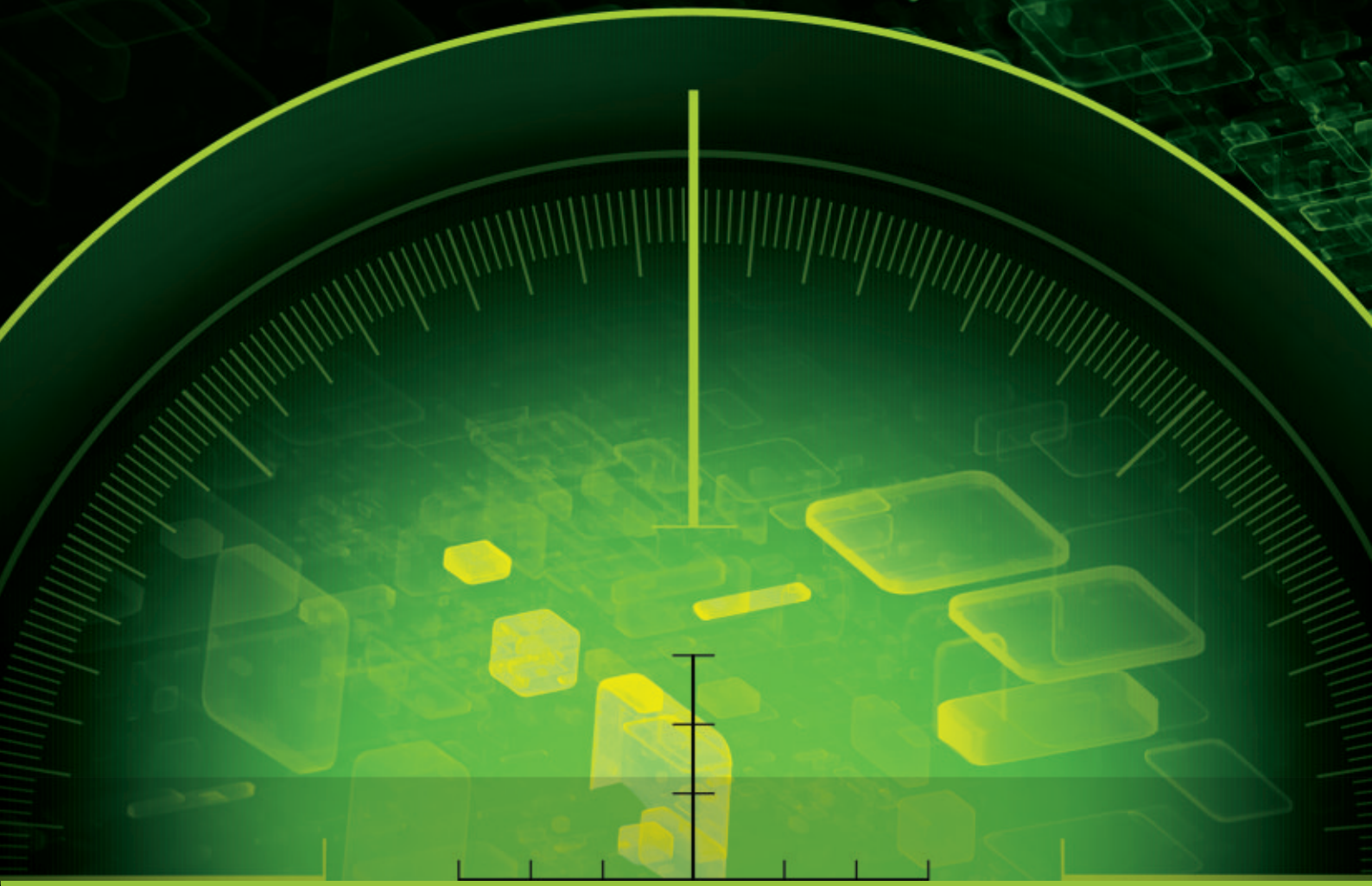
eScan™

Anti-Virus & Content Security

eScan Corporate 360

(with MDM & Hybrid Network Support)

User Guide



Document Number: 5BUG/18.11.2015/14.1
Current Software Version: 14.1

Technical Support:	**support@escanav.com**
Sales:	**sales@escanav.com**
Forums:	http://forums.escanav.com
eScan Wiki:	http://www.escanav.com/wiki
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld
Date:	December, 2015

Table of Contents

1. eScan Management Console

It is a web based centralized Management Console that helps the administrator to install and manage eScan Client on the computers connected to the network.

Using this console you can perform following activities –

- Install eScan Client application on the Computers connected to the network that have Windows, Mac or Linux Operating System.
- Monitor the Security Status of the computers connected to the network in the organization.
- Create and Manage policies or tasks for computers on your network.
- Create and View customized reports of the Security Status of the computers.
- Manage Notifications for Alerts and Warnings.

2. Pre-requisites for eScan Server

Before installing eScan ensure that the following pre-requisites are met:

- Log on to computer as an administrator.
- Uninstall the existing anti-virus software, if any.
- Check for free space on the hard disk/partition for installing eScan.
- The IP address for eScan server should be static.
- Determine IP address of the mail server to which you need to send the warning messages (optional).

Note:
• You require a user name and password to send emails, if authentication for the mail server is mandatory for accepting emails.

- **System Requirements**

Windows	Linux	Mac	Android
1. (Windows server & workstations) 2. Platforms Supported Microsoft® Windows® 2012 R2 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-Bit & 64-Bit Editions)	1. (Linux Endpoints) 2. 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)	1. (Mac Endpoints) 2. Platforms Supported Mac OS X 10.9 – Mavericks Mac OS X 10.8 - Mountain Lion Mac OS X 10.7 - Lion Mac OS X 10.6 – Snow Leopard	1. (Android Endpoints) 2. Platforms Supported Android Version 2.3 OS & above; Cyanogen OS 12.0
Hardware for Clients and Server (Server) CPU: 2GHz Intel™ Core™ Duo processor or equivalent Memory: 4 GB & above Disk Space: 8 GB & above (Endpoints): 1.4 Ghz minimum (2.0 Ghz recommended) Intel Pentium or equivalent 1.0 GB minimum (1.5 GB recommended) Disk space : 800 MB and more	**Hardware Requirements (Endpoints)** CPU - Intel® Pentium or compatible or equivalent. Memory – 512 MB and above Disk Space – 500 MB free hard drive space for installation of the application and storage of temporary files	**Hardware Requirements (Endpoints)** CPU - Intel based Macintosh Memory – 1 GB and More recommended Disk Space – 500 MB and above	**Hardware Requirements (Endpoints)** Minimum Storage requirement – 10-15 MB (with updates)
eScan Console can be accessed by using below browsers: Internet Explorer 7 / 8 / 9 / 10 Firefox 14 & above Google Chrome latest version Google Chrome latest version			

3. Installing eScan Corporate 360 Server

- **Installing eScan from CD/DVD**

  Installing eScan Corporate 360 from the CD/DVD is very simple, just insert the CD/DVD in the ROM and wait for few seconds for auto run to start the installation process and follow the instructions on screen. In case if installation does not start on its own then locate and double click on the MDMcwn2k3ek on CD Rom, this will open the wizard based setup of eScan Corporate 360 on your computer. To complete the installation follow the instructions on screen. Denote

- **Downloading and installing eScan Corporate 360 Server from internet**

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

  For installing eScan Server from the setup file downloaded from Internet, just double click on the MDMcwn2k3ek.exe and follow the instructions on screen to complete the installation process.

- **Installation Process**

The installation process comprises of following steps –

- **Step 1 - Selecting Language**

Selecting the Setup Language will mark the beginning of the Installation process of eScan server. You will be welcomed with the following window for selecting Language. Refer **Figure 4.1**

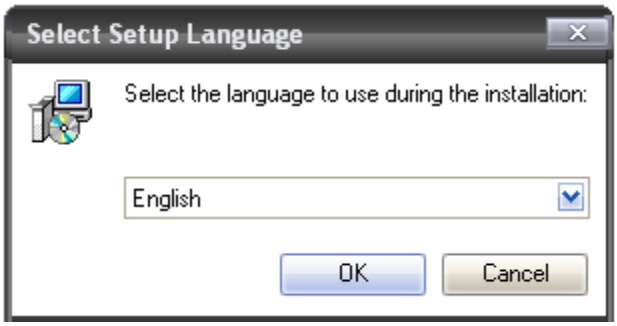


Figure 4.1

Using the Drop Down menu present on the Window, select the desired language for Installation and click **OK** to proceed. You will be forwarded to the main window of the Installation Wizard. Refer **Figure 4.2**

Note:
• The Default Language shown in the Drop down Menu is dependent on the Language of the Operating System installed on the Computer. Currently we support below languages -English, German, French, Dutch, Italian, Portuguese, Spanish, Turkish, Chinese Traditional, Chinese Simplified, Greek, Korean, Russian, Polish, Latin Spanish, Croatian, Estonian, Brazilian Portuguese, Swedish, Romanian, Japanese.

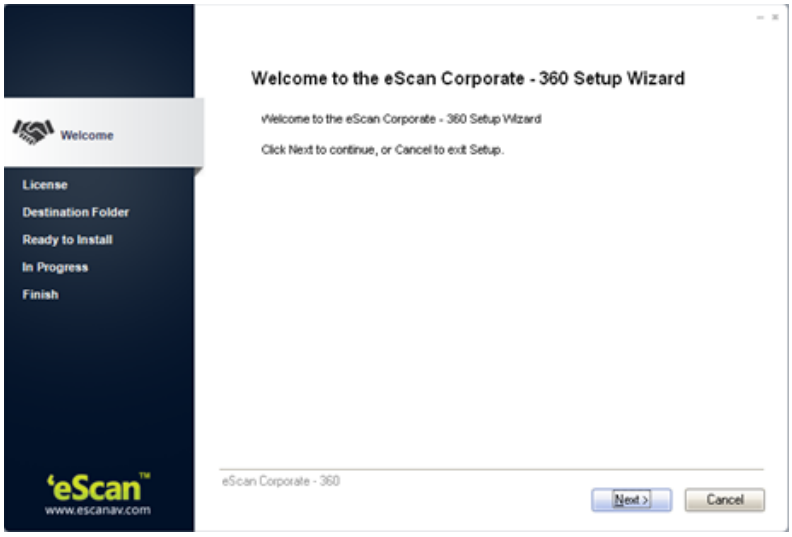


Figure 4.2

- **Step 2 – Accepting the License Agreement**

To proceed with the installation click **Next**, this will forward you to the License Agreement Screen; Accept the License agreement by clicking option and click **Next**. Refer Figure 4.3.

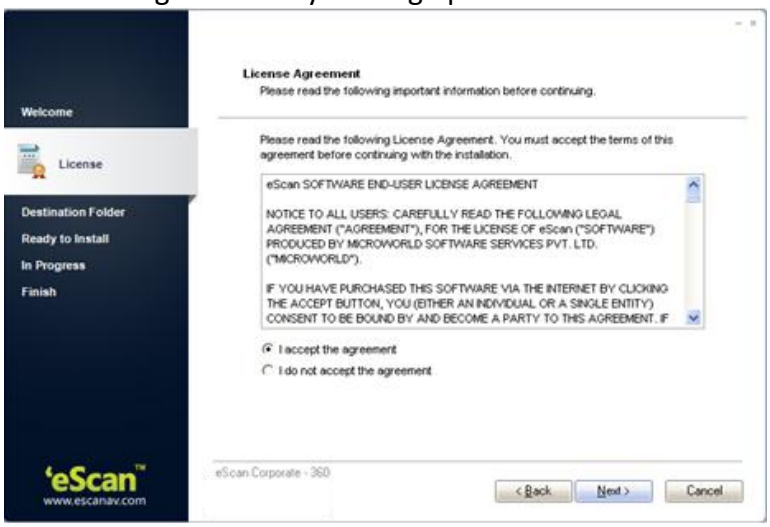


Figure 4.3

- **Step 3 – Selecting the Destination Folder**

Select the destination folder where you wish to install eScan Management Console on your computer. Use browse option to browse the Destination Folder for installing eScan Management Console. Click **Next** to proceed with the installation. Refer Figure 4.4

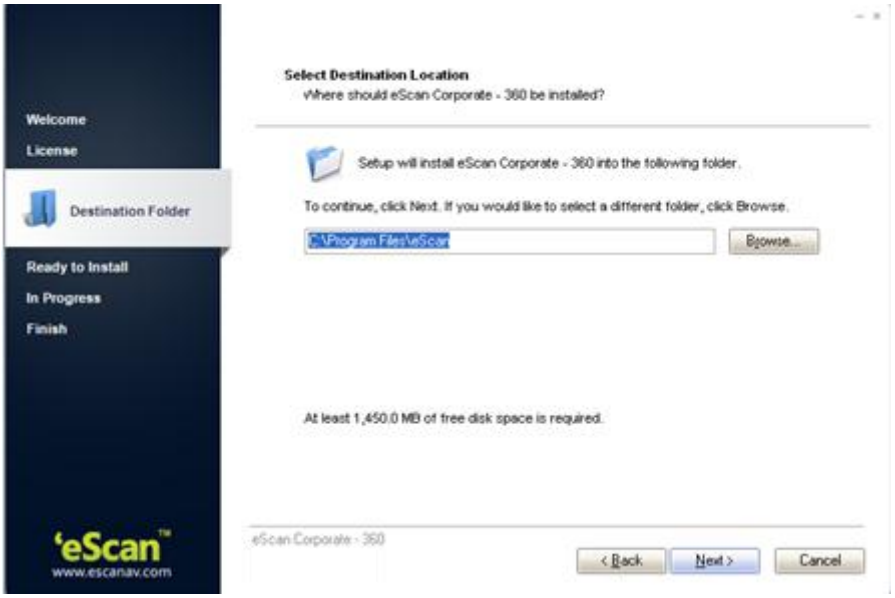


Figure 4.4

Note:
• Default Path for eScan installation on a 32 bit Computer - C:\Program Files\eScan
• Default path for eScan installation on a 64 bit Computer - C:\Program Files (x86)\eScan

- **Step 4 – Ready to Install?**

  This window displays the destination location where eScan Management Console will be installed. Check the destination location, if you are ready to install eScan Management Console on your computer, click **Install** to proceed. Refer Figure 4.5

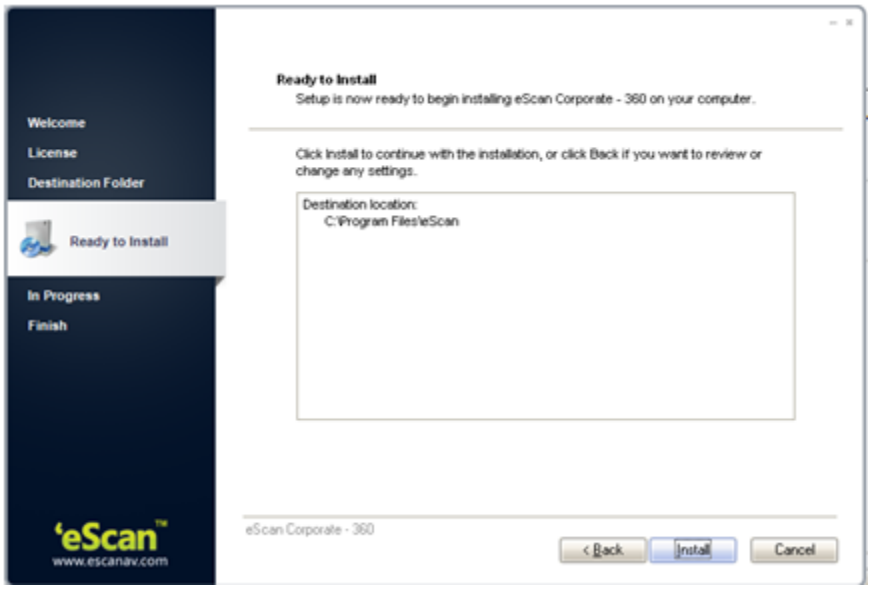


Figure 4.5

- **Step 5 – Installation Progress**

  The installation will start and the progress will be displayed on the following window. Refer Figure 4.6

Figure 4.6

- **Step 6 – Configuring eScan Management Console**

During the installation eScan Management Console Configuration Wizard will guide to Configure settings for SQL Server hosting as well as Login settings for the eScan Management Console. This is vital for completing the installation process. Refer Figure 4.7

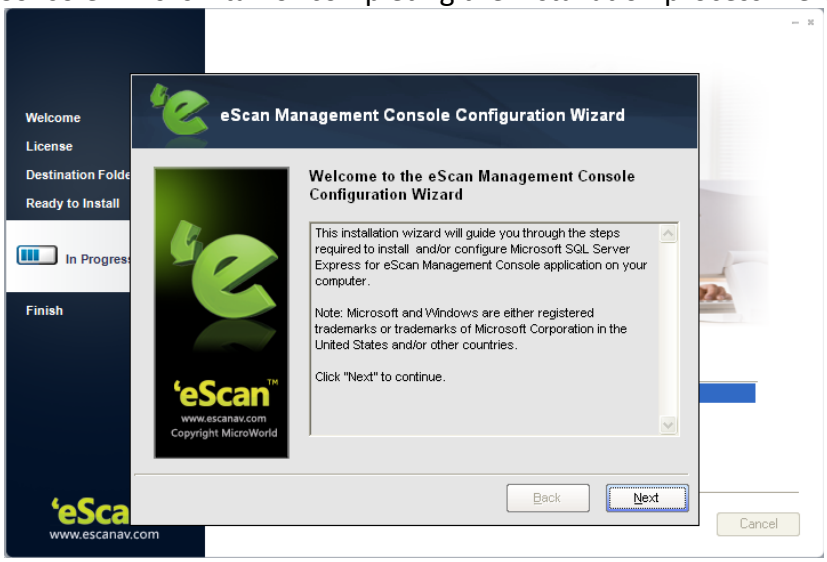


Figure 4.7

- **Step 7 – Selecting the Computer for Hosting SQL Server**

  Using various options present on this window you can select desired computer or instance for hosting SQL Server. Refer Figure 4.8

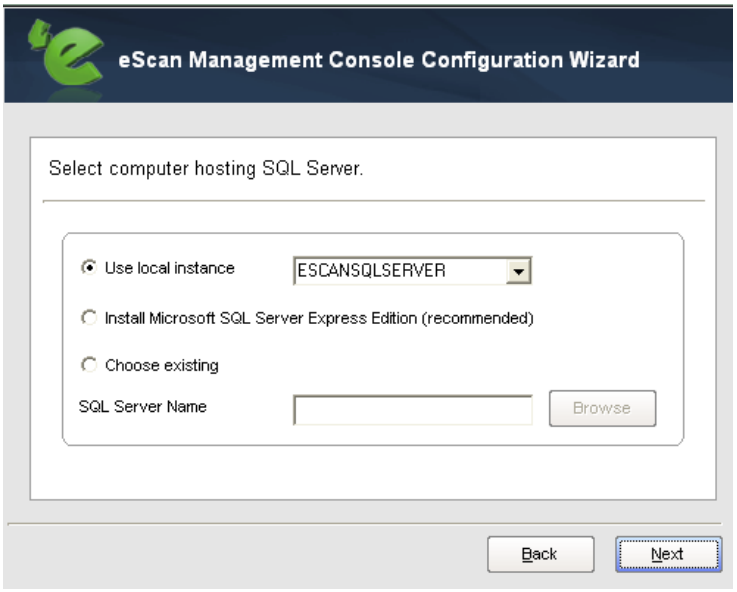


Figure 4.8

Options	Description
Use Local Instance	**[Radio button]** Use this drop down to select the desired instance of the SQL Server. It displays a list of local instances present on the system. This option is being used if you already have SQL Instance running locally.
Install Microsoft SQL Server Express Edition	**[Radio Button]** Select this option to Install Microsoft SQL Server Express Edition. It is **recommended** to select this option for Server installation. This option is selected if you do not have SQL installed on the system on which eScan server is being installed.
Choose Existing	**[Radio Button]** Select this option if you have already created an instance for eScan Database on any SQL Server installed on any computer connected to the network. Use the Browse option to Locate the server instance. This option is being used if you already have an instance running locally or in your local area network.

Click **Next** to proceed with the Installation process. SQL Server installation Wizard will start.

- **Step 8 – Installing SQL Server**

Click **Install** to start the installation of SQL Server. Refer Figure 4.9.

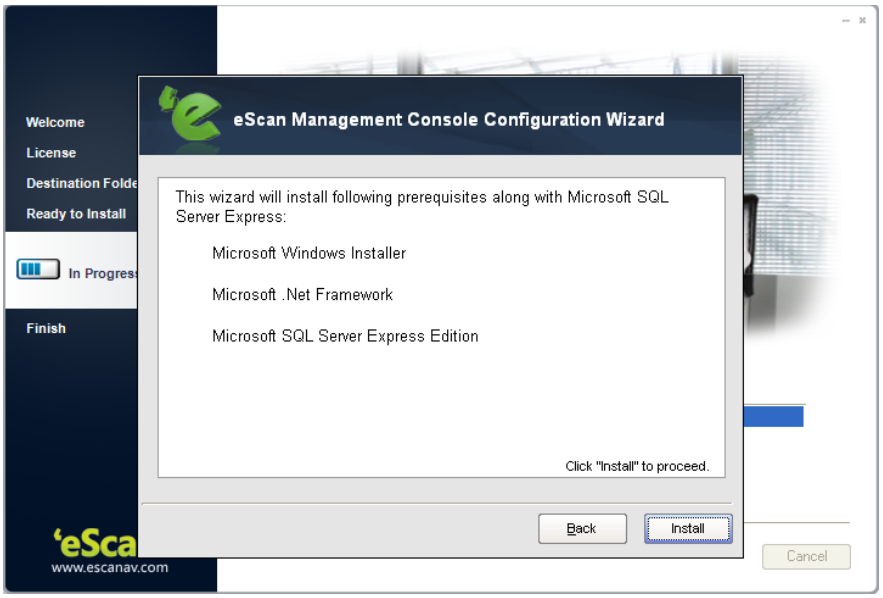


Figure 4.9

The wizard will inform you on successful installation of Microsoft SQL Server Express. Refer Figure 4.10

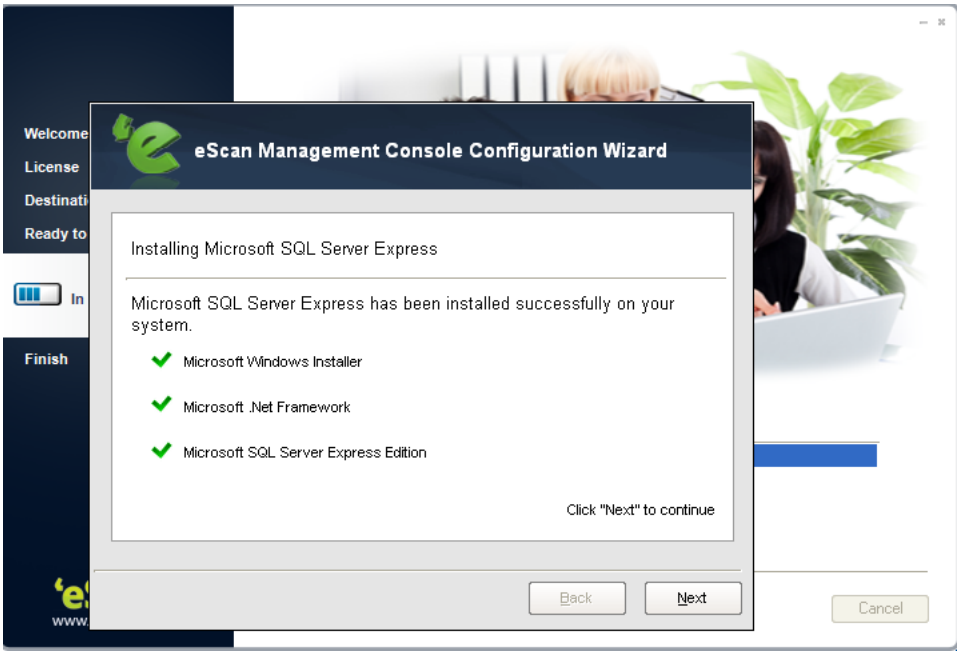


Figure 4.10

Click **Next** to continue. You will be forwarded to the eScan Management Console Login information Window.

- **Step 9 - Filling Login Credentials for eScan Management Console**

Fill up the required Login credentials that will be required to Login into the eScan Management Console. Click **Next** when done. Refer Figure 4.11.

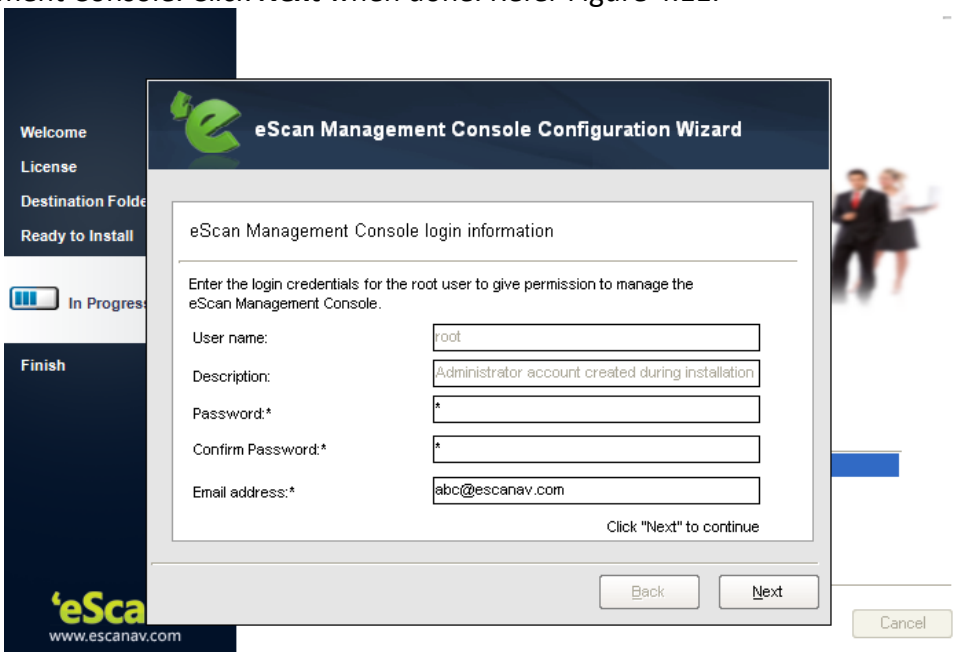


Figure 4.11

- **Step 10 – Completing eScan Management Console Configuration**

  For completing the Configuration of eScan Management Console, click **Finish**. Refer Figure 4.12.

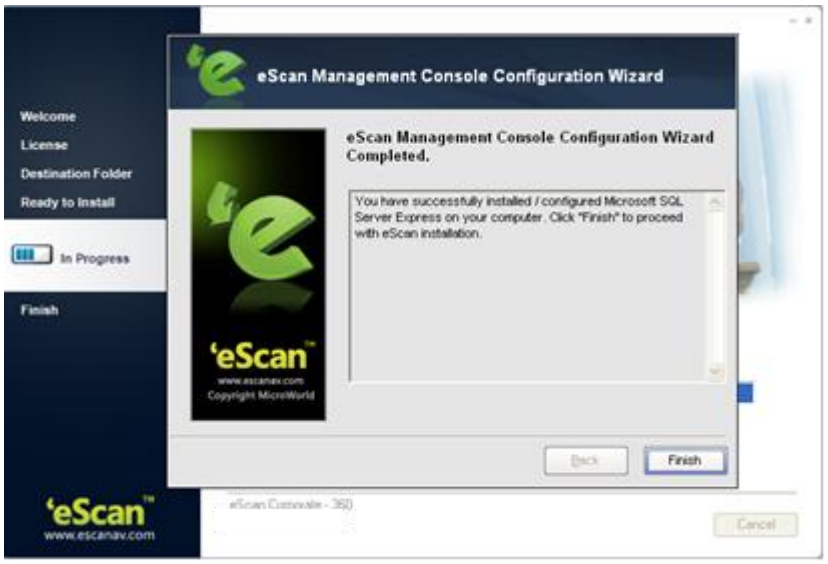


Figure 4.12

- **Step 11 – Scanning Computer for Viruses and infection**

Before finishing the installation process, eScan will scan the computer for viruses, you can cancel the scanning by clicking **Cancel** on the eScan Antivirus Toolkit window. Refer Figure 4.13.

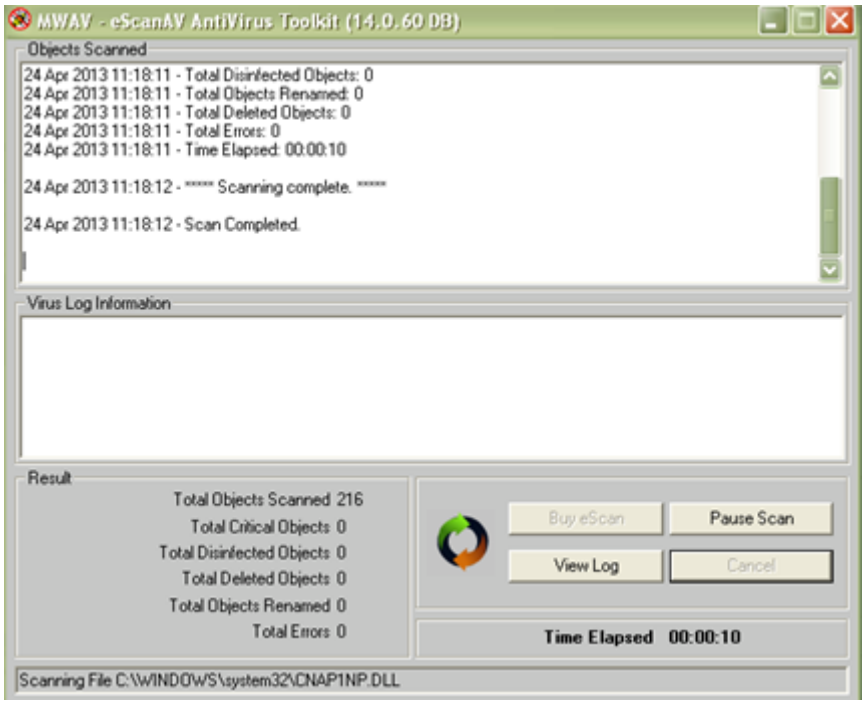


Figure 4.13

Once the scanning is complete or you have cancelled the scanning, you will be forwarded to the **Finish window**. Click **Finish** to complete the installation process. Please restart the computer before using **eScan Management Console**.

4. Components of eScan Server

The eScan Server comprises the following components.

eScan Server - This is a core component which allows you to manage, deploy and configure eScan on Endpoints. It stores the configuration information and log files about the Endpoints which are present in the network. It also communicates with other components mentioned below.

Agent – It manages the connection between the eScan server and the client computer.

eScan Management Console - It is a Web-based application hosted on the eScan Server. It allows administrators to manage eScan on Endpoints in the network.

Microsoft SQL Server Express Edition- Database for storing events and logs, already included in the eScan Setup file.
(NOTE : On Windows 8 / 8.1 / 2008 /2012 operating systems, SQL 2008 Express edition will be installed else SQL 2005 Express edition will be installed.)
Apache - For running eScan Management Console. Already included in the eScan Setup file.

(NOTE: Uninstallation of eScan server will not remove SQL and APACHE software from the system.)

6. User Interface of eScan Management Console

- **Taskbar Menu –**

  Click **eScan Management Console** icon present in the taskbar on your desktop (on eScan Server only). This will open the **Login Page** of eScan Management Console in your default web browser.

  - **Options on Right Click (eScan Management Console Icon in taskbar)**

Options	Description
Client Live Updater	Using this option you can get live event feeds from all Endpoints on your network. This feed consists of IP Address, Username of the Endpoints, Module Names and Client actions. This Live Feed list can be exported to Excel if required.
Open Web Console	Click on this option to open eScan Management Console in a web browser.
Stop Announcement	Click on this option to stop broadcast from and towards the server.
About eScan Management Console	Click on this option to know more about eScan.
Shut Down	Click on this option to shut down the server. (Note : This is not recommended to shut down the server component, this will stop the communications between client and server)

- **The Login Page**

Enter the Username and Password defined by you during installation of eScan Corporate- 360 to Login to the **eScan Management Console**. **Refer Figure 6.1**

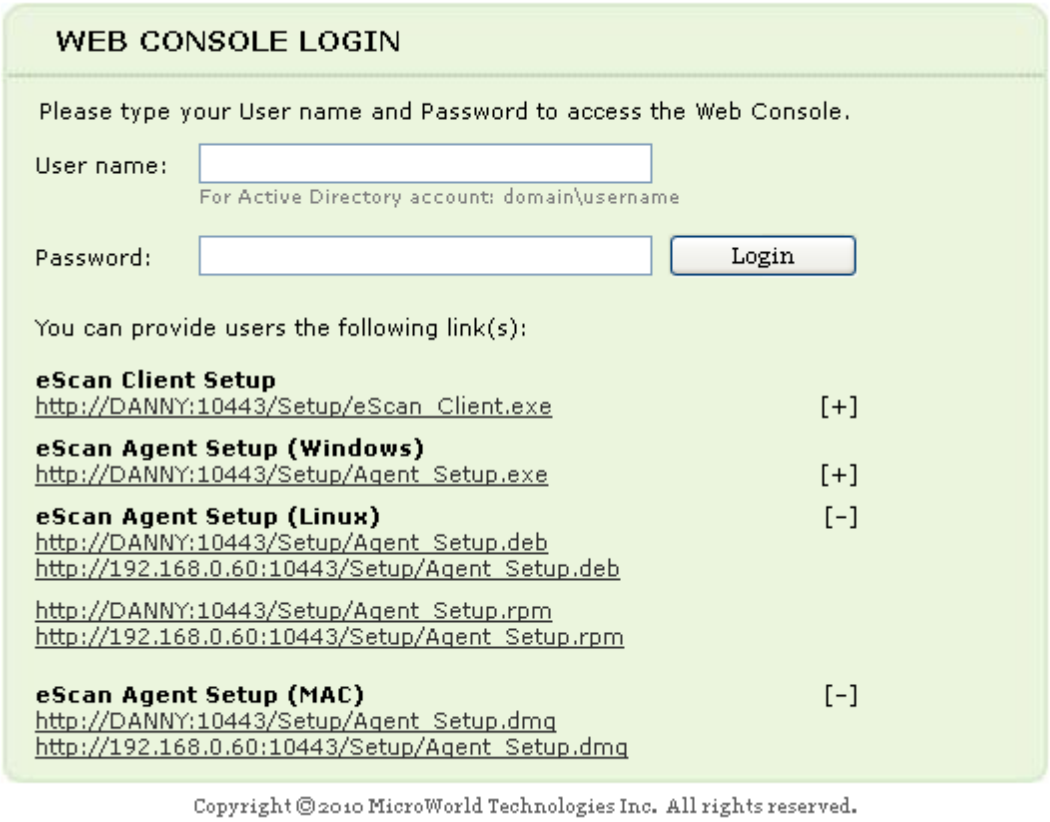


Figure 6.1

Note:
• Please note that "**root**" is the super user being created by default by eScan during Installation, see - **Filling Login Credentials for eScan Management Console.**

Options	Description
Username	**[Field]** Enter the username to login to eScan Management Console.
Password	**[Field]** Enter the Password to login to eScan Management Console.

Login	**[Button]** Enter the Username and Password and click **Login** to enter the eScan Management Console.
eScan Client and Agent Setup Links	**[Download Links]** Client setup links (for Windows) is present on the Web Console Login page; you can send these links on mail to the users of the Endpoints where remote installation is not possible. Using this link they can download the Client setup and install it manually on their computers. Or they can directly access eScan Management console from their desktop.
eScan Agent Setup Link	**[Download Link]** You can give this link on mail to the user of the Endpoints from where you are not able to get system information or communication is breaking frequently. Once the Agent is downloaded and installed on the Managed Computer. It will establish the connection between Server and Client computer. ***Please note that installation of eScan on Linux and MAC computers can only be done manually by downloading AGENT on MAC or Linux computers from the links***

- **Main Interface - eScan Management Console - Refer Figure 6.2**

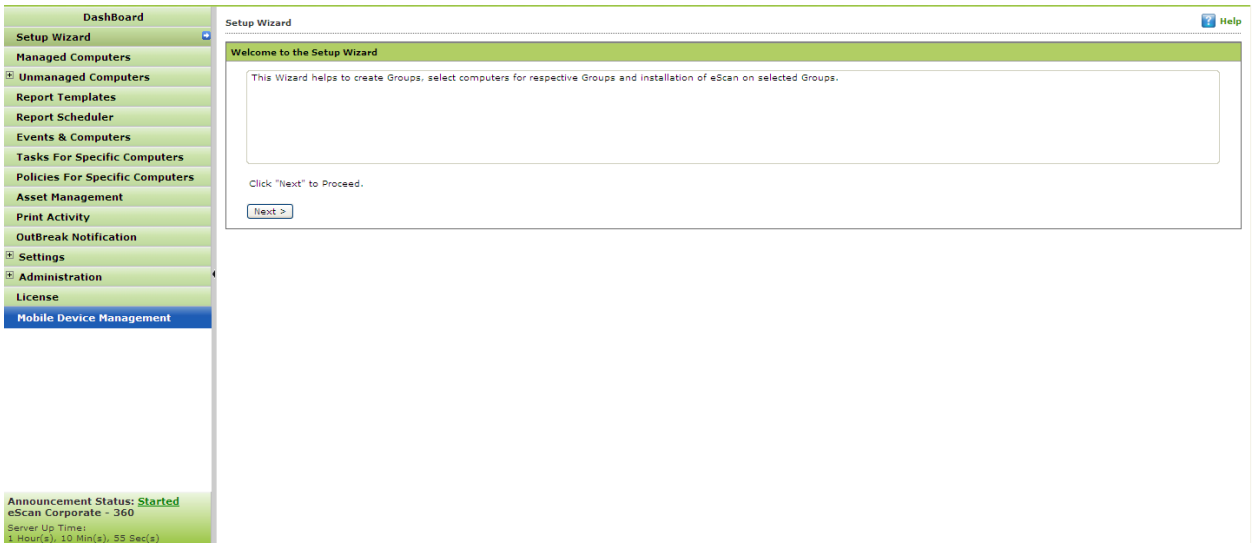


Figure 6.2

Note:
Icons on every status Label signifies that the status is displayed for the computers having operating system as ***Windows,*** ***MAC OS X*** *or* ***Linux****.*

Links	Description
About eScan	**[Link]** Click on this link to visit our Home page – www.escanav.com
Username	**[Link]** Click on this link to edit User Login details like Full name, Password and email address that you use to Login in the eScan Management Console.
Log off	**[Link]** Click on this link to Log out of the eScan Management Console.
Date of Virus Signatures	It displays the last date on which the Virus signatures were updated on eScan Server. Click on this link to update virus signatures on eScan Server.
Navigation Panel	Present on the Left in eScan Management Console, it displays all Modules of eScan Management Console providing access to numerous functionalities present under them.

- **eScan Management Console - Navigation Panel**

  Navigation Panel appears on the left side after you login to eScan Management console and gives you direct access to various options present in the console for managing computers, installing, updating and configuring eScan on the Endpoints connected the network. Using this panel you can also configure settings for the Web console and manage user roles and permissions for Management Console. Using this console you can easily ensure total security of endpoints from malware infections and viruses. It also helps you in configuring notification mails for warning or alert in case of occurrence of a virus outbreak. **Refer - Figure 6.3**

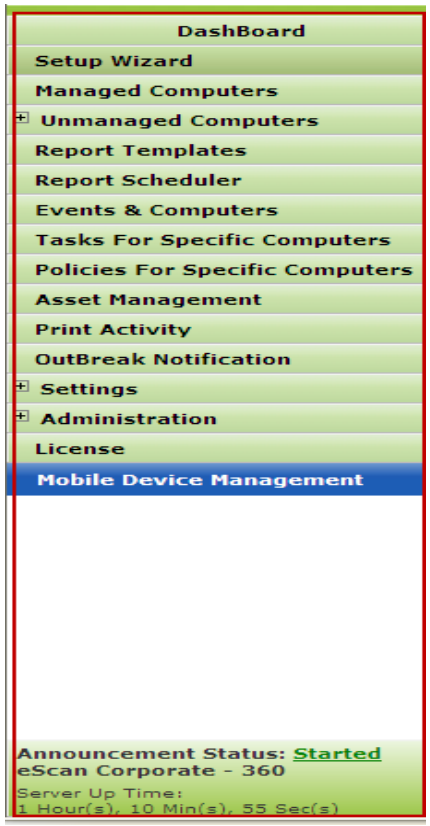


Figure 6.3

- **Overview of the Navigation Panel** –

  Various options present in the Navigation Panel of eScan Management Console are as follows –

- **Dashboard** - The dashboard of eScan Management Console displays charts showing deployment status, Protection status, Protection Statistics and top 10 Summary and the monitoring done by Management Console of the Endpoints for virus infections and security violations. For **more details click here**. Refer - Figure 6.4

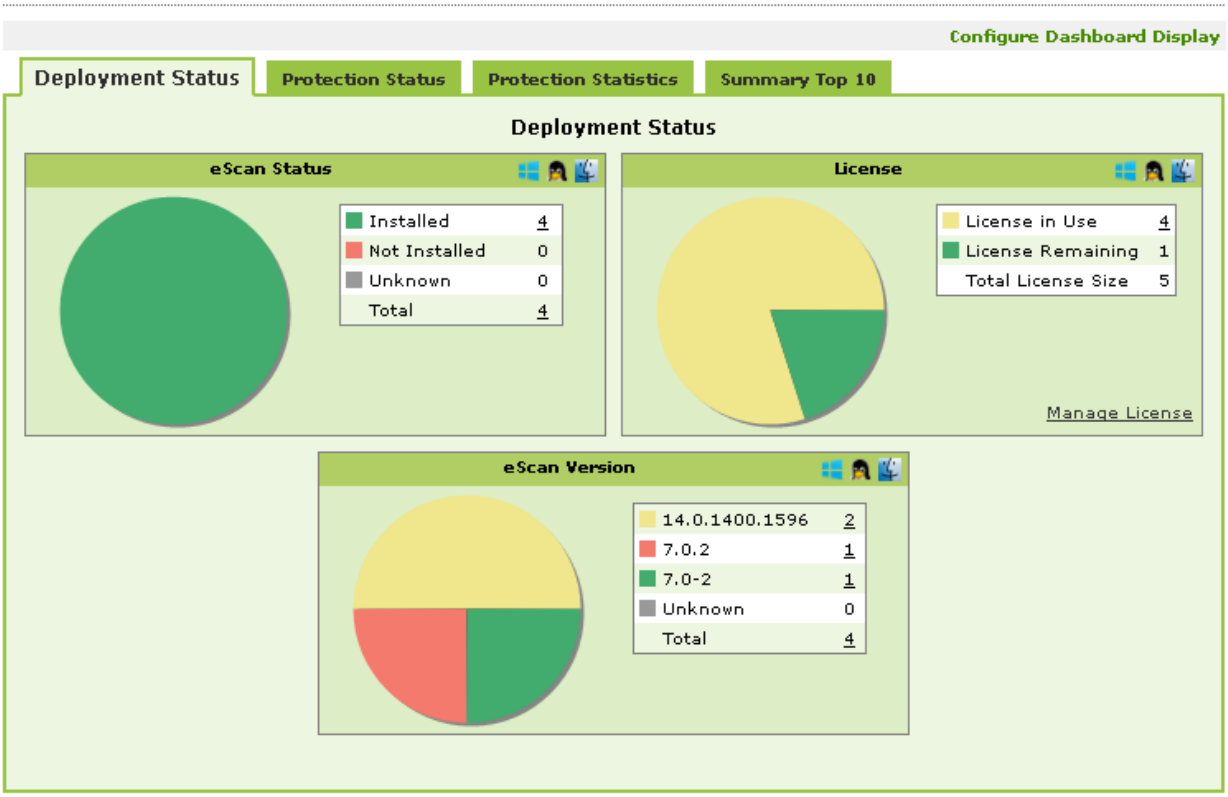


Figure 6.4

Note:
• *Icons on every status Label signifies that the status is displayed for the computers having operating system as* ***Windows,*** ***Mac OS X*** *or* ***Linux****.*

- **Setup Wizard -** It guides you in step by step creation of groups, adding computers to respective groups, adding hosts from the network and installing client on the connected computer at a desired path/ location on that computer. Once you have completed the setup using setup wizard this module will not be visible when you open eScan Management console from next time. Refer - Figure 6.5

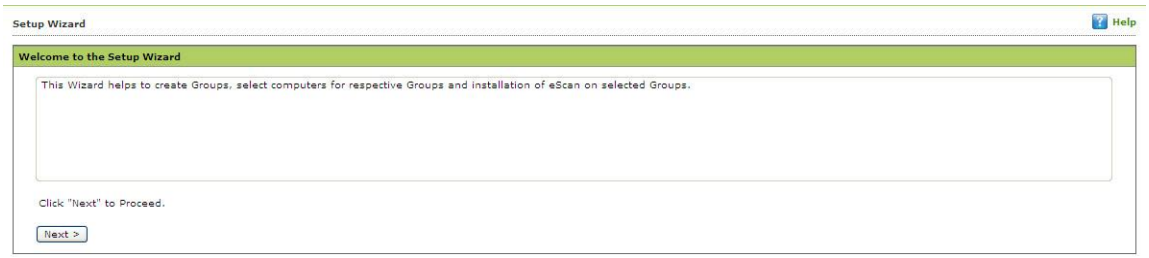


Figure 6.5

- **Managed Computers –** It consists of a Console tree on the left and a task pane on right. Using this section you can define / configure Policies for Endpoints. It provides various options for creating groups, adding tasks, deploying or uninstalling client application, moving computers from one group to the other and redefining properties of the Endpoints from normal to roaming users and vice versa. For **more details click here**. Refer - Figure 6.6

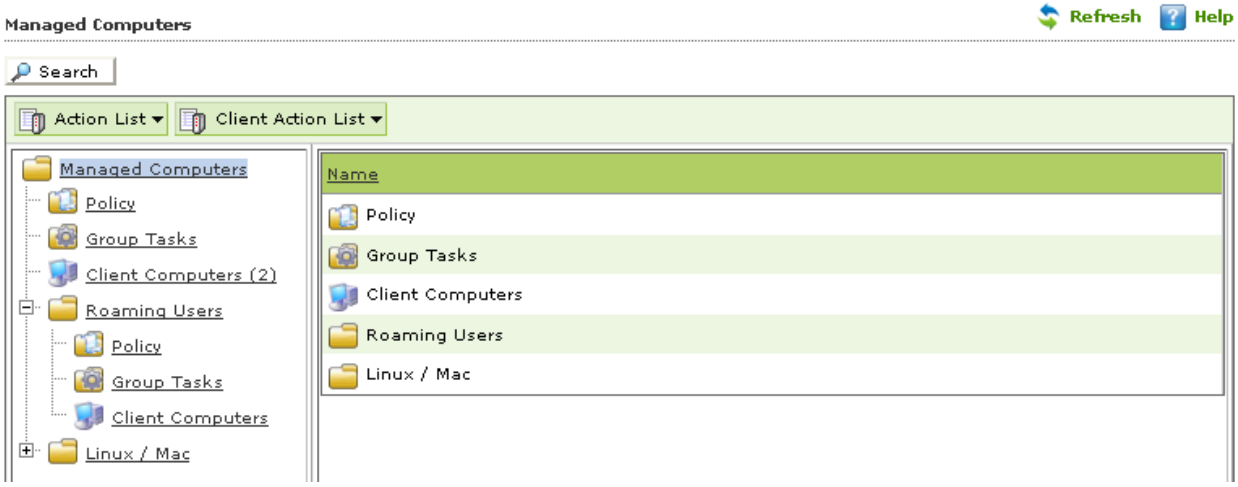


Figure 6.6

- **Unmanaged Computers –** This section displays information about the computers that have not yet been assigned to any group. This section also allows you to set the host configuration, move computers to a group, view the properties of a computer, or refresh the information about a client computer by using the **Action List** menu. This section consists of **Network Computers, IP Range, Active Directory** and **New Computers Found.** Refer - Figure 6.7

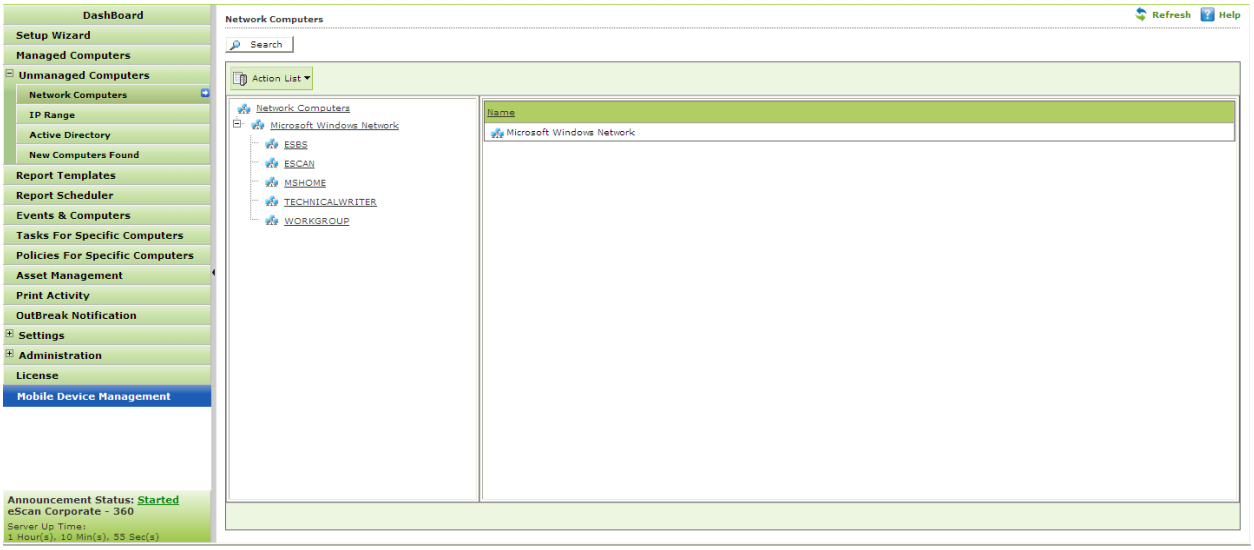


Figure 6.7

- **Report Templates -** The **Reports Template** page allows you to create and view customized reports based on a given template, for a given period; sorted by date, computer, or action taken; and for a selected condition or target group. It also provides options for configuring or scheduling reports, viewing report properties, and refreshing or deleting existing reports. For **more details click here**. Refer - Figure 6.8

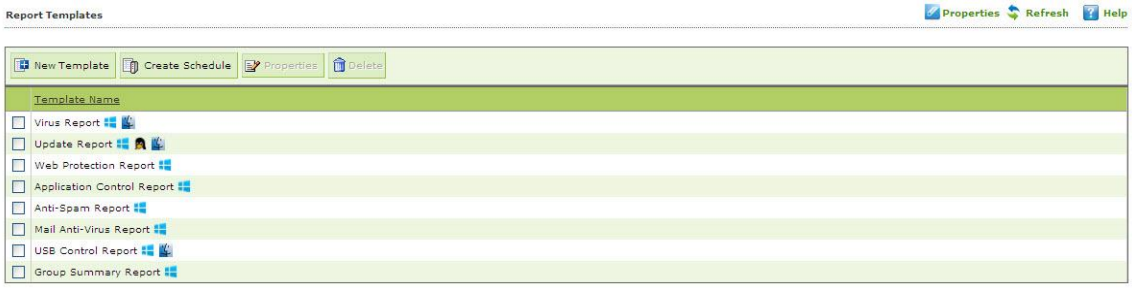


Figure 6.8

Note:
• *Icons on every status Label signifies that the status is displayed for the computers having operating system as* ***Windows,*** ***Mac OSX*** *or* ***Linux****.*

- **Report Scheduler -** The **Report Scheduler** page allows you to schedule a new reporting task, run an already created reporting schedule or view its properties. For **more details click here**. Refer - Figure 6.9

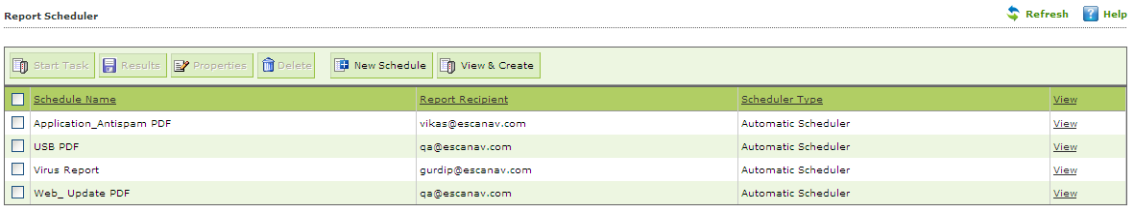


Figure 6.9

- **Events and Computers -** The Events & Computers page enables you to monitor various activities performed on client's computer. You can view log of all events based on Event Status, Computer Selection or Software/ Hardware Changes on that client computer. Using the Settings option on the screen you can define settings as desired. For **more details click here.** Refer - Figure 6.10

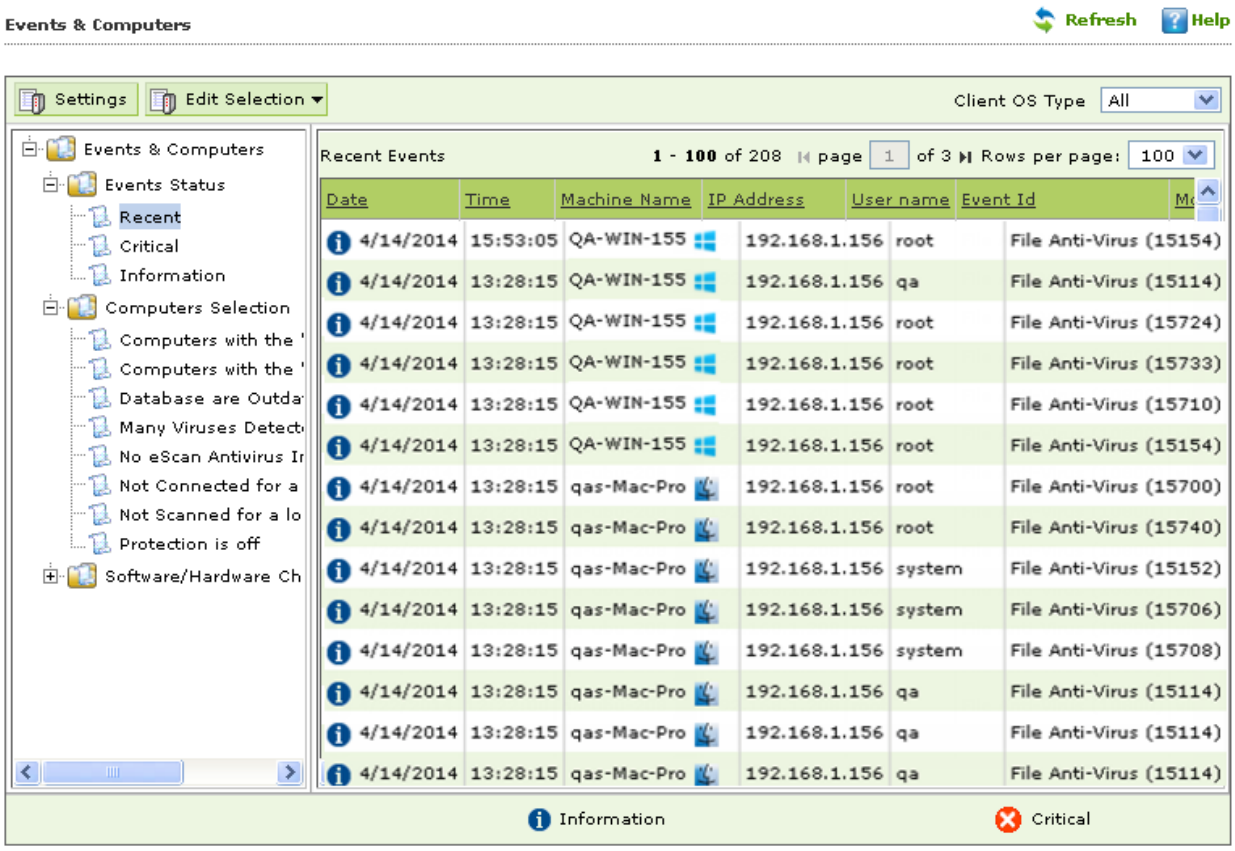


Figure 6.10

- **Tasks for Specific Computers** – Using this section create and run tasks on specific computers, it also allows you to schedule or modify created tasks for selected computers or groups. You can easily re-define settings of already created tasks for desired machines. It also allows you to view results of the completed tasks. For **more details click here**. Refer - Figure 6.11

Figure 6.11

- **Policies for Specific Computers -** Using this section you can define rule set for specific computers in the managed computers group. It also allows you to define the rule sets that you have already created. Refer - Figure 6.12

Figure 6.12

Note – Precedence will be given to Policy for specific computer over group policy

- **Asset Management -** This module provides you the entire Hardware configuration and list of software installed on Endpoints in a tabular format. Using this module, you can easily keep a track of all the Hardware as well as Software resources installed on all the Endpoints connected to the Network. Based on different Search criteria you can easily filter the information as per you requirement. It also allows you to export the entire system information available through this module in PDF, Microsoft Excel or HTML formats. Refer - Figure 6.13

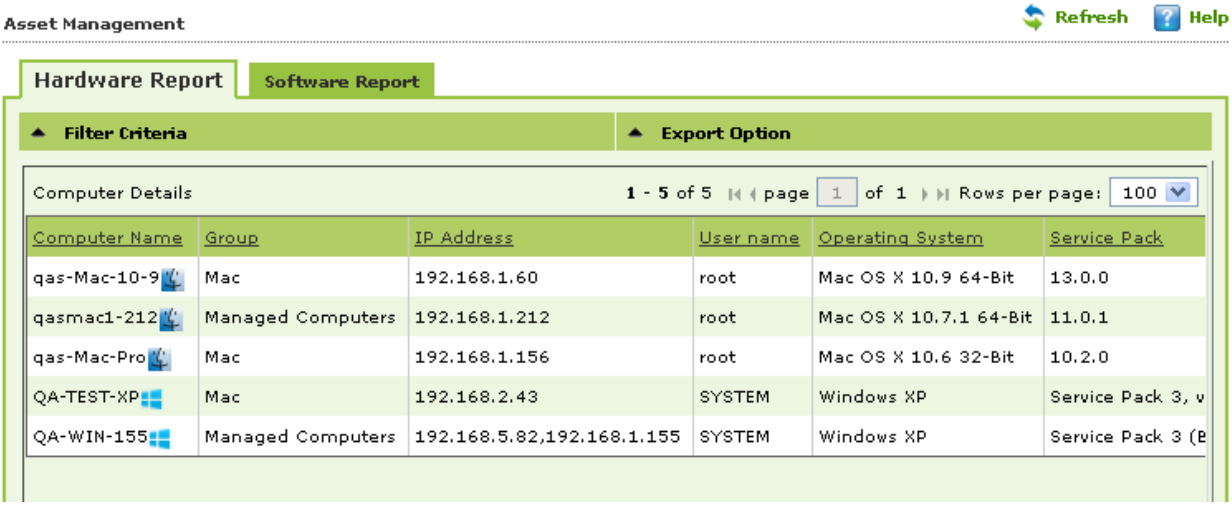


Figure 6.13

Print Activity - It monitors and logs printing tasks done by all the Endpoints, it gives you a report of all Printing Jobs done by Endpoints through any Printer connected to the network. It also gives you a Log report of all PDF conversions through PDF Converters done on individual Machine connected to the network. Refer - Figure 6.14

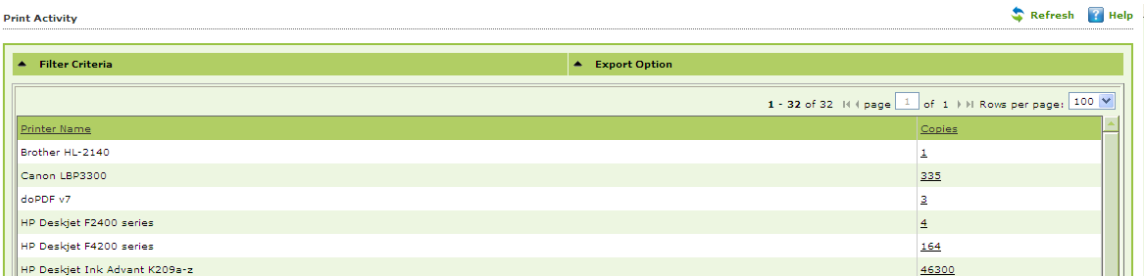


Figure 6.14

- **Outbreak Notification –** Using this section, you can configure settings for sending notification when Virus count exceeds the limit defined by you. Refer - Figure 6.15

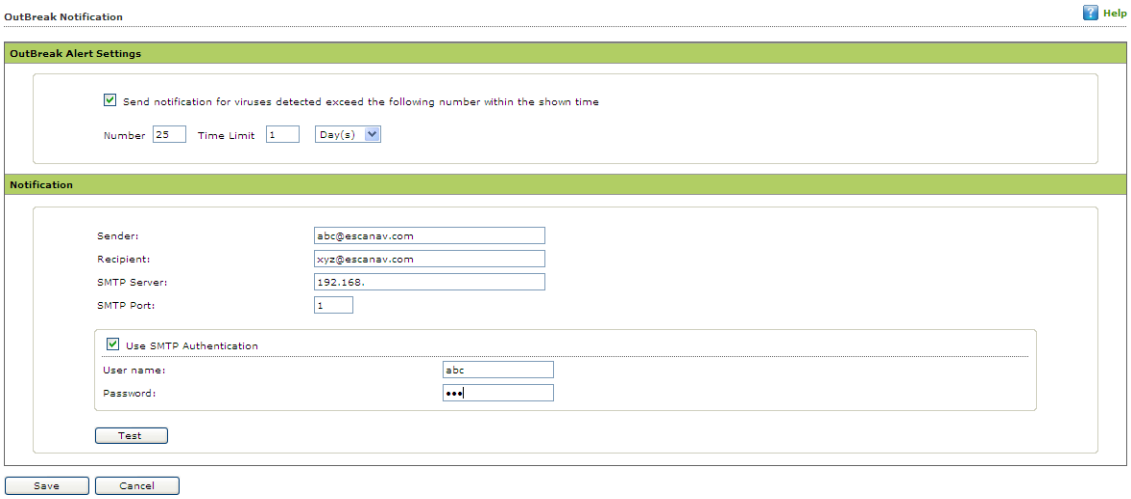


Figure 6.15

- **Settings -** Using this section you can define important settings for FTP downloads, maintaining Logs, eScan Management Console timeout settings, update download settings along with important settings for escan. For more information **Click Here**

- **Administration -** Using this section you can create User Accounts and allocate them Admin rights for using eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. Using this option you can allocate rights to the other employees which will allow them to install eScan Client and implement Policies and tasks on other computers. For more information **Click Here**

- **License -** The eScan Web Console enables you to manage license of users. You can add, activate, and view the total number of licenses available for deployment, number of licenses deployed, and number of licenses remaining with their corresponding values. You

can also move the licensed computers to non-licensed computers and non-licensed computers to licensed computers. Refer - Figure 6.16

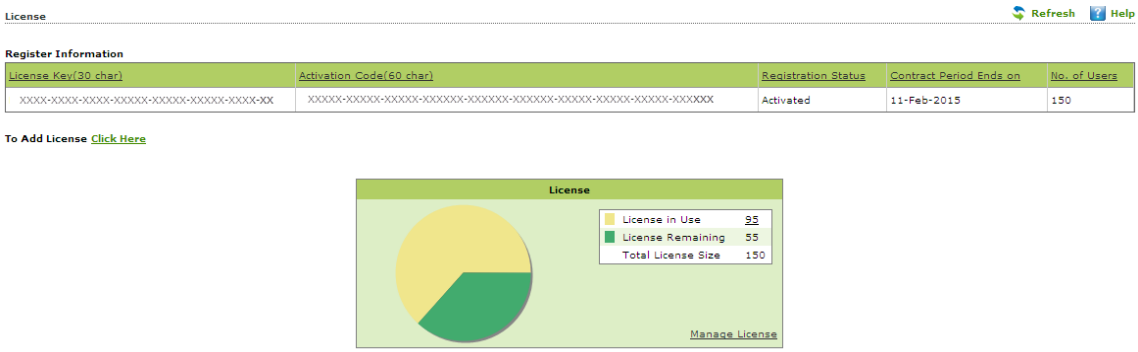
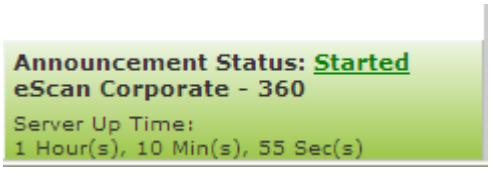


Figure 6.16

- **Server Status info –** It displays the Anouncement info of the server along with the Server up time .



- **Dashboard and its Configuration**

It displays the **Deployment Status**, **Protection Status**, and **Protection Statistics** and **Summary Top 10** of eScan and it modules graphically in the form of pie charts.

This section displays the Pie chart view of the following –

- **Deployment Status**

  It displays the deployment status of eScan client on the Endpoints. Displays charts showing status of eScan Client installation, Licenses and eScan versions installed on Endpoints.

