



Anti-Virus for Linux Desktops

User Guide

Product Version: 22.0.000.xxxx
Document Version: 22.0.000.xxxx



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



Copyright © 2022 by MicroWorld Software Services Private Limited. All rights reserved.

Any technical documentation provided by MicroWorld is copyrighted and owned by MicroWorld. 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. This user guide may include typographical errors, technical or other inaccuracies. MicroWorld does not offer any warranty to this user guide's accuracy or use. Any use of the user guide or the information contained therein is at the risk of the user. MicroWorld reserves the right to make changes without any prior notice. No part of this user guide 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 Software Services Private Limited.

The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, and MailScan are trademarks of MicroWorld. Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All other product names referenced in this user guide are trademarks or registered trademarks of their respective companies and are hereby acknowledged. MicroWorld disclaims proprietary interest in the marks and names of others.

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

Document Number:	5BUG/10.06.2022/22.7.xx
Current Software Version:	22.7.xxx.xxxx
Technical Support:	support@escanav.com
Sales:	sales@escanav.com
Forums:	http://forums.escanav.com/
eScan Wiki:	https://wiki.escanav.com/wiki/index.php/Main_Page
Live Chat:	https://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld Software Services Private Limited
Date:	June 2022

Table of Contents

Introduction.....	4
Pre-requisites.....	5
Installation	5
Command-line Installation.....	5
GUI Installation	7
Graphical User Interface	8
Modules	9
eScan AV for Linux Desktop - Modules	10
Real Time Monitor.....	10
AV Monitor.....	10
Advance settings	11
Quarantine.....	12
Scan.....	13
On-demand.....	13
Update	20
Set Password	23
File Integrity Monitor	24
AV Monitor.....	24
Advance Settings	25
Device Control.....	26
Web Control.....	28
Firewall	29
Configuration	30
Support.....	38
Live chat.....	38
eScan online help	38
MicroWorld forum.....	38
Create debug diagnostics	39
Submit Sample	39
Feedback	39
License	40
Online Registration Process	40
Offline Registration Process	45



Contact Us.....	51
Forums	51
Chat Support	51
Email Support	51

Introduction

MicroWorld's eScan Anti-Virus for Linux Desktop scans and protects the system from viruses and other threats, thus offering effective and complete security. It is designed to understand different file types, data-streams, and compression formats. It can look inside data-streams and identify complex file architectures. This solution has a user-friendly interface and automatically downloads updates from internet to protect computers against upcoming cyber threats.

eScan AV for Linux Desktop enables you to run an On-Demand scan to provide additional protection. An On-Demand scan is initiated by the user where user can scan anything from a single file to everything on the system that has permission to read. The scanning process can be initiated either manually or by scheduling the on-demand scan to run unattended. The Real-Time Monitoring module protects your device from cyber threats in real-time. In case, if any infected object is detected, eScan allows you to take action against it. Users can set administrative password to access the eScan GUI and also it allows to set password authentication for the uninstallation of eScan by using Set Password module.

A Device Control feature safeguards your data from data leaks and data breaches. The user can establish settings such as allowing or blocking USB and CD/DVD access, prompting for the password whenever a USB is plugged in, and many more. The feature Web Control provides access to the websites on category based to keep protected from unsolicited websites. To avoid cyber attacks through network traffic, eScan Firewall module has set of pre-defined access control rules that helps to filter the two-way traffic and blocks the unauthorized access on system. The Firewall acts as a gateway between internet and system, to monitor all incoming and outgoing traffic. eScan allows you to validate the difference between current file status and original file using the File Integrity Monitor module through admin can track the modifications in the file.

Features of eScan AV for Linux Desktop:

- Proactive AV protection intercepts all known threats
- Automatic updates for the most up-to-date virus protection
- Includes scan scheduler and custom scan profiles
- Provides comprehensive log of scanning activity
- Cross file system scanning
- USB and CD/DVD access controls
- Real time monitoring to protect system from malware
- Prevents data leaks and data breaches
- Control over incoming and outgoing network traffic
- Access to the websites on internet based on categories
- Password restriction to access the GUI and uninstall eScan
- Ease to get alerts about modifications done in the original file

Pre-requisites

Administrative Privilege:	root / sudo user privilege
CPU:	Intel® series 1GHz & above
Memory:	2 GB RAM & above
Disk space:	2 GB & above of free disk space
Platforms Supported:	RHEL 4 & above (32 & 64-bit) CentOS 5.10 & above (32 & 64-bit) SLES 10 SP3 & above (32 & 64-bit) Debian 4.0 & above (32 & 64-bit) OpenSuSe 10.1 & above (32 & 64-bit) Fedora 5.0 & above (32 & 64-bit) Ubuntu 6.06 & above (32 & 64-bit) Mint 12 and above (32 and 64 bit)

Installation

Click on the following link and download the installation package:

<https://www.escanav.com/en/linux-antivirus/antivirus-for-linux-desktop.asp>

To install the downloaded package, use any one from the following methods:

- **Command-line Installation**
- **GUI Installation**

Command-line Installation

To perform command-line installation, user must be logged on to the system as root / sudo user.

1. Open the Terminal.
2. Go to the directory where the downloaded eScan package is located.
3. Execute the following commands as per the Linux OS configuration:
 - To install from RPM package: **rpm -ivh <RPM package>**
Here, it will be **rpm -ivh escan-antivirus-wks.x86_64.rpm**
 - To install from Debian (deb) package: **dpkg -i <Deb package>**
In case of deb, for example, **dpkg -i escan-antivirus-wks.x86_64.deb**

This will start the installation process.

```

File Edit View Search Terminal Help
[escan@support ~]$ su -
Password:
[root@support ~]# cd /home/escan/Desktop/Setup
[root@support Setup]# ls
escan-antivirus-wks.x86_64.rpm
[root@support Setup]# rpm -ivh escan-antivirus-wks.x86_64.rpm
Preparing... ##### [100%]
 1:escan-antivirus-wks ##### ( 65%)

```

After the installation is finished, the terminal displays a success message.

```
File Edit View Search Terminal Help
[root@support Setup]# rpm -ivh escan-antivirus-wks.x86_64.rpm
Preparing... ##### [100%]
 1:escan-antivirus-wks ##### [100%]

Checking dependencies for Webfilter...
Checking Kernel version...ok
Checking gcc....Installed.
Checking make....Installed.
Checking kernel headers....Installed.
Checking Required files...
Compiling kernel module...
Compiled kernel module for web protection successfully

Checking dependencies for portblocker...
Checking Kernel version...ok
Checking gcc....Installed.
Checking make....Installed.
Checking kernel headers....Installed.
Checking Required files...
Compiling kernel module...
Compiled kernel module for port protection successfully
Starting MicroWorld epsdaemon: [ OK ]
Starting MicroWorld rtscanner: [ OK ]
Reloading crond: [ OK ]

##### eScan for Linux #####
#                                     #
#                                     #
#      eScan for Linux installed successfully.      #
#                                     #
#                                     #
#####
```

4. To verify whether the installation is complete, user can view the log in the log file:
cat/var/MicroWorld/var/log/Install.log

GUI Installation

To perform the installation through GUI manually, follow the below steps:

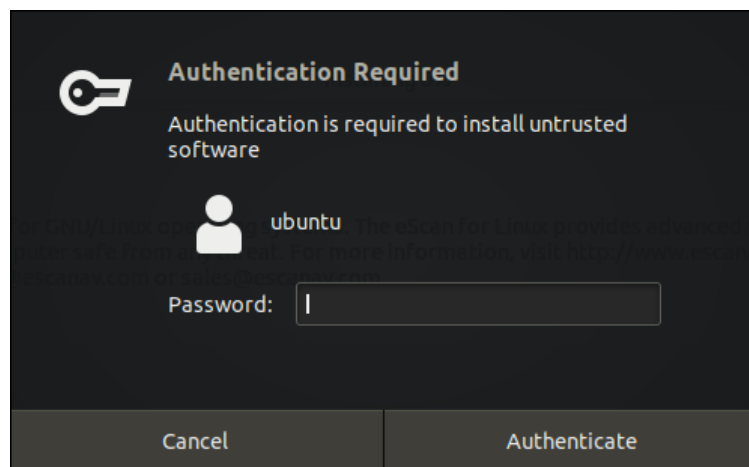
1. Double-click the downloaded eScan Setup file.

Following prompt appears.



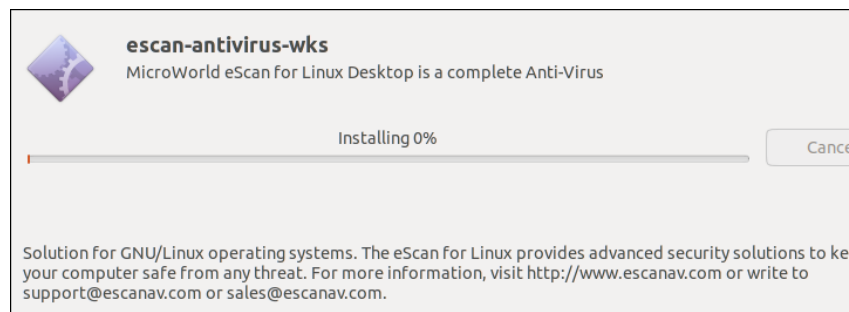
2. Click **Install**.

The Authentication prompt appears.



3. Enter the root password and then click **Authenticate**.

The Installation wizard proceeds to install eScan.



eScan Anti-Virus gets installed on the system.

Graphical User Interface

The eScan AV for Linux Desktop has user friendly GUI that can be accessible from the desktop and allows to perform and configure various tasks including on-demand scan, file integrity and real time monitoring, firewall setup, device and web controls, and many more. It also displays information about the current version of the product and virus definition.



On Bottom-left corner of the screen, it displays the date and time when the computer was last scanned along with date of the Anti-Virus signatures available on the system.

Modules

eScan AV for Linux Desktop allows to configure the following modules:

- **Real Time Monitor:** This module is used to configure the monitoring of the specific files/directories on real-time basis. To learn more, [click here](#).
- **Scan:** The Scan module allows to access On-Demand scan features and schedule scans as per requirement. To learn more, [click here](#).
- **Update:** The Update module allows to configure Anti-Virus updates on a system. To learn more, [click here](#).
- **Set Password:** The Set Password module allows to set the administrative password to access and eScan Linux GUI to uninstall the eScan from the system. To learn more, [click here](#).
- **File Integrity Monitor:** The File Integrity Monitor module allows to monitor the difference between current file status and original file status. To learn more, [click here](#).
- **Device Control:** The Device Control module allows to configure the settings for the external/portable devices such as CD/DVD and USB. To learn more, [click here](#).
- **Web Control:** The Web control module allows to configure (allowing or blocking) the web access features as per requirement. To learn more, [click here](#).
- **Firewall:** The Firewall module lets you put up the restrictions for incoming and outgoing traffic to the system. To learn more, [click here](#).
- **Support:** Use this module to contact with eScan support using links live chat, eScan online help, submit sample and feedback. To learn more, [click here](#).
- **License Information:** The License module lets you manage your license. To learn more, [click here](#).

eScan AV for Linux Desktop - Modules

The eScan AV for Linux Desktop comprises of modules Scan, Real Time Monitor, Update, Web Control, File Integrity Monitor, Firewall, and Device Control to ensure the protection of system from the Trojan, malware and other cyber attacks.

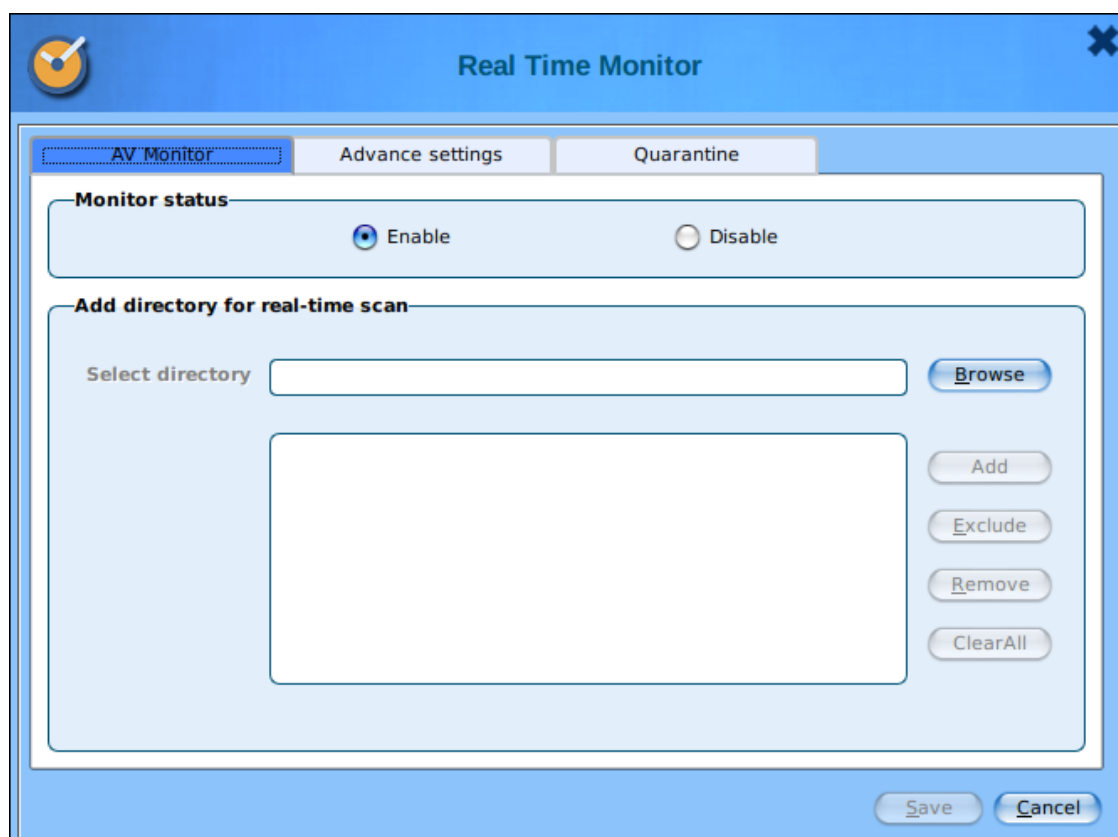
Real Time Monitor

This option is used to configure the monitoring of the specific files/directories on real-time basis. It consists of three tabs that are AV Monitor, Advance settings, and Quarantine.

