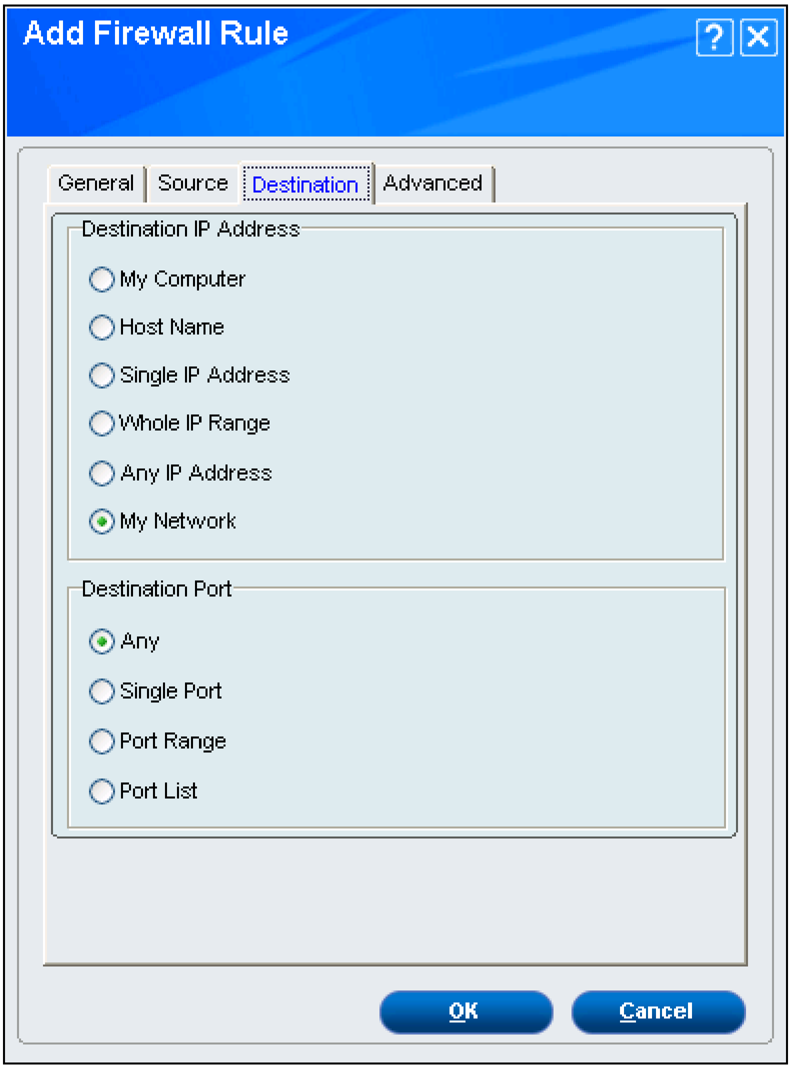
○ My Computer
○ Host Name
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

Source Port

● Any
○ Single Port
○ Port Range
○ Port List

Destination

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



Add Firewall Rule

Destination IP Address

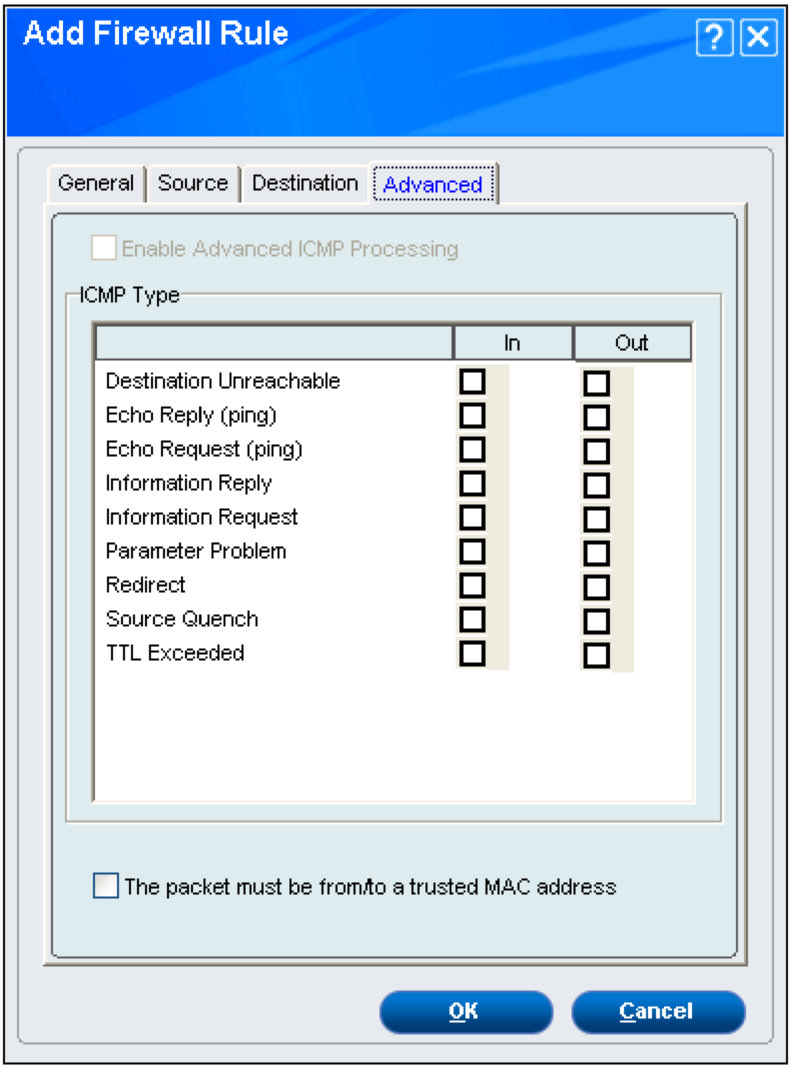
○ My Computer
○ Host Name
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

Destination Port

● Any
○ Single Port
○ Port Range
○ Port List

Advanced

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



□ Enable Advanced ICMP Processing

ICMP Type

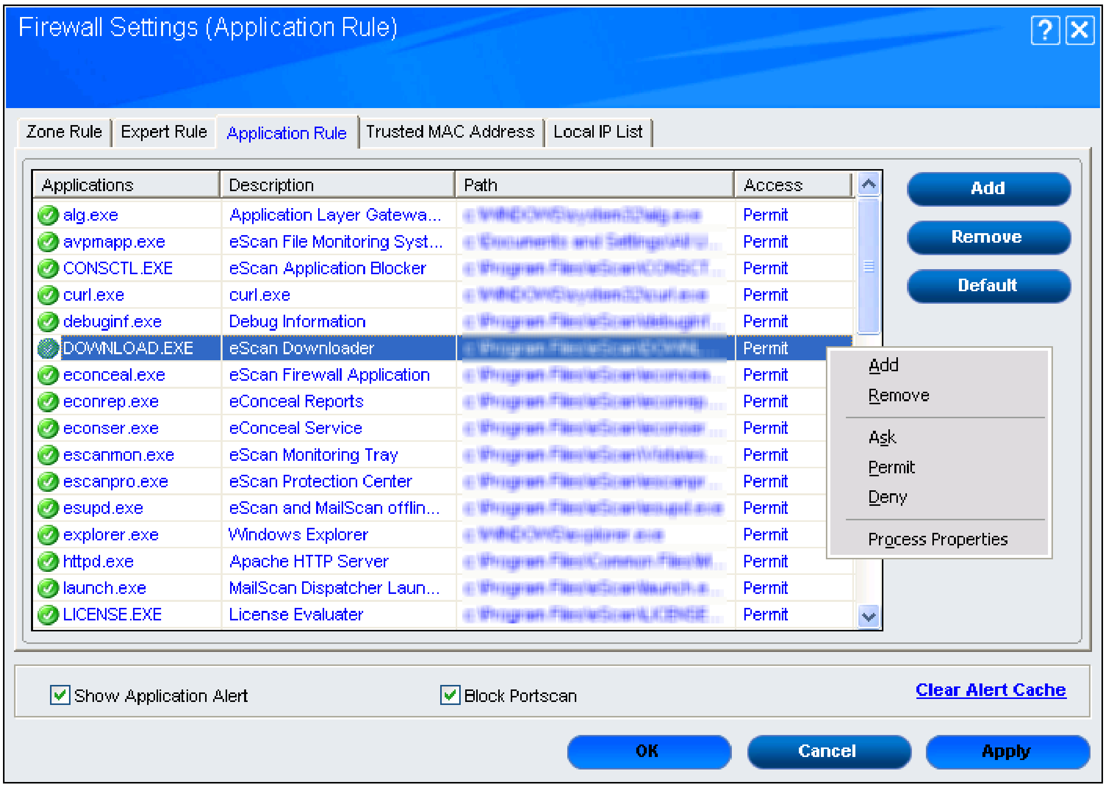
	In	Out
Destination Unreachable	□	□
Echo Reply (ping)	□	□
Echo Request (ping)	□	□
Information Reply	□	□
Information Request	□	□
Parameter Problem	□	□
Redirect	□	□
Source Quench	□	□
TTL Exceeded	□	□

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

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

Application Rule

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

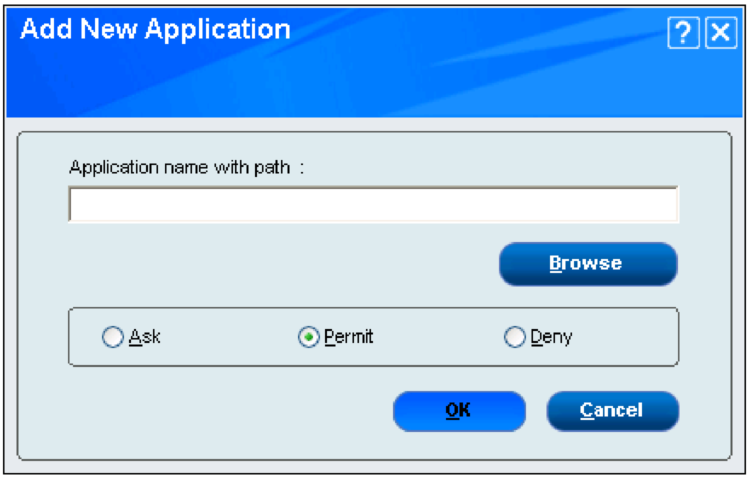


Applications	Description	Path	Access
alg.exe	Application Layer Gatewa...	[illegible]	Permit
avpmapp.exe	eScan File Monitoring Syst...	[illegible]	Permit
CONSCTL.EXE	eScan Application Blocker	[illegible]	Permit
curl.exe	curl.exe	[illegible]	Permit
debuginf.exe	Debug Information	[illegible]	Permit
DOWNLOAD.EXE	eScan Downloader	[illegible]	Permit
econceal.exe	eScan Firewall Application	[illegible]	Permit
econrep.exe	eConceal Reports	[illegible]	Permit
econser.exe	eConceal Service	[illegible]	Permit
escanmon.exe	eScan Monitoring Tray	[illegible]	Permit
escanpro.exe	eScan Protection Center	[illegible]	Permit
esupd.exe	eScan and MailScan offlin...	[illegible]	Permit
explorer.exe	Windows Explorer	[illegible]	Permit
httpd.exe	Apache HTTP Server	[illegible]	Permit
launch.exe	MailScan Dispatcher Laun...	[illegible]	Permit
LICENSE.EXE	License Evaluater	[illegible]	Permit

☑ Show Application Alert ☑ Block Portscan

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

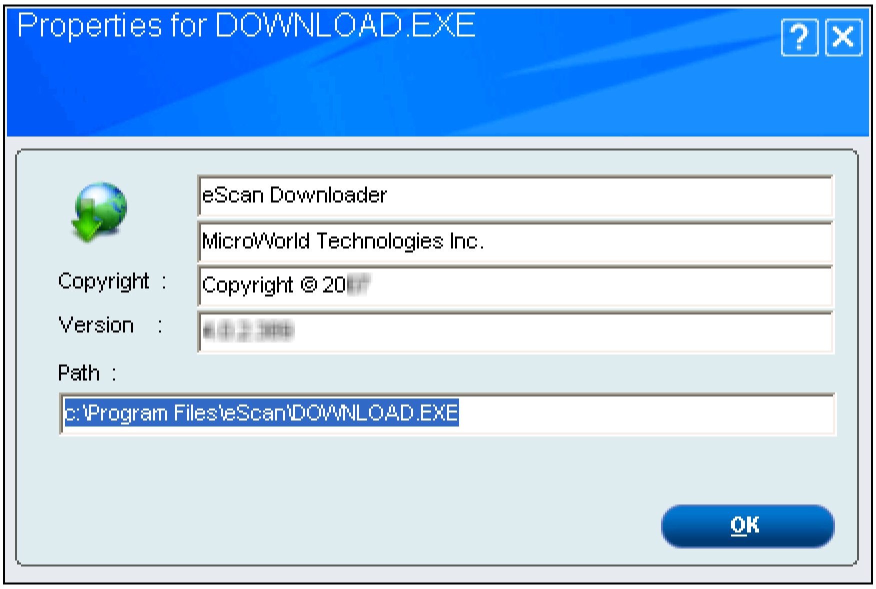
- **Add**: Use this option to add new application to the Application Rule list. Click **Browse** button to select name of the application that you want to add.



Application name with path :

○ Ask ● Permit ○ Deny

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



Properties for DOWNLOAD.EXE

eScan Downloader

MicroWorld Technologies Inc.

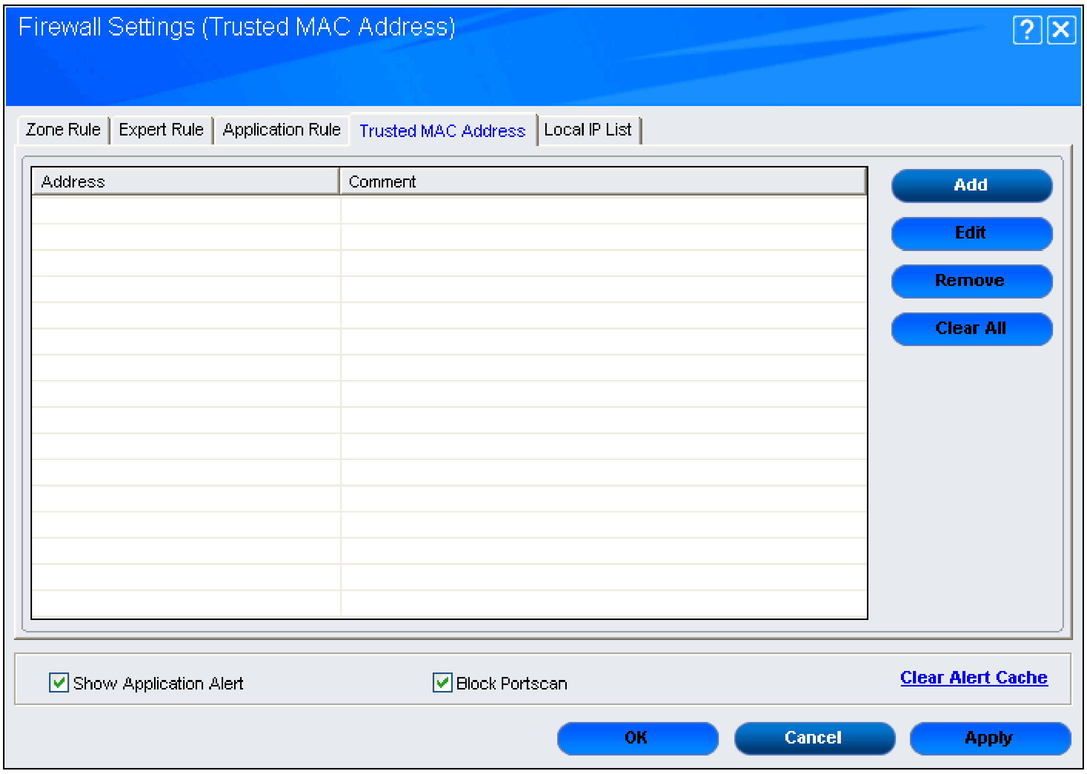
Copyright : Copyright © 20[redacted]

Version : [redacted]

Path : c:\Program Files\eScan\DOWNLOAD.EXE

Trusted MAC Address

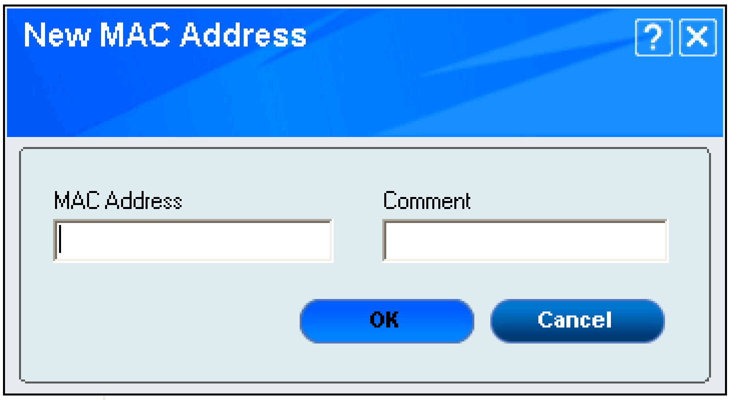
This section contains a list of Trusted Mac Addresses. A Mac address is a hardware address that uniquely identifies each node of a network.



☑ Show Application Alert ☑ Block Portscan

This tab has 4 buttons which are as follows:

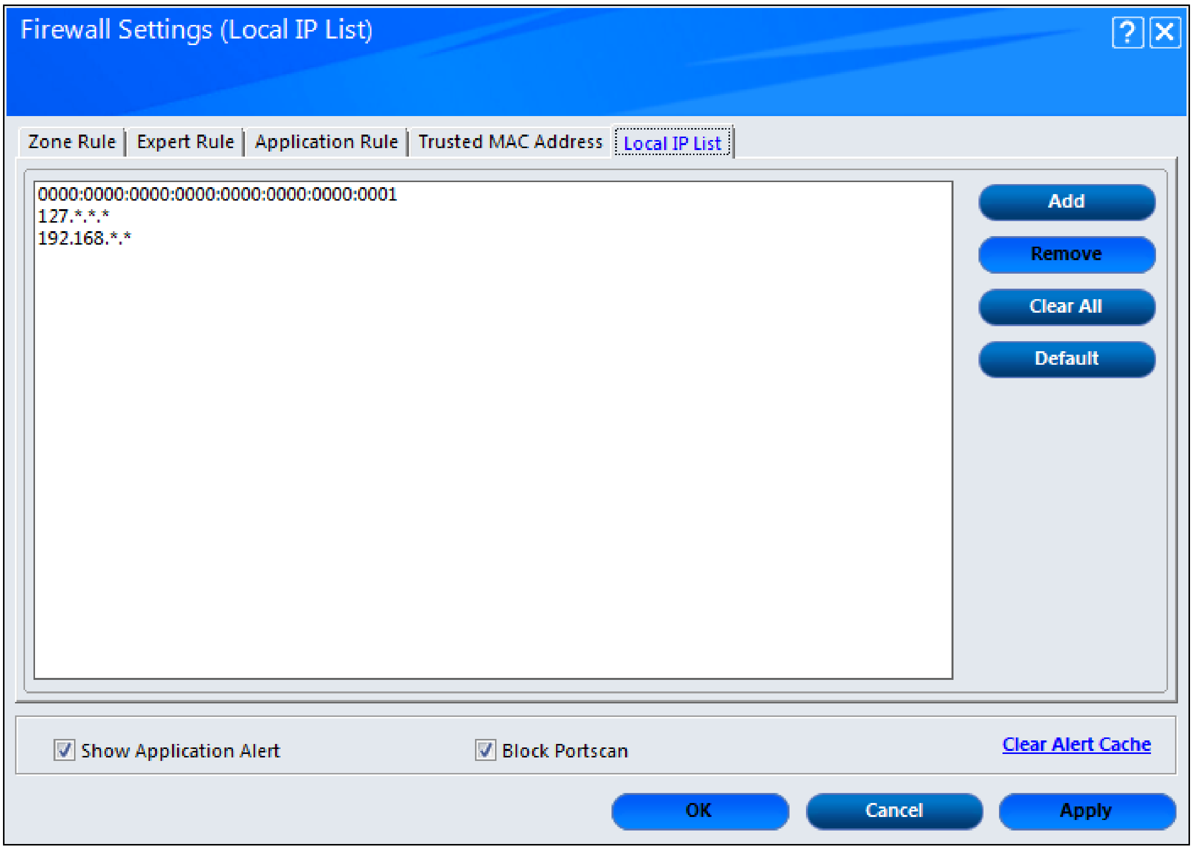
- **Add**: You can add new Mac address using this button. Once this button is clicked, you will see a New MAC Address dialogue box. Enter the **MAC Address** and **Comment** in this dialogue box and click **OK**. Click **Cancel** to close the dialogue box.



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

Local IP List

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

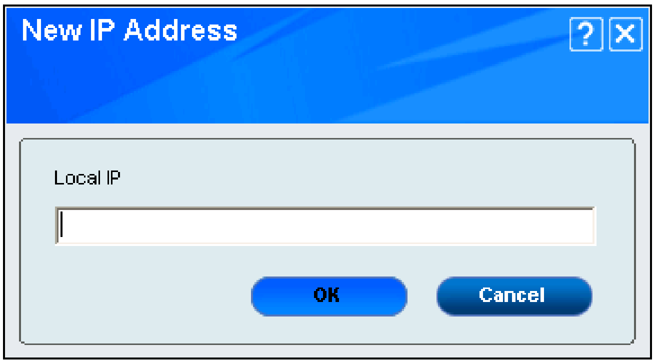


```
0000:0000:0000:0000:0000:0000:0000:0001
127.*.*.*
192.168.*.*
```

☑ Show Application Alert ☑ Block Portscan

This tab has 4 buttons which are as follows:

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



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

Show Application Alert

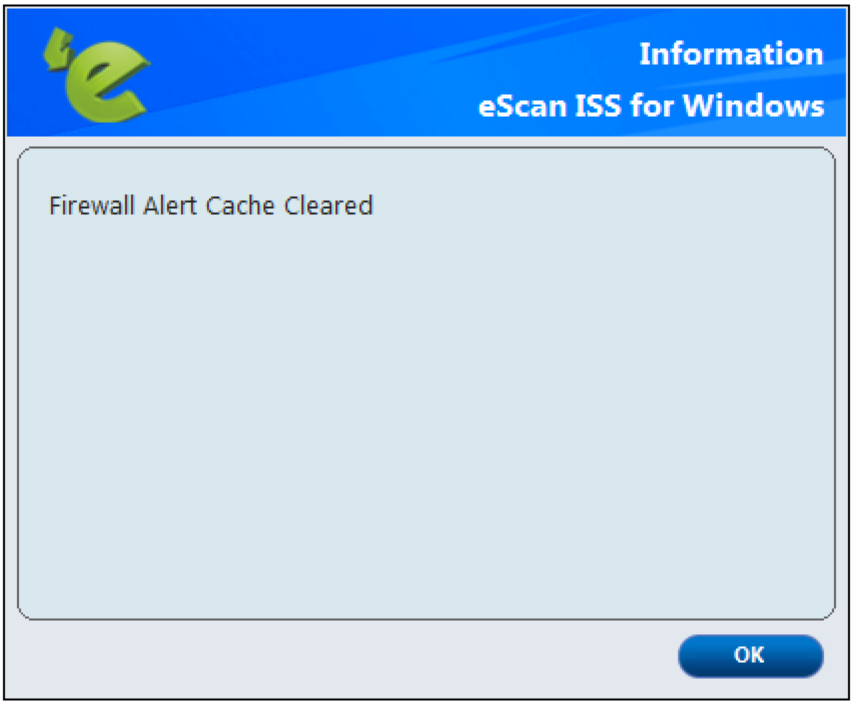
This check box is selected by default and provides you firewall alert when an application is blocked as per an application rule.

Block Portscan

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

Clear Alert Cache

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



Firewall Alert Cache Cleared

Reports

This setting gives you following details:

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

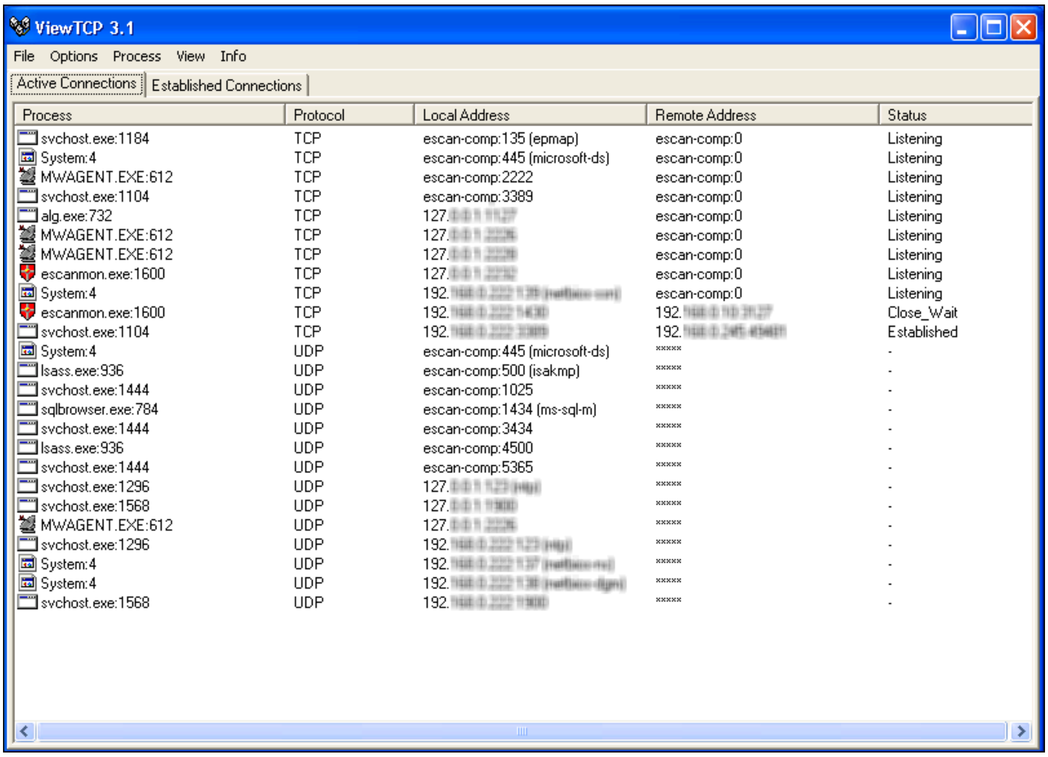
Outbound Packets Allowed
It shows the total number of outbound packets allowed by the firewall.