- **eScan Status -**

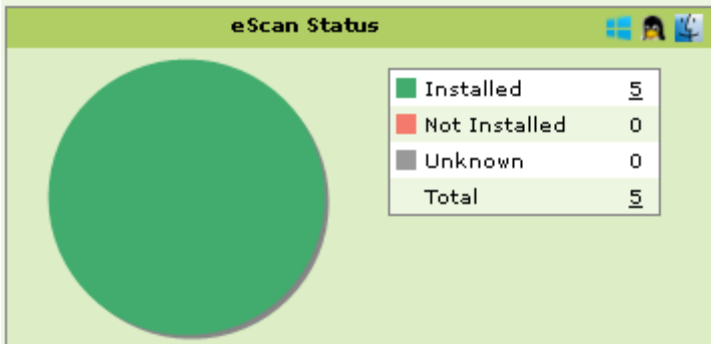


Figure 6.17

- **Installed** - Total number of Computers where eScan Client is installed.
- **Not Installed** - Total number of Computers where eScan Client is not installed.
- **Unknown** - Total number of Computers whose status about the Client installation is unknown. (Server is unable to receive information from the Computers for a long time)
- **Total –** Total number of computers where eScan is installed, not installed or the installation status is unknown.

- **License –**

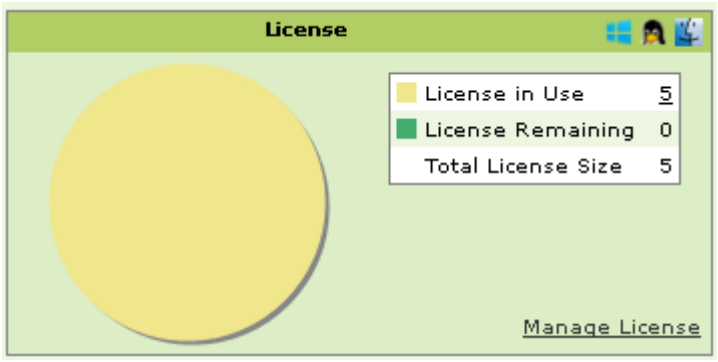


Figure 6.18

- **License in Use** - Total number of Licenses that have been activated.
- Total number of **Licenses remaining**.
- **Total license** size i.e. – The total number of Licenses purchased, it includes the number of licenses that are used as well as un-used.

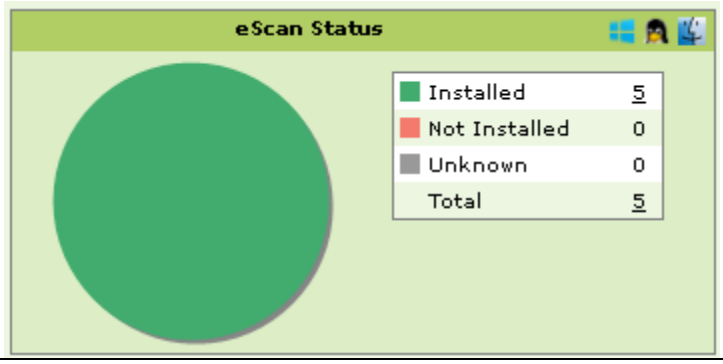
- **eScan Version -**

It gives you a pie chart view of the total number of versions installed on the computers on the network.

- Also displays number of computers on which specific versions are installed.

Note:

- To know more details about the computers, *click on the number of computers links for listed options*.



Note:

- Windows, Mac, Linux Icons at the top of every chart denote that the information is displayed for computers with respective operating systems (Windows, Macintosh or Linux). Know more details about the computers, click on the number of computers links for listed options.

- **Protection Status -** It displays the status of all the modules of eScan Client along with Update status on Endpoints.

  - **Update Status –**

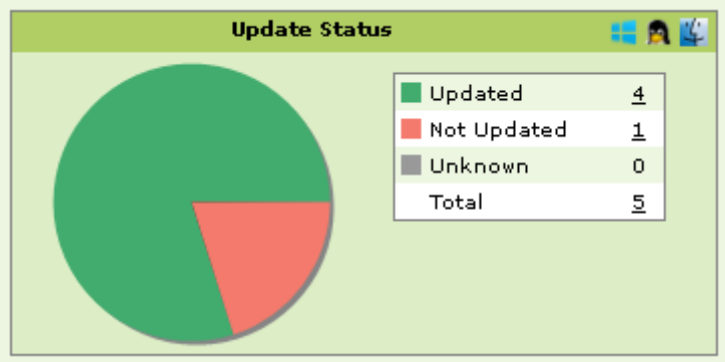


Figure 6.19

  - **Updated** - Number of computers on which eScan Client is updated.
  - **Not Updated** - Number of computers on which eScan Client is not updated.
  - **Unknown** - Number of computers where the status is unknown.
  - **Total** - Displays the status of total number of computers where the status is updated, not updated or unknown.

- **Scan Status –**

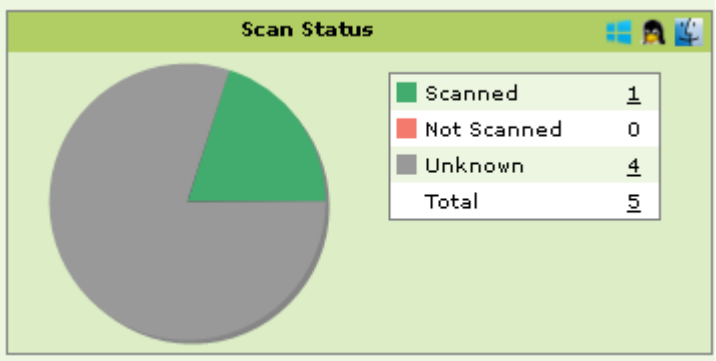


Figure 6.20

- Scanned - Total number of computers that have been scanned in last 30 days for viruses and malware infections.
- **Not Scanned** - Total number of computers that have not been scanned in last 30 days for viruses and malware infections.
- **Unknown** - Number of computers where the status is unknown.
- **Total** - Displays the total number of computers that have been scanned, not scanned or their scanning status is unknown. It includes computers with **Windows**, **Mac** or **Linux** operating system.

- **File Antivirus –**

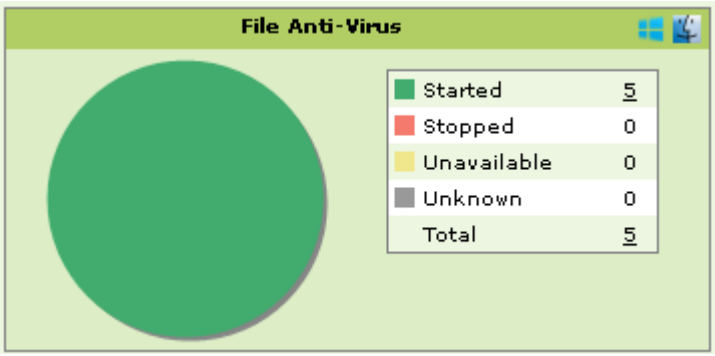


Figure 6.21

- **Started** - Number of computers on which the File Antivirus Module is in Started State or turned on.
- **Stopped** - Number of computers on which the Module is in Stopped State or turned off.
- **Unavailable** – Number of computers where the Module is not present.
- **Unknown** - Number of computers where the status is unknown.

- **Total** - Total number of Managed computer where File Antivirus Module is started, stopped, Unavailable or the status is unknown.

- **Proactive –**

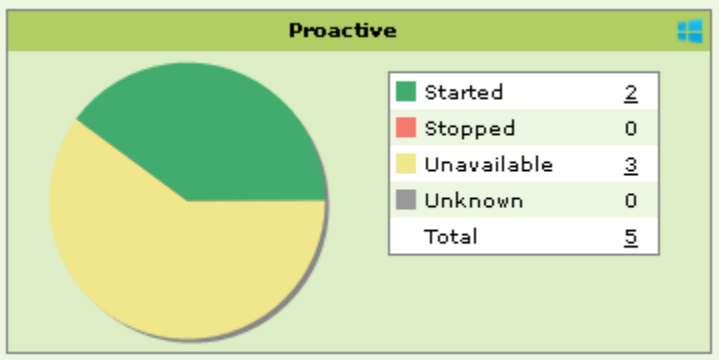


Figure 6.22

- **Started** - Number of computers on which Proactive scanning is in Started state.
- **Stopped** - Number of computers on which Proactive scanning is in stopped state.
- **Unavailable** – Number of computers where Proactive scanning Module is not available. This Module is available only in Computers with Windows Operating system.
- **Unknown** - Number of computers where the status is unknown.
- **Total** - Total number of computers where Proactive scanning is Started, Stopped, Unavailable or the status is Unknown.

- **Mail Antivirus –**

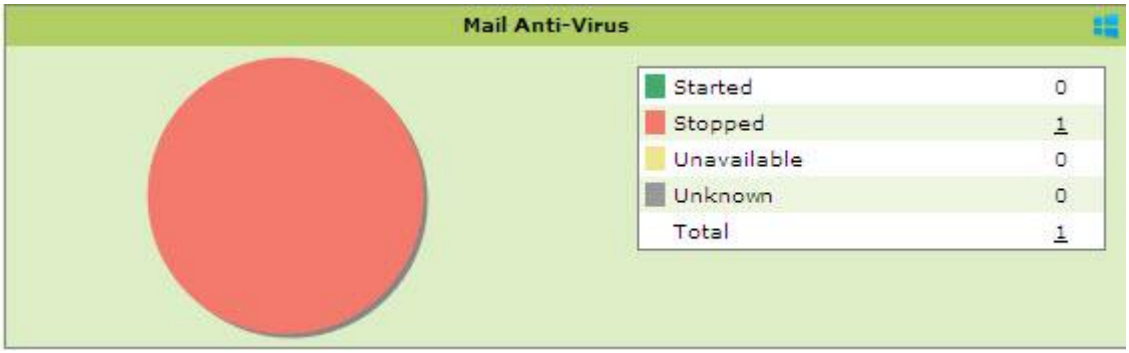


Figure 6.23

- **Started** - Number of computers on which the Mail Antivirus Module is in Started State or turned on.
- **Stopped** - Number of computers on which Mail Antivirus Module is in Stopped State or turned off.
- **Unknown** - Number of computers where the status is unknown.
- **Total –** Displays the total number of computers where Mail Anti-Virus module of eScan is started, stopped, unavailable, or the status is not known.

- **Anti-Spam –**

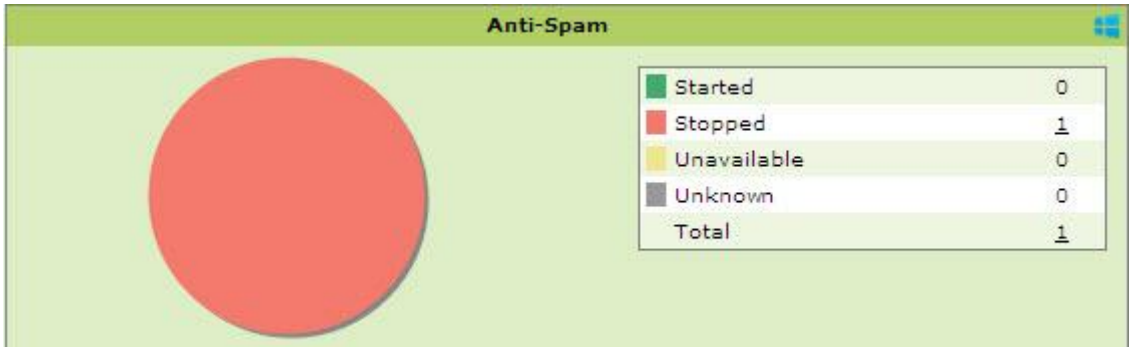


Figure 6.24

- **Started** - Number of computers on which the Anti -spam Module is in Started State or turned on.
- **Stopped** - Number of computers on which Anti-spam Module is in Stopped State or turned off.
- **Unknown** - Number of computers where the status is unknown.
- **Unavailable** – Total number of computers where Anti-Spam module is not available.
- **Total** - Total number of computers where Anti-Spam module of eScan is started, stopped, unavailable or the status is unknown.

- **Web Anti –Phishing –**

Figure 6.25

- **Started** - Number of computers on which Web Anti -Phishing is enabled.
- **Stopped** - Number of computers on which Web Anti -Phishing is disabled.
- **Unknown** - Number of computers where the status is unknown.
- **Unavailable** - Total number of computers where Web Anti-Phishing module of eScan is unavailable.
- **Total** – Total number of computers where Web Anti-Phishing module of eScan is started, stopped, unavailable or the status is unknown.

- **Mail Anti – Phishing**

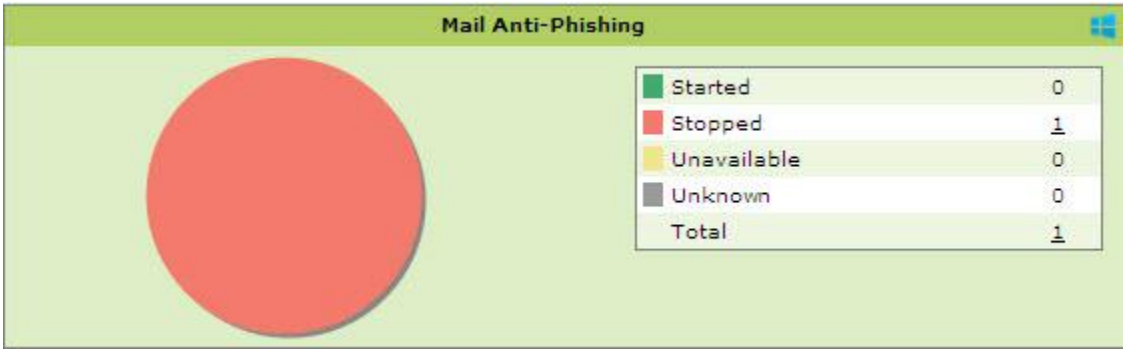


Figure 6.26

- **Started** - Number of computers on which Mail Anti -Phishing is enabled.
- **Stopped** - Number of computers on which Mail Anti -Phishing is disabled.
- **Unknown** - Number of computers where the status is unknown.
- **Unavailable** – Number of computers where Mail Anti-Phishing module of eScan is unavailable.
- **Total** - Total number of computers where Mail Anti-Phishing module of eScan is started, stopped, unavailable, or the status is unknown.

- **Web Protection**

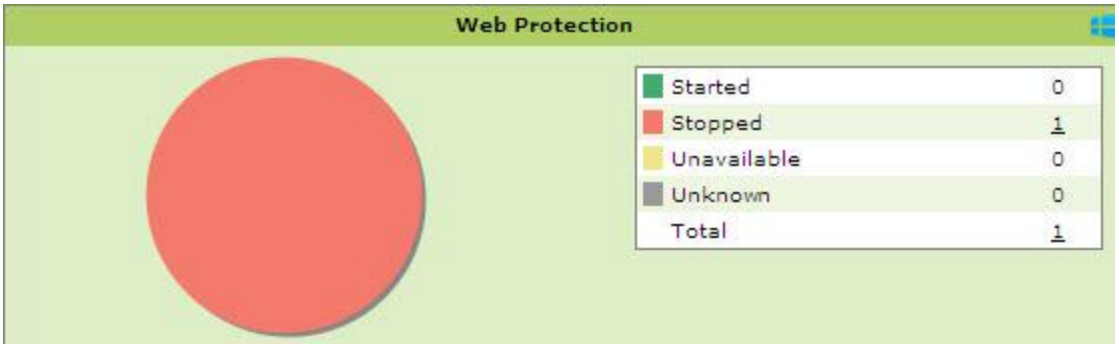


Figure 6.27

- **Started** - Number of computers on which the Web Protection Module is in Started State or turned on.
- **Stopped** - Number of computers on which Web Protection Module is in Stopped State or turned off.
- **Unavailable** - Number of computers where Web Protection module of eScan is unavailable.
- **Unknown** - Number of computers where the status is unknown.
- **Total** - Total number of computers where Web Protection module of eScan is started, stopped, unavailable or the status is unknown.

- **Firewall**

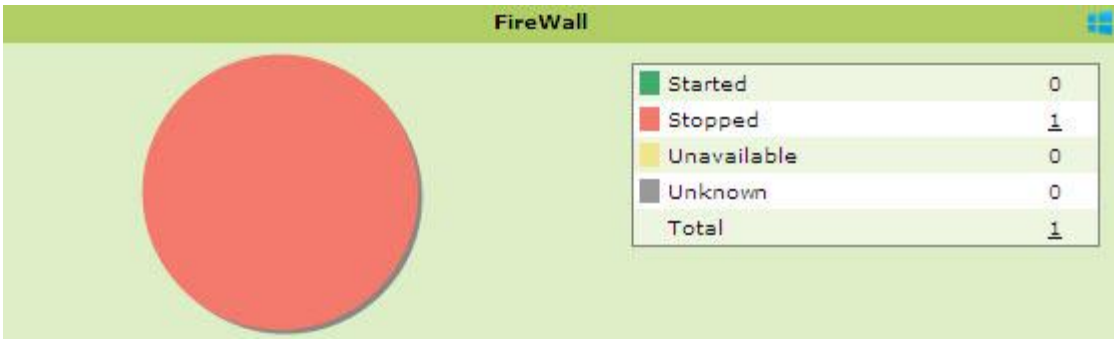


Figure 6.28

- **Started** - Number of computers on which Firewall Module is in Started State or turned on.
- **Stopped** - Number of computers on which Firewall Module is in Stopped State or turned off.
- **Unavailable** - Number of Computers where Firewall module of eScan is unavailable.
- **Unknown** - Number of computers where the status is unknown.
- **Total** - Total number of computers where Firewall module of eScan is started, stopped, unavailable or the status is unknown.

- **Endpoint Security**

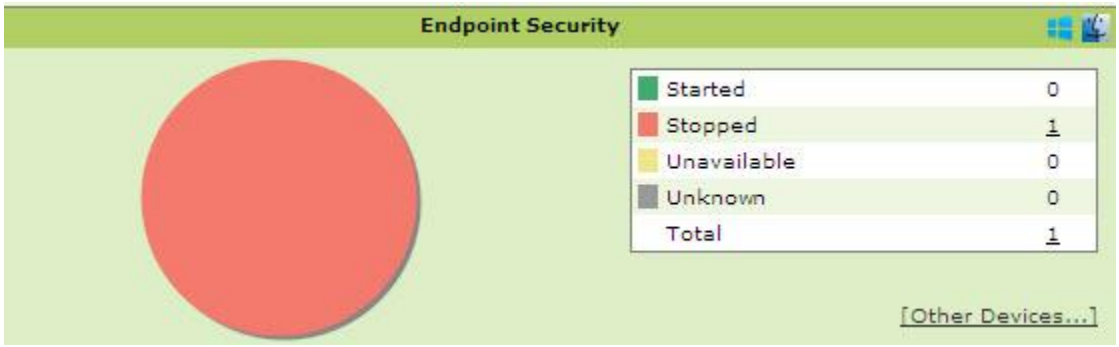


Figure 6.29

- **Started** - Number of computers on which the Endpoint Security Module is in Started State or turned on.
- **Stopped** - Number of computers on which Endpoint Security Module is in Stopped State or turned off.
- **Unavailable** – Number of computers where Endpoint Security modules of eScan is not available.
- **Unknown** - Number of computers where the status is unknown.
- **Total** - Total number of computers where Endpoint Security module of eScan is started, stopped, unavailable or the status is unknown.

- **Privacy**

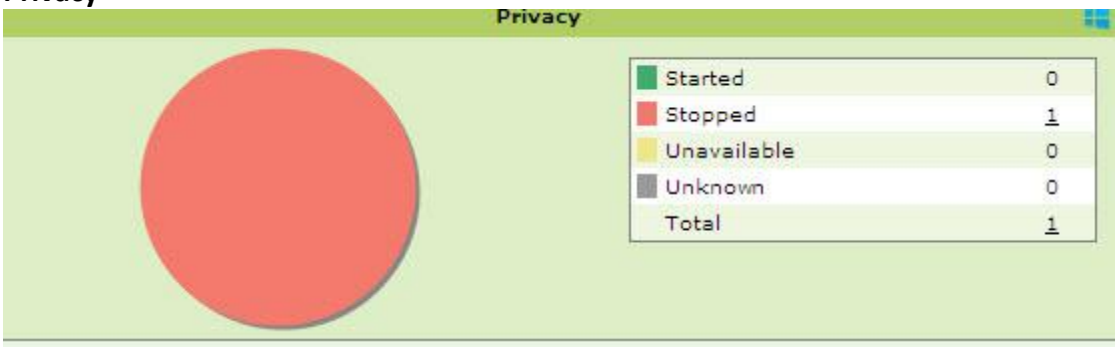


Figure 6.30

- **Started** - Number of computers on which Privacy Control Module is in Started State or turned on.
- **Stopped** - Number of computers on which Privacy Control Module is in Stopped State or turned off.
- **Unavailable** - Number of computers where Privacy module of eScan is not available.
- **Unknown** - Number of computers where status is unknown.
- **Total** - Total number of computers where Privacy module of eScan is started, stopped, unavailable or the status is unknown.

Note:
•  Icons at the top of every chart denote that the information is displayed for computers with respective operating systems (Windows, Macintosh or Linux). To know further details, click on the number of computers links for listed options.

- **Protection Statistics**

  This tab displays activity statistics of all Modules of eScan Client on all the Endpoints in pie charts. It displays the actions taken by eScan modules on the Endpoints as Count. You can reset the Protection Statistics using the **Reset Counter** option present in the window.

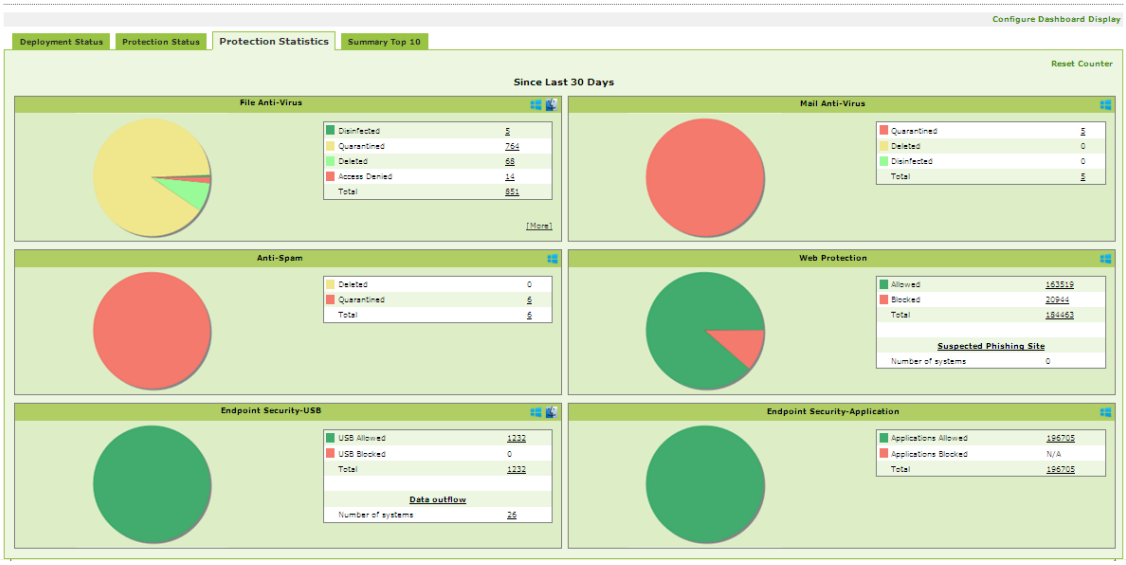


Figure 6.31

Note:
• Reset Counter option resets the Protection Statistics to 0, this option is useful when a group of Endpoints is infected with a Virus and **you have scanned and secured the computers. To monitor the group for** infection you can reset the counter to 0.

- When you click count you can see the details of the affected Computer, action taken and group to which it belongs to.

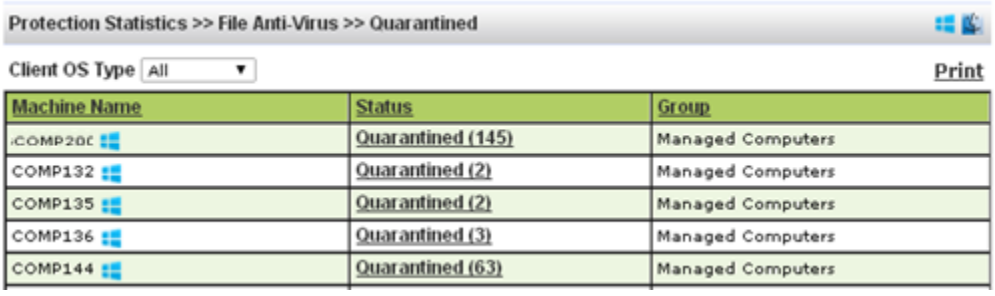


Figure 6.32

- Click on the status link to view the infected file name.

Protection Statistics >> File Anti-Virus >> Quarantined (COMP144)

Print

Date/Time	File Name	Description	User name
3/10/2014 12:11:38	C:\Documents and Settings\Deepali.COMP144\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache\f_00089b	Infected by Virus: JS:Exploit.BlackHole.QY (DB)	DEEPALI
3/10/2014 12:17:16	C:\Documents and Settings\Deepali.COMP144\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache\f_0008ba	Infected by Virus: JS:Exploit.BlackHole.QY (DB)	DEEPALI
3/18/2014 12:01:28	G:\firework.mp3.exe	Infected by Virus: Trojan.Generic.6709978 (DB)	DEEPALI

Figure 6.33

- Additional Protection Statistics can be viewed using the [More] option present on the interface.

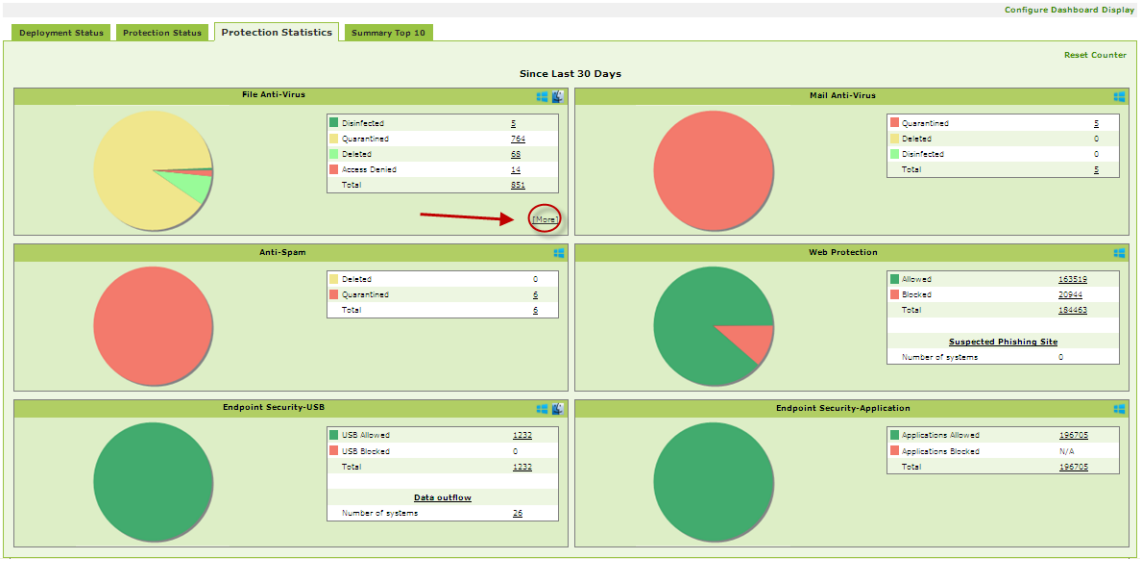


Figure 6.34

- It displays the statistics counter for the following –

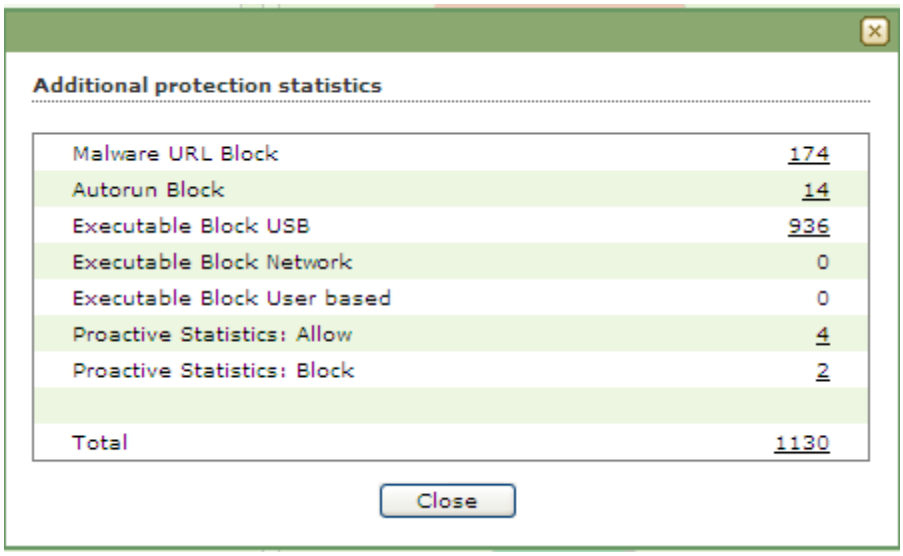


Figure 6.35

Note:
• Icons at the top of every chart denote that the information is displayed for computers with respective operating systems (Windows, Macintosh or Linux). *Know more details about the computers, click on the number of computers links for listed options*.

- **Summary top 10**

  This Tab displays top 10 Summary of various actions taken by eScan on all Endpoints. It displays list of applications allowed / blocked / computer names along with the chart and graph of the actions taken by eScan on occurrence of an event (Like unauthorized USB insertion in USB port of any Managed Computer) or detection of an infection. You can exclude or include desired options using **Configure Dashboard Display** Option present in the eScan Management Console.

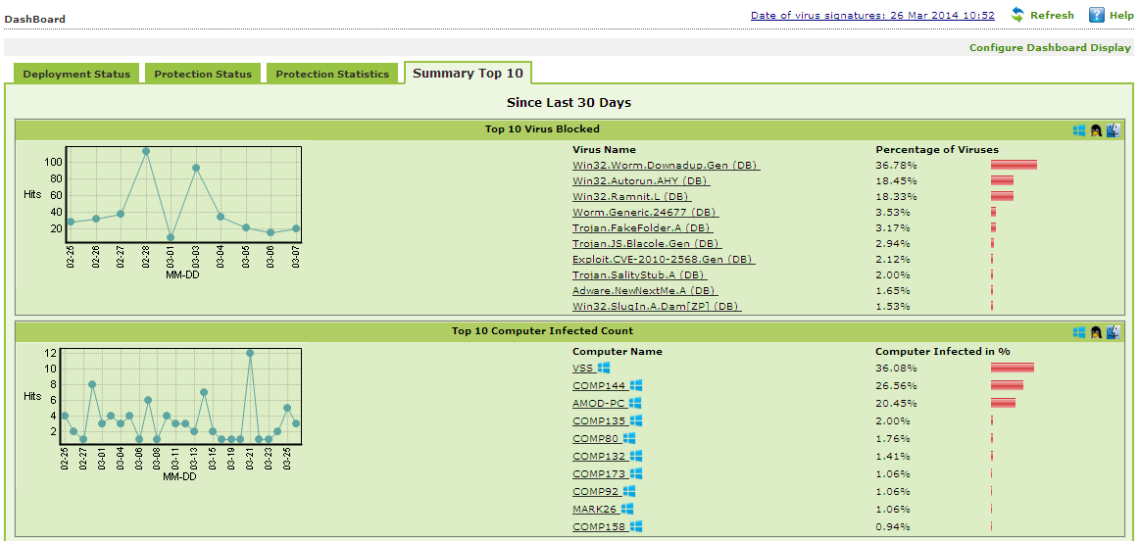


Figure 6.36

- **Configuring Dashboard**

You can configure the Dashboard to show pie charts and details of status, statistics and summary for desired modules. You can configure Dashboard display using following Steps --

- Click **Configure Dashboard Display** option present on the top Right Corner of the interface. Refer Figure – 6.37

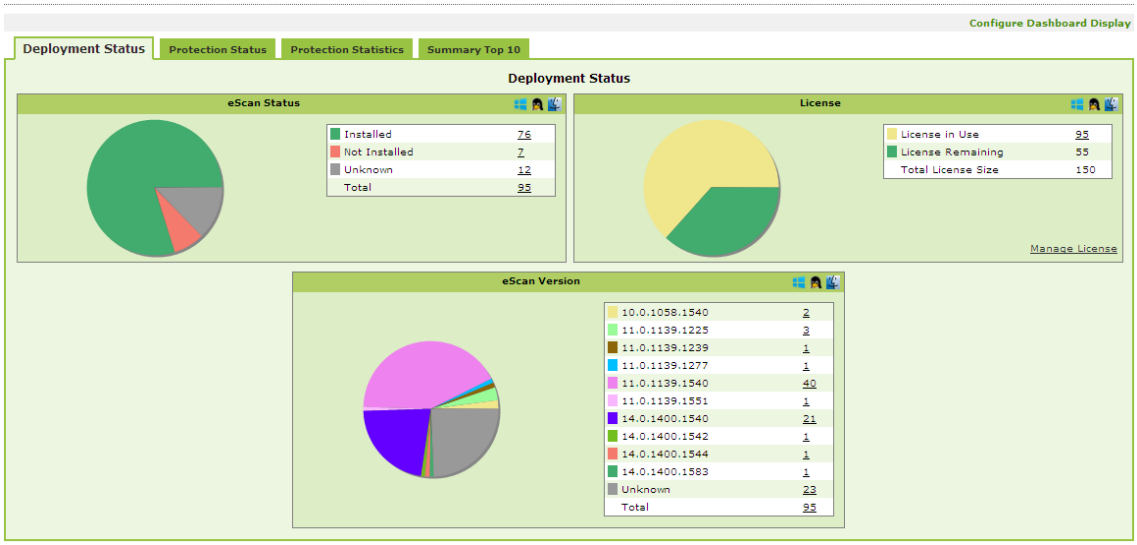


Figure – 6.37

- Now select **Checkbox** to choose the desired Module / Option that you wish to include in the Tabs present in Dashboard.

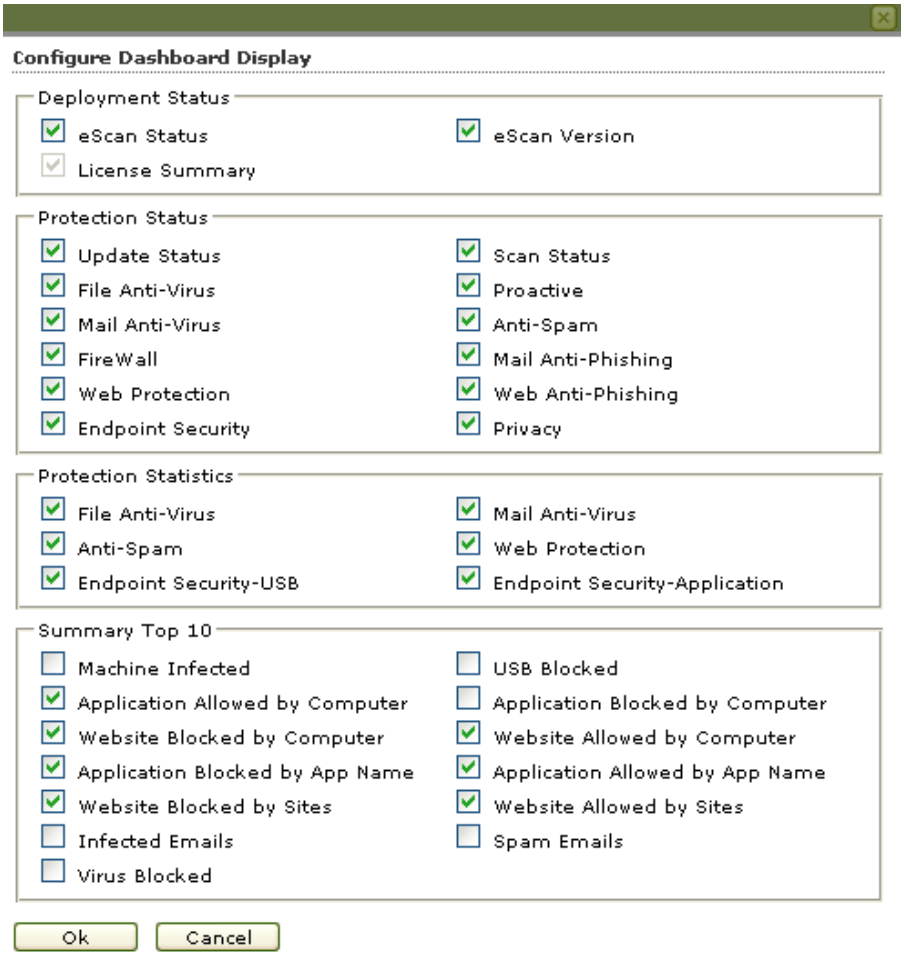


Figure 6.38

- Click **Ok** to save settings and close the window. **Charts**, **Information** and **Summary** for the selected modules will be displayed in respective tabs.

Note:
• Icons at the top of every chart denote that the information is displayed for computers with respective operating systems (Windows, Macintosh or Linux). *Know more details about the computers, click on the number of computers links for listed options*.

7. Managing Computers

This section helps you in creating logical computer groups, defining policies for the created groups, and creating tasks for the desired group of computers. It is recommended that you group all the computers on the network in Logical group; it will help you in defining tasks and policies and monitoring activity on every computer present on the network. These groups can be based on departments, user roles or designations in the company. Let us see the steps towards securing all the computers on the network.

- **Create Logical Computer Groups**
- **Move Computers to the created Computer Groups**

Creating Logical Computer Groups

For securing and managing Computers present on the network, create groups and then add all computers in the groups created by you. It will help in better management, monitoring and security of the Endpoints. You can create the groups using following steps.

1. Click **Managed Computers** option present in the Navigation Panel. Refer Figure - 7.1

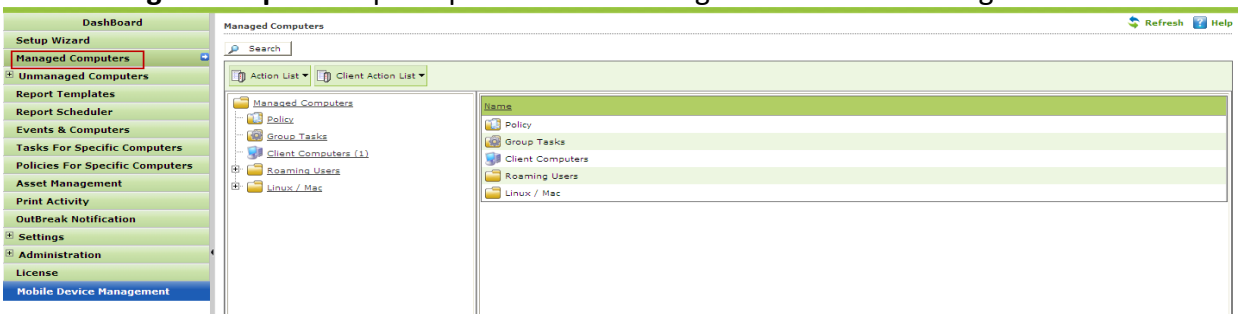


Figure - 7.1

2. This will open the **Managed Computers** section on the right; now click **New Group** option present in Action List drop down menu on the interface. Refer Figure -7.2

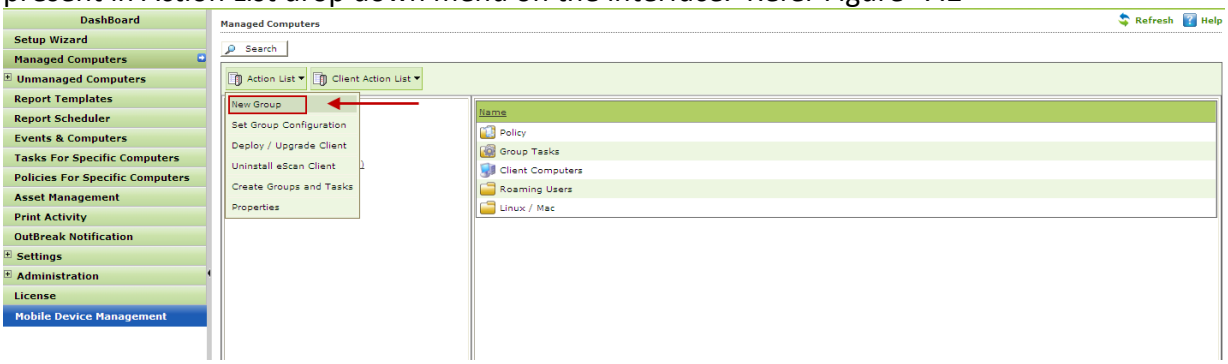


Figure -7.2

Creating New Group window will pop up, Fill in the New Group Name and Select the Group type as Normal user or Roaming user as desired using the drop down present on the interface.

Figure 7.3

Figure -7.4

3. Click **Ok**, the group will be created under **Managed Computers** in eScan Management Console. Refer Figure – 7.5

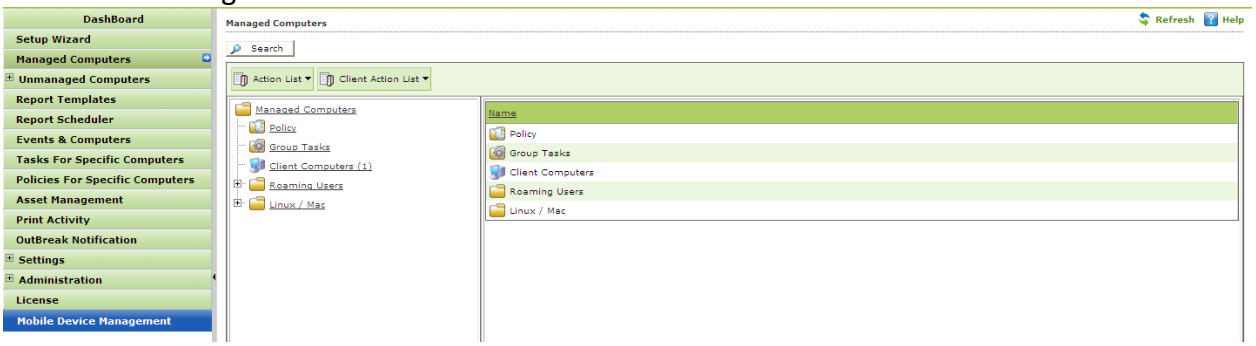


Figure – 7.5

Moving Computers to the created Groups

For installing eScan Client on the computers connected to the network and define policies and tasks on the basis of the groups they belong to, you will be required to move computers to the created groups. You can move the computers from **Unmanaged Computers** to desired groups created in the **Managed Computers** using the following options present in eScan Management Console –

- Moving Computers from **Network Computers.**
- Moving all Computers within selected **IP Range.**
- Moving Computers from **Active Directory.**
- Moving Computers from the **New Computers Found** List.

i. **Moving Computers from the Network Computers -** You can move the computers from the list of computers present in the Network Computers using the following steps –

1. Click **Network Computers** option present in the **Navigation Panel** under Unmanaged Computers. Refer Figure -7.6

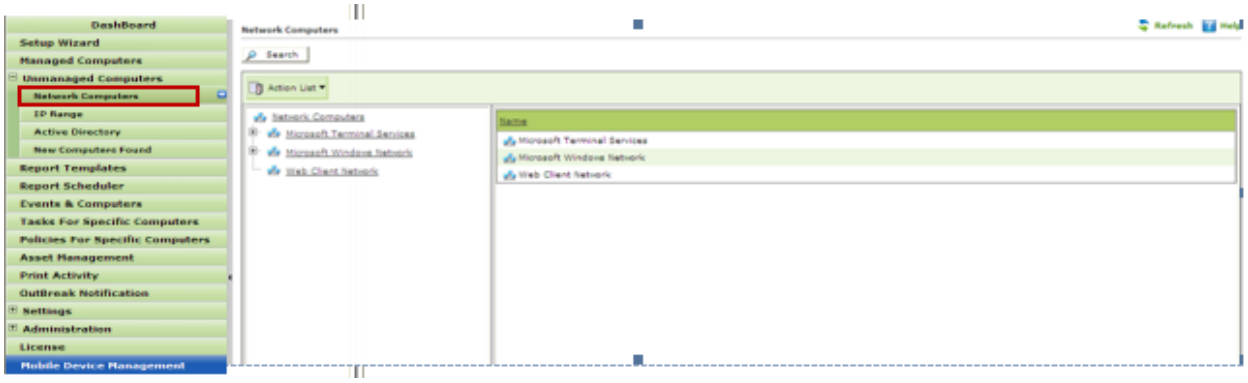


Figure -7.6

2. Now expand the **Microsoft Windows Network** tree and select the **workgroup** from where you wish to move computers to the desired group created in Managed Computers section. Refer Figure -7.7

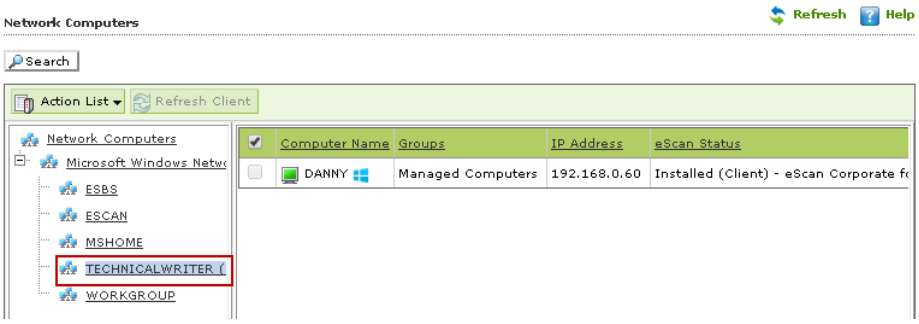


Figure -7.7

3. Now select the Computer(s) that you wish to move to the desired groups that you created under Managed computers. You can do so by selecting the check box beside the **Computer Names**. Refer Figure -7.8

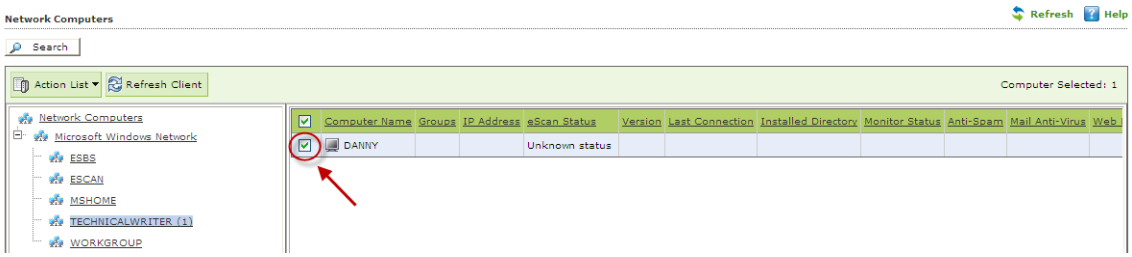


Figure -7.8

Also see <u>Viewing Properties</u> and <u>Setting Host Configuration</u>

4. Click **Move to Group** option present in the **Action List** drop down menu present on the interface. Refer Figure – 7.9

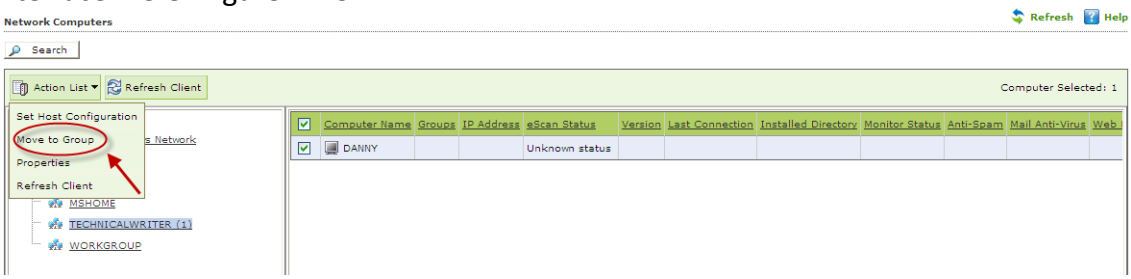


Figure – 7.9

5. Select Group window will open on the screen. Expand the Managed Computers tree to view the groups that you created earlier.
Refer Figure – 7.10

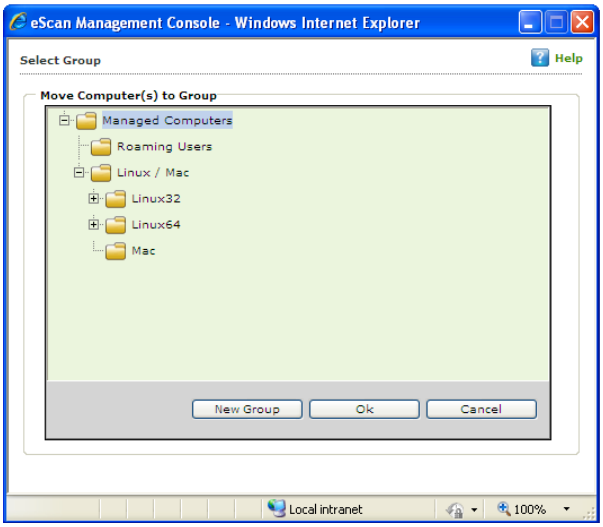


Figure – 7.10

6. Now select the group where you wish to move the selected computer(s). Refer **Figure – 7.11**

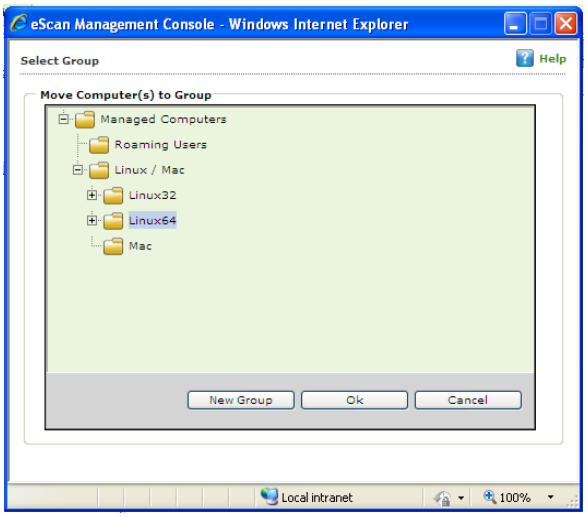


Figure – 7.11

7. Now Click **Ok**, selected Computer(s) will be moved to the group. Click **Cancel** if you do not wish to move the selected Computers to this group.

Also see Creating New Group from the Select Group window.

Viewing Properties of Selected Computer

You can view the Properties of the Selected Computer using following Steps –

1. Select the desired computer in the Network Computers List to View its Properties. Refer **Figure 7.12**

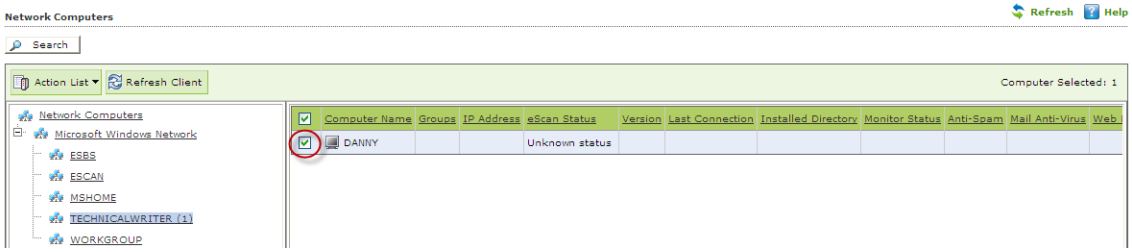


Figure -7.12

2. Now click **Properties** option in the **Action List** Drop down menu present on the interface. Refer **Figure – 7.13**

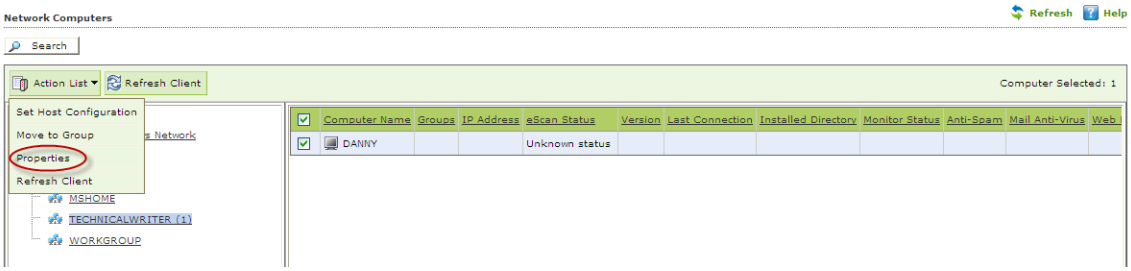


Figure – 7.13

3. This will open the **Properties** Window on a pop up. It displays general information of the computer like Computer Name, IP Address, User name and Operating System, along with details of the Antivirus installed, its version and update summary. It also displays protection status of all the Modules of eScan client. Refer **Figure – 7.14**

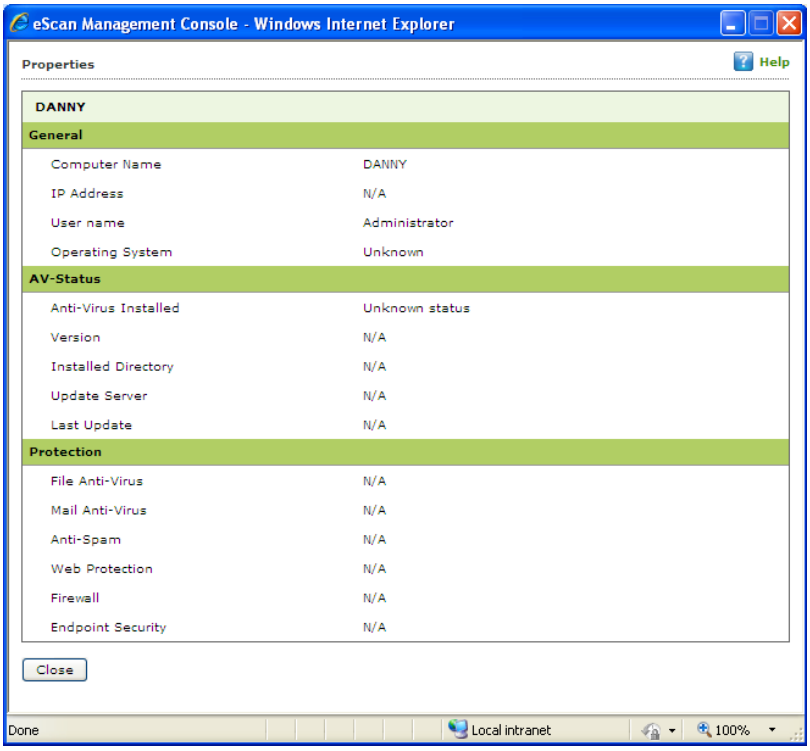


Figure – 7.14

Note:
• In case of Multiple Selection of Computers, the Properties option will be disabled.

- **Setting Host Configuration**

  For any computer with Windows operating system connected to the network, if you are not able to view / fetch its details using the Properties option. You can get the details after setting Host configuration that builds communication between the Server and the selected computer on the network.

  You can set Host Configuration using following Steps –

  1. Select the desired computer the Properties of which you wish to view/ fetch.
  2. Now click **Set Host Configuration** option present in the **Action List** drop down menu. Refer **Figure - 7.15**

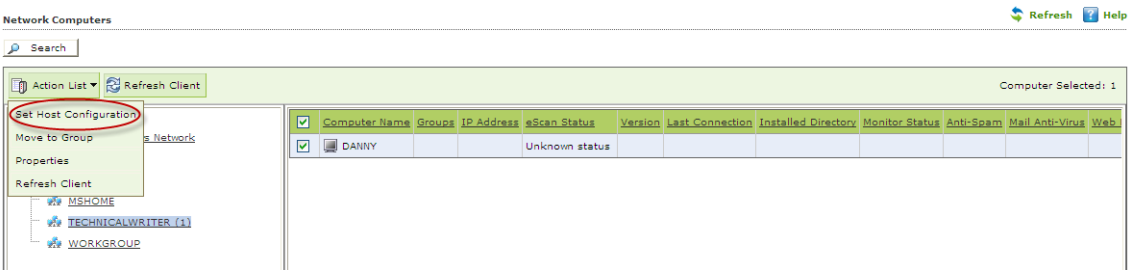


Figure – 7.15

3. Now write Remarks and define the Administrator Username and Password and then click **Save**. Refer **Figure - 7.16**

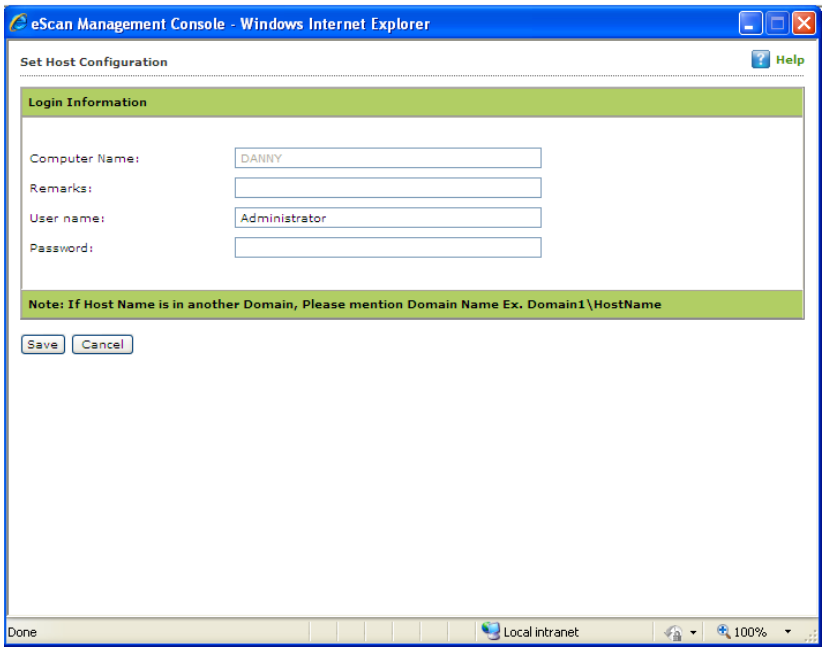


Figure - 7.16

4. You can now view the properties of the selected computer using the Properties option present in the Action List.

- **Creating New Group from the Select Group window**

  (The Select Group Window opens when you click Move to Group)
  Refer **Figure - 7.17**

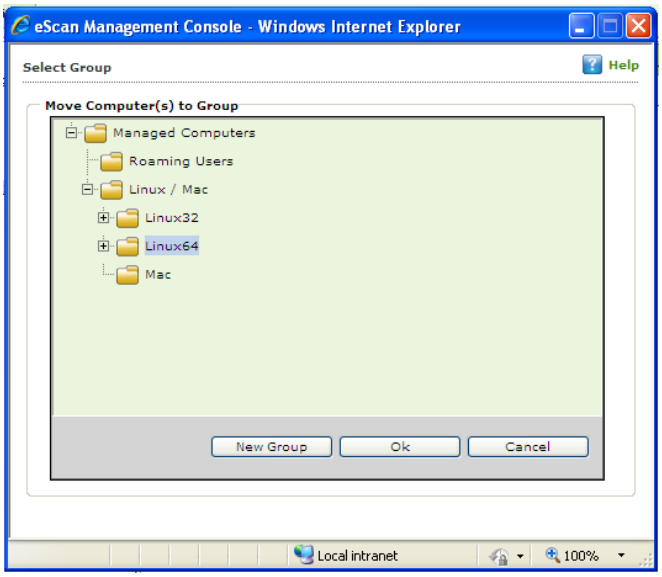


Figure - 7.17

You can create a **New Group** from this window using the following steps –

1. Click **New Group**, write the name of the Group and click **Ok**. Refer **Figure – 7.18**

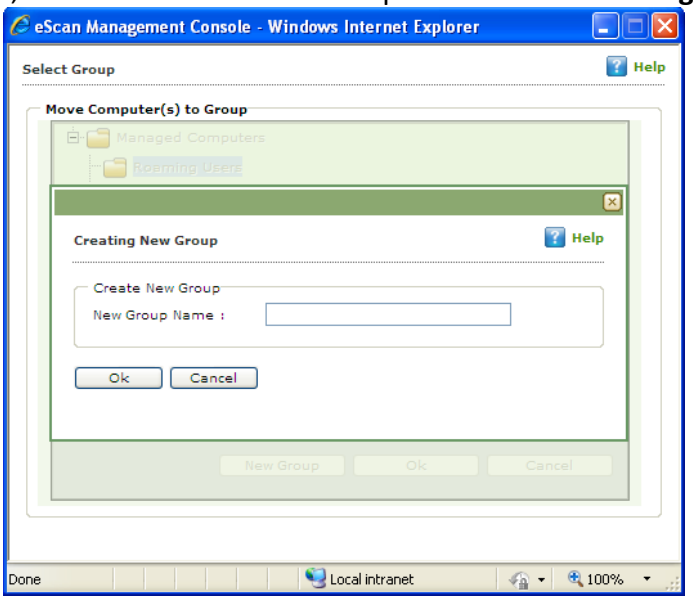


Figure – 7.18

2. The Group will be created instantly. Refer **Figure – 7.19**

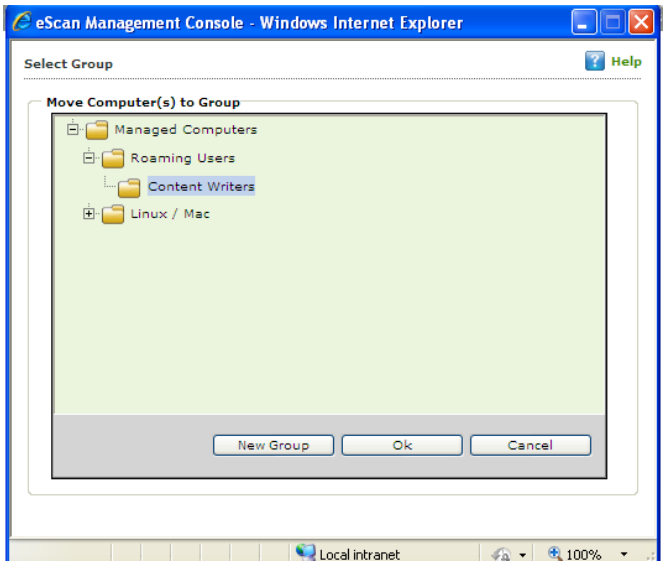


Figure – 7.19

- **Moving all Computers within selected IP Range to a Group –**

It includes following steps --

- **Adding New IP Range -** You can **Add** the Computers within certain IP range using the **IP Range** option present under **Unmanaged Computers**. It can be done using the following simple steps –

1. Click **IP range** option under Unmanaged Computers, and then click **New IP Range** option in the Window. Refer **Figure - 7.20**

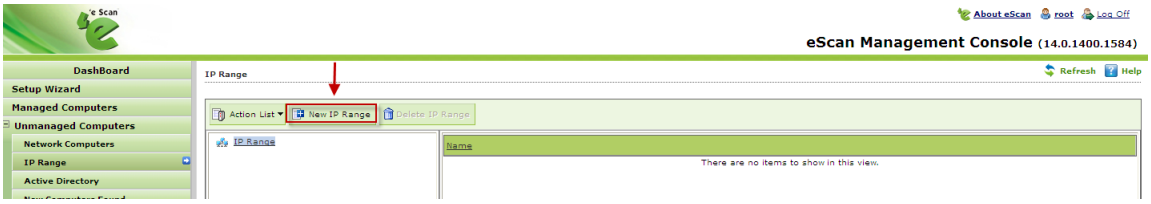


Figure - 7.20

2. You will be forwarded to **Specify IP Range** window. Specify the desired IP Range and click **Ok**. Refer **Figure – 7.21**

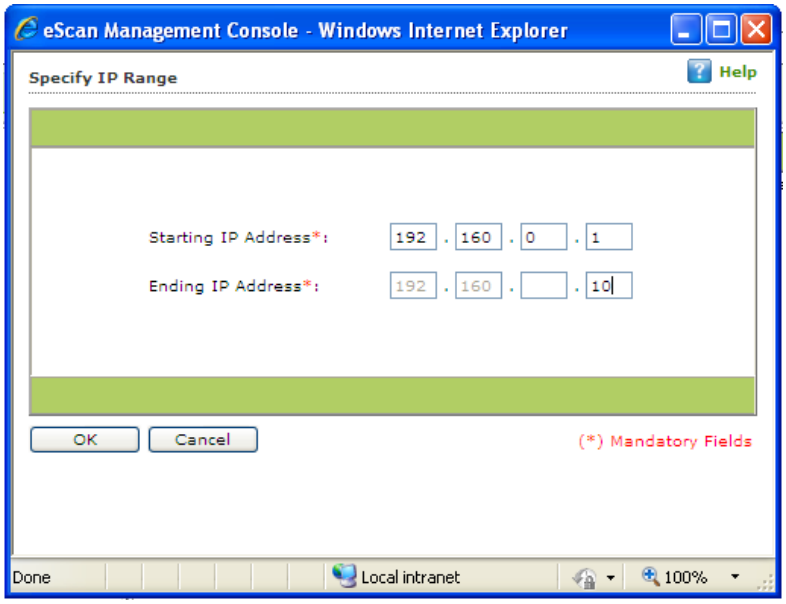


Figure – 7.21

3. The selected IP Range will be added to the IP Range tree. All computers present in that IP Range will be displayed when you select the IP Range on the interface.
Refer **Figure – 7.22.**

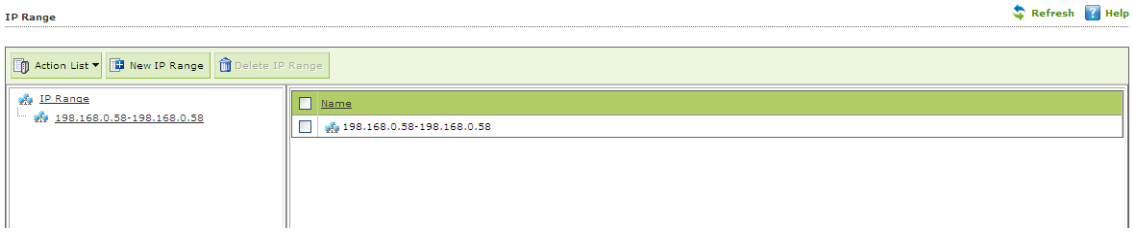


Figure – 7.22

Other details like IP Address of the computer, its group, Protection status (Unmanaged / Unknown/Protected / Not installed, Critical / Unknown); the table also displays Status of all modules of eScan.