AV Monitor

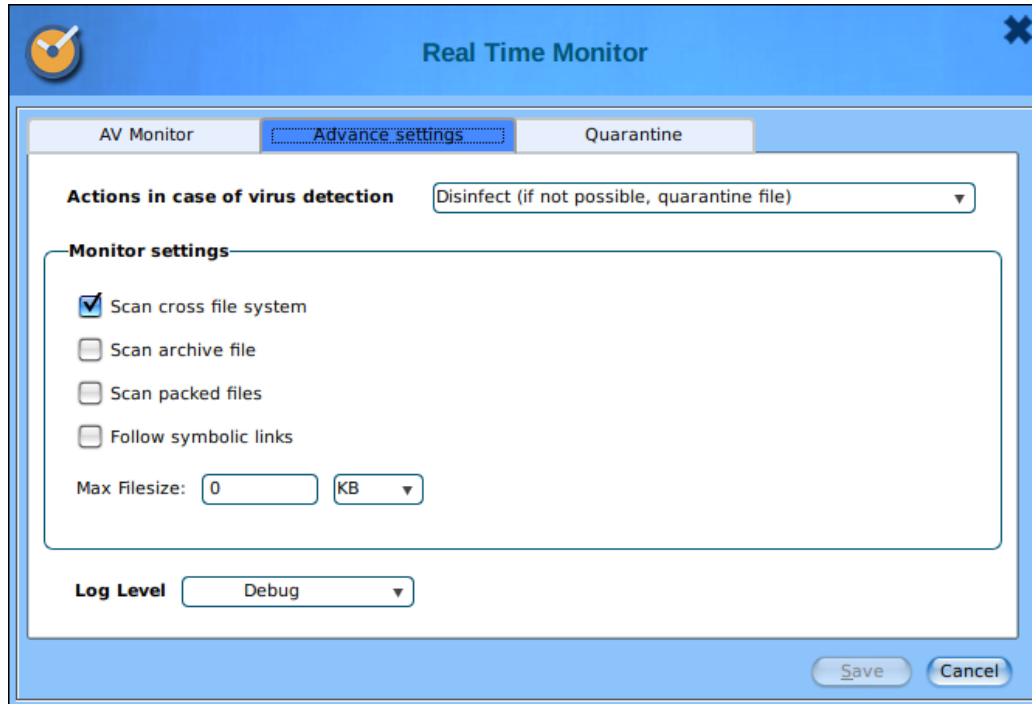
- To perform Real-Time Monitoring, select **Enable** option (by default it is selected).
- After enabling it, add files/directories for monitoring as per the requirements by clicking option **Browse**.
- User can perform actions **Exclude**, **Remove** and **Clear All** on directories as per the requirement.

In case, user wants to stop Real-Time Monitoring feature, select **Disable** option.



Advance settings

This tab will allow to define actions on virus detection and scan settings as per need, which are as follows:



Actions in case of virus detection

It displays a list of actions eScan should take, after the virus detection. By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions available in drop down list:

- **Log Only:** This option indicates or alerts the user about the virus detection (No Action is taken, only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect the file and if disinfection is not possible, it logs the information only for the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect the file and if is not possible, it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible, it quarantines the infected object.
- **Delete:** This option directly deletes the infected object.
- **Quarantine:** This option directly quarantines the infected object.

Monitor settings

- **Scan cross file system:** This checkbox facilitates scanning of files over cross-file systems.
- **Scan archive file:** This checkbox facilitates scanning of archived files.
- **Scan packed files:** This checkbox facilitates scanning of packed files.
- **Follow symbolic links:** This checkbox facilitates scanning of files that follows the symbolic links.

Max Filesize: This option let's you to define the maximum file size that can be scanned.

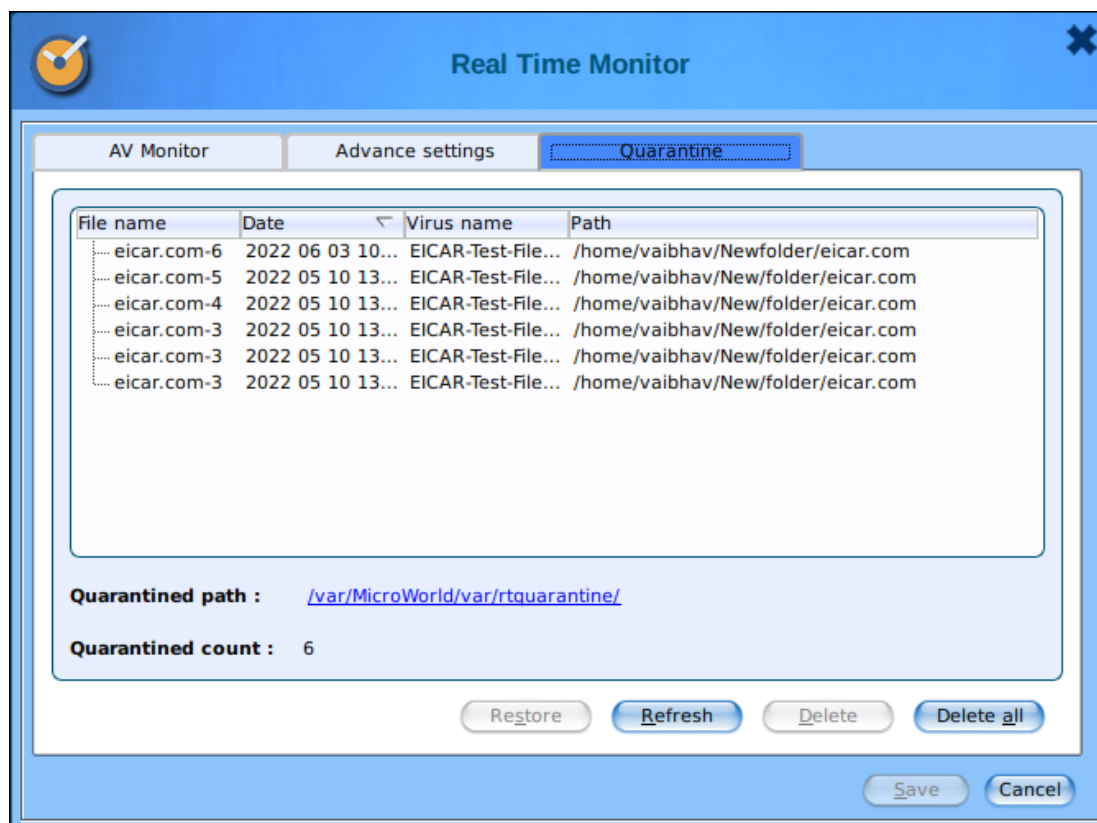
Log Level

This dropdown menu used to configure the log level i.e. options to log information about files and the action taken on them:

- **Minimum:** This option specifies only a minimum detail of the objects scanned in the eScan log.
- **Informative:** This option specifies only details of the infected objects in the eScan log.
- **Detail:** This option specifies a detailed eScan log.
- **Debug:** This option specifies the details that can be used for troubleshooting purpose in case of any issue.

Quarantine

This option will display the information about the files that were quarantined along with the location where these files are placed. The default path for the quarantined file is **/var/MicroWorld/var/rtquarantine**. It also displays the count of quarantined files.

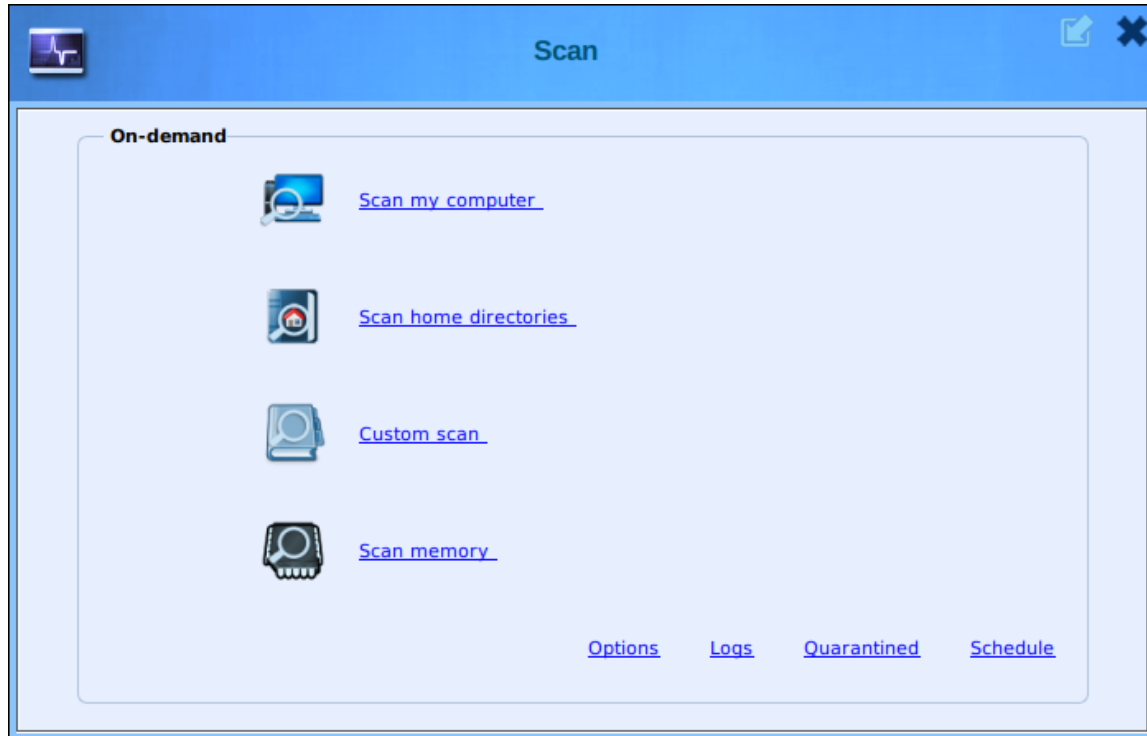


- **Restore:** This tab used to restore the quarantined files.
- **Refresh:** This button will refresh the list of quarantined files.
- **Delete:** To delete the specific file from the list, click this option.
- **Delete all:** Click this option to delete all the files at a time.

After making necessary configuration, click on **Save**.

Scan

The Scan module helps user to perform On-Demand scans for files, directories, storage devices and memory. It checks the computer for security threats such as viruses, spyware, and other malware. In addition, user can perform a custom scan for particular files/directories. It creates logs of all performed scan operations.



This module provides options for scanning the computer and peripheral storage devices, configuring the On-Demand scan and scheduling scans as per requirement.

On-demand

Below options are used to perform on-demand scans on files, directories, and storage devices.

Scan my computer

This option allows to scan entire system. By clicking on this option, user will get a popup window and gives the detail of the scan after completion.

Scan home directories

This option provides with scanning options for the home directories. By clicking on this option, user will get a popup window and gives the detail of the scan performed.

Custom scan

This option helps to configure the scan for specific files/directory according to the specific need of the users.

Scan memory

This option allows scanning of memory. By clicking on this option, user will get a popup window and gives the detail of the scanning.

Options

Configure On-Demand Scan by clicking the **Options** button. This will display the various alternatives for configuring the on-demand scan as per need.

- **Actions in case of virus detection**

This list helps to configure the action that should be performed on the file when it finds as infected. The actions are as follows:

- **Log Only:** This option indicates or alerts the user about the virus detection (No Action is taken, only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible, it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible, it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible, it quarantines the infected object.
- **Disinfect (if not possible, rename file):** This action tries to clean the file and if it is not possible to disinfect the file, it renames the file.
- **Disinfect (if not possible, ask user):** This option tries to disinfect and if disinfection is not possible, it asks the user for what action has to be taken on that file.
- **Delete:** This option directly deletes the infected file.
- **Quarantine:** This option directly quarantines the infected file.
- **Rename:** This option directly renames the infected file.
- **Ask user:** It directly displays the popup to take required action on infected file.

- **Priority of scanner**

This option helps to set the priority of the scanner in correlation with other processes running on the computer. The priority levels can be

- High (short runtime)

- Normal (normal runtime)
 - Low (long runtime)
- **Scan settings**

This option provides various scan settings that are as follows:

 - **Include sub-directory:** This checkbox ensures that eScan scans all the sub directories recursively under every directory and not only the first level of directories. By default, it is selected.
 - **Mails:** This checkbox allows real-time scanning of mails. By default, it is selected.
 - **Heuristic:** Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application. By default, it is selected.
 - **Packed:** This checkbox provides real-time protection to scan packed files (compressed executable). By default, it is selected.
 - **Cross File System:** This checkbox facilitates scanning of files in Cross file systems (can work across multiple types of OS environments).
 - **Archives:** This checkbox provides real-time protection to scan archived files such as zip, rar, and so on. By default, it is selected.
 - **Follow Symbolic Links:** This checkbox facilitates scanning of files that follows the symbolic links.
- **Max Filesize:** This option lets you to define the maximum file size that can be scanning.
- **Log settings**

This option is used to configure the log settings. User can set the custom log location. User can configure the log level i.e. options to log information about files (All or Infected or Minimum) and the action taken on them.
- **Exclude options**

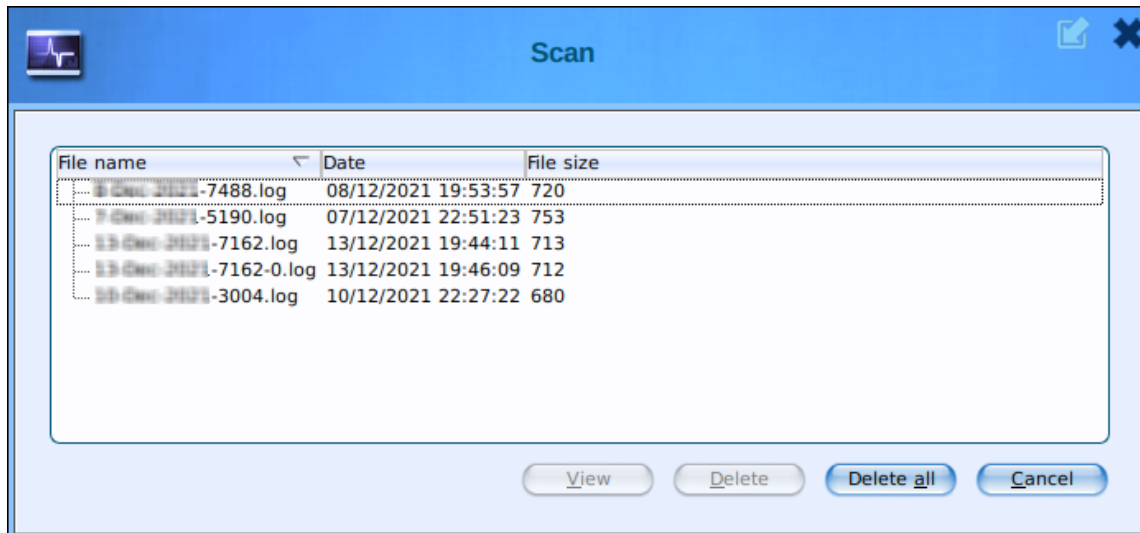
This option is used to exclude all the listed files, directories, and sub directories from monitoring during the scan. User can exclude specific types of files from scanning and also add or delete the list using +/- option.
- **Scan all running process(es) at startup**

This checkbox facilitate the scanning of memory at the startup of the system. By default this option is selected.

After making necessary changes, click on **Save**.

Logs

This option will display information about the generated logs such as File name, Date of scanning and File size. User can view and delete the log as per the requirement.