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

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

This setting also has following links available:

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

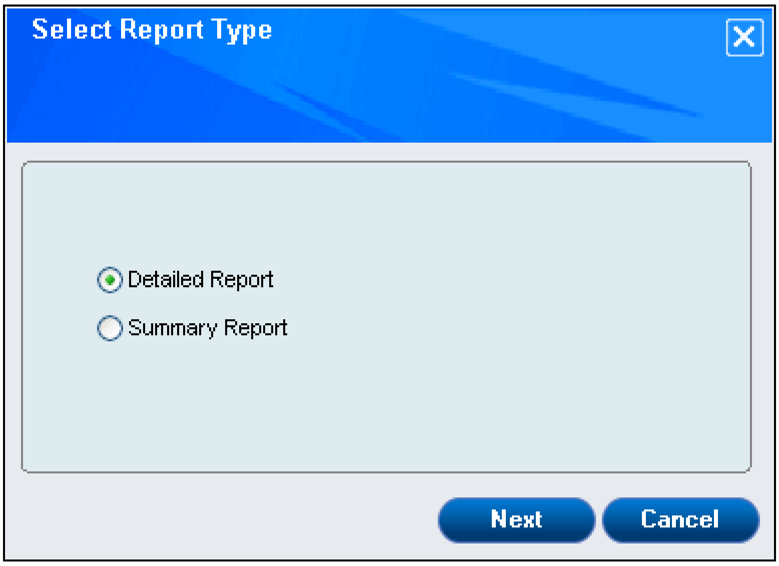


Process	Protocol	Local Address	Remote Address	Status
svchost.exe:1184	TCP	escan-comp:135 (epmap)	escan-comp:0	Listening
System:4	TCP	escan-comp:445 (microsoft-ds)	escan-comp:0	Listening
MWAGENT.EXE:612	TCP	escan-comp:2222	escan-comp:0	Listening
svchost.exe:1104	TCP	escan-comp:3389	escan-comp:0	Listening
alg.exe:732	TCP	127.[redacted]	escan-comp:0	Listening
MWAGENT.EXE:612	TCP	127.[redacted]	escan-comp:0	Listening
MWAGENT.EXE:612	TCP	127.[redacted]	escan-comp:0	Listening
escanmon.exe:1600	TCP	127.[redacted]	escan-comp:0	Listening
System:4	TCP	192.[redacted]	escan-comp:0	Listening
escanmon.exe:1600	TCP	192.[redacted]	192.[redacted]	Close_Wait
svchost.exe:1104	TCP	192.[redacted]	192.[redacted]	Established
System:4	UDP	escan-comp:445 (microsoft-ds)	*****	-
lsass.exe:936	UDP	escan-comp:500 (isakmp)	*****	-
svchost.exe:1444	UDP	escan-comp:1025	*****	-
sqlbrowser.exe:784	UDP	escan-comp:1434 (ms-sql-m)	*****	-
svchost.exe:1444	UDP	escan-comp:3434	*****	-
lsass.exe:936	UDP	escan-comp:4500	*****	-
svchost.exe:1444	UDP	escan-comp:5365	*****	-
svchost.exe:1296	UDP	127.[redacted]	*****	-
svchost.exe:1568	UDP	127.[redacted]	*****	-
MWAGENT.EXE:612	UDP	127.[redacted]	*****	-
svchost.exe:1296	UDP	192.[redacted]	*****	-
System:4	UDP	192.[redacted]	*****	-
System:4	UDP	192.[redacted]	*****	-
svchost.exe:1568	UDP	192.[redacted]	*****	-

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

View Summary

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

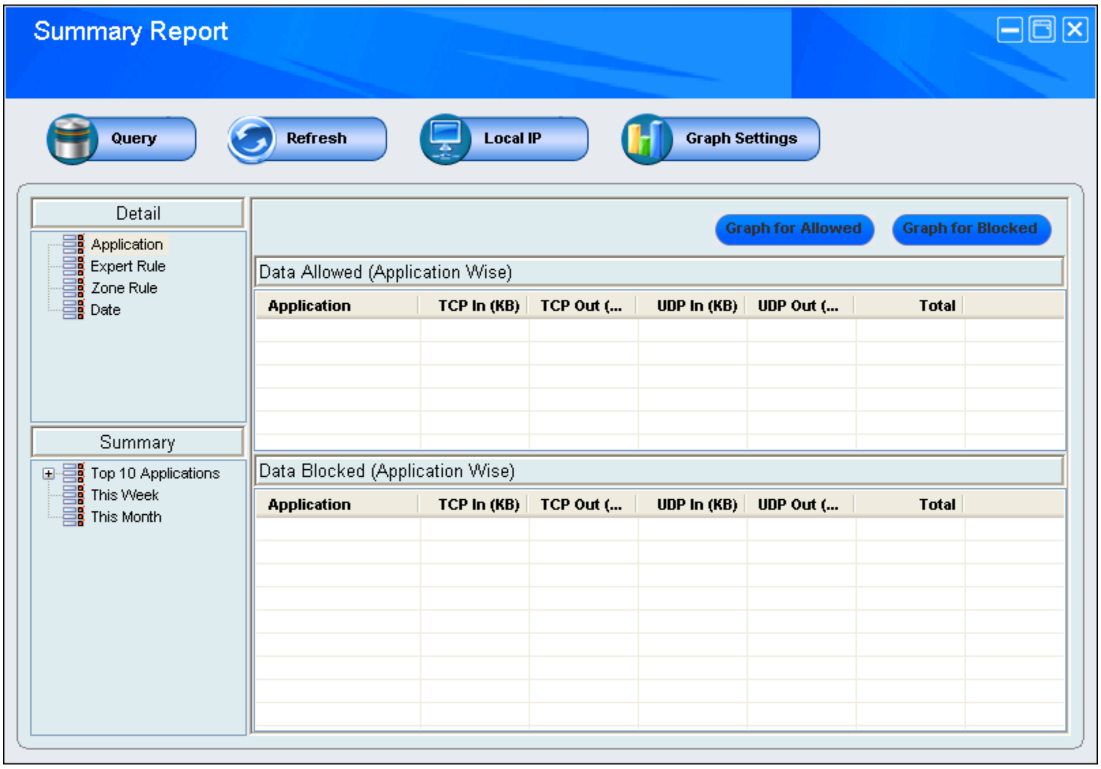


Select Report Type

● Detailed Report

○ Summary Report

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



Summary Report

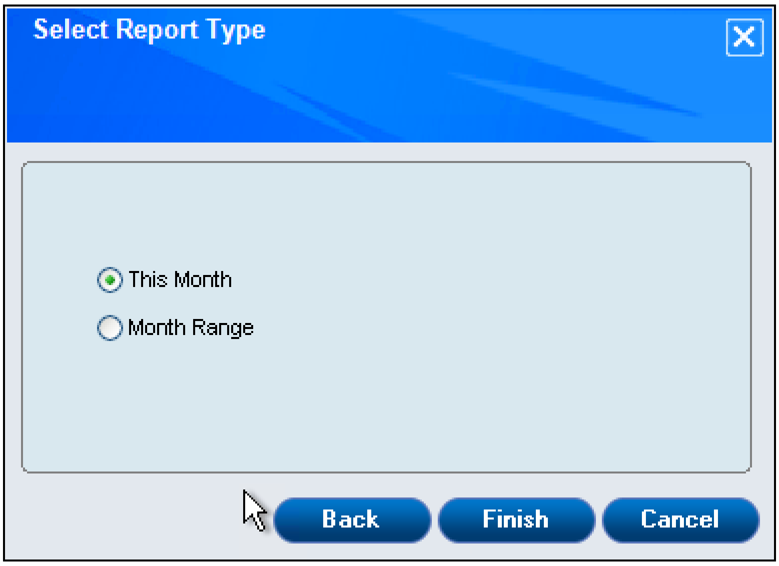
Data Allowed (Application Wise)

Application	TCP In (KB)	TCP Out (...	UDP In (KB)	UDP Out (...	Total

Data Blocked (Application Wise)

Application	TCP In (KB)	TCP Out (...	UDP In (KB)	UDP Out (...	Total

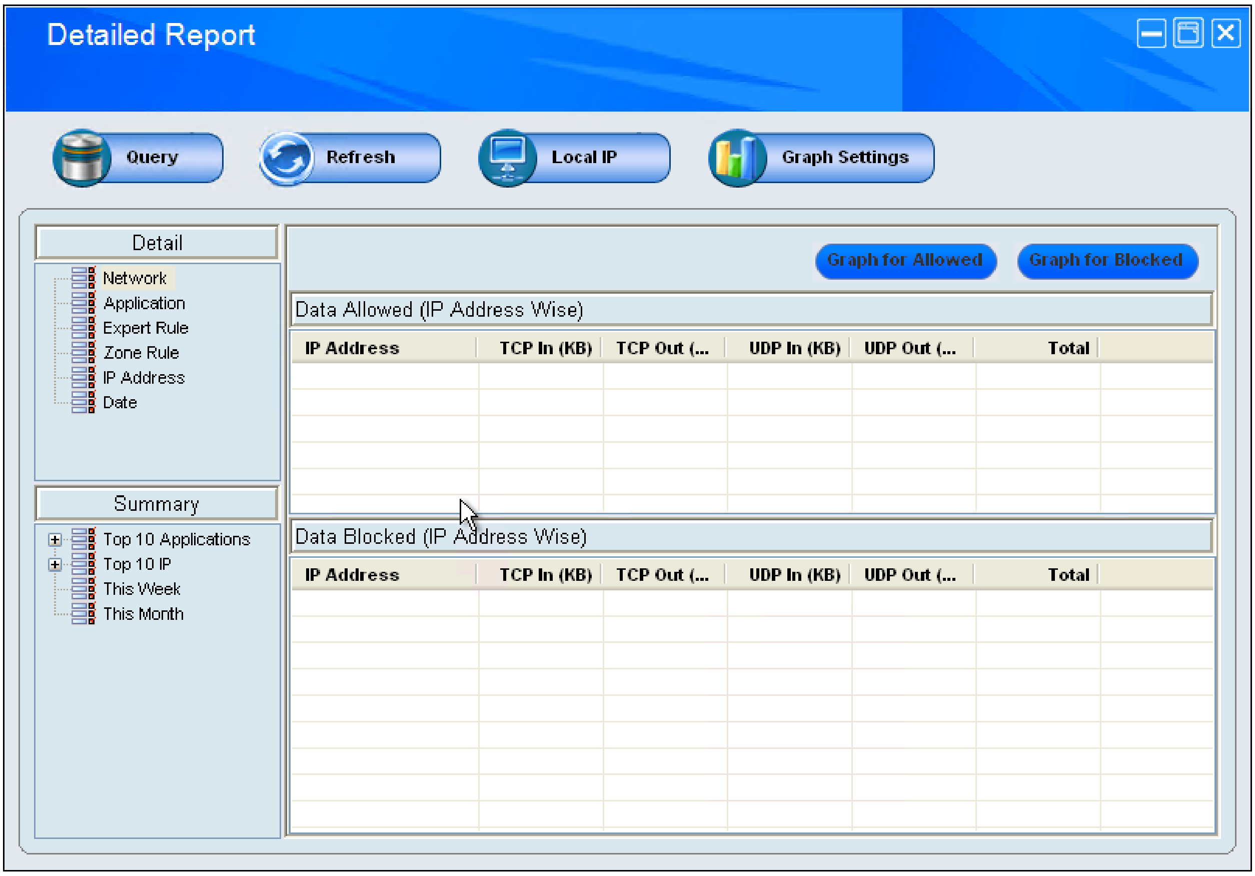
If you select **Detailed Report** in the **Select Report Type**, you will get option to select the month range or current month.



Select Report Type

● This Month
○ Month Range

You will get the detailed report of the same.



Detailed Report

Data Allowed (IP Address Wise)

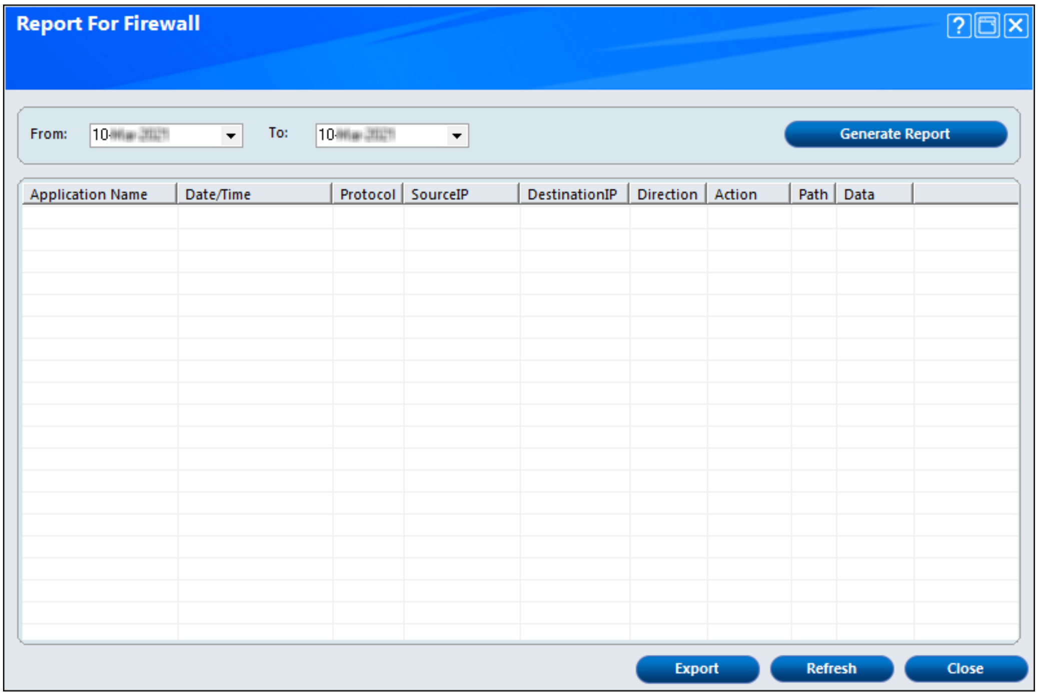
IP Address	TCP In (KB)	TCP Out (...	UDP In (KB)	UDP Out (...	Total

Data Blocked (IP Address Wise)

IP Address	TCP In (KB)	TCP Out (...	UDP In (KB)	UDP Out (...	Total

View Report

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



Report For Firewall

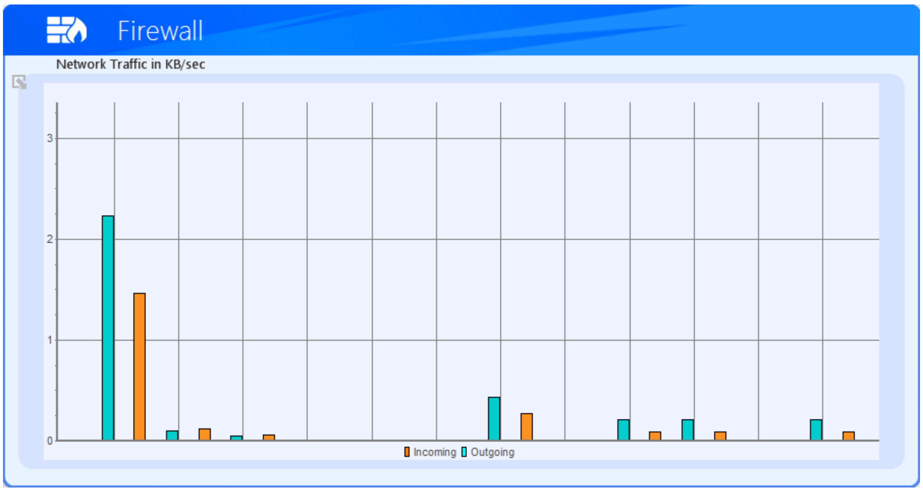
From: 10[redacted] To: 10[redacted] Generate Report

Application Name	Date/Time	Protocol	SourceIP	DestinationIP	Direction	Action	Path	Data

You can export reports in the following format:

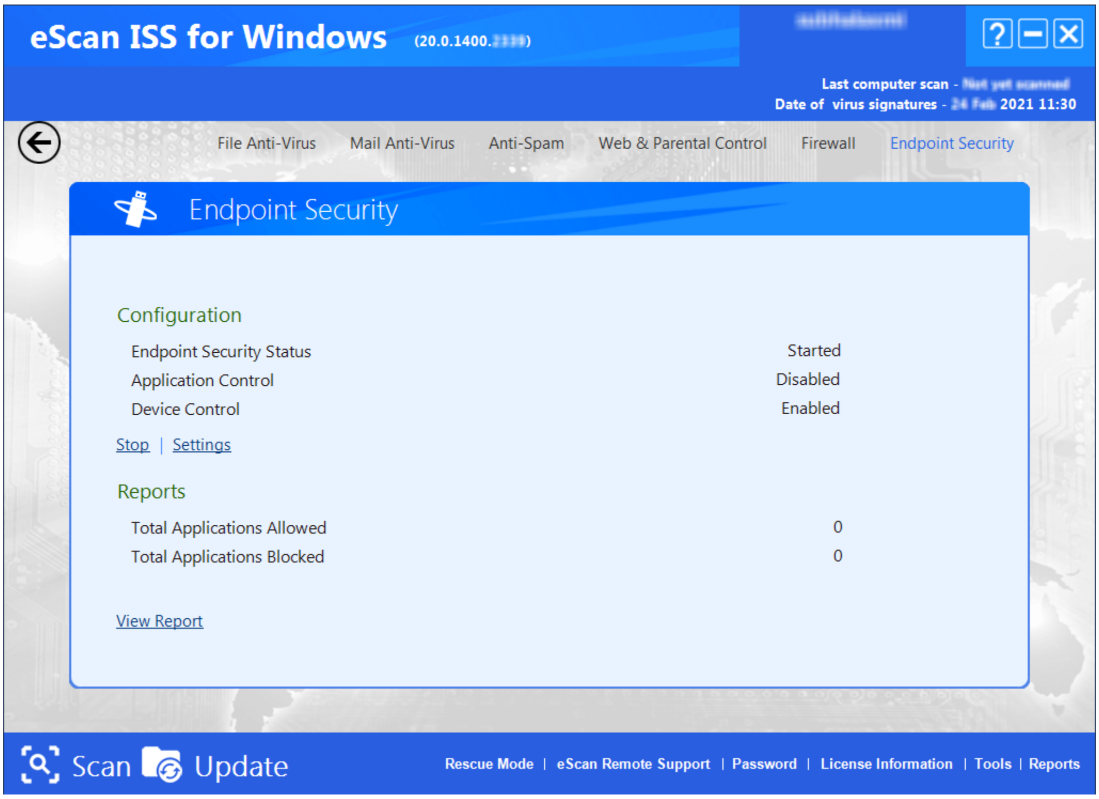
- PDF
- HTML
- CSV

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



Endpoint Security

Endpoint Security 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.


eScan ISS for Windows (20.0.1400.[redacted])
[redacted]
File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 11:30

Endpoint Security

Configuration

Endpoint Security Status	Started
Application Control	Disabled
Device Control	Enabled

Stop | Settings

Reports

Total Applications Allowed	0
Total Applications Blocked	0

View Report

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

Configuration

This section displays the following information:

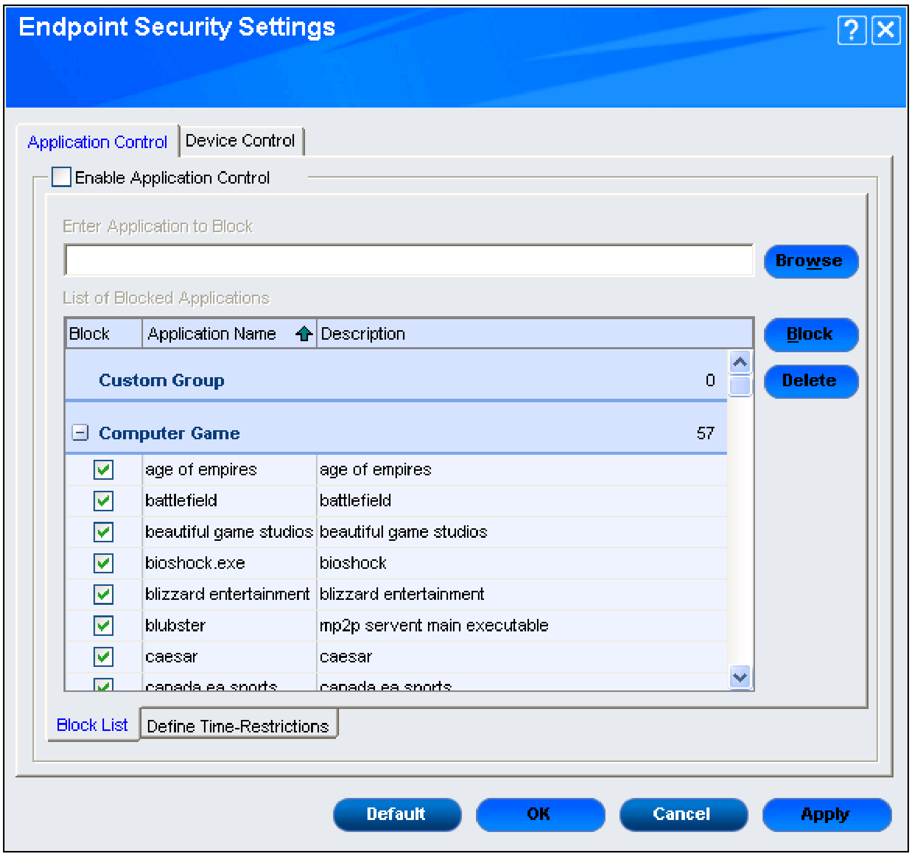
- **Endpoint Security Status:** It displays the status of whether Endpoint Security module is started or stopped.
- **Application Control:** It displays the status of Application Control.
- **Device Control:** It displays the status of Device Control.
- **Start/Stop:** Click on this option to enable or disable Endpoint Security module.
- **Settings:** To learn more, click here.

Settings

When you click this button, the Endpoint Security Settings window appears and it has two tabs, namely Application Control and Device Control.

Application Control

This tab helps you control execution of applications on the computer. You can configure the following option.



□ Enable Application Control

Enter Application to Block

List of Blocked Applications

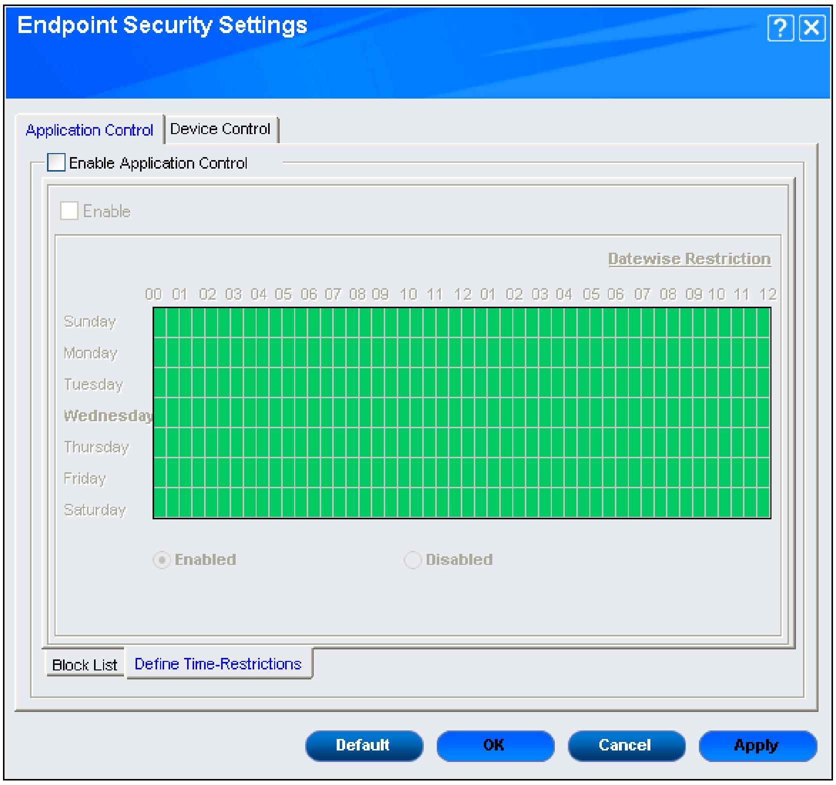
Block	Application Name	Description
	Custom Group	0
⊟	Computer Game	57
☑	age of empires	age of empires
☑	battlefield	battlefield
☑	beautiful game studios	beautiful game studios
☑	bioshock.exe	bioshock
☑	blizzard entertainment	blizzard entertainment
☑	blubster	mp2p servent main executable
☑	caesar	caesar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

- **Block list:** This tab helps you to configure settings for blocking the unwanted applications. You can do it by configuring it using following settings:
  - **Enable Application Control:** This check box enables Application Control feature, which helps you to block application.
    - **Enter Application to Block:** This field and **Browse** button is available only when you select **Enable Application Control** check box. Type or click the **Browse** button to select name of the application that you want to block, and then click the **Block** button. If you want to delete an application, click an appropriate application from the group that you want to delete, and then click the **Delete** button.
  - **List of Blocked Applications**: It contains the list of blocked executables of applications that are pre-defined by MicroWorld. By default, all the applications listed in pre-defined category are blocked. You can also add application that you want to block, but only to the **Custom Group** category. 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 blocked 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.

- **Define Time-Restrictions**: This feature helps you define time restriction on when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day.



Endpoint Security Settings

Application Control | Device Control

☐ Enable Application Control

☐ Enable

● Enabled ○ Disabled

This tab has following setting for configuration:

- **Enable:** By default, this check box appears dimmed. It is available only if you select the **Enable Application Control** check box and you can define time restriction.
    - **Enabled:** This option is available by default as **Enable** check box is selected already. This option allows access to the applications on certain days at specific time, and then you can select the days and time by clicking the appropriate boxes from the matrix.
    - **Disabled:** This option is available only when you select **Enable** check box. This option blocks access to the applications on certain days at specific time, and then you can select the days and time by clicking the appropriate boxes in the matrix.
    - **Datewise Restriction:** This option lets you define datewise restrictions when you want to allow or block access to the applications based on specific dates and between pre-defined hours during that date.

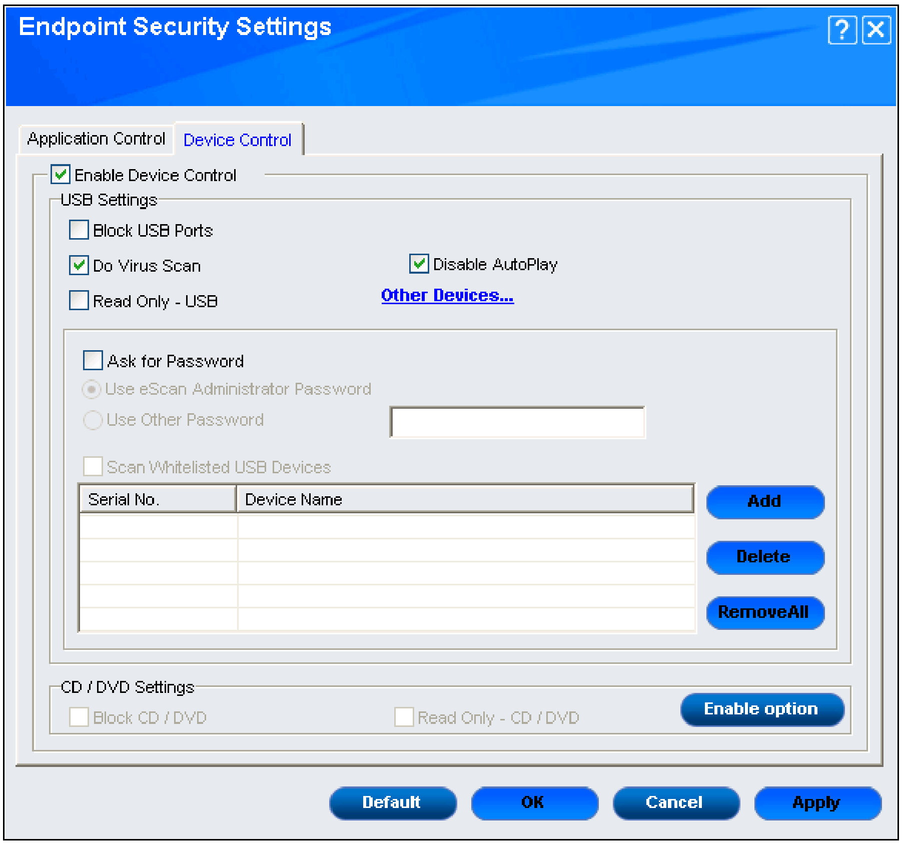
Device Control

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

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

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

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



Endpoint Security Settings

Application Control | Device Control

☑ Enable Device Control

USB Settings

☐ Block USB Ports

☑ Do Virus Scan ☑ Disable AutoPlay

☐ Read Only - USB Other Devices...

☐ Ask for Password

● Use eScan Administrator Password

○ Use Other Password

☐ Scan Whitelisted USB Devices

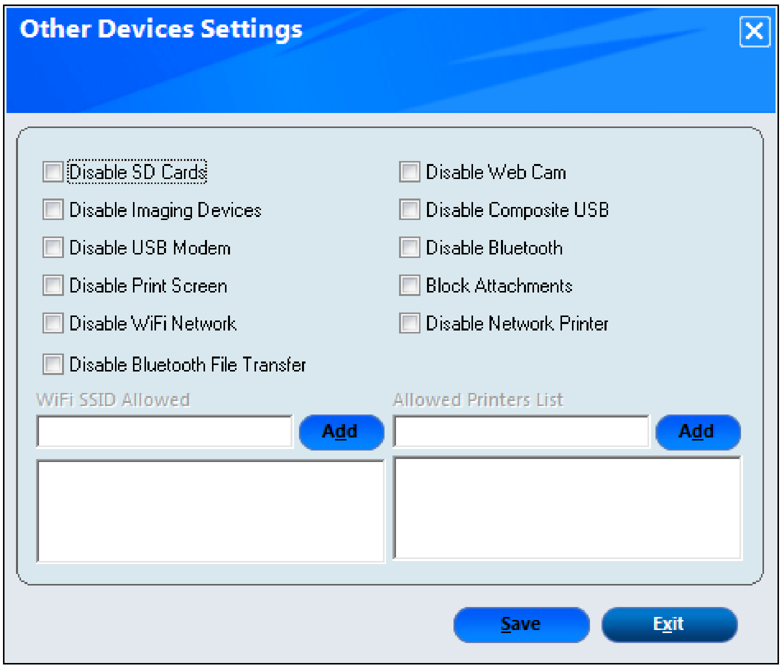
Serial No.	Device Name

CD / DVD Settings

☐ Block CD / DVD ☐ Read Only - CD / DVD

You can configure the following settings:

- **Enable Device Control:** This check box is available by default and monitors the devices connected to your computer. When you select this check box, all the fields become available.
- **USB Settings:** This section helps you to customize the settings for controlling access to USB storage devices.
  - **Block USB Ports:** This field is available only when you select **Enable Device Control** check box. This check box blocks all USB ports of system. When you select this check box, **Ask for Password**, **Do Virus Scan**, **Disable AutoPlay** and **Read Only- USB** button becomes unavailable.
  - **Do Virus Scan:** This field is available by default and runs a virus scan whenever a USB Device is plugged in, It is recommended that you always keep this check box selected.
  - **Read Only - USB:** This check box allows access to the USB device in a read-only mode.
  - **Disable AutoPlay:** This check box is available by default and disables the automatic execution of any program stored on a USB storage device when you connect the device.
  - **Other Devices**: Here you can add WiFi and Printers that can be whitelisted. This link will open a popup with following options:



Other Devices Settings

□ Disable SD Cards
□ Disable Imaging Devices
□ Disable USB Modem
□ Disable Print Screen
□ Disable WiFi Network
□ Disable Bluetooth File Transfer
□ Disable Web Cam
□ Disable Composite USB
□ Disable Bluetooth
□ Block Attachments
□ Disable Network Printer

WiFi SSID Allowed

Allowed Printers List

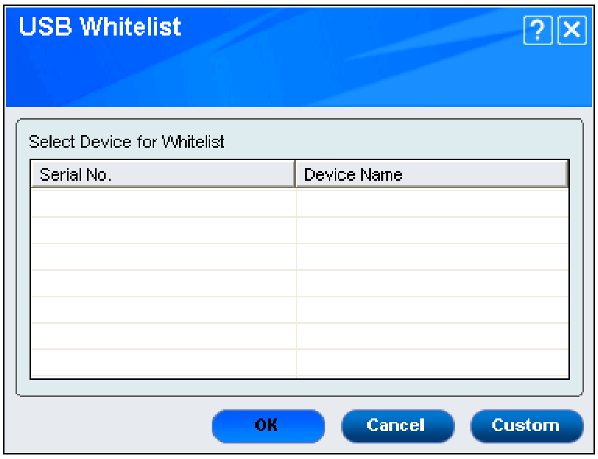
- **Disable SD Cards:** This option disable the SD cards.
- **Disable Web Cam:** This check box disable the access of web cam.
- **Disable Imaging Devices**: This check box disable the access of imaging device.
- **Disable Composite USB**: This check box disable the access of composite USB.
- **Disable USB Modem**: This check box disable the access of USB Modem.
- **Disable Bluetooth**: This check box disable the access of Bluetooth.