- **Action List (Menu)**

  - **Setting Host Configuration -** Select the computer and define the Host Configuration settings using Set Host Configuration option present in Action List. This will help you in fetching Computer Properties before adding them to a group under Managed Computers. (For Endpoints with Windows operating system)

  - **Viewing Properties -** Select the Computer in the table and click Properties in the Action list, this will display all the details of the selected computer.

- **Refreshing Client –** Click this option to fetch latest information / details of the selected computer. This option is present on IP Range window as well as under Action List Menu.

- **Delete IP Range**

1. Select the desired IP Range and click Delete IP Range option present on the screen. Refer **Figure – 7.23**

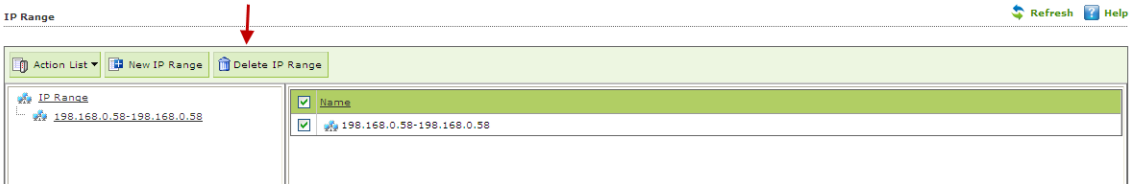


Figure – 7.23

2. To confirm the deletion click **OK** on the Pop up window.
   Refer **Figure 7.24**

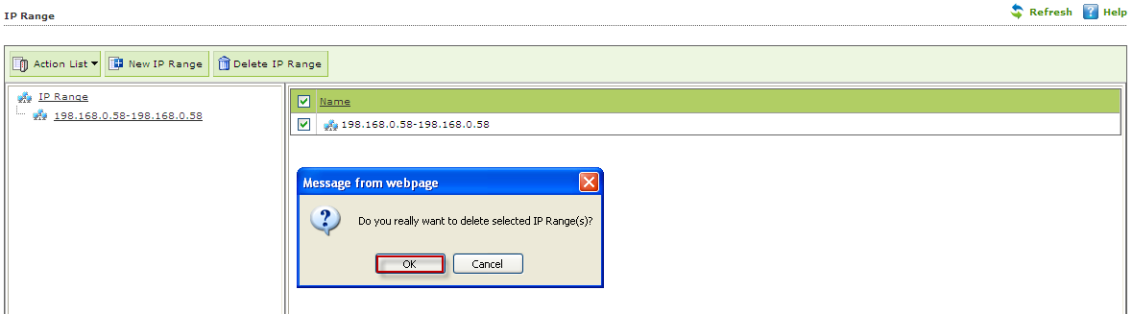


Figure – 7.24

3. The selected **IP range** will be deleted instantly.

- **Moving to a Group**

You can move the selected IP Range to any group under Managed Computers using following simple steps.

1. Select the IP range and all computers present in the selected IP Range that you wish to move from unmanaged computers to a group in Managed Computer. Refer **Figure - 7.25**

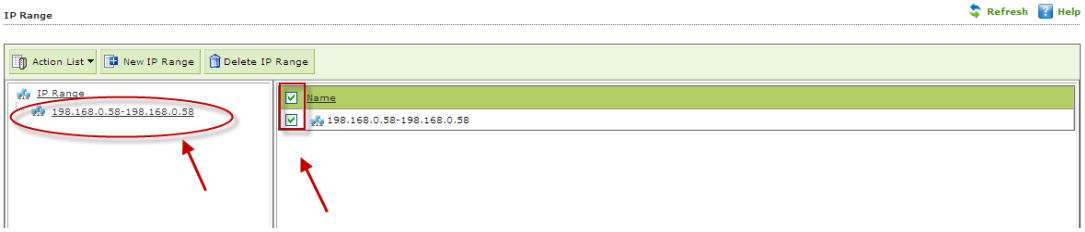


Figure – 7.25

2. Now Click **Move to Group** under **Action List** drop down menu. Refer **Figure - 7.26**

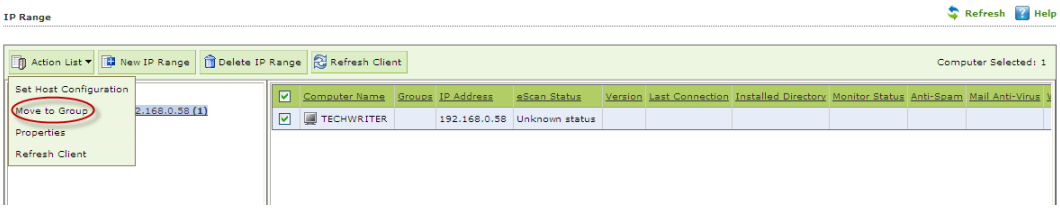


Figure – 7.26

3. You will be forwarded to the Select Group Window. Select the Group where you wish to Move the selected computers in the IP Range and Click **OK.** Refer **Figure -7.27**

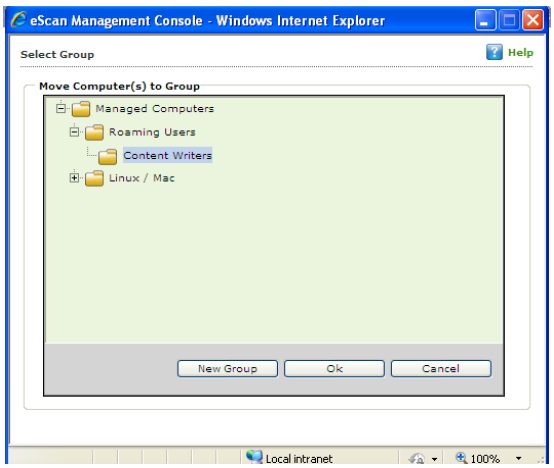


Figure – 7.27

4. The Selected Computer(s) will be moved to the selected group under **Managed Computers** section. Refer **Figure – 7.28**

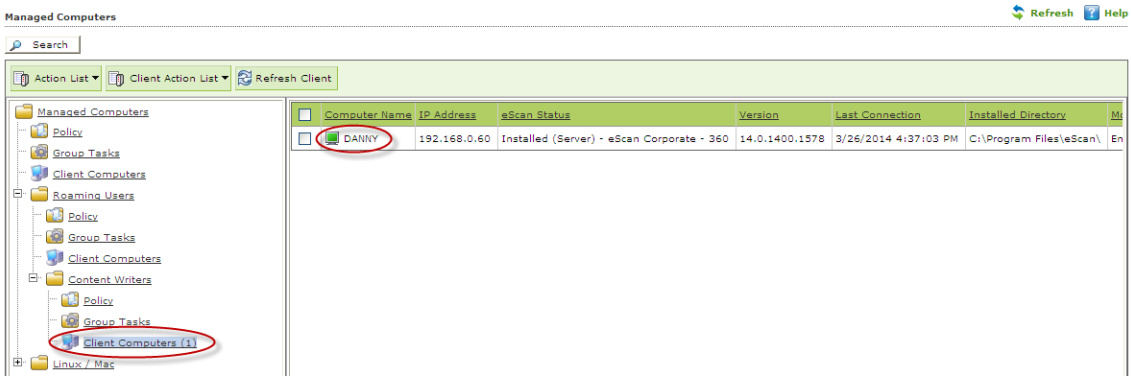


Figure – 7.28

i. **Moving Computer from Active Directory –** You can use the following simple steps to add computers from the Active Directory.

1. Click **Active directory** under Unmanaged Computers in the Navigation Panel of eScan management Console and Select **Active Directory** present in the tree. Now Click **Properties**. Refer **Figure – 7.29**

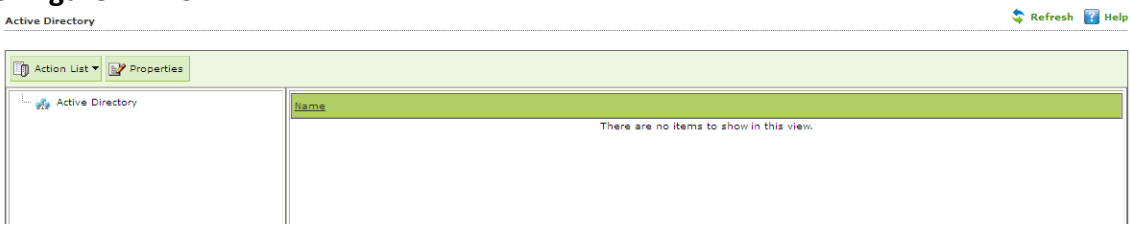


Figure – 7.29

2. You will be forwarded to the Properties window. Click **Add**. Refer **Figure 7.30**

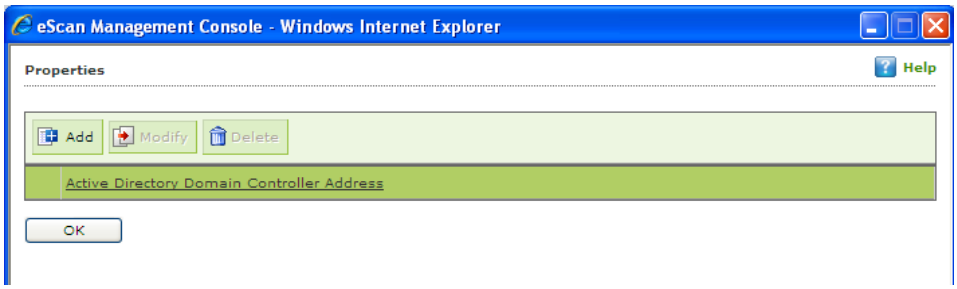


Figure 7.30

3. You will be forwarded to the Login Settings window. Fill in the required Login Credentials of Administrator to fetch data available on the Active Directory and click **OK**. Refer **Figure 7.31**

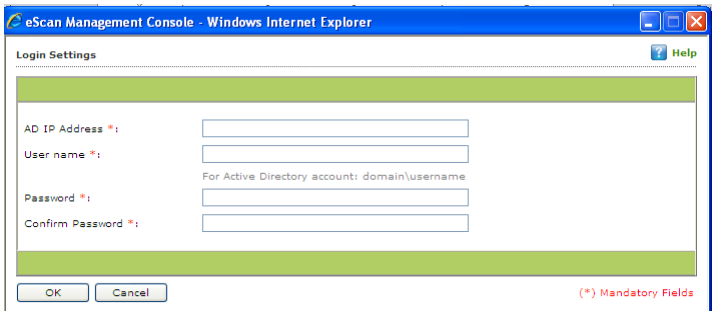


Figure 7.31

4. The details including IP Addresses from active directory will be added instantly. Refer **Figure 7.32**

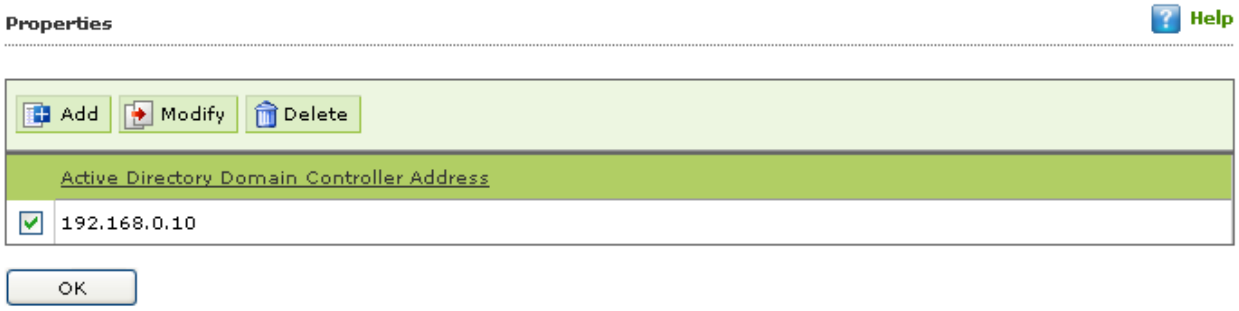


Figure 7.32

5. Select the Active Directory and click **OK**. The selected Active Directory will be added to the Active directory tree, to view the details click on the directory present under Active directory tree. Refer **Figure 7.33**

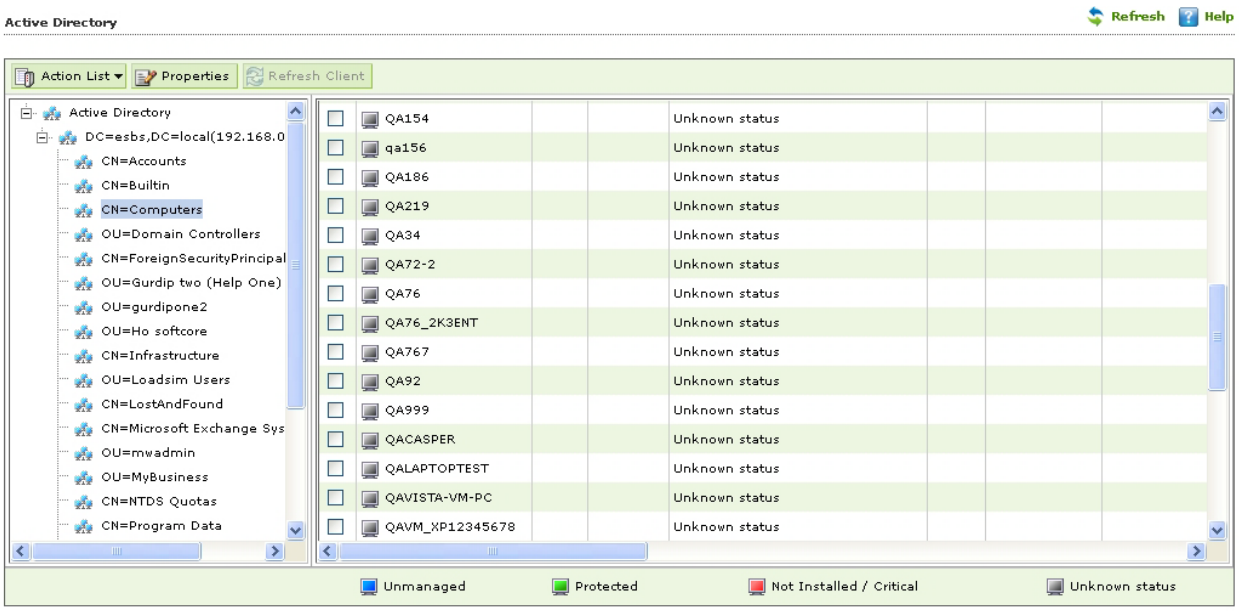


Figure 7.33

6. To move computers present in the Active Directory, select the computers in the list and click **Move to Group** option under Action List menu. Refer **Figure 7.34**

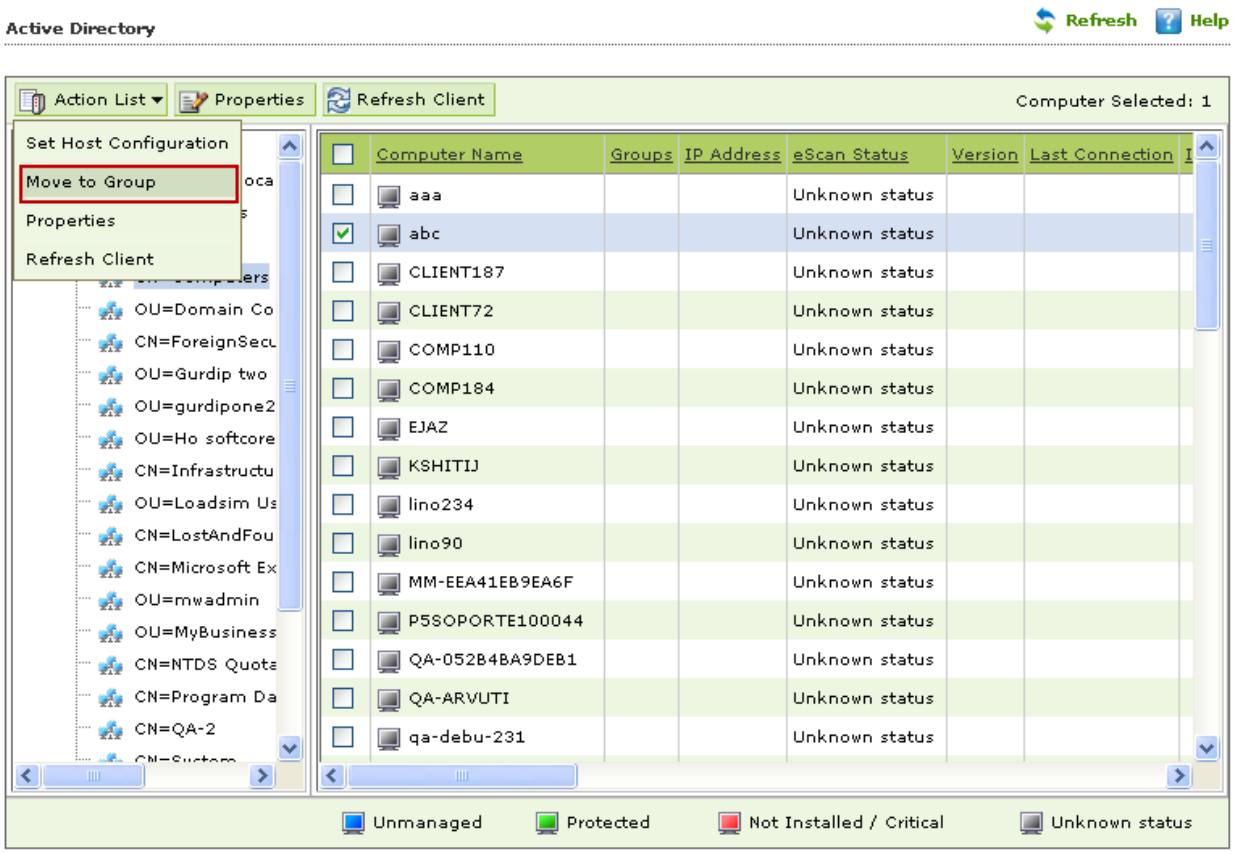


Figure 7.34

7. Select the Group and Click **OK**. Refer **Figure 7.35**

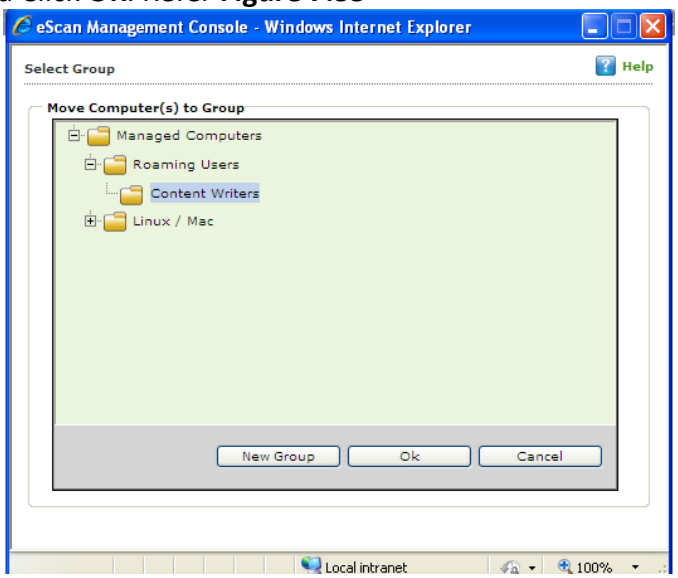


Figure 7.35

8. The selected computers will be moved to the selected group.

i. **Moving Computers from New Computers Found list -** List of all new computers connected to the network is generated in New Computers found list under Unmanaged Computers. Using the Action List Menu you can Set Host Configuration, Move Selected Computers to a Group, view Properties, Refresh Client or Export the New Computers List to excel file format if desired.

   Once the Computers are moved from Unmanaged Computers to Groups under Managed Computers, you can Perform Tasks, Set host configuration, Manage Policies, Deploy / Upgrade Client or deploy a Hotfix on all or any of the Managed Computer individually or in group.

ii. **Setting Host Configuration -** Select the computer and define the Host Configuration settings using Set Host Configuration option present under Client Action List. This will help you in fetching Computer details before adding them to a group under Managed Computers.

- **Active Directory Synchronization**

With Active Directory synchronization, you can synchronize eScan Centralized Console groups with Active Directory containers. New computers and containers discovered in Active Directory are copied into eScan Centralized Console automatically and the notification of the same can be sent to the system administrator. You can also choose to Auto Install or Protect discovered Windows workstations automatically. This allows you to minimize the time in which computers can become infected and reduce the amount of work you need to do to organize and protect computers.

Note:
• Endpoints running Mac OS, Linux, or Android are not installed automatically. You must install eScan on such computers manually.
• Ensure that your protect Windows Critical Server Manually if they are a part of Active Directory, before start of the Synchronization.
• If any computer or container is removed, it will also be removed from eScan Console when it synchronizes with Active Directory.
• By Default, the synchronization interval is of 60 minutes. You can set it to a minimum of 5 minutes.

After you have set up synchronization, you can set up email alerts to be sent to your chosen recipients about new computers and containers discovered during future synchronizations. If you choose to protect computers in synchronized Enterprise Console groups automatically, you can also set up alerts about automatic protection failures.

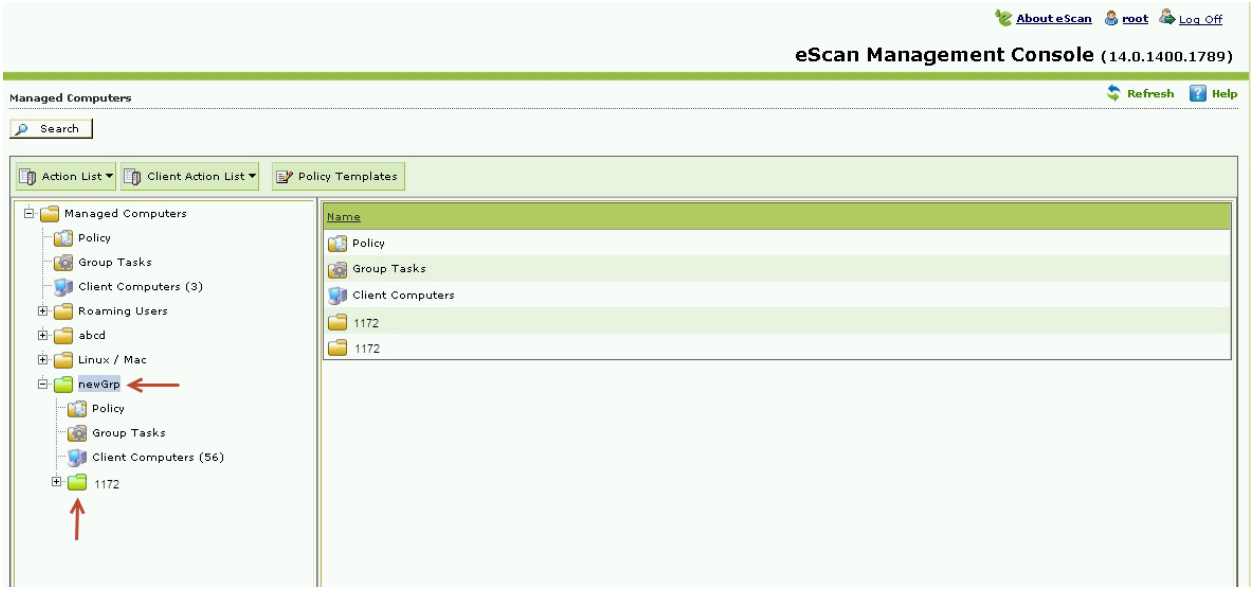
- **Auto installation of clients within Active Directory**

  Once the Active Directory is synced with the eScan Server, it will automatically install eScan on all the client machines in the Active Directory.

- **How does Active Directory synchronization work?**

  In eScan Console, you can have both "normal," unsynchronized groups that you manage yourself and groups synchronized with Active Directory.
  When setting up synchronization, you select or create a synchronization point: an eScan Console group to be synchronized with an Active Directory container. All computers and subgroups contained in the Active Directory are copied into eScan Console and kept synchronized with Active Directory.

Note:
• Active Directory groups will be denoted by Dark Green Color.

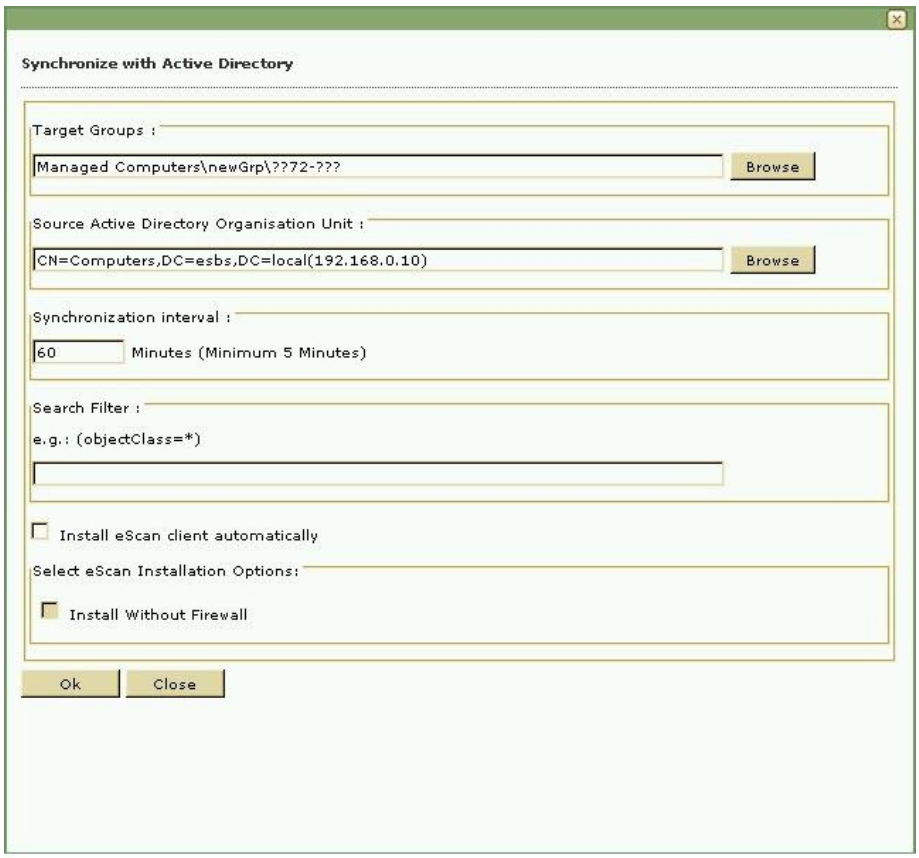


After you set up synchronization with Active Directory, the synchronized part of eScan Console group structure matches exactly the Active Directory container it is synchronized with. This means the following:

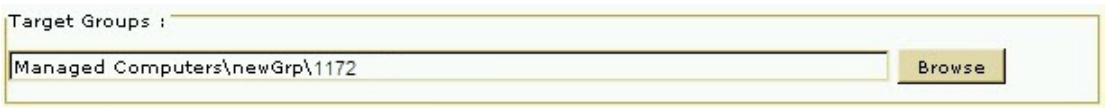
1. If a new computer is added to the Active Directory container, then it also appears in eScan Console.
2. If a computer is removed from Active Directory or is moved into an unsynchronized container, then the computer is moved to the unassigned group in eScan Console.

Note:
• A computer will not receive any new policies if it is moved to an unassigned group.

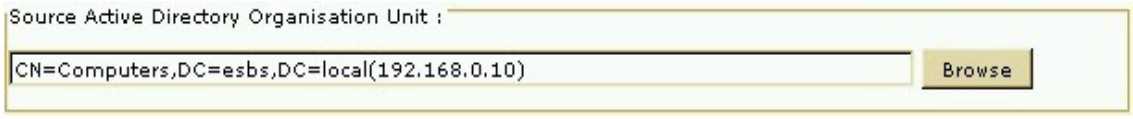
3. If a computer is moved from one synchronized container to another, then the computer is moved from one eScan Console group to the other.
4. If a computer already exists in an eScan Console group when it is first synchronized, then it is moved from that group to the synchronized group that matches its location in Active Directory.
5. When a computer is moved into a new group with different policies, then new policies are sent to the computer.



- **Target Groups:** Click browse and select the group on the management console to be synced with the Active Directory. This will create a tree structure as of the Source Active Directory Organization unit under the selected group.



- **Source Active Directory Organization Unit:** Click **browse** and select the path of the source Active Directory. The target groups in the above column will be synced with the group in this path.

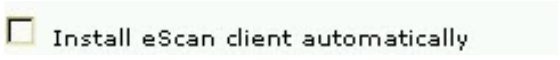


- **Synchronization Interval:** This option will allow you to set the synchronization intervals, the active directory will be automatically synced after the defined time period. The minimum interval that can be defined is of five minutes.

- **Search Filter:** Enter a value in the field and the search will be based on the strings mentioned here.

- **Install eScan client automatically:** Select this check box to install eScan automatically on to the client computers in the group. eScan will be automatically installed on the computers that are newly added in the group whenever next AD synchronization takes place .

Note:
• If at the time of synchronization, a computer in a group is shut down or not available, eScan will try to install eScan client automatically after every 60 minutes.



- **Install without Firewall:** Select this check box to install eScan without firewall on managed computers.

- Click **OK** to Apply settings

Note:
Automatic installation is applicable for Mac, Linux and Android platforms.

- **Properties**

  It will display the properties of the selected managed group and the Update Agents for the specified group. The properties of the group will be displayed into two sections: General and Update Agents.

  - **General:** This tab will display the following details about the selected group
  - **Name:** It will display the name of the group.
  - **Parent group:** It will display the name of the parent group that the group belongs to
  - **Group type:** It will display the type of users in a particular group, whether it is normal users or roaming users.
  - **Contains:** It will display the number of subgroups and computers under the group.
  - **Created:** It will display the date and time when this group was created.

- **Update Agent**

  This tab will allow you to add or remove computers as Update Agents. The computers added to this tab. This will reduce the traffic between the eScan Corporate Server and the client.

  Features of Update Agents:

  1. Download the antivirus signature updates from the eScan Server and share with other client machines on the network.
  2. Download the policy updates from the escan Corporate Server and share with the client in the group or the network
  3. The update agent will take event updates from the client computers in the group or network and share it with the eScan Corporate Server.
  4. Remote Deployment of clients can be done through Update Agents.

  Advantages of Update Agents

  1. Update Agent can be installed on any client computer connected to the network (where eScan is already installed).

2. Update Agent will take the signature updates from eScan Corporate Server and distribute the same to other managed computers in the group. (Bandwidth is saved).
3. Update Agent will alternatively query eScan Update servers on internet for getting updates whenever there is a connectivity problem between the update agent and eScan Corporate Server.

8. Managing Installations

After grouping all computers in logical groups using eScan Management Console, you can now install eScan Client as well as other third party software on the computers connected to your network. [**Conditions Apply**]

This section will give you an overview on following activities –

- **Installing eScan Client** - eScan client can be installed on computers connected to the network in the following ways
  - **Remote Installation** – It allows you to install eScan Client on all the computers in a selected group at once. You can initiate and monitor eScan Client installation using eScan Management Console. **For more click here**
  - **Manual Installation** – In case remote installation fails, you can allow computer users to install eScan client manually on their computers. It does not require any remote assistance. **For more Click here**
  - **Installing eScan using agent** - Installation of agent ensures that you have Administrator rights on the computer and you can now remotely install eScan Client on that computer. **For more click here**
- **Installing other Softwares (3rd Party softwares)** – eScan Management Console allows you to install third party softwares on networked computers remotely. **For more click here**.
- **Deploying hotfixes** - Using this option you can deploy hotfixes that eScan Server has downloaded from eScan website. This option is highlighted only when downloaded hotfix is saved in program files\escan\wgwin folder.
- **Connecting to the Client** – Using this option you can take the remote access of the selected Client Computer.
- **Viewing Installed Software List** – Using this option you can view list of softwares installed on Endpoints connected to your network.

- **Force Download –** This option is present under Client Action list in Managed Computer Section. You can update eScan client on any networked computer by using this option. It is required in cases where client has not been updated on the computer for many days. Select the Client Computer and click Force Download in the Action List Menu. It will initiate the Forced download process on selected Client computer.

Note: Conditions for third party software installation
• After starting the installation from **eScan Management Console**, no manual intervention should be required to complete the installation on Client Machine. Only automated installations can be done through **eScan Management Console.**
• Care should be taken that the installation file is not huge as it may impact internal network speed of your organization.

- **Send Message**

Send Message is a new add-on feature implemented in eScan Console, through which you can make broadcast to multiple Endpoints. If System Administrator wants to send an announcement or an alert message asking user to log off the system or contact the System administrator, this can be easily done using eScan console, without installing any third party software on the client system.

- **Sending a message to client:**

  - Select the Client computer and then go to Client Action List, now click Send Message and type your message and Click Send. The message will be sent instantly to the selected computer.

Note:
• The character limit is 120 only; if the system is not switched on or not connected to network for some reason, you will need to resend the message again to those endpoints.

- **Outbreak Prevention**

  This option allows the administrator to Deploy outbreak prevention policies during an outbreak that restricts access to network resources from selected computer groups for a defined period of time.

  - **Deploy Outbreak Prevention**

Administrator can define following policies:

- **Limit Access to shared folders-** After implementing outbreak Prevention policies, all computers in the selected group will have read only access to Shared Folders on their individual computers. The user can access the file but cannot modify it while accessing from any other computer.

- **Deny Write Access to Local Files and folders-** All Computers in the selected group will not have permissions to modify or create new file or folder in the selected folders or files as defined by the administrator.

- **Block Specific Ports-** Select and Block a Port or a Port Range for TCP/ UDP Protocols. The user will be notified at the start or after restoring original policies through a customizable popup message on client computer if desired.

- **Block All Ports (Other than trusted client-server ports):** Select this option and it will block all the ports except the trusted client-server ports in case of a virus outbreak.
- **Automatically restore outbreak prevention:** The administrator can set the hours (using the dropdown) after which the system will automatically restore the outbreak prevention settings.

- **Restore Outbreak Prevention**

  - **Notify Client users after restoring the original Settings:** Select this option to send notification to client users after restoring the original Settings.

Note:
The above outbreak prevention policies will be enforced on all the selected computers or groups. Incorrect configuration of these policy settings can cause major problems with the computers.

- **Remote Installation of eScan Client –**
  - **Preparing Client Computer for Remote Deployment**

    To install eScan Corporate 360 on the client system, check if the basic system requirements are in place.

  - **Configuring the settings on -**
    - **Windows XP Professional systems (Windows XP, 2000, 2003, all editions)**

      1. Click **Start**, and then click **Control Panel**.
      2. Double-click the **Administrative Tools** icon.
      3. Double-click the **Local Security Policy** icon.

4. On the navigation pane, click **Local Policies** folder, and then click **Security Options** folder.
5. Double-click **Network Access: Sharing and Security Model for Local accounts policy.**
6. Select Classic - Local user authenticate as themselves option from the drop-down list.
7. Click **Apply**, and then click **OK**.
8. **Double-click** the **Accounts**: **Limit local account use of blank passwords to console logon only policy**. The Accounts: Limit local account use of blank passwords to console logon only… dialog box appears.
9. Click **Disabled** option.
10. Click **Apply**, and then click **OK**.
    If Windows firewall is enabled on all locations, select **File and Printer Sharing** check box, under **Exceptions** tab (***Control Panel >> Windows Firewall >> Exception***).

- **For Windows XP Home:**

  Since Windows XP Home has limitations with regards to remote deployment, MWAgent should be installed on your system. You can download MWAgent from the eScan Web Console.

- **For Windows Vista /Windows 7 / Windows 8 / Windows 8.1**

1. Click **Start** on your desktop, and then click **Run.**
2. Now type **secpol.msc**, and then click **OK**. You will be forwarded to **Local Security Settings** window.
3. On the navigation pane, click **Local Policies** folder, and then click **Security Options** folder. The security policy appears.
4. Double-click **Network Access**: **Sharing and Security Model for Local accounts policy**.
5. Select Classic - Local users authenticate as themselves option present in the drop-down list.
6. Now click **Apply**, and then click **OK**.
7. Double-click the Accounts: Limit local account use of blank passwords to console logon only policy.
8. Click **Disabled** option. Now Click **Apply** and then click **OK**. If the firewall is enabled, select **File and Printer Sharing** check box, under **Exceptions** tab.
9. On desktop Click **Start**, and right-click **My Computer**, now click **Manage**. You will be forwarded to the Computer Management window.
10. On the navigation pane, click **Local Users and Groups** option, and then click **Users** folder, and double-click **Administrator**. You will be forwarded to the Administrator properties window.
11. Check **Password never expires** and uncheck **Account is disabled** check box.
12. Click **Apply**, and then click **OK**.

You can install eScan remotely on any computer or group present in Managed Computer using the following simple steps –

- **Option – 1 – Installing eScan Client on all Computers present in a Group**

1. Click **Managed Computer**

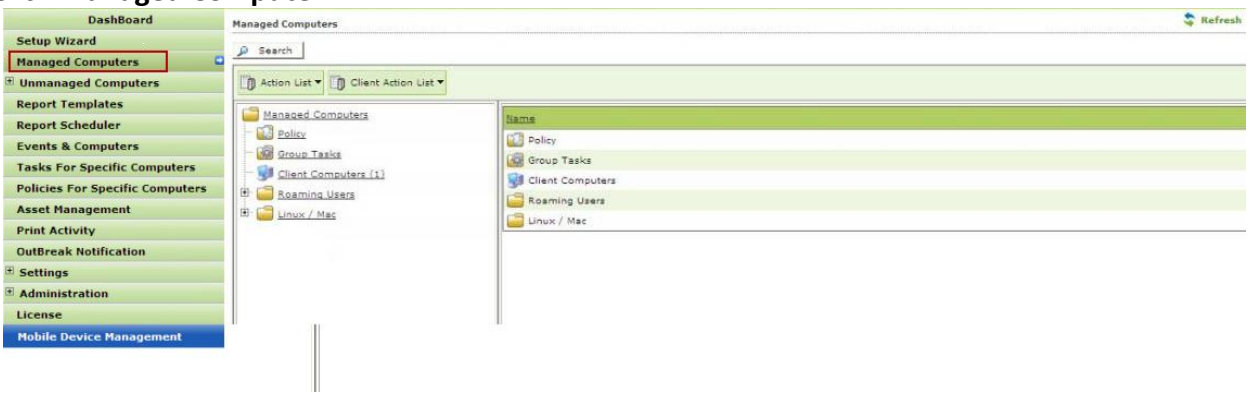


Figure 8.1

2. Now Select the **Group** where you wish to install eScan Client. Refer **Figure 8.2**

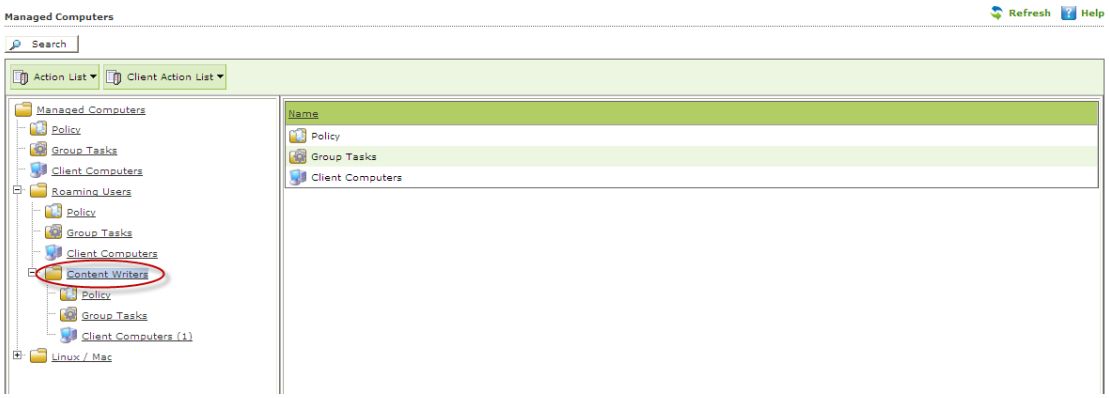


Figure 8.2

3. Now click **Deploy/ Upgrade Client** option present in the Action List drop down menu. Refer Figure 8.3

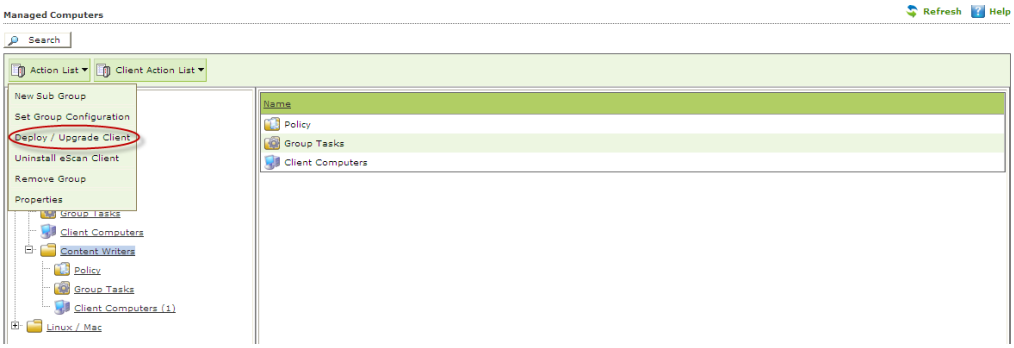


Figure 8.3

If you want to deploy only on specific computers then select those specific computers and follow all the above mentioned process from the client Action list drop down.

4. You will be forwarded to Client Installation Window, select the desired options and Click **install**. Refer **Figure 8.4**

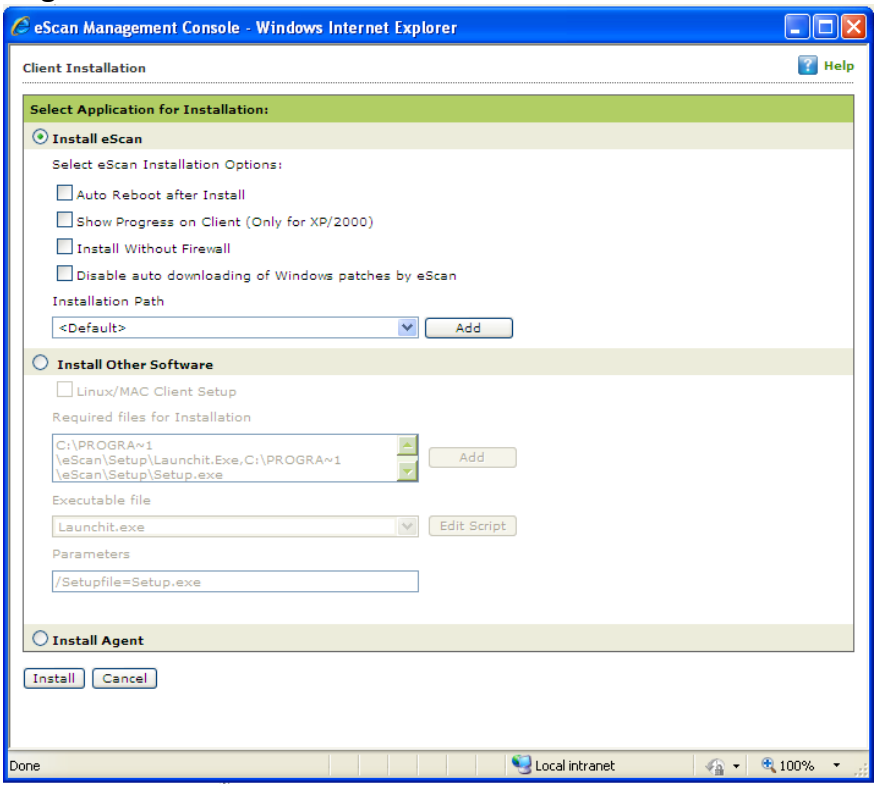


Figure 8.4

5. By Default eScan is installed at the following Path on Client computer.

C:\Program Files\eScan (default path for 32-bit computer) or C:\Program Files (x86)\eScan (default path for 64-bit computers)

6. You can also define the installation path where you wish to install eScan using the **Add** option. Refer **Figure 8.5**

Figure 8.5

7. Click **Install**.
8. The progress of File transfer will be displayed. Refer **Figure 8.5**
9. The progress of File transfer will be displayed.
10. Refer **Figure 8.6**

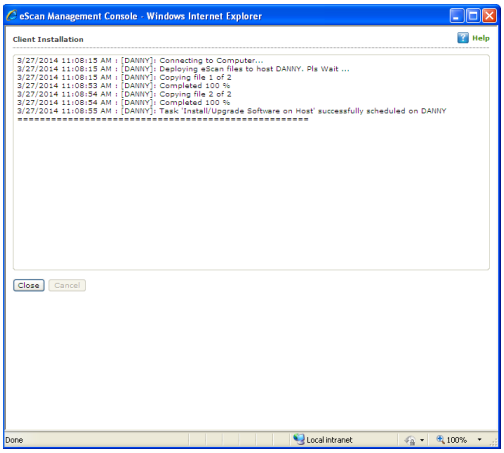


Figure 8.6

11. After Installation the eScan status will be updated in Managed Computers list "**Installed (Client) - eScan Corporate 360 for Windows**".

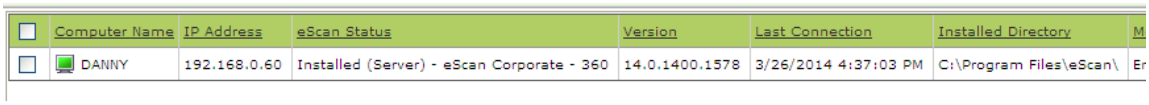


Figure 8.7

- **Option – 2 – Installing eScan Client on an individual Computer in a Group**

1. Click Managed Computer.

2. Now Select the **Group** which that computer belongs to.

3. Click **Client Computers** option present under the Group tree. Refer **Figure- 8.8**

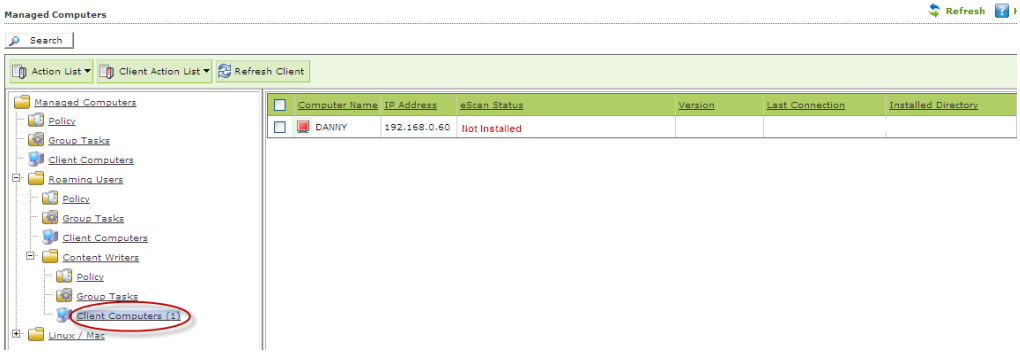


Figure 8.8

4. All computers present in the group will be visible in the list on the right. Select the computers where you wish to install eScan Client. Refer **Figure – 8.9**

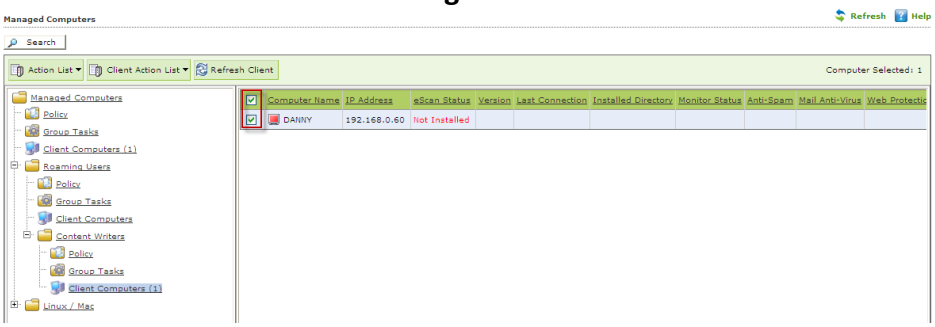


Figure – 8.9

5. Now click **Deploy / Upgrade Client** under Client Action List menu. Refer **Figure – 8.10**

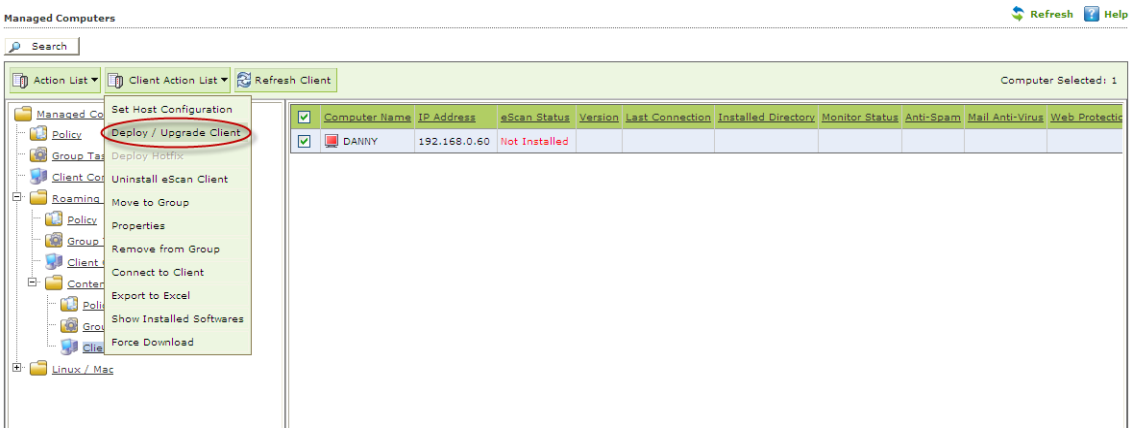


Figure – 8.10

6. You will be forwarded to the Client Installation window.

7. Now Select Install eScan option and also select the desired eScan installation option using the respective checkboxes present on the interface.

8. By Default eScan is installed at the following Path on Client computer.

   C:\Program Files\eScan (default path for 32-bit computer) or C:\Program Files (x86)\eScan (default path for 64-bit computers)

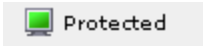
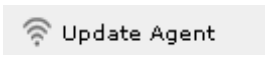
9. You can also define the installation path where you wish to install eScan using the Add option present on the interface.

10. Click Install to initiate the installation process on Client Computer. eScan Server will start copying files required for installing eScan Client on the client computer and progress of file transfer will be displayed on the interface.

11. After installation eScan status will be "**Installed (Client) - eScan Corporate 360 for Windows**".

Figure – 8.11

- **eScan Client Protection Status**

Status Name	Description
	This status is displayed when the File anti-virus module of eScan Client is enabled and eScan was updated in last 2 days.
	This status is displayed when either eScan is not installed on any computer or File AV / Real time Protection is disabled.
	This status is displayed when communication is broken between server and Client due to any reason.
	This status is displayed when a Computer is defined as an Update agent for the group.

- **Viewing Properties of a Group**

The Properties option present under Action List Menu in Managed Computers displays following important details of the Group.

- **General Tab**

  - Group Name
  - Parent Group
  - Group Type – Normal or Roaming User
  - Sub Groups or Number of Computers in that Group
  - Date of Creation of the Group

- **Update Agents**

  This tab displays list of computers that are acting as Update Agent for other Computers in the group, it gives you an option to **Add** or **Remove** a computer from this list. When you **Add** a computer to this list it becomes Update Agent for other computers in the group.

- **Creating Sub Groups**

  You can create a Sub Group under any group by using the following simple steps –

1. Click **Managed Computers.**
2. Select the Group under which you wish to create a **Sub Group**.
   Refer **Figure – 8.12**

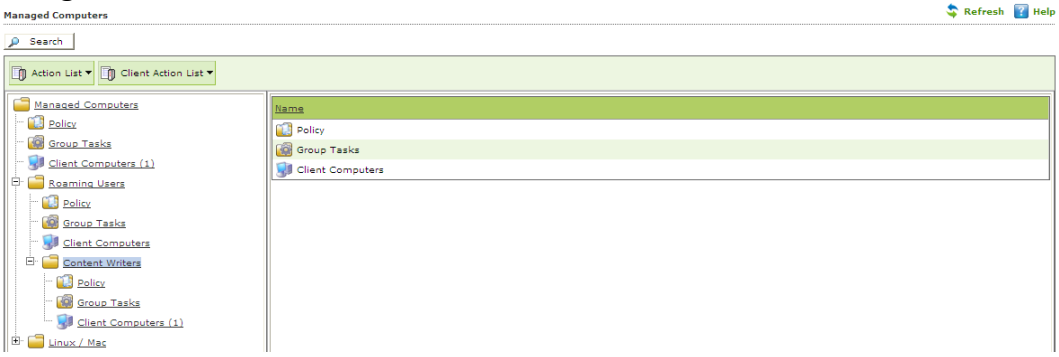


Figure – 8.12

3. Now click **New Sub Group** under **Action List** menu. Refer **Figure – 8.13**

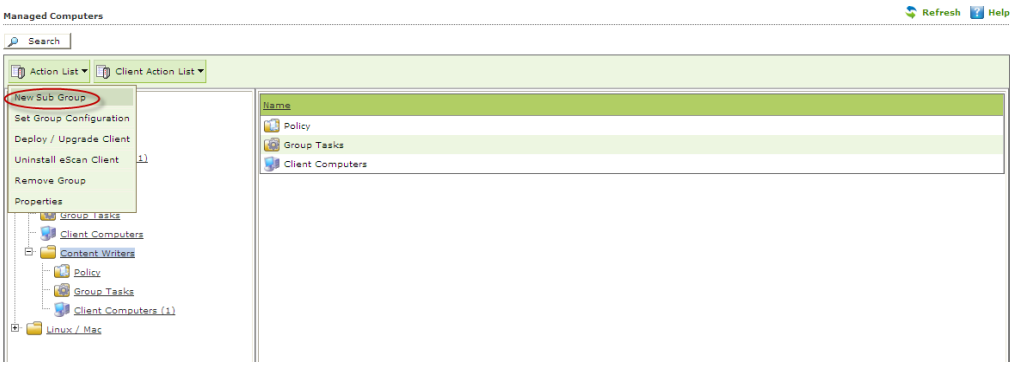


Figure – 8.13

4. You will be forwarded to Creating New Group window, write the name of the Group, Select the Group type using the Drop Down (**Normal User, Roaming User**) and click **Ok**. Refer **Figure – 8.14**

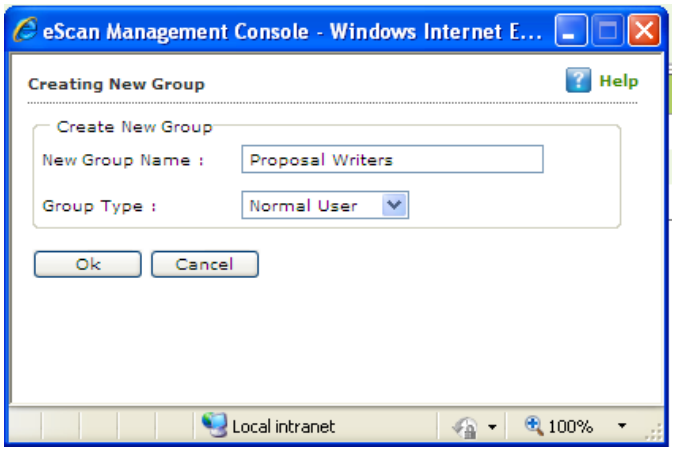


Figure – 8.14

5. The created group will be added under the Parent Group.

- **Removing a Group**

1. Select the Group that you wish to remove from the Managed Computers list and Click **Remove Group** under Action Menu. Refer **Figure – 8.15**

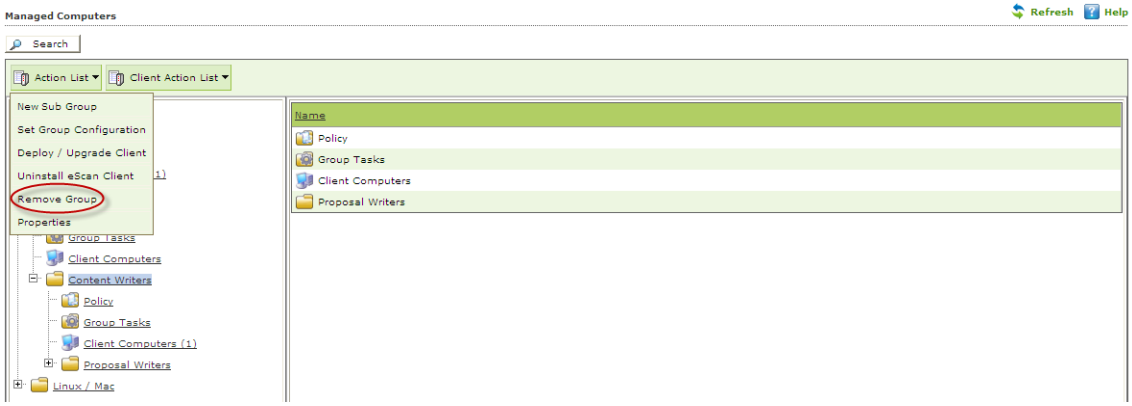


Figure – 8.15

2. To confirm click **OK**. The Selected Group will be removed instantly. Please note that you cannot delete a Group until it is empty.

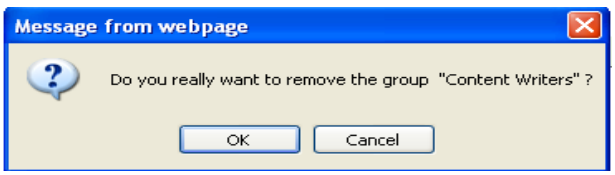


Figure – 8.16

- **Setting Group Configuration**

Using this option you can define single Username and Password to login for all the computers in the group. It can be done using the following simple steps –

1. Click **Managed Computers**.
2. Now Select the Group for setting the Configuration.
3. Now click **Set Group Configuration** under **Action List** dropdown menu.
4. Now define the Username and Password for the group and click **Save**.
5. The settings will be configured instantly.

Note – This is the System Login and Password that will be required for Login on any computer in that group. This option is valid for Computers with Windows Operating system only.

- **Refreshing Client**

Use the following steps to refresh the status of eScan Client on any networked computer.

1. Click **Managed Computer**.
2. Select the **Computer(s)** present under any Group.

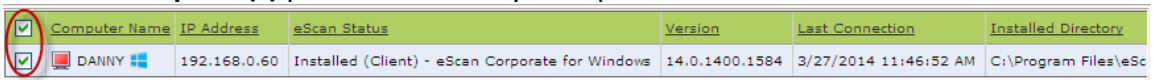


Figure – 8.17

3. Now click **Refresh**.
4. The Status will be refreshed once the process is over.

- **Moving Computer from one Group to Other**

Use the following steps to move selected computers from one group to other –

1. Click **Managed Computers.**
2. Select the desired computers present in a group.
3. Now click **Move to Group** option under **Client Action List** drop-down menu.
4. Select the group in the tree to which you wish to move the selected computers and click **OK**.
5. The selected computers will be moved to this group instantly.

- **Viewing Installed Software (on Client Computer)**

  Use the following Steps to remove selected computers from a group --

  1. Click **Managed Computers.**
  2. Select the desired computer present under Managed Computers.
  3. Now click **Show Installed Software** under **Client Action List** drop-down menu.
  4. List of all the Software installed on that computer will be displayed on pop up window in an instant.

- **Removing Endpoints from a Group in Managed Computers**

  Use the following Steps to remove selected computers from a group --

  1. Click **Managed Computers.**
  2. Select the desired computers present in a group that you wish to remove from Managed Computers.
  3. Now click **Remove from Group** option present under **Client Action List** drop-down menu.
  4. Click **OK** to confirm.

- **Installing eScan on Linux and MAC Computers**

  For installing eScan on Linux or Mac computer please install the Agent on the Linux or Mac computers and then proceed to install eScan, it can be done with the following simple steps –

  1. **Install Agent on Linux or Mac Computers.**
  2. **Install eScan Client after installing Agent on Linux or Mac Computers.**

- **Steps for Installing Agent on linux and Mac Computers**

  - **Installing Agent on Linux(Debian based Operating System**) –

    1. Download agent from the link sent on mail and save it at the desired path on the computer where you wish to install eScan Client.
    2. Open the terminal for installing Agent.
    3. Installation of Agent requires root or sudo user authentication.
    4. After Login as root or sudo user, go to the path where the **Agent_setup.deb** file has been saved.

5. Install the agent from the path using the following command – ***dpkg – i***. (**for RPM based setup – Rpm-ivh)** – Refer **Figure 8.18**

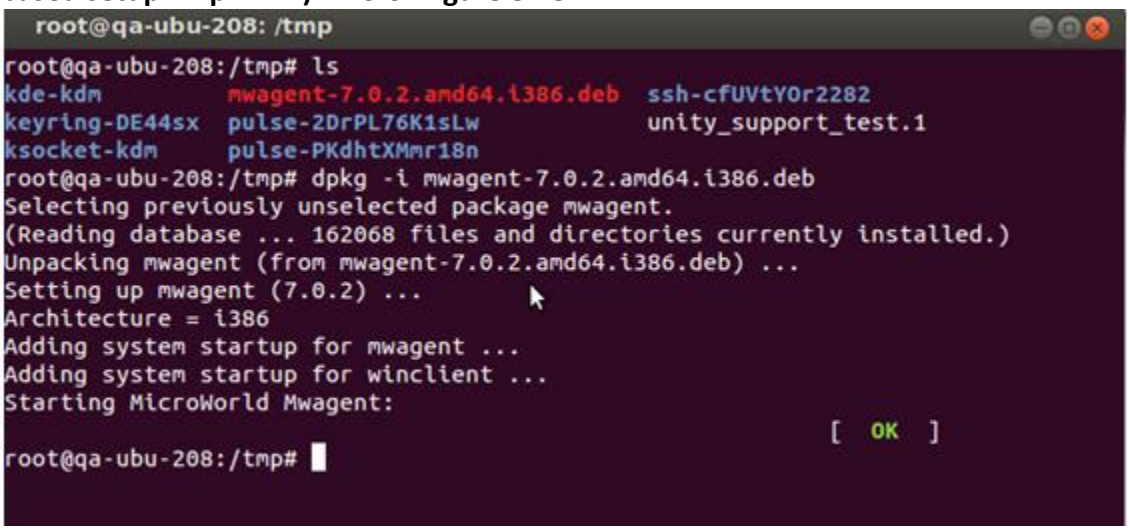


Figure 8.18

6. Agent installation will start, on completion you will be informed through a message and the Agent will start on you computer.