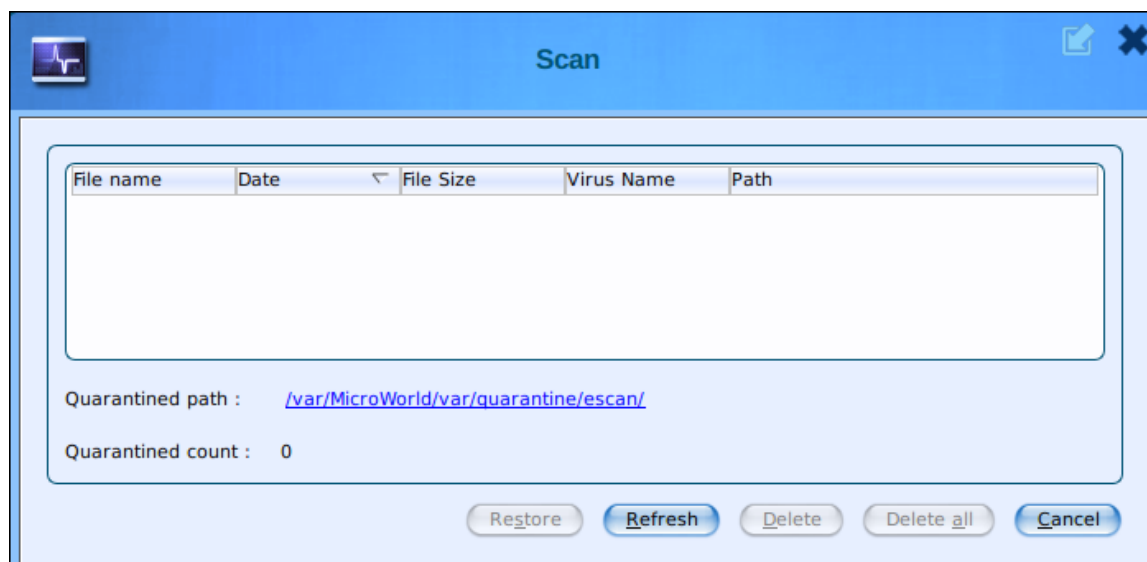


- **View:** This option is to view the particular log.
- **Delete:** To delete the specific log from the list, click this option.
- **Delete all:** Click this option to delete all the logs in one click.

Quarantined

This option will display the information about the files that were quarantined along with the location where these files are placed.

The default path for the quarantined file is `/var/MicroWorld/var/quarantine/escan/`



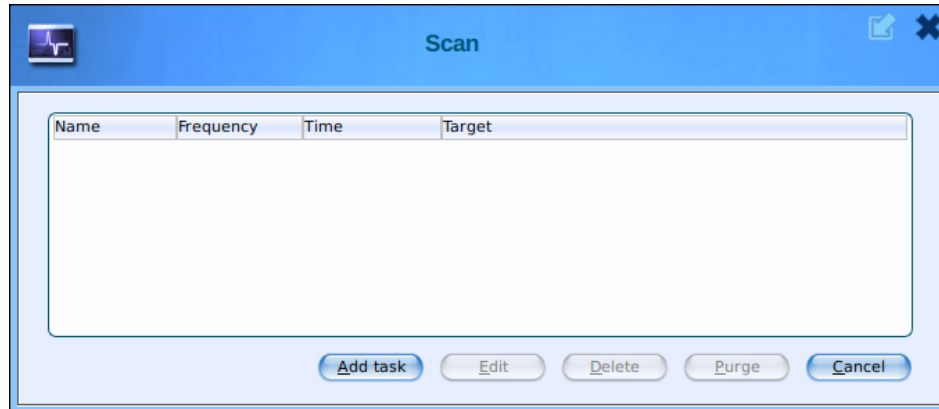
User can **Refresh**, **Delete** (single or multiple) and **Restore** the quarantined objects as per requirement.

Schedule

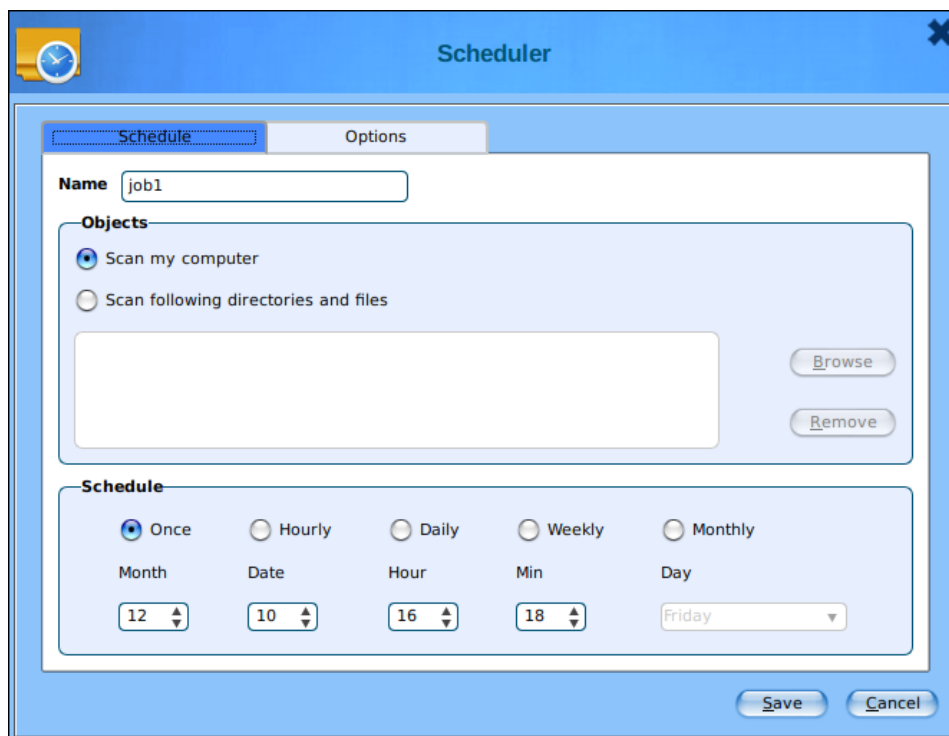
This option is used to schedule on-demand scanning of the computer and storage devices for malicious objects at specific date and time. In a table, it displays name of the schedule, frequency of occurrence, and the time it will be run again.

To create a schedule, perform the below steps:

1. Click **Schedule**.



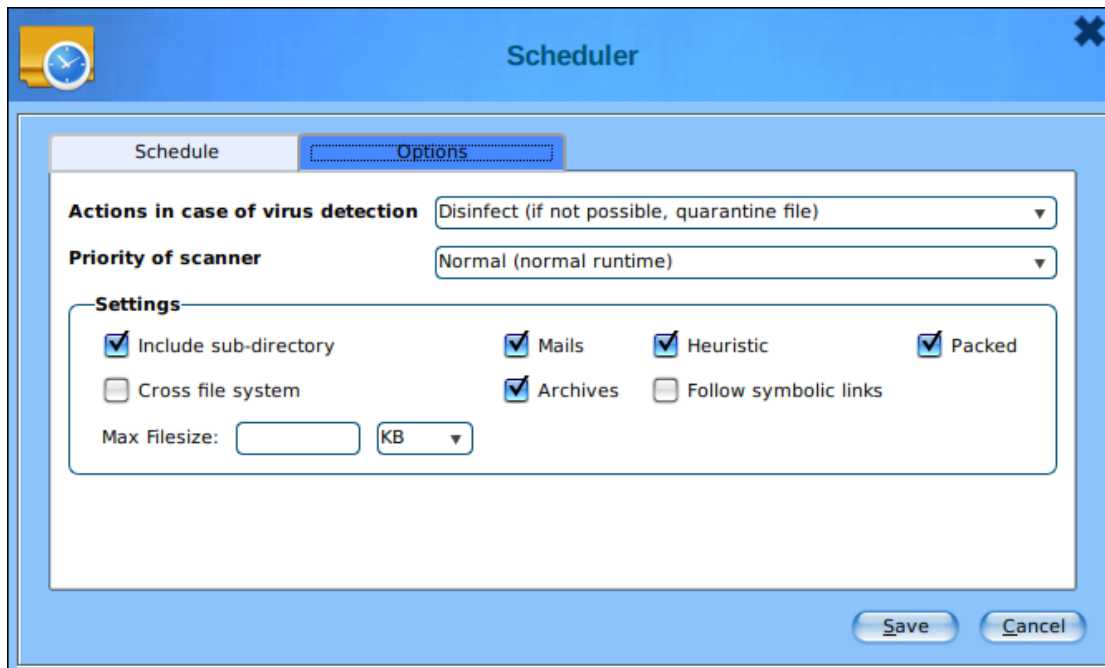
2. In the schedule screen, click **Add task**.
Scheduler window appears.



3. In the Schedule tab, enter the name of the schedule and select the objects.
 - **Scan my computer:** This option scans the whole computer.
 - **Scan following directories and files:** This option scans specific directories and files. User can add and remove the files and directories as per the requirement. To add files or directories, click on **Browse** and to delete the added files, click on **Remove**.
4. Schedule the on-demand scan for a

- **Once:** Select date and time to perform scan only for once.
- **Hourly:** Select time to perform an hourly scan.
- **Daily:** Performs scan on daily basis on defined time.
- **Weekly:** Select a day and time to scan on weekly basis.
- **Monthly:** Performs scanning every month as per the date and time is set.

Options



In **Options** tab, configure the following options:

- **Actions in case of virus detection**

It displays a list of actions eScan should take, in case of virus detection. By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- **Log Only:** This option indicates or alerts the user about the virus detection (No Action is taken, only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible, it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible, it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible, it quarantines the infected object.
- **Disinfect (if not possible, rename file):** This action tries to disinfect the file and if it is not possible to disinfect the file, it renames the file.
- **Delete:** This option directly deletes the infected object.
- **Quarantine:** This option directly quarantines the infected object.
- **Rename:** This option directly renames the infected object.

- **Priority of scanner**

This option helps to set the priority of a scanner in correlation to other processes running on the computer. The priority level can be

- High (short runtime)
- Normal (normal runtime)
- Low (long runtime)

- **Settings**

This option provides various scan settings that are as follows:

- **Include sub-directory:** This checkbox ensures that eScan scans all the sub directories recursively under every directory and not only the first level of directories.
- **Mails:** This checkbox provides real-time protection to mails. By default, it is selected.
- **Heuristic:** Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Packed:** This checkbox provides real-time protection to packed files (compressed executable).
- **Cross File System:** This checkbox facilitates scanning of files in Cross file systems (can work across multiple types of OS environments).
- **Archives:** This checkbox provides real-time protection to archived files such as zip, rar, and so on.
- **Follow Symbolic Links:** This checkbox facilitates scanning of files that follows the symbolic links.

- **Max Filesize:** This option lets you to define the maximum file size that can be scanned.

After configuring the schedule, click on **Save**.

The task will be saved and run according to the configuration.

Edit

To modify the existing schedule, select the specific task from the list, click **Edit**. After making necessary changes, click **Save**. The task will be modified accordingly.

Delete

To delete the existing schedule, select the specific task from the list, click **Delete**. A confirmation window will be prompted, click **Yes**. The selected scheduled task will be deleted.

Purge

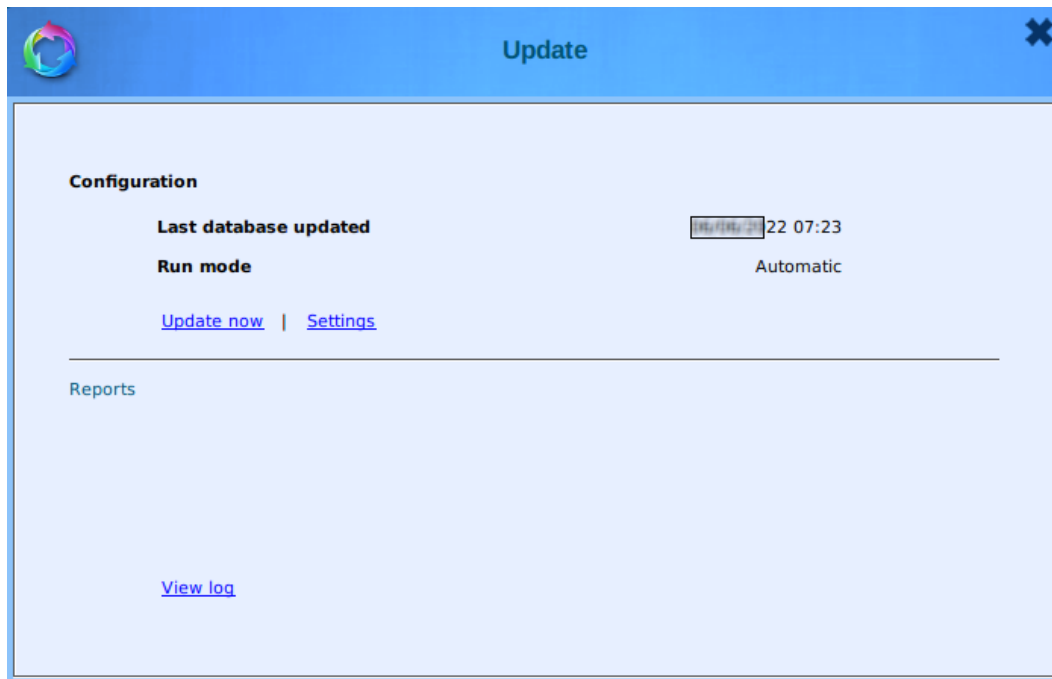
This option lets you to clear the scheduler after the task has been completed.



The **Purge** option is only for scan scheduled for the **Once**.

Update

The Update module automatically keeps the virus definitions up-to-date and protects the system from emerging variant of viruses and other malicious programs. User can configure eScan to download updates automatically from internet.



This module will display the following information under Configuration section:

Last database updated

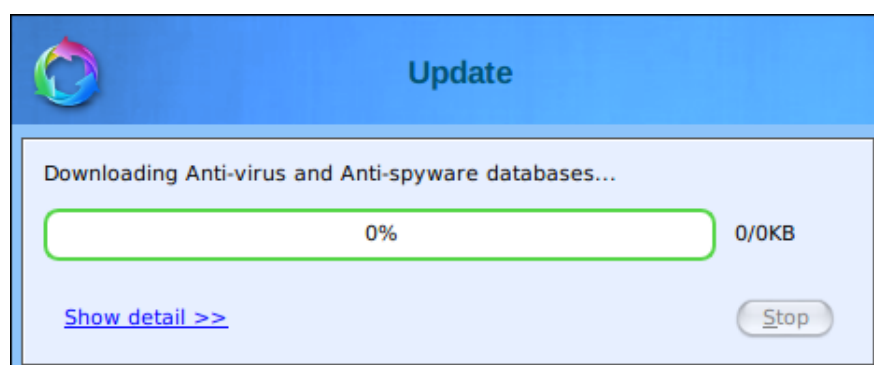
It displays the time and date of the last virus definition was updated.

Run mode

It displays the type of update mode used by eScan. The run mode can be either Automatic or Scheduled.

Update Now

Clicking this button starts downloading the Anti-Virus and Anti-Spyware signature definition from internet.



Settings

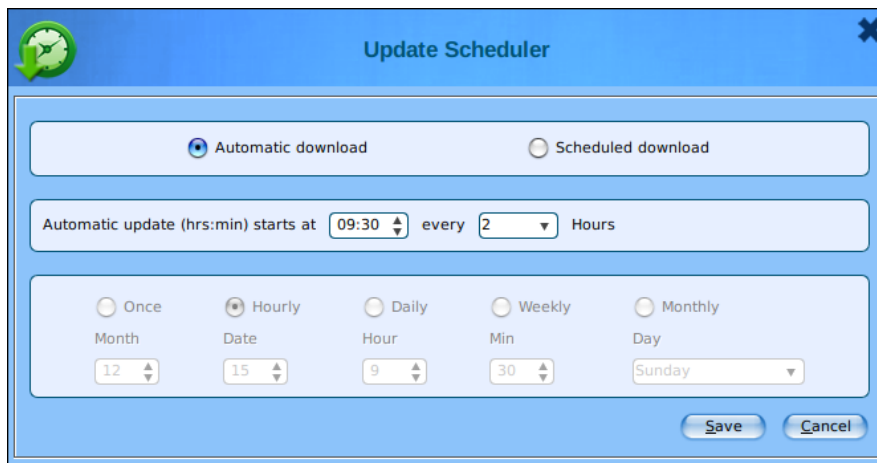
This option allows to configure the Update module to download AV signature from the internet automatically or by scheduling the update task.