        - **Disable Print Screen**: This check box disables the access of print screen.
        - **Block Attachments**: This check box blocks all the attachments.
        - **Disable WiFi Network**: This check box disable the access of WiFi expect for the whitelisted WiFi network.
        - **Disable Network Printer**: This check box disable the access of network printer expect for the whitelisted network printer.
        - **Disable Bluetooth File Transfer**: This check box disable the access of Bluetooth file transfer.

- **Ask for Password:** This field is available only when you select **Enable Device Control** check box. Select this check box, if you want eScan to prompt for a password, whenever a USB storage device is connected to the computer. Do any one of the following:
    - **Use eScan Administrator Password:** This option uses eScan Administrator password for accessing USB device.
    - **Use Other Password:** This option assign a unique password for accessing USB storage device. You have to enter your unique password for accessing USB.
- **Scan Whitelisted USB Device**: This check box allows to scan even the USB devices that are whitelisted, before accessing.

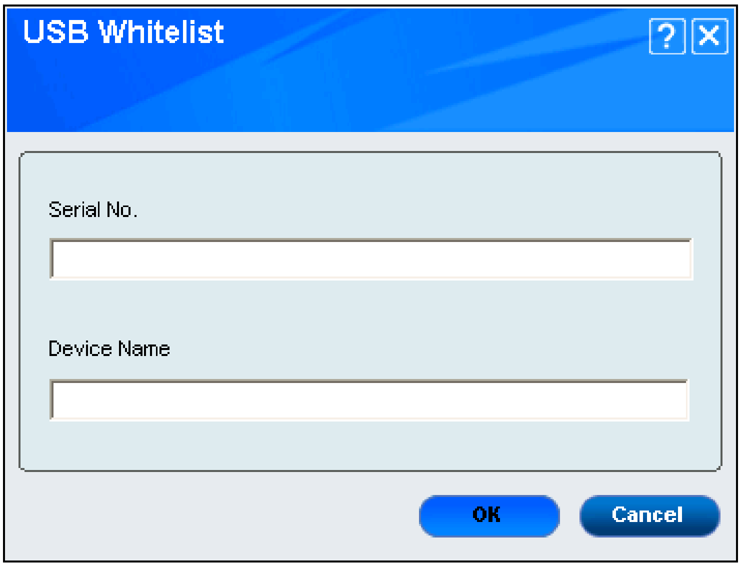
  eScan provides a greater level of endpoint security by prompting you for a password, whenever you connect a USB drive. To disable password protection for a specific device, you can add it to the whitelist along with its name and serial number. Due to which, next time when you connect the device it does not prompt you for a password for accessing the device.

This section displays the serial number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking the **Add** button you will get a popup window. It also displays the list of USB's connected previously to the system before adding to white list.

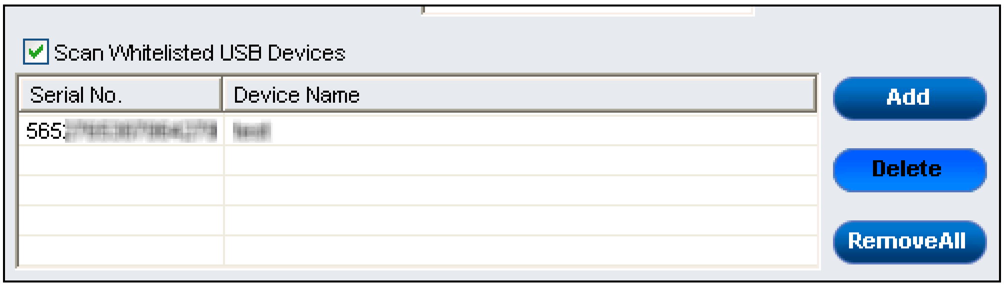


Serial No.	Device Name

Click on **Custom** button and enter the **Serial No.** of device and **Device Name**.



Click on **OK**, the device will be added in the list.



☑ Scan Whitelisted USB Devices

Serial No.	Device Name
565[redacted]	[redacted]

- **Scan Whitelisted USB Devices:** This field scans all USB devices that are added to the whitelist.
- **CD/DVD Settings**: This section helps you to customize the settings for controlling access to CD/DVD.
    - **Enable option**: Click on this button to enable CD/DVD settings.
    - **Block CD/DVD**: This field is available only when you click **Enable option** button. This check box blocks all CD/DVD access.
    - **Read Only – CD/DVD**: Select this check box to allow read-only access for CD/DVD.

Default
This button applies the default settings.

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

Cancel
This button cancels the configured settings or to close the window.

Apply
This button applies the configured settings.

Reports

It displays following count along with the report:

Total Applications Allowed

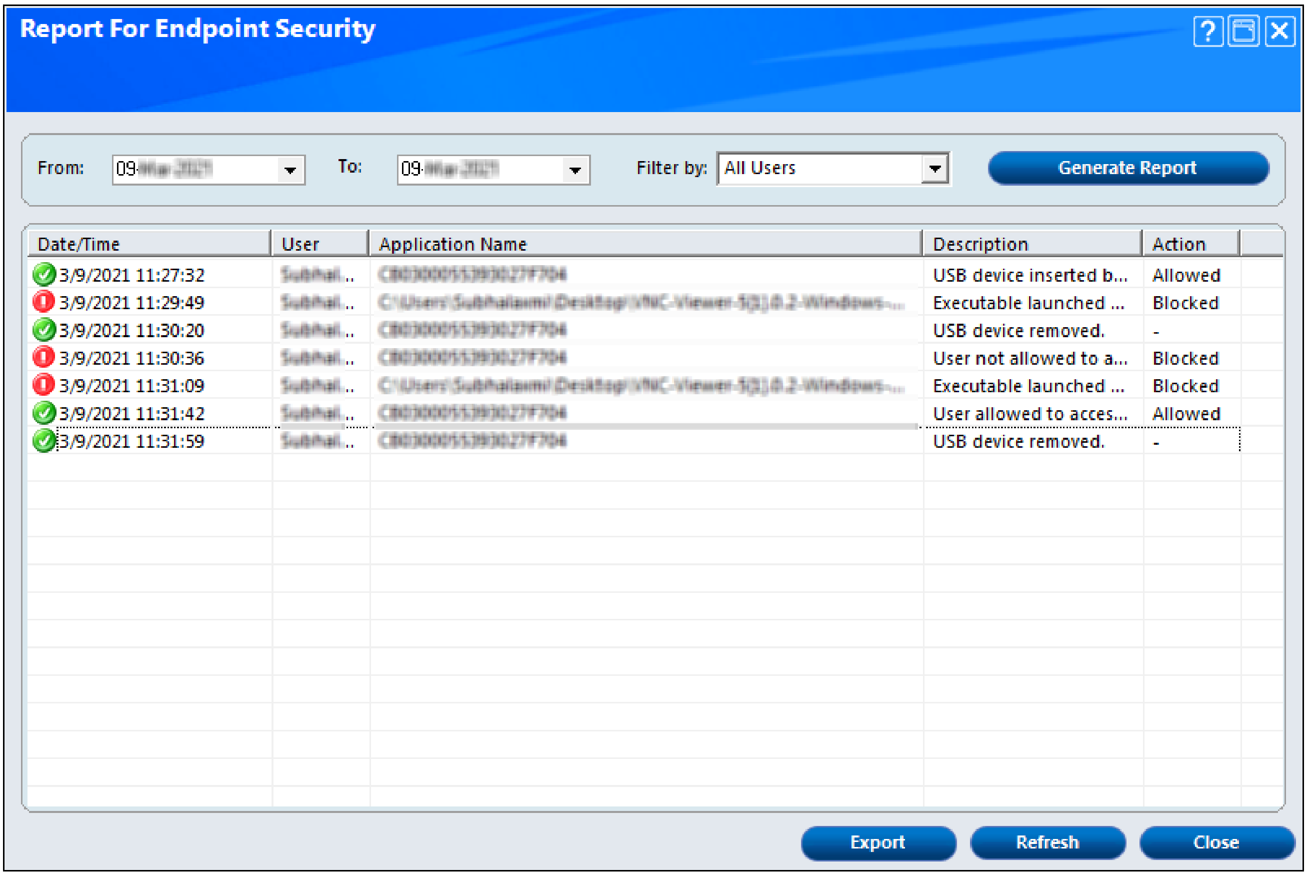
It shows the total number of applications allowed by Application Control module.

Total Application Blocked

It shows the total number of applications blocked by Application Control module.

View Report

This link opens the Report For Endpoint Security window. This window includes the **Generate Report** button, which displays the report for the Endpoint Security module for a given range of dates in a tabular format.



From: 09-[redacted] To: 09-[redacted] Filter by: All Users

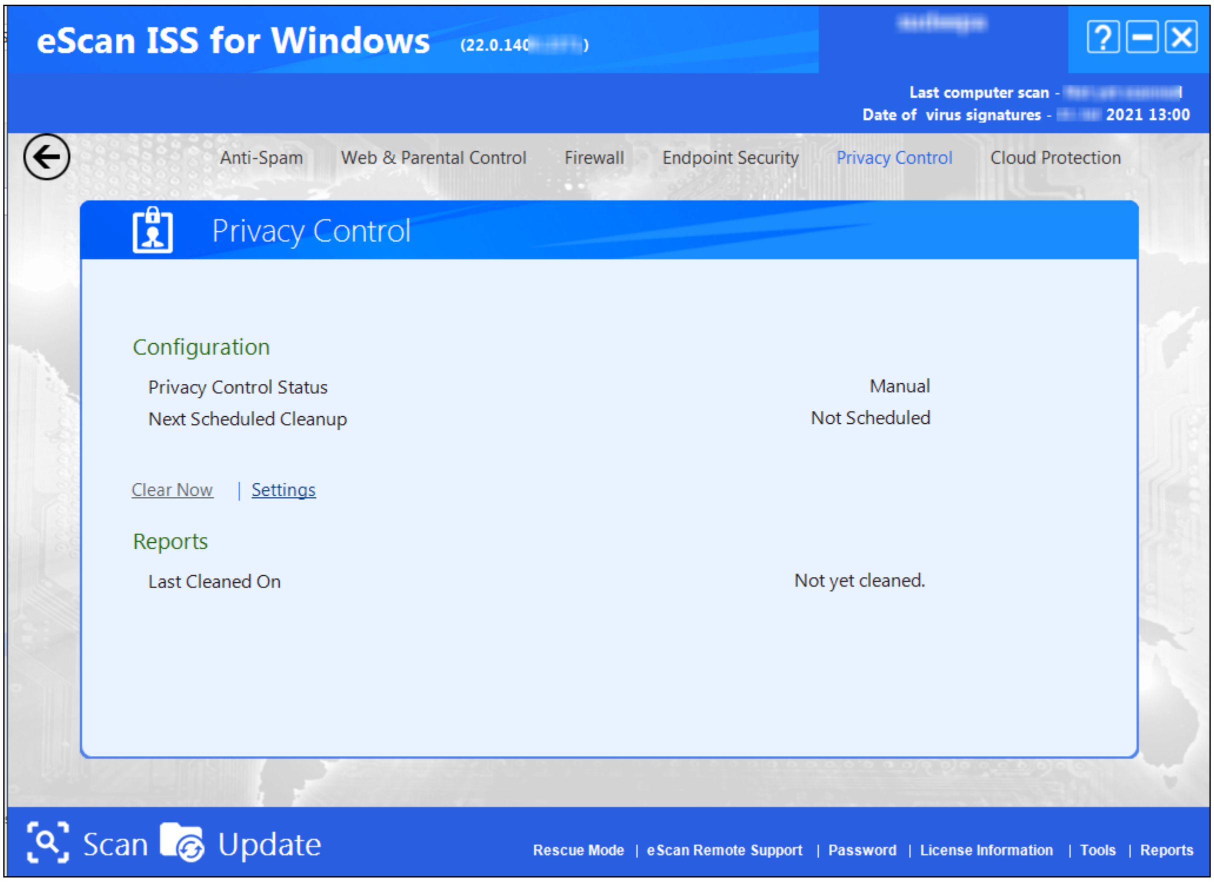
Date/Time	User	Application Name	Description	Action
✓ 3/9/2021 11:27:32	[redacted]	[redacted]	USB device inserted b...	Allowed
! 3/9/2021 11:29:49	[redacted]	[redacted]	Executable launched ...	Blocked
✓ 3/9/2021 11:30:20	[redacted]	[redacted]	USB device removed.	-
! 3/9/2021 11:30:36	[redacted]	[redacted]	User not allowed to a...	Blocked
! 3/9/2021 11:31:09	[redacted]	[redacted]	Executable launched ...	Blocked
✓ 3/9/2021 11:31:42	[redacted]	[redacted]	User allowed to acces...	Allowed
✓ 3/9/2021 11:31:59	[redacted]	[redacted]	USB device removed.	-

You can export reports in the following format:

- PDF
- HTML
- CSV

Privacy Control

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


eScan ISS for Windows (22.0.140[redacted])
[redacted]
Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 13:00
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Privacy Control
Cloud Protection
Privacy Control
Clear Now
Settings
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Configuration

Privacy Control Status: Manual

Next Scheduled Cleanup: Not Scheduled

Reports

Last Cleaned On: Not yet cleaned.

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

Configuration

This section displays the following information:

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

In addition, you can perform the following tasks:

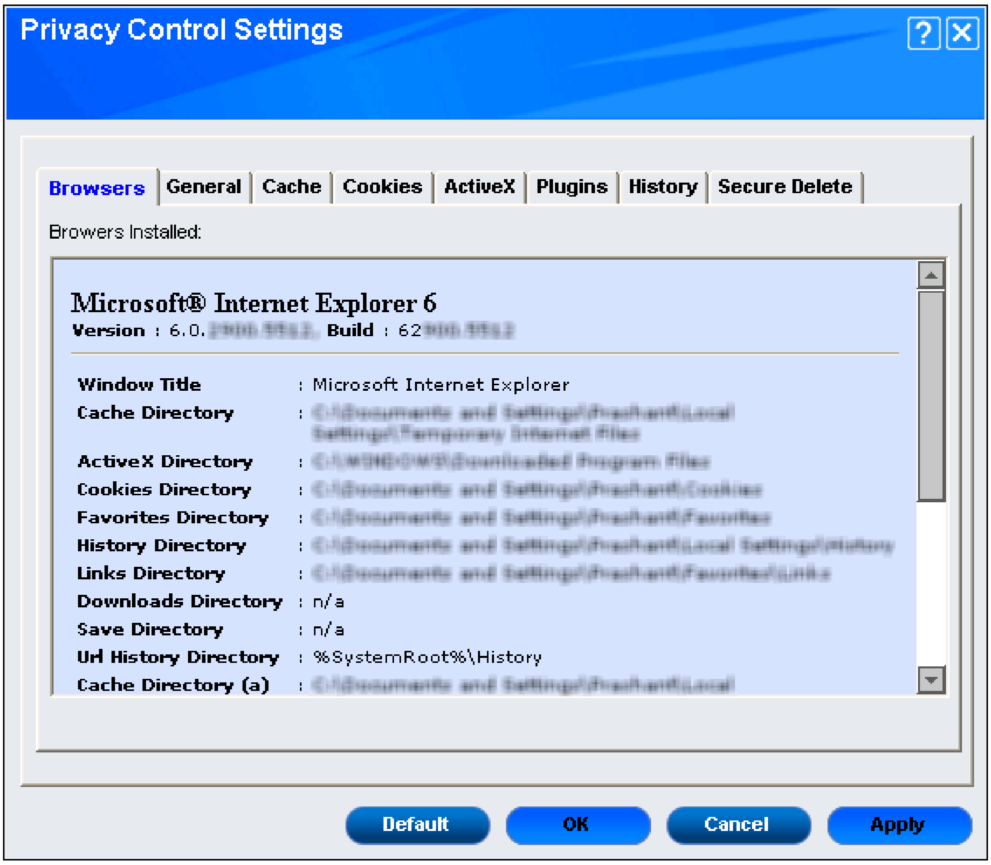
- **Clear Now**: This button clears the information specified under **Options** in the Browser Clean up dialog box.
- **Settings**: To learn more, click here.

Settings

Under Settings we have following tabs -- Browsers, General, Cache, Cookies, ActiveX, Plugins, History and Secure Delete. Let's see them in detail.

Browsers

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



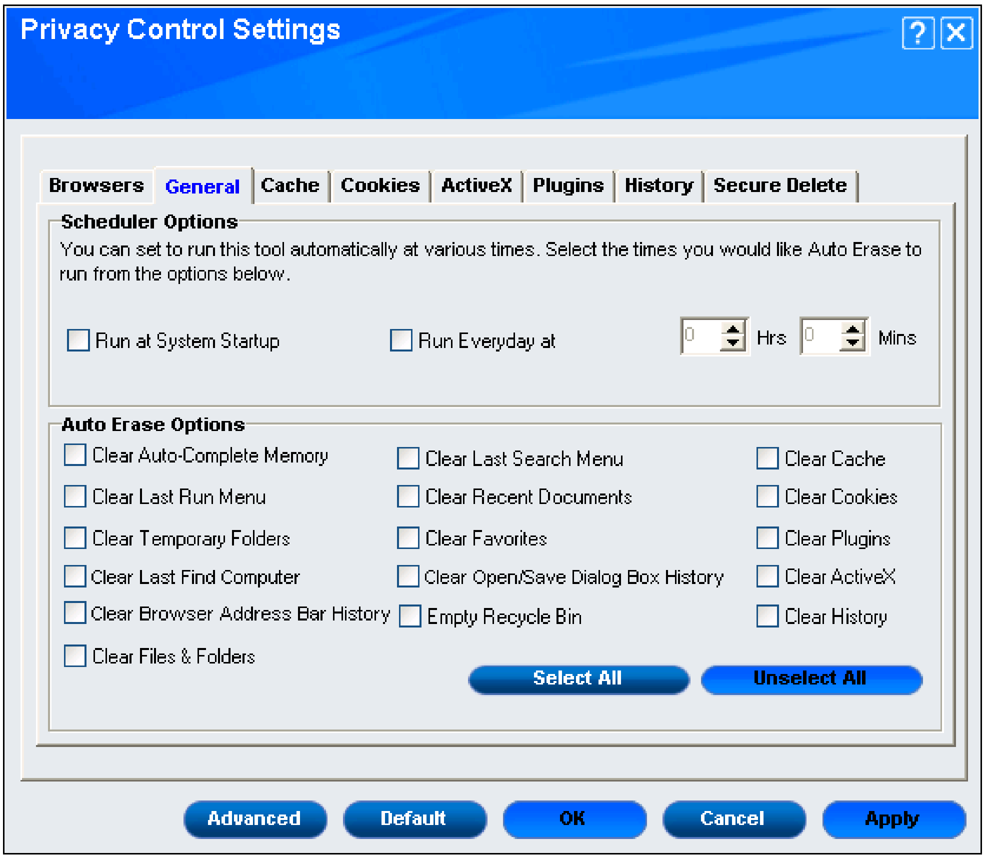
Browers Installed:

Microsoft® Internet Explorer 6
Version : 6.0.[redacted] **Build** : 62[redacted]

Window Title	: Microsoft Internet Explorer
Cache Directory	: [redacted]
ActiveX Directory	: [redacted]
Cookies Directory	: [redacted]
Favorites Directory	: [redacted]
History Directory	: [redacted]
Links Directory	: [redacted]
Downloads Directory	: n/a
Save Directory	: n/a
Url History Directory	: %SystemRoot%\History
Cache Directory (a)	: [redacted]

General

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



Privacy Control Settings

Browsers | General | Cache | Cookies | ActiveX | Plugins | History | Secure Delete

Scheduler Options

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

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

Auto Erase Options

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

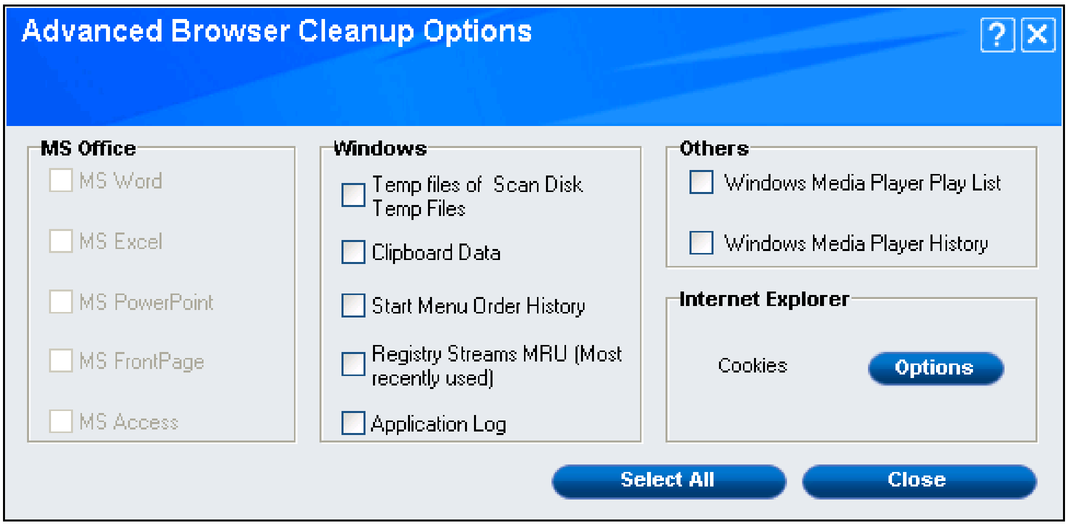
You can configure the following settings:

- **Scheduler Options:** You can set the scheduler to run at specific time and erase private information, such as your browsing history from your computer. You can perform the following settings:
  - **Run at System Startup:** This check box executes auto erase tool at system startup if selected. It automatically executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.
  - **Run Everyday at:** This check box specifies the time at which you want auto erase tool to run. It auto-executes the Privacy Control module at a specified time and performs the desired auto-erase functions.

    The **Hrs** and **Mins** field is available only when you select **Run Everyday at** check box. Set the time in hours and minutes in appropriate boxes.
- **Auto Erase Options:** The browser stores traceable information of the websites that you have visited in certain folders. This information can be viewed by others. This option allows you to remove all traces of websites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. Select the following options based on your requirement:

- **Clear Auto-Complete Memory:** Auto-Complete Memory refers to the suggested matches that appear when you type text in the Address bar, the Run dialog box, or forms in Web pages. Hackers can use this information to monitor your surfing habits. When you select this check box, Privacy Control clears all this information from the computer.
- **Clear Last Run Menu:** This check box clears the information in the Run dialog box.
- **Clear Temporary Folders:** This check box clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive of the computer and boosts the performance of the computer.
- **Clear Last Find Computer:** This check box clears name of the computer for which you searched last.
- **Clear Browser Address Bar History:** This check box clears websites from the browser's address bar history.
- **Clear Files & Folders:** This option will delete files and folders added in secure delete. Use this option with caution as it permanently deletes unwanted files and folders from the computer to free space on the computer.
- **Clear Last Search Menu:** This check box clears name of the objects that you last searched for by using the Search Menu.
- **Clear Recent Documents:** This check box clears names of the objects found in Recent Documents of your system.
- **Clear Favorites:** This check box clears Favorites added by the user in the computer.
- **Clear Open/Save Dialog Box History:** This check box clears the links of all the opened and saved files.
- **Empty Recycle Bin:** This check box clears the Recycle Bin. You should use this option with caution because it permanently clears the recycle bin.
- **Clear Cache:** This check box clears the all Temporary Internet Files in the system.
- **Clear Cookies:** This check box clears the Cookies stored by websites in the browser's cache.
- **Clear Plugins:** This check box removes the browser plug-in.
- **Clear ActiveX:** This check box clears the ActiveX controls.
- **Clear History:** This check box clears the history of all the websites that you have visited.

- **Advanced:** Click on **Advanced Browser Cleanup Options** popup appears. Select the required check box and close.



Advanced Browser Cleanup Options

MS Office
□ MS Word
□ MS Excel
□ MS PowerPoint
□ MS FrontPage
□ MS Access

Windows
□ Temp files of Scan Disk Temp Files
□ Clipboard Data
□ Start Menu Order History
□ Registry Streams MRU (Most recently used)
□ Application Log

Others
□ Windows Media Player Play List
□ Windows Media Player History

Internet Explorer
Cookies Options

Select All Close

  - **MS Office:** The most recently opened MS office files will be cleared if these options are selected.
  - **Windows:** The respective unwanted files like temp files will be cleared.
  - **Others:** The recent Windows media player playlist and its history will be cleared.
  - **Internet Explorer:** Cookies will be cleared as per requirement.

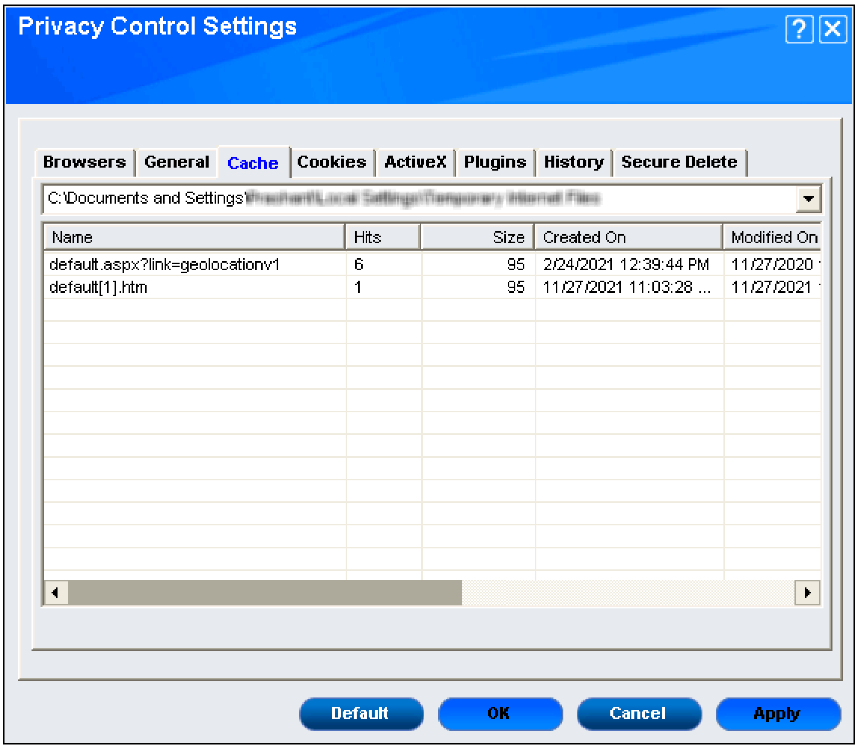
Select All: To select all the options at once, click on this button.

Close: This button closes the popup window.

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

Cache

A **cache** is a hardware or software component that stores data so future requests for that data can be served faster; the data stored in a cache might be the result of an earlier computation, or the duplicate of data stored elsewhere. A cache hit occurs when the requested data can be found in a cache, while a cache miss occurs when it cannot. The cache tab displays the cache components such as name, hit, modified date, storage path, size, created date, and last accessed date.