- **Installing Agent on Mac Computers** –

1. Download agent from the link sent on mail and save it at the desired path on the computer where you wish to install eScan Client.
2. Go to the Path where Agent is saved.
3. Double click on the **Agent_Setup.dmg** file to start the installation.
4. This will start the Agent Installation Wizard. Refer **Figure 8.19**

Figure 8.19

5. Now double click on eScan Agent, as shown above. This will start the installation process. You will be forwarded to the Introduction Window.
6. Click Continue. Refer **Figure 8.20**

Figure 8.20

7. This will forward you to the Read Me window, read the system requirement and click continue. Refer **Figure 8.21**

Figure 8.21

8. You will be forwarded to License Window. Read the agreement and click continue. Confirm by clicking **Agree**. Refer **Figure 8.22**

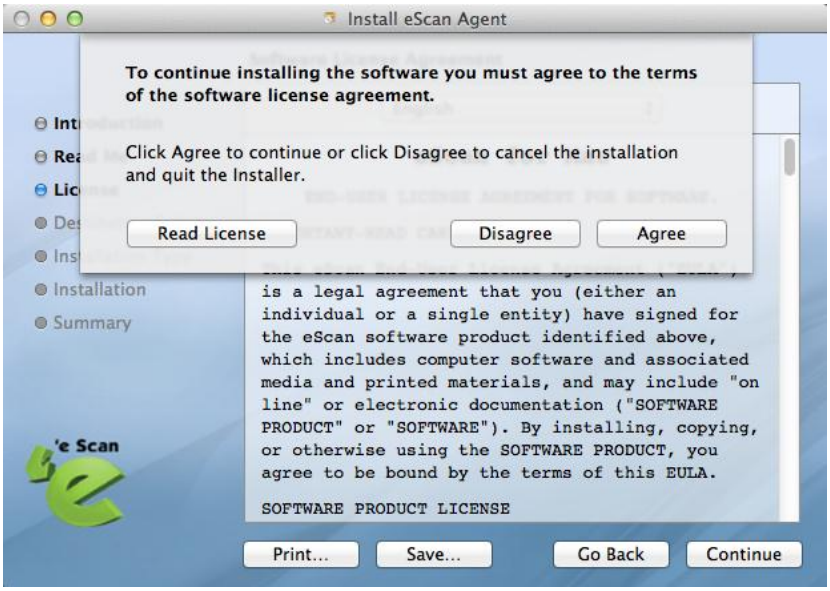


Figure 8.22

9. Now select **eScan Agent Install** by clicking on the checkbox and click **Continue**. Refer **Figure 8.23**

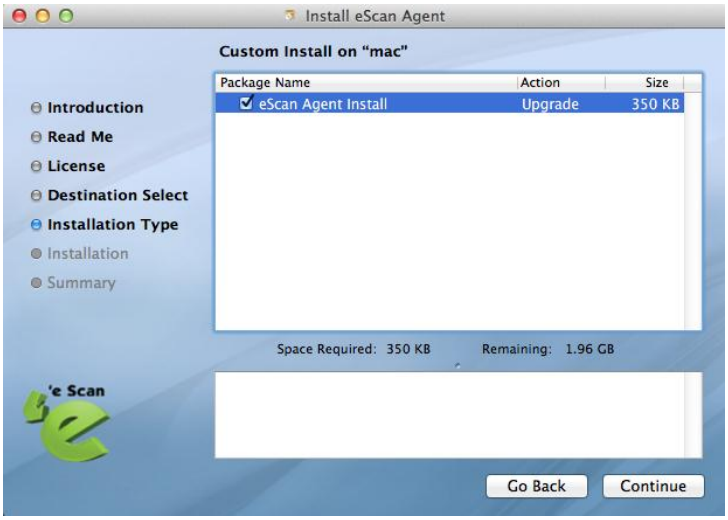


Figure 8.23

10. Select the desired destination folder "**Change install Location**" and click install.
11. You will be informed once the installation is over. Click **Close**. Refer **Figure 8.24**

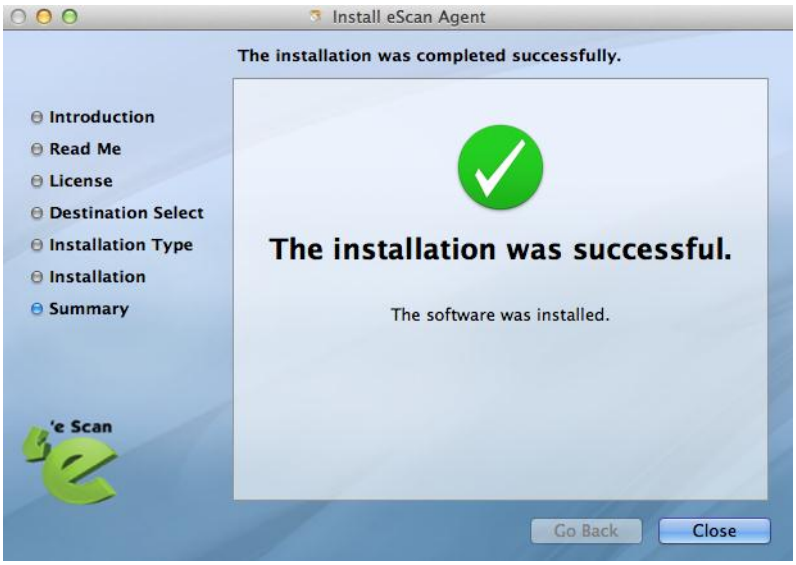


Figure 8.24

- **Steps for installing eScan Client on Linux or Macintosh Computers**

1. Install Agent on Linux or Mac computers manually.
2. Now Login to eScan Management Console and Select the computer and Refresh the Client using refresh Client option in eScan Management Console.
3. A link will be created for downloading the setup file of eScan Client for that computer,you will be re-directed to escanav.com from where you can download the setup file. Refer Figure 8.25

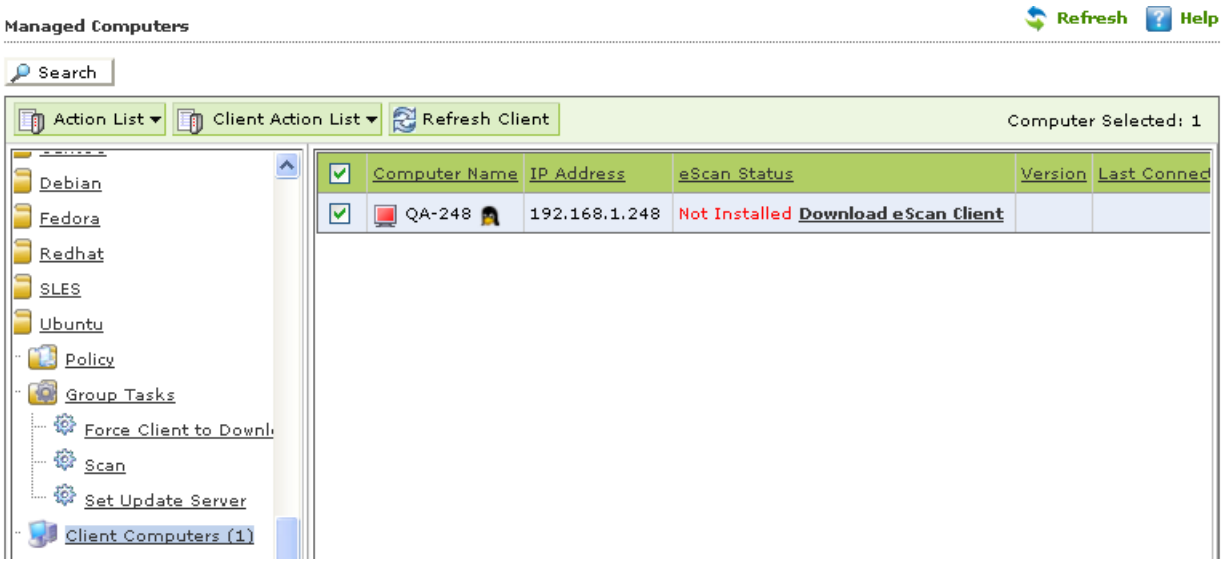


Figure 8.25

4. Download the client Setup from the link on the computer where eScan Corporate 360 server is installed.
5. For deploying the downloaded setup on selected Linux/ MAC computer Click on Deploy/ Upgrade client option present under Client Action List menu, click on Install other software and select Linux / MAC Client setup option, Figure 1

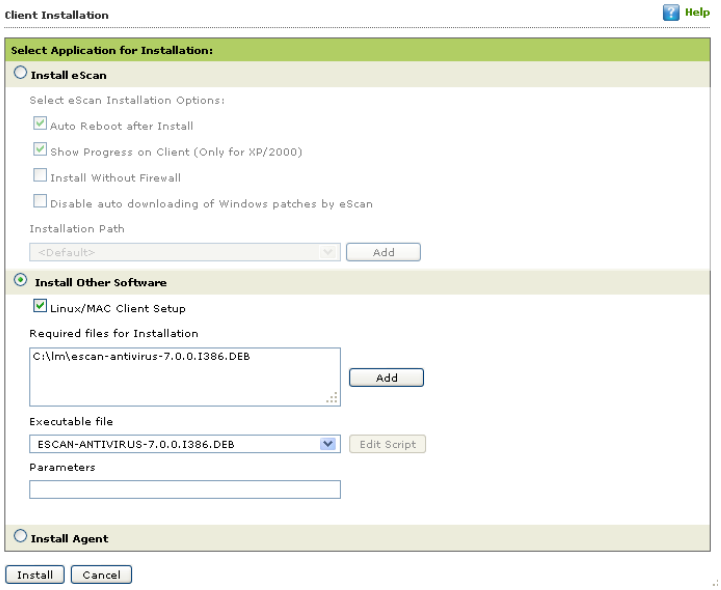
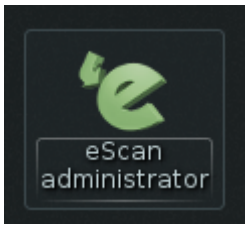


Figure 8.26

6. Click Install to initiate the installation process.
7. You will be informed once the installation is over.

In Linux

- eScan Administrator Icon will be displayed on desktop.



In Mac

- An Icon of eScan will become visible in the **Dock** on the desktop. You can access eScan using the same icon.

- **Uninstalling eScan Client(Windows, Mac and Linux)**

  Use the following simple steps for uninstalling eScan Client on any networked computer.

1. Select the Computer and click **Uninstall eScan Client** under Client Action List menu. Refer **Figure – 8.27**

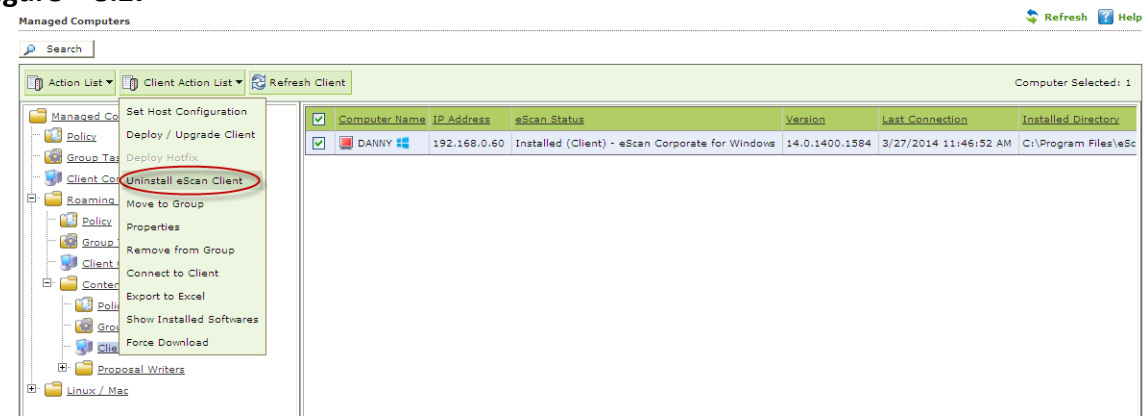


Figure – 8.27

2. You will be forwarded to the **Client Uninstallation** window Refer **Figure – 8.28**

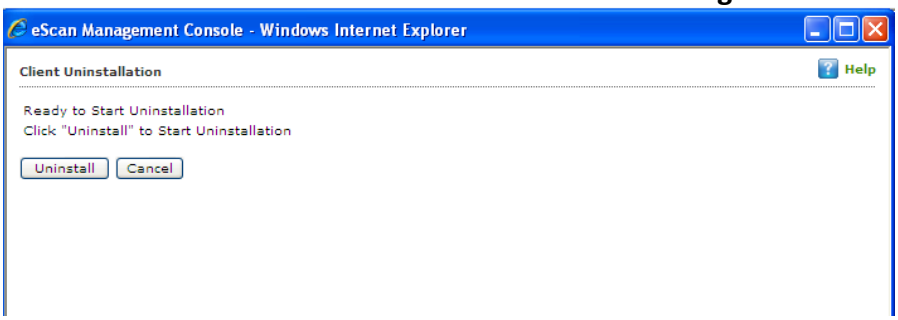


Figure – 8.28

3. The task will start instantly. **eScan Management Console** will display the progress details. Refer **Figure – 8.29**

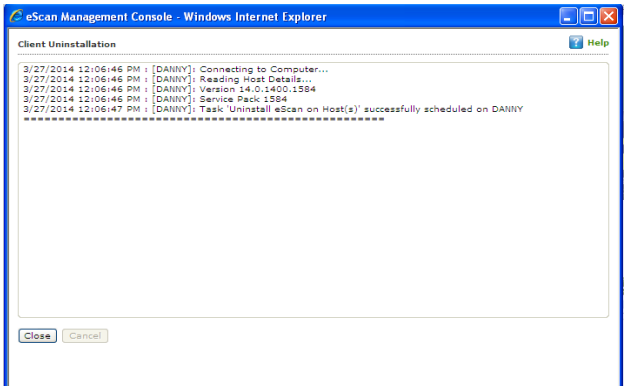


Figure – 8.29

4. Click **Close** when the Uninstallation process is over.

Note:
• You can uninstall eScan Client from all the computers in the group by selecting the Group and then Click **Uninstall eScan Client** under Action List drop down menu.

Manually Installing eScan Client on Network Computers

Manual Installation is required on computers where remote installation through eScan Management Console is not possible. Download link for manually installing **eScan Client** or **Agent** are displayed on the **Login Page** of eScan Management Console. Refer **Figure - 8.30**

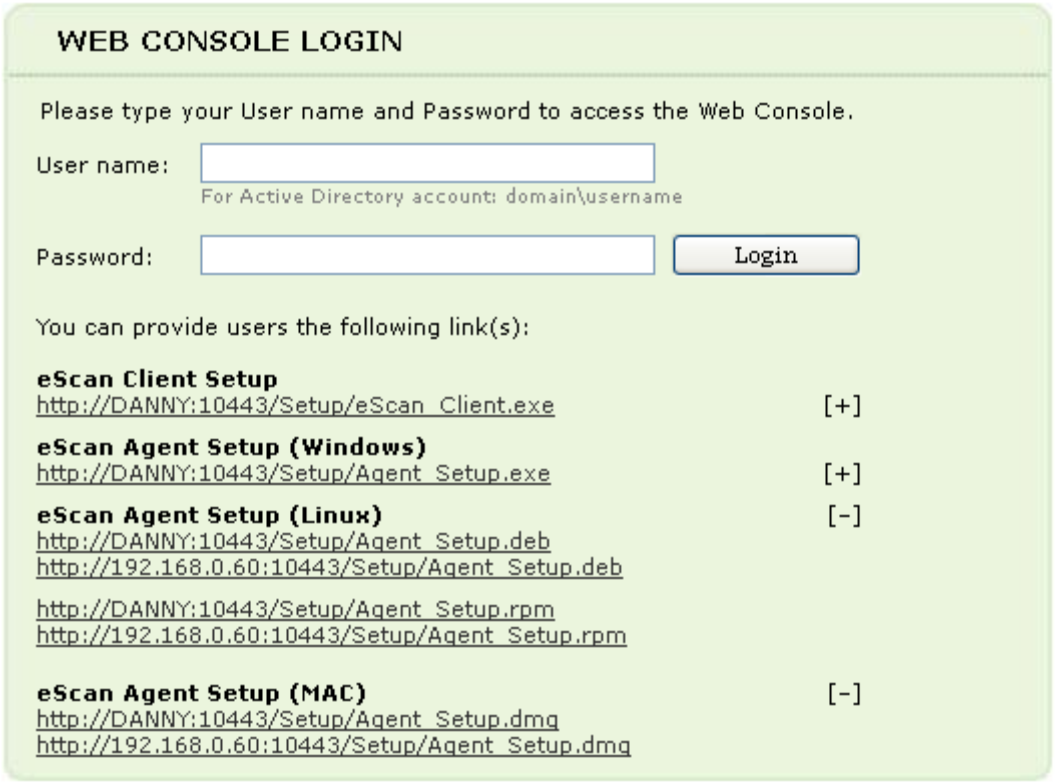


Figure - 8.30

Forward this link to the user of the Client computer on mail and guide him through the installation process. Also check - Show Client Setup Link

- **Installing eScan client using agent**

Use the following simple steps to Install eScan using agent --

- **Remotely Installing agent on Client Computer(s)**

1. Click **Managed Computers**.
2. Select the Group to which the Computer(s) belongs to.
3. Now select the Computer(s) from the listed Computers in the Group.
4. Select the Deploy / Upgrade Client option under Client Action List drop-down menu.
5. Select **Install Agent** option and click **Install**.
6. This will install **agent** on selected computers.

This option useful in case when there are glitches in the network connectivity between server and Client Computer, it will overcome those glitches thus speeds up the client installation on the selected computers.

- **Manually Installing agent on Client Computer(s) –** For manually installing agent on Endpoints. Please send the link that is displayed on the Login Page of eScan Management Console to the users of the Client Computer on mail. Refer **Figure – 8.31**

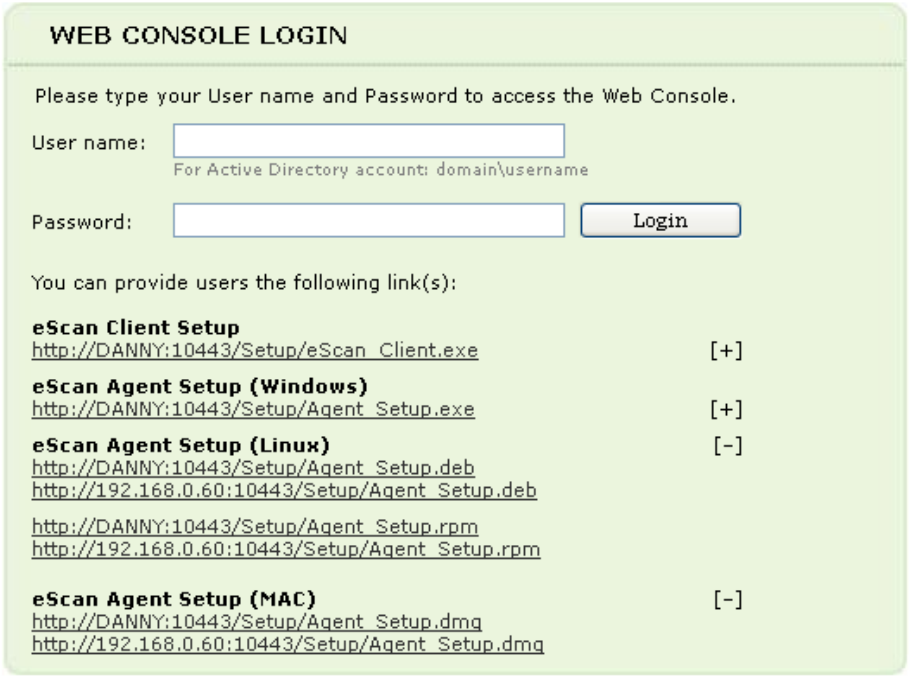


Figure – 8.31

Also check - Show Agent Setup Link

Installing other Softwares (3rd Party Software)

Using eScan Management Console, you can easily install other third party applications on any networked computer in Managed Computers. This can be done using the following simple steps –

1. Click **Managed Computers.**
2. Select the desired computer present under Managed Computers.
3. Now click **Deploy / Upgrade Client** under Client Action List drop-down Menu.
4. You will be forwarded to the **Client Installation** window. Select install Other Software option. Refer **Figure - 8.32**

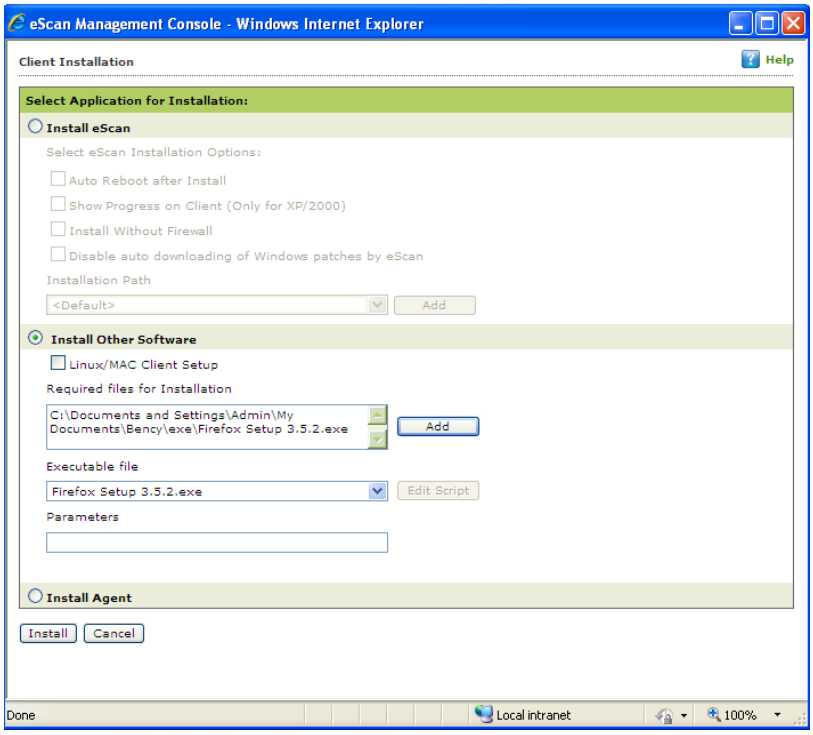


Figure - 8.32

5. Now Click **Add** and give the exact path of the EXE (on eScan Server) that you wish to install on the selected Computer. Click Add. Refer **Figure - 8.33**

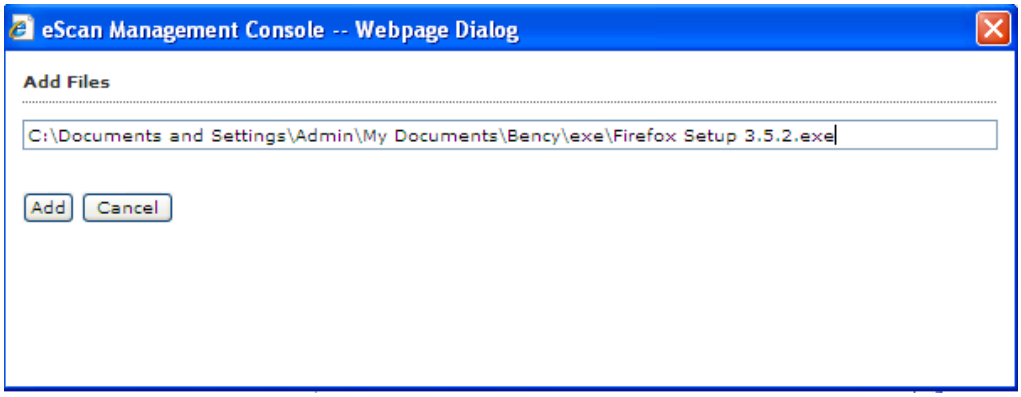


Figure - 8.33

6. The selected EXE will be added to the "Required files for Installation" list. Refer **Figure - 8.34.**

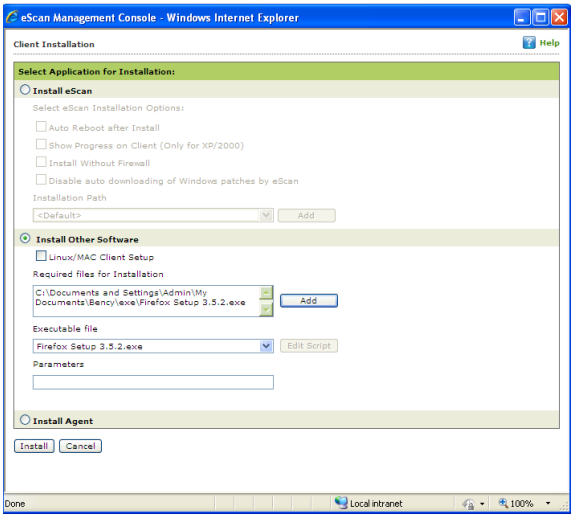


Figure - 8.34

7. The Executable Filename will be displayed in the respective dropdown menu present on the interface.
8. You can define the command line Parameters if required.
9. Click **Install** to initiate the Installation process.
10. You will be confirmed through a message on completion. Refer **Figure 8.35**

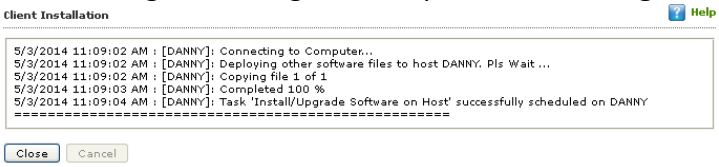


Figure 8.35

"Task 'Install/Upgrade Software on Host' successfully scheduled on… "

9. Managing Policies and Tasks for the Group

You can control all modules of eScan Client by defining Policy templates and creating tasks through eScan Management Console.

- **Defining Policies for the Group** - Using the policy template you can define rule sets for all modules of eScan client to be implemented on the Managed Computer Groups. eScan allows you to define security policies for Windows, Mac and Linux Computers connected to the network

- **Defining Policies for Computers with Windows operating system** – eScan allows you to define policies for the following Modules of eScan Client on Windows operating system

Modules	Description
File Anti-virus	This would scan all the existing files and folders for any infection. It will allow you to report / disinfect/ quarantine/delete objects. This will also save a copy of report file for future reference, and will display attention messages.
Anti-Spam	This will prevent you from receiving spam mails by checking the content of outgoing and incoming mails, quarantines advertisement mails.
Firewall	This will help you in putting up a restriction to incoming and outgoing traffic and hacking. You can define the firewall settings here. You can define the IP range, permitted applications, trusted MAC addresses and local IP addresses.
Privacy Control	This will allow you to schedule to an auto erase of your cache, ActiveX, cookies, plugins, and history. You can also secure delete your files and folders where the files will be deleted directly and no traces of that could be found.
Mail Anti-Virus	This will allow you to analyze all the incoming mails. This analyses the mails by breaking it into three sections the header, subject and the body. Once analyzed for any virus it will combine and send it to your mail box.
Web Protection	This will allow you to define the sites that you do not want to allow access to. You can define the site names you want to block, do a time based access restriction.
Endpoint Security	This will control the application from the point of end users by allowing/ restricting USB, block listing, white listing, and defining time restrictions.

- **Defining Policies for Computers with Mac or Linux operating system** – eScan allows you to create policy templates for the following modules of eScan Client on Mac or Linux operating system.

Modules	Description
File Anti-virus *This option is present under Protection in eScan for Mac.*	This would scan all the existing files and folders for any infection. It will allow you to report / disinfect/ quarantine/delete objects. This will also save a copy of report file for future reference, and will display attention messages. This option available only in Mac computers.
Endpoint Security *Block USB storage device - This option is present in settings under Protection Module in eScan for Mac*	This will allow you to block USB storage device from accessing your computer. This option is available only in Mac computers.
On demand Scanning *This feature is present in Options under Scan Module in eScan for Mac and Linux as well.*	This will allow you to define the categories that you want to be scanned. For example: you can scan only the mails or archives etc. as per your requirement.
Schedule Scan *This feature is present in Scheduler under Scan Module in eScan for Mac and as Scheduler Module n eScan for Linux.*	This will allow you to schedule the scan on the basis of time, what you want to scan and what action to be taken in case of a virus and what you want to be excluded while scanning. For example. You can schedule to scan the mails, sub directories and archives on a daily basis and also define the action that needs to be taken in case a virus is found; you can also exclude the scan by mask or files or folders.

Steps for Defining Policy templates for the group

1. Go to managed computers and click **Policy Templates**; this will open the Policy Templates window. Click **New Template** and select the rule –sets that you want to define.(Click here for more details)
2. Enter a template name and Click **Save**. You can see that the new template is listed.
   - **New Template:** This option will allow you to create a new template, define the policy details for this particular template. It will allow you to create any number of templates.
   - **Properties:** This option will allow you to view the properties of an existing template. You can also make changes to the existing policy details or even enable or disable a particular policy.
   - **Delete:** This option will allow you to delete the existing templates.
   - **Assign to Group(s):** This option will allow you to assign the policy template to group(s). All the policies that are defined in the particular template will be applied to the group(s).

- **Assign to Computer(s):** This option will allow you to assign the policy template to specific computer(s). Select the particular template and click on Assign to computer(s) and select the particular computer under managed groups.
- **Copy Template:** This option will allow you to duplicate the existing policy template, make changes and save as new policy template.

3. After creating the policy templates, select the particular managed group to which you want to deploy the policies.
4. Select the particular managed group and click policy templates, the list of existing policy templates will be displayed.
5. Select the template as per your requirement and click **Assign to group** or assign to computers as per your requirement.

Note:
You can apply the same policy templates to multiple managed computers and/ or multiple computers.

Rule –sets for Policy templates

Set the rule –sets for each escan module by selecting the module and then click on edit.

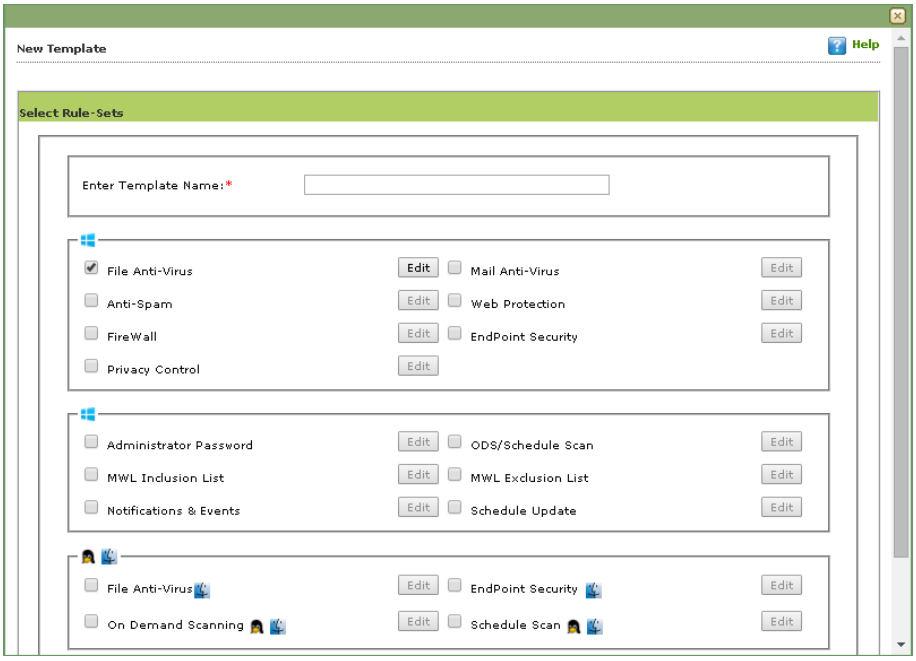


Figure – 9.3

- Select the Module in the group and Click **Edit** to define the policies for the Module. Refer **Figure – 9.4**

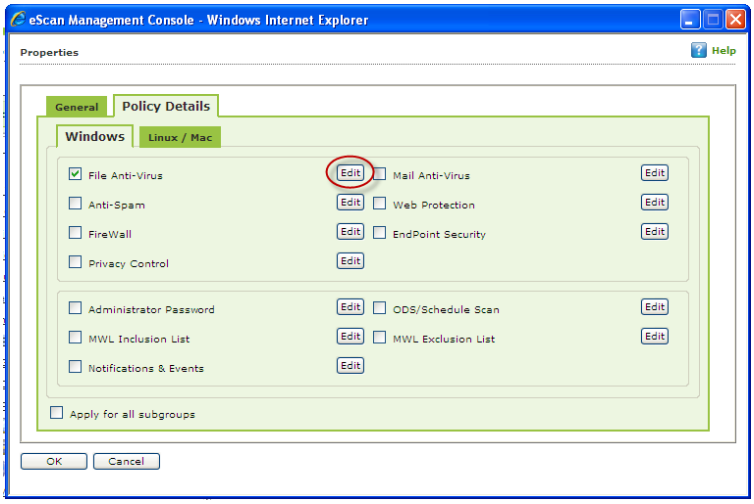
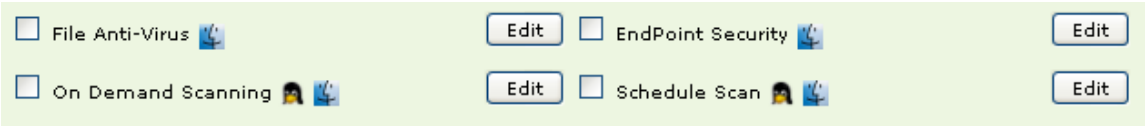


Figure – 9.4

Note: Using Linux / Mac tab, you can define settings for eScan on Linux and Mac machine. It allows you to define settings for the following modules –



Linux , Mac Icon denotes that you can **Edit** settings for the selected module in the respective operating system.

- You will be forwarded to a page where you can define actions and policies specifically for that module which you wish to be implemented on all Endpoints in that group. Refer **Figure 9.5**

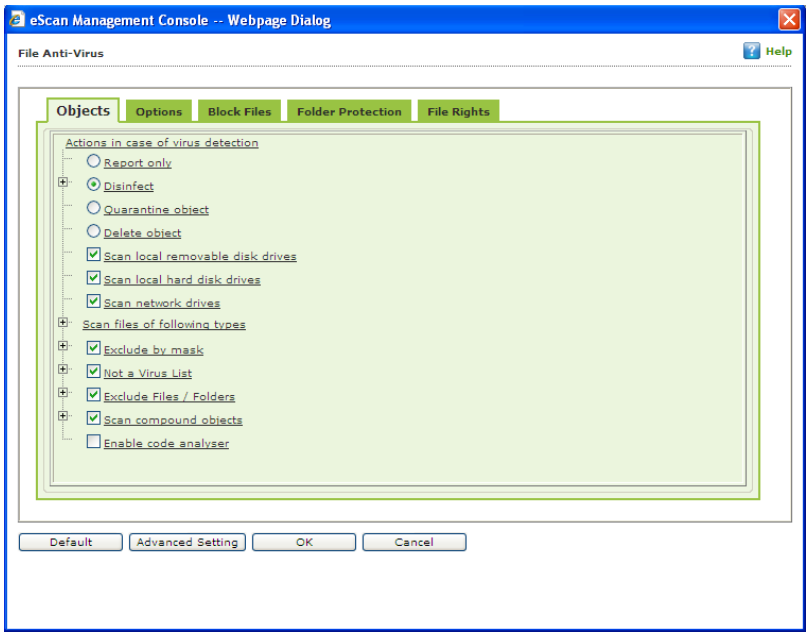


Figure 9.5

- **eScan Management Console** allows you to define policy template for every option present in all the Modules of eScan Client . All Policies are automatically implemented after Next update on the Endpoints.

- Using **Advanced Settings** option you can define Policies for more advanced options in eScan Client. These policies are defined in the .ini file or registry of the Endpoints. Refer **Figure – 9.6**

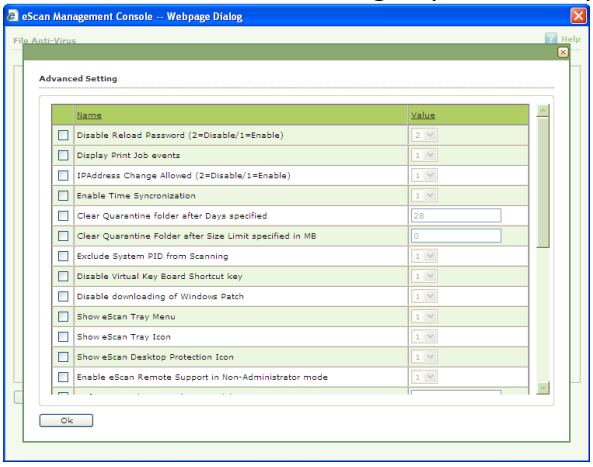


Figure – 9.6

Configurable eScan Policies for Windows Computers

1. **File Anti-Virus**

> Objects

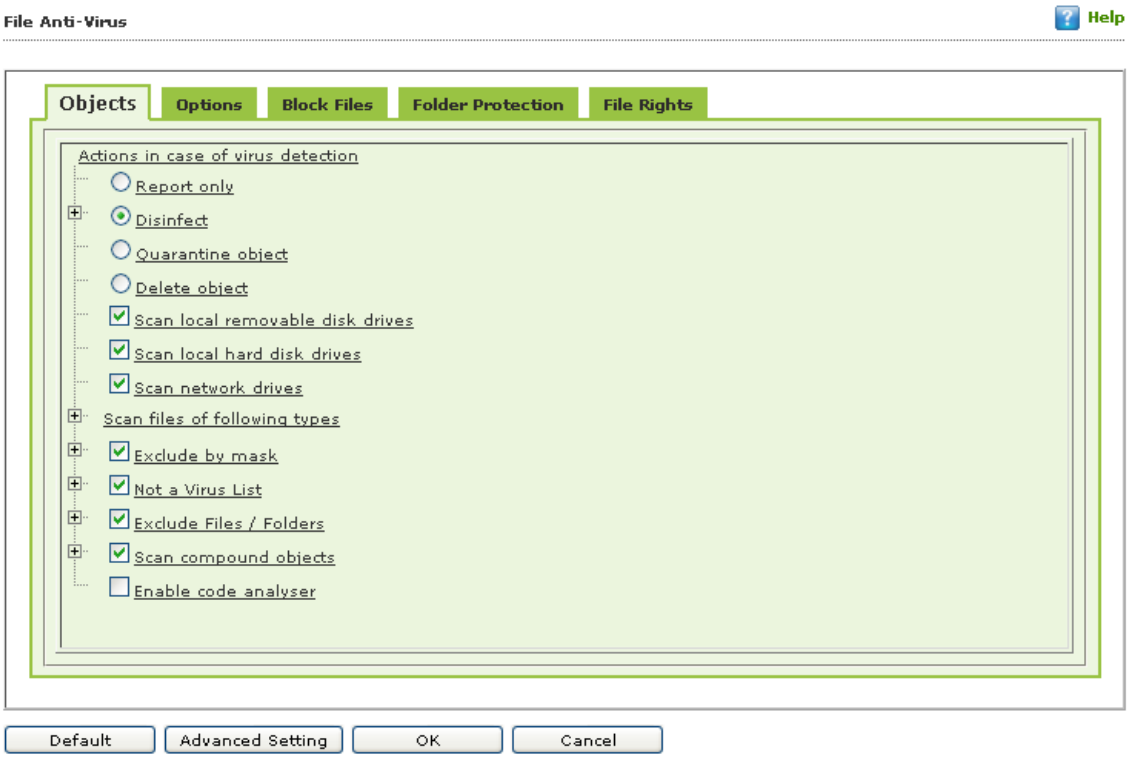


Figure – 9.7

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

- **Actions in case of virus detection:** This section lists the different actions that File Anti-Virus can perform when it detects a virus infection. These actions are Report only, Disinfect, Quarantine, and Delete object. Out of these, the **Disinfect** option is selected by default. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected folder**
  - **Scan local removable disk drives:** ***[Default]*** - Select this check box if you need to scan all the local removable drives attached to the computer.
  - **Scan local hard disk drives:** ***[Default]*** You should select this check box if you need to scan all the local hard drives installed to the computer.
  - **Scan network drives:** ***[Default]*** You should select this check box if you need to scan all the network drives, including mapped folders and drives, connected to the computer.
  - **Scan files of following types:** You should select this option if you need to scan all files, only infectable files, and files by extension (Scan by mask). eScan provides you

with a list of default files and file types that it scans by extension. You can add more items to this list or remove items as per your requirements by using the **Add / Delete** option.

- **Exclude by mask: [*Default]*** You should select this check box if you need the File Anti-Virus monitor to exclude all the objects in the Exclude by mask list during real time monitoring or scanning. You can add or delete a file or a particular file extension by double-clicking the **Add / Delete** option.
- **Not a virus list: *[Default]*** File Anti- Virus is capable of detecting riskware. Riskware refers to software that are originally not intended to be malicious but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote admin software, to the riskware list in the **Not a virus list** dialog box by double-clicking the **Add / Delete** option if you are certain that they are not malicious. The riskware list is empty by default.
- **Exclude Files/Folders: *[Default]*** You should select this check box if you want File Anti-Virus to exclude all the listed files, folders, and sub folders while it is monitoring or scanning folders. The Files/Folders added to this list will be excluded from the real –time scan as well as on-demand scan. You can add or delete files/folders from the list of by clicking the **Add / Delete** option.
- **Scan compound objects: *[Default]*** You should select this check box if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected.
- **Enable code Analyzer:** You should select this check box if you want eScan to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. When this check box is selected, File Anti-Virus not only scans and detects infected objects by using the definitions or updates, but it also checks for suspicious files stored on your computer.

> Options

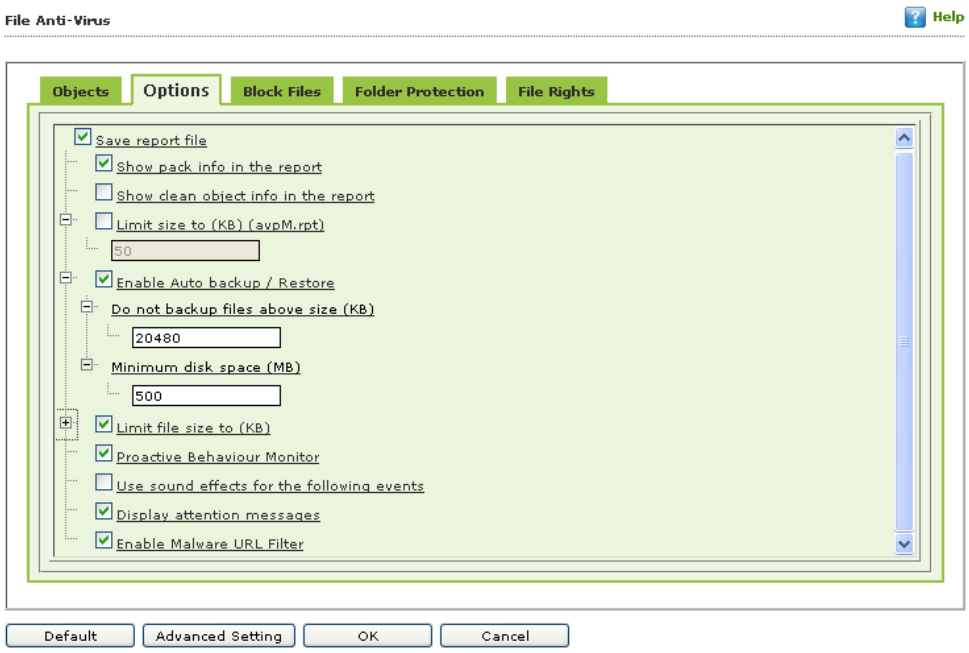


Figure – 9.8

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

You can configure the following settings:

- **Save report file:** ***[Default]*** You should select this check box if you need eScan to save the reports generated by the File Anti-Virus module. The report file logs information about the scanned files and the action taken by File Anti-Virus when an infected file was found during the scan.

- **Show pack info in the report:** ***[Default]*** You should select this check box if you need File Anti-Virus to add information regarding scanned compressed files, such as .ZIP and .RAR files to the Monvir.log file.
- **Show clean object info in the report:** You should select this check box if you need File Anti-Virus to add information regarding uninfected files found during a scan operation to the Monvir.log file. You can select this option to find out which files are not infected.
- **Limit size to (Kb) (avpM.rpt):** Select this check box if you need File Anti-Virus to limit the size of the Monvir.log file and avpM.rpt file. You can double-click the size box and specify the size of the log file.

- **Enable Auto backup / Restore:** ***[Default]*** This check box helps you back up the critical files of the Windows® operating system installed on your computer and then **automatically** restore the clean files when eScan finds an infection in any of the system files that cannot be disinfected. You can do the following settings:

- **Do not backup files above size (KB):** ***[Default]*** This option helps you prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified.
- **Minimum disk space (MB**): *[Default]* eScan Auto-backup will first check for the minimum available space limit defined for a hard disk drive. If the minimum define space is available then only the Auto-backup will function, if not it will stop without notifying. You can allot the Minimum disk space to be checked from this option.
- **Limit file size to (KB):** ***[Default]*** This check box enables you to set a limit size for the objects or files to be scanned. The default value is set to **20480 Kb**.
- **Enable Proactive Scan:** When you select this check box, File Anti-Virus monitors your computer for suspicious applications and prompts you to block such applications when they try to execute.
- **Use sound effects for the following events:** This check box helps you configure eScan to play a sound file and show you the details regarding the infection within a message box when any malicious software is detected by File Anti- Virus. However, you need to ensure that the computer's speakers are switched on.
- **Display attention messages:** ***[Default]*** When this option is selected, eScan displays an alert, which displays the path and name of the infected object and the action taken by the File Anti-Virus module.

> Block Files

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

You can configure the following settings:

- **Deny access of executables on USB Drives:** You should select this check box if you need to prevent executables stored on USB drives from being accessed.
- **Deny access of AUTORUN.INF on USB and Fixed Drives:** ***[Default]*** You should select this check box if you need to prevent executables from USB and fixed drives from being accessed.
- **Deny access of executable from Network:** You should select this check box if you need to prevent executables on the client computer from being accessed from the network.
- **User defined whitelist:** This option is effective when the **Deny access of executable from Network** tab is enabled. You can use this option to enter the folders that need to be whitelisted so that executables can be accessed in the network from the folders mentioned under this list. You need to click the **Add** button.

Add

Enter the complete path of the folder to be whitelisted on the client systems. You can either whitelist the parent folder only or select the **Include subfolder** option for whitelisting the child folders as well.

- **Deny Access of following files:** ***[Default]*** You should select this check box if you need to prevent the files in the list from running on the Endpoints.
- **Quarantine Access-denied files:** You should select this check box if you need to quarantine files that have been Access-denied.

You can prevent specific files from running on the eScan client computer by adding them to the Block Files list. By default, this list contains the value %sysdir%*.EXE@. You need to click the **Add** Button.

Add

Enter the full name of the file to be blocked from execution on the client systems.

> Folder Protection

Figure – 9.9

This tab helps you protect specific folders from being modified or deleted by adding them to the Folder Protection list. It allows you to configure the following setting:

- **Protect files in following folders from modification and deletion:** ***[Default]*** This option is selected by default. You should select this check box if you need the File Anti-Virus module to protect files in specific folders from being modified or deleted on the client systems. You need to click the **Add** button.

Add

Enter the complete path of the folder to be protected on the client systems. You can either protect the parent folder only or select the **Include subfolder** option for protecting the child folders as well.

Default

Note: - Click the Default button, if you want to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

> File Rights

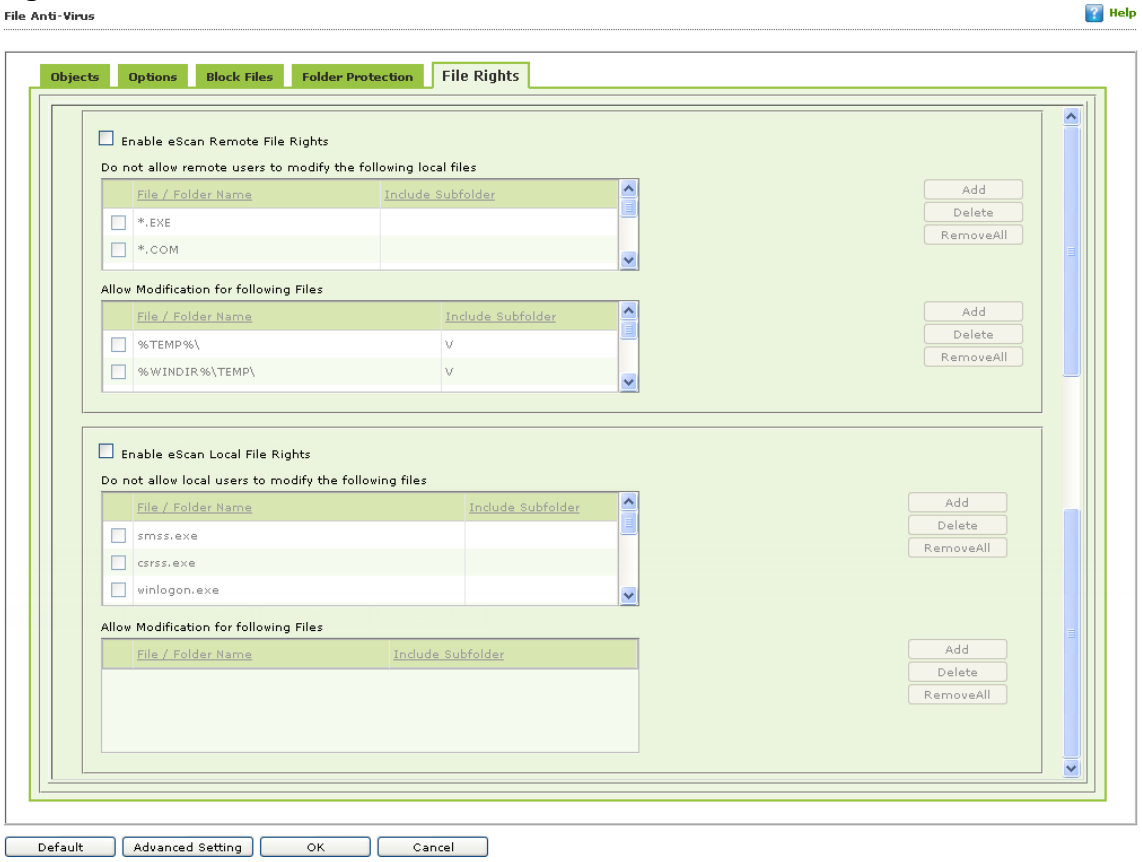


Figure – 9.10

Use options present under this tab to restrict or allow remote or local users from modifying Folders, subfolders, Files or Files with certain extensions. eScan allows you to Add/ remove Folders, subfolders, Files or Files with certain extensions to restrict or allow the user to modify them.

Advanced Settings

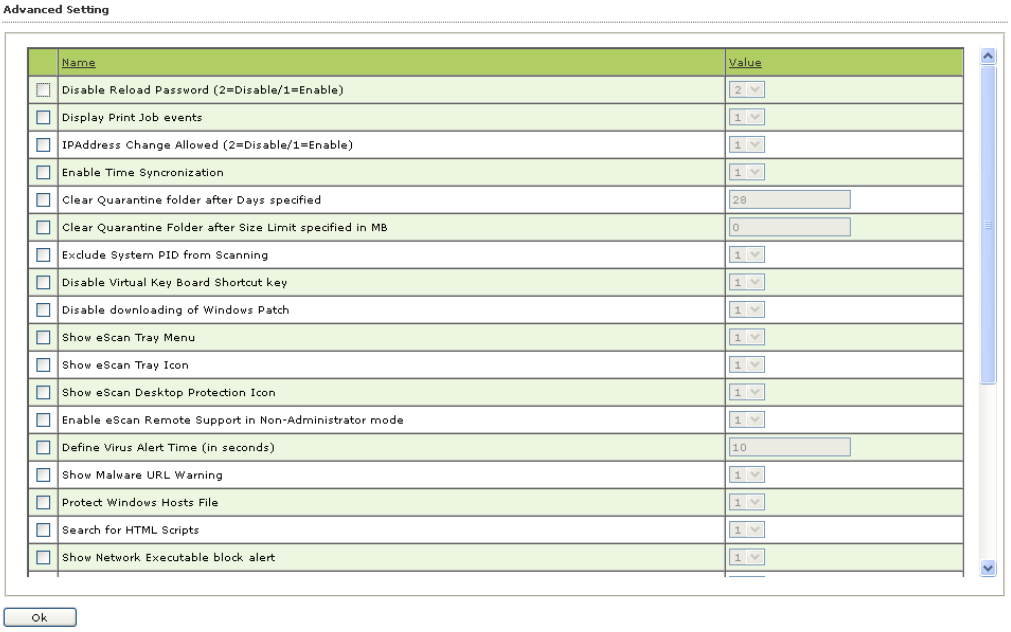


Figure – 9.11

It allows you to configure advanced settings for eScan.

Sr. No.	Name	Description
1.	Disable Reload Password (2=Disable/1=Enable)	It allows you to enable or disable Password for reloading eScan. If enabled, when the user tries to reload eScan, he will be asked to enter Password. This is the administrator password for eScan Protection Center.
2.	Display Print Job events (1 = Enable / 0= Disable)	It allows you to capture events for the Print Jobs from Managed Endpoints.
3.	IP Address Change Allowed (2=Disable/1=Enable)	It allows you to Enable / Disable IP Address Change by the user on his computer.
4.	Enable Time Synchronization (1 = Enable / 0= Disable)	It allows you to Enable / Disable time synchronization with internet if internet connections are available.
5.	Clear Quarantine folder after Days specified	It allows you to specify number of days after which the Quarantine folder should

		be cleared on Managed Endpoints.
6.	Clear Quarantine Folder after Size Limit specified in MB	It allows you to specify size Limit for the Quarantine Folder. If the defined size limit is exceeded the Quarantine Folder will be cleared on Managed Endpoints.
7.	Exclude System PID from Scanning(1 = Enable / 0= Disable)	It allows you to exclude system process ID (Microsoft assigned System PIDs) from scanning on Managed Endpoints.
8.	Disable Virtual Key Board Shortcut key (1 = Enable / 0= Disable)	It allows you to Disable shortcut for using Virtual Keyboard on Managed Endpoints.
9.	Disable downloading of Windows Patch(1 = Enable / 0= Disable)	It allows you to Disable downloading of Windows Patches on Managed Endpoints.
10.	Show eScan Tray Menu (1=Show / 0=Hide)	It allows you to Hide or Show eScan Tray menu on Managed Computers.
11.	Show eScan Tray Icon(1=Show / 0=Hide)	It allows you to Hide or Show eScan Tray Icon on Managed Computers.
12.	Show eScan Desktop Protection Icon (1=Show / 0=Hide)	It allows you to Hide or Show eScan Protection Icon on Managed Computers.
13.	Enable eScan Remote Support in Non-Administrator mode(1 = Enable / 0= Disable)	It allows you to Enable / disable eScan Remote Support in Non -Administrator Mode. eScan will not prompt for entering Administrator Password to start eScan Remote Support from Managed Endpoints.
14.	Define Virus Alert Time (in seconds)	It allows you define time period in seconds to display Virus Alert on Managed Endpoints.

15.	Show Malware URL Warning(1=Show / 0=Hide)	It allows you to show or hide Malware URL warning messages on Managed Endpoints.
16.	Protect Windows Hosts File (1 = Allow / 0= Disallow)	Use this option to Allow/ Disallow modifications to Windows Host Files.
17.	Search for HTML Scripts(1 = Allow / 0= Disallow)	Use this option to Allow/ Disallow search for html script (infection) in files. This option will have impact on system performance.
18.	Show Network Executable block alert (1=Show / 0=Hide)	This option allows you to show/ hide Network executable block alerts on Managed Endpoints.
19.	Show USB Executable Block Alert (1=Show / 0=Hide)	This option allows you to show/ hide USB executable block alerts on Managed Endpoints.
20.	Show eScan Tray Icon on Terminal Client (1=Show / 0=Hide)	This option allows you to show/ hide eScan Tray Icon on Terminal Clients on Managed Endpoints.
21.	Enable eScan Self Protection(1 = Enable / 0= Disable)	It allows you to Enable / disable eScan Self Protection on Managed Endpoints, if this feature is Enabled, no changes or modifications can be made in any eScan File.
22.	Enable eScan Registry Protection (1 = Enable / 0= Disable)	It allows you to Enable / disable eScan Registry Protection. User cannot make changes in protected registry entries if it is enabled on Managed Endpoints
23.	Enable backup of DLL files (1 = Enable / 0= Disable)	It allows you to Enable / disable backup of DLL files on Managed Endpoints
24.	Integrate Server Service dependency with Real time monitor. (1 = Enable / 0= Disable)	It allows you to Integrate Server Service dependency with Real time monitor.

25.	Send Installed Software Events(1 = Enable / 0= Disable)	It allows you to receive Installed Software Events from Managed Endpoints.
26.	Enable Winsock Protection (Require Restart) (1 = Enable / 0= Disable)	It allows you to Enable / disable protection at the Winsock Layer
27.	Enable Cloud (1 = Enable / 0= Disable)	It allows you to Enable / disable eScan Cloud Security Protection on Managed Endpoints.
28.	Enable Cloud Scanning (1 = Enable / 0= Disable)	It allows you to Enable / disable Cloud Scanning on Managed Endpoints.
29.	Remove LNK (Real Time) (1 = Enable / 0= Disable)	It allows you to Enable / disable Removal of LNK on Real time.

2. Mail Anti-Virus

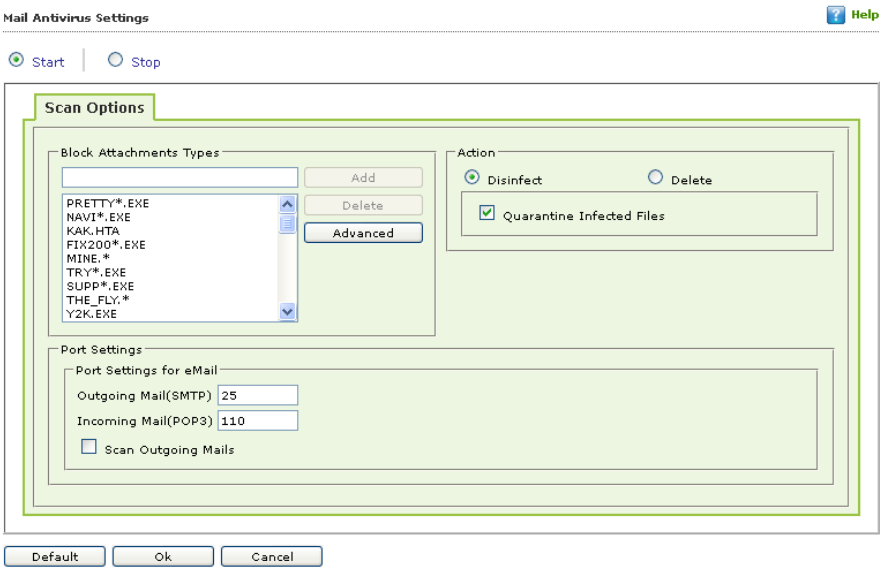


Figure – 9.12

Mail Anti-Virus is a part of the Protection feature of eScan. This module scans all incoming and outgoing e-mails for viruses, spyware, adware, and other malicious objects. It helps you send virus warnings to client computers on the Mail Anti- Virus activities. By default, Mail Anti -Virus scans only the incoming e mails and attachments, but you can configure it to scan outgoing e-mails and attachments as well. Moreover, it helps you notify the sender or system administrator whenever

you receive an infected e-mail or attachment. This page provides you with options for configuring the module.

Scan Options

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

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

- **Action:** This section helps you configure the actions to be performed on infected e mails. These operations are as follows:

  1. **Disinfect:** ***[Default]*** You should select this option if you need Mail Anti-Virus to disinfect infected e mails or attachments.
  2. **Delete:** You should select this option if you need Mail Anti-Virus to delete infected e mails or attachments.
  3. **Quarantine Infected Files:** ***[Default]*** You should select this check box if you need Mail Anti-Virus to quarantine infected e mails or attachments. The default path for storing quarantined e mails or attachments is C:\Program Files\eScan\QUARANT. However, you can specify a different path for storing quarantined files, if required.

- **Port Settings for email:** You can also specify the ports for incoming and outgoing e mails so that eScan can scan the e mails sent or received through those ports.

  1. **Outgoing Mail (SMTP):** ***[Default: 25]*** you need to specify a port number for SMTP.
  2. **Incoming Mail (POP3):** ***[Default: 110]*** You need to specify a port number for POP3.
  3. **Scan Outgoing Mails:** You should select this check box if you need to Mail Anti-Virus to scan outgoing e-mails as well.

- **Advanced:** You can click this button to open the **Advanced Scan Options** dialog box. This dialog box helps you configure the following advanced scanning options:

  - **Delete all Attachment in email if disinfection is not possible:** You should select this check box if you need to delete all the e mail attachments that cannot be cleaned.

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

3. Anti – Spam

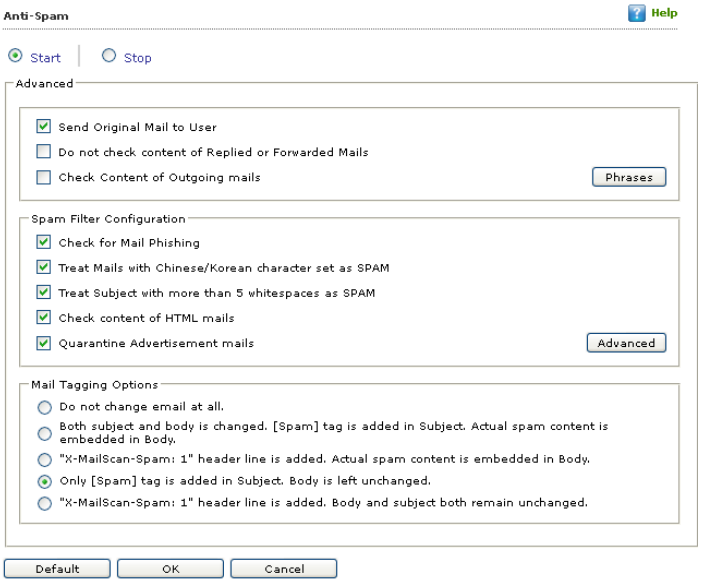


Figure – 9.13

Anti-Spam is a part of eScan\'s Protection feature. This module filters all your junk and spam e mails by using the NILP technology and sends content warnings to specified recipients. This page provides you with options for configuring the module. You can configure the following settings.

1. **Advanced**

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

   - **Send Original Mail to User:** ***[Default]*** This check box is selected by default. eScan creates Spam folder within the e mail client. When an e mail is tagged as SPAM, it is moved to this folder. You should select this check box, if you need to send original e mail that is tagged as spam to the recipient as well.
   - **Do not check content of Replied or Forwarded Mails:** You can select this check box, if you need to ensure that eScan does not check the contents of e mails that you have either replied or forwarded to other recipients.
   - **Check Content of Outgoing mails:** You can select this check box, if you need Anti-Spam to check outgoing e mails for restricted content.
   - **Phrases:** You can click the **Phrases** button to open the **Phrases** dialog box. This dialog box helps you configure additional e mail-related options. In addition, it allows you to specify a list of words that the user can either allow or block. This list is called the **user specified whitelist**. You can specify certain words or phrases so that mails containing those words or phrases in the subject, header, or body are recognized as spam and are quarantined or deleted. All the fields are available only when you select the **Enable E-mail Content Scanning** check box. The dialog box uses the following color codes to categorize e-mails.
   - **User specified whitelist of words/phrases:** (Color Code: **GREEN**) You should click this option to list the words or phrases that are present in the whitelist. A phrase that is added to the whitelist cannot be edited, enabled, or disabled.
   - **User specified List of Blocked words/phrases:** (Color Code: **RED**) You should click this option to list the words or phrases that are defined in block list.
   - **User specified words/phrases disabled:** (Color Code: **GRAY**) You should click this option to list the words or phrases that are defined excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

2. **Spam Filter Configuration:** This section provides you with options for configuring the spam filter. All options in this section are selected by default.

   - **Check for Mail Phishing:** ***[Default]*** You should select this check box, if you need Anti-Spam to check for fraudulent e-mails and quarantine them.
   - **Treat Mails with Chinese /Korean character set as SPAM:** ***[Default]*** When this check box is selected, eScan scans e mails with Chinese or Korean characters. This check is based on the research data conducted by MicroWorld's various spam e mail samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their e mails.

- **Treat Subject with more than 5 whitespaces as SPAM:** ***[Default]*** In its research, MicroWorld found that spam e-mails usually contain more than five consecutive white spaces. When this check box is selected, Anti -Spam checks the spacing between characters or words in the subject line of e mails and treats e mails with more than five whitespaces in their subject lines as spam e mails.
- **Check content of HTML mails:** ***[Default]*** You should select this check box when you need Anti-Spam to scan e-mails in HTML format along with textual content.
- **Quarantine Advertisement mails:** ***[Default]*** You should select this check box when you need Anti-Spam to check for advertisement types of e-mails and quarantine them.
- **Advanced:** Click this button to open the **Advanced Spam Filtering Options** dialog box. This dialog box helps you configure the following advanced options for controlling spam.
- **Enable Non-Intrusive Learning Pattern (NILP) check: [Default]** NILP is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each e mail and prevents spam and phishing e mails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each e mail and categorize it as spam or ham based on the behavioral pattern of the user. You should select this check box if you need to enable NILP check.
- **Enable email Header check:** ***[Default]*** You should select this check box if you need to check the validity of certain generic fields like From, To, and CC in an e mail and marks it as spam if any of the headers are invalid.
- **Enable X Spam Rules check:** ***[Default]*** X Spam Rules are rules that describe certain characteristics of an e mail. It checks whether the words in the content of e mails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The X Spam Rules Check technology matches X Spam Rules with the mail header, body, and attachments of each e mail to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify e mails and takes action on them.
- **Enable Sender Policy Framework (SPF) check:** SPF is a world standard framework that is adopted by eScan to prevent hackers from forging sender addresses. It acts a powerful mechanism for controlling phishing mails. You should select this check box if you need Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.
- **Enable Spam URI Real-time Blacklist (SURBL) check:** You should select this option if you need Anti-Spam to check the URLs in the message body of an e-mail. If the URL is listed in the SURBL site, the e-mail will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **Enable Real-time Black-hole List (RBL) check:** You should select this option if you need Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the e-mail will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **RBL Servers:** RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The

RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.

- **Auto Spam Whitelist:** Unlike normal RBLs, SURBL scans e mails for names or URLs of spam Web sites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid e-mail addresses that can bypass the above Spam filtering options. It thus allows e-mails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

3. **Mail Tagging Options:** Anti -Spam also includes some mail tagging options, which are described as follows:

- **Do not change email at all:** You should select this option when you need to prevent Anti -Spam from adding the *[Spam]* tag to e mails that have been identified as spam.
- **Both subject and body is changed: *[Spam]* tag is added in Subject: Actual spam content is embedded in Body:** This option helps you identify spam e mails. When you select this option, Anti -Spam adds a *[Spam]* tag in the subject line and the body of the e mail that has been identified as spam.
- **"X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body:** This option helps you add a [Spam] tag in the body of the e mail that has been identified as spam. In addition, it adds a line in the header line of the e mail.
- **Only *[Spam]* tag is added in Subject: Body is left unchanged: *[Default]*** This option helps you add the *[Spam]* tag only in the subject of the e mail, which has been identified as spam.
- **"X MailScan Spam: 1" header line is added: Body and subject both remain unchanged:** This option helps you add a header line to the e mail. However, it does not add any tag to the subject line or body of the e mail.

3. Web Protection

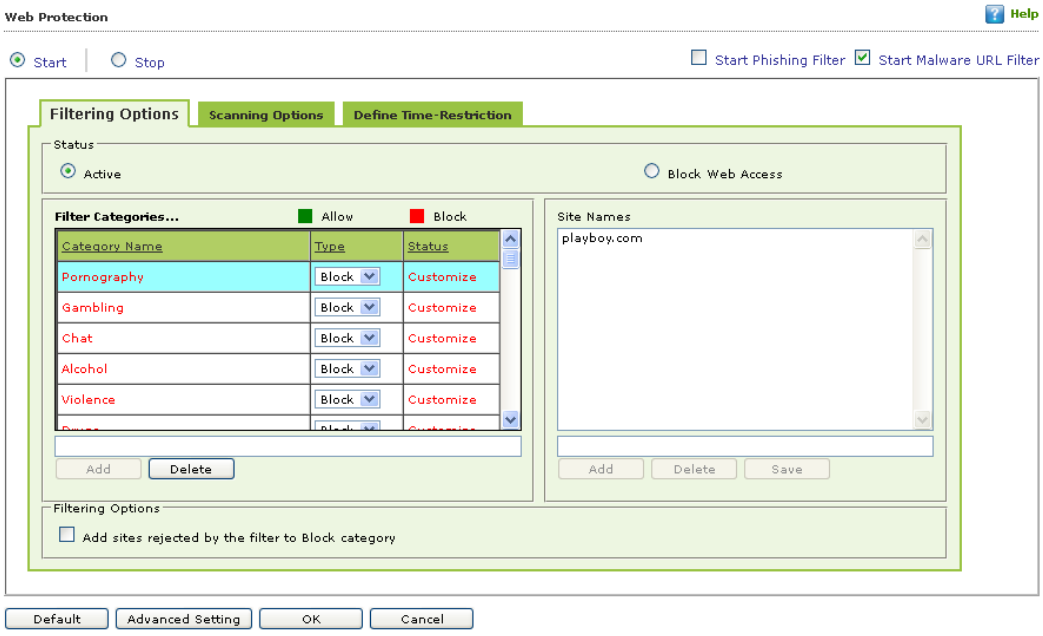


Figure – 9.14

Web Protection is a part of eScan's Protection feature. This module uses highly advanced algorithms based the occurrence of specific words or phrases in the contents of the Web site 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 harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related Web sites during work hours. You can configure the following settings.