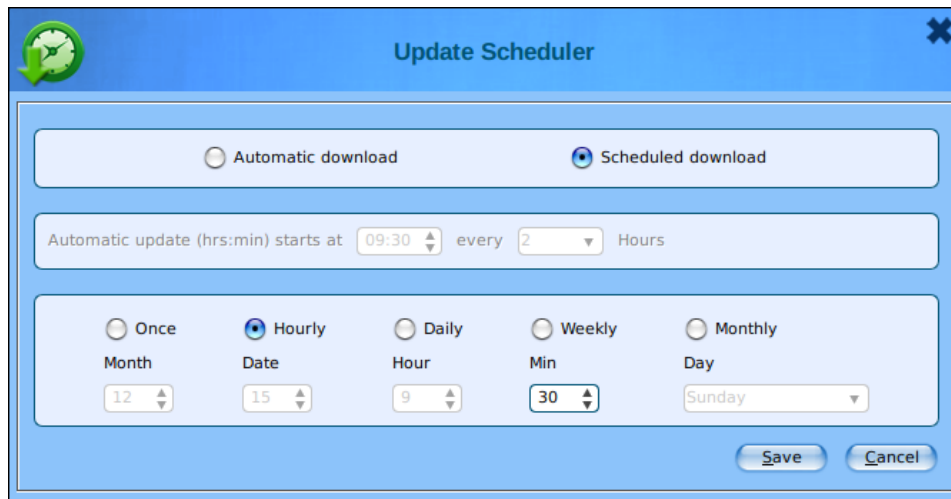
Set update schedule: To schedule an update task, click on three dots present in front of Set update schedule. Update Scheduler window appears.

In the Update Scheduler window,

- **Automatic download:** This option downloads the update automatically after a specific time interval. User can configure the time i.e. start time and time interval (in hours) between the two respective updates.



- **Scheduled download:** This option schedules the download task on specified time and date. User can configure it as mentioned below,
 - **Once:** Select date and time to download update only for once.
 - **Hourly:** Select time to download an update on hourly basis.
 - **Daily:** Downloads an update on daily basis on defined time.
 - **Weekly:** Select a day and time to download an update on weekly basis.
 - **Monthly:** Downloads update every month as per the date and time is set.



The 'Update Scheduler' dialog box has a blue title bar with a green update icon and a close button. It contains two radio buttons: 'Automatic download' (unselected) and 'Scheduled download' (selected). Below these, a text field shows 'Automatic update (hrs:min) starts at 09:30 every 2 Hours'. At the bottom, there are five radio buttons for frequency: 'Once' (unselected), 'Hourly' (selected), 'Daily' (unselected), 'Weekly' (unselected), and 'Monthly' (unselected). Under 'Hourly', there are five sub-sections: 'Month' (12), 'Date' (15), 'Hour' (9), 'Min' (30), and 'Day' (Sunday). 'Save' and 'Cancel' buttons are at the bottom right.

After performing all necessary configurations, click on **Save**.

Warn, if Virus signature is more than ____ days old: This will alert the user when AV updates are more than the specified number of days.

Proxy settings: To configure the Proxy settings for connecting to the internet to download the AV updates.

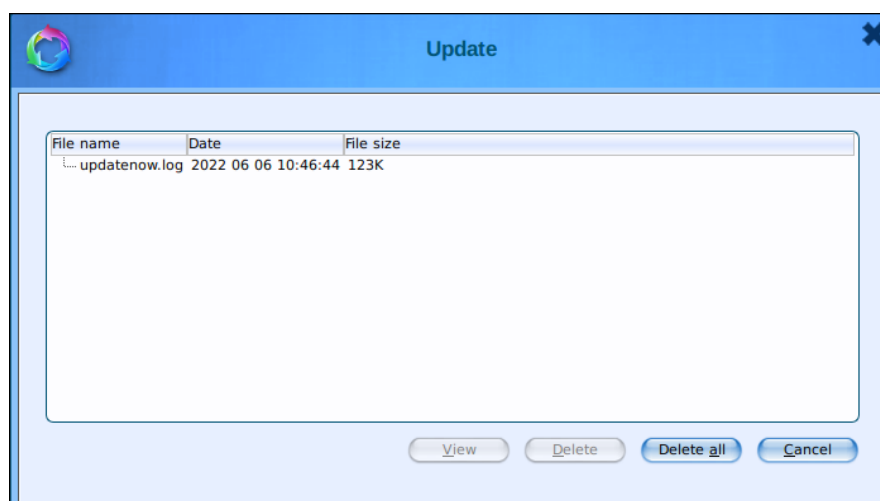
- **Download via Proxy:** This option lets to enable and configure the proxy setting.
 - **IP:** Enter the IP address of the Internet proxy.
 - **Port:** Enter the Port of the internet proxy.
- **Proxy Authentication:** Enter the credentials in case the Proxy requires authentication.
 - **Name:** Enter the user name for the proxy.
 - **Password:** Enter the password.

After configuring the necessary settings, click on **Save**.

View log

Click on this button, the Update window appears.

This window displays the latest activity report for the Update module.



The 'Update' window has a blue title bar with a colorful update icon and a close button. It contains a table with the following data:

File name	Date	File size
update.now.log	2022 06 06 10:46:44	123K

At the bottom, there are four buttons: 'View', 'Delete', 'Delete all', and 'Cancel'.

User can view and delete logs as per requirement.

Set Password

This module helps to set or modify the administrator password for accessing the eScan Linux GUI and password authentication during uninstallation of eScan.



The dialog box is titled "Set/Modify Password" and features a yellow key icon in the top-left corner. It contains two radio buttons: "Admin Password" (selected) and "Uninstall Password". Below these are three text input fields: "Enter old password", "Enter new password", and "Confirm new password". A checkbox labeled "Remove Password" is located to the right of the "Enter new password" field. At the bottom right, there are "Ok" and "Cancel" buttons.

Set Password

- **Admin Password:** Click this option, if you want to set the admin password to access eScan GUI.
- **Uninstall Password:** Click this option, if you want to set password to uninstall the eScan.

Enter old Password

To modify a password, it is mandatory to enter an old password.

Enter new Password

Enter the new password.

Confirm new Password

Re-enter the new password for confirmation.

Remove Password

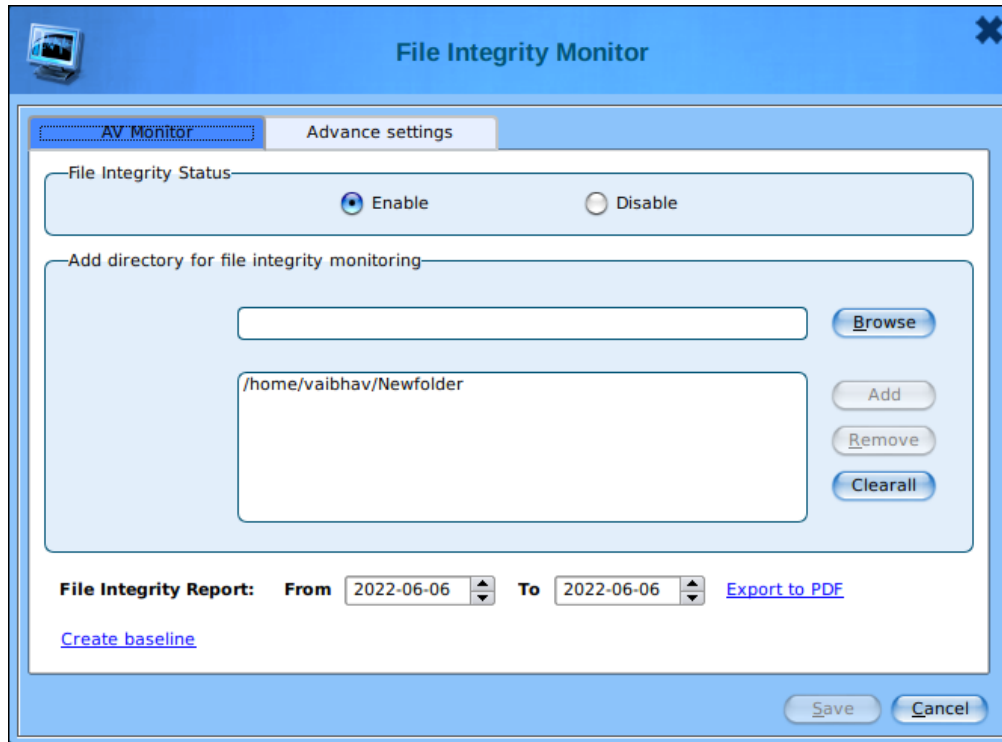
Select this checkbox to remove the existing password.

After filling all fields, click on **OK**.

The New password will be saved.

File Integrity Monitor

eScan's File Integrity Monitor (FIM) is an in-built control for Linux that monitors modifications in files using verification method between file's current state and original state to detect potential compromises. It alert and provide you report with changes has been monitored in the file.



AV Monitor

- **File Integrity Status**
 - Enable: Select this check box to enable the File Integrity Monitoring.
 - Disable: Select this check box to disable the File Integrity Monitoring.
- **Add the directory for the integrity monitoring**
 - To add the directory, click **Browse**.
Select directories to add watch window appears.
 - Select the directory.
 - You can also select the directory name from the pre-defined list in the below table.
 - To delete a specific directory, select the directory and click **Remove**.
 - To remove all the directory from monitoring at a time, click **Clear All**.
- **File Integrity Report:** eScan FIM also provides report that helps to detect the modifications/violations made in the file.
 - To generate a File Integrity Report, select the appropriate dates in **From** and **To** boxes and then click **Export to PDF**.
 - Select the appropriate path for PDF report, give file an appropriate name, and then click **Save**.
- **Create baseline:** This will create a baseline for the selected directories and the FIM will begin monitoring changes for the selected directories.

Advance Settings

This tab allows to configure the advanced settings for File Integrity Monitoring.

File integrity check alert

Select this checkbox to popup an alert, when any modification detect by the module.

Send the integrity monitor report daily

Select this checkbox to email the generated file integrity monitoring report to user on daily basis. The Mail settings section will be enabled after selecting this checkbox.

- **Mail settings:** It allows to configure the following options to send the monitoring report.
 - Recipient Email ID: Enter a valid recipient email id to whom, you want to send report.
 - Send daily report at (hh:mm): Set the time to send report daily at that time.
 - Sender Email ID: Enter a valid email id of the person who sending the report.
 - SMTP Server: Enter the SMTP server IP address.
 - SMTP Port: Enter the SMTP Port number.

If the SMTP server requires authentication, select **SMTP Authentication** check box and enter the login credentials.

- SMTP User: Enter the SMTP user name.
- SMTP Password: Enter the password.

After making necessary changes, click on **Save**.

Device Control

The Device Control module protects the computer from accessing the unauthorized portable storage devices. User can configure various options such as allowing/blocking of USB access and CD/DVD access, prompting for the password whenever USB is plugged in, and many more. The devices are also scanned immediately when connected to the endpoints to prevent any infected files running and infecting the system.



Following options are available under device control for configuration:

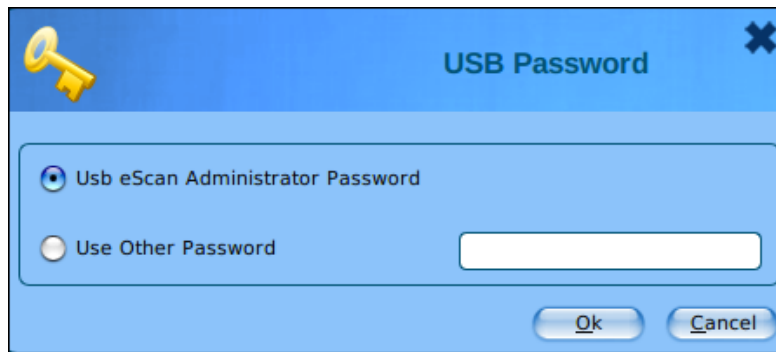
CD/DVD Control

This section allows to configure the settings for controlling access to CD/DVD.

- **Read Only:** This option allows only read-only access for CD/DVD.
- **Block:** This option blocks all CD/DVD access.
- **Disable:** This option disables the CD/DVD Control feature.

USB Control

- **Allow all:** This option allows the access to all connected USB storage devices except the ones that have been listed. For this option, the listed USB devices will be acting as black listed.
- **Block all:** This option blocks the access to all connected USB storage devices except the ones that have been listed. For this option, the listed USB devices will be acting as whitelisted.
- **Ask Password:** This option allows to set password to access the USB devices. After this option is enabled, eScan will prompt for password whenever a USB storage device is connected to the system. To set the password for USB device, select **Ask Password** option. User can either set a password or use the administrator password.



- **Use eScan Administrator password:** This option assigns eScan Administrator password for accessing USB storage device.
- **Use Other Password:** This option assigns a unique password for accessing USB storage device.
- **Disable:** This option disables the USB Control feature.

Refresh: Click this option to refresh the list of devices.

Add: To add device in the list, click **Add**.

Remove: To delete existing device from the list, click **Remove**.

Remove All: To delete all the devices from the list, click **Remove All**.

Monitor copy to USB

This option monitors the objects that are copied in the USB storage devices.

Autoscan USB

This option will scan USB devices as soon as it is connected to the system.

Log Level

Logs simply inform about the state of daemon, show critical messages, or warnings. User can get extensive log according to the value defined.

After setting the password, click on **Save**.

Web Control

The Web Control module is powered by advanced technologies that allow to manage the web access of the system during the online activities. It prevents the browsers from accessing the malicious/phishing websites.

The screenshot shows the 'Web Control' window with the following elements:

- Mode Selection:** Three radio buttons at the top: 'Allow all' (selected), 'Block all', and 'Disable'.
- Category List:** A table with three columns: Category, Status, and Action.

Category	Status	Action
Pornography	Block	Block ▼
Gambling	Block	Block ▼
Alcohol	Allow	Allow ▼
Violence	Block	Block ▼
Drugs	Block	Block ▼
- Sites Section:** A large empty text area labeled 'Sites :'. Below it are 'Add' and 'Delete' buttons.
- Log Level:** A dropdown menu set to '4'.
- Alerts:** A checked checkbox for 'Show Alert', followed by 'Save' and 'Cancel' buttons.

- **Allow all:** This option allows full access to all the websites except those categories which are added in Block status. By default, this option is enabled.
- **Block all:** This option blocks all the websites except those categories which are added in Allow status.
- **Disable:** This option disables the Web Control feature.

Add: To add category of website, click **Add**.

Delete: User can delete the category of website using this option.

Site

This section adds the website names. In this section, add a list of websites that do not belong to the category. You can also add and delete websites depending on your requirements.

Log Level: Log simply informs about the state of daemon, critical messages or warnings. User can get extensive log according to the value set.