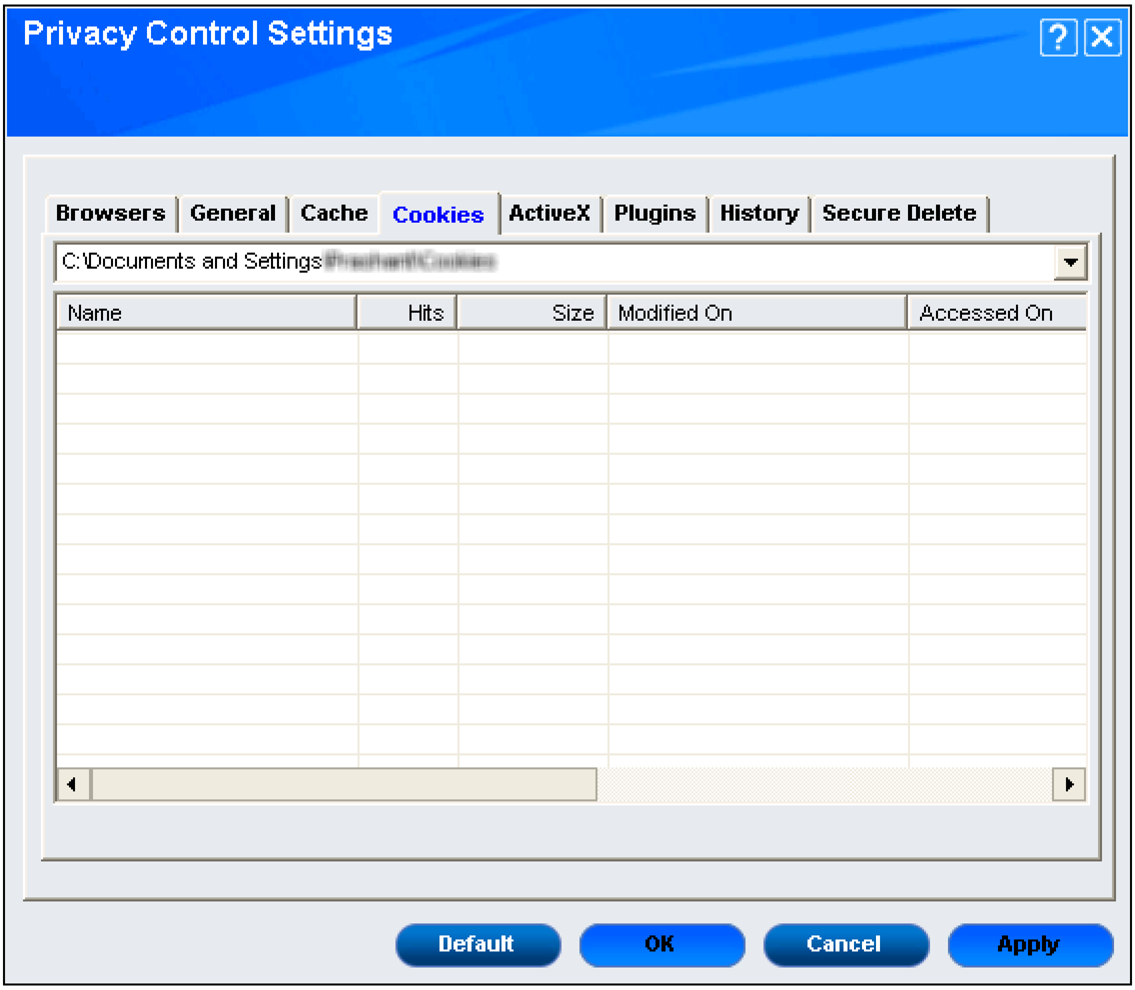
C:\Documents and Settings\[redacted]

Name	Hits	Size	Created On	Modified On
default.aspx?link=geolocationv1	6	95	2/24/2021 12:39:44 PM	11/27/2020
default[1].htm	1	95	11/27/2021 11:03:28 ...	11/27/2021

Cookies

An **HTTP cookie** (also called **web cookie**, **Internet cookie**, **browser cookie**, or simply **cookie**) is a small piece of data sent from a website that is stored on the user's computer by the web browser while he/she is browsing. They can also be used to remember arbitrary pieces of information that the user previously entered into form fields such as names, addresses, passwords, and credit card numbers.

Cookies tab displays the cookie data such as name, hits, modified date, storage path, size, created date, expiry date, and last accessed date.

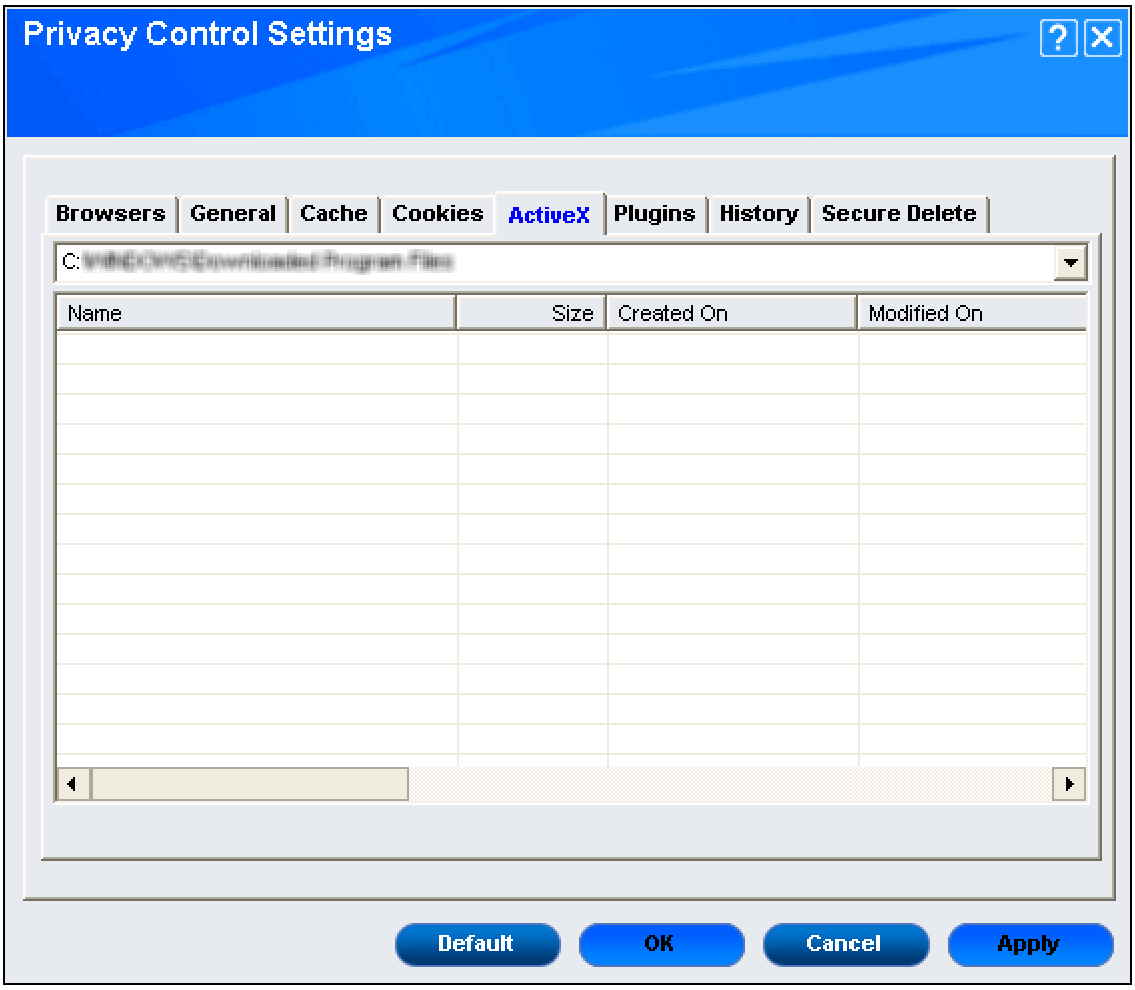


C:\Documents and Settings\[redacted]

ActiveX

ActiveX is a framework for defining reusable software components (also known as ActiveX controls) in a programming-language independent way. Because ActiveX encapsulates specific functionality as ActiveX controls, it can be seamlessly incorporated into many software applications. The Internet Explorer web browser allows for ActiveX controls to be embedded into web pages. ActiveX controls officially run only in the Internet Explorer browser running on a Windows operating system.

This tab displays the ActiveX details such as name, modified date, storage path, size, created date, version, description, company name, comments, and last accessed date.

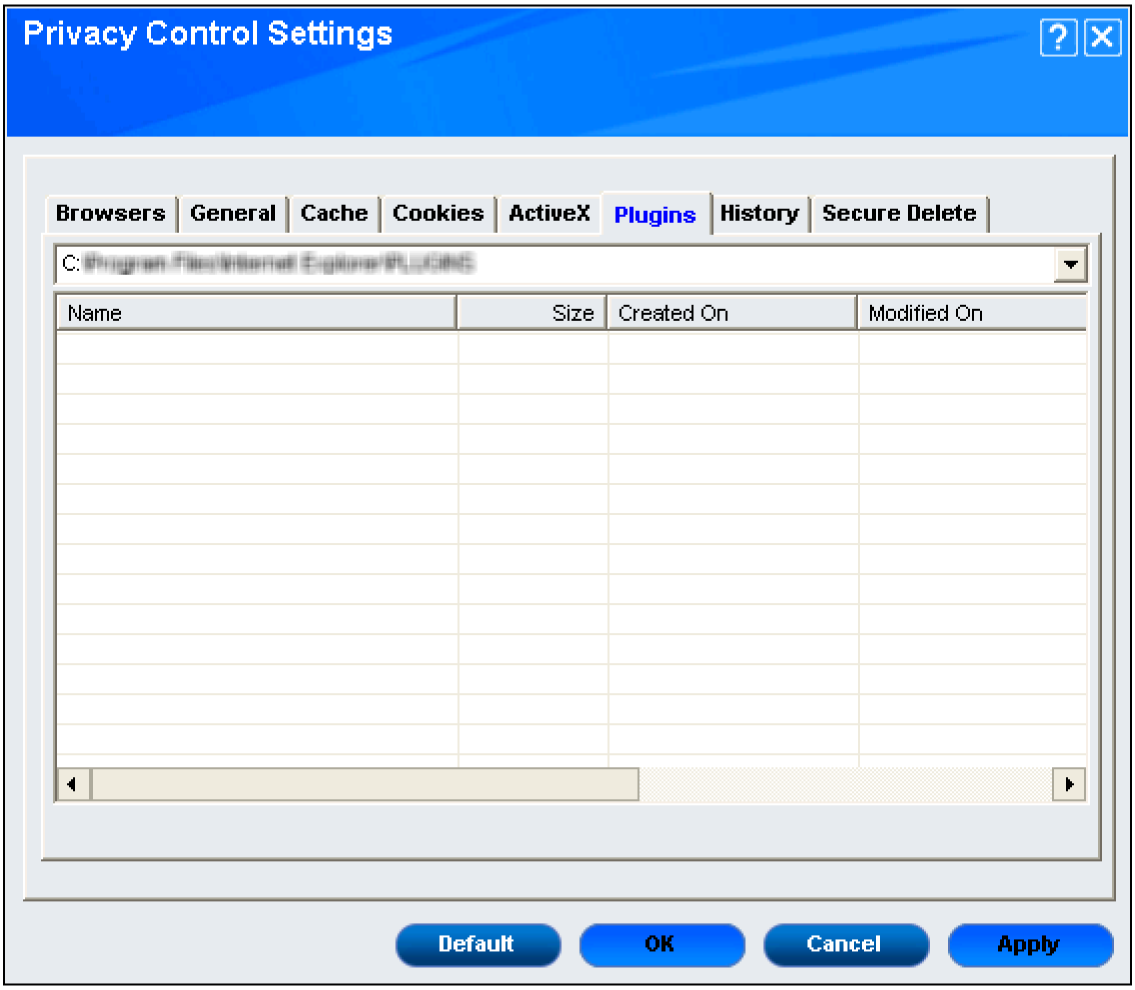

Privacy Control Settings

C:[redacted]

Plugins

When a program supports plug-ins, it enables customization. The common examples are the plug-ins used in web browsers to add new features such as search-engines, virus scanners, or the ability to use a new file type such as a new video format.

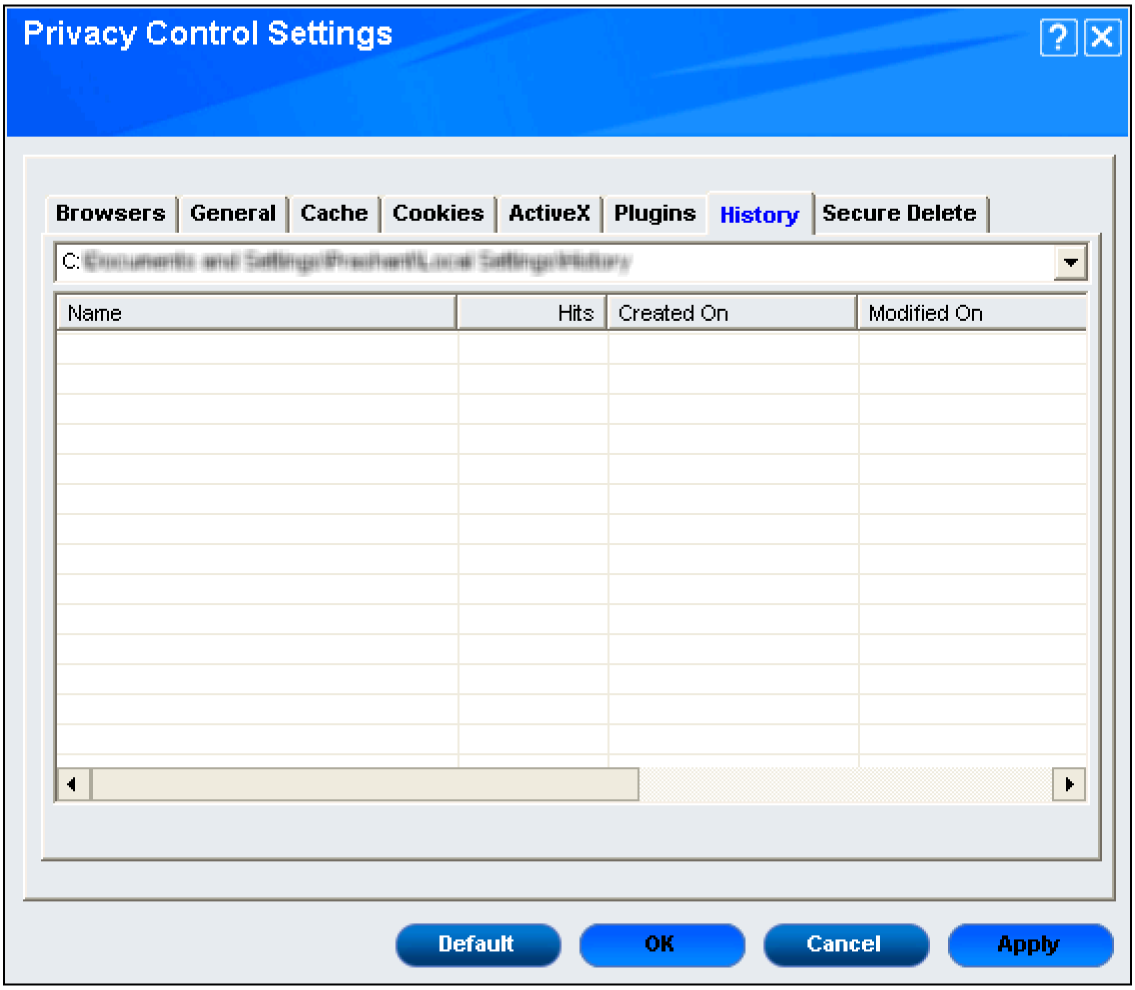
This tab displays all the Plugin details such as name, size, created date, modified date, storage path, and last accessed date.



Name	Size	Created On	Modified On

History

This tab displays History details such as name, hits, created date, modified date, storage path, and last accessed date.

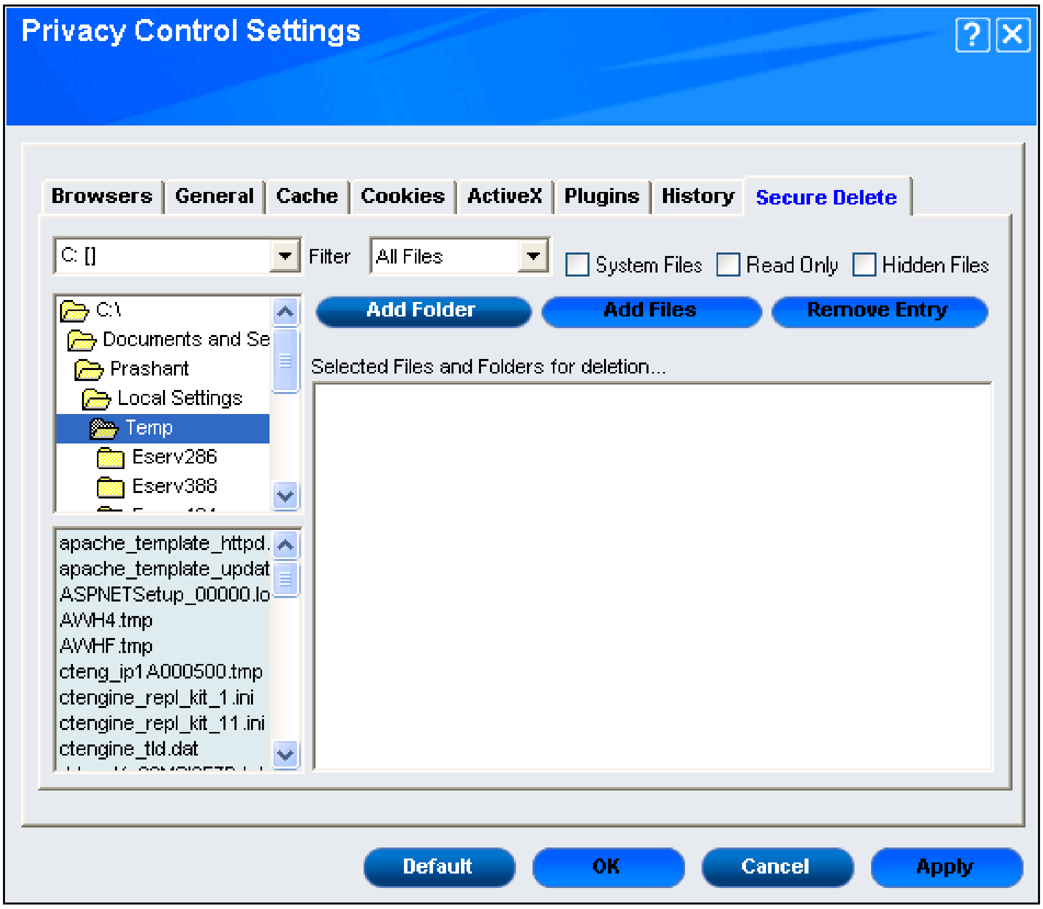


C:[redacted]

Name	Hits	Created On	Modified On

Secure Delete

This tab securely deletes files and folders present in the system. You can securely delete the added files and folders through **Add Files** and **Add Folders** button respectively. You can also remove the files and folder from **Select Files and Folders for deletion**, list using **Remove Entry** button. You can apply filter for selecting the files and folders. You can filter folders based on the drives available and files based on text files, executable, icon files, shell links, URLs, images.



C: []

Filter: All Files

□ System Files □ Read Only □ Hidden Files

C:\
Documents and Se
Prashant
Local Settings
Temp
Eserv286
Eserv388

apache_template_httpd.
apache_template_updat
ASPNETSetup_00000.lo
AVVH4.tmp
AVVHF.tmp
cteng_ip1A000500.tmp
ctengine_repl_kit_1.ini
ctengine_repl_kit_11.ini
ctengine_tld.dat

Selected Files and Folders for deletion...

It also provides filter according to the following entity:

- **System Files**: This check box displays all the files and folders of the system.
- **Read-only**: This check box displays only read-only files and folders.
- **Hidden Files**: This check box displays all the hidden files and folders in the system.

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

Default
Click this button to apply the default settings.

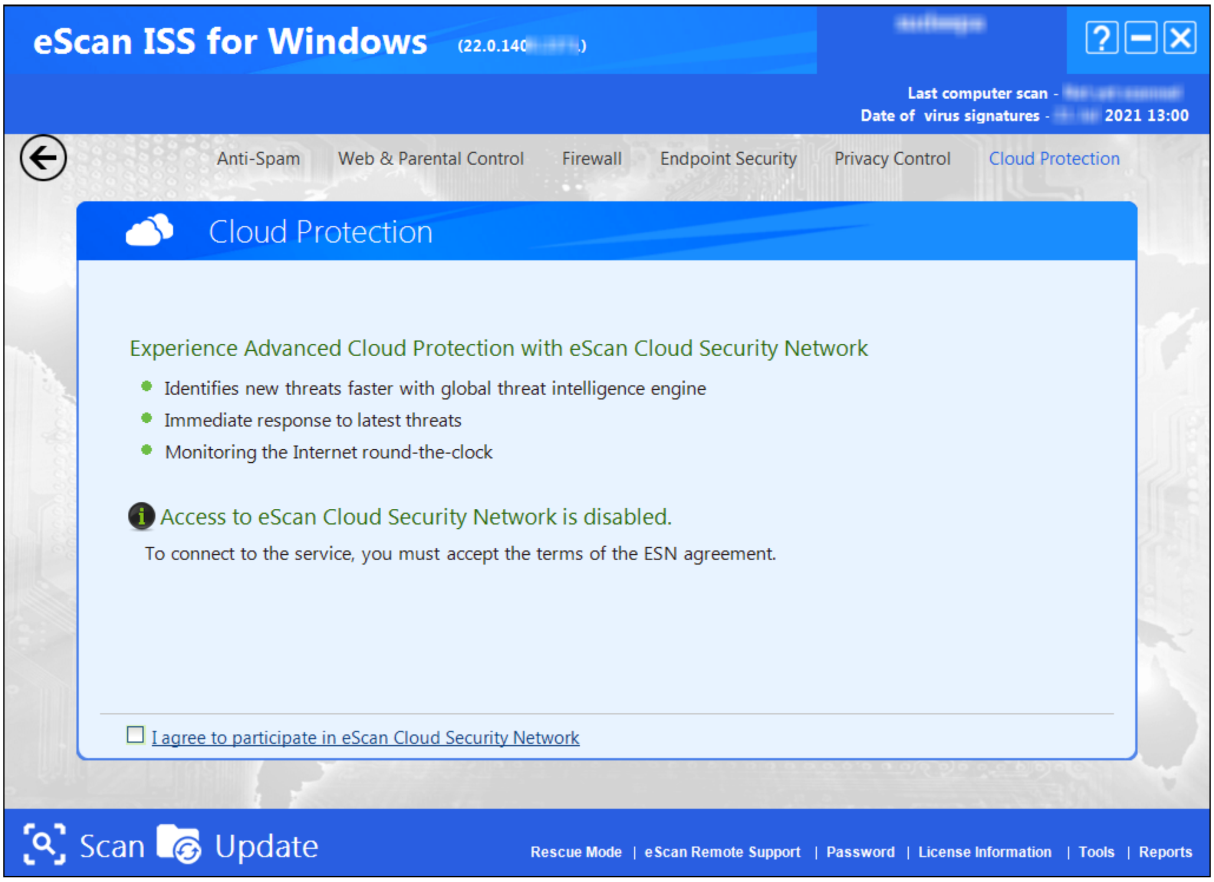
OK
Click this button after you click the Apply button to apply the configured settings.

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

Apply
Click this button to apply the configured settings.

Cloud Protection

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



eScan ISS for Windows (22.0.140[redacted])
[redacted]
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Privacy Control
Cloud Protection
Cloud Protection
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 13:00

Experience Advanced Cloud Protection with eScan Cloud Security Network

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

Access to eScan Cloud Security Network is disabled.

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

☐ I agree to participate in eScan Cloud Security Network

The following are the basics of cloud-based ESN:

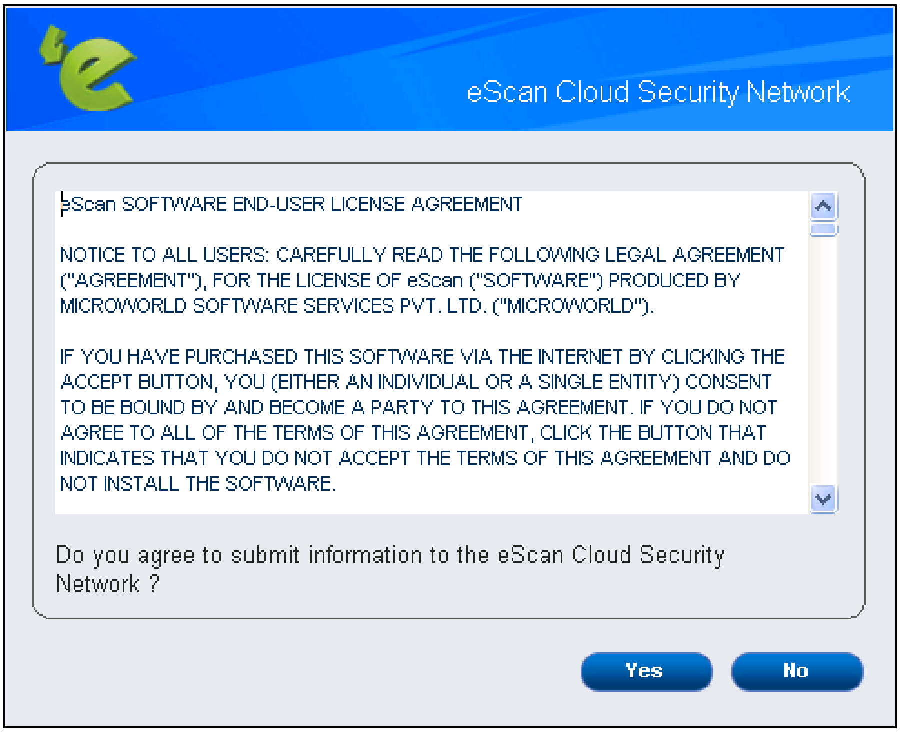
- Continuous global monitoring of real-life threats and immediate delivery of collected data to eScan host servers.
- Analysis of collected data and the creation of protection measures against new threats, and the fast distribution of those measures to users.
- ESN automatically collects information and sends the data to eScan labs. Information about suspicious files downloaded and executed on computers is also collected, regardless of their source, such as websites, email attachments, peer-to-peer networks, and so on.
  This is done strictly voluntarily and confidentially – the user of any one of eScan SOHO products has to agree to participate in the system. In any case, strict confidentiality is maintained and no personal information, such as user names, passwords, or any other personal details are collected.
  The decision on the safety of a program is made based on internal algorithms like the file is having a valid digital signature or not and number of other factors.

As soon as a program is declared malicious or unsafe, the information becomes available to eScan product users even before the signature for that piece of malware is created and updated on their computers.
Thus, eScan clients receive prompt information about new and unknown threats minutes after the launch of a cyber-attack, compared to hours for traditional signature database update.

NOTE	The Cloud Protection module is enabled, by default.