A. Filtering Options: This tab has predefined categories that help you control access to the Internet.

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

The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings_block_category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

- **Category: [Category name]:** This section shows the **Words / Phrases** list, which lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the Web sites belonging to the selected category. You can also add or delete filter categories depending on your requirement.
- **Filter Options:** This section includes the **Add sites rejected by the filter to Block category** check box. You should select this check box if you need eScan to add Web sites that are denied access to the Block category database automatically.

B. Scanning Options: This tab helps you enable content matching and content rating for Web sites. It also helps you block images, ActiveX controls, media components, and applications from appearing within the browser.

- **ActiveX Blocking:** An ActiveX control is component program that can be automatically downloaded and executed by a Web browser. It is similar to a Java applet. ActiveX controls may include malicious code and therefore may pose as a security hazard.

- **Java Applets:** Java Applets are programs that are written in the Java programming language. These applets can be embedded in an HTML page and can be viewed from a Java enabled Web browser. Applets enhance the interactivity in Web pages and provide users with an enhanced Web experience. However, some applets contain malicious code that may either disrupt the processes running on your computer or steal sensitive information. You can select the Java Applets check box to block applets from being downloaded to your computer.
- **Scripts (Java & VB):** Scripts are usually written in scripting languages such as JavaScript and VBScript. A script is a list of commands that can execute without user input. With the help of scripts, you can automate certain tasks within an application to work in a particular computing scenario. Hackers often use malicious script to steal information about the victims. When you select the **Scripts (Java & VB)** check box, eScan blocks script from being downloaded to your computer from the Internet.
- **Check for Virus: [Default]** This check box is selected by default. You should select this check box if you need eScan to scan and block all Web sites that contain malicious code.

- **Actions:** This section helps you select the actions that eScan should perform when it detects a security violation.

- **Log Violations: [Default]** This check box is selected by default. You should select this check box if you need Web Protection to log all security violations for your future reference.
- **Shutdown Program in 30 Secs:** You should select this check box if you need Web Protection to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.

- **Port Setting:** This section helps you specify the port numbers that eScan should monitor for suspicious traffic.

- **Internet Access (HTTP Port):** Web browsers commonly use the port numbers 80, 8080, 3128, 6588, 4480, and 88 for accessing the Internet. You can add port numbers to the **Internet Access (HTTP Port)** box to monitor the traffic on those ports.

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

C. **Define Time Restriction:** This section helps you define policies to restrict access to the Internet.

- **Enable Time Restrictions for Web Access:** You should select this check box if you want to set restrictions on when a user can access the Internet. By default, all the fields appear disabled. The fields are available only when you select this check box.

The time restriction feature is a grid-based module. The grid is divided into columns based on the days of the week vertically and the time interval horizontally.

- **Active:** Click this button and select the appropriate grid if you want to keep web access active on certain days for a specific interval.
- **Inactive:** Select this option if you want to keep web access inactive on certain days for a specific interval.
- **Block Web Access:** Select this option if you want to block web access on certain days for a specific interval.

  For Example: As an Admin you can define the following settings

  - Allow users to access the web during lunch hours i.e. 1-2: 30 (you can choose any preferred time of your choice)
  - Block the web access for the rest of the time or for 9 am to 11 am in the morning and 5 pm to 7 pm in the evening. (You can choose any preferred time of your choice).
  - Inactivate the web protection module after midnight till 5 am (you can choose any preferred time of your choice).

4. Firewall

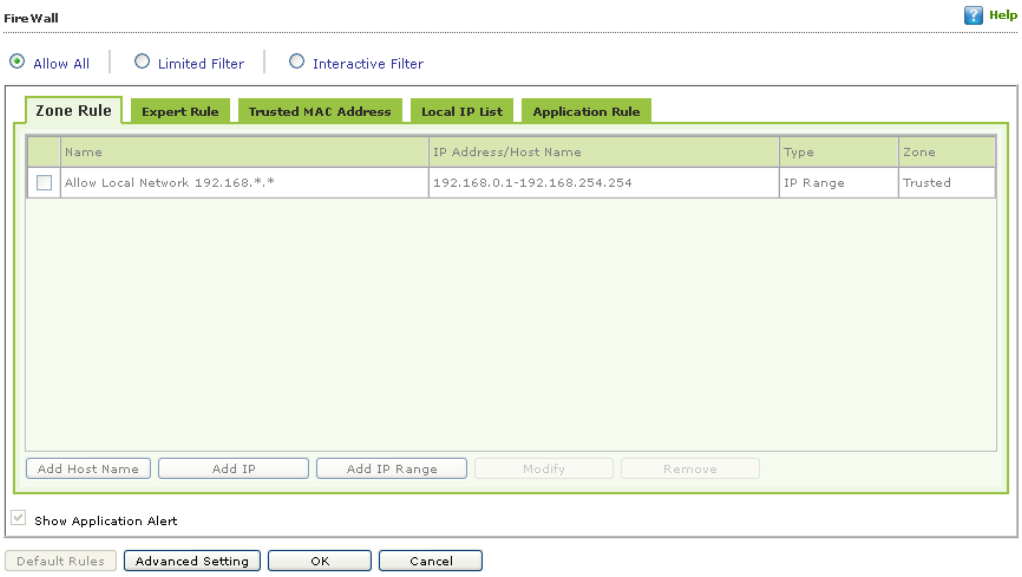


Figure – 9.15

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

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

By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and **Interactive Filter** to turn off and block all. The eScan Firewall also allows you to specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include Zone Rules, Expert Rules, Trusted Media

Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. You can configure the following settings to be deployed to the eScan client systems.

Allow All – Clicking on this button will disable the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored / filtered.
Limited Filter – Clicking on this button will enable eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed / blocked as per the conditions or rules defined in the Firewall.
Interactive **-** Clicking on this button will enable eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed / blocked as per the conditions or rules defined in the Firewall.

There are **four tabs** – **Zone Rule**, **Expert Rule**, **Trusted MAC Address**, and **Local IP List**, which are as follows:

A. **Zone Rule -** This is a set of network access rules to make the decision of allowing / blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked.

Buttons (to configure a Zone Rule)

1. **Add Host Name –** This option enables you to add a "host" in the Zone Rule. When clicked on this button, enter the HOST name of the system, select the Zone (Trusted / Blocked) and enter a name for the Zone Rule. Click on OK button to create the Zone Rule.
2. **Add IP –** This option enables you to add an IP address of a system to be added in the Zone rule. When clicked on this button, enter the IP address of the system, select the Zone (Trusted / Blocked) and enter a name for the Zone Rule. Click on OK button to create the Zone Rule.
3. **Add IP Range –** This option enables you to add an IP range to be added in the Zone rule. When clicked on this button, add the IP Range (i.e. a range of IP that the Zone rule should be applied), select the Zone (Trusted / Blocked) and enter a name for the Zone Rule. Click on OK button to create the Zone Rule.
4. **Modify –** To modify / change any listed Zone Rule(s), select the zone rule to be modified and click on the Modify button.
5. **Remove -** To delete any listed Zone Rule(s), select the zone rule to be deleted and click on the remove button.

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

- **Source IP Address / Host Name**
- **Source Port Number**
- **Destination IP Address / Host Name**
- **Destination Port Number**

Buttons (to configure an Expert Rule)

Add – Click on the Add button to create a new Expert Rule. In the Add Firewall Rule Window:

i. **General tab** – In this section, specify the Rule settings

- **Rule Name –** Provide a name to the Rule,
- **Rule Action –** Action to be taken, whether to Permit Packet or Deny Packet,
- **Protocol –** Select the network protocol (eg.TCP, UDP, ARP etc…) on which the Rule will be applied
- **Apply rule on Interface –** Select the Network Interface on which the Rule will be applied.

ii. **Source tab** – In this section, specify / select the location from where the outgoing network traffic originates.

- **Source IP Address –**
  - **My Computer –** The rule will be applied for the outgoing traffic originating from your computer.
  - **Host Name –** The rule will be applied for the outgoing traffic originating from the computer as per the host name specified.
  - **Single IP Address –** The rule will be applied for the outgoing traffic originating from the computer as per the IP address specified.
  - **Whole IP Range –** To enable the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the outgoing traffic from the computer(s) which is within the defined IP range.
  - **Any IP Address –** When this option is selected, the rule will be applied for the traffic originating from ANY IP Addresses.

- **Source Port –**
  - **Any –** When this option is selected, the rule will be applied for the outgoing traffic originating from ANY port(s).
  - **Single Port –** When this option is selected, the rule will be applied for the outgoing traffic originating from the specified / defined port.

- **Port Range –** To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.
- **Port List –** A list of port can be specified / added. The rule will be applied for the outgoing traffic originating from the ports as per specified in the list.

NOTE: The rule will be applied when the selected Source IP Address and Source Port matches together.

Destination tab – In this section, specify / select the location of the computer where the incoming network traffic is destined.

- **Destination IP Address –**
  - **My Computer –** The rule will be applied for the incoming traffic to your computer.
  - **Host Name –** The rule will be applied for the incoming traffic to the computer as per the host name specified.
  - **Single IP Address –** The rule will be applied for the incoming traffic to the computer as per the IP address specified.
  - **Whole IP Range –** To apply the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the incoming traffic to the computer(s) which is within the defined IP range.
  - **Any IP Address –** When this option is selected, the rule will be applied for the incoming traffic to ANY IP Addresses.

- **Destination Port –**
  - **Any –** When this option is selected, the rule will be applied for the incoming traffic to ANY port.
  - **Single Port –** When this option is selected, the rule will be applied for the incoming traffic to the specified / defined port.
  - **Port Range –** To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the incoming traffic to the port which is within the defined range of ports.
  - **Port List –** A list of port can be specified / added. The rule will be applied for incoming traffic originating from the ports as per specified in the list.
    NOTE: The rule will be applied when the selected Destination IP Address and Destination Port matches together.

- **Advanced tab** – This tab contains advance setting for Expert Rule.
  - **Enable Advanced ICMP Processing -** This is activated when the ICMP protocol is selected in the General tab.

- **The packet must be from/to a trusted MAC address –** When this option is selected, the rule will only be applied on the MAC address defined / listed in the Trusted MAC Address tab.
- **Log information when this rule applies –** This will enable to log information of the Rule when it is implied.

1. **Modify** – This button will enable to change or modify any Expert Rule.
2. **Remove** – This button will delete a rule from the Expert Rule.
3. **Shift Up and Shift Down** – The UP and DOWN arrow button will enable to move the rules up or down as required and will take precedence over the rule listed below it.
4. **Enable Rule / Disable Rule** – These buttons allow you to enable or disable a particular selected rule from the list.

C. **Trusted MAC Address –** This section contains the information of the MAC address of the system. A MAC address (Media Access Control address) is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the Advance Tab of the Expert Rule).

Buttons (to configure the Trusted MAC Address)

1. **Add –** To add a MAC address click on this button. Enter the MAC address to be added in the list for eg. 00-13-8F-27-00-47
2. **Edit –** To modify / change the MAC Address click on this button.
3. **Remove –** To delete the MAC Address click on this button.
4. **Clear All –** To delete all the listed MAC Address click on this button.

D. **Local IP List –** This section contains a list of Local IP addresses.
Buttons (to configure the Local IP List)

1. **Add –** To add a Local IP address click on this button.
2. **Remove –** To remove a Local IP address click on this button.
3. **Clear All –** To clear all the Local IP address in the list click on this button.
4. **Default List –** To load the default list of IP address click on this button.

Other Buttons

- **Clear Alert Cache** - This option will clear / delete all the information stored by the Firewall cache
- **Show Application Alert** – Selecting this option will display an eScan FireWall Alert displaying the blocking of any application as defined in the Application Rule.
- **Default Rules** - This button will load / reset the rules to the Default settings present during the installation of eScan. This will remove all the settings defined by user.

5. Endpoint Security

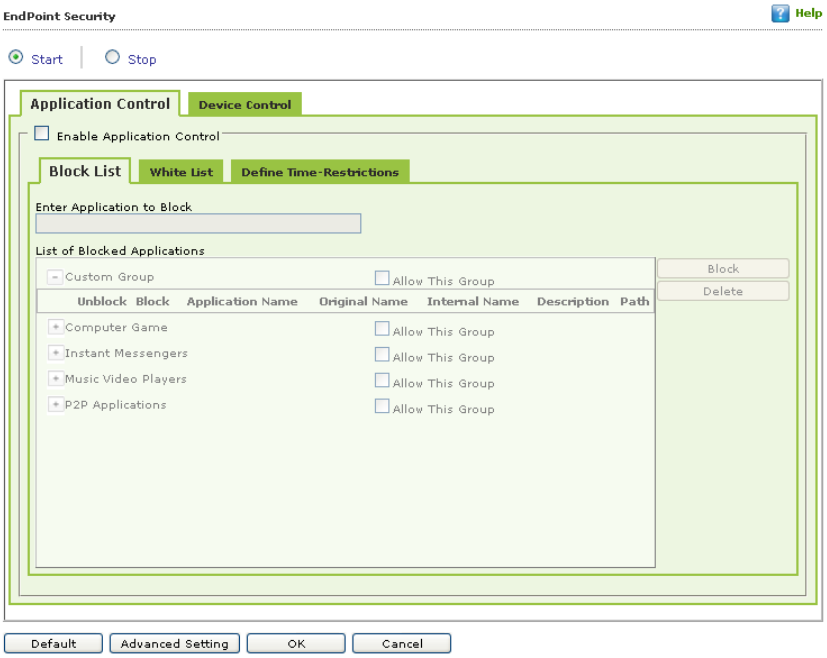


Figure – 9.16

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

This page provides you with information regarding the status of the module and options for configuring it.

- **Start / Stop:** It enables you to enable or disable **Endpoint Security** module. Click the appropriate option.

There are two tabs – Application Control and USB Control, which are as follows:

1. *Application Control*

This tab helps you control the execution of programs on the computer. All the controls on this tab are disabled by default.

You can configure the following settings.

- **Enable Application Control:** You should select this check box if you need to enable the Application Control feature of the Endpoint Security module.

- **Enter Application to Block:** It indicates the name of the application you want to block from execution. Type the full name of the application to be blocked.
- **List of Blocked Applications:** This list contains blocked executables of applications that are predefined by MicroWorld. Each of the applications listed in the predefined categories are blocked by default. In addition, you can also add executables that you need to block only to the Custom Group category. If you want, you can unblock the predefined application by clicking the **UnBlock** link. The predefined categories include computer games, instant messengers, music & video players, and P2P applications.

2. ***USB Control*** **-** The Endpoint Security feature of eScan protects your computer from unauthorized portable storage devices prompting you for the password whenever you plug in such devices. The devices are also scanned immediately when connected to prevent any infected files running and infecting the computer.

You can configure the following settings:

- **Enable USB Control:** ***[Default]*** You should select this check box if you need to monitor all the USB storages devices connected to your computer. This will enable all the options on this tab.

    - **Settings:** This section helps you customize the settings for controlling access to USB storage devices.

    - **Block USB Ports:** Select this check box if you want to block all the USB ports.
    - **Ask for Password:** Select this check box, if you want eScan to prompt for a password whenever a USB storage device is connected to the computer. You have to type the correct password to access USB storage device. It is recommended that you always keep this check box selected.

    - **Use eScan Administrator:** This option is available only when you select the **Ask for Password** check box. Click this option if you want to assign eScan Administrator password for accessing USB storage device.
    - **Use Other Password:** This option is available only when you select the **Ask for Password** check box. Click this option if you want assign a unique password for accessing USB storage device.

    - **Do Virus Scan:** ***[Default]*** When you select this check box, the Endpoint Security module runs a virus scan if the USB storage device is activated. It is recommended that you always keep this check box selected.
    - **Disable AutoPlay:** ***[Default]*** When you select this check box, eScan disables the automatic execution of any program stored on a USB storage device when you connect the device.

- **Read Only USB:** Select this check box, if you want to allow access of the USB device in read-only mode.
- **Record Files Copied To USB:** Select this check box, if you want eScan to create a record of the files copied from the system to USB drive.
- **Whitelist:** eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password but will directly display the files or folders stored on 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 on the **Add** button. The **Whitelist** section displays the following button.
- **Scan Whitelisted USB Devices:** By default, eScan does not scan whitelisted USB devices. You should select this option, if you want eScan to scan USB devices that have been added to the whitelist.
- You can click on the **Add** button to enter the **Serial number** (unique for each USB device) and **Device Name** of the USB device to be whitelisted. The Serial Number and the Device Name details are shown in Endpoint security module in eScan Protection Center under the same sub-section. You need to insert the USB device on the eScan server and copy the details onto the eScan web console settings.

Advanced Settings

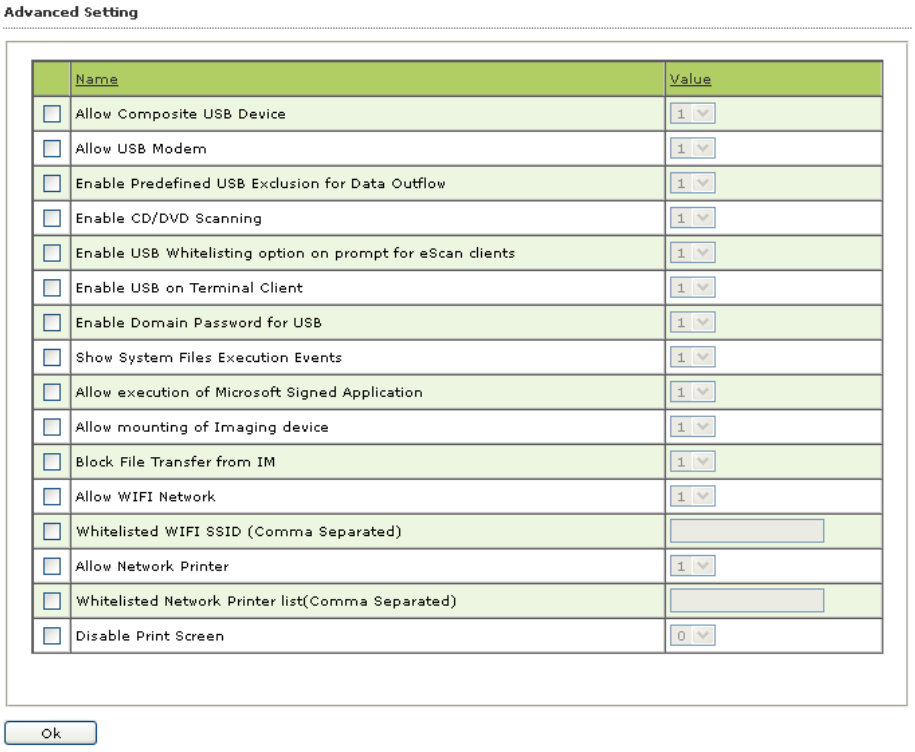


Figure – 9.17

Option	Description
Allow Composite Devices (Allow=1, Disallow =0)	Allows you to allow or disallow Scanning of Composite Devices connected to the Managed Endpoints.
Allow USB Modem(Allow=1, Disallow =0)	Allows you to allow or disallow USB Modems on the Managed Endpoints.
Enable Predefined USB Exclusion for Data Outflow (Enable=1, Disable =0)	Allow you to Enable / Disable Exclusion of Predefined USBs for Data Outflow, it will not record data outflow through USB drive specified by you.
Enable CD/DVD Scanning(Enable=1, Disable =0)	Allows you to allow or disallow Scanning of CD/DVD on Managed Endpoints.
Enable USB Whitelisting option on prompt for eScan clients (Enable=1, Disable =0)	Allow you to Enable / Disable USB whitelisting on prompt on the managed Endpoints.
Enable USB on Terminal Client (Enable=1, Disable =0)	Allow you to Enable / Disable USB on Terminal Client
Enable Domain Password for USB(Enable=1, Disable =0)	Allows you to Enable/Disable Password for USB usage on managed endpoints.
Show System Files Execution Events (Enable=1, Disable =0)	Allows you to Enable/Disable to receive events for System Files execution.
Allow execution of Microsoft Signed Application(Allow=1, Disallow =0)	Allow / Disallow execution of Microsoft Signed Application.
Allow mounting of Imaging device(Allow=1, Disallow =0)	Allow / Disallow mounting of Imaging Devices on Managed endpoints.
Block File Transfer from IM(Allow=1, Block =0)	Allow / Block files transfer from Instant Messengers on managed Endpoints.
Allow WIFI Network(Allow=1, Block =0)	Allow / Block access of Managed Endpoints to WIFI network.
Whitelisted WIFI SSID (Comma Separated)	Allow you to enlist /whitelist WIFI SSID for network access to managed endpoints.
Allow Network Printer (Allow=1, Block =0)	Allow access to network printers from managed endpoints.
Whitelisted Network Printer list(Comma Separated)	Allow you to enlist /whitelist Network Printers for managed endpoints.
Disable Print Screen (Enable=1, Disable =0)	Allows you to disable/enable Print Screen on Managed Endpoints.

Default

Note:- Click the Default button, if you want to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

6. Privacy Control

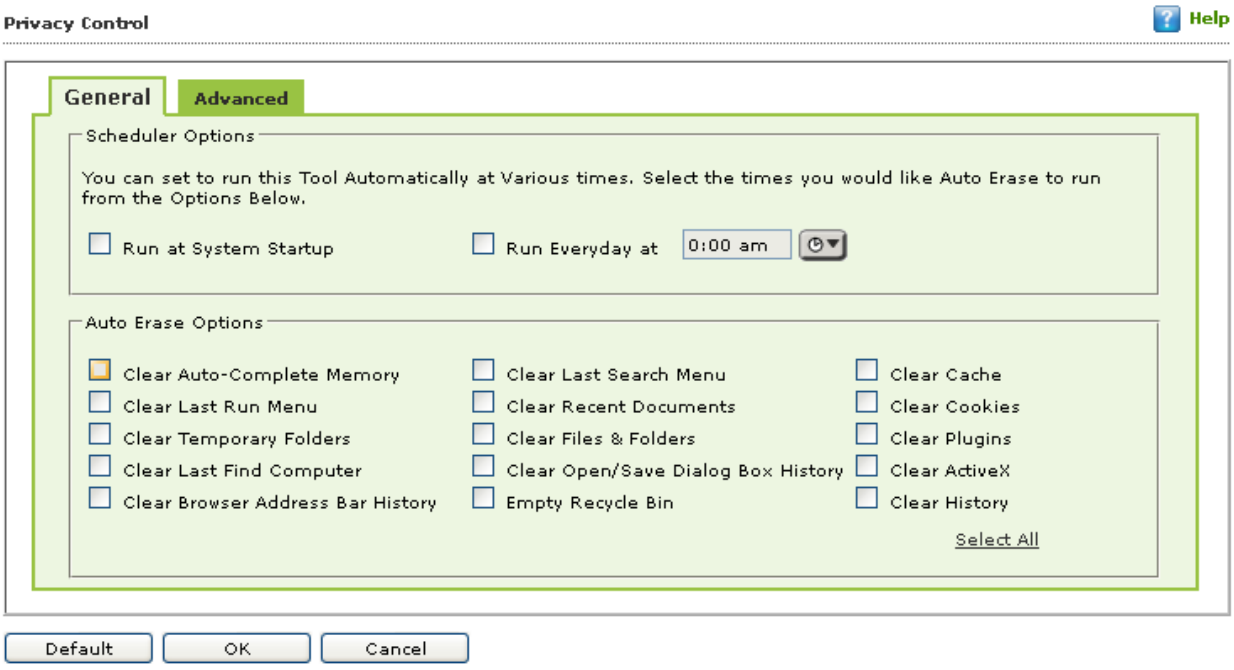


Figure – 9.18

Privacy Control is a part of eScan's Protection feature. It protects your confidential information from theft by deleting all the temporary information stored on your computer. This module comes with the eScan Browser Cleanup feature, which allows you to use the Internet without leaving any history or residual data on your hard drive by erasing details of sites and Web pages you have accessed while browsing. This page provides you with options for configuring the module. There are two tabs – **General** and **Advanced**, which are as follows:

1. *General*

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

You can configure the following settings.

- **Scheduler Options:** You can set the scheduler to run at specific times and erase private information, such as your browsing history from your computer. The following settings are available in the **Scheduler Options** section.

    - **Run at System Startup:** It auto executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.
    - **Run Everyday at:** It auto-executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.
- **Auto Erase Options:** The browser stores traceable information of the Web sites that you have visited in certain folders. This information can be viewed by others. eScan allows you to remove all traces of Web sites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. You can select the following options based on your requirements.

    - **Clear Auto Complete Memory:** Auto Complete Memory refers to the suggested matches that appear when you type text in the Address bar, the Run dialog box, or forms in Web pages. Hackers can use this information to monitor your surfing habits. When you select this check box, Privacy Control clears all this information from the computer.
    - **Clear Last Run Menu:** When you select this check box, Privacy Control clears this information in the Run dialog box.
    - **Clear Temporary Folders:** When you select this check box, Privacy Control clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive of the computer and boosts the performance of the computer.
    - **Clear Last Find Computer:** When you select this check box, Privacy Control clears the name of the computer for which you searched last.
    - **Clear Browser Address Bar History:** When you select this check box, Privacy Control clears the Web sites from the browser's address bar history.
    - **Clear Last Search Menu:** When you select this check box, Privacy Control clears the name of the objects that you last searched for by using the Search Menu.
    - **Clear Recent Documents:** When you select this check box, Privacy Control clears the names of the objects found in Recent Documents.
    - **Clear Files & Folders:** When you select this check box, Privacy Control deletes selected Files and Folders. You should use this option with caution because it permanently deletes unwanted files and folders from the computer to free space on the computer.
    - **Clear Open / Save Dialog box History:** When you select this check box, Privacy Control clears the links of all the opened and saved files.

- **Empty Recycle Bin:** When you select this check box, Privacy Control clears the Recycle Bin. You should use this option with caution because it permanently clears the recycle bin.
- **Clear Cache:** When you select this check box, Privacy Control clears the Temporary Internet Files.
- **Clear Cookies:** When you select this check box, Privacy Control clears the Cookies stored by Web sites in the browser's cache.
- **Clear Plugins:** When you select this check box, Privacy Control removes the browser plug-in.
- **Clear ActiveX:** When you select this check box, Privacy Control clears the ActiveX controls.
- **Clear History:** When you select this check box, Privacy Control clears the history of all the Web sites that you have visited.

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

- **Select All/ Unselect All:** You can click this button to select / unselect all the auto erase options.

2. *Advanced*

This tab helps you to select the MS Office files, Windows files and other Windows media files.

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

It also allows you to do the following (Windows Operating System)

Define Administrator password - Administrator Password enables you to create and change password for administrative login of eScan protection center. It also enables you to keep the password as blank, wherein you can login to eScan protection center without entering any password.

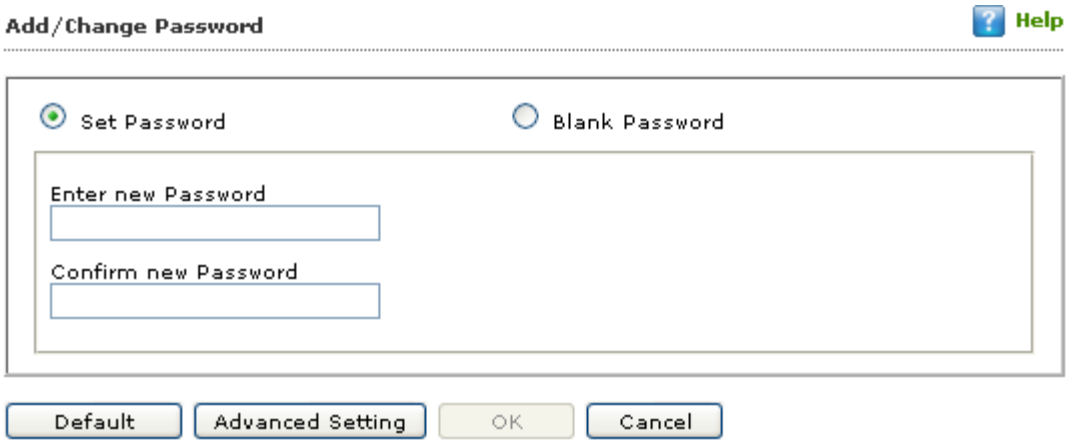


Figure – 9.19

Advanced Setting

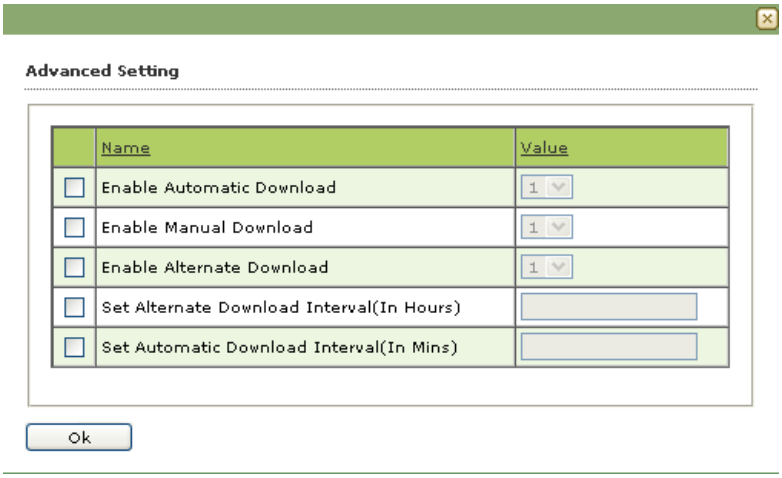


Figure – 9.20

Sr. No.	Name	Description
1.	Enable Automatic Download (1 = Enable / 0= Disable)	It allows you to Enable / disable Automatic download of Antivirus signature updates.
2.	Enable Manual Download (1 = Enable / 0= Disable)	It allows you to Enable / disable Manual download of Antivirus signature updates
3.	Enable Alternate Download(1 = Enable / 0= Disable)	It allows you to Enable / disable download of signatures from eScan (Internet) if eScan Server is not reachable.
4.	Set Alternate Download Interval(In Hours)	It allows you to define time interval to check for updates from eScan (Internet) and download it on managed endpoints.
5.	Set Automatic Download Interval (In Mins)	It allows you to define time interval to check for updates from for automatic download on managed endpoints.

MWL (MicroWorld WinSock Layer) Inclusion List contains the name of all executables files which will bind itself to MWTSP.DLL. All other files are excluded.

Note:-Click the ***Default*** button, if you want to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

You can do the following activities.

- **Adding files** to inclusion list
- **Deleting files** from inclusion list
- **Removing all files** from inclusion list

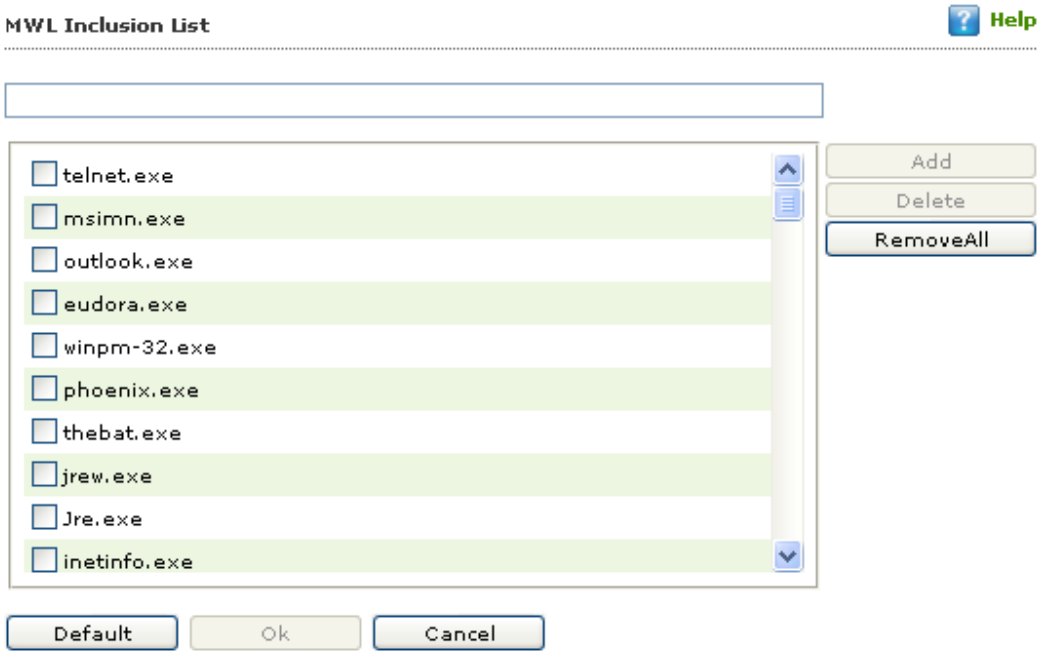


Figure – 9.21

- **Adding files to inclusion list**. It enables you to add executable files to the list.

    1. Type the executable file name in the given field, and then click the **Add** button. The file gets added to the list.
    2. Click the **OK** button.

- **Deleting files from inclusion list**. It enables you to delete executable files from the list.

    1. Select the appropriate file checkbox, and then click the **Delete** button. For example, Eudora.exe, winpm-32.exe, phoenix.exe, and so on. A message appears, whether you want to delete or not.
    2. Click **OK**. The file gets deleted from the list.

- **Removing all files from inclusion list**. It enables you to remove all executable files from the list.

    1. Click **Remove All**. A message appears, whether you want to remove the list or not.
    2. Click **OK**. All the files get removed from the list.

1. MWL Exclusion List

MWL (MicroWorld WinSock Layer) Exclusion List contains the name of all executable files which will not bind itself to **MWTSP.DLL**.

Note:- Click the ***Default*** button, if you want to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.
You can do the following activities.

- **Adding files** to exclusion list
- **Deleting files** from exclusion list
- **Removing all files** from exclusion list

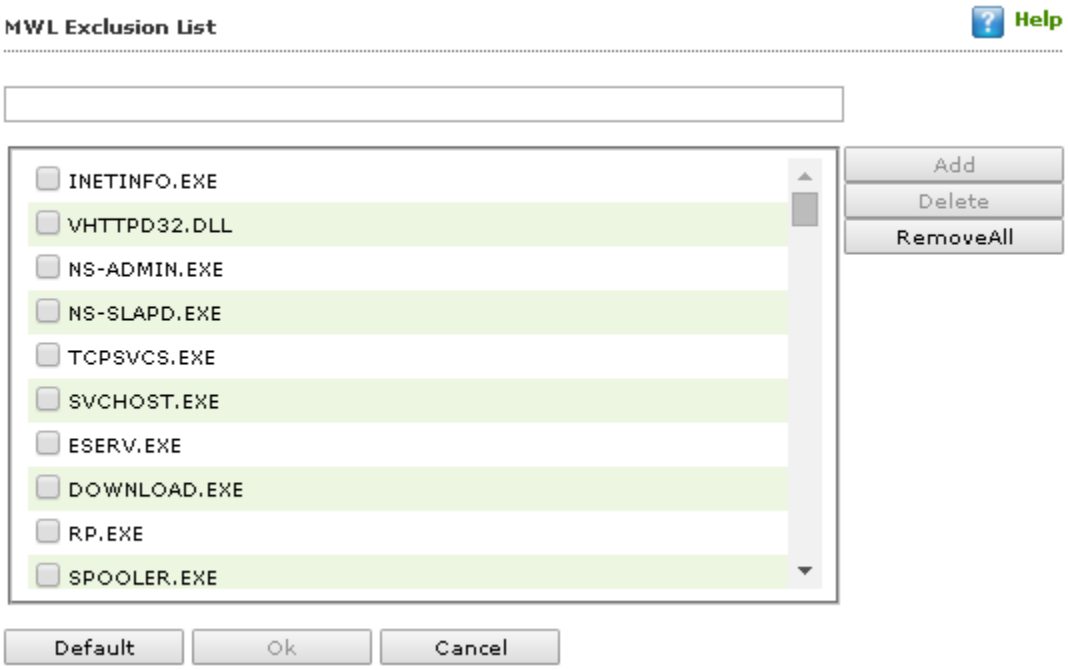


Figure – 9.22

- **Adding files to exclusion list. It enables you to add executable files to the list.**

    1. Type the executable file name in the given field, and then click the **Add** button. The file gets added to the list.

- **Deleting files from exclusion list.** It enables you to delete executable files from the list.

    1. Select the appropriate file checkbox, and then click the **Delete** button. For example, INETINFO.EXE, VHTTPD32.DLL, NS-ADMIN.EXE, and so on. A message appears, whether you want to delete or not.
    2. Click **OK**. The file gets deleted from the list.

- **Removing all files from exclusion list.** It enables you to remove all executable files from the list.

1. Click **Remove All**. A message appears, whether you want to remove the list or not.
2. Click **OK**. All the files get removed from the list.

1. **Notifications and Events**

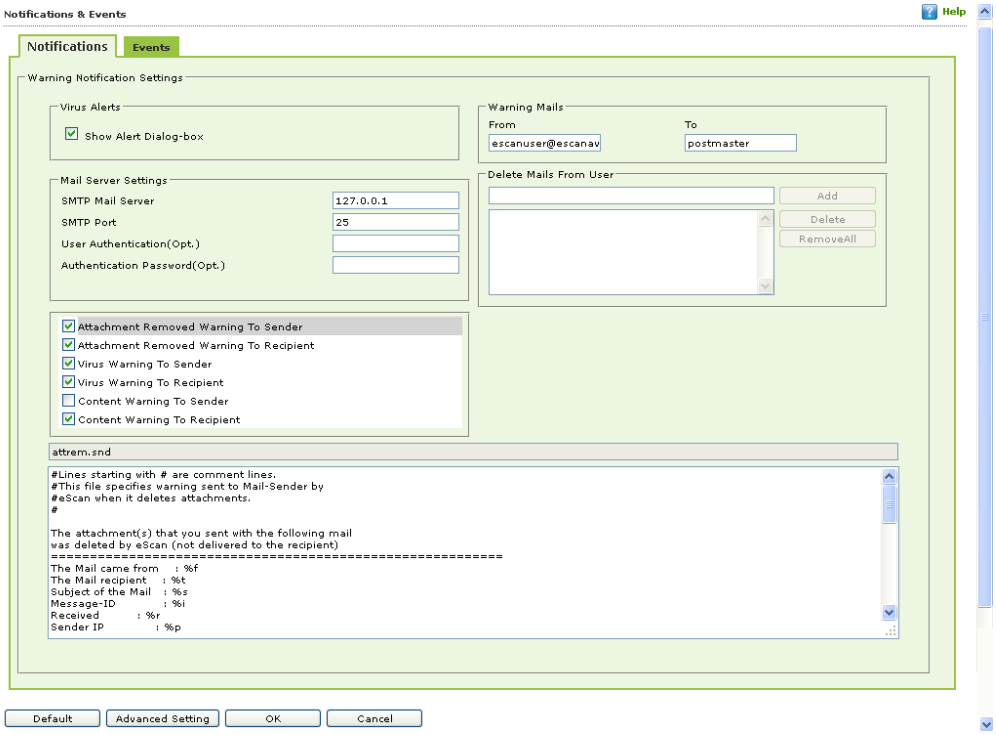


Figure – 9.23

Notifications enable you to configure the notification settings. It helps you to send e mails to specific recipients when malicious code is detected in an e-mail or e-mail attachment. It also helps you to send alerts and warning messages to the sender or recipient of an infected message. You can configure the following settings:

- **Virus Alerts:** ***[Default]*** You should select this check box if you need Mail Anti-Virus to alert you when it detects a malicious object in an e-mail.
- **Warning Mails:** You configure this setting if you need Mail Anti -Virus to send warning e mails and alerts to a given sender or recipient. The default sender is **escanuser@escanav.com** and the default recipient is **postmaster**.
- **Mail Server Settings:** Define settings for mail server for sending email notifications
- **Attachment Removed Warning To Sender:** ***[Default]*** You should select this check box if you need Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this e-mail when it encounters a virus-infected attachment in an e-mail. The content of the e-mail that is sent is displayed in the preview box.

- **Attachment Removed Warning To Recipient:** ***[Default]*** You should select this check box if you need Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The content of the e-mail that is sent is displayed in the preview box.
- **Virus Warning To Sender:** ***[Default]*** You should select this check box if you need Mail Anti-Virus to send a virus-warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
- **Virus Warning To Recipient:** ***[Default]*** You should select this check box if you need Mail Anti-Virus to send a virus-warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- **Content Warning To Sender:** You should select this check box if you need Mail scanner to send a content warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
- **Content Warning To Recipient:** ***[Default]*** You should select this check box if you need Mail scanner to send a content warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- **Delete Mails From User:** You can configure eScan to automatically delete e mails that have been sent by specific users. For this, you need to add the e mail addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. Once you type text in the **Delete Mails From User** field, the buttons appear.

7. **Events**

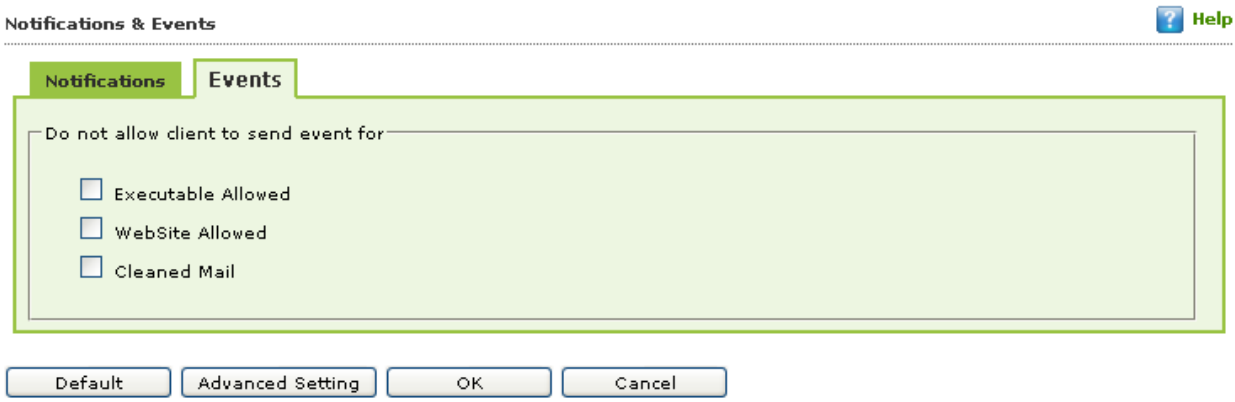


Figure – 9.24

Define settings to stop client from sending Event of certain types of Executables Allowed, Website Allowed, and Cleaned Mail as per your selection.

Schedule Update

Automatic download: Select this option to automatically download the updates from the eScan Server.

Schedule Download: Define Settings for Scheduling update on endpoints; you can schedule an update on a daily, weekly, or monthly basis and at a defined time.

Configurable eScan Policies for Linux and Mac Computers

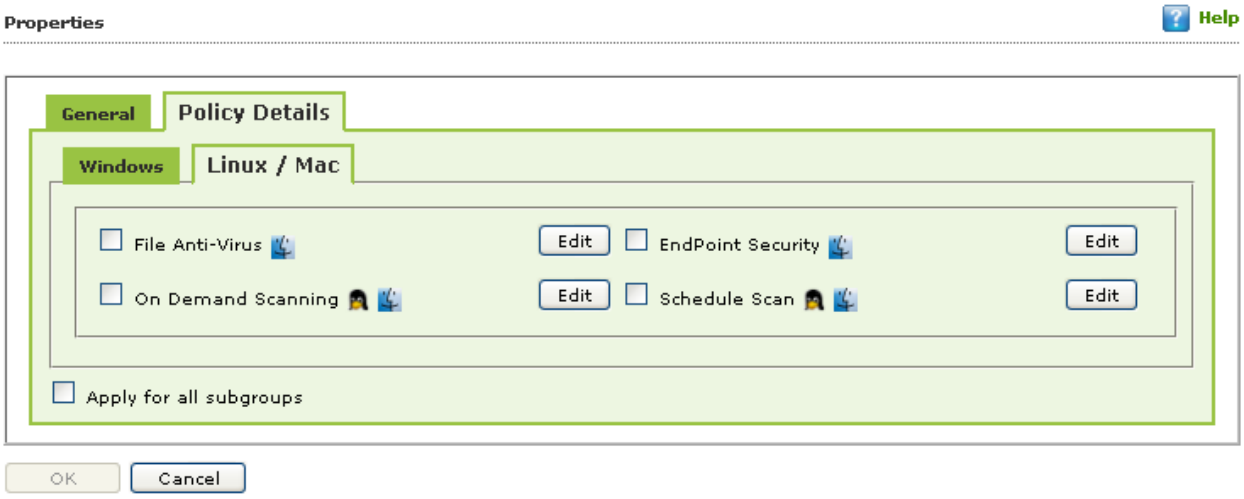


Figure – 9.25

To define policies for Mac or Linux computers, select Policy option present under the desired computer group in Managed Computers section of eScan. Now click on Properties button present on the interface and then click on Policy Details tab and open Linux / Mac tab present on the interface. eScan allows you to define settings for File Anti-Virus, Endpoint Security, On Demand scanning and Schedule Scan module for Linux and Mac Computers connected to the network. Use the **Edit** button to configure the eScan module settings for computers with respective operating systems.

Note – Icons present beside every module denotes that the settings are valid for the respective operating systems only.

Configuring Module Settings for Linux and Mac Computers

It allows you to define settings for Scanning; you can also define action to be taken in case of an infection. It also allows you to define the number of days for which the logs should be kept as well as create list for Masks, Files or Folders to be excluded from scanning.

- **File Anti-Virus –** Settings valid for eScan Client on **Mac** Computers only**.**

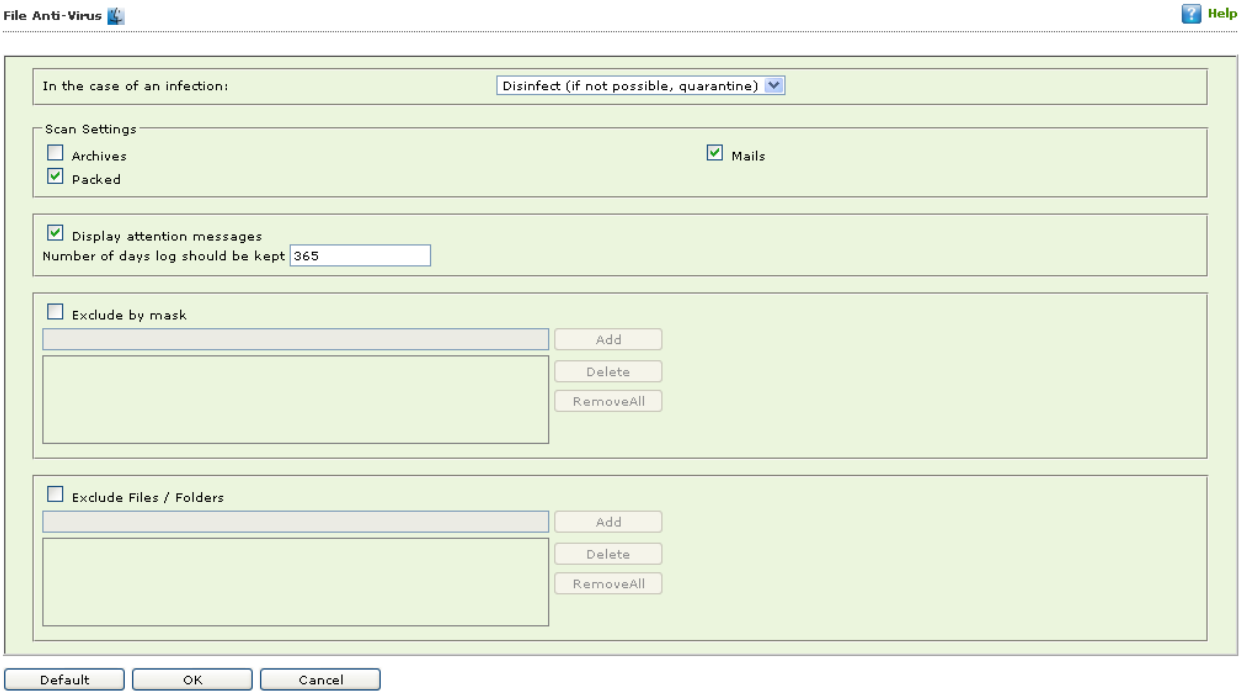


Figure – 9.26

- **Actions in case of infection [Dropdown]**

  It indicates a type of action which you want eScan real-time protection to 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: It indicates or alerts the user about the infection detected (No Action is taken, only logs are maintained).
Disinfect (if not possible, log): It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
Disinfect (if not possible, delete file): It tries to disinfect and if disinfection is not possible it deletes the infected object.
Disinfect (if not possible, quarantine file): It tries to disinfect and if disinfection is not possible it quarantines the infected object.
Delete: It directly deletes the infected object.
Quarantine: It directly quarantines the infected object.
Scan Settings
Mails - It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.

- **Archives -** It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.

- **Packed -** It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.

- **Exclude file types (Mask) -** Select this check box if you want eScan real-time protection to exclude specific file extensions.

- **Exclude Folders and files -** Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan allows you add, Remove any or all Added Files or Folders whenever required.

  You can restore default eScan settings by clicking on the **Default** button present at the bottom of the interface.

8. **Endpoint Security** (Settings valid for eScan client on **Mac** systems only.)

Figure – 9.27

Use this option to Block access to USB Storage device by selecting the Check box.

Configure Settings for On Demand Scanning – valid for Linux and Mac Computers

Using ODS Settings you can define actions in case of infection, you can also define list of files by mask, Files or Folders to be excluded from Scanning. It also allows you to configure settings for various other Scan options like Include Sub directories, Mails, Archives Heuristic Scanning etc by selecting respective checkbox options present at the bottom of the interface.

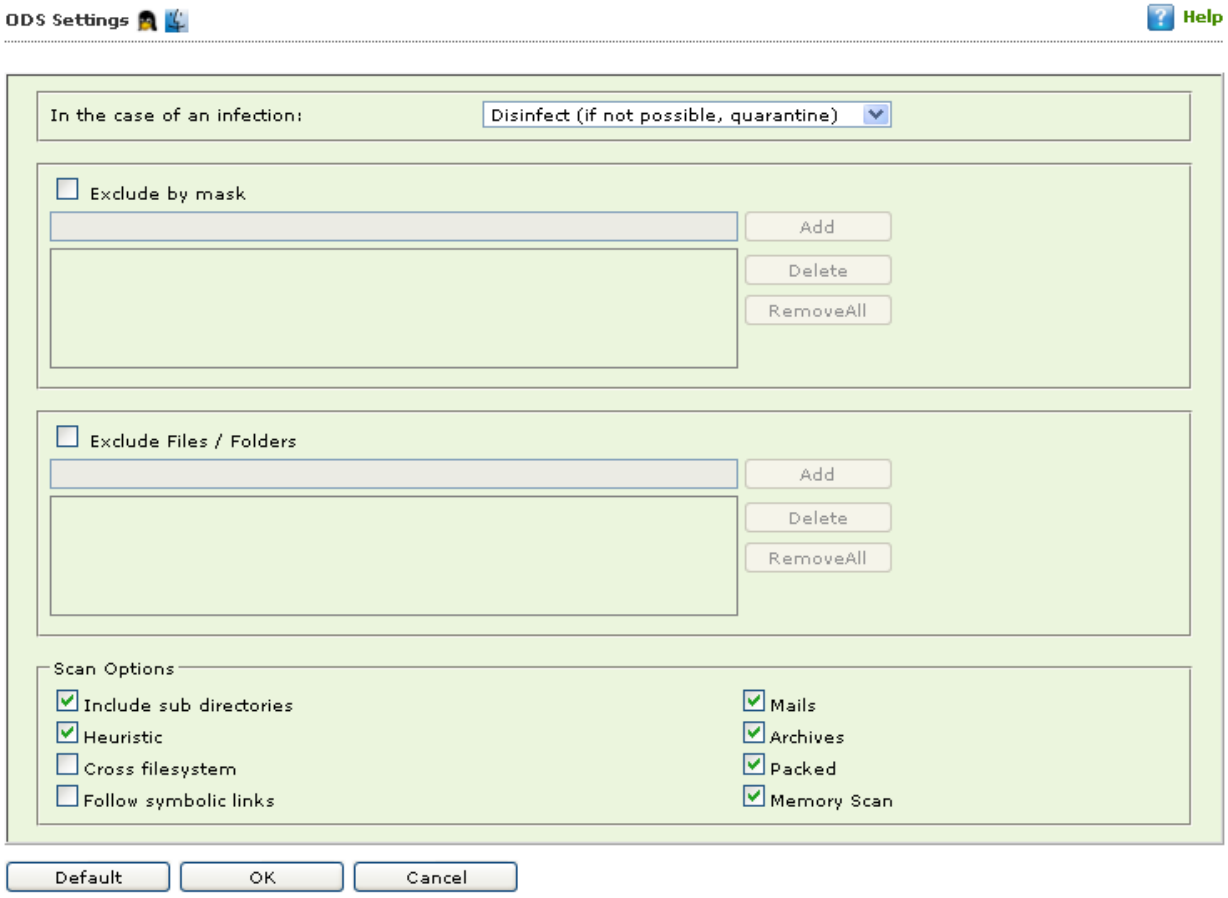


Figure – 9.28

- **Actions in case of infection [Dropdown]**

  It indicates a type of action which you want eScan real-time protection to 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: It indicates or alerts the user about the infection detected.
Disinfect (if not possible, log): It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
Disinfect (if not possible, delete file): It tries to disinfect and if disinfection is not possible it deletes the infected object.
Disinfect (if not possible, quarantine file): It tries to disinfect and if disinfection is not possible it quarantines the infected object.
Delete: It directly deletes the infected object.
Quarantine: It directly quarantines the infected object.

Scan Settings

- **Mails -** It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives -** It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed -** It indicates the compressed executable.
- **Exclude file types (Mask) -** Select this check box if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.
- **Exclude Folders and files -** Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan allows you add, Remove any or all Added Files or Folders whenever required during On Demand Scanning. You can restore default eScan settings by clicking on the **Default** button present at the bottom of the interface.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Symbolic Link Scanning** scans the files following the symbolic links.

9. Schedule Scanning

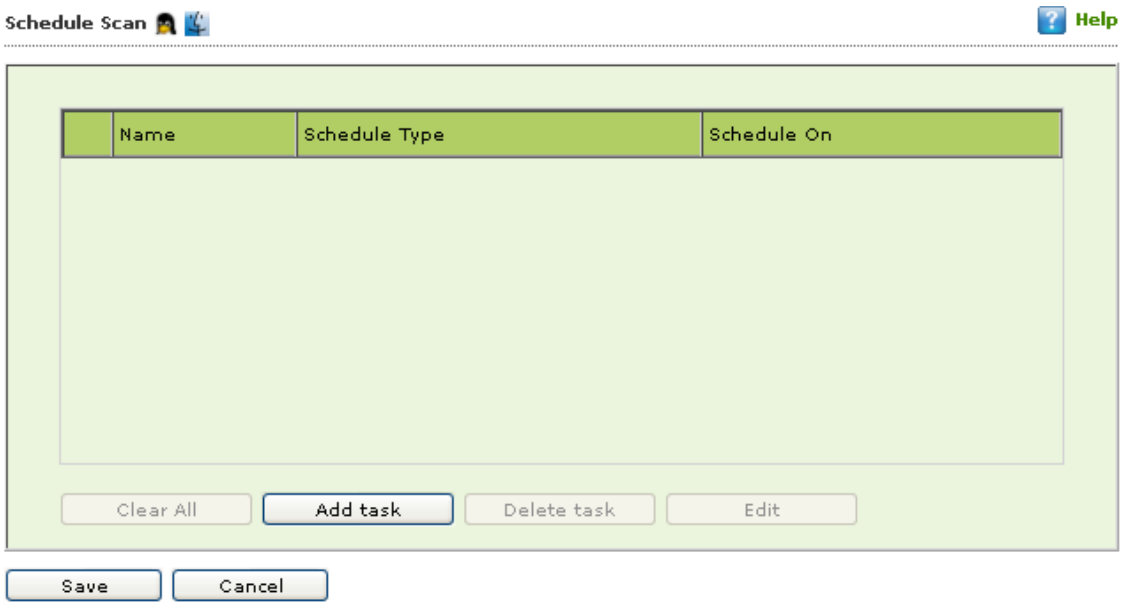


Figure – 9.29

It allows you to add a task for scheduling a scan.

- **Adding a task -** It allows you to schedule and define options for Analysis extent and the Files or Folders to be scanned.

- **Schedule -**

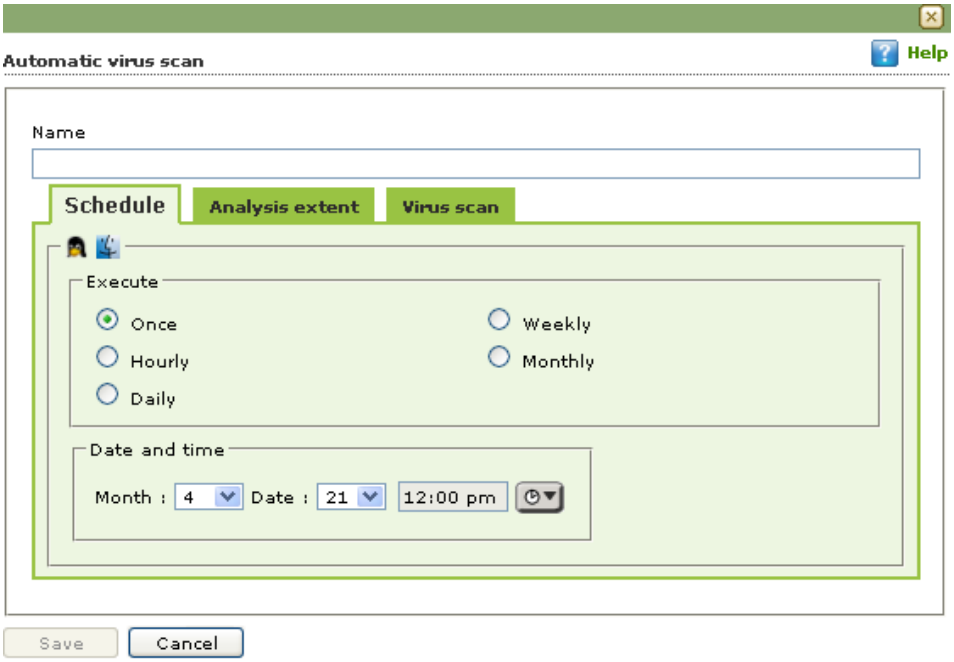


Figure – 9.30

Using this tab you can define the task name and schedule it as desired. You can schedule once, Weekly basis, every hour, monthly or daily. It also allows you to schedule at desired date and time.

- **Analysis Extent**

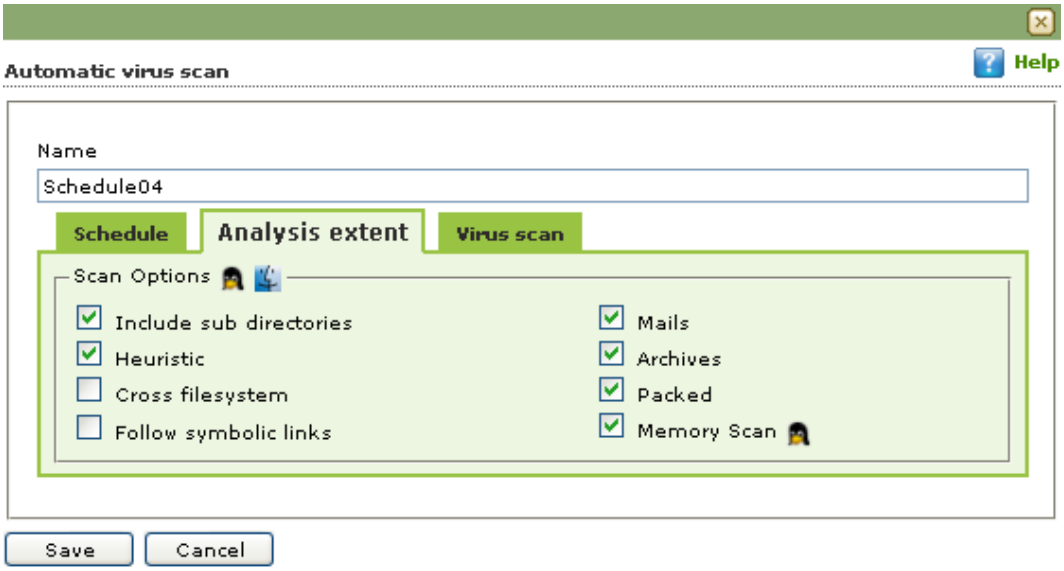


Figure – 9.31

Using this tab you can define the scan options for Linux and Mac computers connected to the network.

1. **Include sub Directories** – Allows you to include sub directories while conducting an automatic scan.
2. **Heuristic Scan** – A heuristic scan is used to detect new, unknown viruses in your systems that have not yet been identified. Heuristic methods are based on the piece-by-piece examination of a virus, looking for a sequence or sequences of instructions that differentiate the virus from 'normal' programs. It allows you to enable Heuristic Scanning at the time of Automatic Scanning.
3. **Cross File System** that facilitates scanning of files over cross-file systems.
4. **Symbolic Link Scanning** scans the files following the symbolic links.
5. **Mails -** It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
6. **Archives -** It indicates the archived files, such as zip, .rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
7. **Packed -** It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.

- **Virus Scan**

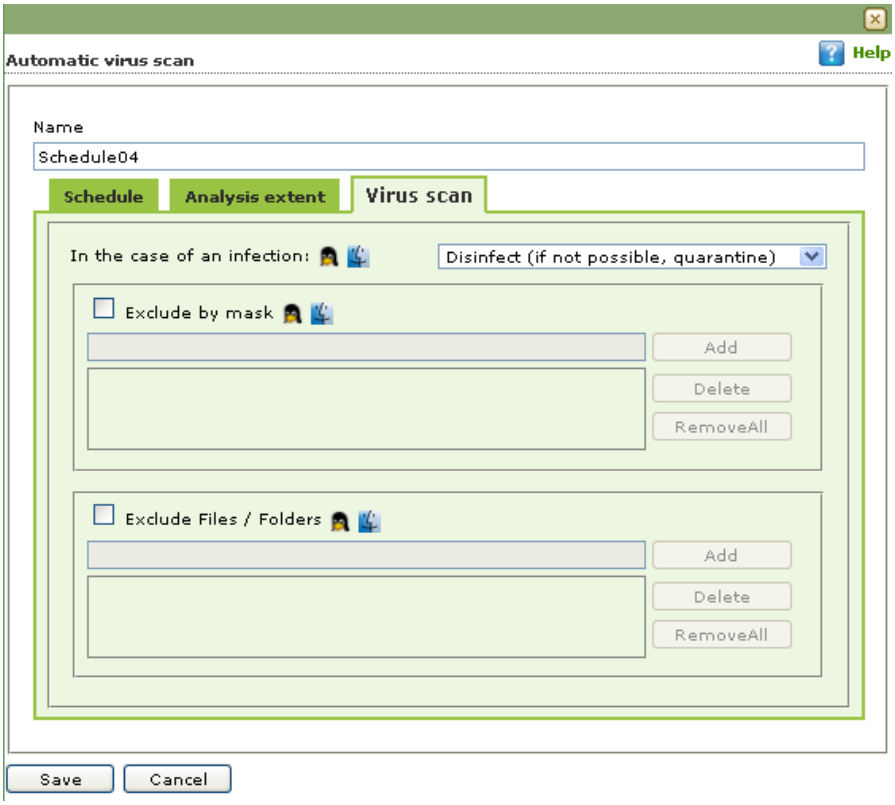


Figure – 9.32

- **Actions in case of Infection [Dropdown]**

  It indicates a type of action which you want eScan real-time protection to 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:** It indicates or alerts the user about the infection detected.
  - **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
  - **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
  - **Disinfect (if not possible, quarantine file):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
  - **Delete:** It directly deletes the infected object.
  - **Quarantine:** It directly quarantines the infected object.

  - **Exclude file types (Mask) -** Select this check box if you want eScan real-time protection to exclude specific files, and then add the directories and files that you want to exclude using **Add** option present on the interface. eScan allows you to Remove any or all Added Files whenever required.

  - **Exclude Folders and files -** Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan allows you add, Remove any or all Added Files or Folders whenever required.

10. **Managing Tasks for the Group -** Using the **Group Tasks** option present in Managed Computers section under Selected Group, you can create a task, start a task, select a task and view its properties, view task results as well as delete an already created task. Tasks can include the following.