Show Alert: It will show alert when websites get blocked.

After making necessary changes, click on **Save**.

Firewall

Firewall is designed to monitor all incoming and outgoing network traffic and protect your system from all types of network attacks. When you connect to the Internet, you expose your device to various security threats. 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 system and network. Therefore, the firewall first checks the rules, analyzes network packets, and then filters them on the basis of specified rules. 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.



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.
- **Filtration System:** This option shows the filtration mode used by Firewall module.

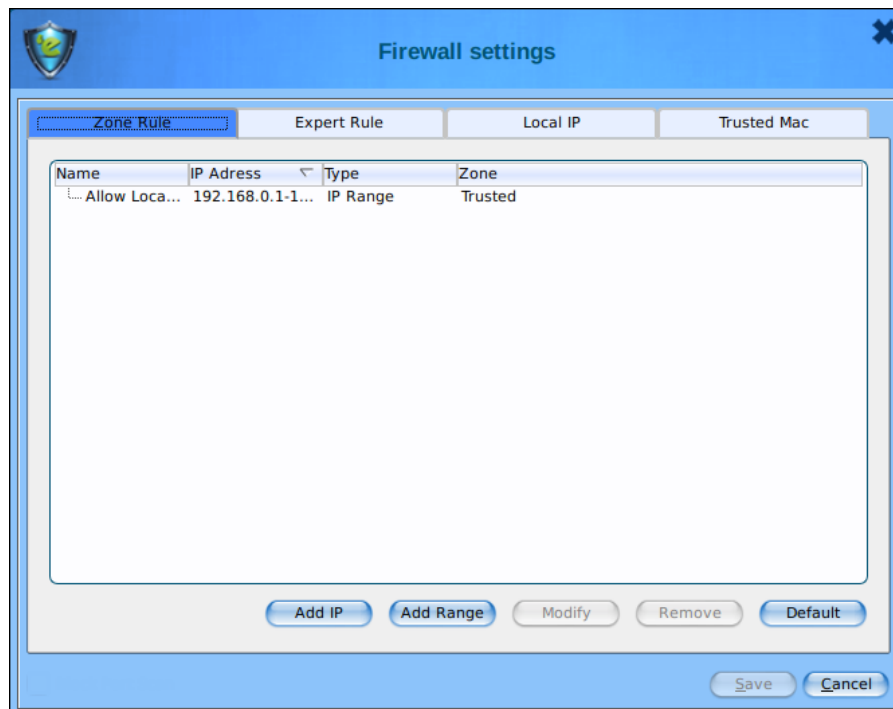
Modes that are available are as follows:

- **Allow All:** This mode allows all the incoming and outgoing network traffic. By default it is selected.
- **Limited Filter:** When this mode is enabled, it monitors all incoming traffic and helps you to allow or block traffic as per the defined conditions or rules.
- **Interactive Filter:** It needs user intervention. It monitors all the incoming and outgoing network traffic and allows or blocks traffic as per configured conditions or rules.
- **Block All:** This mode blocks all the incoming and outgoing network traffic.
- **Settings:** You can configure the firewall setting here.

When you click this option, the Firewall Settings window appears. By default, **Zone Rule** tab appears.

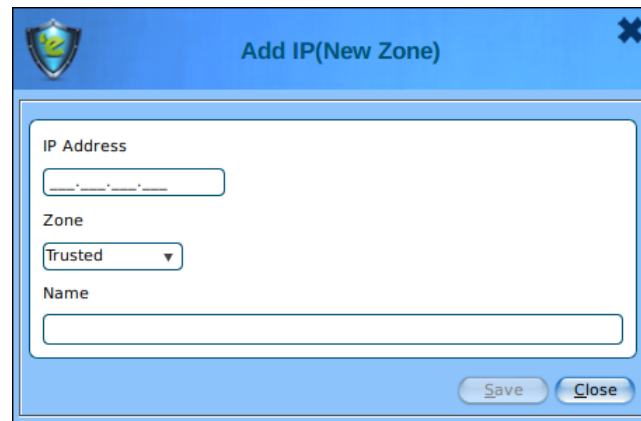
Zone Rule

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



This tab includes the following buttons:

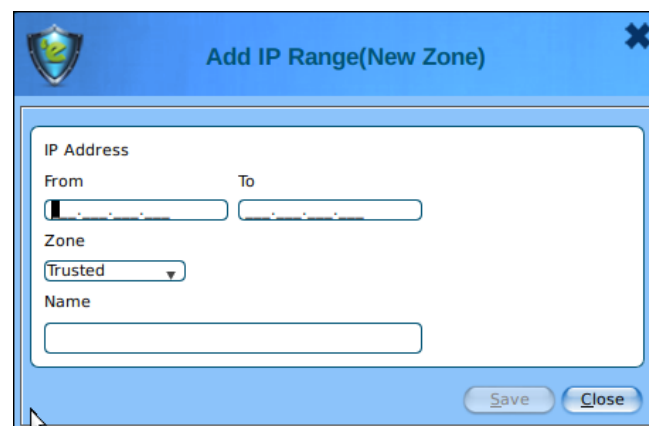
- **Add IP:** This button is used to add a zone rule for a given IP address. To add the zone rule, you must need to provide an IP address for which you are adding the zone rule. Select the type of zone, whether it is **Trusted** or **Blocked** and specify name for the zone rule.



The dialog box titled "Add IP(New Zone)" has a blue header with a shield icon on the left and a close button on the right. The main area contains three fields: "IP Address" with a text input box, "Zone" with a dropdown menu showing "Trusted", and "Name" with a text input box. At the bottom right are "Save" and "Close" buttons.

After entering all details click on **Save**.

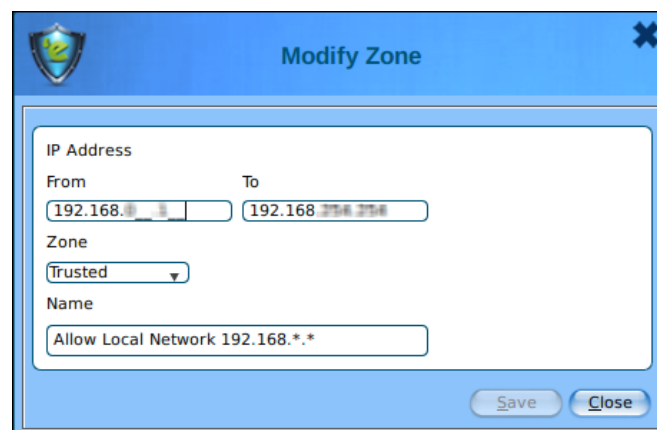
- **Add IP Range:** This button is used to add a zone rule for a range of IP addresses. To add the zone rule, you must need to provide the range of IP address for which you are adding the zone rule, **start IP address** and **end IP address** in the range. Select the type of zone, whether it is **Trusted** or **Blocked** and specify name for the zone rule.



The dialog box titled "Add IP Range(New Zone)" has a blue header with a shield icon on the left and a close button on the right. The main area contains four fields: "IP Address" with "From" and "To" sub-labels and two text input boxes, "Zone" with a dropdown menu showing "Trusted", and "Name" with a text input box. At the bottom right are "Save" and "Close" buttons.

After entering all details click on **Save**.

- **Modify:** This button is used to modify zone rules related to the IP address, or range of IP addresses which is already added in the list.



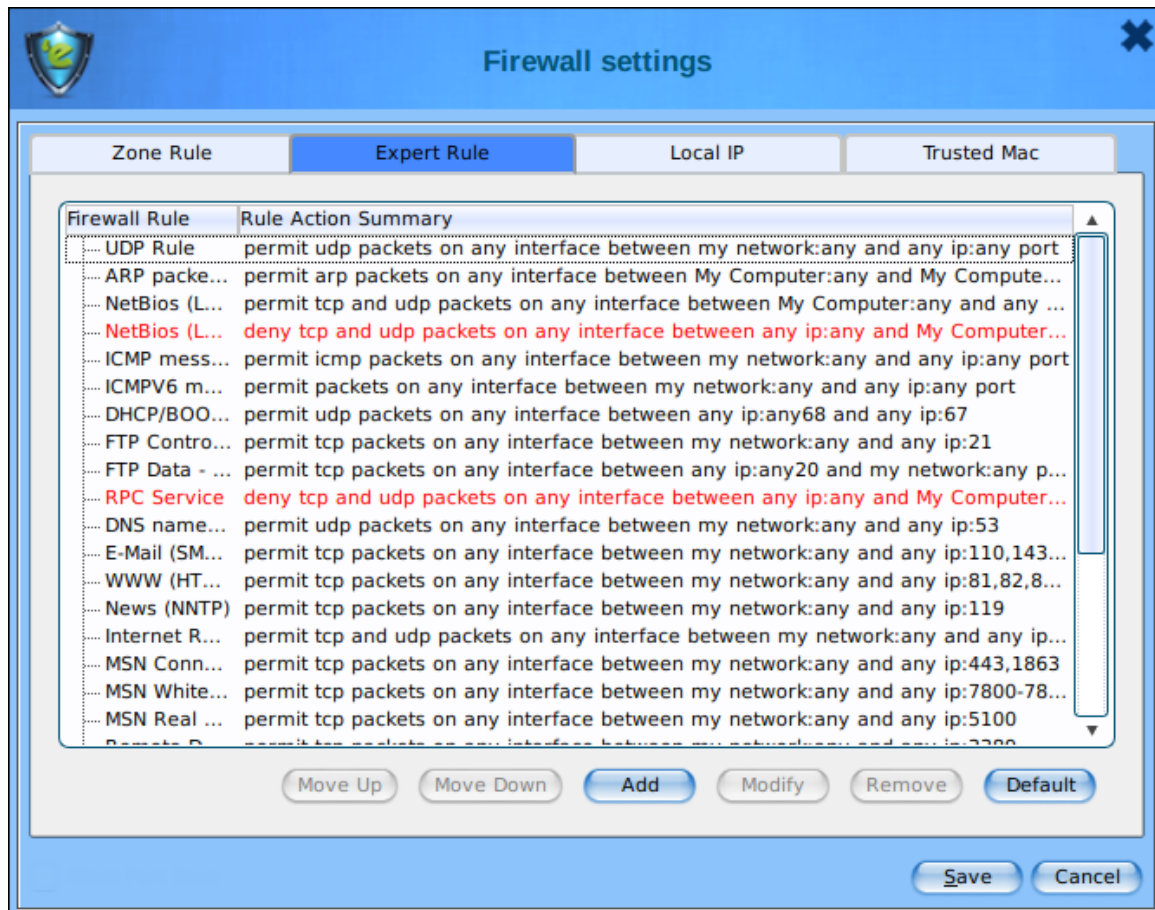
The dialog box titled "Modify Zone" has a blue header with a shield icon on the left and a close button on the right. The main area contains four fields: "IP Address" with "From" and "To" sub-labels and two text input boxes containing "192.168.0.0" and "192.168.255.255", "Zone" with a dropdown menu showing "Trusted", and "Name" with a text input box containing "Allow Local Network 192.168.*.*". At the bottom right are "Save" and "Close" buttons.

After making necessary changes, click on **Save**.

- **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. In addition, you can create new expert rules. However, you should configure these rules only if you have a good understanding of firewall and networking protocols.



- **Move Up:** This button moves the selected rule in upward direction as per requirement.
- **Move Down:** This button moves the selected rule in downward direction.
- **Add:** This button adds new rule. To learn more, [click here](#).
- **Modify:** This button modifies the existing rule in the list.
- **Remove:** This button removes the existing rule from the list.
- **Default:** This button resets the all the configuration to default values.

Adding new rule

1. Click on **Add** button.
Add Firewall Rule window appears.

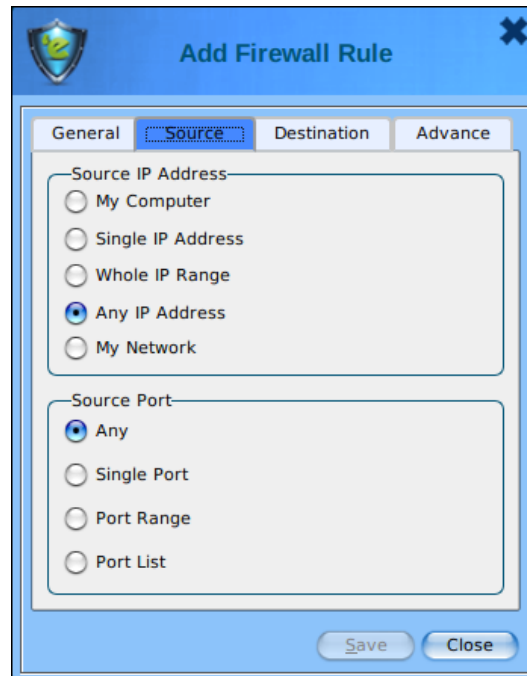
General

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

- **Rule Name:** Enter the rule name.
- **Rule Action:** Click any one of the following types of actions for setting rules.
 - **Permit Packet:** This option allows you to permit packets and is selected by default.
 - **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.
- **Apply Rule on Interface:** This option lets you to select interface to apply the rule. By default, **Any Interface** is selected.

Source

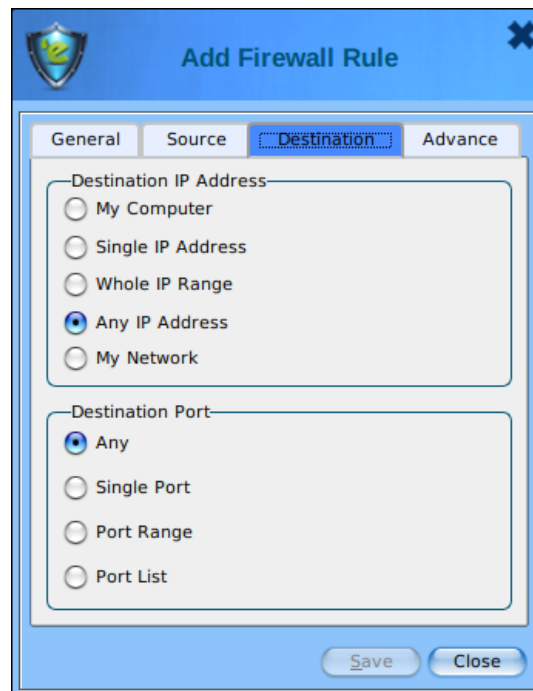
This tab enables you to select the type of source IP address and port wherever applicable. You can select the appropriate option. By default, **Any IP Address** under **Source IP Address** section and **Any** under **Source Port** section are selected.



The screenshot shows the 'Add Firewall Rule' dialog box with the 'Source' tab selected. The 'Source IP Address' section has five radio button options: 'My Computer', 'Single IP Address', 'Whole IP Range', 'Any IP Address' (which is selected), and 'My Network'. The 'Source Port' section has four radio button options: 'Any' (which is selected), 'Single Port', 'Port Range', and 'Port List'. At the bottom right, there are 'Save' and 'Close' buttons.

Destination

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



The screenshot shows the 'Add Firewall Rule' dialog box with the 'Destination' tab selected. The 'Destination IP Address' section has five radio button options: 'My Computer', 'Single IP Address', 'Whole IP Range', 'Any IP Address' (which is selected), and 'My Network'. The 'Destination Port' section has four radio button options: 'Any' (which is selected), 'Single Port', 'Port Range', and 'Port List'. At the bottom right, there are 'Save' and 'Close' buttons.