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

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



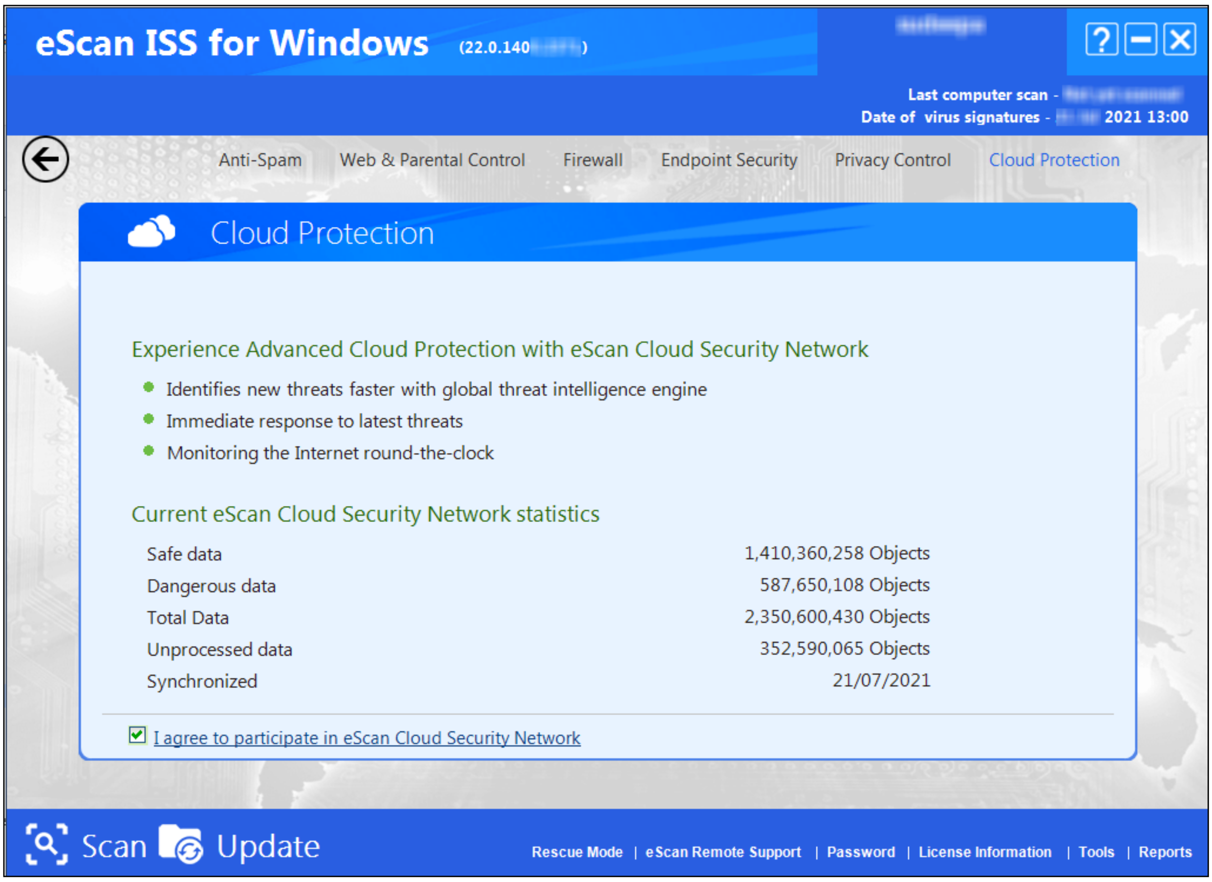
eScan SOFTWARE END-USER LICENSE AGREEMENT

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

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

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

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


eScan ISS for Windows (22.0.140[redacted])
[redacted]
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Privacy Control
Cloud Protection
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 13:00

Cloud Protection

Experience Advanced Cloud Protection with eScan Cloud Security Network

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

Current eScan Cloud Security Network statistics

Safe data	1,410,360,258 Objects
Dangerous data	587,650,108 Objects
Total Data	2,350,600,430 Objects
Unprocessed data	352,590,065 Objects
Synchronized	21/07/2021

☑ I agree to participate in eScan Cloud Security Network

Two-Factor Authentication

The system login password is Single-Factor Authentication which is considered unsecure as it may put your system's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your computer.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering Windows login credentials. So, even if somebody knows your login credentials, the 2FA feature secures data against unauthorized logins.

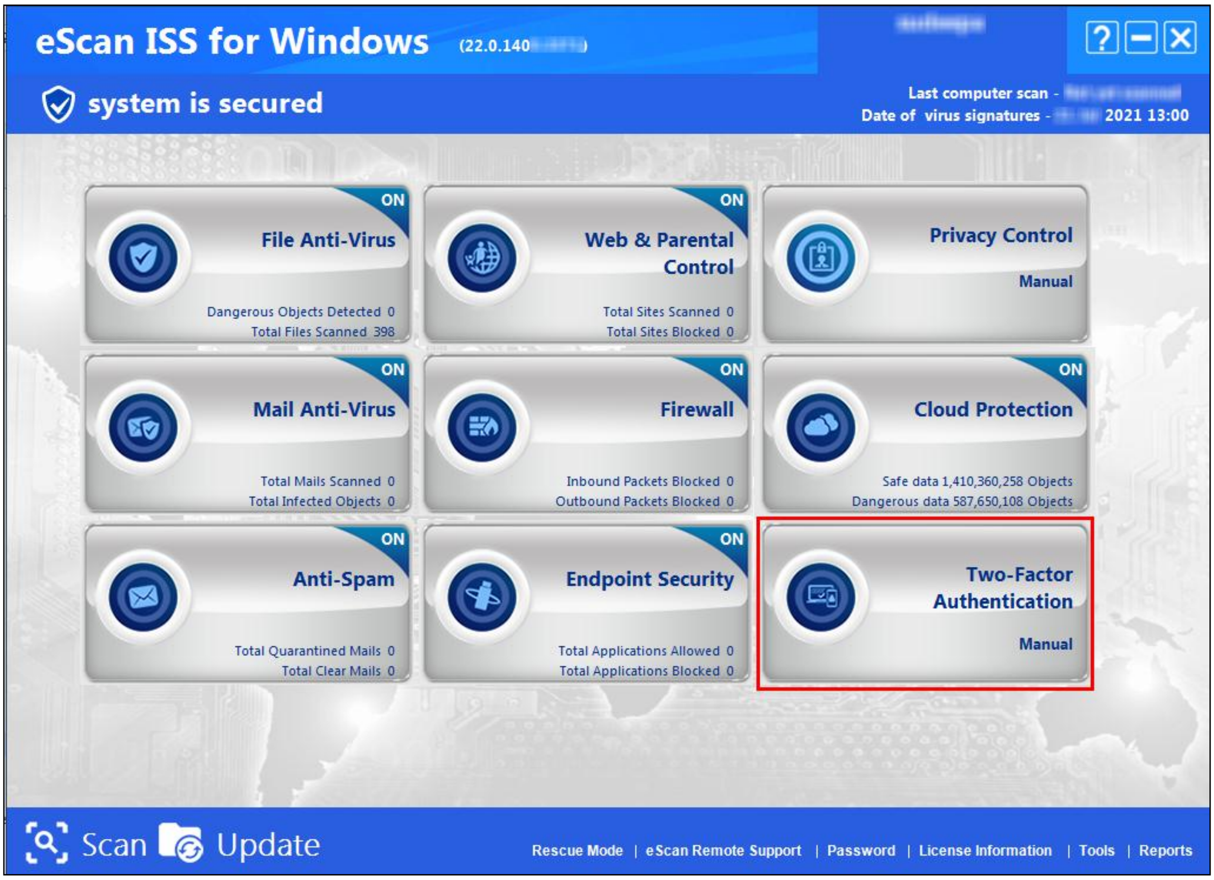
You can use various options to set password for the 2FA. You can set password or you can use the eScan administrator password in case the system is offline (without internet access). To use 2FA online authentication, you need to install the Authenticator app for Android devices from Play Store or for iOS devices from App Store on your smart device. The Authenticator app needs camera access for scanning a QR code in the Authenticator app.

NOTE	Ensure that the smart device's date and time matches with the system's date and time or else TOTPs generated by app won't get validated.

Enabling 2FA login

To enable 2FA login, follow the below steps:

1. Open eScan Protection Center,
   - From desktop, double-click the 🛡 icon.
   - From taskbar, right-click the 🛡 icon and click **Open eScan Protection Center**.



eScan ISS for Windows (22.0.140[redacted])

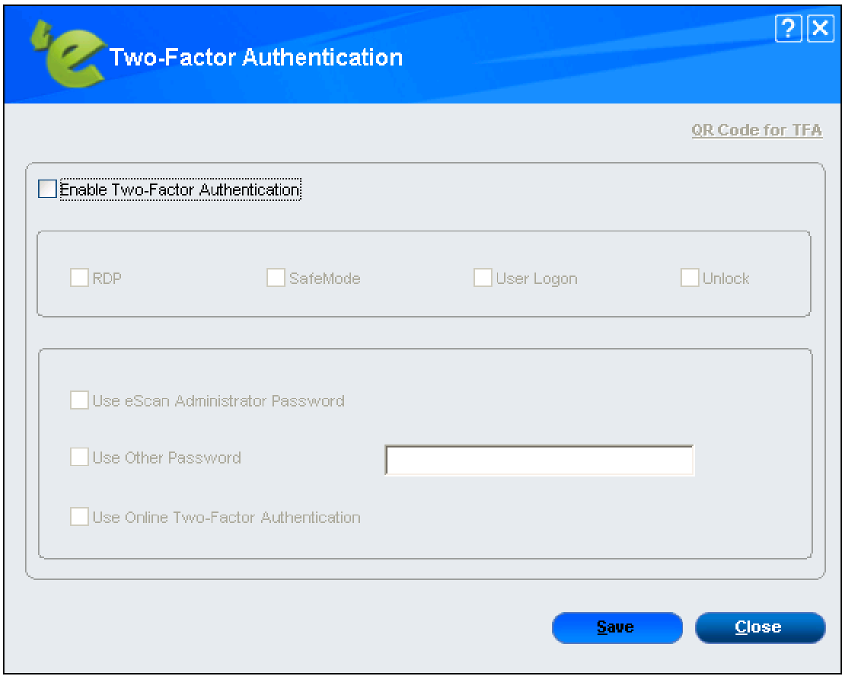
[redacted]

system is secured

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 13:00

?
ON
File Anti-Virus
Dangerous Objects Detected 0
Total Files Scanned 398
ON
Web & Parental Control
Total Sites Scanned 0
Total Sites Blocked 0
Privacy Control
Manual
ON
Mail Anti-Virus
Total Mails Scanned 0
Total Infected Objects 0
ON
Firewall
Inbound Packets Blocked 0
Outbound Packets Blocked 0
ON
Cloud Protection
Safe data 1,410,360,258 Objects
Dangerous data 587,650,108 Objects
ON
Anti-Spam
Total Quarantined Mails 0
Total Clear Mails 0
ON
Endpoint Security
Total Applications Allowed 0
Total Applications Blocked 0
Two-Factor Authentication
Manual
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

2. Click **Two-Factor Authentication**.



Two-Factor Authentication

QR Code for TFA

□ Enable Two-Factor Authentication

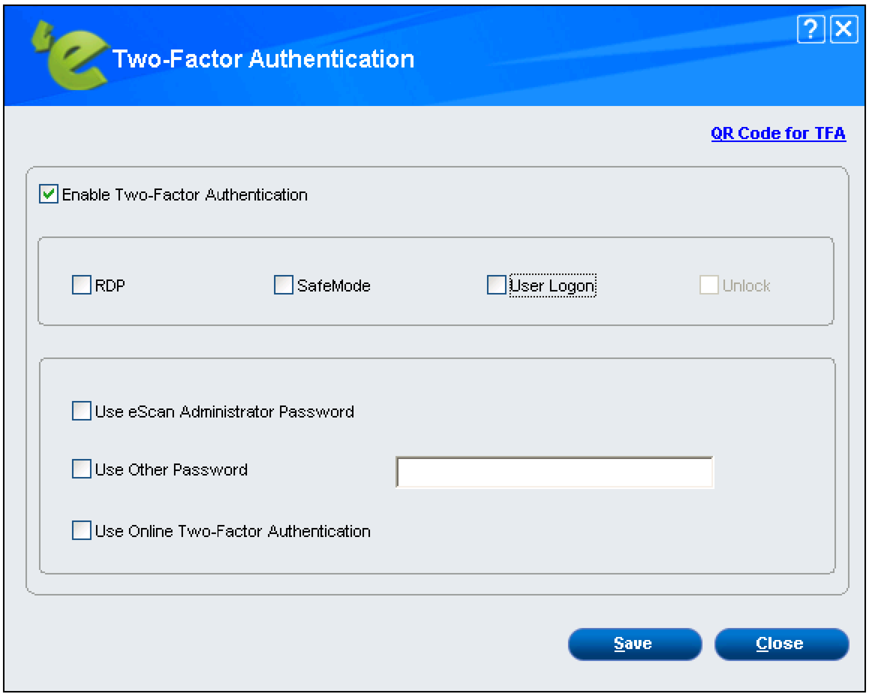
□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

3. Select **Enable Two-Factor Authentication**. This will enable the other configuration settings.



Two-Factor Authentication

QR Code for TFA

☑ Enable Two-Factor Authentication

□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

NOTE	**Unlock** option will be enabled only after selecting **User Logon** option.

4. You can configure it according to your requirement and click **Save**.
   The 2FA will work according to the configuration.

Login Scenarios

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

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

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

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

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

Password Types

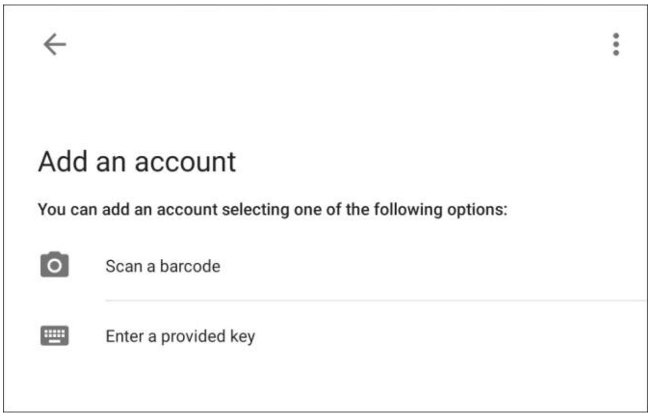
You can use following password types to log in:

Use eScan Administrator Password
You can use the existing eScan Administrator password for 2FA login.

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

Use Online Two-Factor Authentication
To use Online 2FA authentication, follow the steps given below:

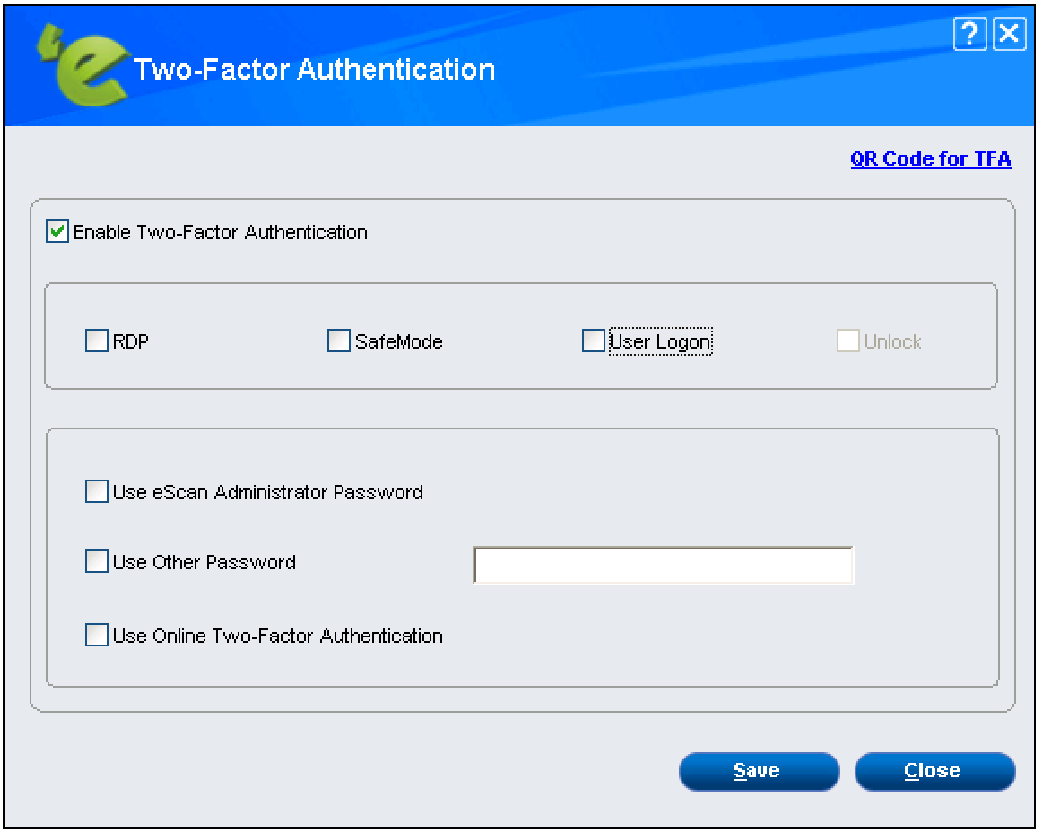
1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
2. Open the Authenticator app and tap **Scan a barcode**.



Add an account

You can add an account selecting one of the following options:

3. Now, open **eScan Protection Center** on your system and click **Two-Factor Authentication**.
4. Select **Enable Two-Factor Authentication** checkbox.



Two-Factor Authentication

QR Code for TFA

☑ Enable Two-Factor Authentication

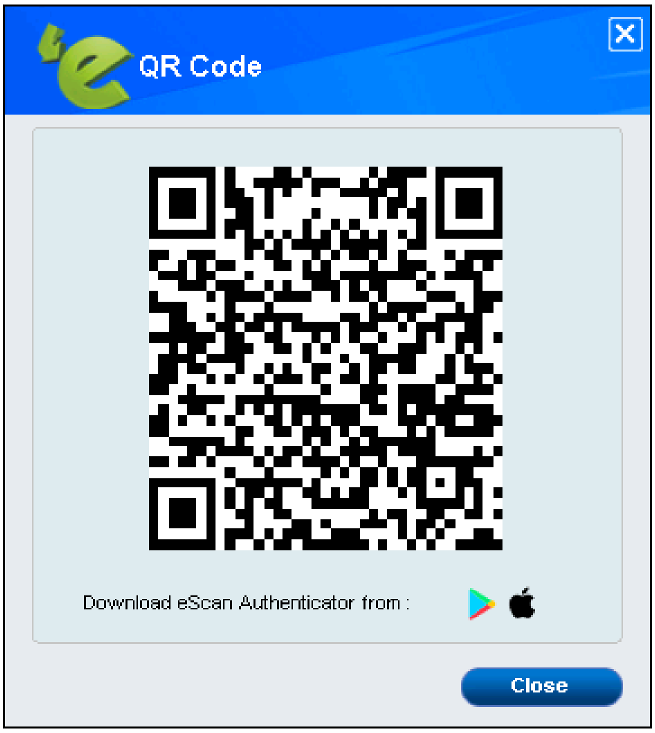
□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

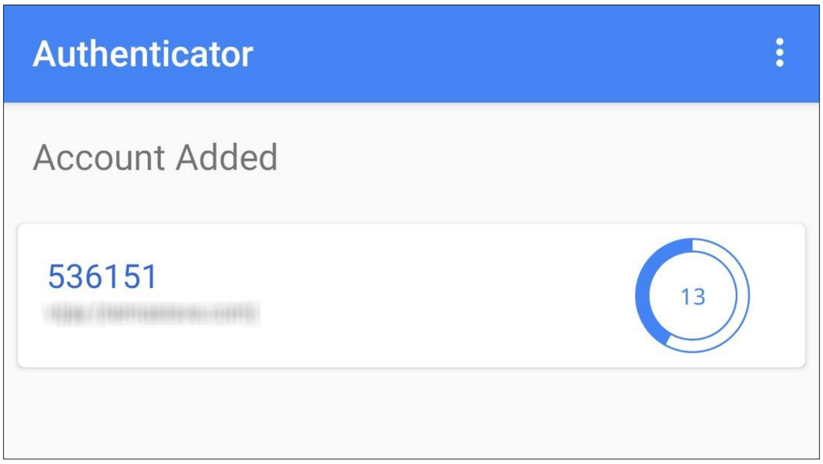
5. Configure the login scenarios according to your need and select **Use Online Two-Factor Authentication.**
6. On the top right corner, click **QR Code for TFA**.
   A QR code appears.



QR Code

Download eScan Authenticator from :

7. Scan the onscreen QR code via the Authenticator app.
   A Time-based One-Time Password (TOTP) appears on smart device.



Authenticator

Account Added

536151

8. You can use this TOTP for login. This TOTP will get updated after every 30 seconds.

Disabling 2FA login

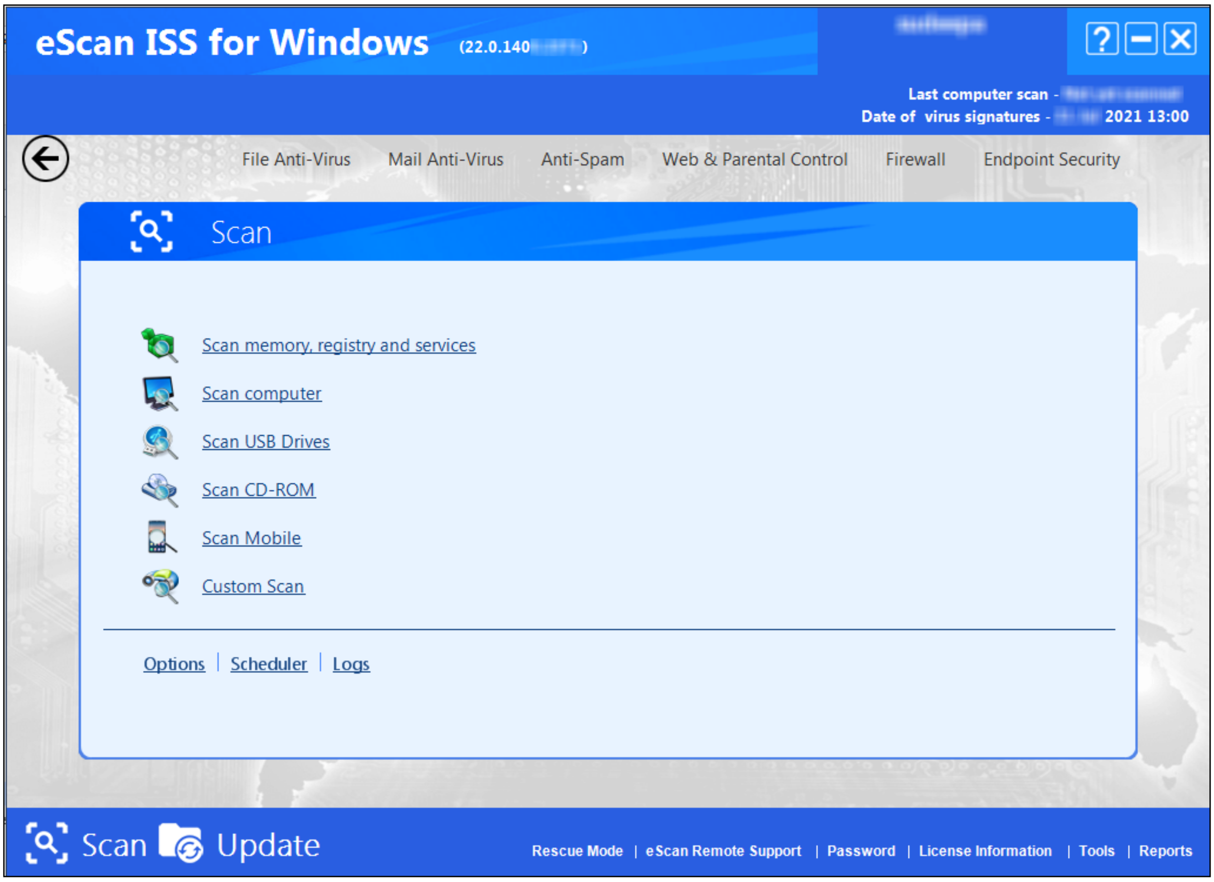
To disable the 2FA login, follow the below steps:

1. Open **eScan Protection Center** > **Two-Factor Authentication**.
2. Uncheck the **Enable Two-Factor Authentication** option.
3. Click **Save**.

The 2FA feature gets disabled.

Scan

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


eScan ISS for Windows (22.0.140[redacted])
[redacted]
Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 13:00
File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Scan
Scan memory, registry and services
Scan computer
Scan USB Drives
Scan CD-ROM
Scan Mobile
Custom Scan
Options | Scheduler | Logs
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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

Scan memory, registry and services

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

Scan computer

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

Scan USB Drives

This option scans USB drives attached to your system.

Scan CD-ROM

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

Scan Mobile

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

Custom Scan

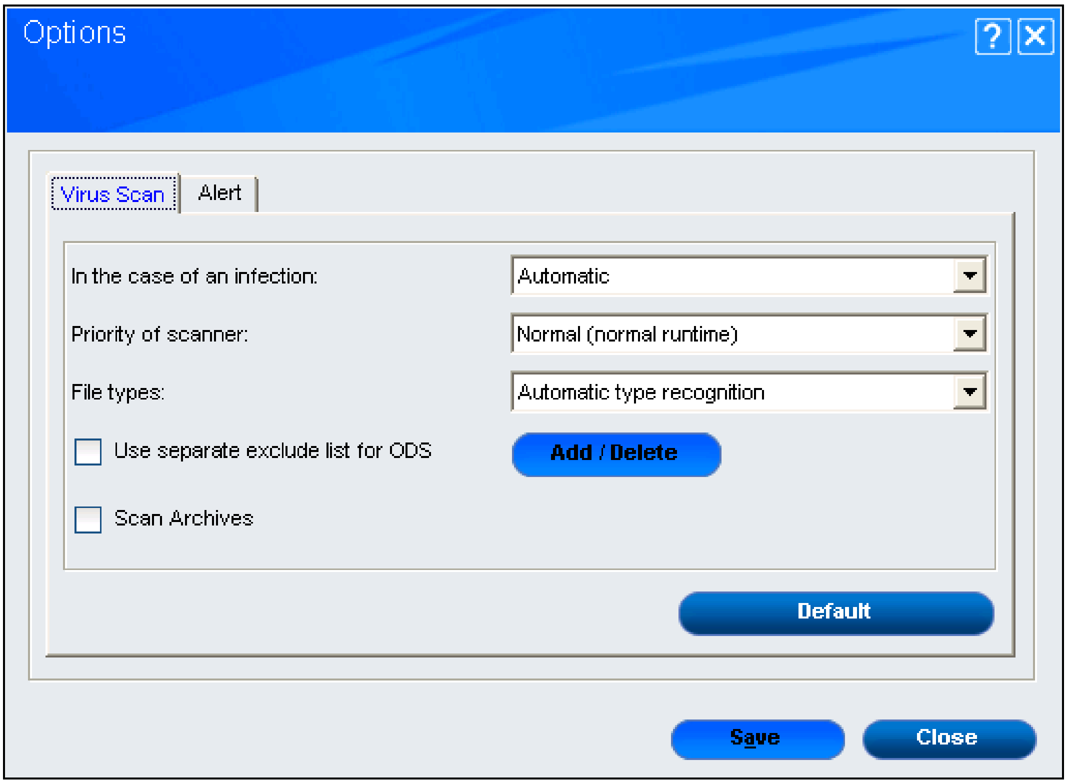
This option helps you to configure the scan according to the specific need of the users.

Options

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

Virus Scan

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

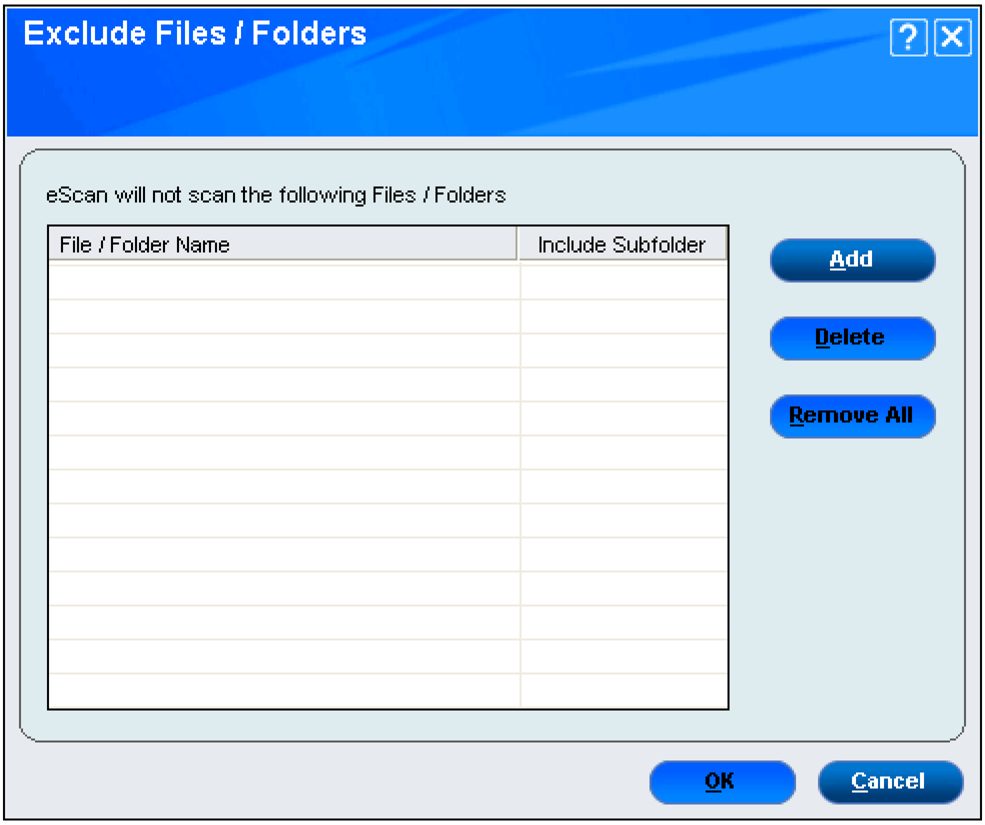


In the case of an infection: Automatic
Priority of scanner: Normal (normal runtime)
File types: Automatic type recognition
□ Use separate exclude list for ODS
□ Scan Archives

This tab has following options to configure your scan:

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

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



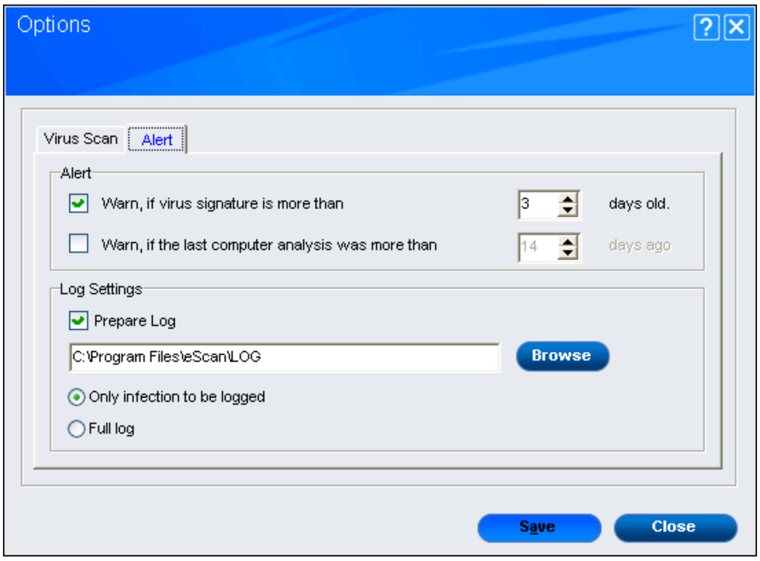
On the **Exclude Folders** dialogue box, you will find following buttons:

  - **Add**: This button will give you a popup window called **Add to Exclude List** and click an appropriate object type such as **File** or **Folder**, and then type or click **Browse** button to select the file or folder that you want to exclude. If you want to include sub folder of a folder, select **Include Subfolder** check box. Then click on the **Add** button.
  - **Delete**: This button deletes any file/folder from the list.
  - **Remove All**: This button removes all the files/folders from the list.