    - **Enable / Disable desired Module**
    - **Set Update Server**
    - **Force Client to Download Updates**
    - **Scheduling Scan on Networked Computers**

- **Steps for Creating a Group Task**

  1. Click **Managed Computers.**
  2. Select the desired group from the tree.
  3. Click **Group Tasks**

4. Now Click **New Task**. Refer **Figure – 9.33**

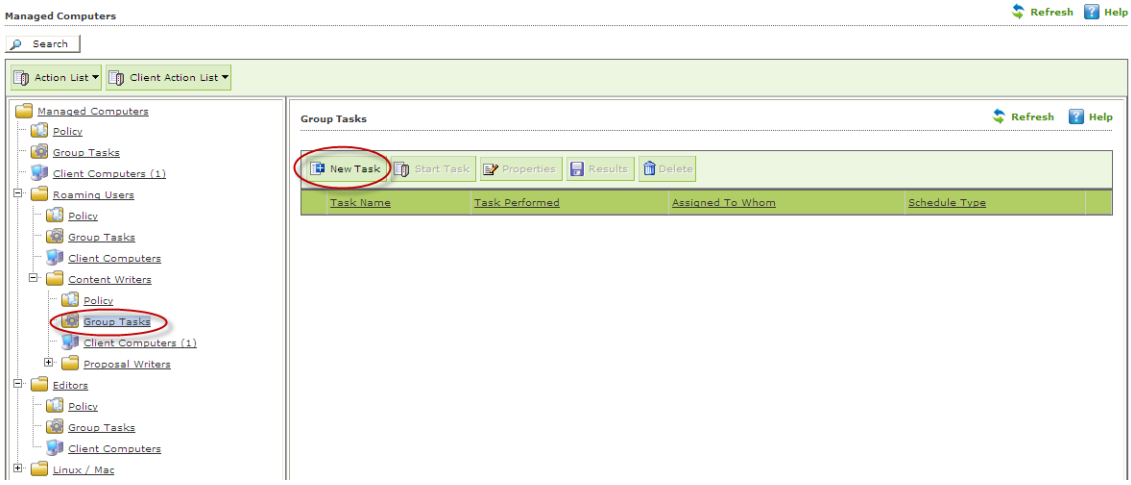


Figure – 9.33

5. You will be forwarded to "**New Task Template**" window. This window allows you to define **Task Name**, **Assign task** as well as **schedule task** on Endpoints. Write the Task Name and configure the desired task settings.
6. Click **Save**. Refer **Figure – 9.34**

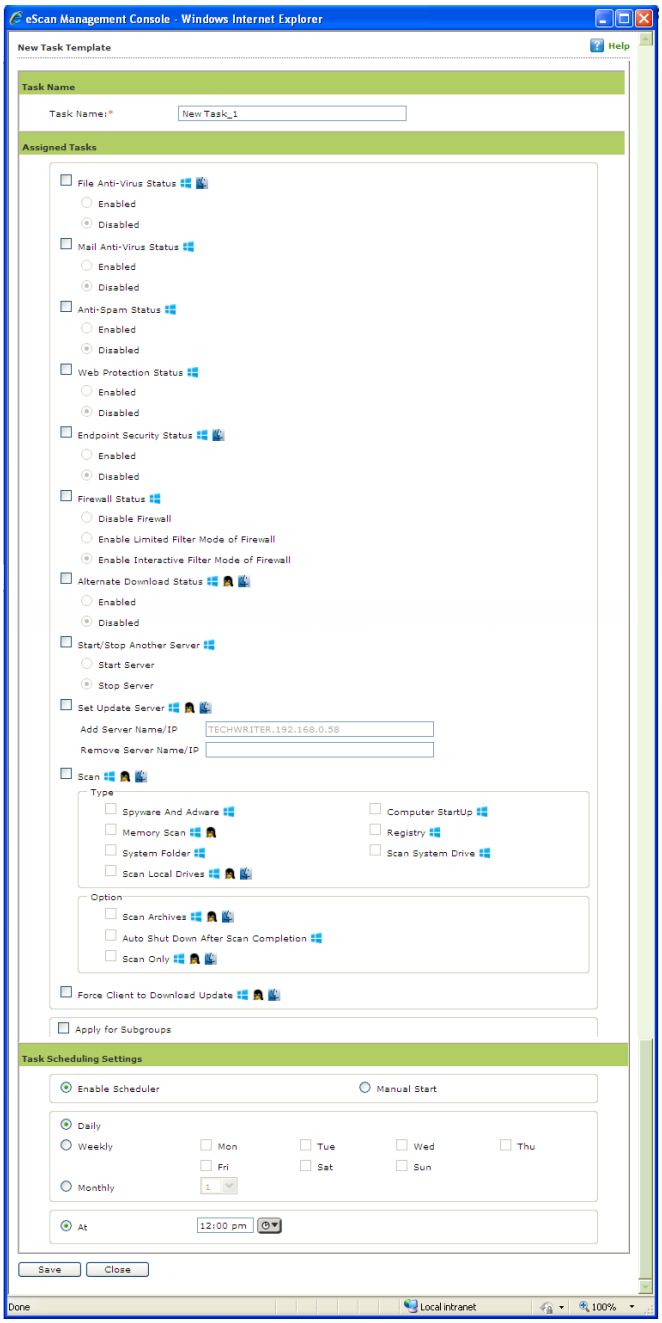


Figure – 9.34

Note: Windows, Linux , Mac Icon denotes that you can configure task settings for the selected module in the respective operating system.

7. The created task will be added to the Group tasks list. Refer **Figure – 9.35**

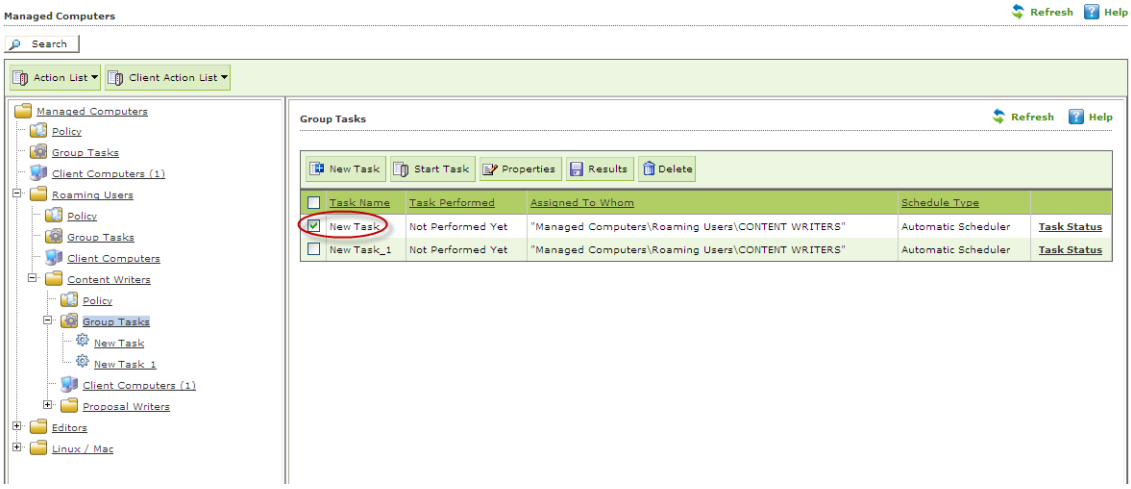


Figure – 9.35

8. Click **Properties** to view the created task. It also allows you to modify or re-define the settings earlier configured by you. It also facilitates the re-scheduling of the created task.
9. Click **Save**. Refer **Figure – 9.36**

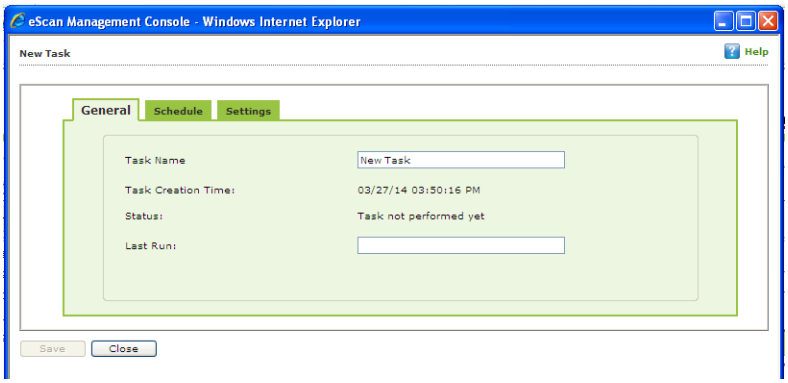


Figure – 9.36

10. Using the **Start Task** option you can initiate the selected task on the Endpoints in the Group. Refer **Figure – 9.37**

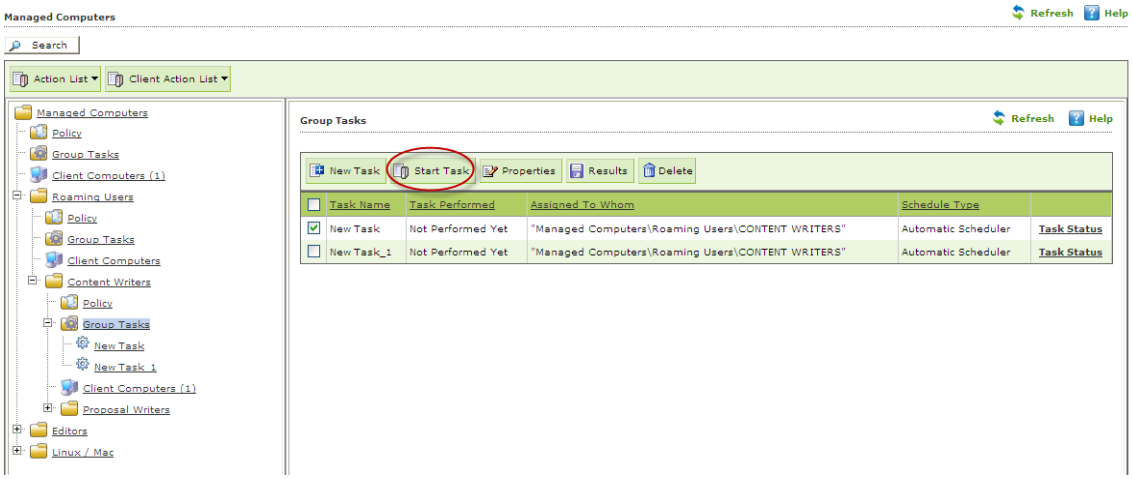


Figure – 9.37

11. Click **Results** to view the details of recently executed tasks.

12. Click Task Status Link to view the status of the listed tasks. It gives you a brief summary of the selected task.

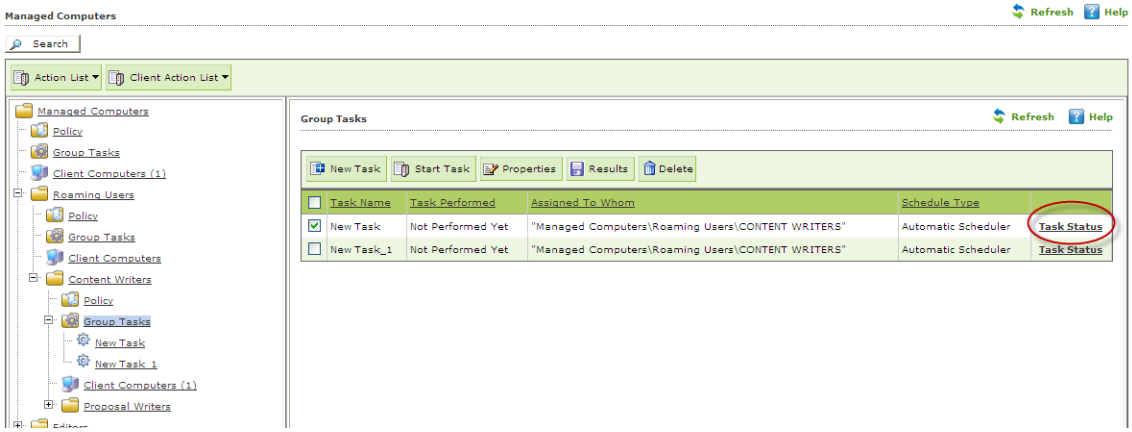


Figure – 9.38

10. Managing Tasks and Policies for Specific Computers

eScan Management Console gives you a flexibility to define and configure tasks and Policies for specific Endpoints in the Managed Computers list. It can easily be done using the following simple steps –

- **Managing Tasks for Specific Computers**

1. Click **Tasks for Specific Computers** in **Navigation Panel** of eScan Management Console.
2. Now Click **New Task**. Refer **Figure 10.1**

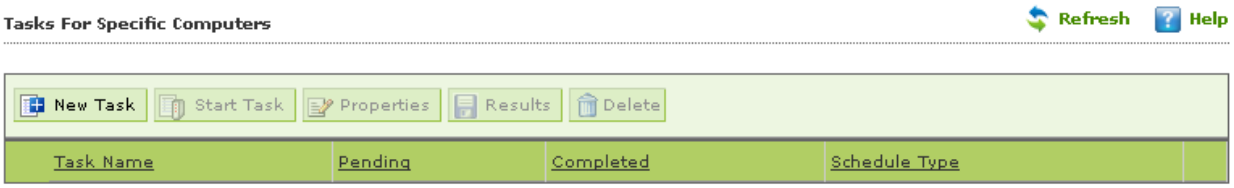


Figure 10.1

3. You will be forwarded to **New Task Template** Window.
    1. Define the **Task Name** in the text field. Refer **Figure 10.2**

Figure 10.2

    2. Select the desired options for assigning tasks. Refer **Figure 10.3**

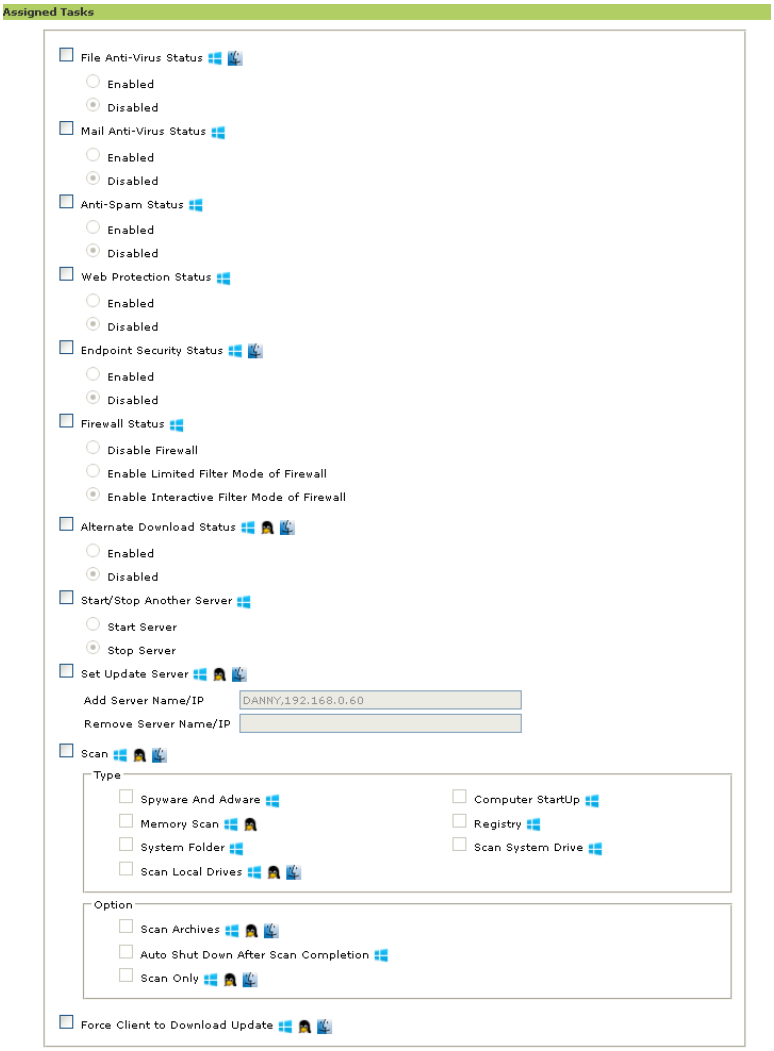


Figure 10.3

Note: Windows, Linux , Mac Icon denotes that you can configure task settings for the selected module in the respective operating system.

3. Use the explorer tree to select the Computers on which you wish to initiate this task. Mark the Computers and click **Add**. Refer **Figure 10.4**

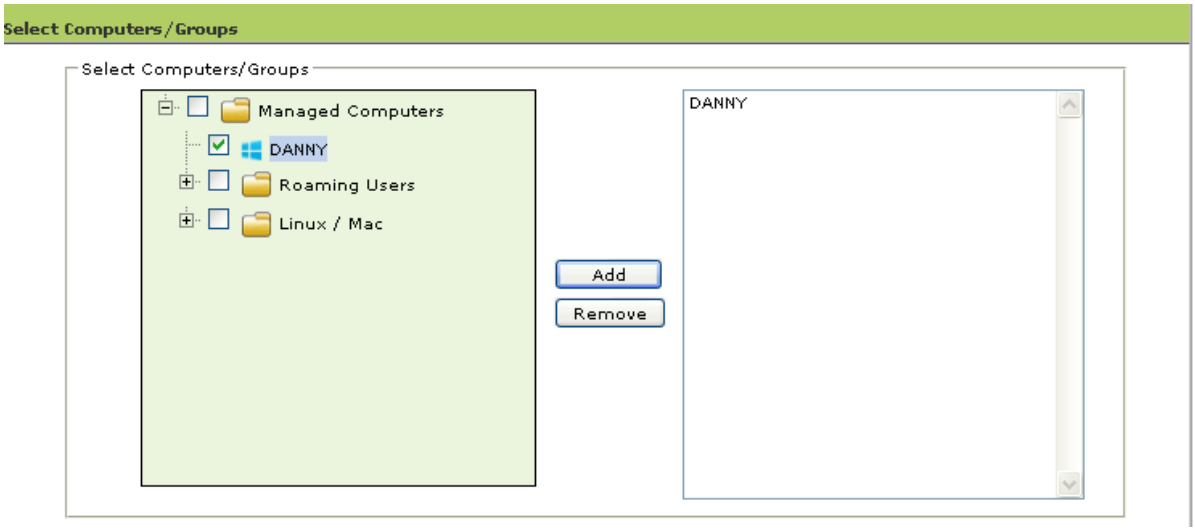


Figure 10.4

4. **Schedule the Task** as desired.

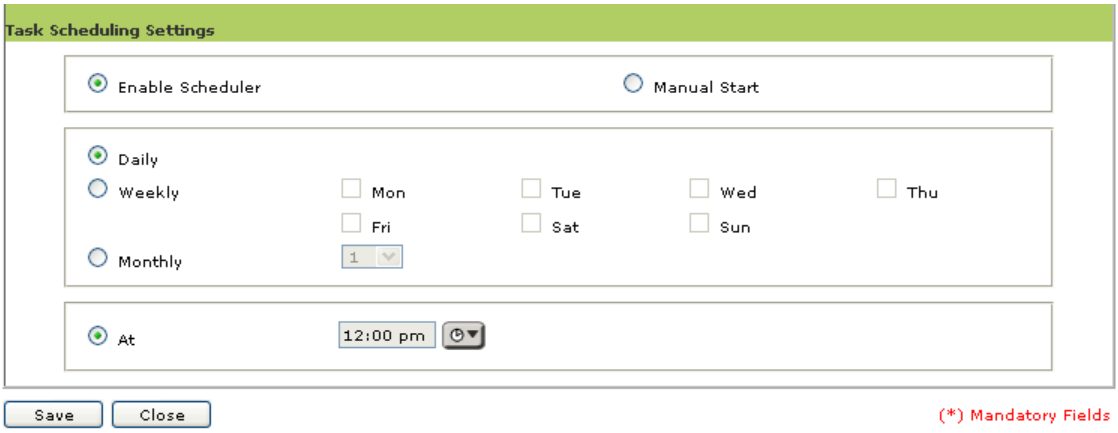


Figure 10.5

5. Click **Save**. The Task will be created and scheduled for selected computers instantly.

- **Managing Policies for Specific Computers**

1. Click **Policies for Specific Computers** option present in **Navigation Panel** of eScan Management Console and click **New Policy**. Refer **Figure 10.6**

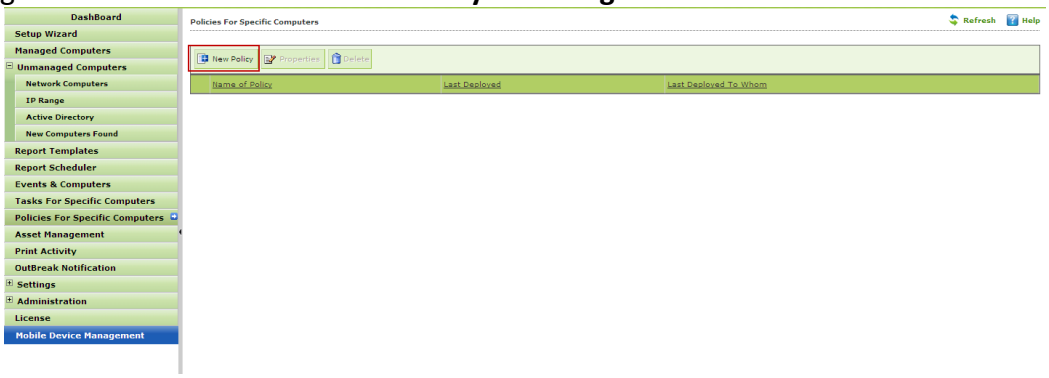


Figure 10.6

2. You will be forwarded to the New Policy window. Define the Policy name and Rules. Select and add the computers where you wish to implement those policies.
3. Click **Deploy**. Refer **Figure 10.7**

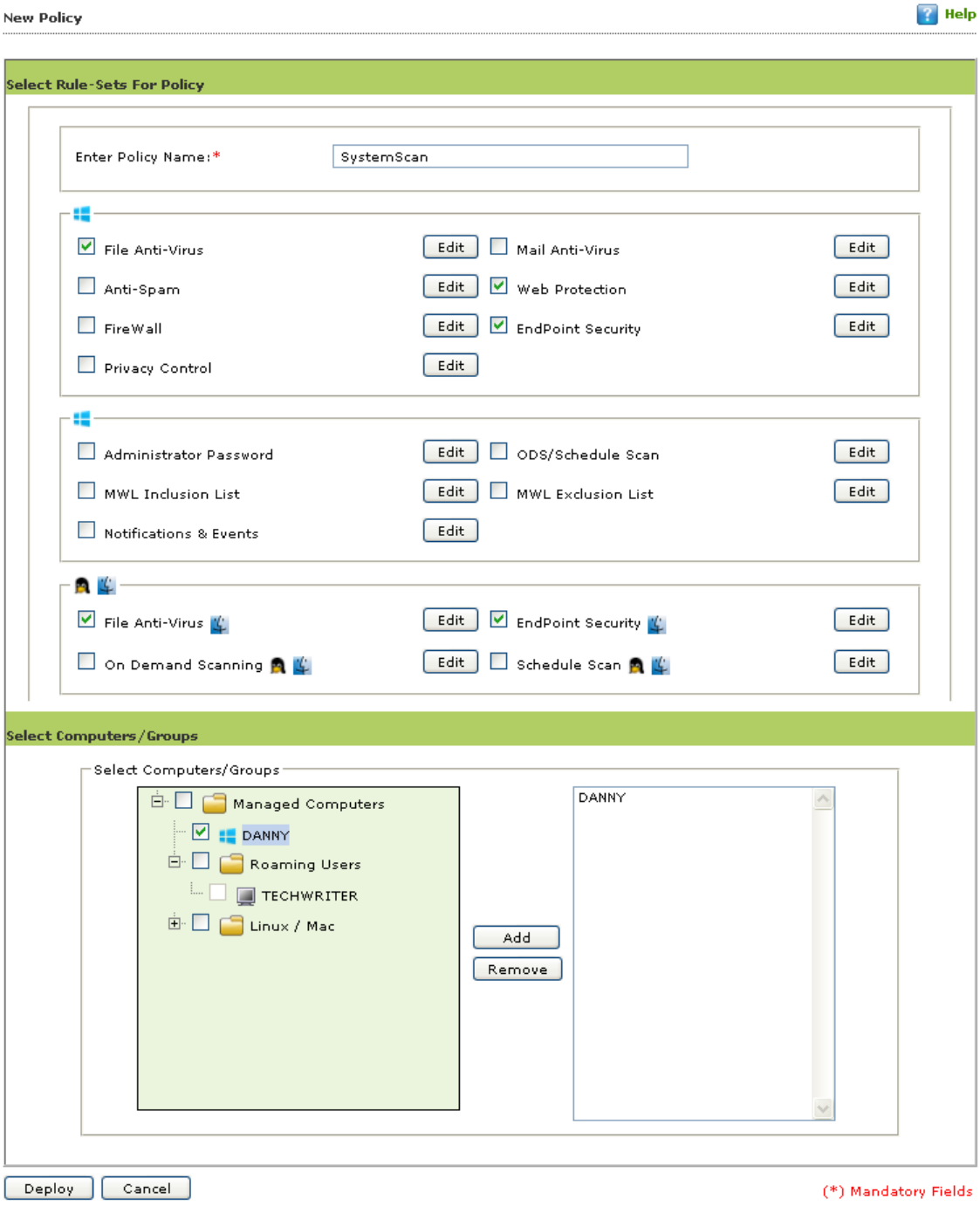


Figure 10.7

4. The policy will be created and deployed on the selected computers.

One Time Password

eScan password protection restricts user access from violating a security policy deployed in a network. e.g. administrator has deployed a security policy to block all USB devices, but someone wants to access it for genuine reason. How would an administrator give him an access without violating the current security policy? OTP delivers the answer for the same by generating one time password for a period of time like 10 minute or one hour for that specified user to disable the module without violating existing policy.

Working:

1. eScan Server Administrator defines a policy for a particular group blocking access to the USB ports through the web console. The USB access is blocked through the endpoint security module through Policies for Specific Computers.
2. For some specific reason, access to a USB port is required in one of the systems within a group where the security policy has been defined. The administrator is notified of this request manually.
3. The administrator generates a one-time password on the server and manually notifies the user who requires access to the USB port for a specific time period.
4. The user utilizes the one-time password within the group for accessing the USB port for the specified time period defined by the administrator. Other systems within the group cannot access the USB ports as the security policy is set for them thus ensuring that the group policy is not infringed.

How to Access

Use the following simple steps to access OTPass.EXE. **Refer Figure 10.8**

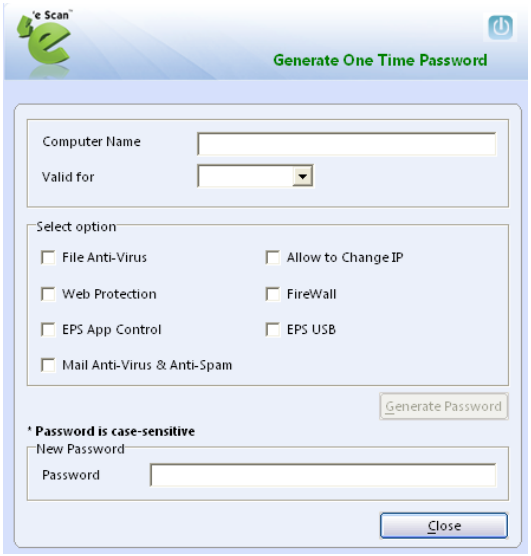


Figure 10.8

1. Open Windows Explorer.
2. Go to the path where eScan is installed.
3. Open eScan Folder.
4. Find and open OTPass.exe.
5. Now type the **Computer Name** for which you wish to generate the password in the respective field.
6. Select the time for which the password will be valid on the selected computer using the Valid for drop down present on the interface. **Refer Figure 10.9**

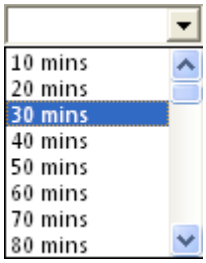


Figure 10.9

7. Select the Module that you wish to enable or disable usingcheck boxes present on the interface and click on Generate Passowrd button. **Refer Figure 10.10**

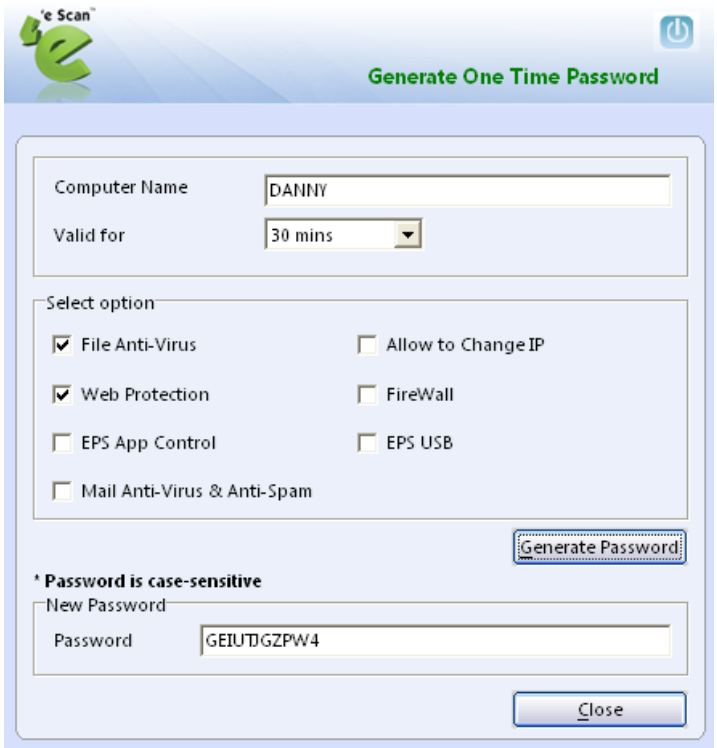


Figure 10.10

8. Send this password to the user.

9. To Pause the selected module on his computer, the user should open eScan Corporate 360 Client using right click on eScan Corporate 360 for Windows icon and click Pause Protection from the task bar. Refer **Figure 10.11**

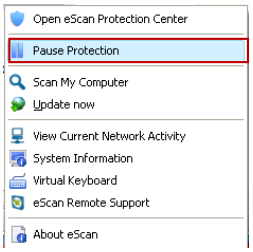


Figure 10.11

11.Managing and Scheduling Reports

eScan Management console provides you with predefined templates based on eScan modules. It provides you an option to create custom reports based on certain criteria.

The eScan Web Console comes with comprehensive reporting capabilities for viewing the status of the modules, scheduled tasks, and events. It allows you to view predefined reports, create new reports based on predefined reports, and customize existing reports for computers or for a group of computers.

- **Scheduling an existing Report Template**

1. Click **Reports Template** in the navigation bar and select the desired Template.
2. Click **Create schedule**. Refer **Figure 11.1**

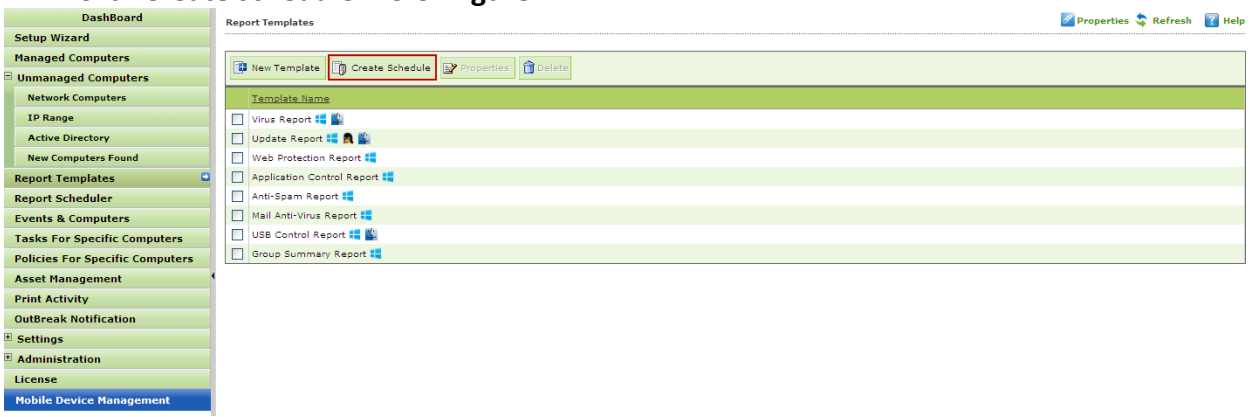


Figure 11.1

3. Now define the **Report Name** and filter the criteria for generating report by expanding the tree. Refer **Figure 11.2**

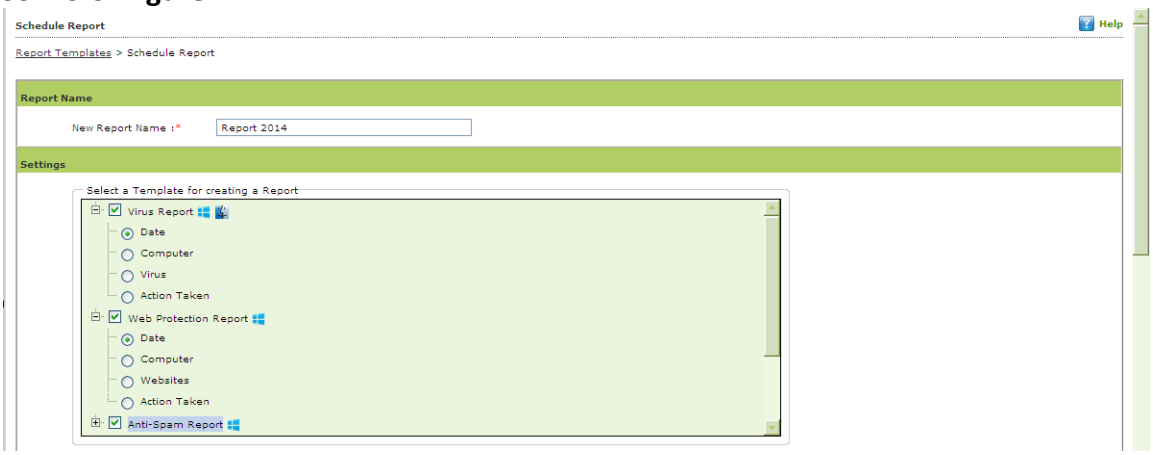


Figure 11.2

4. Select the **Conditions** and **Target Groups** for generating Reports. Refer **Figure 11.3.**

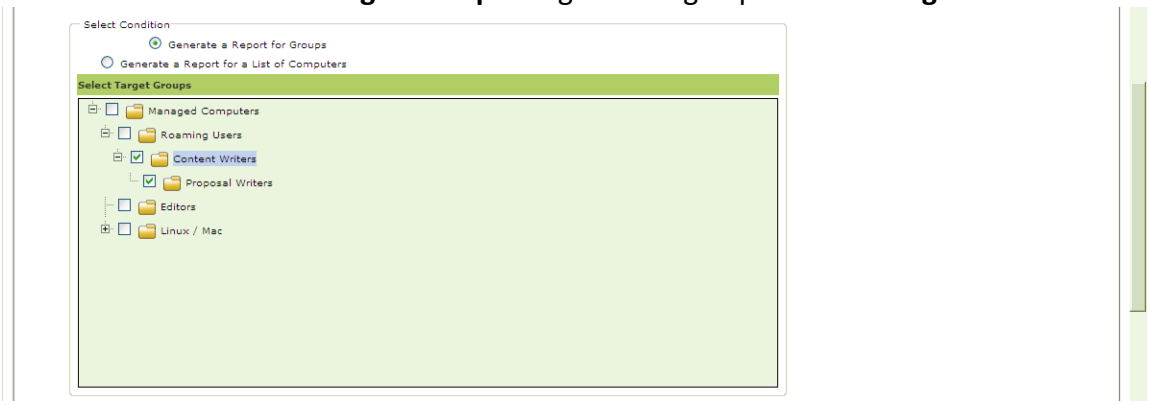


Figure 11.3

5. Define email and Server settings for sending reports by mail, also select the Format for the report, you can generate report in html, CSV,PDF and Excel formats, as required by you.

6. Schedule the report as desired and click **OK.** Refer **Figure 11.5**

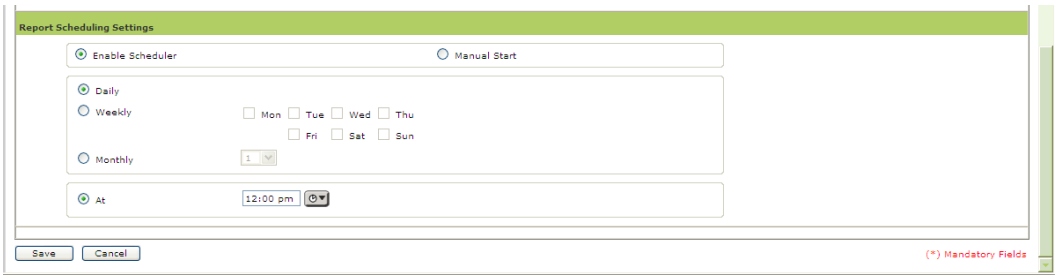


Figure 11.5

7. Report will be created and scheduled instantly. Refer **Figure 11.6**

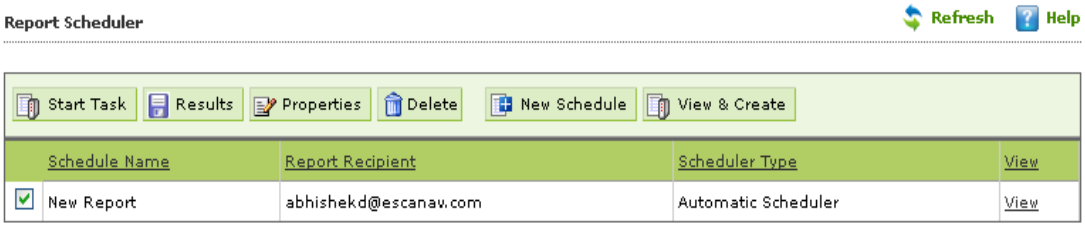


Figure 11.6

Note:
• Options to create and schedule reports are also present in Report Scheduler section of **eScan Management Console.**

12. Viewing Events

eScan Management Console maintains the record of all the event sent by the client computer. Through events & computers tab Administrator can monitor the Events; Computer Selection gives an option to sort the computer with specific properties.

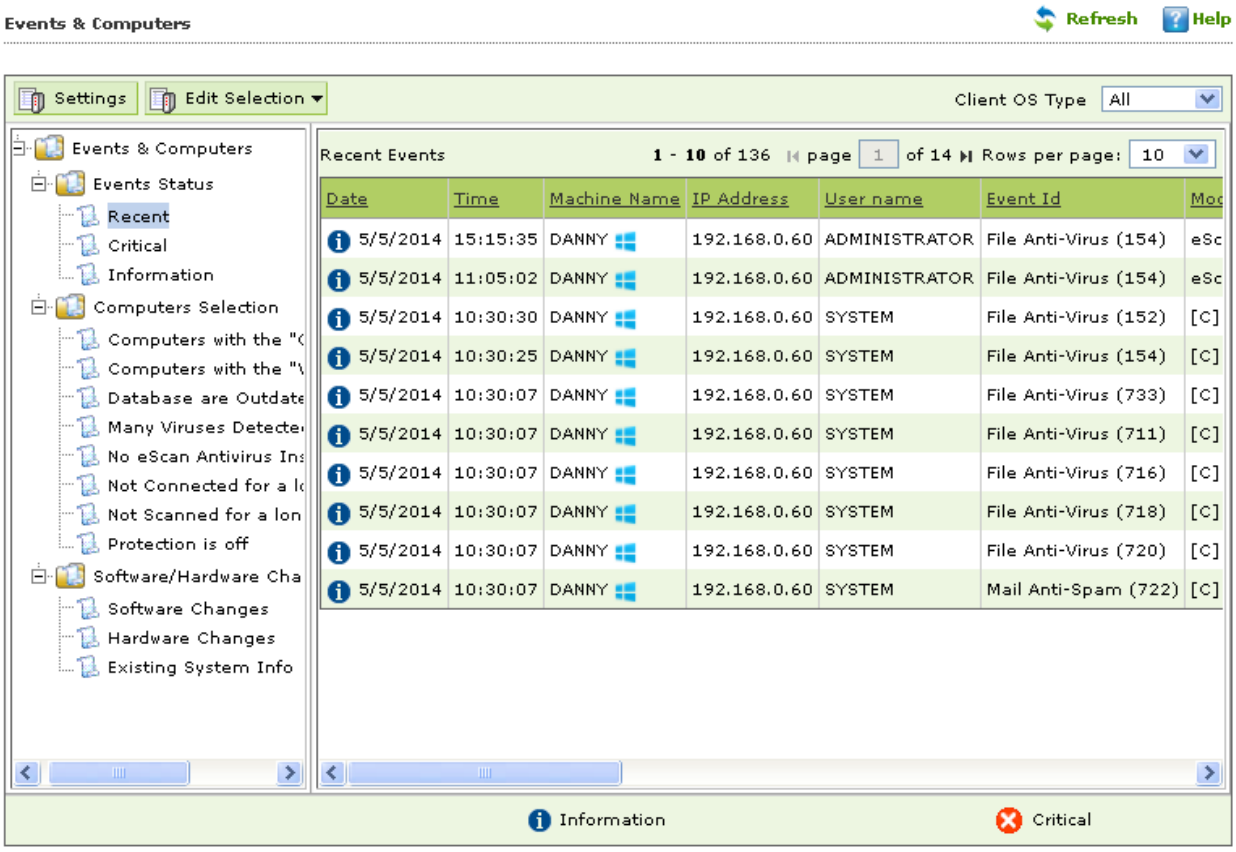


Figure 12.1

- **Event Status**

Status	Description
Recent	Recent events that are either critical or normal
Critical	Shows recent critical events like virus detection, monitor disable etc.
Information	It will show all the informative events like virus database update, status.

- **Computer Selection**

  You can use this node to sort out computers with specific properties, such as outdated databases, critical status, warning status or many virus detected. It allows you to select the computer and take action accordingly. You can also set the criteria for each node in computer selection accordingly by which you can sort the computer.

Node Name	Description
Computer with critical status	This node records all the system that has critical status.
Computer with warning status	This node will show all the system with warning status.
Database is outdated	This node will have all the system whose virus database is older/ outdated.
Many Viruses Detected	When the virus count will exceeds the specified limit that system will fall in this node.
No eScan Installed	Computers where eScan client is not installed will be shown in this node
Not connected for a long time	This node will have the systems that are not connected to the server (status can't be taken by the server) for a long time.
Not scanned for a long time	This node will show all the systems which are not scanned from a long time (specified time).
Protection is off	The system whose File Protection is disabled will fall under this node. We can specify the option by which Protection status will be checked.

- **Software/Hardware Changes**

  This node displays all the records for the software/ hardware changes.

  - **Software Changes:-** This node displays the records of the software changes that happen on the system i.e. installation/uninstallation or upgrade of software.
  - **Hardware Changes: -** This node displays the records of hardware changes of a computer like IP address change or any other hardware change.
  - **Existing system Info. : -** Under this node, record regarding the existing hardware information is displayed.

- **Defining Settings**

  You can define the Settings for Events, Computer Selection and Software / Hardware changes by clicking on the settings option and defining the desired settings using the Tabs and options present on the Events and Computer settings window.

A. Event Status

Basically, events are activities performed on client's computer. There are three types of event status – Recent, Critical, and Information. You can select the status as per your requirement.

- **Events Name**

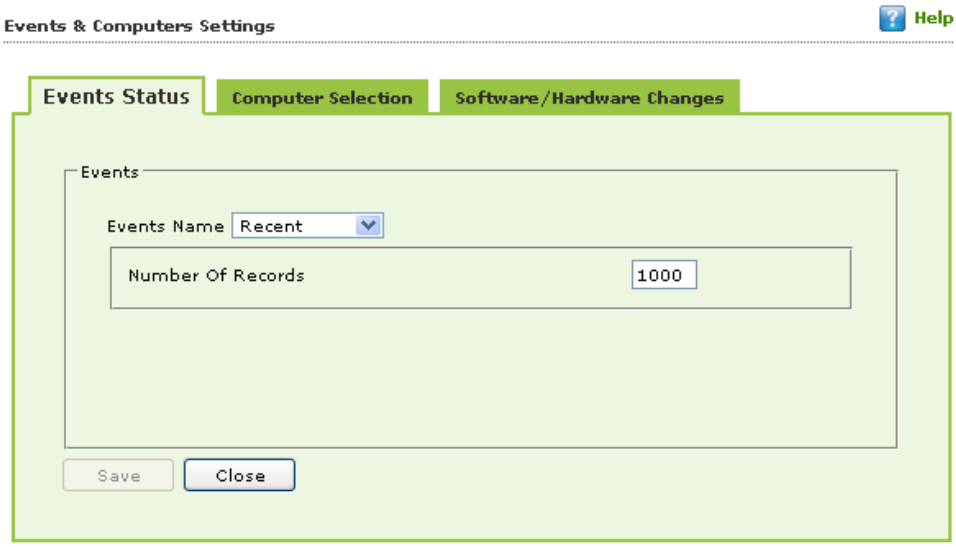


Figure 12.2

On the basis of severity, that is, the level of importance, events are categorized in to the following three types:

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Critical:** It displays all critical events occurred on managed client computers, such as virus detection, monitor disabled status, and so on.
- **Information:** It displays all informative type of events, such as virus database update, status, and so on.

Saving event status settings

Perform the following steps to save the event status settings:

1. Type the number of events that you want to view in a list, in the Number of Records field.
2. Click the Save button.

The settings get saved.

B. Computer Selection

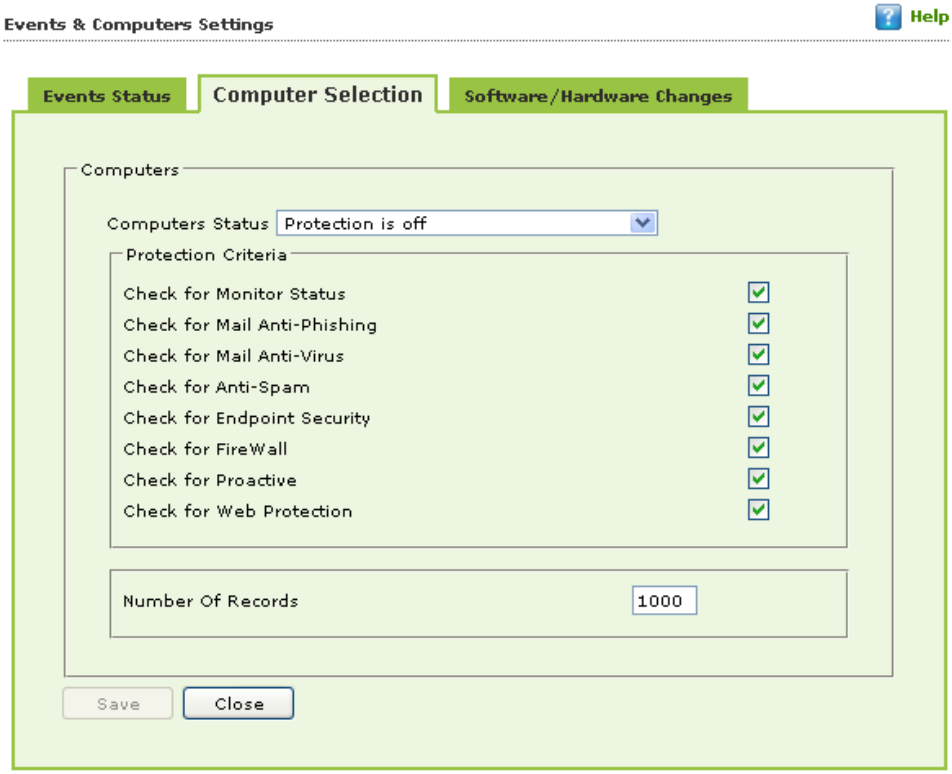


Figure 12.3

The **Computer Selection** enables you to select and save the computer status settings. This module enables you to do the following activities:

- **Computers**
    - Types and criteria's of **Computer Status**

1. Computers with the "Critical Status"
2. Computers with the "Warning Status"
3. Database are Outdated
4. Many viruses Detected
5. No eScan Antivirus Installed
6. Not connected to the eScan server for a long time
7. Not scanned for a long time
8. Protection is off

1. **Computers with the "Critical Status":** It displays the list of systems which are critical in status, as per the criteria\'s selected in computer settings. Specify the following field details.

Field	Description
Check for eScan Not Installed	Select this check box if you want to view the list of client systems under managed computers on which eScan has not been installed.
Check for Monitor Status	Select this check box if you want to view the client systems on which eScan monitor is not enabled.
Check for Not Scanned	Select this check box if you want to view the list of client systems which has not been scanned.
Check for Database Not Updated	Select this check box if you want to view the list of client systems on which database has not been updated.
Check for Not Connected	Select this check box if you want to view the list of eScan client systems that have not been communicated with eScan server.
Database Not Updated from more than	Type the number of days from when the database has not been updated.
System Not Scanned for more than	Type the number of days from when the system has not been scanned.
System Not Connected for more than	Type the number of days from when the client system has not been connected to eScan server.
Number Of Records	Type the number of client systems that you want to view in the list.

2. **Computers with the "Warning Status":** It displays the list of systems which are warning in status, as per the criteria\'s selected in computer settings. Specify the following field details.

Field	Description
Check for Not Scanned	Select this check box if you want to view the list of client systems which has not been scanned.
Check for Database Not Updated	Select this check box if you want to view the list of client systems on which database has not been updated.
Check for Not Connected	Select this check box if you want to view the list of eScan client systems that have not been communicated with eScan server.
Check for Protection off	Select this check box if you want to view the list of client systems on which protection for any module is inactive, that is disabled.
Check for Many Viruses	Select this check box if you want to view the list of client systems on which maximum viruses are detected.
Database Not Updated from more than	Type the number of days from when the database has not been updated.
System Not Scanned for more than	Type the number of days from when the system has not been scanned.
System Not Connected for more than	Type the number of days from when the client system has not been connected to eScan server.
Number Of Virus	Type the number of viruses detected on client system.
Number Of Records	Type the number of client system that you want to view in the list.

3. **Database are Outdated:** It displays the list of systems on which virus database is outdated. Specify the following field details.

Field	Description
Database Not Updated from more than	Type the number of days from when the database has not been updated.
Number Of Records	Type the number of client system that you want to view in the list.

4. **Many viruses Detected:** It displays the list of systems on which number of viruses exceeds the specified count in computer settings. Specify the following field details.

Field	Description
Number Of Virus	Type the number of viruses detected on client system.
Number Of Records	Type the number of client system that you want to view in the list.

5. **No eScan Antivirus Installed:** It displays the list of systems on which eScan has not been installed. Specify the following field detail.

Field	Description
Number Of Records	Type the number of client system that you want to view in the list.

6. **Not connected to the eScan server for a long time:** It displays the list of systems which have not been connected to the server from a long time. Specify the following field detail.

Field	Description
Number Of Records	Type the number of client system that you want to view in the list.

7. **Not scanned for a long time:** It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Specify the following field details.

Field	Description
System Not Scanned for more than	Type the number of days from when the system has not been scanned.
Number Of Records	Type the number of client system that you want to view in the list.

8. **Protection is off:** It displays the list of systems on which protection is inactive for any module, as per the protection criteria\'s selected in computer settings. It shows the status as "Disabled" in the list. Specify the following field details.

Protection Criteria	
Check for Monitor Status	Select this check box if you want to view the client systems on which eScan monitor is not enabled.
Check for Mail Anti-Phishing	Select this check box if you want to view the list of client systems on which **Mail Anti-Phishing** protection is inactive, that is disabled.
Check for Mail Anti-Virus	Select this check box if you want to view the list of client systems on which **Mail Anti-Virus** protection is inactive, that is disabled.
Check for Mail Anti-Spam	Select this check box if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive, that is disabled.
Check for Endpoint Security	Select this check box if you want to view the list of client systems on which **Endpoint Security** protection is inactive, that is disabled.
Check for Firewall	Select this check box if you want to view the list of client systems on which **Firewall** protection is inactive, that is disabled.
Check for Proactive	Select this check box if you want to view the list of client systems on which **Proactive** protection is inactive, that is disabled.
Check for Web Protection	Select this check box if you want to view the list of client systems on which protection of **Web Protection** module is inactive, that is disabled.
Number Of Records	Type the number of client system that you want to view in the list.

Saving computer settings

Perform the following steps to save the computer settings:

1. Click the **Computers Selection** tab.
2. Select type of status for which you want to set criteria, from the **Computer status** drop-down list.

3. Select the appropriate check boxes, and then type field details in the available fields. For more information, refer [Types and criteria's of computer status-] section.
4. Click the '***Save'*** button.

The settings get saved.

C. Software/ Hardware Changes

You can set these settings, if you want to get updates on any changes made in the software, hardware, and to existing system. The **Software/ Hardware Changes** enable you to do the following activities:

- **Updates**
  - Type of **Updates**

1. Software changes
2. Hardware changes
3. Existing system info

Changing software/hardware settings

Perform the following steps to change the **Software / Hardware Settings**:

1. Click the **Software/Hardware Changes** tab.
2. Specify the following field details.

Field	Description
Software/Hardware Changes	Select the type of update made in the system from the drop-down list.
Number of Days	Type the number of days, to view changes made within the specified days.
Number of Records	Type the number of client systems that you want to view in the list.

Note:- Example of **Number of Days**, if you have typed 2 days, then you can view the list of client systems on which any software/hardware changes have been made in the last 2 days.

3. Click the '***Save'*** button.
   The settings get saved.

13. Asset Management

This module provides you the entire Hardware configuration and list of softwares installed on Managed Computers in a tabular format. Using this Module, you can easily keep a track of all the Hardware as well as Software resources installed on all the Managed Computers connected to the Network. Based on different Search criteria you can easily filter the information as per your requirement. It also allows you to Export the entire system information available through this module in PDF, Ms Excel or HTML formats.

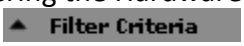
- **Viewing Hardware Reports**

  For Viewing the Hardware Configuration of all the Managed Computers connected to the Network, Click on the Asset Management section present in the Navigation Panel on the Left in the eScan eScan Management Console. Following Information will populate in the table on the right.

S.No.	Column Name	Description
1.	**Computer Name**	It displays the Host Name of the Computers as defined by the Administrator.
2.	**Group**	It displays the Name of the Group to which that Computer belongs to, as defined in Managed Computer section of eScan Management Console.
3.	**IP Address**	It displays the IP address of the Endpoints.
4.	**User Name**	It displays the current Username of the Endpoints (who is logged on the system).
5.	**Operating System**	It displays the Operating system installed on the Endpoints.
6.	**Service Pack**	It displays the Service Pack version and build installed on the Endpoints.
7.	**OS Version**	It displays the version of the Operating system installed in the Endpoints.

8.	**OS Installed Date**	It displays the Date and Time of Installation of the Operating system on the Endpoints.
9.	**Internet Explorer**	It displays the version of internet explorer installed on the Endpoints.
10.	**Processor**	It displays the Processor details like Processor Name, Type and Processing Speed of the Endpoints.
11.	**Motherboard**	It displays the details of the motherboard of the Endpoints.
12.	**RAM**	It displays the details of the RAM installed on the Endpoints.
13.	**HDD**	It displays the details of the Hard Disk like number of Partitions and their respective sizes.
14.	**MAC Address**	It displays the MAC Address of the Endpoints.
15.	**Software**	By clicking on the view link present in this Column, you can view the list of softwares along with the installation dates on the Managed Computer.
The status is displayed for the computers having operating system as  **Windows,**  **Macintosh** or  **Linux**		

By clicking on the **View** link present in **Software** Column, you can view the list of Software along with the installation dates on the Endpoints.

For Filtering the Hardware Report as per your requirements, click on the drop Menu Link of Filter Criteria 

in **Asset Management** section. The Hardware report can be filtered on the basis of following Criteria. Refer **Figure 13.1**

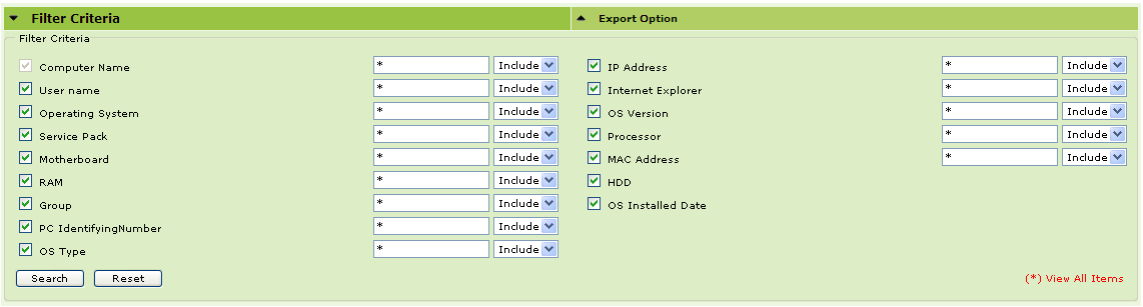


Figure 13.1

Note:
• You can define criteria for the text / Column Content to be included or excluded in your Search result using the drop downs present on the interface.

- **Viewing the Software Report**

This section displays list of Software along with the number of Endpoints on which they are installed. To view the Software Report, click Asset Management and then Click Software Report Tab present on the right. This will populate the Software Name with Computer Count in a tabular format.

For knowing the Computer Details where specific Software is installed, click on the Computer Count present in the Computer Count Column. A window with the respective Computer Details will pop up.

For Filtering the Software Report as per your desire, click on the Drop Menu Link of Filter Criteria  in Asset Management Section. The Software report can be filtered on the basis of following Criteria.

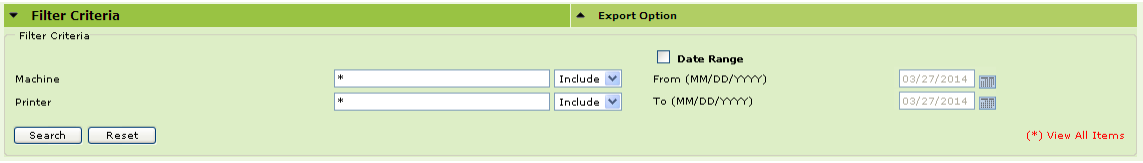


Figure 13.2

You can filter your search on the basis of Software Name or the Computer Name, using the drop down present on the interface; you can either include the search string entered by you in your search or exclude it if desired. System will populate the results accordingly.

- **Export Options: Exporting the Hardware / Software Report**

eScan Management Consoles offers Exporting of Hardware Report in PDF, Excel or HTML formats.

It can easily be done by Clicking on Drop Menu Link of Export Option 

in **Asset Management** Section. It will display the following options.

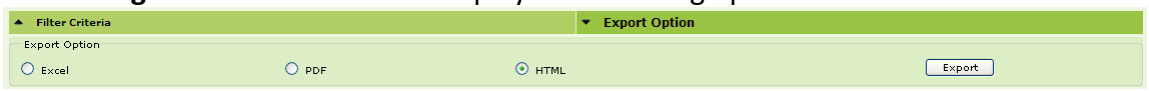


Figure 13.3

Click on the desired Radio button for exporting the report in available formats. When the Export is over, you will be informed with the following message –

Figure 13.4

For Opening/ Downloading the exported files click on the link as shown above.

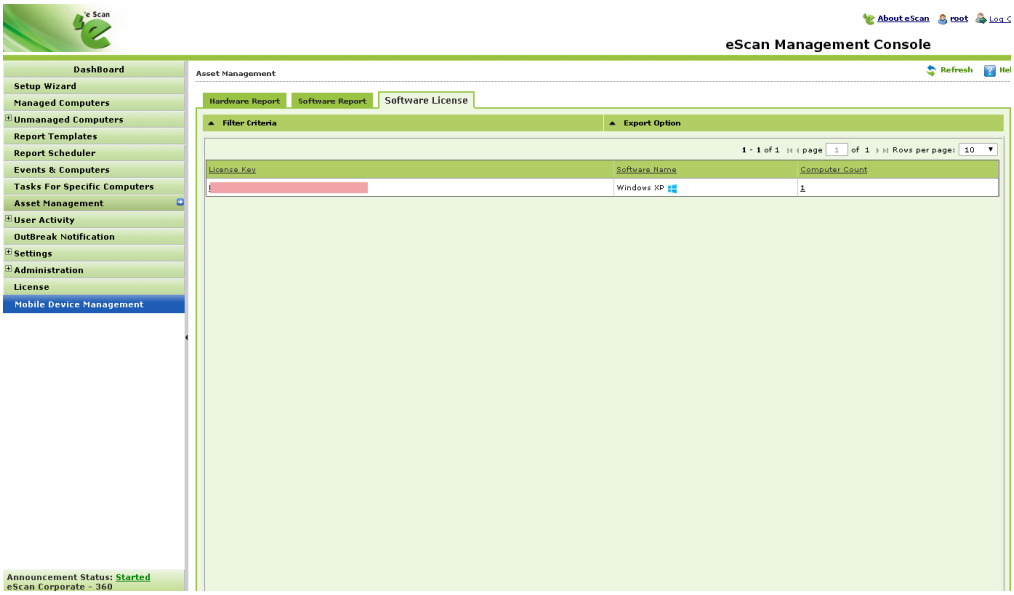


Figure 13.5

This option will display the License details of the Windows Operating System and Microsoft Office installed on the Client systems along with the computer count and the details of the system where it is installed.

- **Software Licensing**

The Software License option will display the License details of the Windows Operating System and Microsoft Office installed on the Client systems along with the computer count and the details of the system where it is installed.

14. User Activity

It will monitor the user activity such as the print activity and Remote session activity of managed computers and create a log of the activities. It monitors and logs printing tasks done by all the endpoints, it gives you a report of all Printing Jobs done by endpoints through any printer connected to the network.

It also gives you options for filtering the reports on the basis of excluding or including the computer/machine name or a printer within a desired date range, operation type, group and exporting the report in PDF, Excel or HTML formats.

- **Viewing the Print Activity Log**

  Click **Print Activity** under Dashboard on the left in eScan Management Console. A table with the List of Printers and number of copies printed by them will populate on left. Options for Filtering or Exporting the log in desired formats are also present on the same interface. Refer **Figure 14.1**

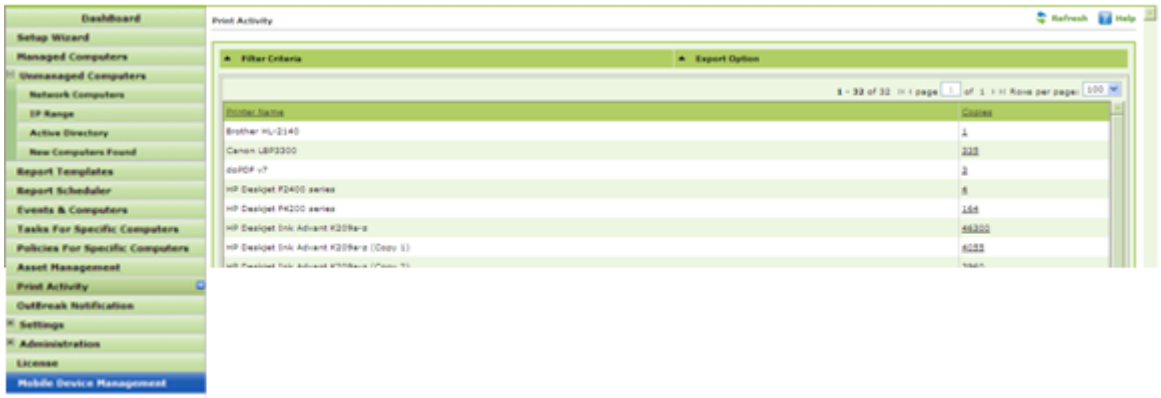


Figure 14.1

S.No.	Field Name	Description
1.	Client Date	It displays the Printing date of Client Machine
2.	Machine Name	It displays the name of the Machine from which the Prints were taken.
3.	IP Address	It displays the IP Address of the machine from where the Prints were taken.
4.	Username	It displays the Username of the Machine from where the Prints were taken.
5.	Document Name	It displays the document name that was printed.
6.	Copies	It displays the number of copies of the document that were printed.
7.	Pages	It displays the number of Pages that were printed.

This window also gives you option to Export the Log report generated on this widow in the desired formats, you can easily do so by selecting the desired export option using the Drop down present on the screen, and then click **Export**. After the Export is complete you will be informed through the following message.

Figure 14.3

Click on the link to open and save the converted file.

The log report generated in this section keeps the log of number of copies printed through any printer, the File name of the Printed file, the Date on which Print was taken (Client Machine), Machine Name, along with the Username of the computer and its IP address.

Filter Criteria

For Filtering the Print Activity Log as desired, click **Filter** Criteria on the main interface of Print Activity section, following options will be populated on screen. Refer **Figure 14.4**

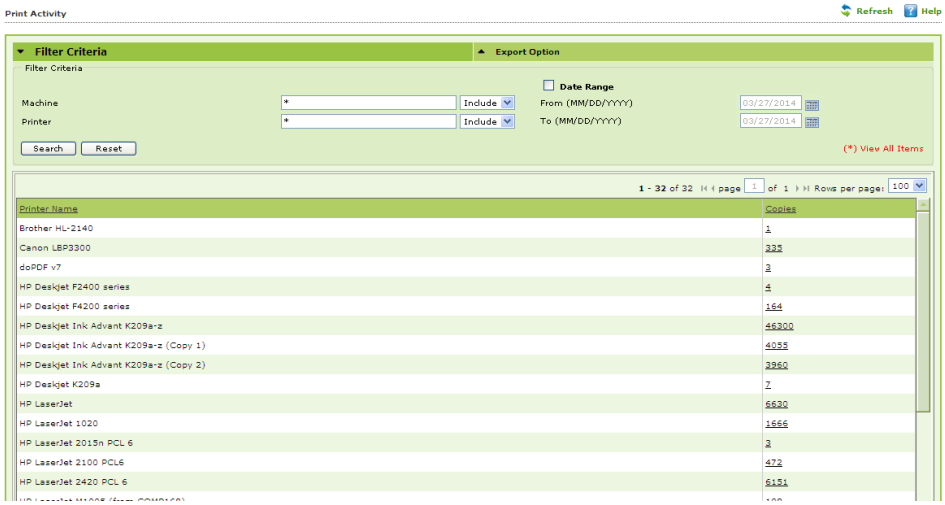


Figure 14.4

Sr. No.	Option	Description
1.	Machine	Type the desired machine name that you wish to exclude or include in your Log.
2.	Include	Select this to include the machines to the log report.
3.	Exclude	Select this to exclude the machines from the log report.
4.	Printer	Type the desired printer name that you wish to exclude or include in your log.
5.	Date Range	Tick on this checkbox, if you wish to generate report between certain dates.
6.	From((MM/DD/YYYY)	Select the starting date for report generation.
7.	To(MM/DD/YYYY)	Select the Ending date for report generation.
8.	Search	Click this option to Filter the Log on the defined criteria.
9.	Reset	Click this option to reset the defined criteria for filtering.