Advance

This tab is specifically meant for ICMP processing, the fields on this tab are available only when you select ICMP from **Protocol** drop-down list, under **General** tab.

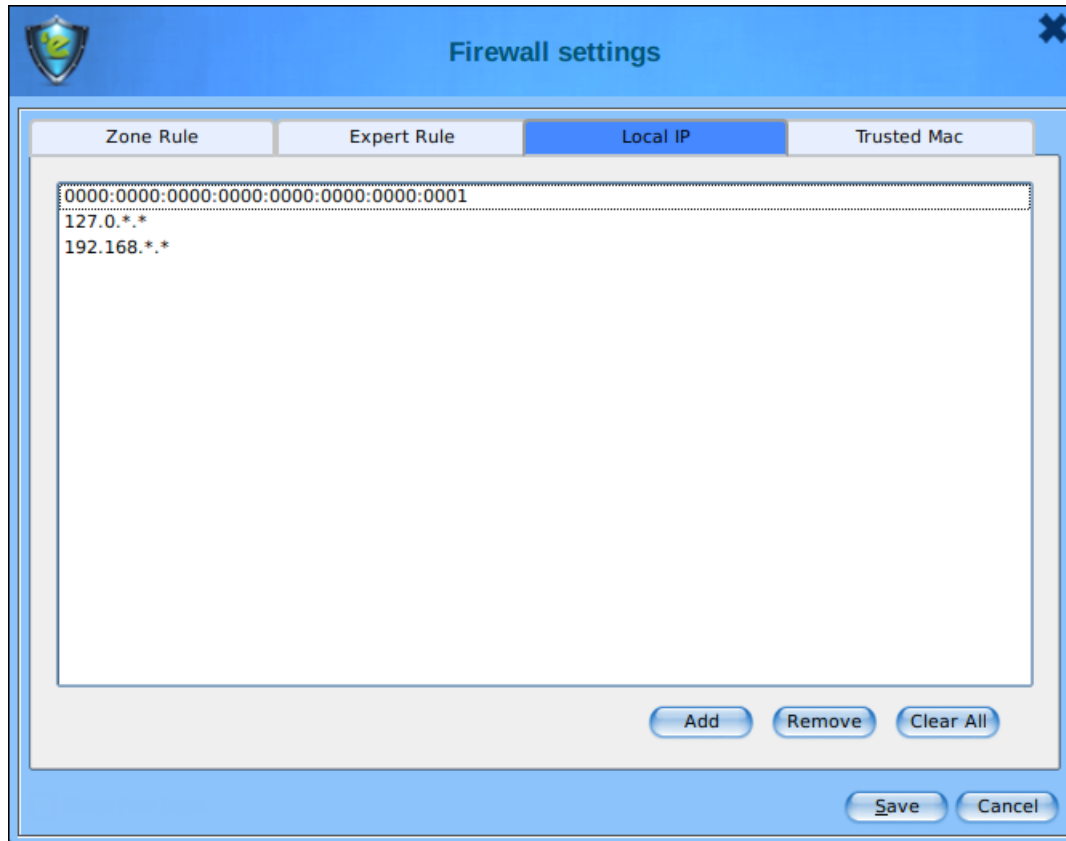
If user wants **Enable Advance ICMP Processing**, select the checkbox. From the given list of ICMP type, select IN and OUT option accordingly. When **The Packet Must Be From/To Trusted MAC** checkbox is selected, the rule will be applied on the all MAC address excluding addresses defined/listed in the Trusted MAC Address tab.

ICMP Type	IN	OUT
Destination Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Echo Reply(ping)	<input type="checkbox"/>	<input type="checkbox"/>
Echo Reques(ping)	<input type="checkbox"/>	<input type="checkbox"/>
Parameter Problem	<input type="checkbox"/>	<input type="checkbox"/>
Redirect	<input type="checkbox"/>	<input type="checkbox"/>
Source Quench	<input type="checkbox"/>	<input type="checkbox"/>
TTL Exceeded	<input type="checkbox"/>	<input type="checkbox"/>

After configuring all the tab according to your need, click on **Save** to add the new rule. It will be added in the list.

Local IP

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.



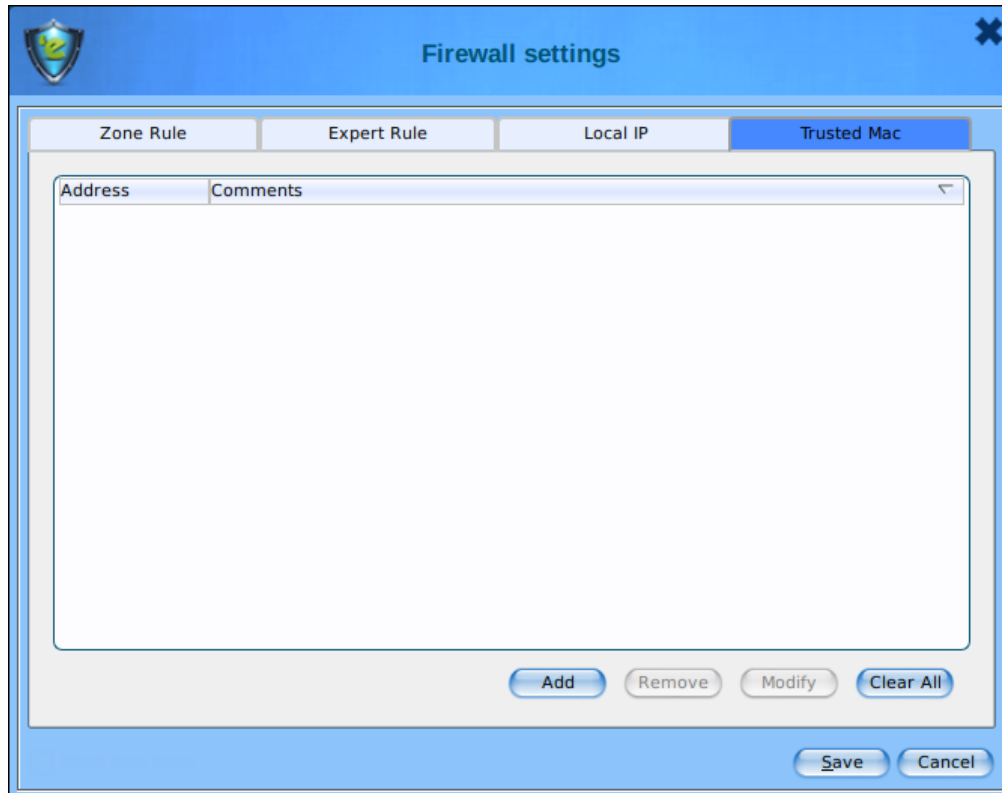
- **Add:** You can add new IP address using this button. Once this button is clicked, **New IP Address** dialogue box appears. Enter the **IP Address** in this dialogue box and click **Save**.



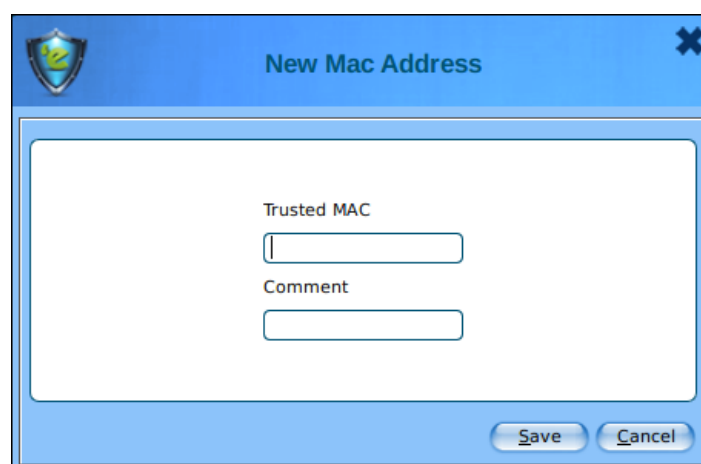
- **Remove:** This button removes the existing individual IP entries from the list.
- **Clear All:** This button clears all the IP addresses in the list.

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.



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

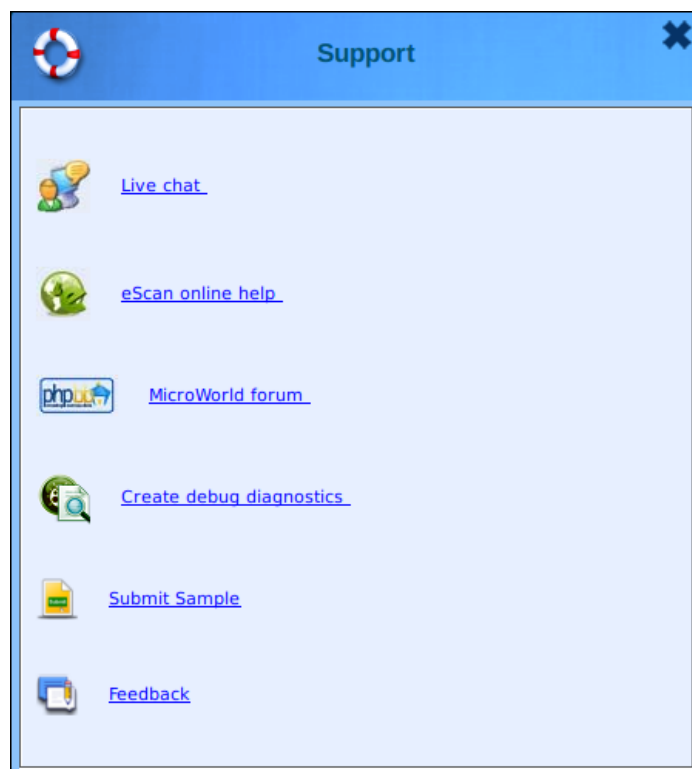


- **Remove:** This button removes the individual existing Mac entry from the list.
- **Modify:** This button edits the existing entries in the list.
- **Clear All:** This button clears all the Mac addresses in the list.

After making all the configuration, click on **Save**.

Support

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



Live chat

To work this feature user need an active internet connection. User can contact eScan 24 x 7 online technical support team through chat either by clicking the **Live Chat** button or by visiting the following link:

<http://www.eScanav.com/english/livechat.asp>

eScan online help

For using this feature user need to have active internet connection. It is present on the eScan wiki and provides with comprehensive information about products and features of eScan. User can visit eScan online help pages either by clicking the **eScan Online Help** button or by visiting the following link:

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

MicroWorld forum

For using this feature user should have active internet connection. This link helps to join the MicroWorld forum and read the discussion threads on MicroWorld. User can visit MicroWorld Forum pages either by clicking the **MicroWorld Forum** button or by visiting the following link:

<http://forum.escanav.com/>

Create debug diagnostics

This link is used to generate debug file (ZIP file consisting of logs, configurations, and more) that can be used for troubleshooting. The debug file can be sent to eScan team for further analysis in case of any technical issue or suspicious activity.

Submit Sample

This option allows the user to submit the virus samples to the eScan support team. Click on **Submit Sample** link, to upload the virus samples. Click on given link, a new web page opens, where user have to click **Samples** option, and then click **Next >>** button. Fill up the details in the ticket form, and then click **Submit** button. User can also use the following link:

<http://support.mwti.net/support/index.php?/Tickets/Submit>

Feedback

You can always send your feedback to us for improvement, click on the **Feedback** link or visit the following link; you will be redirected to our online feedback form. Please fill and submit.

<https://www.escanav.com/english/content/company/feedback/>

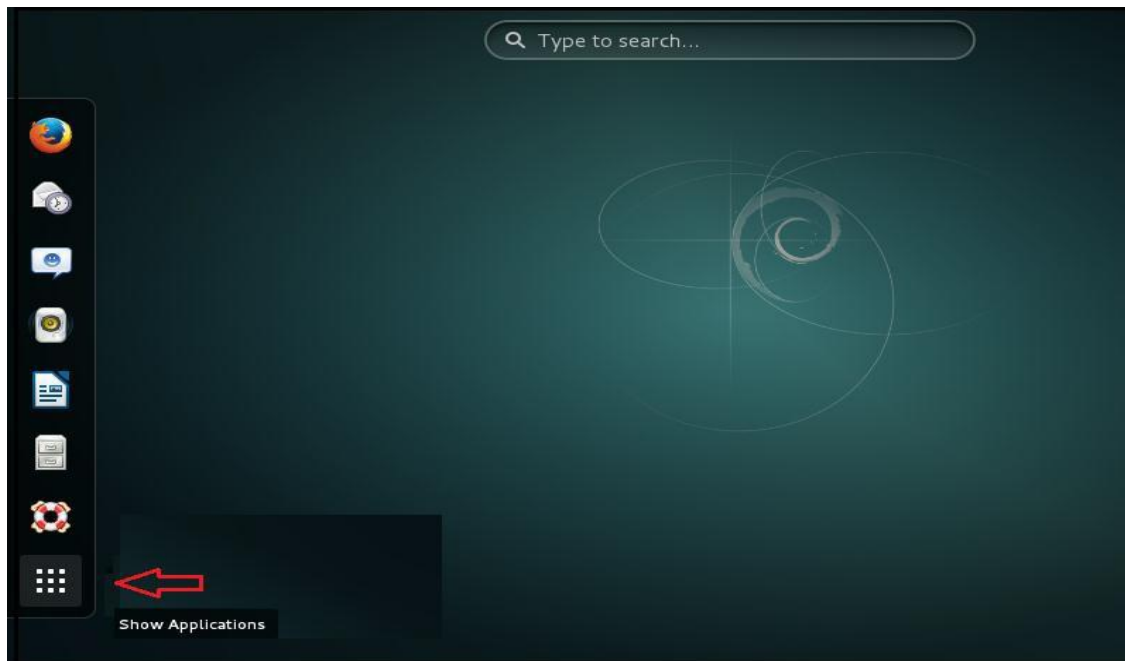
License

After installing eScan Anti-Virus Linux for Desktop, register the product within the 30 days of trial period. Follow any of the two methods for registration process:

- **Online Registration Process**
- **Offline Registration Process**

Online Registration Process

1. On home screen, click **Activities** > **Show Applications**.



2. Click **eScan GUI**.



The Authentication Required prompt appears.