- **Scan Archives:** This check box scans both archived and packed files.
- **Default**: This button resets the entire scan configuration to default settings.

Alert

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



Alert

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

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

Log Settings

☑ Prepare Log

C:\Program Files\eScan\LOG

● Only infection to be logged

○ Full log

This tab has following options to configure the setting:

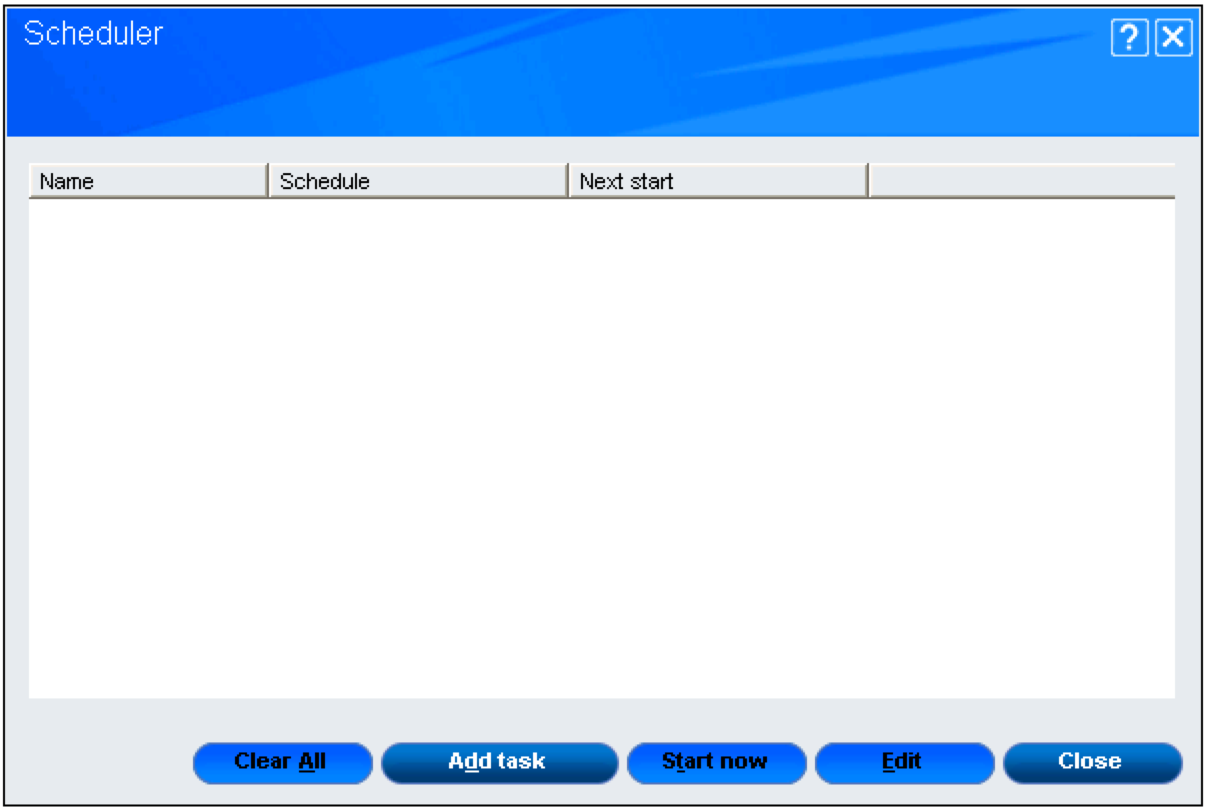
- **Alert:** In this section, you can configure the notification displayed when the virus definitions are outdated or when a specified number of days have elapsed since you have last scanned your computer. This section gives you following sub-options:
  - **Warn, if virus signature is more than:** This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

Both the tabs have 2 common buttons:

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

Scheduler

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



We can configure the following options:

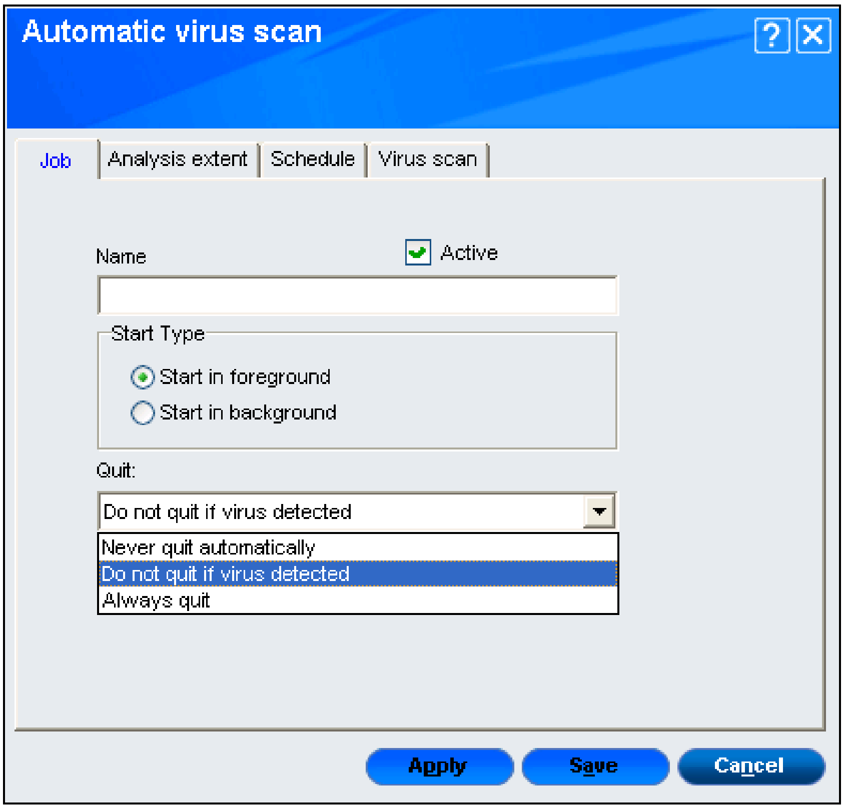
- **Add task**: To learn more, click here.
- **Clear All**: This option will clear all the task from the list.
- **Start now**: Once you select the task from the list, you can use this button to start the scanning.
- **Edit**: This option will allow you to edit the existing task from the list.
- **Close**: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

Adding a task

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

Job

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



Name ☑ Active

Start Type

● Start in foreground

○ Start in background

Quit:

Do not quit if virus detected

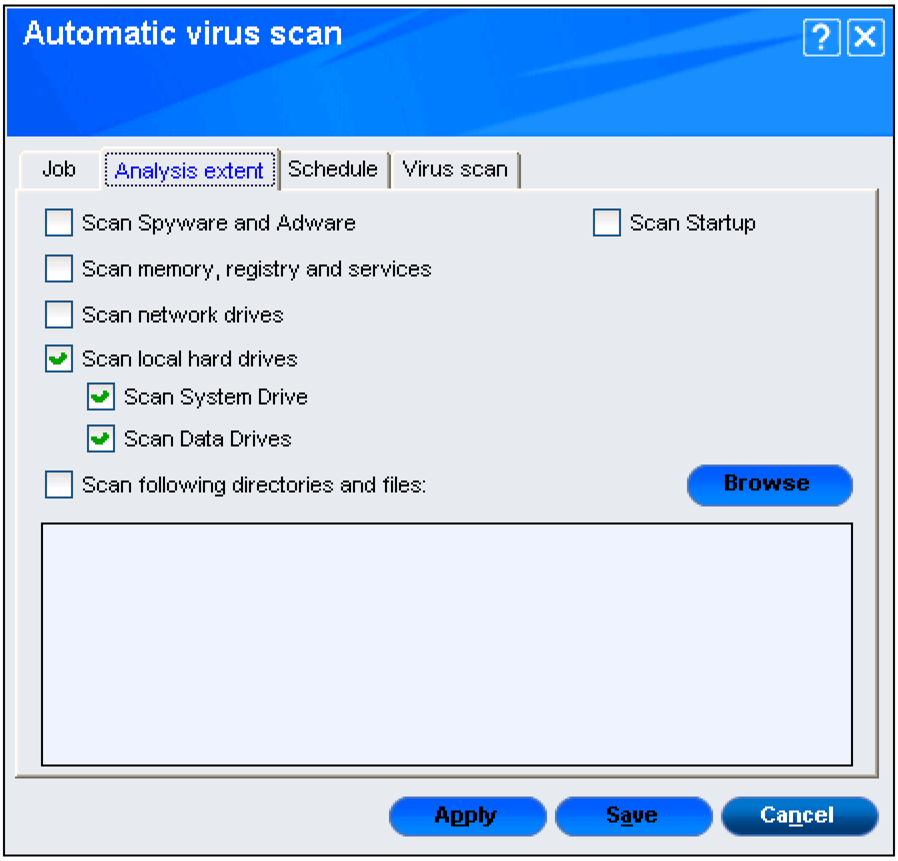
Never quit automatically
Do not quit if virus detected
Always quit

Specify the following details:

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

Analysis extent

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



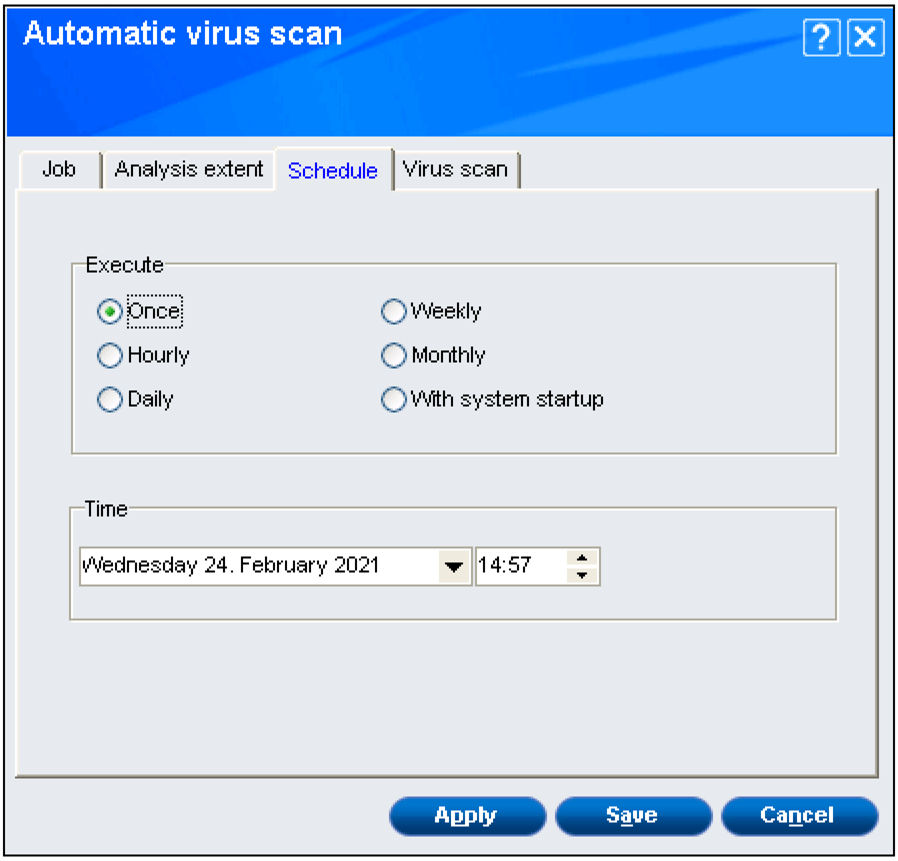
□ Scan Spyware and Adware
□ Scan Startup
□ Scan memory, registry and services
□ Scan network drives
☑ Scan local hard drives
☑ Scan System Drive
☑ Scan Data Drives
□ Scan following directories and files:

This has following options to configure:

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

Schedule

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



Execute

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

Time

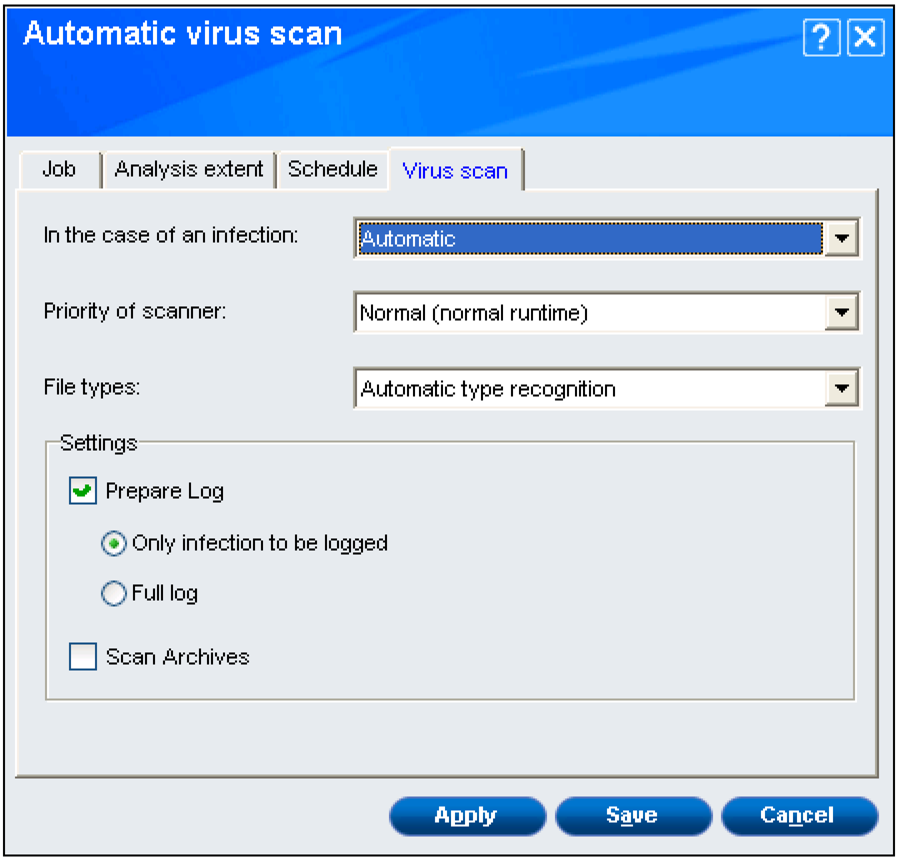
Wednesday 24. February 2021 14:57

It has following options to configure:

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

Virus scan

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



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

To learn more, click here.

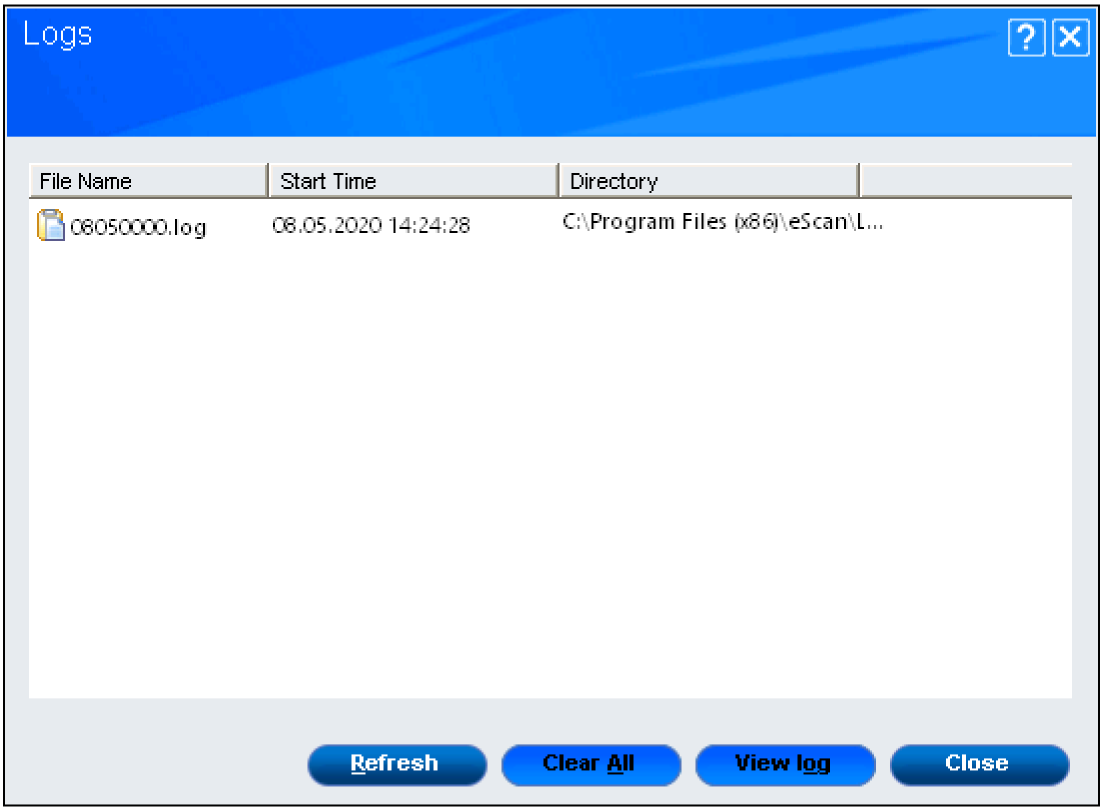
Apply: Click on this button, to apply the configured settings.

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

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

Logs

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



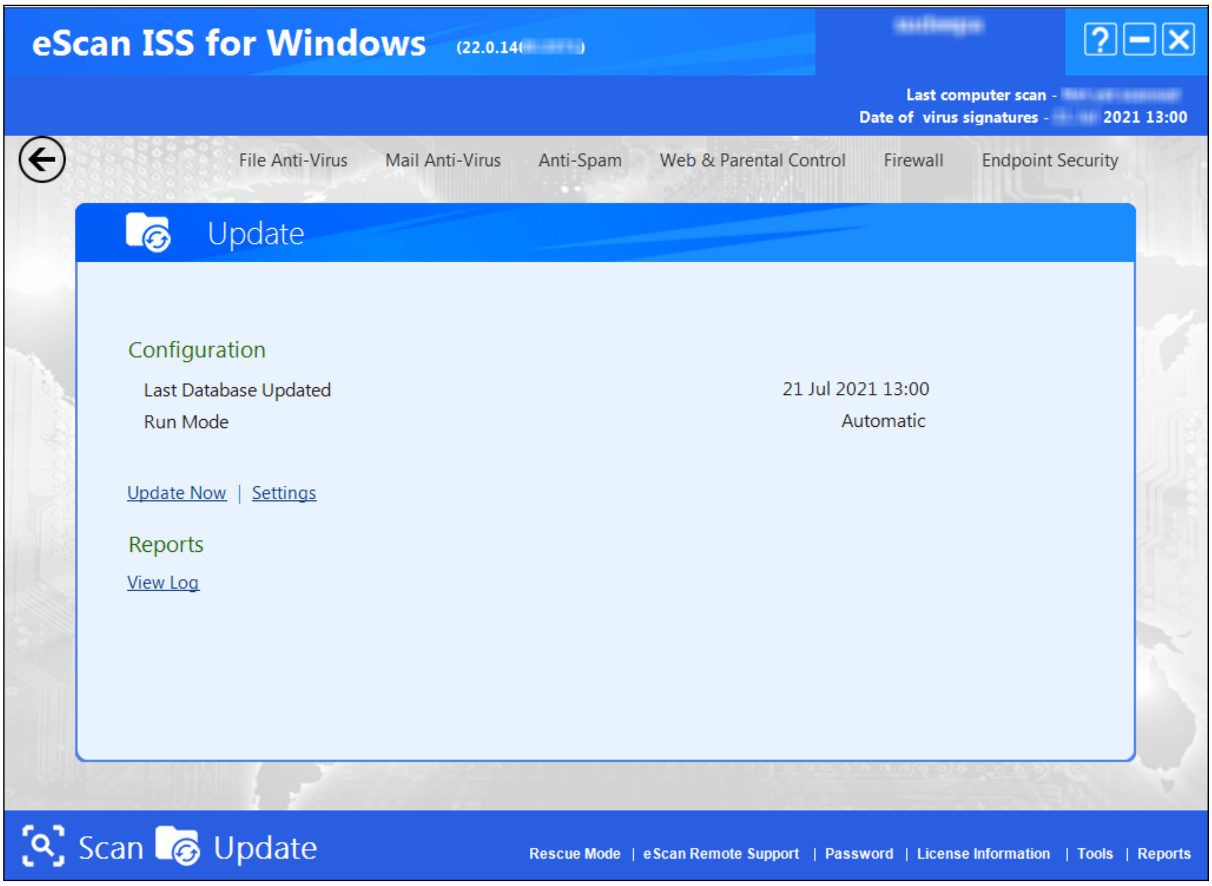
File Name	Start Time	Directory
08050000.log	08.05.2020 14:24:28	C:\Program Files (x86)\eScan\L...

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

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

Update

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



eScan ISS for Windows (22.0.14[redacted])

[redacted]

Last computer scan - [redacted]
Date of virus signatures - [redacted] 2021 13:00

Update

Configuration

Last Database Updated	21 Jul 2021 13:00
Run Mode	Automatic

Update Now | Settings

Reports

View Log

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

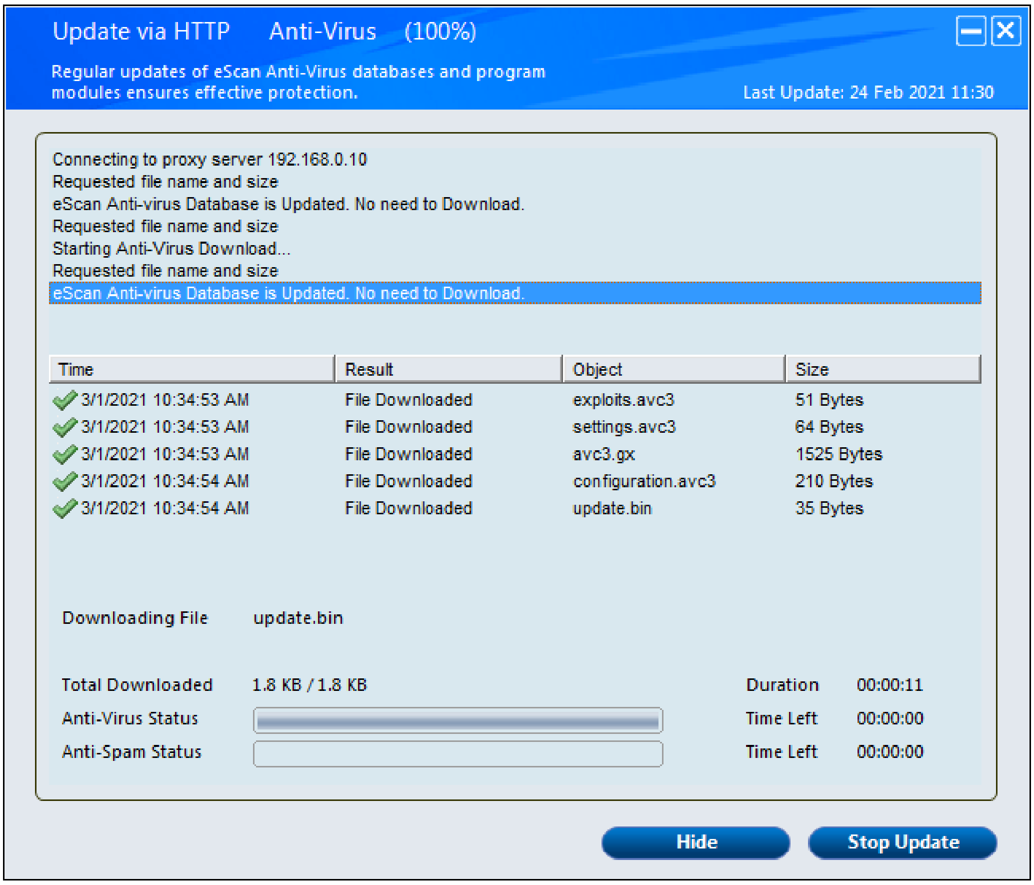
You can access tabbed page for the Update module by clicking the **Update** button. The update tabbed page provides you with information regarding the type of update mode and date on which the database was last updated. It also provides you with options for configuring the module and helps you to view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

You can configure the following sections through this module.

Configuration

This section displays the following information:

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



Update via HTTP Anti-Virus (100%)

Regular updates of eScan Anti-Virus databases and program modules ensures effective protection.

Last Update: 24 Feb 2021 11:30

```
Connecting to proxy server 192.168.0.10
Requested file name and size
eScan Anti-virus Database is Updated. No need to Download.
Requested file name and size
Starting Anti-Virus Download...
Requested file name and size
eScan Anti-virus Database is Updated. No need to Download.
```

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

Downloading File update.bin

Total Downloaded 1.8 KB / 1.8 KB

Duration 00:00:11

Anti-Virus Status

Time Left 00:00:00

Anti-Spam Status

Time Left 00:00:00

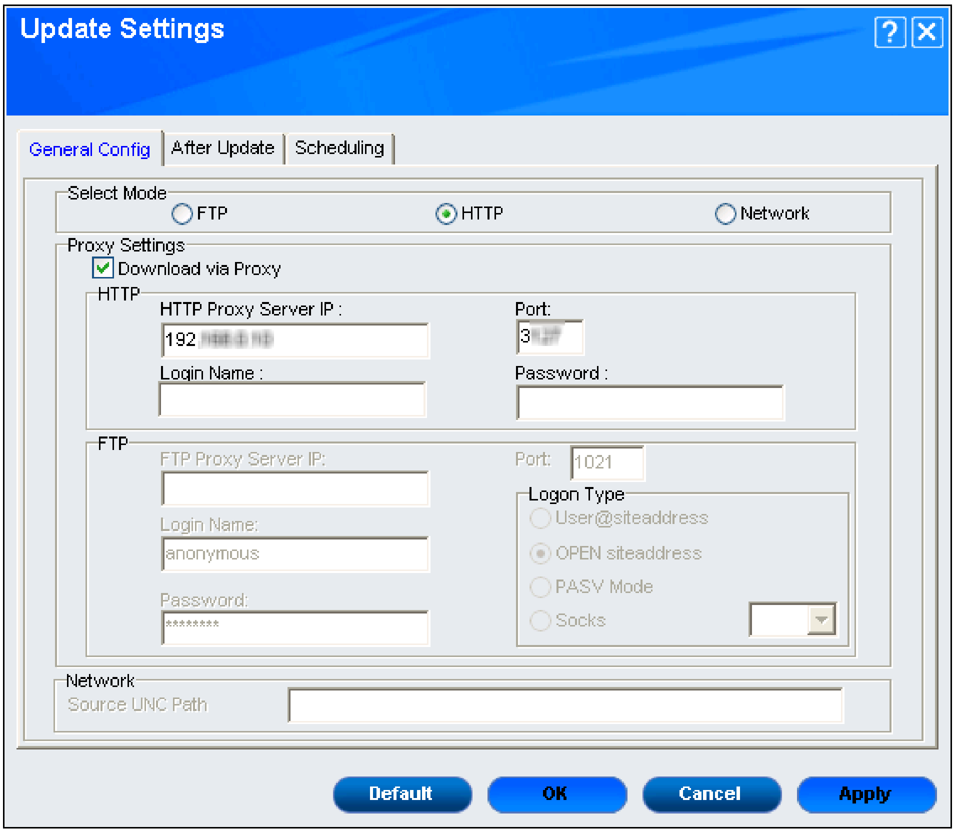
- **Settings**: To learn more, click here.