- **Exporting the Print Activity Log**

  eScan Management Console offers exporting of print activity logs in PDF, Excel or HTML formats.

  It can easily be done by clicking on drop menu link of export option 

 in print activity section. It will display the following options.

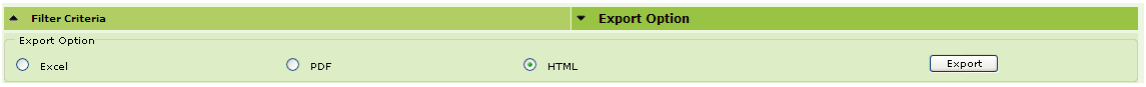


Figure 14.5

Click on the desired radio button for exporting the report in available formats. When the export is over, you will be informed with the following message –

Figure 14.6

For Opening/Viewing / Saving the exported files click on the link as shown above.

- **Session Activity Report**

  eScan Management Console monitors and logs the session activity of the managed computers. It will display a report of the endpoint startup/ shutdown/ logon/ log off/ remote session connects/ disconnects. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers. It will be helpful for audit compliance purposes. Additionally in case of a misuse of the computer at a specific time can be tracked down to the user through remote Logon details captured in the report.

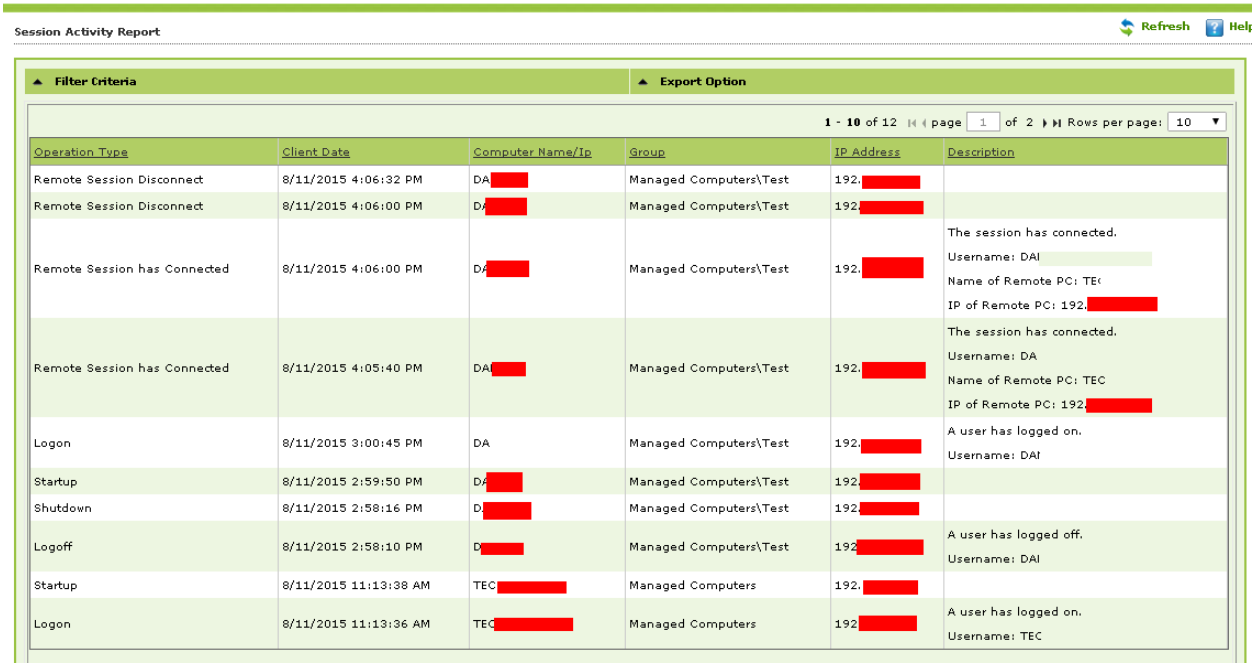


Figure 14.7

The log report generated in this section keeps the log of the operation type, computer name, group name, IP address and the description of the activity. It also gives you options for filtering the report on the basis of excluding or including the computer name, operation type, IP Address, Group, description and date range. It will also allow you to export the report in PDF, Excel or HTML formats.

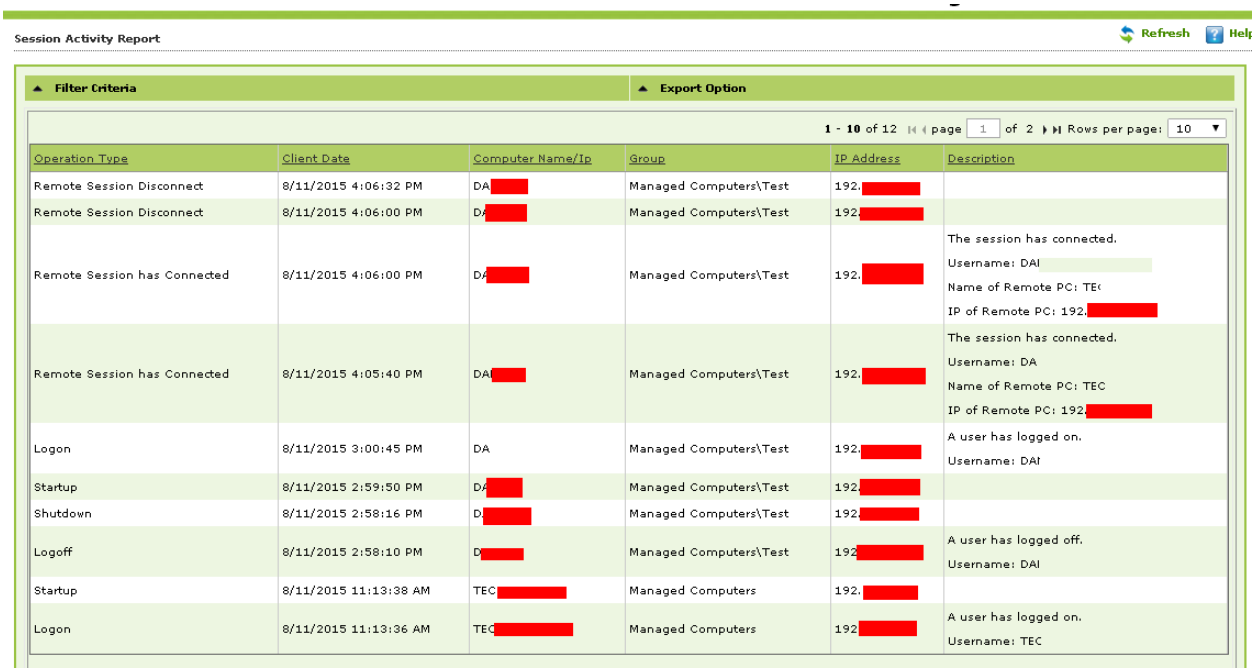


Figure 14.8

The log report generated in this section keeps the log of the operation type, client date, computer name id, group name, IP address and the description of the activity. It also gives you options for Filtering the report on the basis of excluding or including the computer name, operation type, IP address, Group, description and date range.

It also gives you options for filtering the report on the basis of excluding or including the machine name or a printer within a desired date range, and exporting the report in PDF, Excel or HTML formats.

15. Outbreak Notifications

You can configure settings for sending notification when Virus count exceeds the limit defined by you. It can be done using the following simple steps –

1. Click **Outbreak Notifications** in the Navigation panel of eScan Management Console.
2. Define the criteria for Outbreak Alert and Notification settings in the respective fields present on the interface and click **Save**. Refer **Figure 15.1**

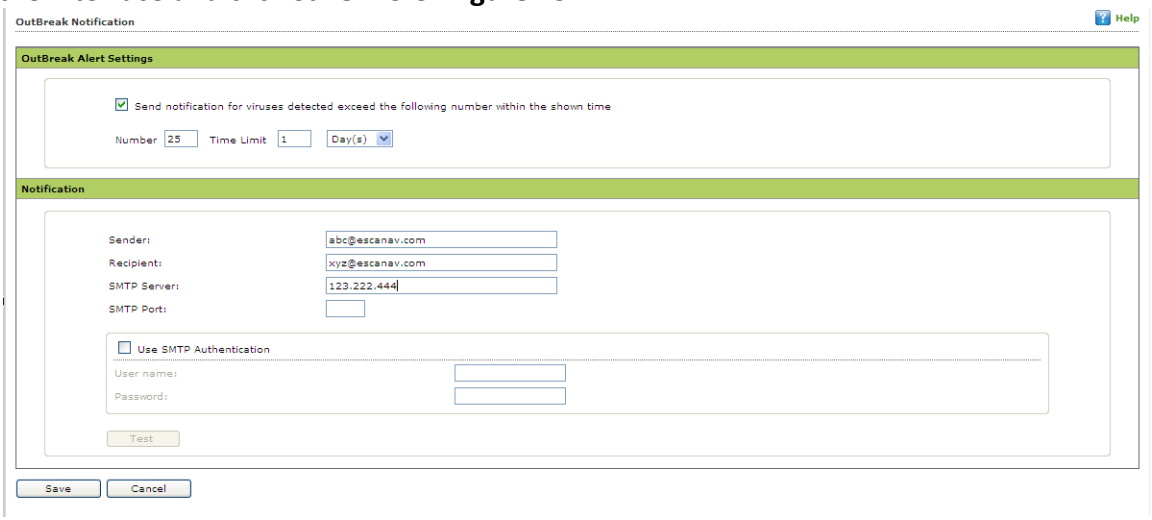


Figure 15.1

3. Settings will be saved and notification mails will be sent to the defined recipients whenever the Virus count exceeds the defined Limit.

16. Defining Settings

Using this section you can define important settings for the following

1. **eScan Management Console (EMC)** - Using this section you can define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.

2. **Web Console Settings** - Using this section you can define settings for Web Console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.

3. **Update Settings** - Using this section you can define general configuration settings for, Settings for Update Notifications, and scheduling Update Downloads for the server.

16.1. eScan Management Console Settings

The **EMC Settings** page includes several options that allow you to configure the eScan Management Console. You can configure the FTP settings, Bind to IP Settings, and log settings by selecting the options appropriate for your network.

You can bind announcement of FTP Server to particular IP by selecting the IP address in the list. However, you can choose to leave it as 0.0.0.0, which mean it will announce on all available interface/IP.

You can also enable FTP settings such as allowing upload of log file to eScan Server by Endpoints by selecting the **Allow Upload by Clients** check box. If you are doing that, you can set a limit for the maximum number of FTP sessions allowed. If you specify this number as 0, it means that any number of Endpoints can connect to FTP server for uploading files.

By checking **Delete the user settings and user log files after uninstalling** check box you can opt to delete User settings and Log files once eScan Client is uninstalled on that computer. You can also define the number of days for which Log should be maintained by defining the days in the field for **No of days Client logs should be kept**. Refer **Figure 16.1**

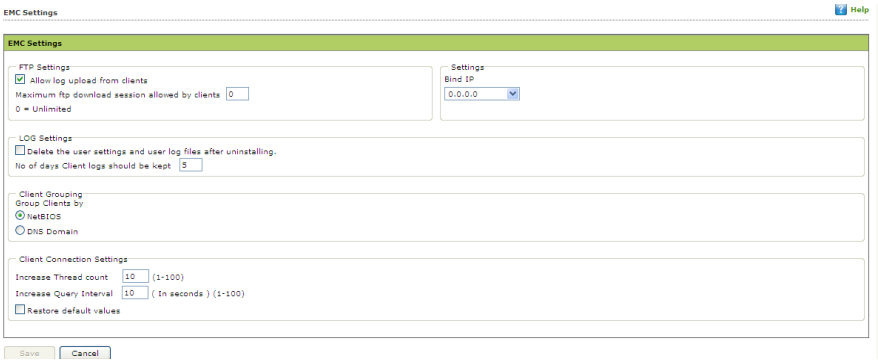


Figure 16.1

The **steps** to configure the EMC settings are as follows:

To configure the Bind IP address, under BIND IP, in the box, click the required IP address. The default IP address is 0.0.0.0.
To allow uploads by Endpoints, under FTP Settings, select the Allow Upload by Clients check box.
To restrict the maximum number of FTP connections, in the Maximum FTP Clients allowed box, type or select the maximum number of FTP Connections to be allowed. The default value is 0; this allows an unlimited number of FTP connections.
To specify the number of days for which EMC should maintain client computer logs, under LOG Settings, in the no. of days Client logs should be kept box, type or select the number of days.
Under Client Grouping section, you can sort group clients either by NetBIOS or DNS domain. This setting is especially useful only during fresh client installations. After installation, it enables you to manually manage domains and the clients grouped under them.

- Click **NetBIOS**, if you want to sort clients only by hostname.
- Click **DNS** Domain, if you want to sort clients by hostname containing the domain name.
- Click **Save** button implement the defined settings.

16.2. Web Console settings

Using this section you can define settings for **Web Console timeout**, **Dashboard Settings**, **Login Page settings**, **SQL Server Connection** settings, **SQL Database compression** settings.

1. **Web Console timeout settings -** Select the Enable timeout settings option and define the time to automatically Log out Web Console when idle beyond the defined minutes.

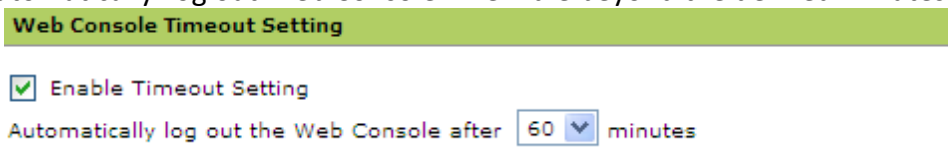


Figure 16.2

2. **Dashboard Settings** - Define the number of Days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard of eScan Management Console.

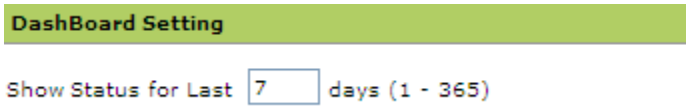


Figure 16.3

3. **Login page Settings -** Define the settings to show or Hide Link for downloading eScan Client and MWAgent to facilitate manual download and installation on Endpoints.

4. **SQL Server Connection settings –** Select the SQL server and define Server instance, and Host Name along with the credentials for connecting to the database.

5. **SQL Database Purge Settings** - Define the size Limit for the database as well as specify the number of days to compress the Database folder if it is older than the defined period.

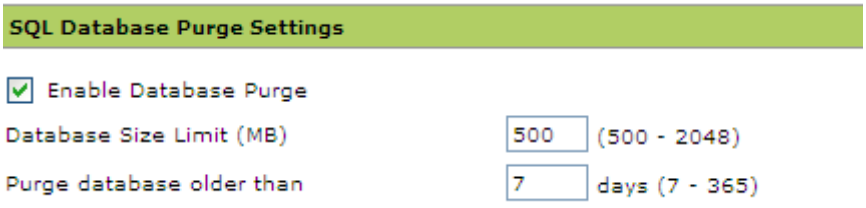


Figure 16.4

Click **Save** to save the defined settings

16.3. Update Settings

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 the local network by using FTP or HTTP.
You can access the update settings page from the navigation Panel. This page provides you with information regarding the mode of update. It also provides you with options for configuring the module. It also helps the Update module to download updates automatically.

1. **General Config** - The **General Config** tab provides you with general options for configuring the update module. These include selecting the mode, and configuring the proxy and network settings.

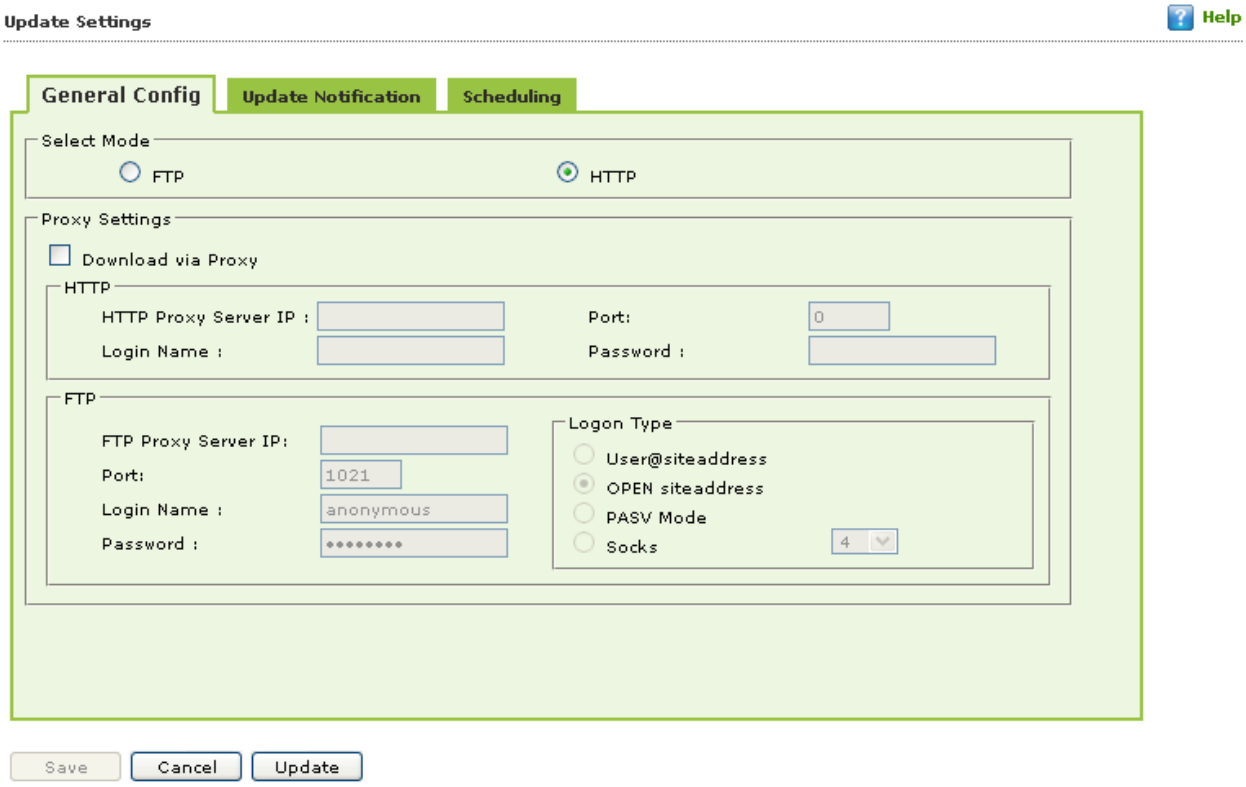


Figure 16.5

You can configure eScan to download updates from eScan update servers by using any of the available modes such as **FTP**, **HTTP**, and **Network**. If you are using HTTP or FTP proxy servers, you need to configure the proxy settings and provide the IP address of the server, the port number, and the authentication credentials of the proxy server. In case of FTP servers, you also need to provide the format for the user id in the **Logon Type** section.

You can also select the Network mode for downloading updates. However, to do this, you must specify the source UNC path in the **Source UNC Path** box.

2. **Update Notification** - The **Update Notification** tab helps you to configure the actions that eScan should perform after updater downloads the eScan updates.

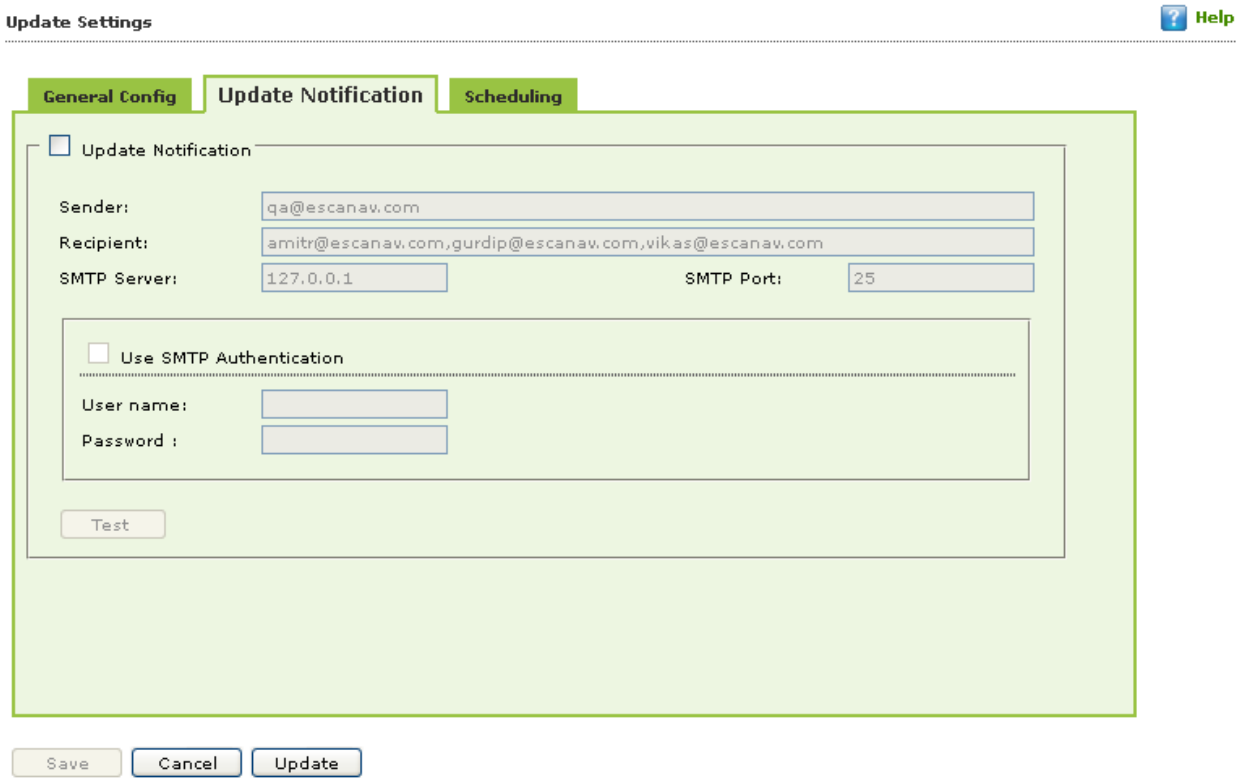


Figure 16.6

You can configure eScan to send an e-mail notification to a specified e-mail address from a specified e-mail address after successful update. To use this feature, you must also specify the IP address of SMTP server and its port number

3. **Scheduling -** The eScan Scheduler automatically checks eScan Web site for updates and downloads the latest updates when they are available. It also allows you to schedule downloads to occur on specific days or at a specific time.

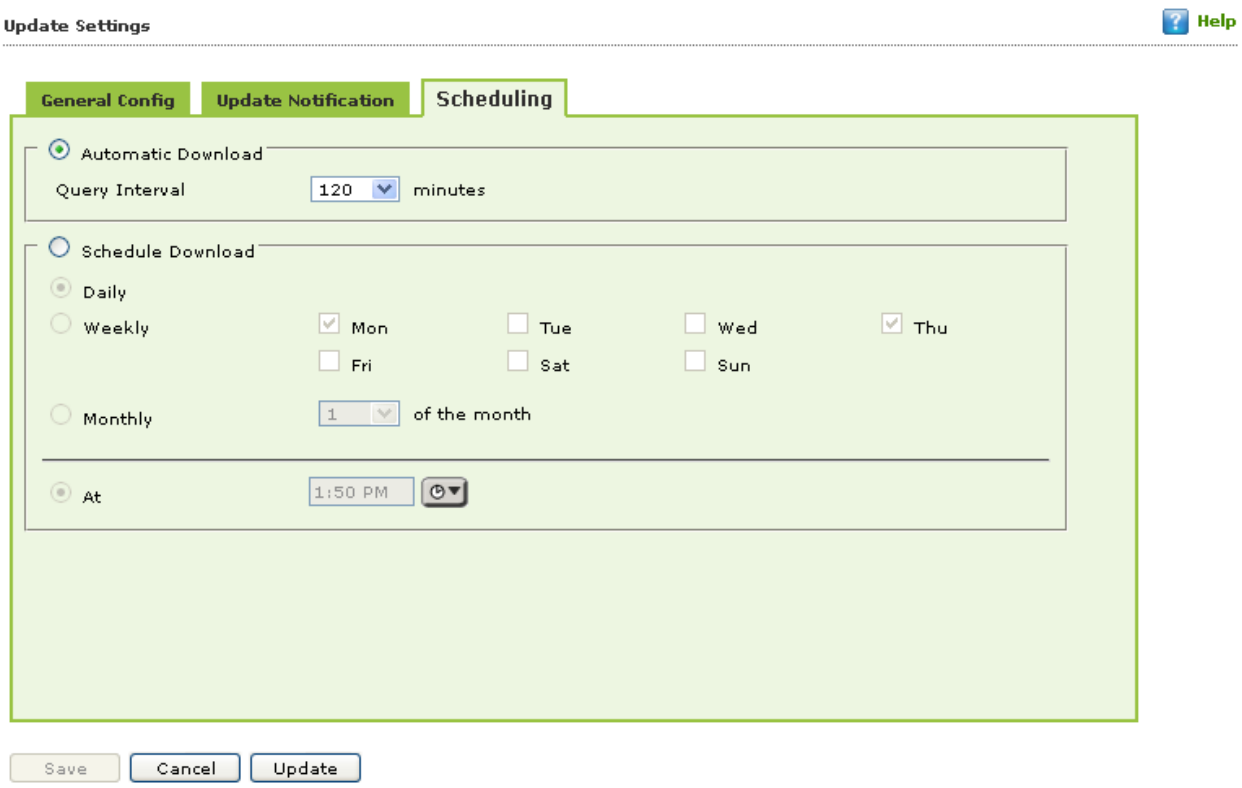


Figure 16.7

You can configure the update module to query and download the latest updates automatically from the MicroWorld Web site by selecting **Automatic Download**. In this case, you may want to specify a query interval after which eScan should query the Web site for latest updates. The default interval is **120** minutes, but you can choose an interval from the **Query Interval** list.

You can also schedule downloads to occur on specific days or on a daily, weekly, or monthly basis and at a specific time. When you configure this setting, the scheduler checks the eScan server for latest updates on the specified day at the specified time and downloads them if they are available.

16.4. Auto Grouping

This will allow you to define the settings to automatically add clients under desired sub groups. The administrator will have to Add Groups and also add client criteria under these groups based on host/host name with wild card/IP address/ IP range.

Advantages of Auto Grouping

1. On Auto Grouping, the clients will be automatically added to the specified managed groups.

2. The clients can be added or removed from Auto Grouping with ease.

It contains the following section:

Group and client selection criteria for Auto adding under Managed Group(s)

How to configure Auto Grouping?

1. Enter the group name and click **Add**.
2. Enter the client criteria and click **Add**, you can add host names, **host names with wildcard**; IP address and IP address range.

For example:

Groups	**Client Criteria**
Group A	**Host names** (Comp101, Comp201)
Group B	**Host names with wild card** (Comp1*)
Group B	**IP Addresses** (162.0.34. 1, 162.0. 55.6, 163. 1. 70.10)
Group C	**IP Address range** (162.15. 30 – 162. 15. 82)

The above example displays the Groups and the client criteria for Auto Grouping into the desired group.

3. Click **Save**. This will save the settings and the **Run** button will be enabled.
4. Click **Run** to start the auto grouping process, this will move the client systems to the desired groups.

A new window will pop up displaying the Auto Grouping process. Close the window once the Auto Grouping process is finished.

Client(s) list excluded from Auto adding under Managed Group(s)

- Enter the client criteria such as host name, host name with wild card, IP address and also by IP range.
- The clients added to this list will be excluded from auto adding under Managed Groups.

17. Managing User Accounts

Using this section you can create User Accounts and allocate those admin rights for using eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. Using this option you can allocate rights to the users on the selected computer group which will allow them to install eScan Client and implement Policies and tasks on other computers.

Perform the following steps to create an account for the local user.

1. On the navigation pane, under **Administration**, click **User Accounts**.
   Refer **Figure - 17.1**

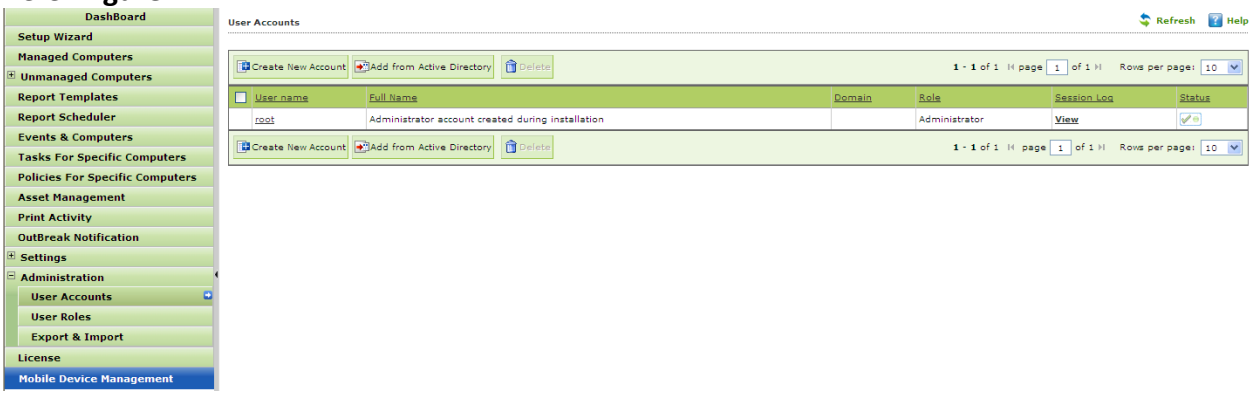


Figure - 17.1

2. Click **Create New Account** button and specify the following fields –

-

Field	Description
Account type and information	
User name*:	Type the user name.
Full Name*:	Type the full name.
Password*:	Type the password.
Confirm Password*:	Re-type the password for confirmation.
Email Address:	Type the e-mail address.
Account Role	
Role*:	Select an appropriate role that you want to assign to the user from the drop-down list.

3. Now Click **Save**.

- **Creating a Role**

Using this section you can create a role and assign it to the User Accounts with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights or Group Admin Role or a Read only Role.

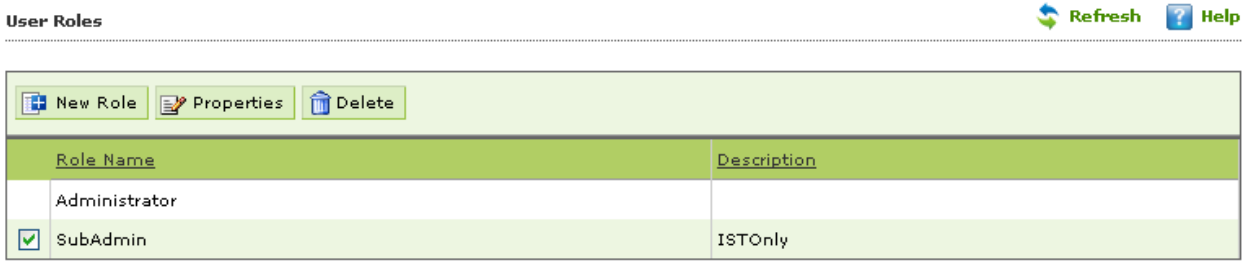


Figure - 17.2

You can re-define the **Properties** of the created role for configuring access to various section of eScan Management Console and the networked Computers.

It allows you to delete any existing role once the task is completed by them.

It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation / uninstallation of eScan Client on network computers or define Policies and tasks for the computers allocated to them.

Creating a New Role

Role based Administration through eScan Management Console enables you to share the configuration and monitoring responsibilities for your organization among several administrators. Using this feature one or more senior administrator can have full configuration privileges for all computers while one or more junior administrators can have less configuring and monitoring authority over group of computers allocated to them. You can assign administrators with pre-defined roles, each with its own set of rights, permissions and groups.
eScan Management Console provide administrators with a streamlined view that is customized to their specific role—showing only what they need to do their job .It is helpful in large organizations where installing and managing eScan client on large number of computers in the organization may consume lot of time and efforts. Using this option you can allocate rights to other administrators to manage selected computer group which will allow them to install eScan and implement Policies and tasks on computers, it also allows them to view eScan reports of the computers in their respective groups. eScan allows you to create Group Administrators with variable rights to manage computers in their group. These rights may include a read only right to access eScan Management

Console and Policies and Tasks implemented on Endpoints or Read and Configure Policies and tasks as defined by you.

Group Admin Role – A Group Admin has rights on a group of computers allocated to them. They can define Policies, schedule tasks and access Sections of eScan Management Console to deploy and manage eScan

Read only Admin Role - A Read only Admin has rights on a group of computers allocated to them only to view defined Policies and scheduled tasks. They cannot modify or configure them. They also have right to view permitted sections of eScan Management Console.

Steps for Creating a New Role

1. Go to User Roles present under Administration and click **New Role** on the interface.

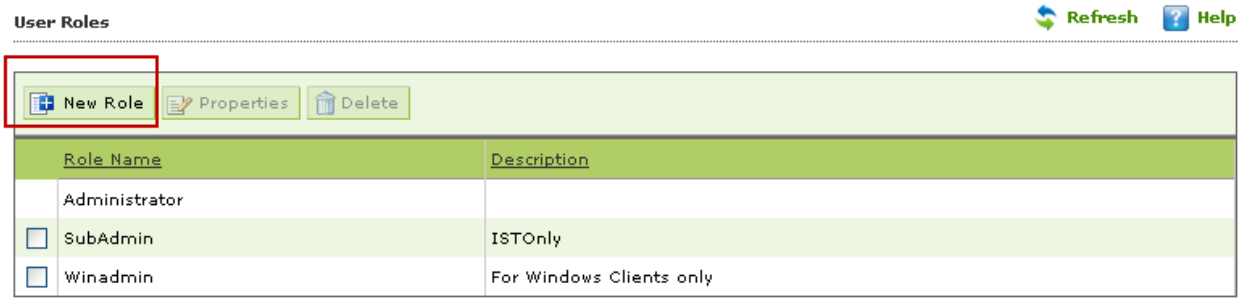


Figure - 17.3

2. Define the **Role Details,** and select the Group that the created Admin will manage and click **OK**.

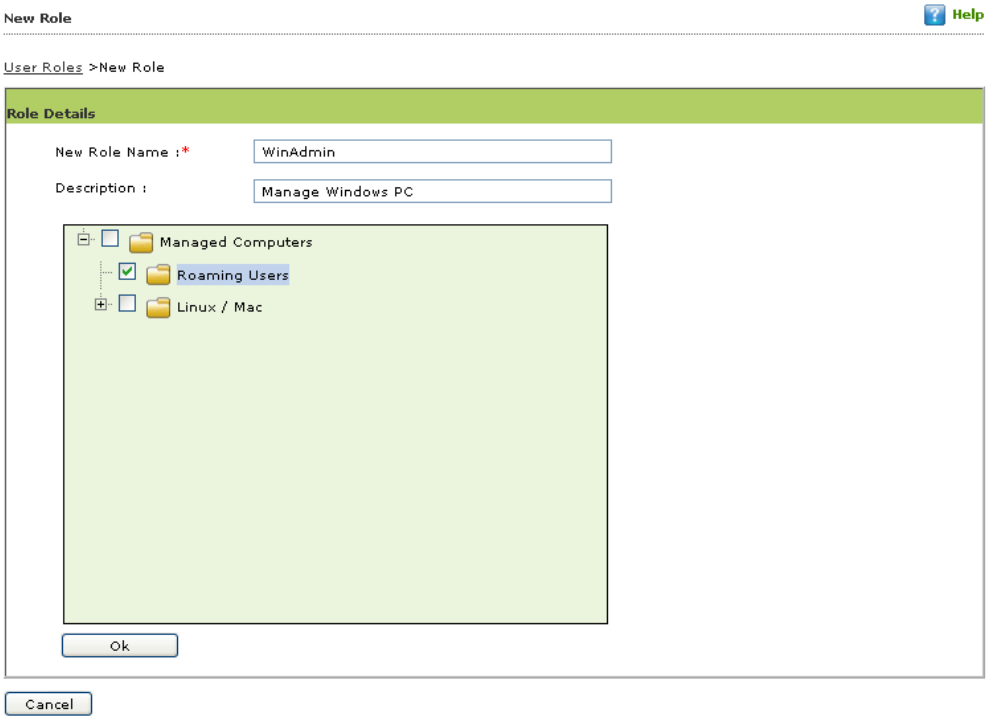


Figure - 17.4

3. You will be forwarded to the **Permissions** Window. Configure the desired settings using the Main Tree Menu and Client Tree Menu tabs.

   - **Main Tree Menu –** It allows you to give permission to the created admin role to **View** or **Configure** settings through eScan Management Console. He will have either **View Rights** or **Configure Rights** over the settings that can be configured through modules of eScan Management Console**.**

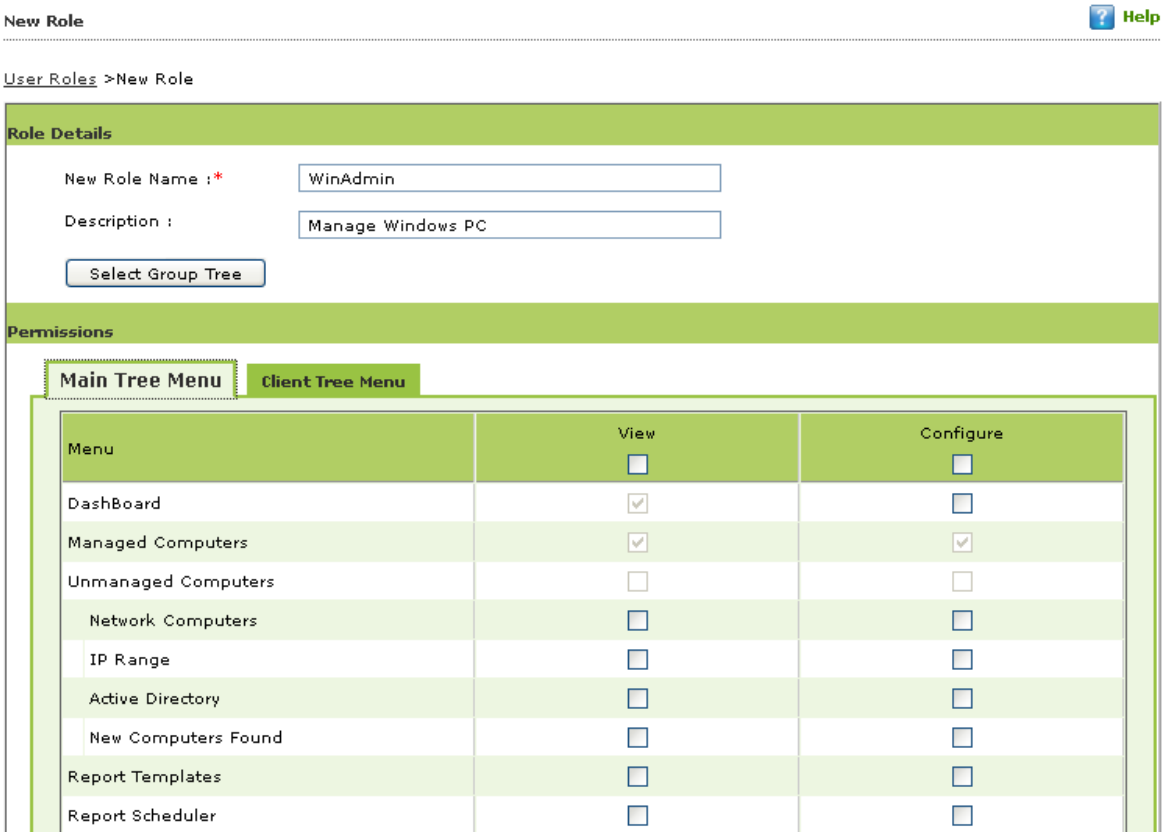


Figure - 17.5

   - **Client Tree View** - Define the Actions that the created admin role can configure for eScan client using eScan Management Console over the allocated group.

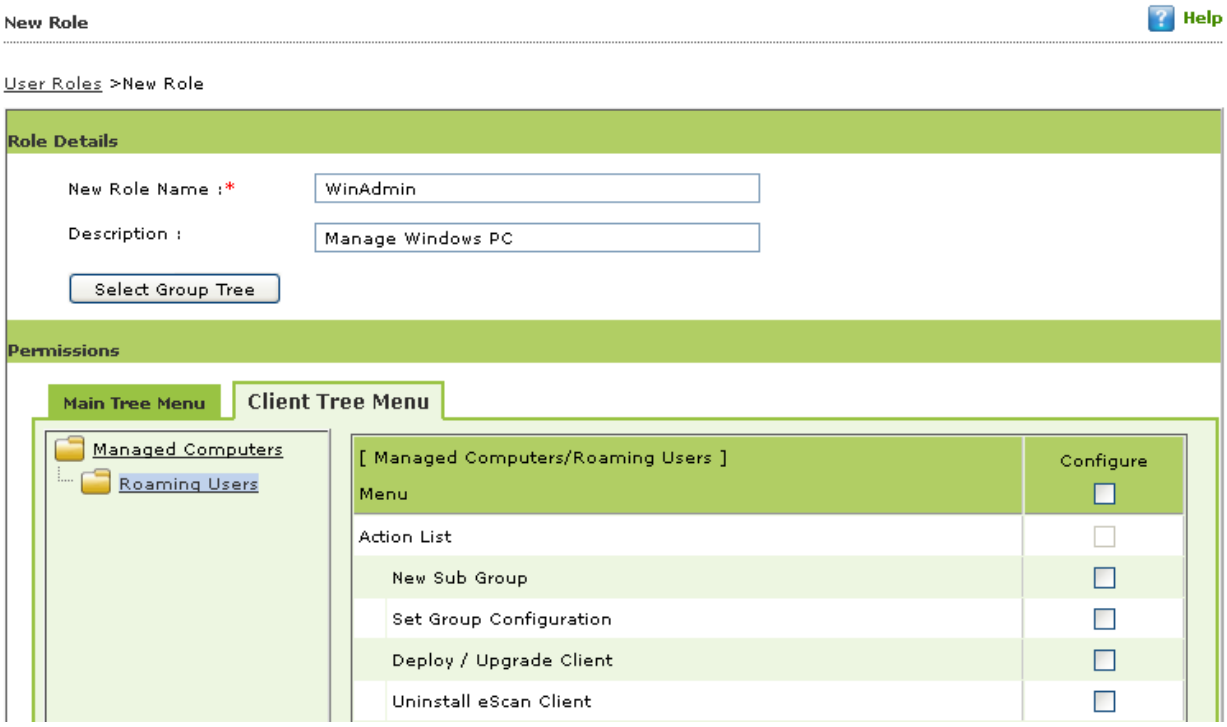


Figure - 17.6

4. Click **Save** at the bottom of the interface after defining the permissions for the created role.

18. Export and Import Settings

The eScan Web Console enables you to take backup, it will be helpful in case you wish to replace eScan server. Export settings along with the database from existing server to the new server.

- **Export Settings**

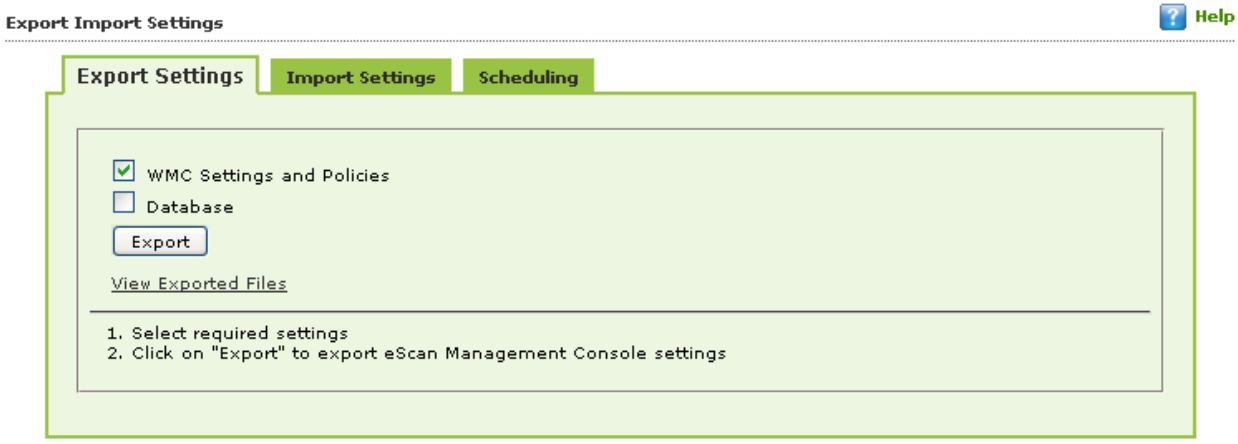


Figure - 18.1

Use the following steps to export the settings.

1. On the navigation pane, under **Administration**, click **Export & Import**.
   The **Export Import Settings** screen appears.
2. Under **Export Settings** section, select an appropriate check box:
   - **WMC Settings and Policies:** Select this check box, if you want to export WMC settings and policies.
   - **Database:** Select this check box, if you want to export eScan database.
3. Click **Export**.
   A message of settings successfully exported appears on the screen.
4. Click **Download Exported File** link, if you want to download the file. In addition, you can also view the date and time of when the file was last downloaded.

- **Import Settings**

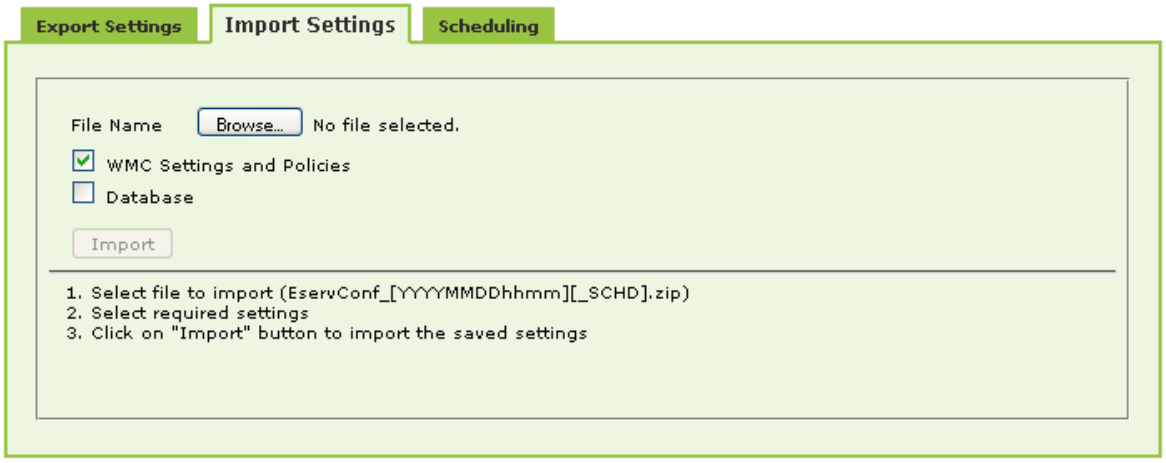


Figure - 18.2

Use the following steps to import the settings.

1. On the navigation pane, under **Administration**, click **Export & Import**.
   The **Export Import Settings** screen appears.
2. Under **Import Settings** section, type the file name or click **Browse** to select the file that you want to import
3. Under **Import Settings** section, select an appropriate check box:
   - **WMC Settings and Policies:** Select this check box, if you want to import WMC settings and policies.
   - **Database:** Select this check box, if you want to import database.
4. Click **Import**.
   A message of settings successfully imported appears on the screen.

- **Schedule**

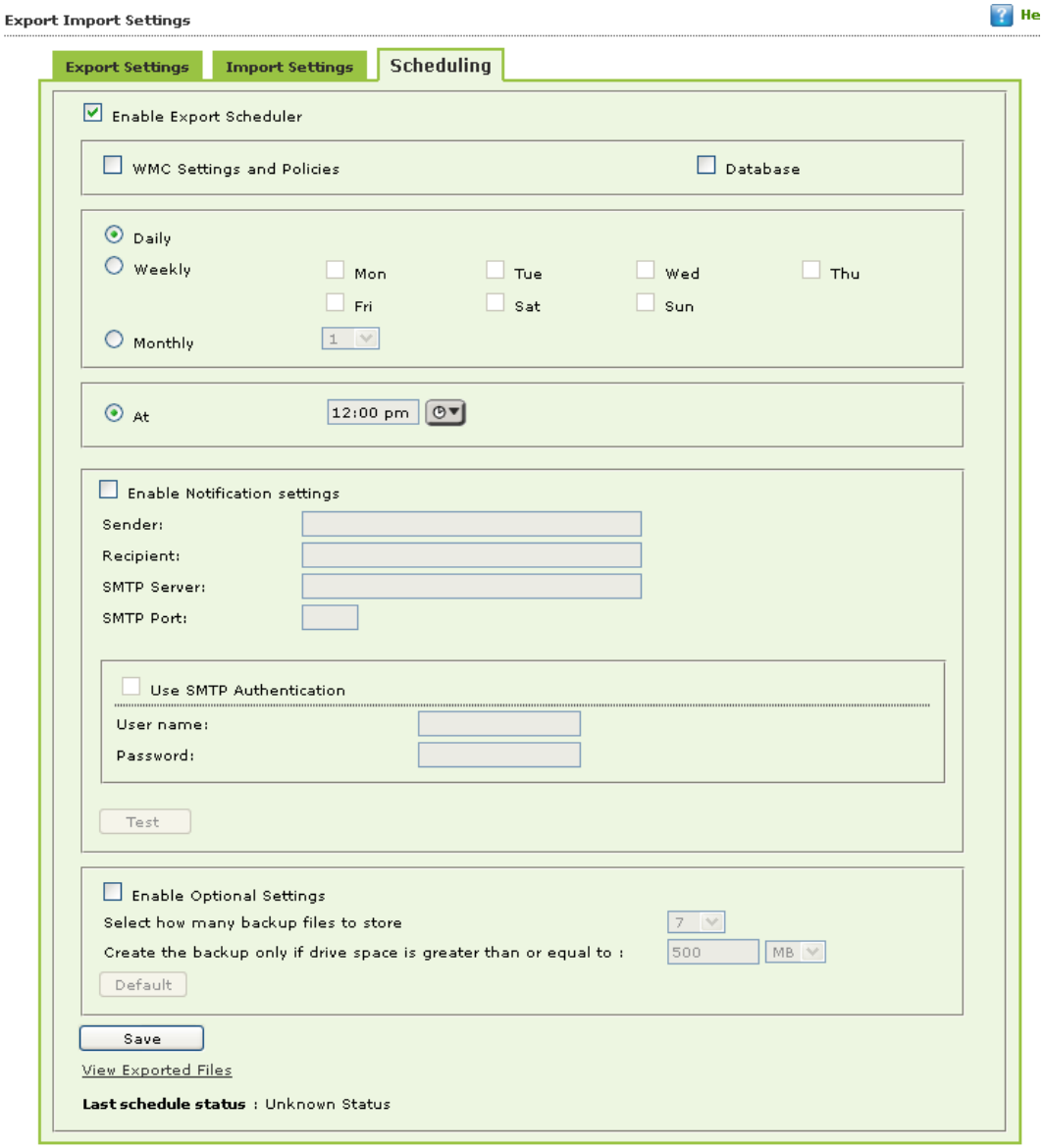


Figure - 18.3

Use this option you can do the following –

1. Enable scheduling of WMC settings and Policies or Database.
2. Schedule the Export/Import at a specific tie that can be daily, weekly or desired day(s) of a week or a desired date in a Month.
3. Send Notifications to specific recipient.
4. Allows you to define Username and Password for SMTP authentication.
5. Allows you to define settings for storing backup files.
6. Displays last schedule status.

19. Managing Licenses

The eScan Web Console enables you to manage license of users. You can add, activate, and view the total number of licenses available for deployment, number of licenses deployed, and number of licenses remaining with their corresponding values. You can also move the licensed computers to non-licensed computers and non-licensed computers to licensed computers.

- **Adding License and Activating License Key**

  It enables you to add licenses of users.

  (You can add only two licenses at a time, it is mandatory that you at least activate one license, because unless and until you activate a license you cannot add more licenses. The **To Add License Click Here** link becomes unavailable after adding two licenses, and to make it available you have to at least activate one license.)

Steps -

1. On the navigation pane, click **License** and click on **Click Here** link.

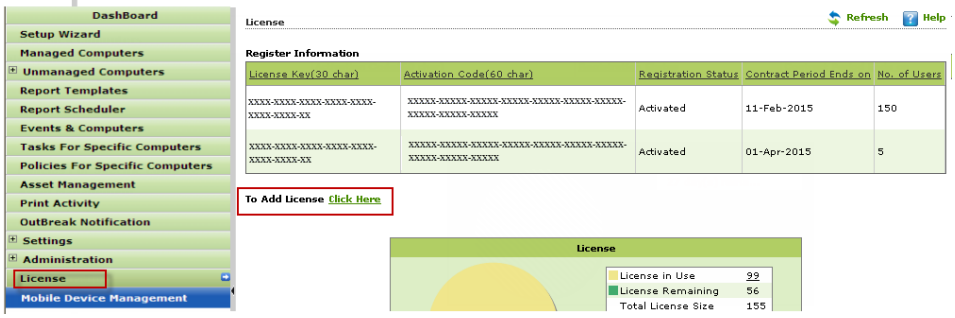


Figure 19.1

2. Add the 30 Digit License key and Click **Ok**. The added license key will be visible displayed in the **Register Information** table.

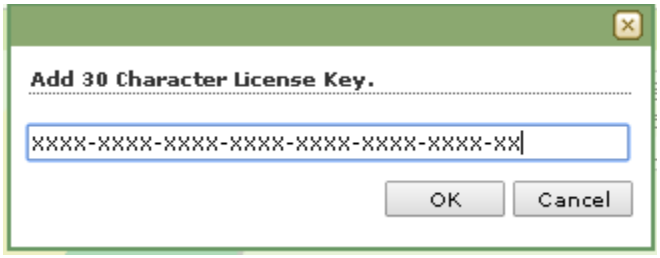


Figure 19.2

3. Click **Activate now** link present in Activation Code Column of Register Information table to activate the license on Client Computer.

Figure 19.3

4. Select the desired option for activation and fill the Personal Information.

Field	Description
Name	Type the machine name.
Phone No.:	Type the phone number.
Address:	Type the address.
Mobile No.:	Type the mobile number.
City	Type the city name.
Fax No.:	Type the fax number.
State:	Type name of the state.
Email Id*:	**[Mandatory]** Type an email ID
Country:	Select the country from the drop-down list.
Postal Code:	Type the postal code.
Email Subscription	Click an appropriate option. **Yes:** Click this option, if you want to subscribe for email. **No:** Click this option, if you do not want to subscribe for email.
Reseller/Dealer*:	Type name of the reseller or dealer. This is a mandatory field.

5. Click **Activate** present at the bottom of the interface. The License key will be activated instantly. (Requires Internet Connection)

- **Moving licensed computers to non-licensed computers**

  Use the following steps to move licensed computers to non-licensed computers.

1. On the navigation pane, click **License**.
2. Under **License** section, click **Manage License** link.

3. Under **Licensed Computers** section, select an appropriate check box, the computer that you want to move to non-licensed computers.

   The **Move to non-license** button is available only when you select an appropriate check box under **Licensed Computers** section, and you can move multiple computers at a time.

4. Click **Move to non-license**.
   The licensed computer moves to non-licensed computers section.

- **Moving non-licensed computers to licensed computers**

  Use the following steps to move non-licensed computers to licensed computers.

1. On the navigation pane, click **License**.
   The **License** screen appears.
2. Under **License** section, click **Manage License** link.
3. Under **Non Licensed Computers** section, select an appropriate check box, the computer that you want to move to licensed computers.

The Move to license button is available only when you select an appropriate check box under Non Licensed Computers section, and you can move multiple computers at a time.

4. Click **Move to license** button.
   The non-licensed computer moves to licensed computers section.

- eScan allows you to manage Licenses for eScan client installed on computers with  **Windows,**  **Macintosh** or  **Linux opreating system.**

20.Introduction - eScan Mobile Device Management

eScan Mobile Device Management solution is specifically designed for Mobile or Smart Phone devices. It helps you secure and protect your Mobile or Smart Phone against viruses, malwares, Trojans, and secures your confidential data. It also enables you to block applications and websites, which ensures security to your device. Using eScan Mobile Device Management Solution you can manage and secure Mobile as well as Smartphones.

eScan Mobile Device Management (MDM) allows you to monitor, secure and manage all your android devices remotely. Using this solution you can control and monitor all security settings, gain real-time visibility of security status into mobile devices accessing your corporate network, and administer consistent policies across all devices.

Components of eScan Mobile Device Management Solution

Component	Description	Required or Optional
eScan Corporate 360	For using eScan Mobile Device Management server, you first need to install eScan Corporate 360 on any of the computer connected to the network.	**Required**
eScan Mobile Device Management	After adding the devices in Mobile device Management console, a message is sent on the email address used for enrolling the device with a link to download and Install eScan Mobile Security (Client). The user should enroll the device with same details as used during enrolment on the Mobile Device Management Console(Server)	**Required**
Microsoft SQL Server	The Microsoft SQL Server hosts the databases for MDM server.	**Required**
Active Internet Connection	An active internet connection is mandatory to install eScan Mobile Security. To download and install eScan Mobile Security on the device an email will be sent by the MDM Sever.	**Required**

Features of eScan Mobile Device Management Console (Server)

	eScan Corporate 360 with Mobile Device Management	
Sr.No.	**Features**	**Description**
1	**Dashboard**	
	Deployment Status	
	eScan Status	It displays the pie chart to show the status of eScan installation on Managed Devices. To view Device details you can click on numeric values present beside the chart.
	eScan Version	It displays the pie chart to show the version of eScan installation on Managed Devices. To view Device details you can click on numeric values present beside the chart.
	Android Version	It displays the pie chart to show the Android version of Managed Devices. To view Device details you can click on numeric values present beside the chart.
	Device Sync Status (Successful)	It displays the pie chart to show the sync status of the managed devices. To view Device details you can click on the numeric values present beside the chart.
	Device Compliance	It displays the pie chart to show the device compliance status such as Healthy or non-compliant. It will also display the number of the devices for which the compliance status is unknown.
	Protection Status	
	Update Status	It displays the pie chart to show the update status of eScan on Managed Devices. To view Device details you can click on numeric values present beside the chart.
	Scan Status	It displays the pie chart to show the File Scanning status by eScan on Managed Devices. To view Device details you can click on numeric values present beside the chart.
	Anti-Virus	It displays the Start / Stop status of Ant-Virus Module of eScan on Devices.
	Web Control	It displays the status of Websites blocked started or stopped on managed devices. To view further details you can click on numeric values present beside the chart.
	Application Protection	It displays the status of Applications blocked or started or stopped on managed devices. To view further details you can click on numeric values present beside the chart.
	Call and SMS	It displays the Start / Stop status of call and SMS filter Module of eScan on Devices. To view further details you can click on numeric values present beside the chart.

	Protection Statistics	
	Anti-Virus	It displays the Pie chart to show the activity status of Anti - Virus module of eScan on Managed Devices like number of files scanned, skipped or deleted. To view further details you can click on numeric values present beside the chart.
	Web Control	It displays the Pie chart to show the number of sites allowed or blocked by eScan on Managed Devices. To view further details you can click on numeric values present beside the chart.
	Application Control	It displays the Pie chart to show the number of apps that are allowed to execute or blocked by eScan on Managed Devices. To view further details you can click on numeric values present beside the chart.
	Call Statistics	It displays the Pie chart to show the number of incoming and outgoing calls allowed, incoming and outgoing calls blocked on the Managed Devices. To view further details you can click on numeric values present beside the chart.
	SMS Statistics	It displays the Pie chart to show the number of SMS received or sent from Managed Devices. To view further details you can click on numeric values present beside the chart.
2	**Managed Mobile Device**	
	Group Creation	Allows you to create different groups
	Add Mobile Device	Allows you to add devices
	Move To Group	Allows you to move devices from one group to another group
	Create Policies	Allows you to define policies for Anti-Virus Policy, Call & SMS Filter Policy, Parental Policy, Anti-Theft, Additional Settings Policy, Password Policy, Device Oriented Policy
	Create Tasks	Allows you to create New Task, Start Task, Task Settings, and Schedule Task.
3	**New Mobile Devices Found**	It will show if any device found in the network
4	**Manage Backups**	
	SMS	It allows an administrator to backup and restore SMS from managed devices
	Contacts	It allows an administrator to backup and restore contacts from managed devices
5	**Anti-theft**	
	Wipe	Wipe Data feature that helps users to remotely delete contacts and SMSs from devices that are either lost or stolen.

	Locate	The Locate Device feature helps track the location of the lost device through GPS finder.
	Screaming	Raise an Alarm on the Device for easy location
	Lock	Allows you to remotely lock the device
	Send Message	Allows you to send some message to the device
6	**Asset Management**	
	Hardware Information	It shows consolidated hardware information of managed devices
	Software Information	It shows consolidated software information of managed devices
	Filter Criteria	It allows you to filter report captured from devices based on any or all criteria to be included or excluded in the report.
	Export Options	It allows you to export generated reports in desired formats. eScan supports Excel, PDF and HTML formats
7	**Report Templates**	
	Application Control Report	Generate Application Blocked / Allowed Report for Managed devices
	Inventory Report	Generate Software and Hardware Report for Managed devices
	Update Report	Generate Update status Report for Managed devices
	Virus Report	Generate Virus detected and action taken Report for Managed devices
	Web Control Report	Generate report for webpages blocked/ Allowed by eScan for Managed devices
8	**Report Scheduler**	
	New Report Scheduler	Create a new Report Schedule
	Selection for Applied Clients	Select Devices for report creation
	Report Send Options	Send report on Email
	Report Scheduling Settings	Schedule Automatic or Manual Report on Desired days, date or time
9	**Events & Devices**	It will show all the events received from the Devices
10	**Settings**	Define settings for mail server for sending Email notifications
11	**App Store**	Allows you to Add Apps to the Console that can be pushed to Managed Devices for installation
12	**Call Logs**	It will display the list of incoming, outgoing and missed calls of the managed devices.
13	**Content Library**	It will allow you to deploy documents and other important information to the managed mobile devices.

Features of eScan Mobile Security (Client)

Sr.No.	Features	Description
1.	**Administrator Mode**	You will have to enter the secret code to use eScan in Administrator mode. You can configure settings or make any changes to the settings.
2.	**Device Compliance**	This will display the compliance status of the device as Healthy or non- compliant.
3.	**Anti- Virus**	A real-time scanning and protection against viruses, and other threats.
4.	**Call and SMS Filter**	Blocking of unwanted Calls and SMS.
5.	**Backup**	Take a Backup of SMS and Contacts from managed device to the server.
6.	**Parental Control**	Block execution of Unwanted Applications as well as opening on unwanted websites on the device, as desired.
7.	**Anti-Theft**	Use this option to Enable Anti-theft module on the device, Administrator can use this feature to Locate the Device, Wipe the Data present on the Device (SMS and Address Book), Block Device from being used without Admin password, Raise an Alarm for easy location of the Device, Send Message to the Device through MDM Server.
8.	**Privacy Advisor**	Shows the permissions for installed applications on your device.
9.	**Applications**	This will display the list of downloaded applications and will also allow you to download apps from the app store.
10.	**Content Library**	This will display the documents the administrator shared through the Mobile Device Management console. It will also allow the user to download the deployed documents from here.
11.	**Additional Settings**	Configure Advanced Settings for your device for showing notifications, sound notifications, create secret code, Write logs, and Uninstall eScan from Device, Sync with the Server, and Change Server and Port Address.

21.Getting started with eScan Mobile Device Management

This chapter helps you start using eScan's Mobile Device Management (Here after referred as eScan MDM) and provides you the basic usage instructions. Currently eScan MDM console will get installed along with eScan Corporate 360 Installation. Once eScan Corporate 360 is installed, using eScan corporate 360 console you can access eScan MDM as shown in the image below.

Note:
There is no separate installable file for eScan MDM, once available it will be updated on our website as well as in the user guide.