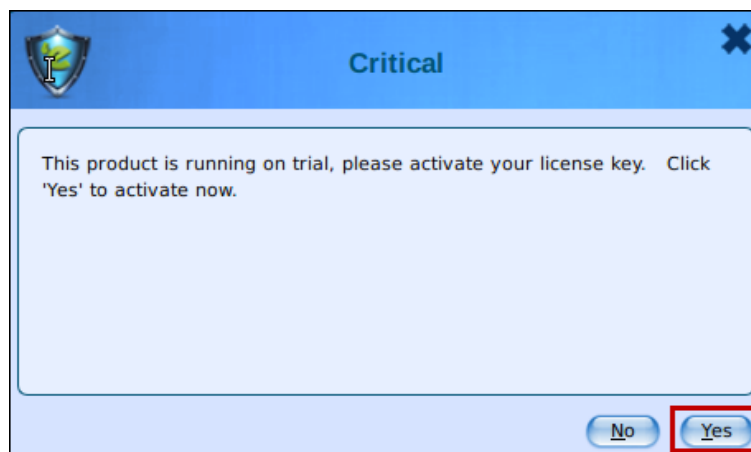


3. In the **Password** textbox, enter the authentication password and then click **Authenticate**.

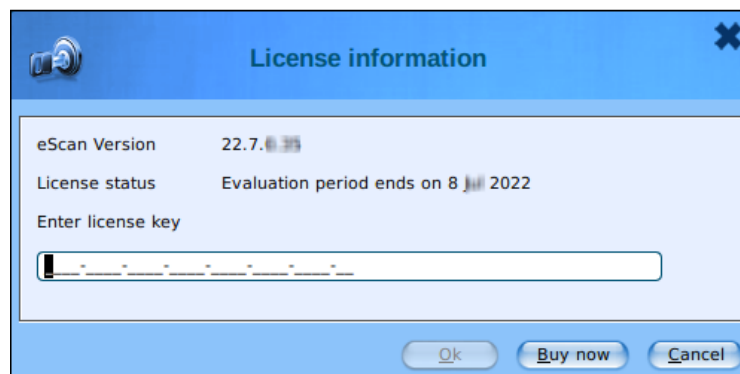
NOTE

The **Authenticate** button will get enabled only after entering the correct authentication password.

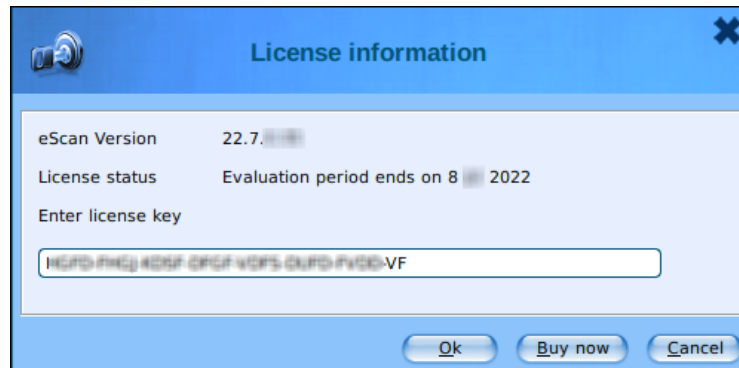
After clicking Authenticate, the Critical window appears displaying the product activation message.



4. To proceed with the product activation, click **Yes**.
The License Information prompt appears.



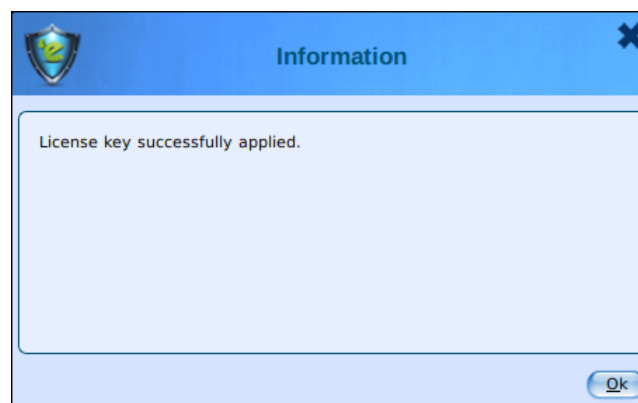
5. Enter the 30-character license key and then click **OK**.



NOTE

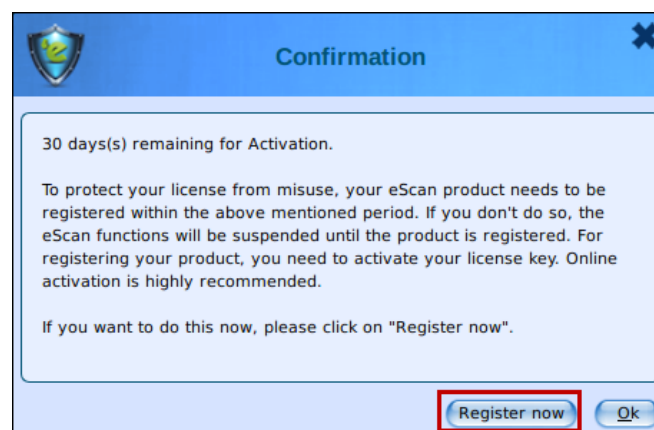
Click on **Buy now** option, if user does not have license key.

After entering the correct license key, a success message appears.



6. Click **OK**.

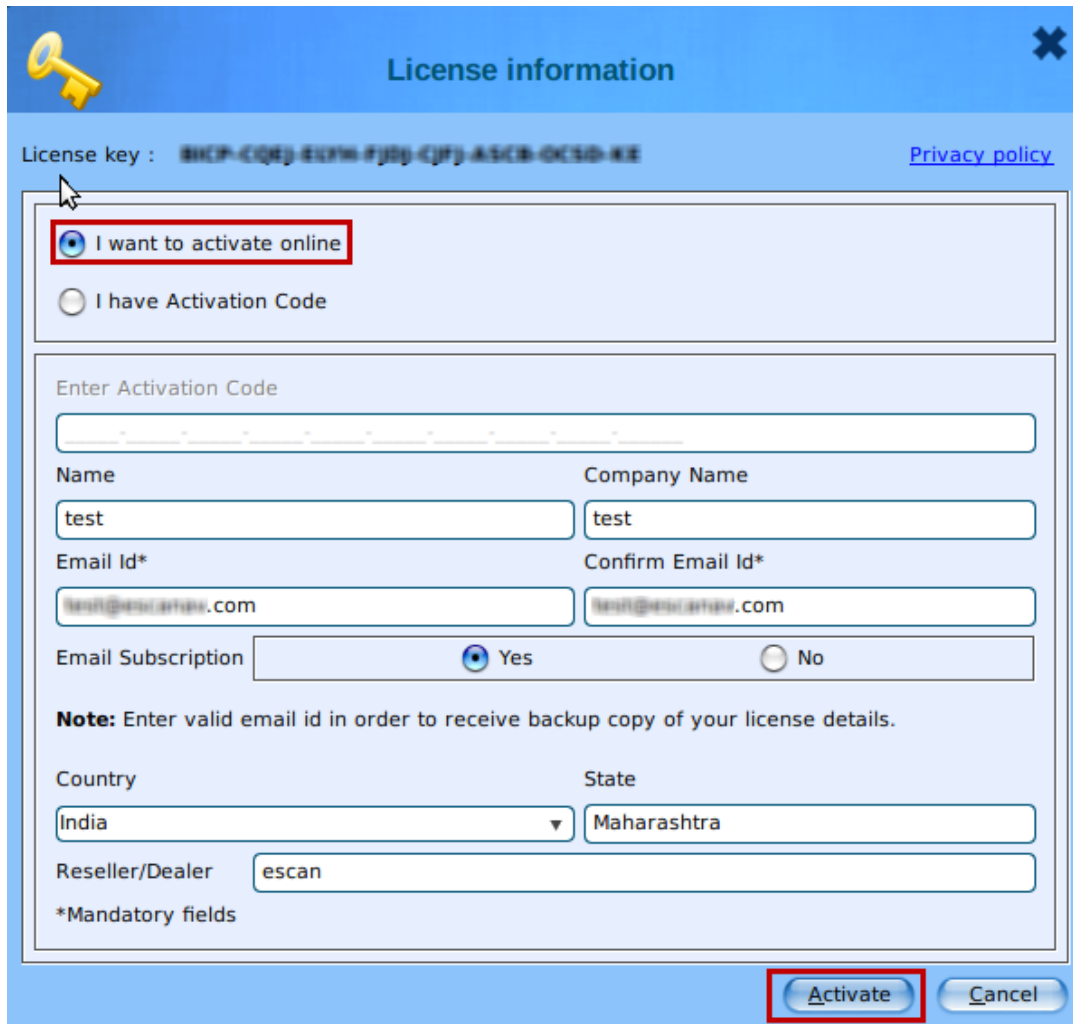
The Confirmation prompt appears displaying the product registration message.



NOTE

Registering the product within the activation period allows us to send important updates and provide tech support quickly. Also, it protects the license from being misused.

7. To proceed with the registration, click **Register Now**.
The License Information window appears displaying the registration form.



The image shows a 'License information' window with a blue header and a yellow key icon. The window contains a 'License key' field with a value, a 'Privacy policy' link, and two radio buttons: 'I want to activate online' (selected) and 'I have Activation Code'. Below these are input fields for 'Enter Activation Code', 'Name', 'Company Name', 'Email Id*', and 'Confirm Email Id*'. There is also an 'Email Subscription' section with 'Yes' and 'No' radio buttons. A note states: 'Note: Enter valid email id in order to receive backup copy of your license details.' At the bottom, there are 'Country' and 'State' dropdown menus, a 'Reseller/Dealer' text field, and an '*Mandatory fields' label. The 'Activate' button is highlighted with a red box.

License key : **BHCP-CQEQ-EU7M-FJBJ-CJFY-ASCB-OCSD-EE** [Privacy policy](#)

☒ I want to activate online
☐ I have Activation Code

Enter Activation Code

Name Company Name

Email Id* Confirm Email Id*

Email Subscription ☒ Yes ☐ No

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

Country State

Reseller/Dealer

*Mandatory fields

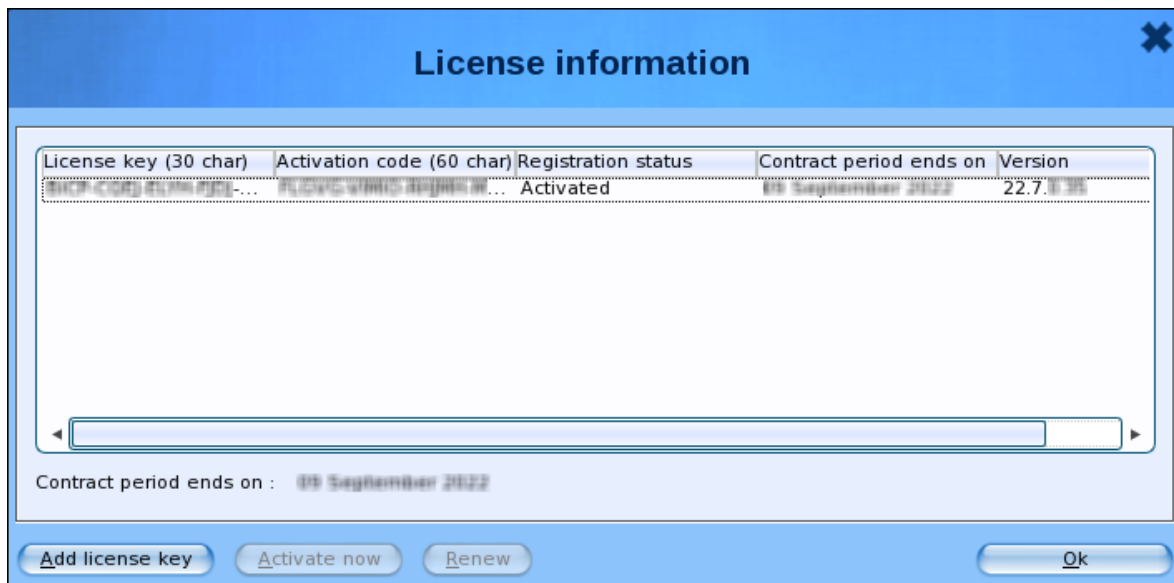
Activate **Cancel**

8. Select the option **I want to activate online** and fill the registration form.
9. After filling the registration form, click **Activate**.

The eScan application connects with the main eScan server to register the product.

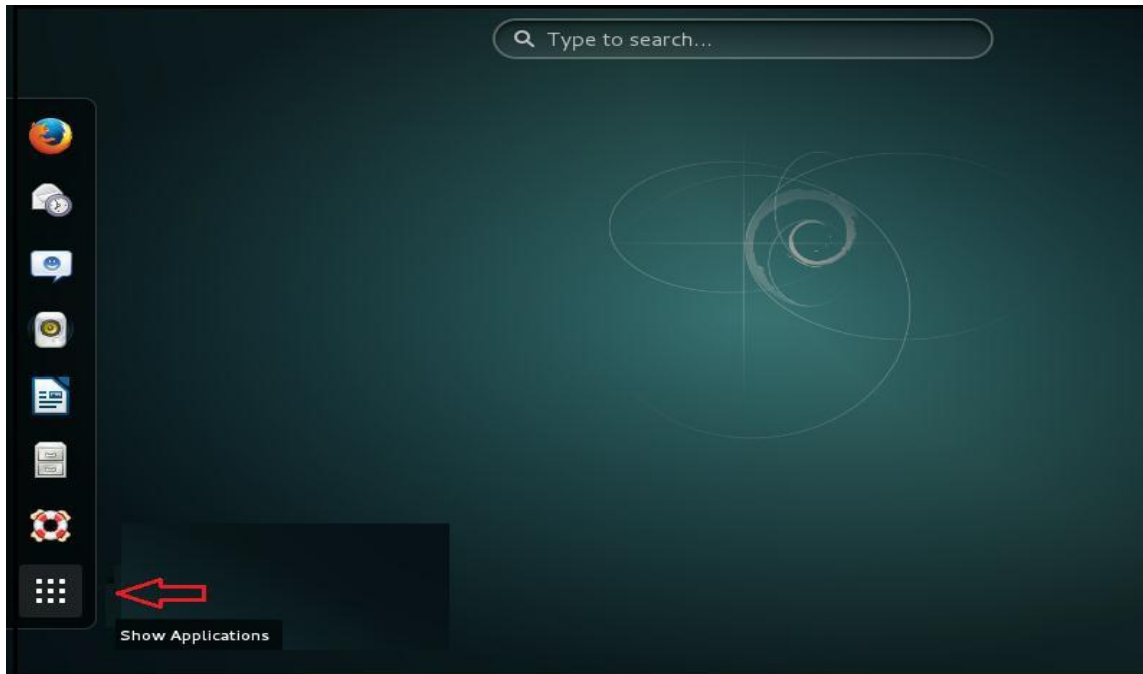
After the successful activation the License Information window appears displaying the following activation details:

- License key
- Activation code
- Registration status
- Contract Expiry Date
- Product Version



Offline Registration Process

1. On home screen, click **Activities** > **Show Applications**.



2. Click **eScan GUI**.



The Authentication Required prompt appears.