Settings

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

General Config

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



Update Settings

General Config | After Update | Scheduling

Select Mode
○ FTP ● HTTP ○ Network

Proxy Settings
☑ Download via Proxy

HTTP
HTTP Proxy Server IP : 192 [redacted]
Port: 3[redacted]
Login Name :
Password :

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

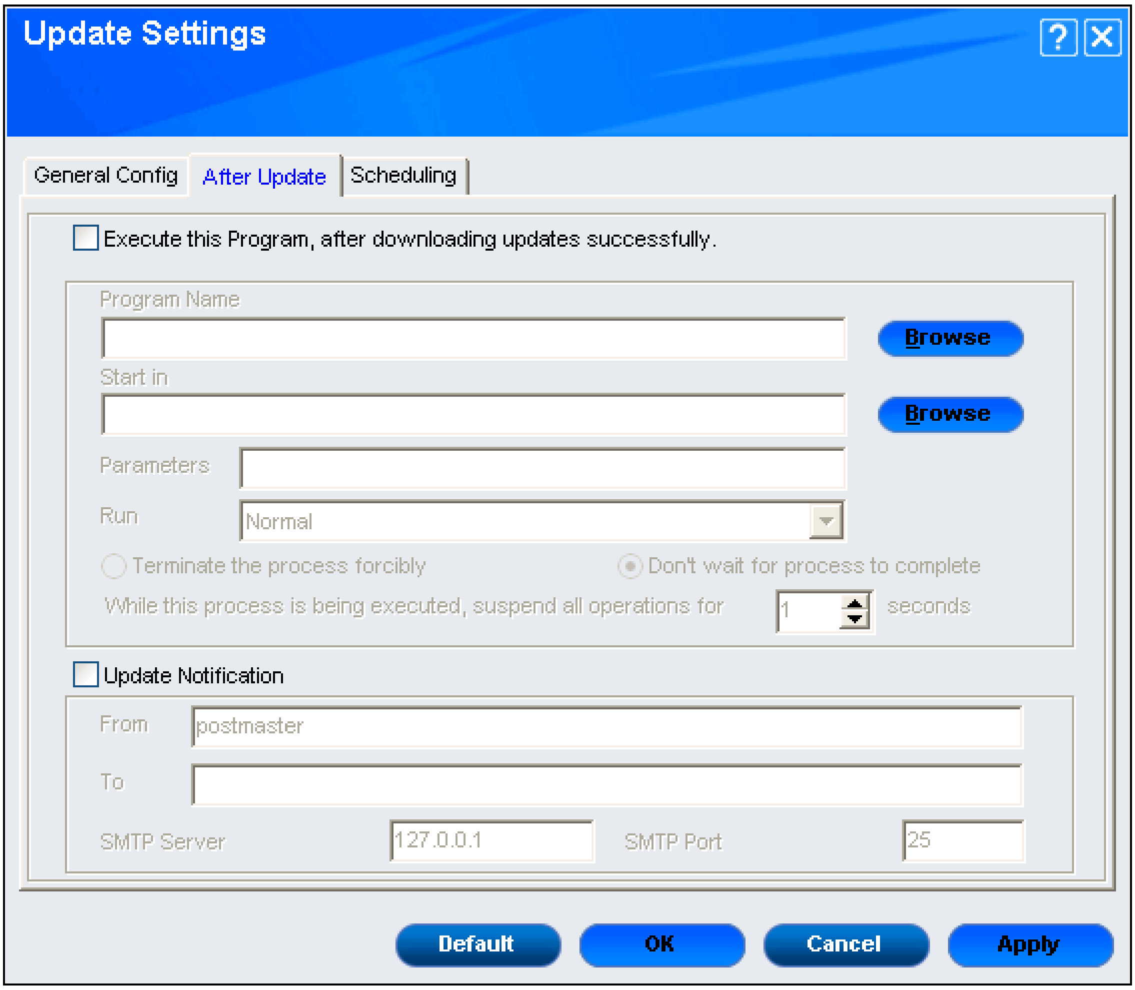
Network
Source UNC Path

It consists of following options to configure:

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

After Update

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



☐ Execute this Program, after downloading updates successfully.

Program Name

Start in

Parameters

Run: Normal

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

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

☐ Update Notification

From: postmaster

To

SMTP Server: 127.0.0.1 SMTP Port: 25

You can configure the following options:

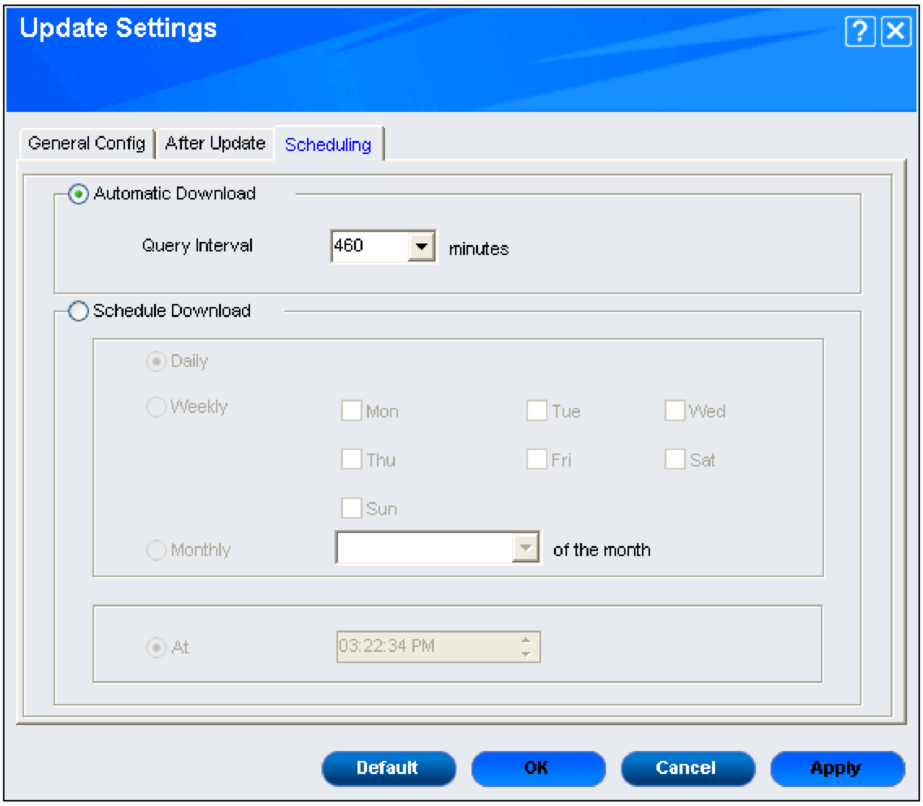
- **Execute this Program, after downloading updates successfully:** When you select this check box, eScan runs a particular application or program after eScan updates are downloaded successfully.
  This section has the following options and will be enabled once you select **Execute this Program, after downloading updates successfully** check box:
  - **Program Name:** Sometimes, you may need a particular program to run after you have downloaded updates for eScan. You can simply specify the path of the program in the **Program Name** box. Alternatively, you can use the **Browse** button to navigate to the path where the program executable is stored.
  - **Start In:** You can also specify the program to execute from a given location. You can either specify the location in the **Start In** box or use the **Browse** button to navigate to the folder where the program should execute.
  - **Parameters:** Some programs require additional parameters to execute. You can specify these start parameters in the **Parameters** box.

- **Run:** The default mode is normal mode. Whenever a program runs, it runs in its own window. You can specify whether the window should be in the maximized, minimized, normal, or hidden state. The default state of the window is normal.
- **Terminate the process forcibly:** You can also forcibly terminate the process to free system resources by selecting this option.
- **Don't wait for process to complete:** A process may require a long time to end. In such cases, you can allow other processes to run along with the specified process by selecting this option.
- **While this process is being executed, suspend all operations for <placeholder> seconds:** The default value is 1. You can also ensure that the no other process runs while the specified process is running for a given time interval by setting the interval in the box.

- **Update Notification:** When you select this option, eScan sends an email notification to the email address specified in the **To** box in the **Update Notification** section.
  - **From:** The default email address provided is escanuser@escanav.com. You can specify the sender's email address in the notification mail in this box.
  - **To:** You can specify the recipient's email address in the notification mail in this box.
  - **SMTP Server:** The default IP set is 127:0:0:1. You can specify the IP address of the SMTP server in this box.
  - **SMTP Port:** The default port set is 25. You can specify the port number of the SMTP port in this box.

Scheduling

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



Update Settings

● Automatic Download

Query Interval: 460 minutes

○ Schedule Download

● Daily

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

○ Monthly: of the month

● At: 03:22:34 PM

It has following options:

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

All the tabs have 4 common buttons:

Default
This button reset the configuration.

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

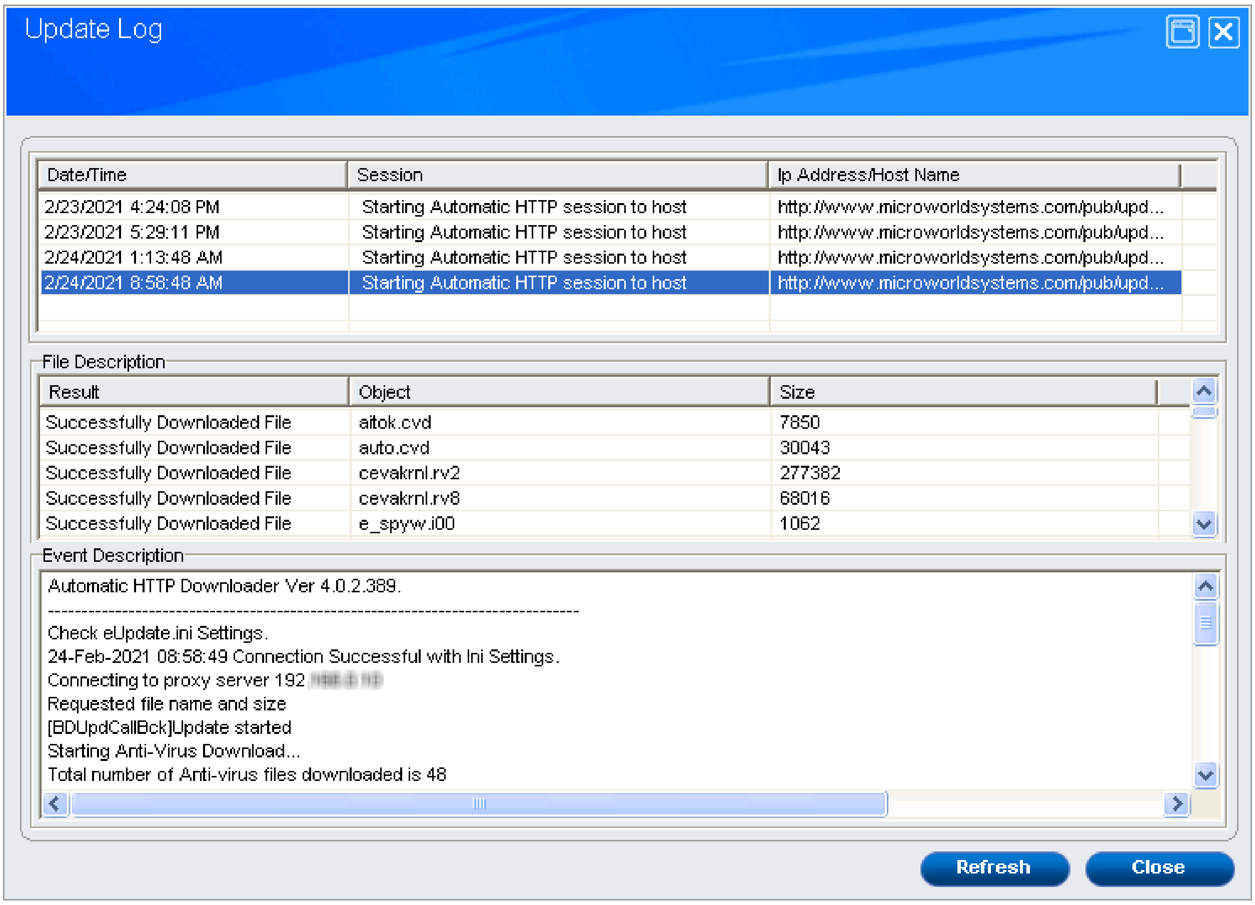
Cancel
This button closes the popup window without applying the configuration.

Apply
This button applies the changes in the configurations.

Reports

This section displays the following information:

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



Update Log

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

File Description

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

Event Description

```
Automatic HTTP Downloader Ver 4.0.2.389.
--------------------------------------------------------------------------------
Check eUpdate.ini Settings.
24-Feb-2021 08:58:49 Connection Successful with Ini Settings.
Connecting to proxy server 192 [redacted]
Requested file name and size
[BDUpdCallBck]Update started
Starting Anti-Virus Download...
Total number of Anti-virus files downloaded is 48
```

This report includes the following information:

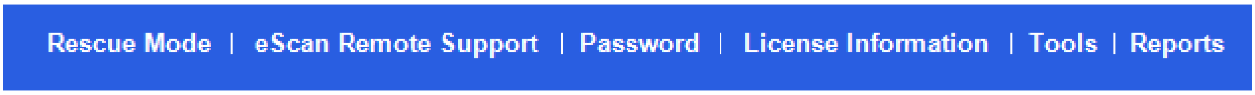
- The timestamp, session description, and host name or IP address.
- The description of file, such as result of the download, name of the object, and its size.
- The description of event, such as the number of files downloaded, time at which the connection was established or terminated, and the errors,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

This window has 2 buttons:

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

Quick Access Links

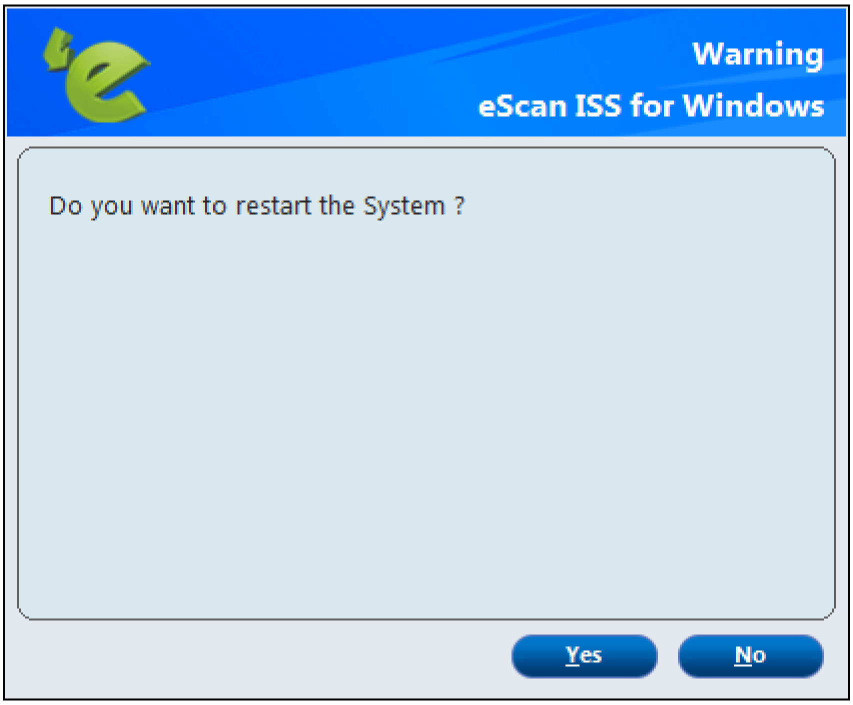
On lower-right corner of the screen, you can view the following quick access links:



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

Rescue Mode

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



Warning

eScan ISS for Windows

Do you want to restart the System ?

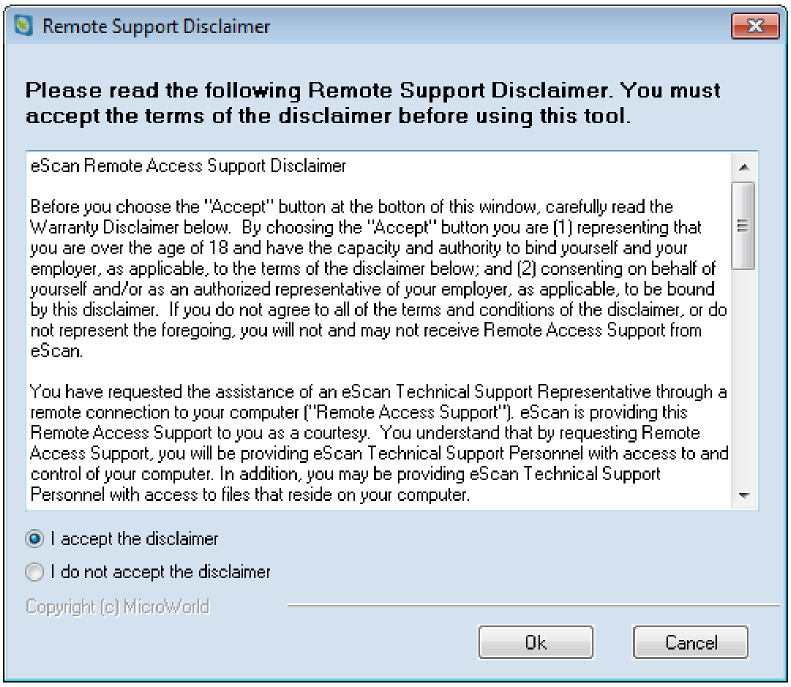
It allows you to boot into a secure environment during system startup without using any optical media. It uses Windows as well as Linux -based environment that not only helps you to scan and clean the system but also allows you to fix registry changes made by viruses and rootkits.

eScan Remote Support

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

Steps for availing remote support:

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



Remote Support Disclaimer

Please read the following Remote Support Disclaimer. You must accept the terms of the disclaimer before using this tool.

eScan Remote Access Support Disclaimer

Before you choose the "Accept" button at the botton of this window, carefully read the Warranty Disclaimer below. By choosing the "Accept" button you are (1) representing that you are over the age of 18 and have the capacity and authority to bind yourself and your employer, as applicable, to the terms of the disclaimer below; and (2) consenting on behalf of yourself and/or as an authorized representative of your employer, as applicable, to be bound by this disclaimer. If you do not agree to all of the terms and conditions of the disclaimer, or do not represent the foregoing, you will not and may not receive Remote Access Support from eScan.

You have requested the assistance of an eScan Technical Support Representative through a remote connection to your computer ("Remote Access Support"). eScan is providing this Remote Access Support to you as a courtesy. You understand that by requesting Remote Access Support, you will be providing eScan Technical Support Personnel with access to and control of your computer. In addition, you may be providing eScan Technical Support Personnel with access to files that reside on your computer.

● I accept the disclaimer

○ I do not accept the disclaimer

Copyright (c) MicroWorld

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

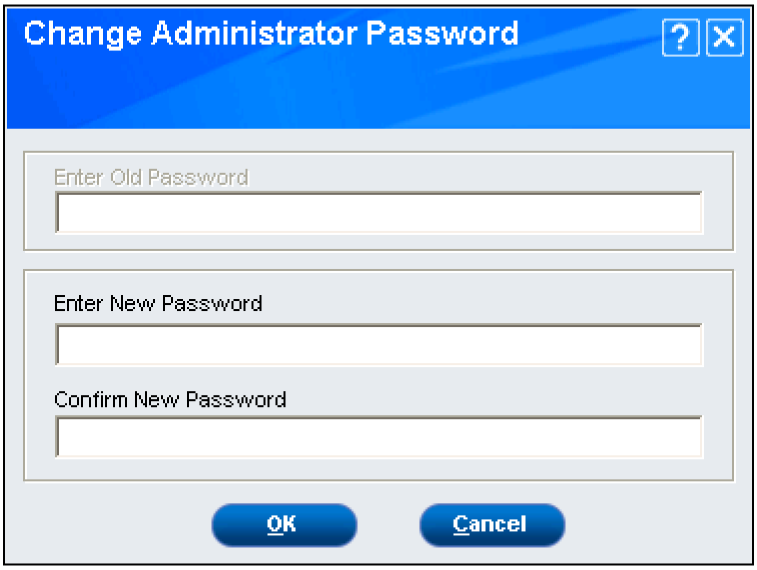
Password

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

Using Password Protection for opening eScan

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

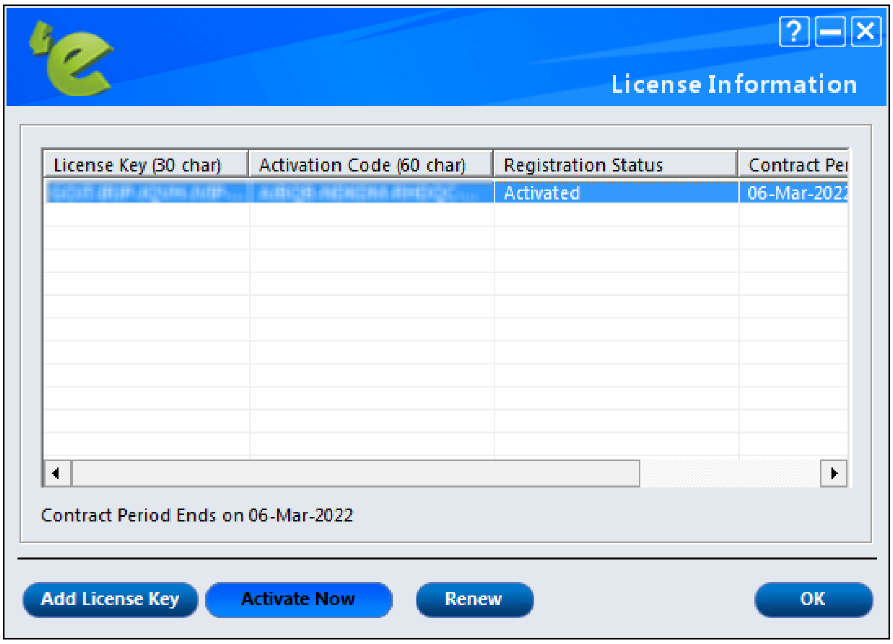
1. Open eScan Window.
2. Click **Password** link at the bottom of the interface.
3. Type a Password in the **Enter New Password** field. It is recommended to enter alphanumeric password.
4. Re-enter the Password in **Confirm New Password** field and click **OK**. You will have to enter this password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



NOTE	For removing the password, Click the password link and Enter 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.

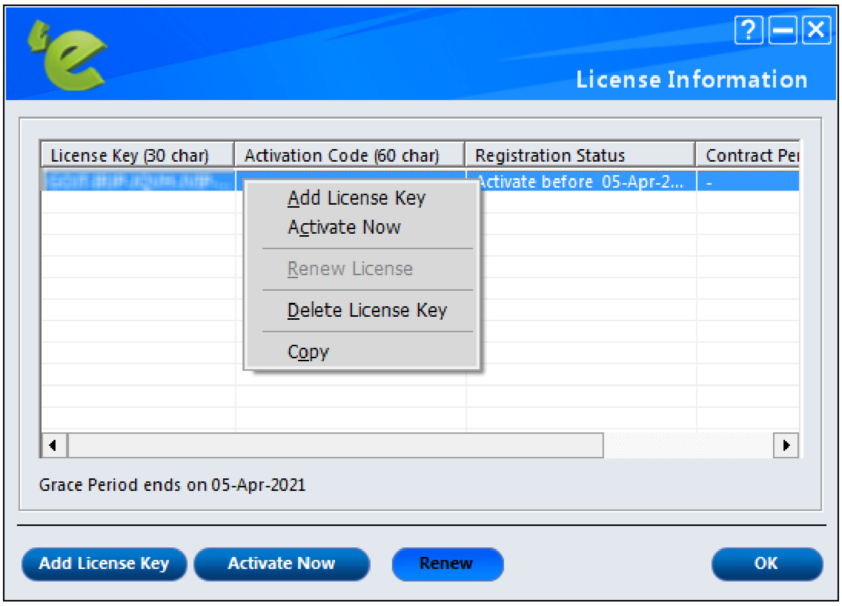


License Key (30 char)	Activation Code (60 char)	Registration Status	Contract Per
[redacted]	[redacted]	Activated	06-Mar-2022

Contract Period Ends on 06-Mar-2022

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

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



License Information

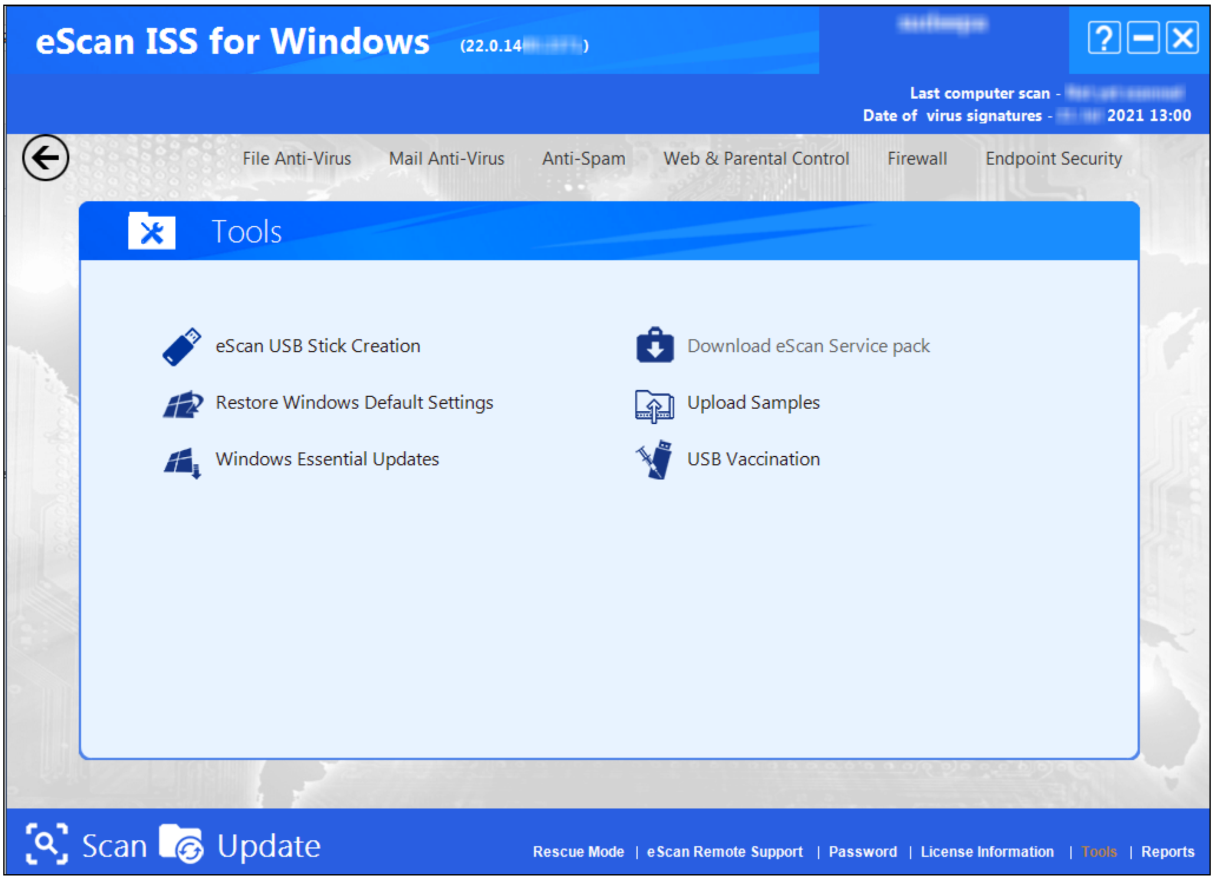
License Key (30 char)	Activation Code (60 char)	Registration Status	Contract Pe
[redacted]		Activate before 05-Apr-2...	-

Grace Period ends on 05-Apr-2021

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

Tools

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

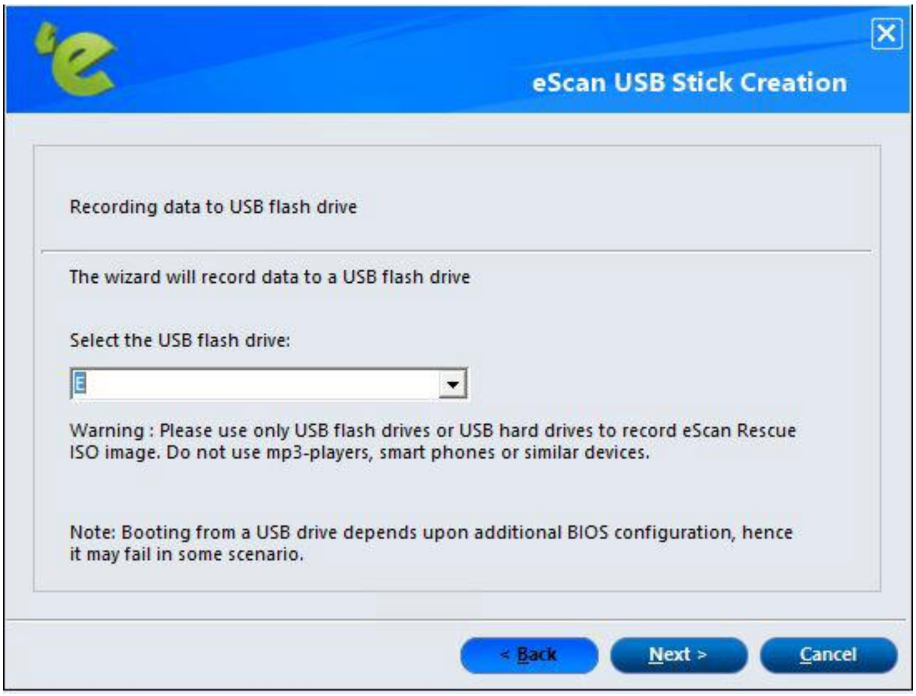


eScan ISS for Windows (22.0.14
Last computer scan -
Date of virus signatures - 2021 13:00
File Anti-Virus
Mail Anti-Virus
Anti-Spam
Web & Parental Control
Firewall
Endpoint Security
Tools
eScan USB Stick Creation
Restore Windows Default Settings
Windows Essential Updates
Download eScan Service pack
Upload Samples
USB Vaccination
Scan
Update
Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

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

eScan USB Stick Creation

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



eScan USB Stick Creation

Recording data to USB flash drive

The wizard will record data to a USB flash drive

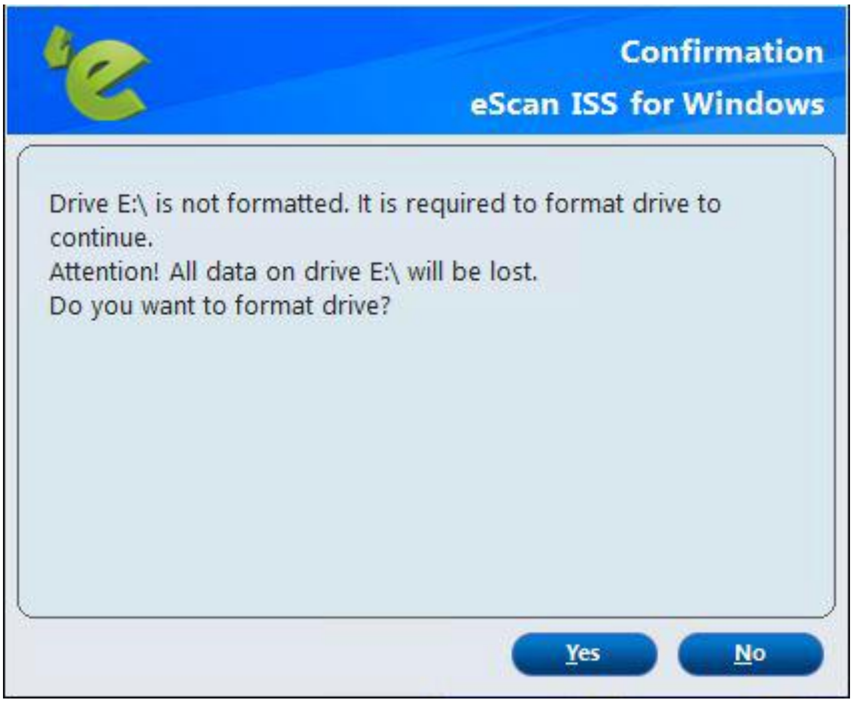
Select the USB flash drive:

E

Warning : Please use only USB flash drives or USB hard drives to record eScan Rescue ISO image. Do not use mp3-players, smart phones or similar devices.

Note: Booting from a USB drive depends upon additional BIOS configuration, hence it may fail in some scenario.

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

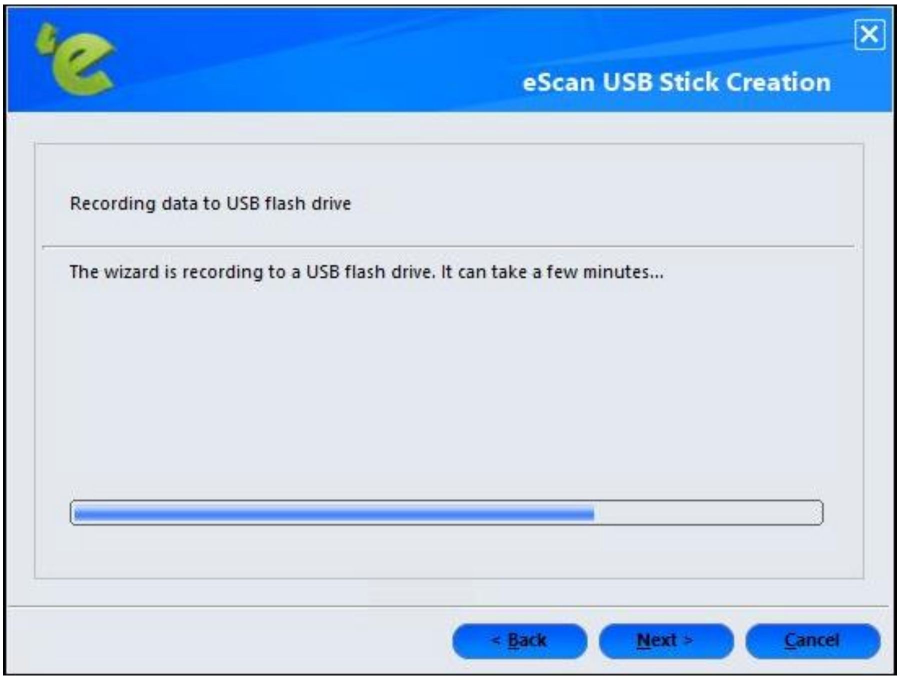


Confirmation

eScan ISS for Windows

Drive E:\ is not formatted. It is required to format drive to continue.
Attention! All data on drive E:\ will be lost.
Do you want to format drive?

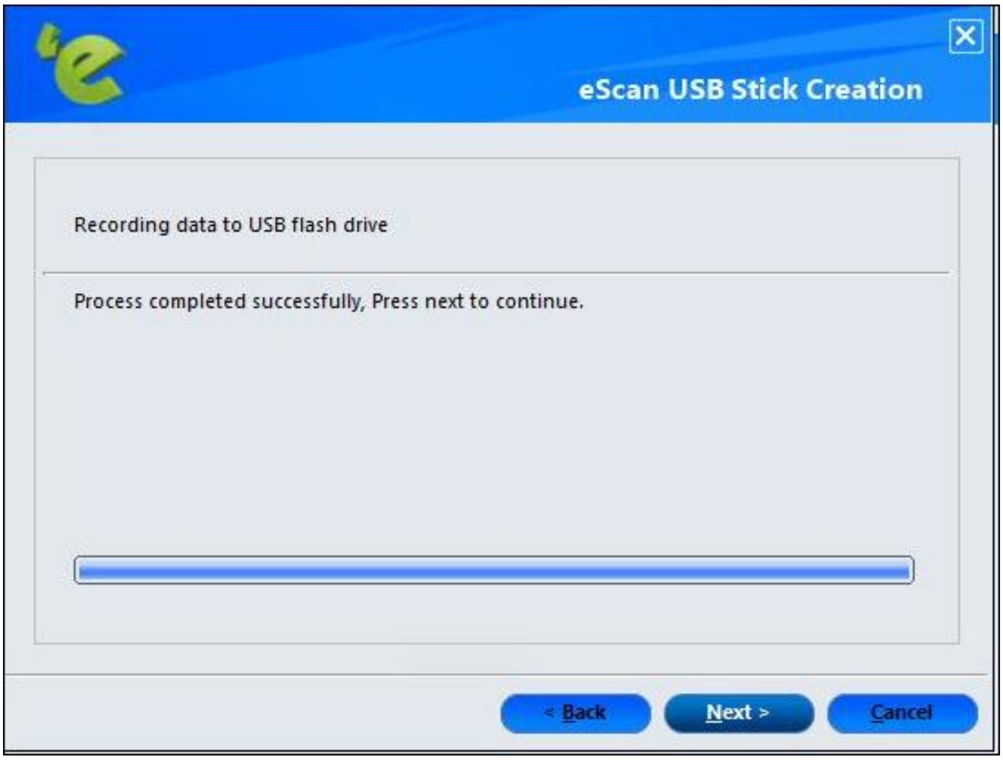
Click **Yes**. The process of recording the data in the USB will be initialized and you will get the following screen:



Recording data to USB flash drive

The wizard is recording to a USB flash drive. It can take a few minutes...

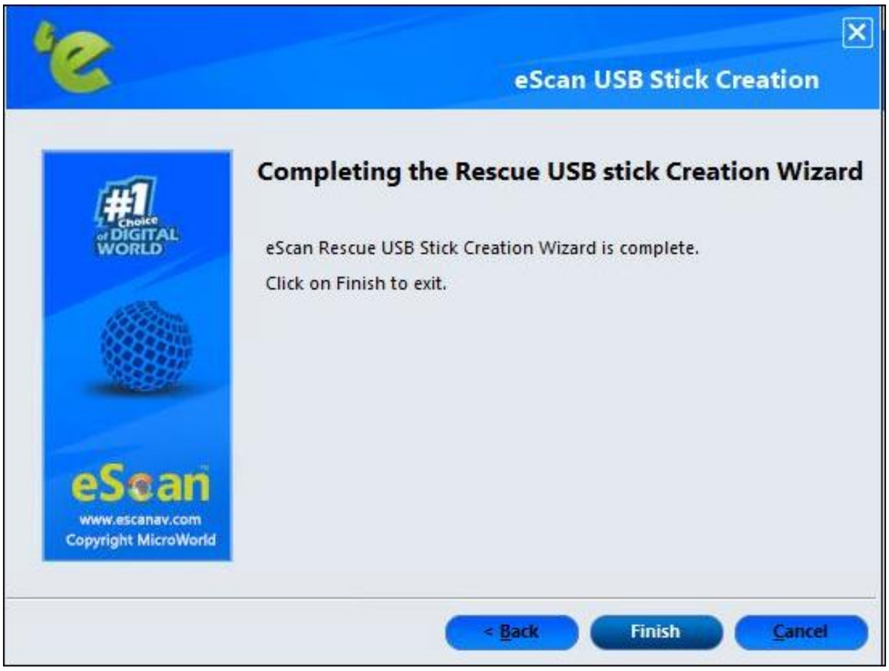
Once the recording process is completed, you will get the following screen. Click **Next>**.



Recording data to USB flash drive

Process completed successfully, Press next to continue.

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



Completing the Rescue USB stick Creation Wizard

eScan Rescue USB Stick Creation Wizard is complete.

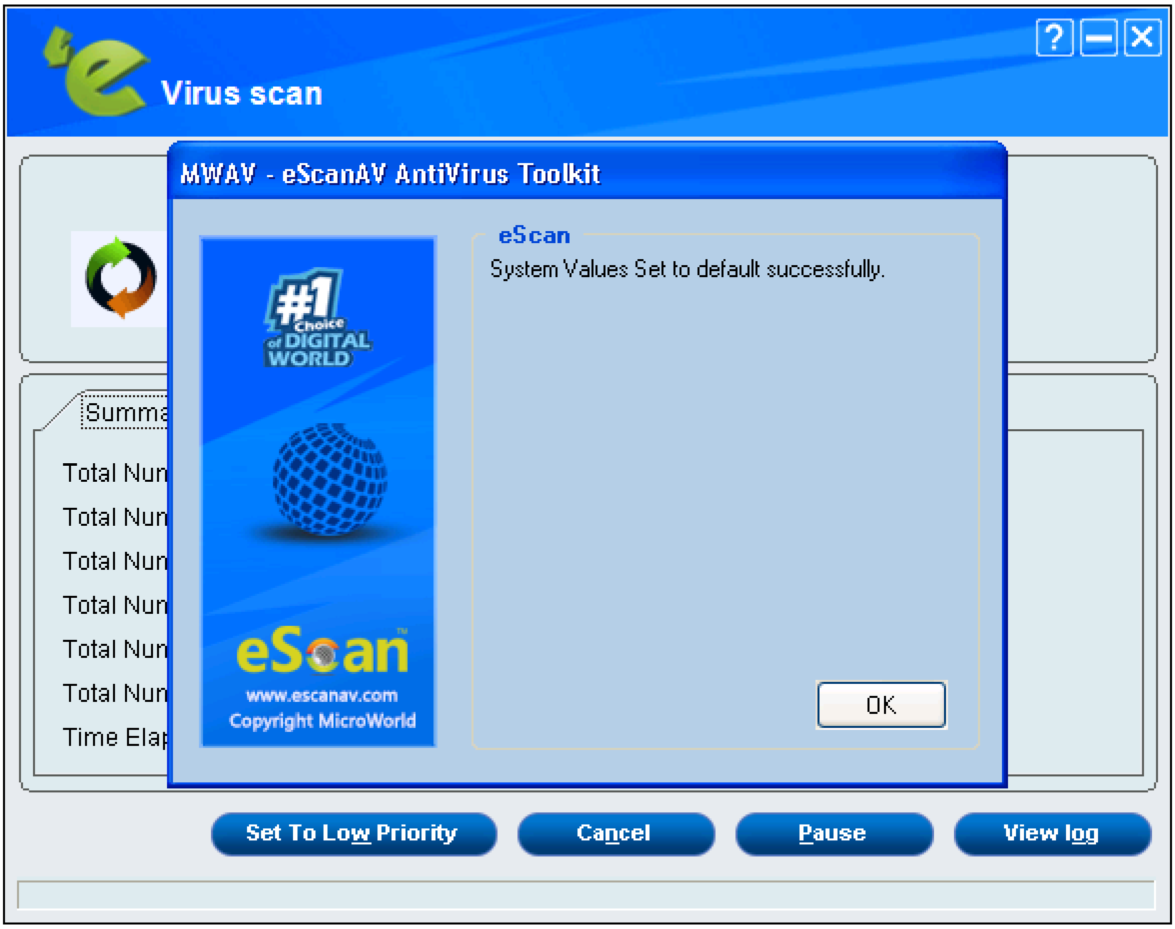
Click on Finish to exit.

Download eScan service pack

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

Restore Windows Default Settings

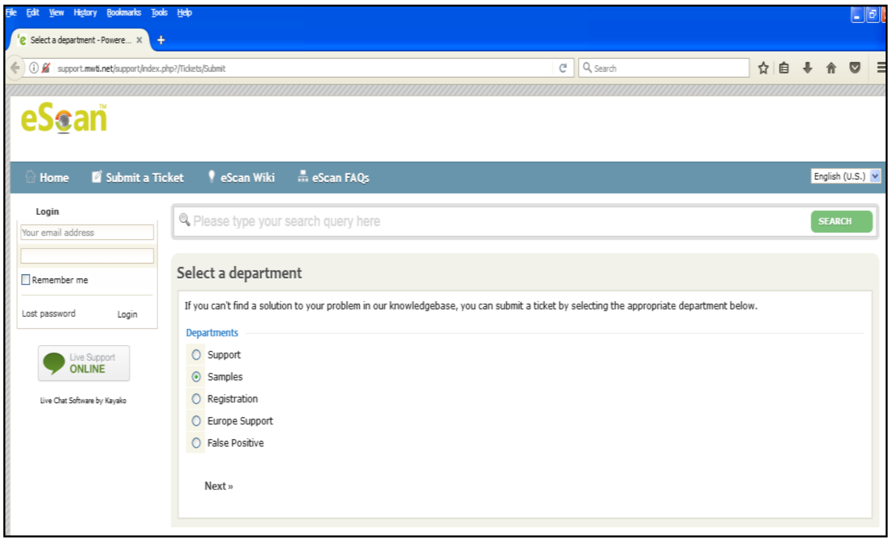
You can restore the Windows® operating system settings, such as desktop and background settings, to eliminate all the modifications made by a virus attack by using this button. eScan automatically scans your computer for viruses when you click this button and sets the system variables to their default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



System Values Set to default successfully.

Upload Samples

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


File Edit View History Bookmarks Tools Help
Select a department - Powere...
support.mwti.net/support/index.php?/Tickets/Submit
Search
eScan
Home
Submit a Ticket
eScan Wiki
eScan FAQs
English (U.S.)
Login
Your email address
Lost password
Login
Live Support ONLINE
Live Chat Software by Kayako
Please type your search query here
SEARCH
Next »

☐ Remember me

Select a department

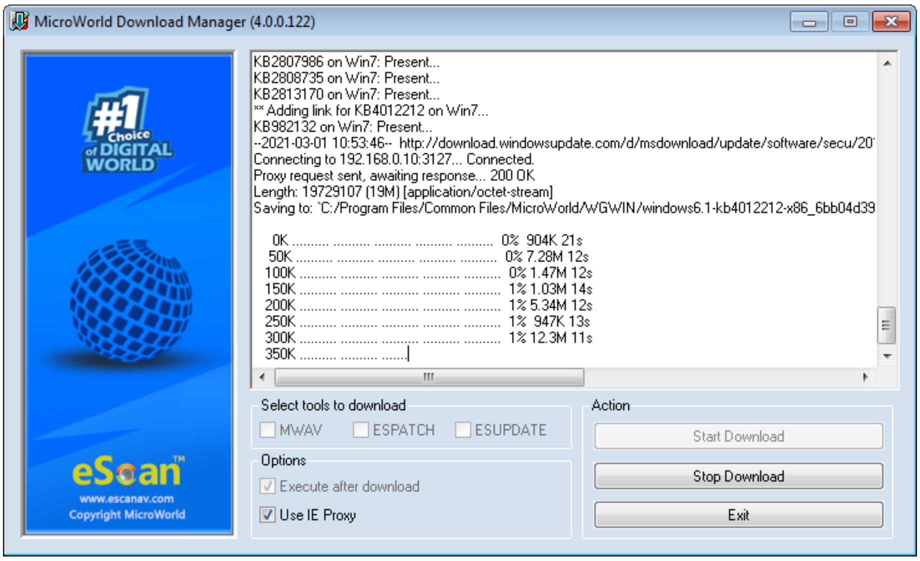
If you can't find a solution to your problem in our knowledgebase, you can submit a ticket by selecting the appropriate department below.

Departments

○ Support
● Samples
○ Registration
○ Europe Support
○ False Positive

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.



```
KB2807986 on Win7: Present...
KB2808735 on Win7: Present...
KB2813170 on Win7: Present...
** Adding link for KB4012212 on Win7...
KB982132 on Win7: Present...
--2021-03-01 10:53:46--  http://download.windowsupdate.com/d/msdownload/update/software/secu/20
Connecting to 192.168.0.10:3127... Connected.
Proxy request sent, awaiting response... 200 OK
Length: 19729107 (19M) [application/octet-stream]
Saving to: `C:/Program Files/Common Files/MicroWorld/WGWIN/windows6.1-kb4012212-x86_6bb04d39

   0K .......... .......... .......... .......... ..........  0%  904K 21s
  50K .......... .......... .......... .......... ..........  0% 7.28M 12s
 100K .......... .......... .......... .......... ..........  0% 1.47M 12s
 150K .......... .......... .......... .......... ..........  1% 1.03M 14s
 200K .......... .......... .......... .......... ..........  1% 5.34M 12s
 250K .......... .......... .......... .......... ..........  1%  947K 13s
 300K .......... .......... .......... .......... ..........  1% 12.3M 11s
 350K .......... .......... .......
```

☐ MWAV ☐ ESPATCH ☐ ESUPDATE

☑ Execute after download

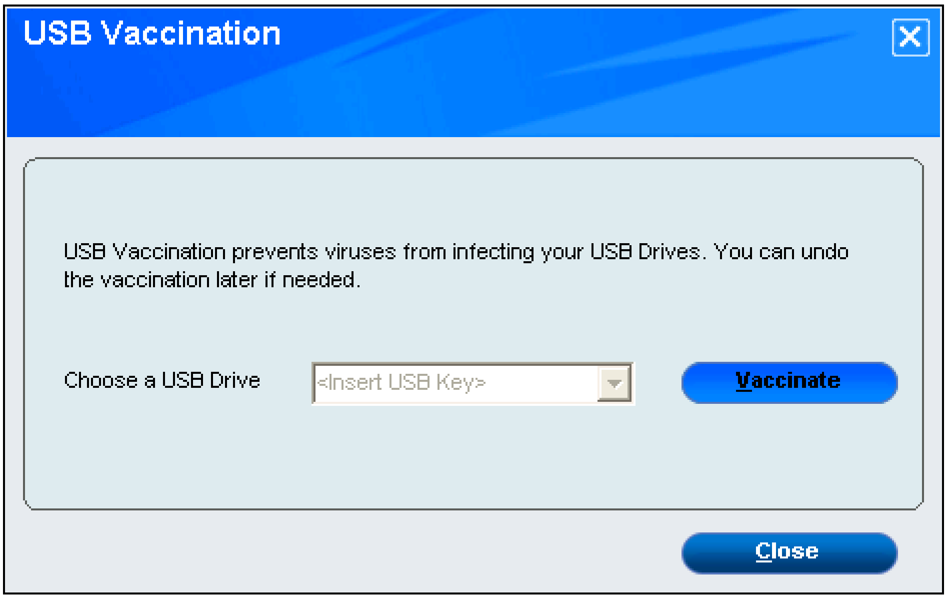
☑ Use IE Proxy

USB Vaccination

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

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

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



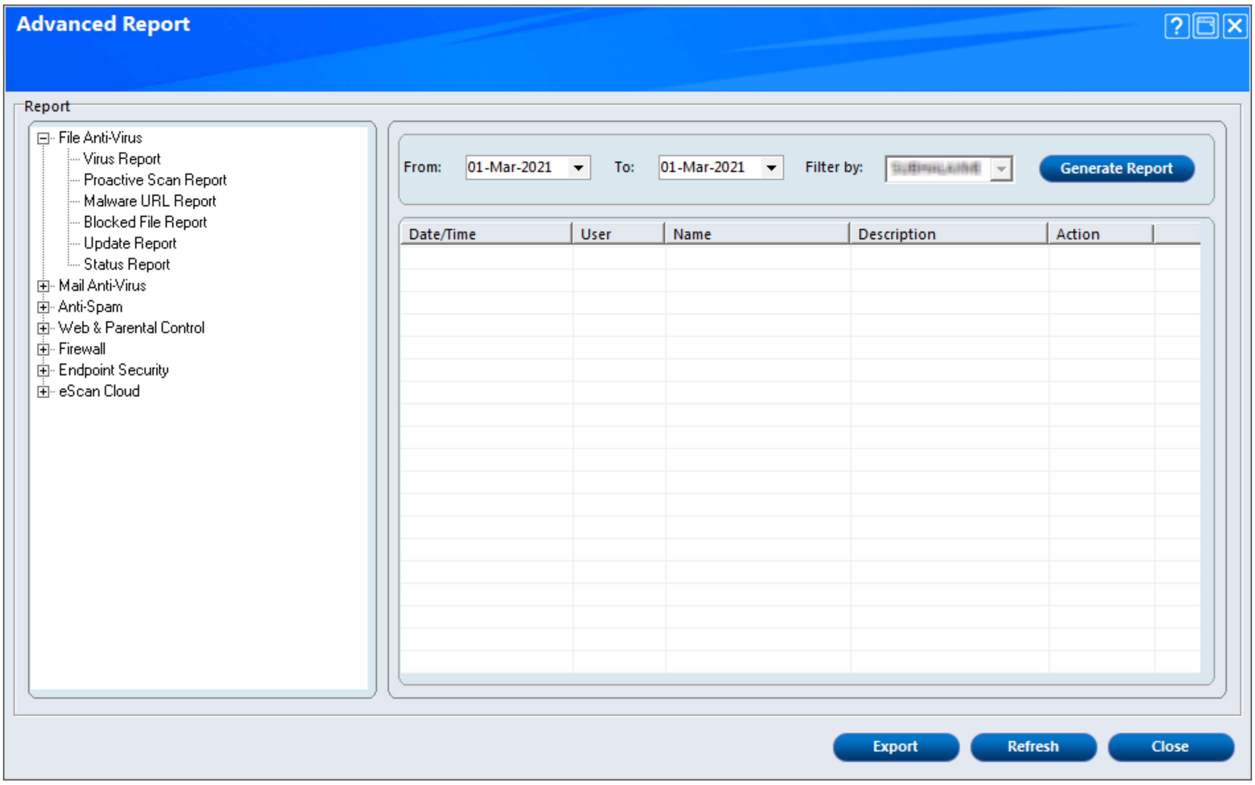
USB Vaccination

USB Vaccination prevents viruses from infecting your USB Drives. You can undo the vaccination later if needed.

Choose a USB Drive <Insert USB Key>

Reports

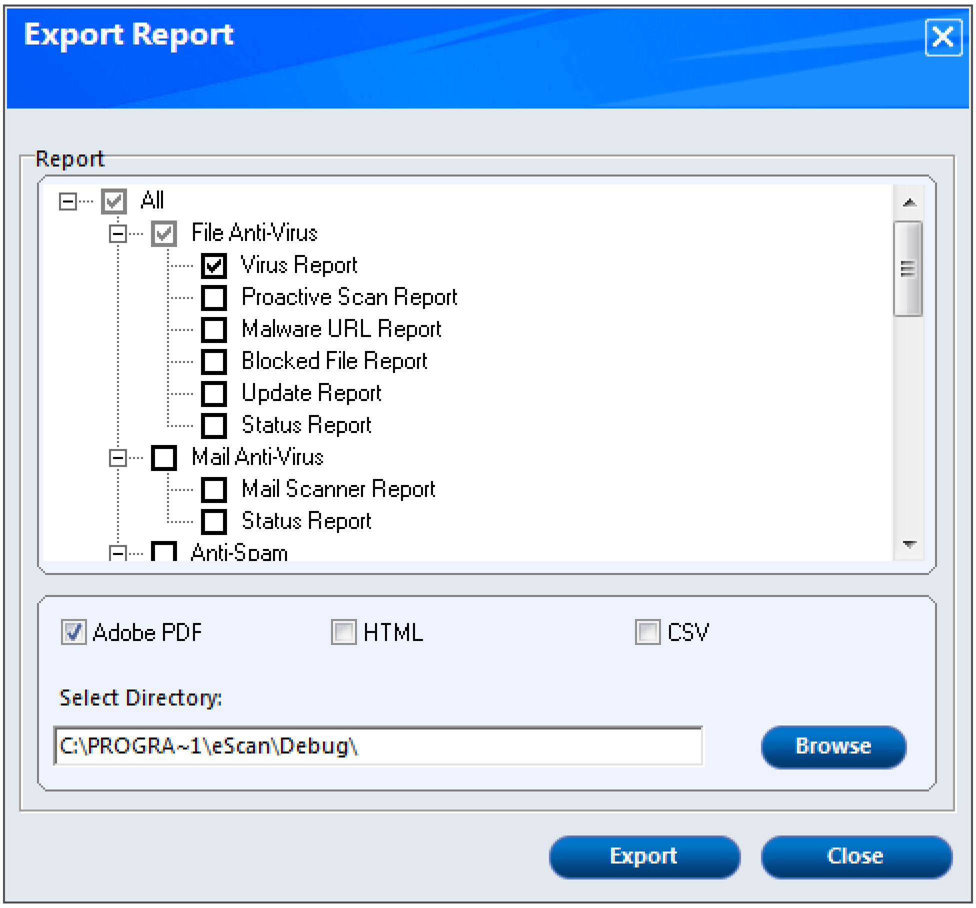
eScan will generate reports for File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Firewall, Endpoint Security, and eScan Cloud modules. Click **Reports** link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to Advance Report window; it displays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



From: 01-Mar-2021 To: 01-Mar-2021 Filter by:

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

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



Export Report

Report

- ☑ All
  - ☑ File Anti-Virus
    - ☑ Virus Report
    - □ Proactive Scan Report
    - □ Malware URL Report
    - □ Blocked File Report
    - □ Update Report
    - □ Status Report
  - □ Mail Anti-Virus
    - □ Mail Scanner Report
    - □ Status Report
  - □ Anti-Spam

☑ Adobe PDF □ HTML □ CSV

Select Directory: C:\PROGRA~1\eScan\Debug\

Procedure to export the report files

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

Contact Us

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

Before you contact technical support team, ensure that your system meets all the requirements and you have Administrator access to it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Chat Support

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

Forum Support

You can even join the MicroWorld Forum to discuss eScan related problems with eScan experts by clicking here.

Email Support

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