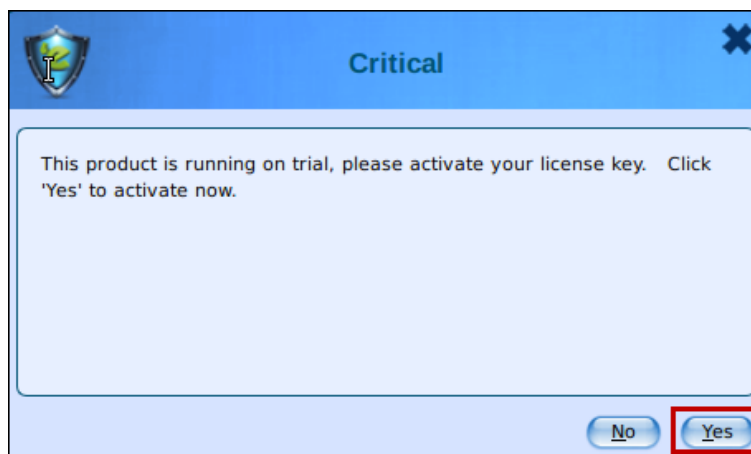


3. In the **Password** textbox, enter the authentication password and then click **Authenticate**.

NOTE

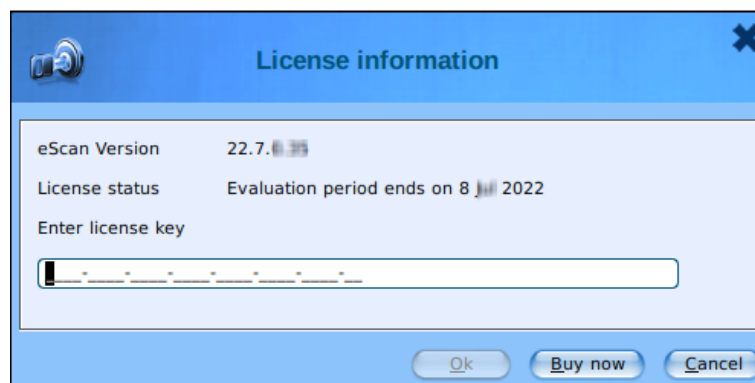
The **Authenticate** button will get enabled only after entering the correct authentication password.

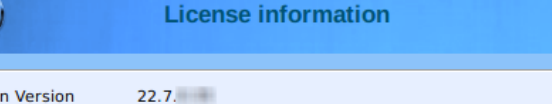
After clicking Authenticate, the Critical window appears displaying the product activation message.



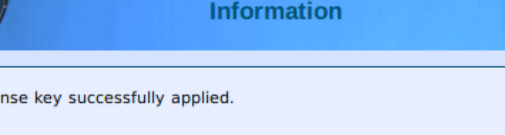
4. To proceed with the product activation, click **Yes**.

The License Information window appears.

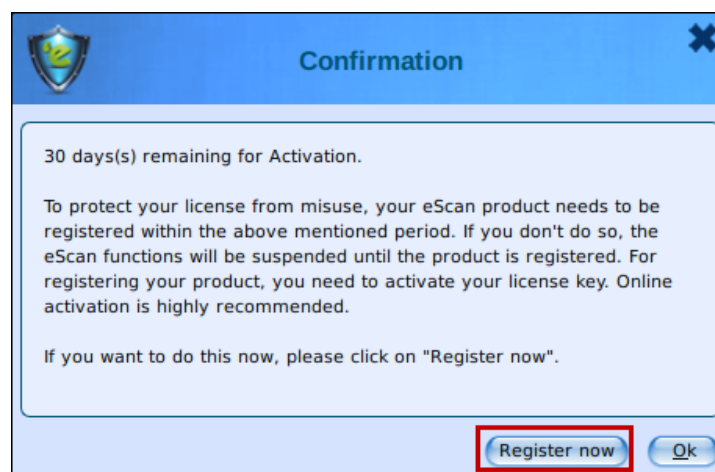


- 
- License information**
- eScan Version 22.7
- License status Evaluation period ends on 8 2022
- Enter license key
- HCRP-PMQJ-KDGF-GRCF-VGRS-QURD-FYGB-VF
- Ok Buy now Cancel

Click on **Buy now** option, if user does not have license key.

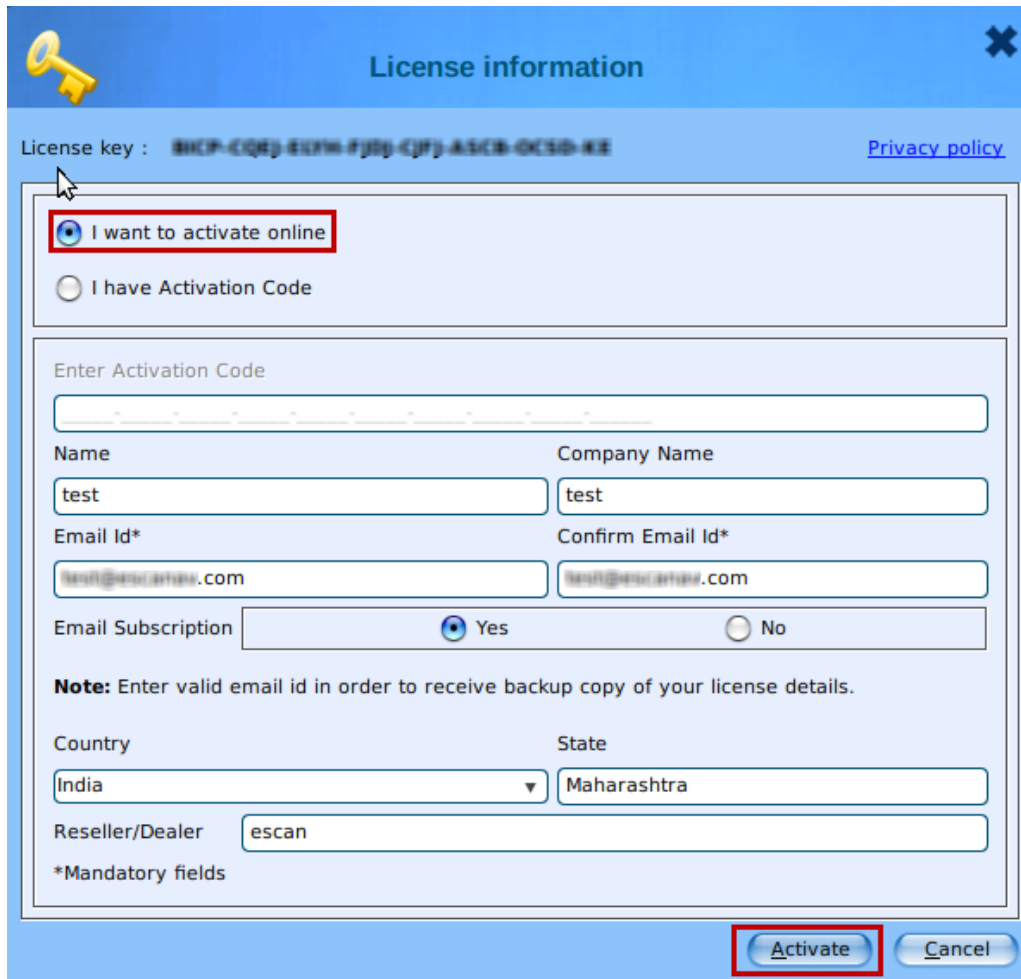


- The Confirmation window appears displaying the product registration message.



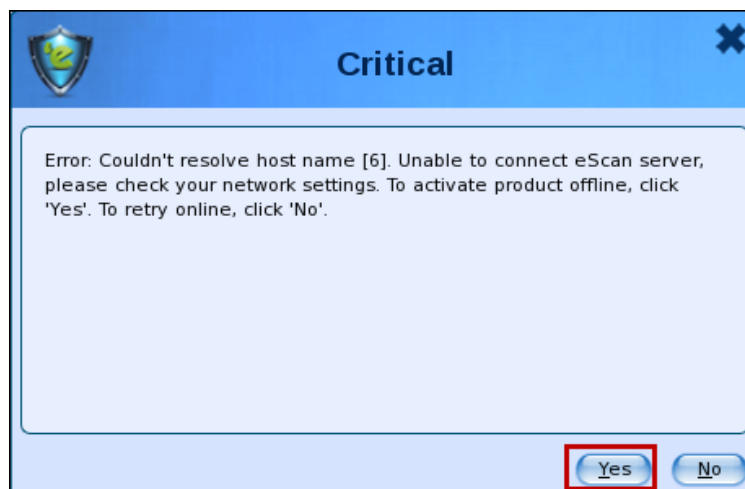
Registering the product within the activation period allows us to send important updates and provide tech support quickly. Also, it protects your license from misuse.

7. To proceed with the registration, click **Register Now**.
The License Information window appears displaying the registration form.



The 'License information' window is displayed with a blue header and a yellow key icon. It contains a license key, a privacy policy link, and two radio buttons for activation. The 'I want to activate online' option is selected and highlighted with a red box. Below this is a section for entering an activation code, followed by fields for Name, Company Name, Email Id*, and Confirm Email Id*. The 'Email Subscription' section has 'Yes' selected. A note states: 'Enter valid email id in order to receive backup copy of your license details.' Below this are dropdowns for Country (India) and State (Maharashtra), and a text field for Reseller/Dealer (escan). A footer note indicates '*Mandatory fields'. At the bottom right, the 'Activate' button is highlighted with a red box, next to a 'Cancel' button.

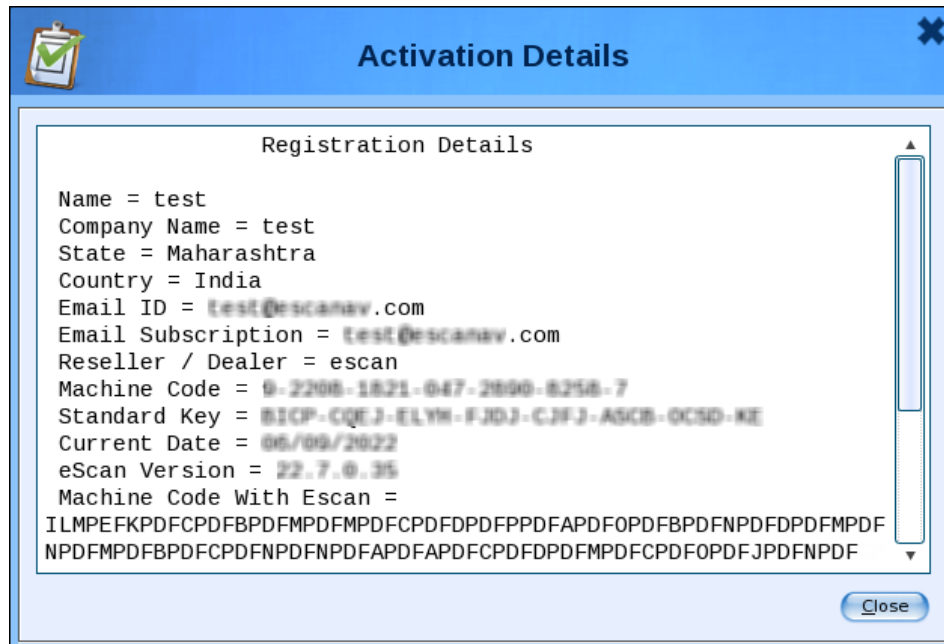
8. Select the option **I want to activate online** and fill the registration form.
9. After filling the registration form, click **Activate**.
If the internet connection isn't active, the Critical window appears.



The 'Critical' window has a blue header with a shield icon. The message reads: 'Error: Couldn't resolve host name [6]. Unable to connect eScan server, please check your network settings. To activate product offline, click 'Yes'. To retry online, click 'No'.' At the bottom right, the 'Yes' button is highlighted with a red box, next to a 'No' button.

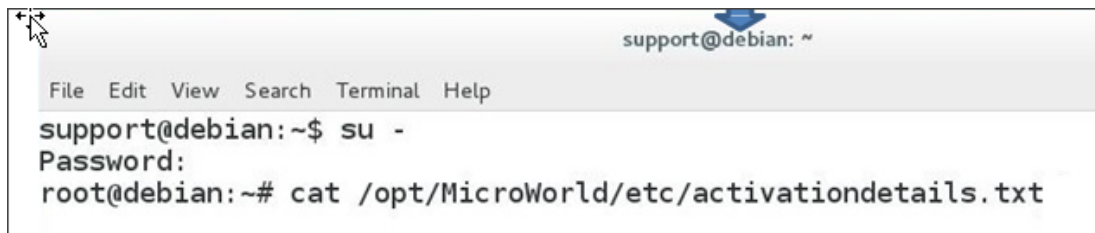
10. To activate product offline, click **Yes**.

Activation Details window appears displaying the registration details.



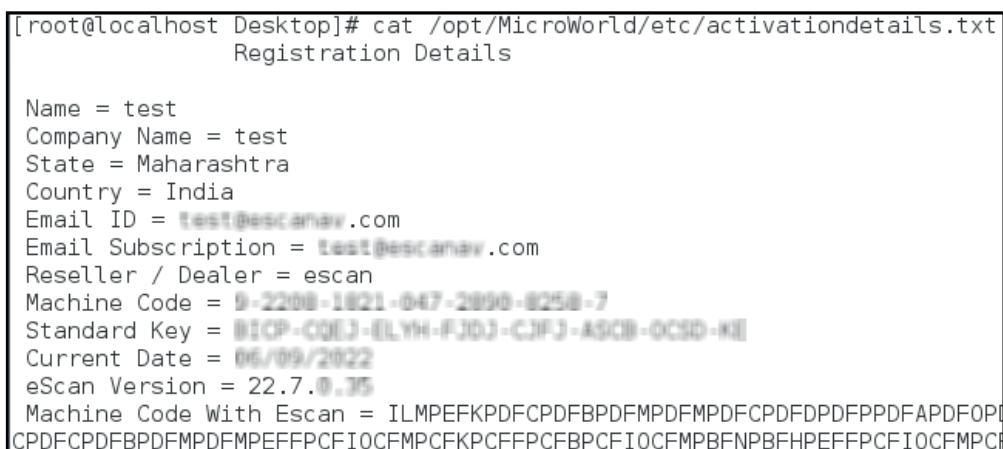
The details submitted in the activation form gets composed in the **activationdetail.txt** file.

This txt file can be found at the following path.




To register the product, send us an email with the activationdetail.txt file as an attachment.

The eScan team will send a reply email containing 60-digit activation code.



11. Go to the License Information window, select the option **I have Activation Code**. In the **Enter Activation Code** box, enter the 60-digit activation code and then click **Activate**.



License information

License key : **8HCP-CQ8J-8U7W-FJ8J-CJ7J-ASCB-0CS8-8E**[Privacy policy](#)

☐ I want to activate online

☒ I have Activation Code

Enter Activation Code

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Name

test

Company Name

test

Email Id*

test@escan.com

Confirm Email Id*

test@escan.com

Email Subscription

☒ Yes ☐ No

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

Country

India

State

Maharashtra

Reseller/Dealer

escan

*Mandatory fields

Activate

Cancel

After the successful activation the License Information window appears displaying the following details:

- License key
- Activation code
- Registration status
- Contract Expiry Date
- Product Version

License information

License key (30 char)	Activation code (60 char)	Registration status	Contract period ends on	Version
BWCP-CHG-DLTP-RPT-...	RLEPC-WHMS-NRPM-A...	Activated	09 September 2022	22.7.1.35

Contract period ends on : 09 September 2022

Add license keyActivate nowRenewOk

Contact Us

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

Before contacting technical support team, ensure that the system meets all the requirements and 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.

Ensure that the following information is available, while contacting technical support:

- Endpoint hardware specifications
- Product version in use and patch level
- Network topology and NIC information
- Gateway, IP address and router details
- List of hardware, software and network changes if any carried out
- Step-by-step description of error/situation
- Step-by-step description of troubleshooting if any attempted
- Screenshots, error messages and log/debug files

In case the Technical Support team, requires to take a remote connection:

- IP address and login credentials of the system will be needed.

Forums

Join the [Forum](#) to discuss eScan related problems with experts.

Chat Support

The eScan Technical Support team is available round the clock for assisting with all the queries via [Live Chat](#).

Email Support

For any queries, suggestions and comments regarding our products or this User Guide, write to us at <mailto:support@escanav.com>