Mobile Device Management Console

You can access the Mobile Device Management Console through a tab provided in eScan Management Console, as shown below -

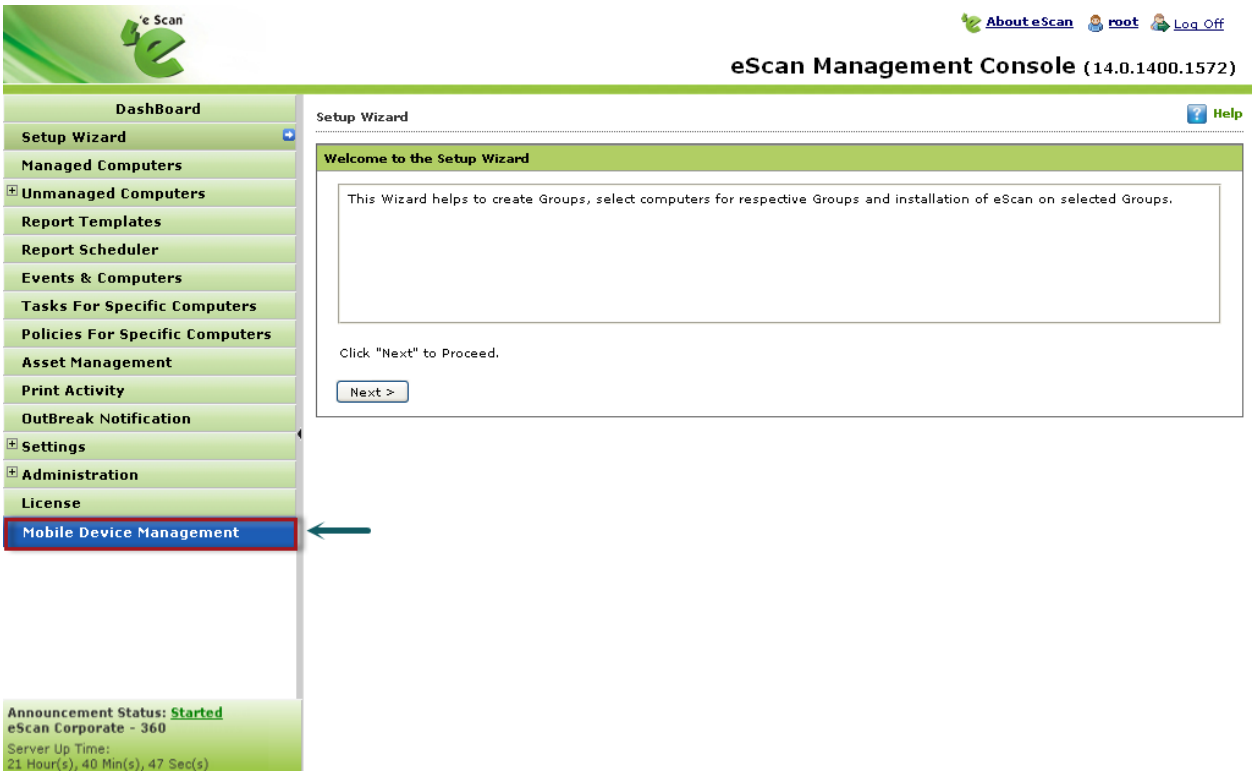


Figure 21.1

The Mobile Device Management Console is the central point for managing and monitoring Mobile Security throughout your corporate and enterprise network. The console comes with a set of

default settings and values that you can configure based on your security requirements and specifications.

You can use the Mobile Device Management Console to do the following:

- Install and Manage the eScan Mobile Security (Client) installed on mobile devices
- Configure security policies for the eScan Mobile Security (Client)
- Configure scan settings on a single or multiple mobile devices
- Group devices into logical groups for easy configuration and management
- View enrollment and update information

Accessing eScan Mobile Device Management Console

Steps to access eScan Mobile Device Management Console –

1. Logon to the eScan Management Console.
2. Now Click **Mobile Device Management** tab present in the Navigation Panel at the bottom left of the interface.
3. Mobile Device Management console will open in a new tab.

22.Working with eScan Mobile Device Management Console

Interactive Dashboard

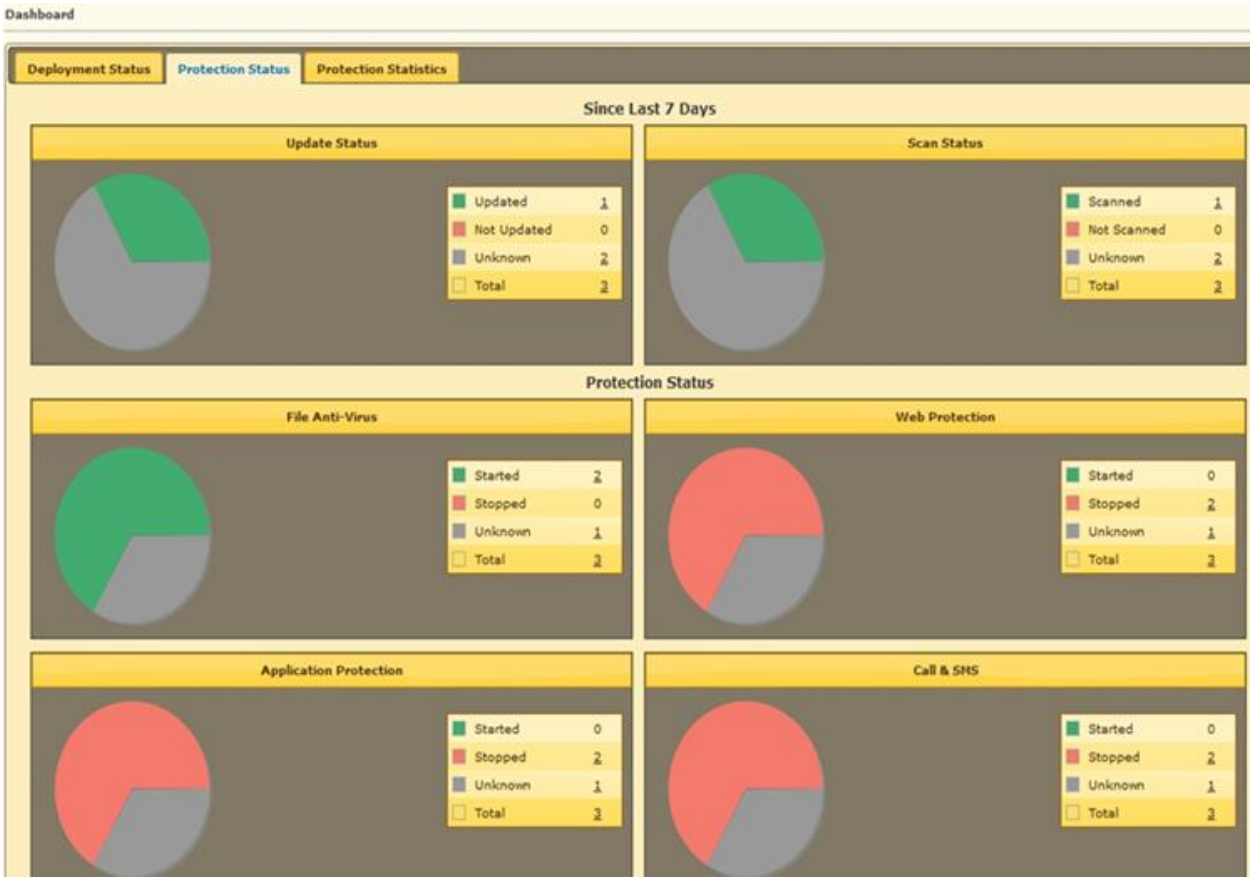


Figure 22.1

Description

This Module displays a real time status of **Deployment Status**, **Protection Status** and **Protection Statistics** in the form of Pie charts.

Following information is displayed in charts present in the tabs under Dashboard module.

1. **Deployment Status -** This Tab displays detailed pie chart view and statistics of the following –

    - **eScan Status** - Displays the pie chart view of devices where eScan Mobile Security(client) is installed, and number of devices for which the eScan Mobile

Security(client) installation status is unknown. You can view details of each device by clicking the numeric values displayed in the legends section.

- **eScan Version –** Displays the versions of eScan installed on Managed Devices**.** You can view details of each device by clicking the numeric values displayed in the legends section

- **Android Version** – Displays the Android Versions and the number of devices with that particular version of android installed on Managed Devices. You can view details of each device by clicking the numeric values displayed in the legends section.

- **Device Sync Status** – Displays the last sync status of the managed device with the server. You can view the statistics of the devices that are synced with the MDM server. You can view the details of each device by clicking the numeric values displayed in the legends section.

- **Device Compliance** – Displays the compliance status of the managed devices as healthy/ non-compliant/ unknown. It will also display the pie chart view of the compliance status. You can view the details of each device by clicking the numeric values displayed in the legends section.

2. **Protection Status -** This Tab displays detailed pie chart view and statistics of the following –

- **Update Status –** Displays the pie chart view of the update/not update status of eScan on Managed Devices. It also displays the information about devices where eScan update status is unknown. You can view details of each device by clicking the numeric values displayed in the legends section.

- **Scan Status -** Displays the pie chart view of the number of Devices Scanned, not scanned and the number of devices for which the scan status is unknown. You can view details of each device by clicking the numeric values displayed in the legends section.

- **Anti-Virus –** Displays the pie chart view for the number of devices where Antivirus module of eScan Mobile Security (Client) is started or stopped or the status is unknown. Further details can be viewed by clicking on the numeric values for respective details. You can view details of each device by clicking the numeric values displayed in the legends section.

- **Web Control** - Displays the pie chart view for the number of devices where Parental Control (Web Control) module of eScan Mobile Security (endpoint) is started or

stopped or the status is unknown. You can view details of each device by clicking the numeric values displayed in the legends section.

- **Application Control -** Displays the pie chart view for the number of devices where Application Protection module of eScan Mobile Security (Client) is started or stopped or the status is unknown. You can view details of each device by clicking the numeric values displayed in the legends section.

- **Call and SMS Filter -** Displays the pie chart view for the number of devices where Call and SMS Filter module of eScan Mobile Security (Client) is started or stopped or the status is unknown. You can view details of each device by clicking the numeric values displayed in the legends section.

3. **Protection Statistics –** This tab displays pie chart view of detailed eScan modules activity on Managed Devices. You can view details of each device by clicking the numeric values displayed in the legends section.

    - **Anti – Virus –** Displays statistics in pie chart as well as numbers for files skipped or deleted during a scanning on Managed Devices. You can view details of each device by clicking the numeric values displayed in the legends section.
    - **Web Control** - Displays statistics in pie chart as well as numbers for websites allowed or blocked on Managed Devices. You can view details of each device by clicking the numeric values displayed in the legends section.
    - **Application Control** - Displays statistics in pie chart as well as numbers for Apps to be allowed or blocked to execute on Managed Devices. You can view details of each device by clicking the numeric values displayed in the legends section.
    - **Call Statistics** – It displays the Pie chart to show the number of incoming and outgoing calls allowed, incoming and outgoing calls blocked on the Managed Devices. You can view details of each device by clicking the numeric values displayed in the legends section.
    - **SMS Statistics** - Displays statistics in pie chart as well as number of SMS received or sent on Managed Devices. Further details can be viewed by clicking on the numeric values for respective details.

Managing Mobile Devices

- Creating Groups, Adding Devices and Uninstalling eScan

Figure 22.2

Sr. No.	Options	Description
1.	**New Group**	Use this Option to Create New Group for categorizing / adding Devices.
2.	**Add New Device**	Use this option to add new devices in created groups.
3.	**Add Multiple Devices**	You can import (*.txt) file with device and user details in the following format for adding multiple devices at once. Mobile no.1,Username1,Email-id1 for example: 9012345678,ABCD,abcd@xyz.com **Note – Please do not put space before or after comma in the above format.**
4.	**Remove Group**	Select a group and click on this option to Remove the selected group under Managed Devices.

Create New Group

Figure 22.3

Steps for Creating a New Group

1. Select the **Managed Devices** group present in the tree under Managed Mobile Devices module.
2. Click **New Group** option present under Action list Menu. You will be forwarded to **Create New Group** window, as shown above.

3. Write the Name of the Group that you wish to create.
4. Click **Save** button present at the bottom of the Window.
5. The created group will be added under Managed Devices group in the Managed Mobile Devices Window.

Add New Device

Once the logical Groups are created, you will be required to Add devices to the respective groups for Managing and securing them efficiently.

Figure 22.4

Steps to Add a New Device –

1. Select the Group where you wish to Add the device, present in the tree under Managed Mobile Devices module.
2. Now Click **Add New Device** option present under **Action List**.
3. Add Device Details in the respective fields present on Add New Device window.
4. Click **Add** button.
5. A Notification mail with a link to download and install eScan Mobile Security (client) will be sent on the email address.

Note:
The user should register the product from the device using the same enrollment details.
The mobile number required here is for indicative purpose and need not be an actual mobile number.

Adding Multiple Devices –

Using Add multiple Devices option present under Action List, you can Add multiple devices to a group by importing details from a Notepad (***. txt)** file in the following format –

Mobile no.1,Username1,Email-id1

Note:
There is no Space after or before comma in the above format
Use a line break to separate each device information
All the fields are Mandatory and please provide correct email-id

Steps to Add Multiple Devices

1. Select the Group in which you wish to add multiple devices using the folder tree present on the Managed Mobile Device window.
2. Now open **Add New Devices** option present under **Action list**.
3. Browse the .txt file that has the required details using the **Browse** option present on the Add Multiple Devices Window.

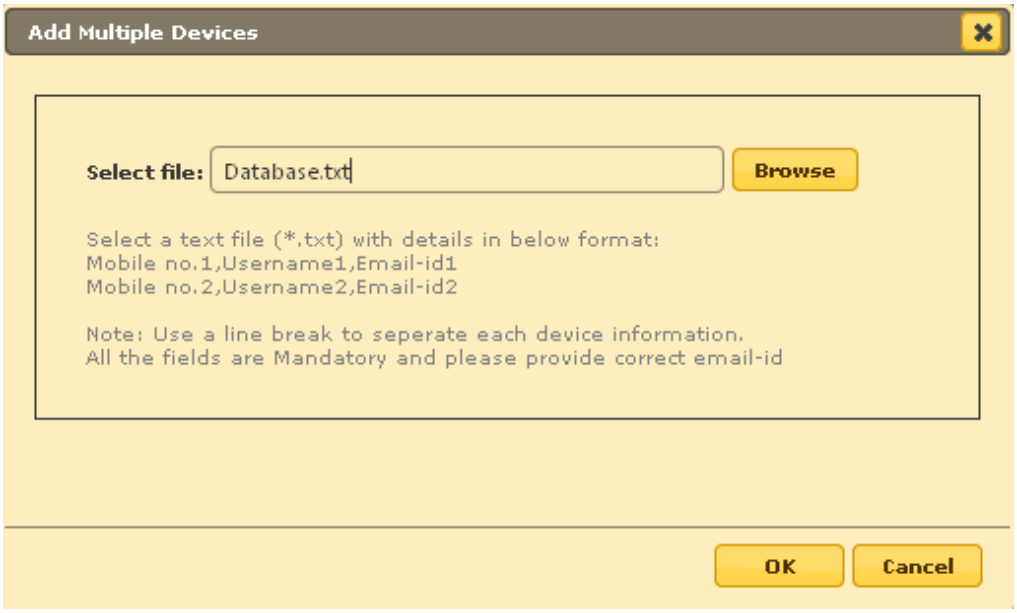


Figure 22.5

4. Click **OK** button to add the devices, all devices from the .**txt** file will be added to the group.

5. Details will be added and visible in Client Devices present under the selected group.

Moving Devices from one Group to the other

After Adding Devices in a group, you can move desired devices from one group to other whenever required.

Steps for Moving Devices from one Group to other –

1. Select the Group where the devices are already added using the tree present in the Managed Mobile Devices.
2. Now select the desired devices that you wish to move from this group to another using the check box present beside it.
3. Now Click **Client Action List** Menu present at the top in the Managed Mobile Devices screen and select Move to Group option, as shown below –

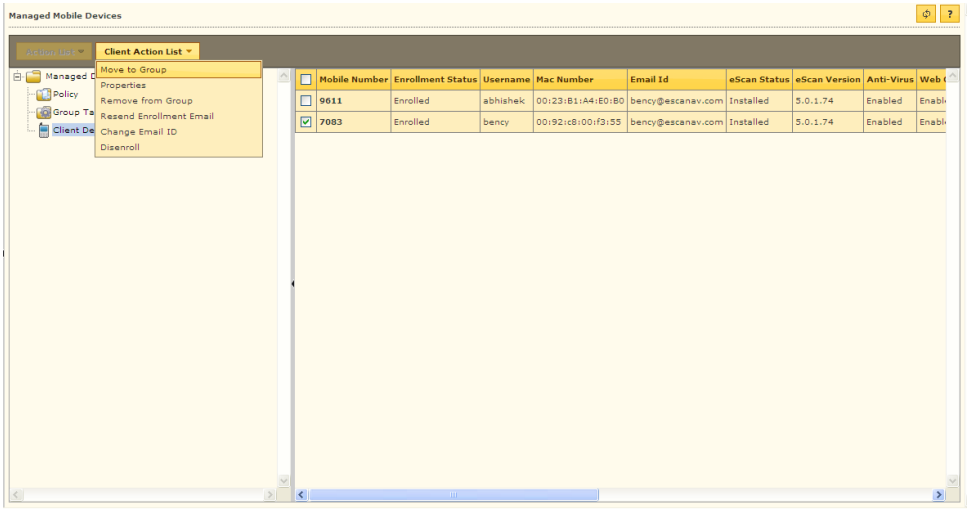


Figure 22.6

4. You will be forwarded to Select Group Window, select the desired group to which you wish to move the selected devices. And click **OK** button.
5. The selected devices will be moved to the group instantly.

Note:
You can create a New Group using the **New Group** option present in the **Select Group** Window.

Viewing Device Properties

Using the following simple steps you can View the Properties/Details of the Added Devices.

Steps for Viewing Device Properties

1. Select the Device present in the list on the Managed Mobile Devices screen to view its properties.
2. Now click **Properties** under Client Action list menu.
3. You will be forwarded to the Device properties window, all details of the device will be displayed on Properties window, as shown below -

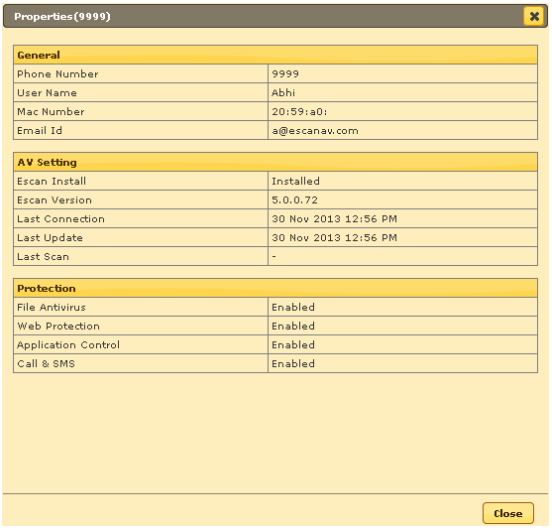


Figure 22.7

4. Click **Close** to close the Properties Window

Removing Device(S) from the Group

Using the following simple steps you can remove the Device(s) from any group whenever required –

1. Using the respective check box select the Device(s) that you wish to remove from the desired Group in Managed Mobile Devices Module. Please note that you can select single or multiple devices for deletion.
2. Now Click **Remove from Group** option present in Client Action List menu.
3. You will be prompted with a message for confirming the deletion, as shown below --

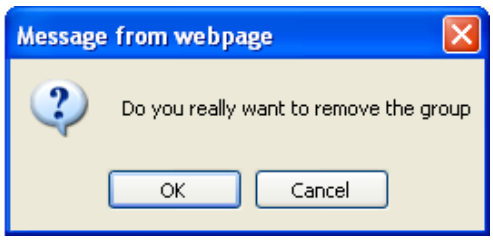


Figure 22.8

4. Click **OK** on the dialog box to delete the selected device from the group.
5. The selected device will be removed instantly from the group.

Note:
If the use has uninstalled eScan Mobile Security (client) from the device using Uninstall option present in Android OS, then the Administrator has to manually remove the device from the Mobile device Management Console.

Resending Enrollment Email

In case the user has not received the Enrolment email sent to him at the time of adding the device, you can resend the email by using Resend Enrollment Email option present under Client Action List menu in Managed Mobile Devices section.

Changing Email Address for Product Enrolment

You can change the email Address for sending enrolment mail using the following simple steps –

1. Select the Device using the respective check box in the Managed Mobile Devices window.
2. Now Click **Client Action List** Menu present at the top.
3. Click **Change Username/Email ID** under Client Action List menu, you will be forwarded to the Change Details Window, as shown below –

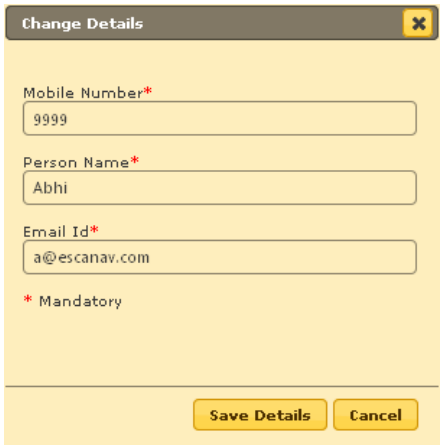


Figure 22.9

4. Make desired changes and click **Save Details** at the bottom of the Change Details window.

Disenroll

Using this option you can Disenroll or remove the device from the list of managed devices.

1. Select the Device using the respective check box in the Managed Mobile Devices window.
2. Now Click **Client Action List** Menu present at the top.
3. Click **Disenroll** under Client Action List menu.
4. Click **OK.**

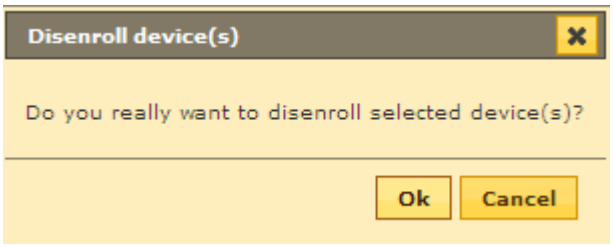


Figure 22.10

Protecting Managed Devices with Policies

Using Policy details options present under Policy, you can configure following settings in eScan Mobile security installed on Managed Devices –

1. Enable / Disable eScan Modules in eScan Mobile Security on Mobile Devices.
2. Define settings for all Modules of eScan Mobile Security on Managed Devices.
3. Configure Settings for Call and SMS Filter.
4. Define Policy for Blacklisting / Whitelisting Applications and Websites.
5. Enable Anti – Theft module on the managed devices.
6. Define additional settings for Notifications and logs.
7. Define Admin password for the managed devices.
8. Switch on GPS on Managed Devices.
9. Initiate installation of APK on mobile device.

Note:
All Policies will be applied on the Managed Devices in selected Group

Steps for Defining Policies for the Group

1. Select the desired group for which you wish to define policies in the Managed Mobile Devices module, click **Policy** under the Group, as shown below –

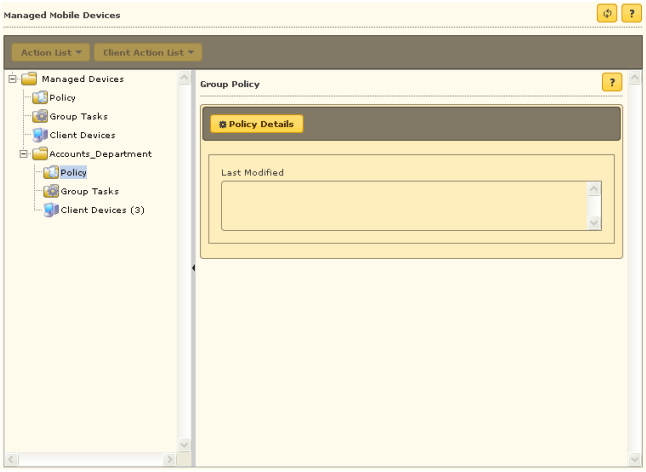


Figure 22.11

2. Now click **Policy Details** on the interface, you will be forwarded to the Policy Details Window.

Figure 22.12

Anti-Virus Policy

Click on Anti-Virus Policy to define policies for Anti-Virus. You can define settings for the following options-

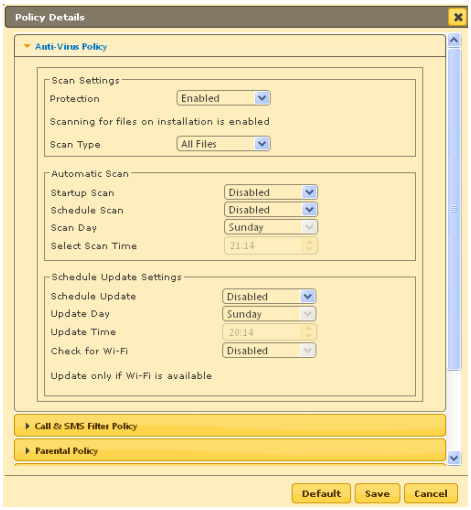


Figure 22.13

Policy Name	Description
Anti – Virus Policy	
Scan Settings	Using options present under this, define settings for Enabling or Disabling Virus Protection on Devices along with Scanning type settings for Managed Devices.
Protection	Select from Dropdown to enable or Disable Protection on Managed Devices in the group.
Scan Type	Select from Dropdown to Scan All Files or Executable on Managed Devices in the Group.
Automatic Scan	Use options present under this to Scan Devices on Startup, or Schedule Scan as per requirement.
Startup Scan	Select from dropdown to Enable or Disable Scanning on Device Startup, as per your requirement
Schedule Scan	Select from dropdown to Schedule Scanning on Managed Devices in the Selected group weekly or daily or else select disable.
Scan Day	Select from drop down to select day for Scanning managed devices present in the group.
Select Scan Time	Use the up and down arrow buttons to define time for Scanning Managed devices in the Group.
Schedule Update Settings	Define Settings for Updating eScan on Devices
Schedule Update	Using this drop down, you can disable update or schedule update weekly, or daily as per your requirement

Update Day	Using this Drop down, you can Schedule update on particular day of the week as per your requirement.
Update Time	Define the time at which you wish the updates to be delivered on the devices. It will be helpful in saving network congestion where large number of devices are added in the MDM Server.
Check for WiFi	Enable or disable the WiFi as per requirement to schedule update or disable the update.

Call and SMS Filter Policy

Click **Call and SMS Filter Policy** to define policies for Filtering Calls and SMS for incoming calls and SMS and for outgoing calls on managed devices.

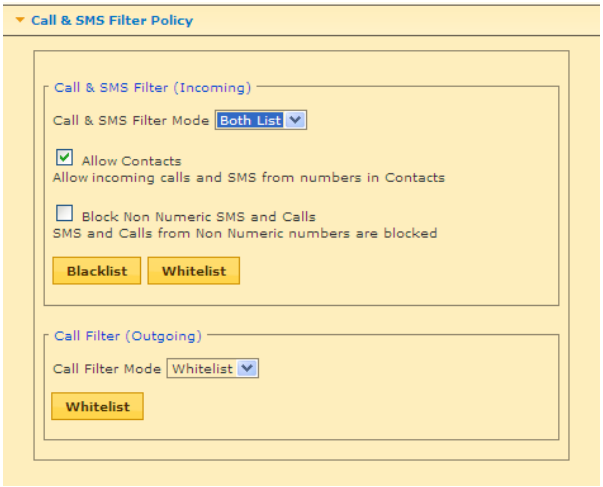


Figure 22.14

It includes following options –

Option	Description
Call and SMS Filter Mode (Incoming)	
White List	Accept the Call From White listed numbers only and reject others
Blacklist	Blocks the calls from all the numbers present in blacklist
Both list	Verify the number to Block or accept the call with the number present in White List and Black List. Reject calls from all other numbers
Allow Contacts	Apart from the numbers present in Blacklist or

	Whitelist, allow calls from Contact list saved on the device.
Block Non Numeric SMS	SMS coming from Non numeric numbers will be blocked
Call Filter Mode (Outgoing)	
Off	All outgoing calls will be allowed if the filter mode is off.
Whitelisted	Outgoing calls will be allowed only to the Whitelisted numbers. Click on the whitelist option to add numbers to whitelist.

Parental Policy

Click **Parental Policy** to define policies for Application and Web Control. It allows you to White List or Black list applications or websites on managed devices.

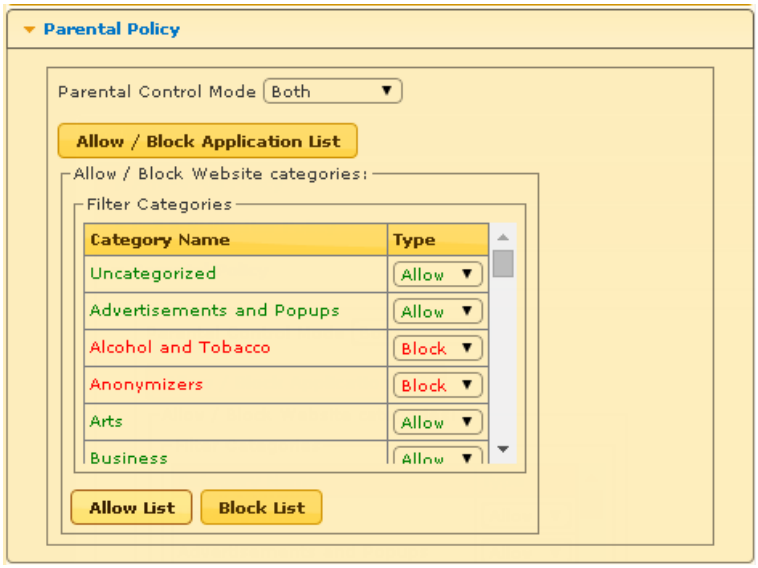


Figure 22.15

Sr. No.	Options	Description
1.	**Parental Control Mode**	Allow or Block Applications, or Websites or Both based on your requirement and Policies
2.	**Add / Block Application List**	1. Apps added to this list will be Allowed/Blocked as per action specified. 2. System apps will be Allowed by default unless explicitly added to "Block" action. 3. User Installed apps will be Blocked by default unless

		explicitly added to "Allow" action. 4. If action is set to "Ask Uninstall" the device will prompt the User to uninstall the App and will remain "Non-Compliant" until the App is uninstalled.
3.	**Allow List**	Websites added to this list will be allowed. You can modify, delete and also remove the list of websites.
4.	**Block List**	Websites added to this list will be blocked. You can modify, delete and remove the list of websites from the Block List.
5.	**Exclusions**	You can allow user to view specified websites or web pages by adding them to exclusions. Web filtering allows user to view websites from the exclusion list regardless of the selected categories.

Anti-Theft Policy

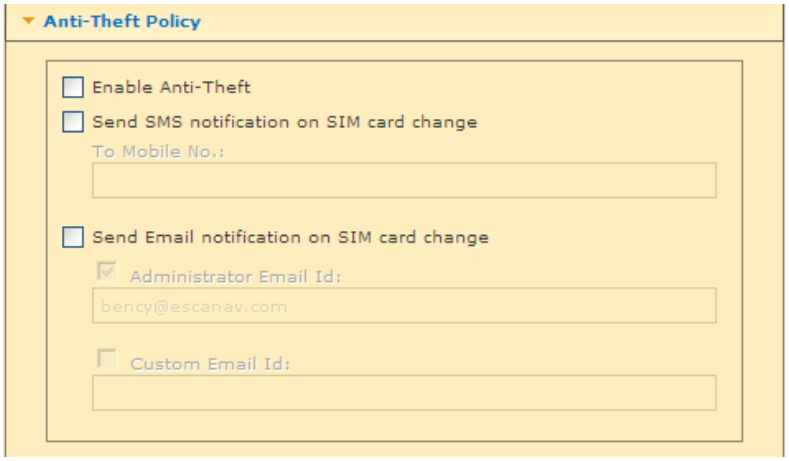


Figure 22.16

Sr. No.	Options	Description
1.	Enable Anti-theft	Tick this checkbox to Enable anti-theft on Managed Devices.

2.	Send SMS notification on SIM card change	Tick this checkbox to receive an SMS notification on changing the SIM card without the permission of the administrator. The notification will send to the number set by the administrator.
3.	Send Email notification on SIM card Change	Tick this checkbox to receive an email notification on changing the SIM card without the permission of the administrator. The email notification will sent to administrators' email id and also the custom email id that the administrator has specified.

Note:
If Anti-theft is not enabled and the device is lost/ stolen, even then it will receive Anti-theft messages, if connected to an internet.

Additional Settings

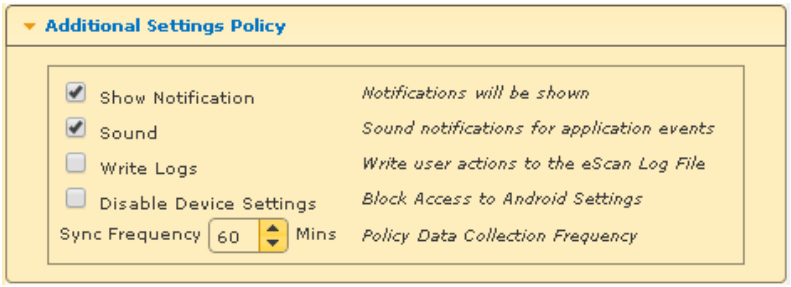


Figure 22.17

Description – Use this option to enable or disable the above option on selected managed devices.

Sr. No.	Options	Description
1.	**Show Notification**	Use this checkbox to Enable Notifications option present under Additional Settings on Managed Devices present in the selected Group. All notification messages will be shown on Devices.

2.	**Sound**	Use this checkbox to Enable Sound option present under Additional Settings on Managed Devices present in the selected Group. Alert sound will be played on the device for application events.
3.	**Write Logs**	Use this checkbox to Enable Write Logs option present under Additional Settings on Managed Devices present in the selected Group. Logs for User actions will be maintained in eScan Log files.
4.	**Disable System Settings**	Use this checkbox to disable/block Android settings.
5.	**Policy Data Collection Frequency**	Define time frequency for collecting Policy Data from devices. By default it is 60 minutes.

Password Policy

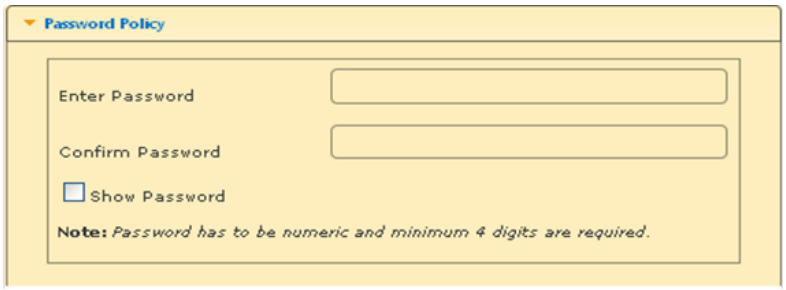


Figure 22.18

Use this option to define Administrative Password that will allow the user to configure settings of eScan Module on respective Managed devices.

Device Oriented Policy

Figure 22.19

Use this option switch on/off GPS on selected managed devices.

Required Applications Policy

Using Import option present under this tab, you can import the applications from App Store for installation on Managed devices in the group through Policy deployment.

For more information on Adding the Apps to App Store, click here

Steps for Importing Apps from App Store

1. Click **Import**.
2. Select the desired app that you wish to install on Managed Devices using the respective check box and click **Save**.

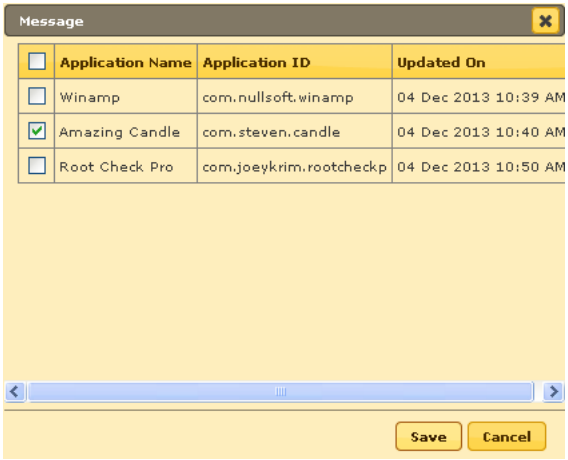


Figure 22.20

3. The selected App will be imported.

4. Click Deploy. The Policy will be deployed on the device instantly if internet connectivity is available on the device. If internet connection is not available, the change will be applied in next scheduled sync time, by default sync time is 60 minutes. The following screen appears confirming the deployment.

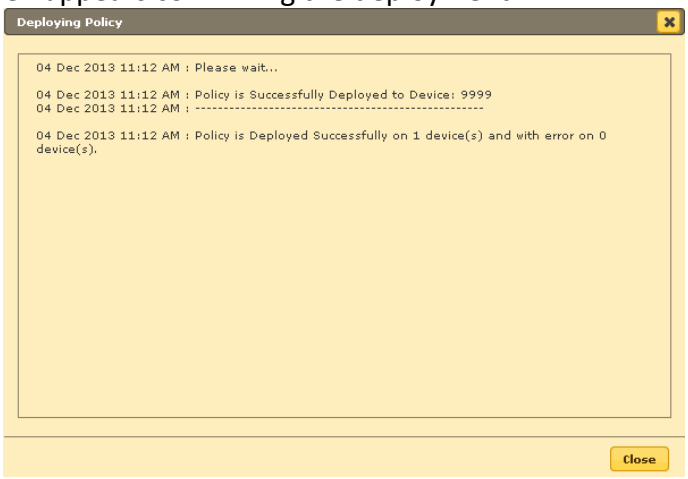


Figure 22.21

On Policy Deployment the user will get the message on Phone to install the app, on acceptance he will be provided with the option to start the installation process. If user cancels the installation, it will alert the user when the next sync happens.

WiFi Settings Policy

The WiFi Settings policy option will allow you to define the settings for your WiFi connections. It will allow you to disable WLAN/ WiFi or restrict the usage of WIFI by allowing the device to connect only to listed WIFI networks and also the device can be automatically locked or raise a sound alarm if the device is not connected to any of the listed WiFi Network connections.

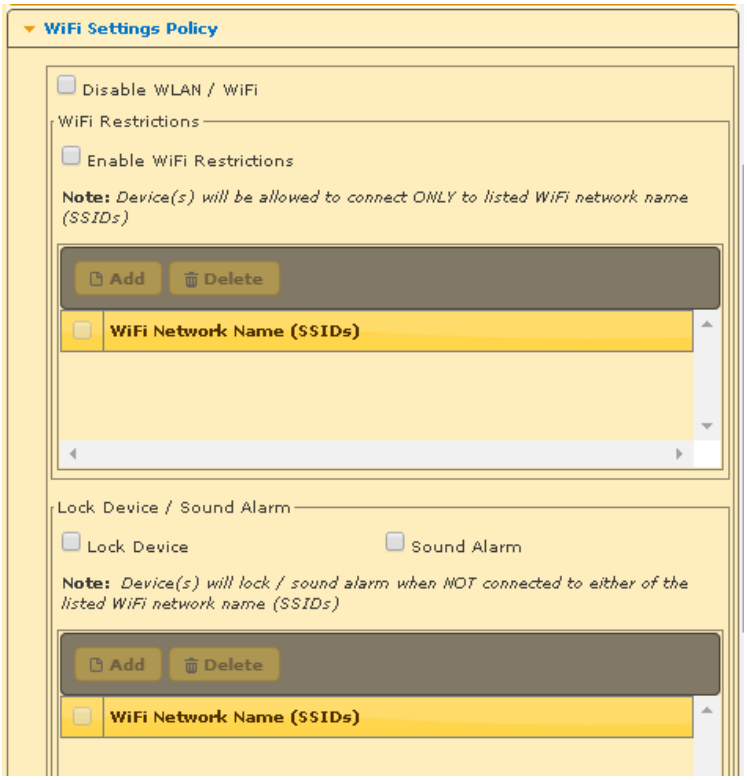


Figure 22.22

Scheduled Backup

This option will allow you to schedule a backup of all the SMS and contacts. It will allow you to define the task to be done. You can take a backup of the contacts and SMS. The backup of contacts and SMS can be saved in two different folders. The back up can be scheduled for daily/ Weekly and even disable the scheduled scan.

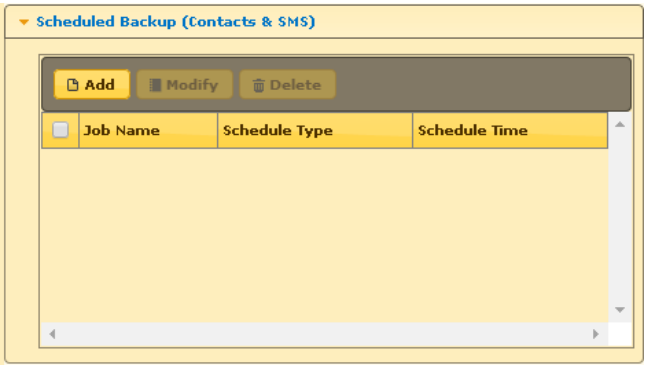


Figure 22.23

Content Library Policy

This option will allow the administrator to share documents with the users. The documents can be imported from the content library and deployed to the users.

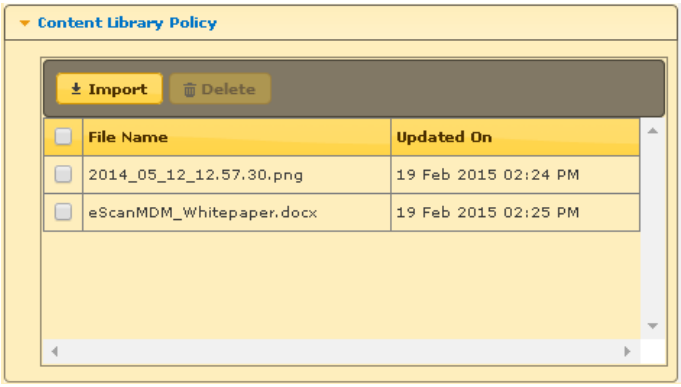


Figure 22.24

Default, Deploy, or Cancel

Figure 22.25

Description - You can select eScan **Default** settings or **Deploy** the setting defined by you for implementing / deploying on selected Managed Devices.

23. Managing Tasks

23.1 Group Tasks

Using eScan's Mobile Device Management Console, you can define and schedule tasks for Scanning on Managed Devices present in the group. It can be done using the Group Tasks option present in the Managed Mobile Devices module of Mobile Device Management Console.

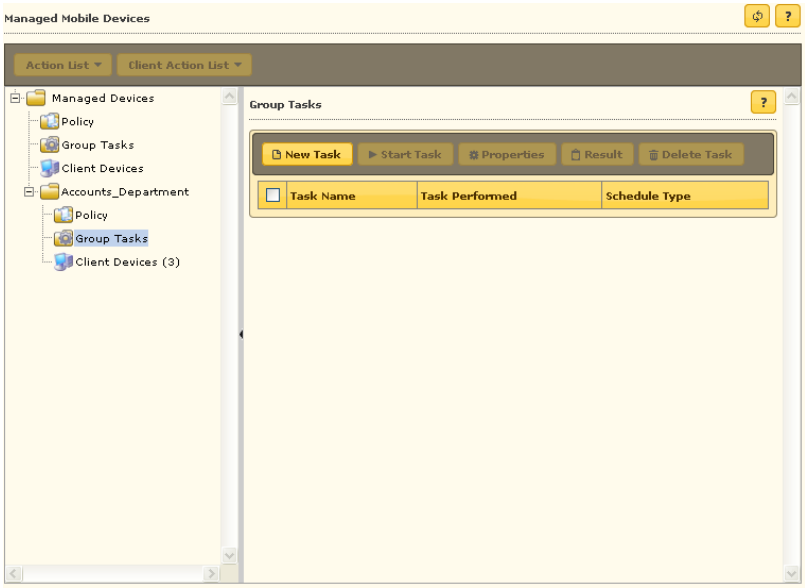


Figure 23.1

Using **New Task** option you can create Group tasks for Device Scanning and eScan Update. It also allows you to schedule the Scanning manually or at a desired date and time.

Creating a New Task

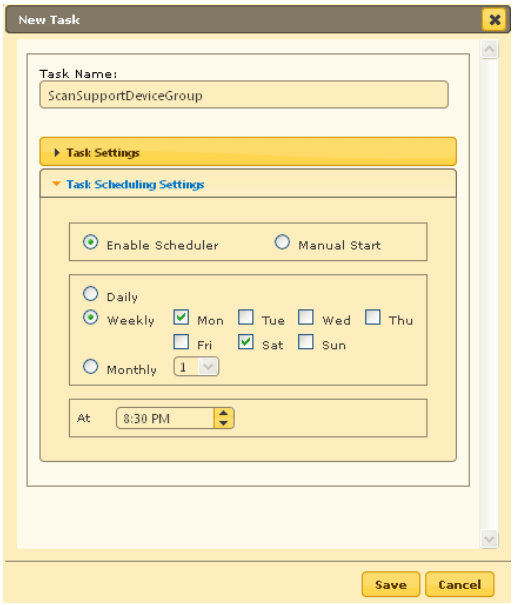


Figure 23.2

Using the **New Task** Window, define the task name and schedule the task as desired.

Steps for Creating a New Task for the Group -

1. Click **Group Task** option under the desired group for creating a New Task to be deployed on devices present under that group.
2. Now click **New Task**, you will be forwarded to the New Task window, where you can define Task Name, settings and schedule the task on Managed Computers in that group as desired by you.
3. Define the Task Name in the respective field present on the interface.
4. Define the task for Scan and Update using respective checkboxes.

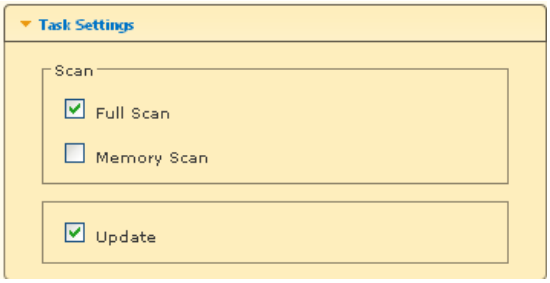


Figure 23.3

5. Schedule the created task using the options present under Task Scheduling Settings, as shown below.

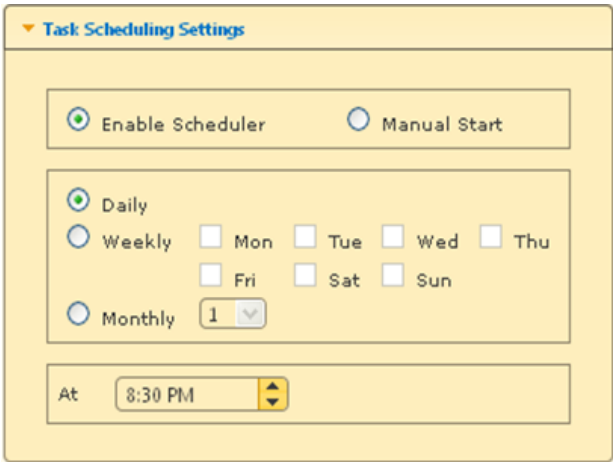


Figure 23.4

6. Click **Save** option present at the bottom of the Window. The task will be created instantly.

Group Task Status

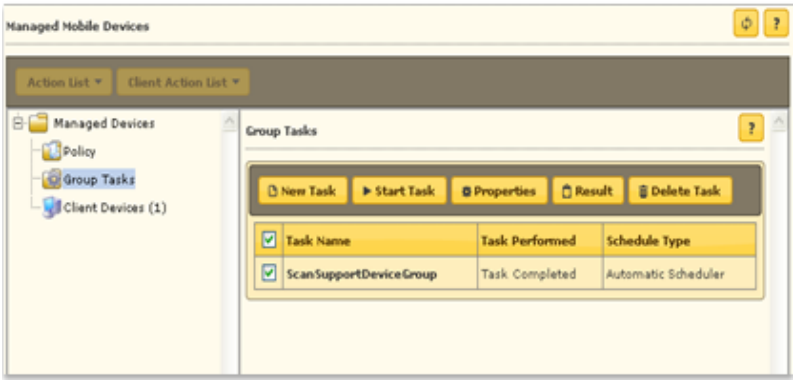


Figure 23.5

S.No.	Options	Description
1.	New Task	Use this option to create a New Task
2.	Start Task	Select a Task and Click on this button to Start the task on the Managed Devices present in the group.
3.	Properties	Use this option to View / Edit properties of the selected task.
4.	Result	Use this option to view detailed Result of the selected task.
5.	Delete	Use this option to Delete the Selected task from the listed tasks.

Viewing Managed Client Devices

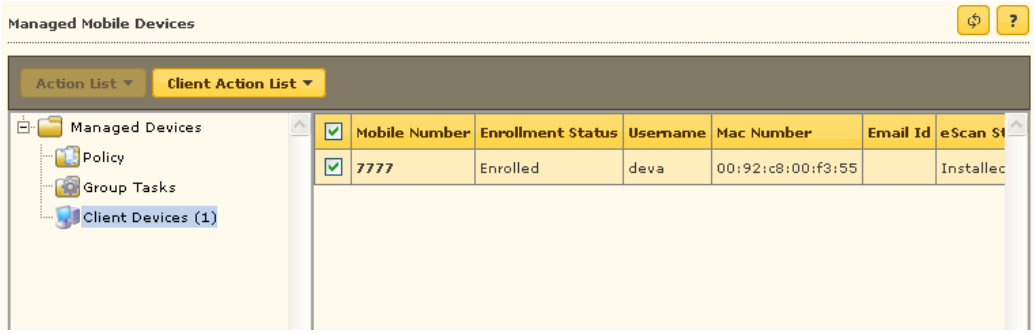


Figure 23.6

Sr. No.	Captured Information	Description
1.	**Mobile Number**	Displays the Mobile Number of the Device
2.	**Enrollment Status**	Displays the Status of the Device Enrollment/ recognition on the MDM Server, If successfully enrolled the status will change to "Enrolled" else it will show as "Pending".
3.	**Username**	Displays the Username of the Enrolled device
4.	**Mac Number**	Displays the Mac address of the enrolled device
5.	**Email Id**	Displays the email address of the user of the enrolled device
6.	**eScan Status**	Displays the installation status of eScan on the enrolled device
7.	**eScan Version**	Displays the eScan Version installed on the device
8.	**Anti-Virus**	Displays the Anti-virus status of the device as enabled or disabled
9.	**Web Control**	Displays the Web control Status of the device as enabled or disabled
10.	**Application Control**	Displays the Application Control Status of the device as enabled or disabled
11.	**Call & SMS Filter**	Displays the Call & SMS filter status of the device as enabled or disabled
12.	**Status for eScan modules**	It displays the Enable/Disable status of eScan Modules – **Anti-Virus, Web Control, Application Control, Call and SMS Filter** on the device
13.	**Last Connection**	It displays the Last connection timing between MDM server and device
14.	**Last Update**	It displays the date and time when eScan was last updated on the device
15.	**Last Scan**	It displays date and time of Last Scan on the device
16.	**Update Server**	It displays the Name / IP address of Update Server
17.	**Client OS**	It displays the OS Name and Version installed on the device
18.	**Applied Policy**	It displays the Name of Applied Policy.
19.	**Policy Date**	It displays the date and time on which the Policy is applied on the device

24. Device Discovery through New Mobile Devices Found

New Mobile Devices Found

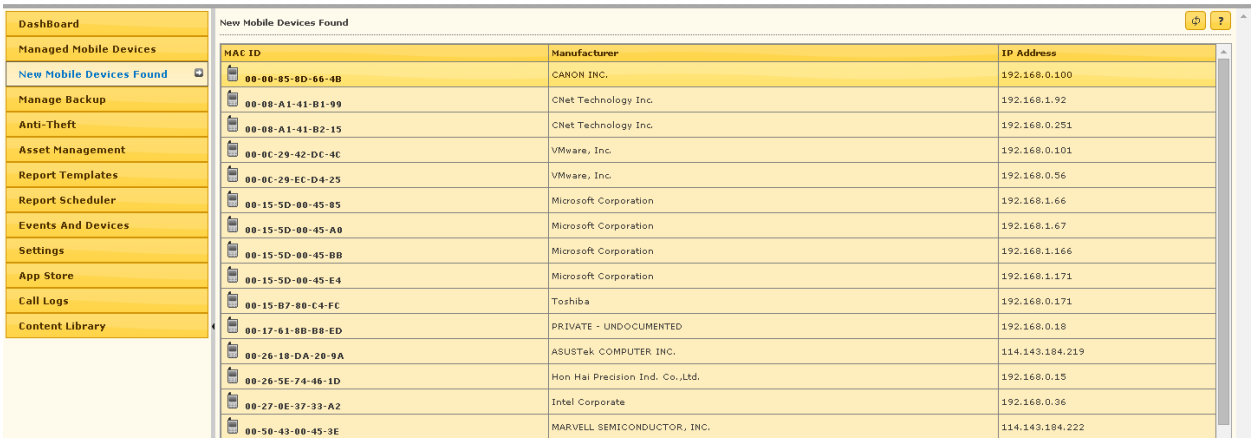


Figure 24.1

MDM automatically detects the devices when they access office network. It displays the Mac ID, Manufacturer Name and IP address of the detected device.

25. Backup Management

25.1. Manage Backup

Using the Manage Backup module of eScan, you can take backup of SMS and Contact list saved on Managed Device to the server and restore it later on the device whenever required.

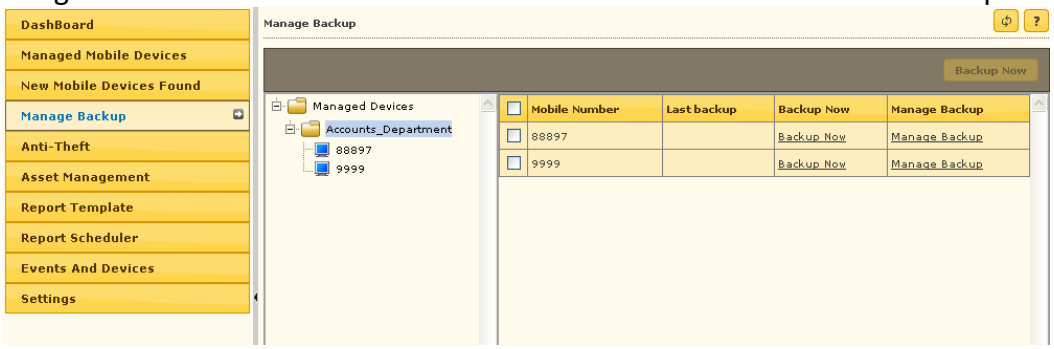


Figure 25.1

Description - eScan's Mobile Device Management allows you to take Backup of SMS and Contacts from the selected Devices/ Groups to the MDM Server.

Steps for Taking SMS Backup from Devices to the Server

1. Select the Devices or Group in Manage Backup module of eScan from where you wish to take backup of SMS to the MDM server.

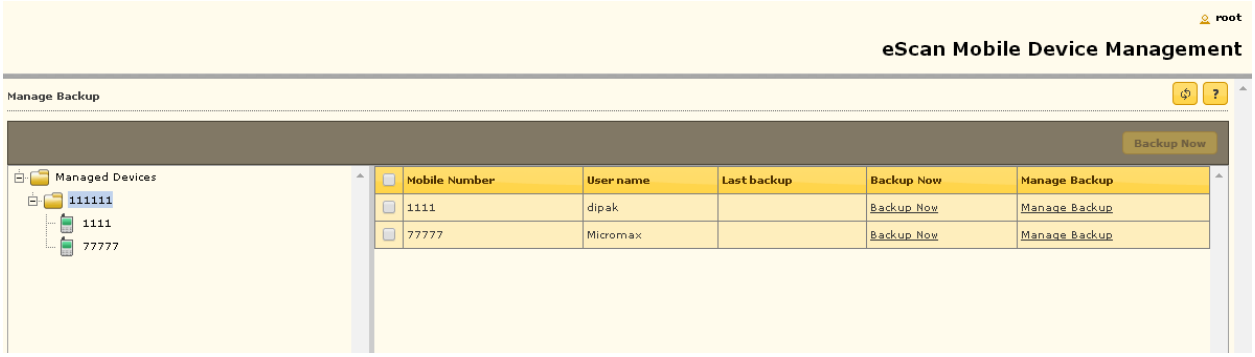


Figure 25.2

2. Now click **Backup Now** and select the desired option using respective check box to take backup.

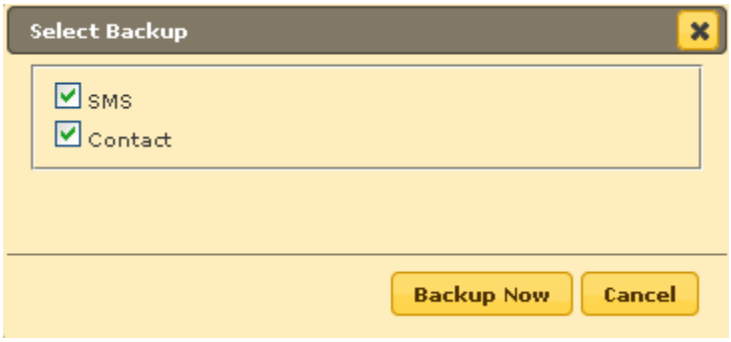


Figure 25.3

3. Click **Backup Now** option to take the Backup.

Note:
This feature will not work if there is no internet connection.

26. Lost Device Protection through Anti-Theft

26.1. Anti-theft – How it Works

If a user loses or misplaces the mobile device, you can remotely locate, lock or delete all the data available on that mobile device.

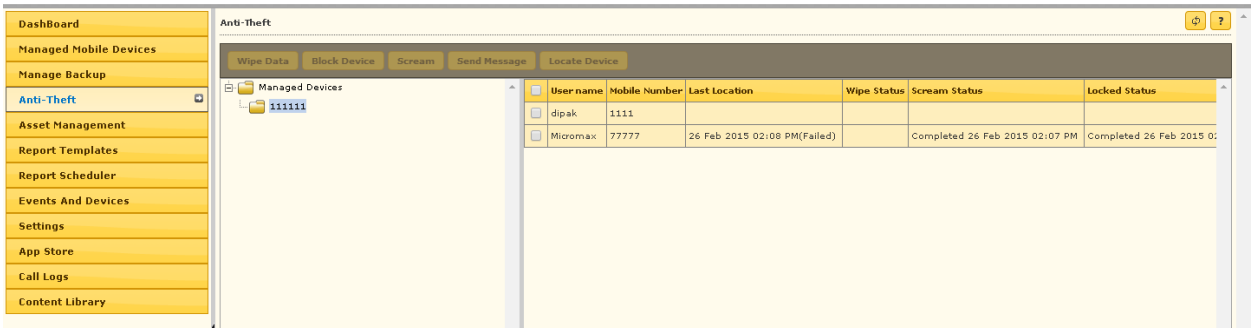


Figure 26.1

Using this Module, you can do the following –

Wipe Data

Using this option you can delete SMS and Address book from the device in case the Device is lost or stolen.

Blocking a Remote Mobile Device

You can send Block instruction from the MDM console to remotely block a mobile device. Users will require to type the Administrative password to unlock the mobile device.

Raising an Alarm on the Device

Use Scream Option to raise an alarm on the device for easily locating the device.

Send Message to a Remote Device

Use this option to send Message to desired Managed Devices.

Locating a Remote Mobile Device

You can locate the mobile device through the wireless network or by using mobile device's GPS. The Mobile Device Management server displays the mobile device location on Google Maps.

Note:
An active internet connection is required to use this feature.

27. Mobile Endpoints- Asset Management

27.1. Asset Management – How it Works

This Module displays detailed description of the Hardware and Software installed on the Managed Devices.

Asset Management – Hardware Information

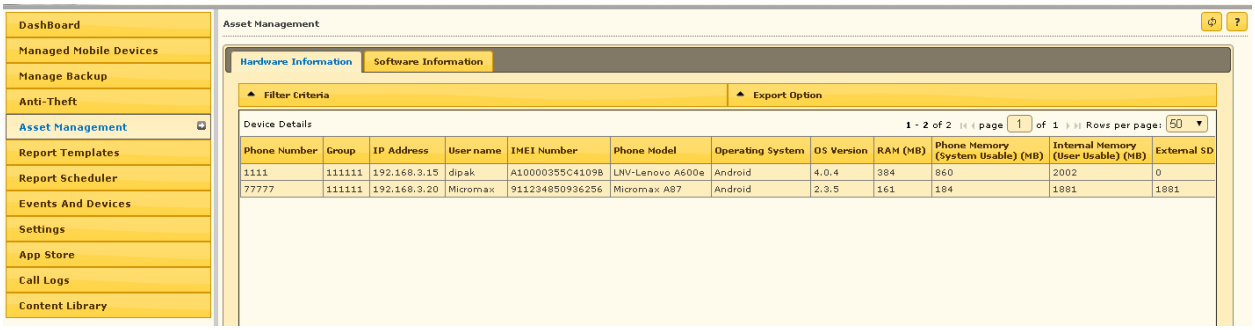


Figure 27.1

Steps for viewing Software and Hardware information –

1. Click **Asset Management** Module present in the Navigation Panel of Mobile Device Management Console.
2. Now select the desired Tab to view related information.

Following Hardware information is captured from Managed Devices --

Sr. No.	Captured Information	Description
1.	**Phone Number**	Displays the Phone number used on the device
2.	**Group**	Displays the Group to which the device is added to
3.	**IP Address**	Displays the IP address of the Device
4.	**Username**	Displays the username with which the device is registered on the MDM Server
5.	**IMEI Number**	Displays the IMEI number of the device
6.	**Phone Model**	Displays the Model details of the device
7.	**Operating System**	Displays the details of the OS of the device
8.	**OS Version**	Displays the OS version of the Device
9.	**RAM(MB)**	Displays the RAM size of the device in MB
10.	**Phone Memory (System Usable)(MB)**	Displays the size of Phone memory used by the system.
11.	**Internal Memory (User Usable) (MB)**	Displays the size of phone memory that can be used by the user.
12.	**External SD (MB)**	Displays the Size of the External SD card in the phone
13.	**Network Type**	Displays the type of the network being used by the device
14.	**Rooted**	Displays if the device is rooted or not
15.	**Roaming Enabled**	Displays the Status of Roaming, enabled or disabled
16.	**Bluetooth**	Displays if Bluetooth is present on the device or not
17.	**WiFi**	Displays if WIFI is present on the device or not
18.	**GPS**	Displays if GPS is present on the device or not
19.	**Software**	Displays the list of software installed on the device

Asset Management – Hardware Information – Filter Criteria

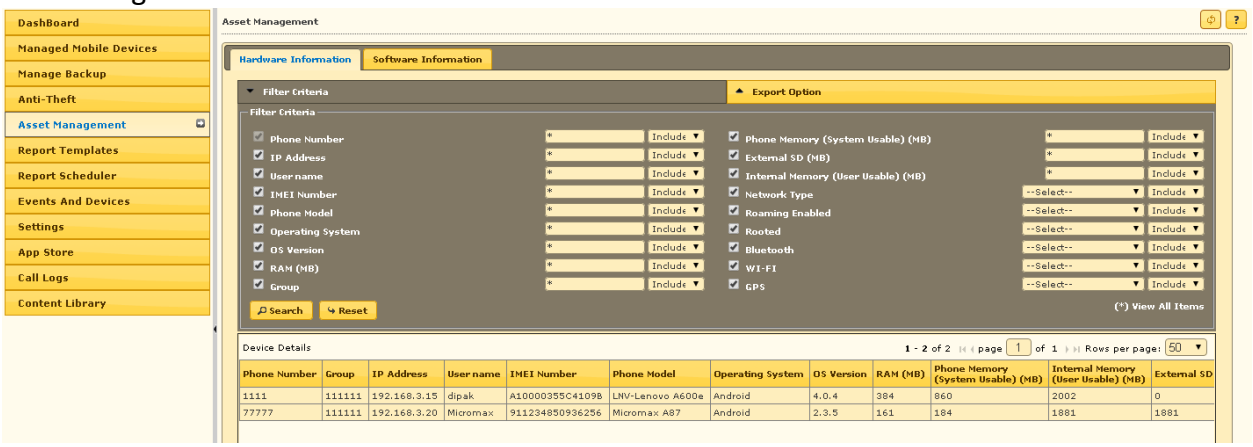


Figure 27.2

Information captured by MDM can be filtered on the basis of any details captured from the device.

Steps for Filtering the Hardware information –

1. Under Hardware information Tab, click **Filter Criteria** option.
2. This will extend the Filter Criteria Module on the interface.

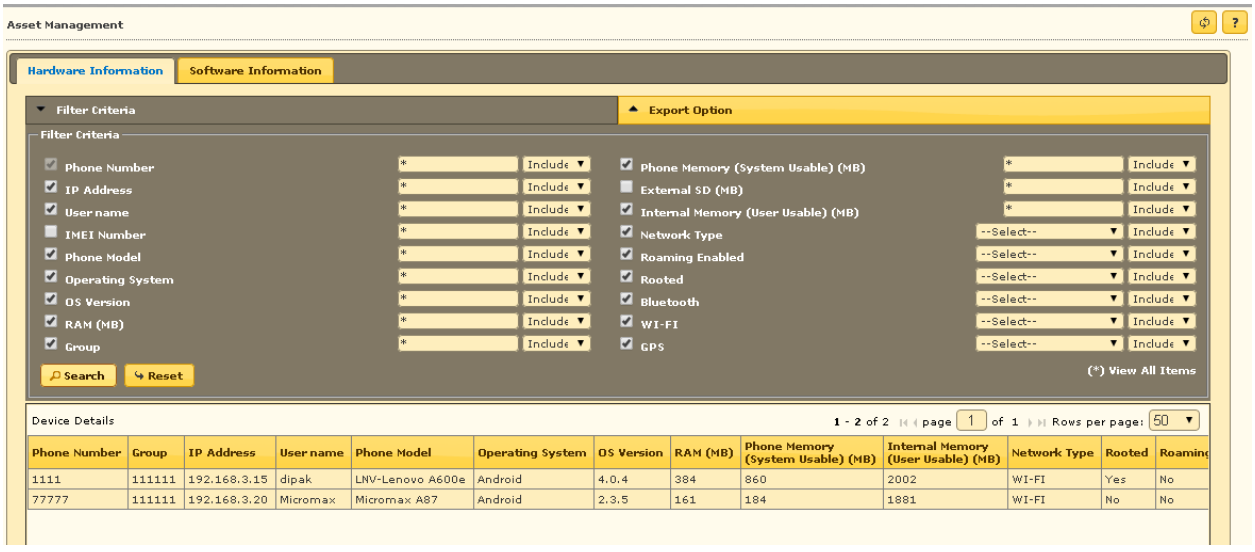


Figure 27.3

3. eScan facilitates filtering of the captured information on large number of criteria as shown in the above figure.
4. Based on your requirement, you can either include the selected criteria in your report or exclude them from the drop down.
5. Select the desired criteria using the respective fields and drop down present on the interface and click **Search** button present at the bottom of interface.
6. Details will be filtered in the table instantly.

Asset Management – Software Information

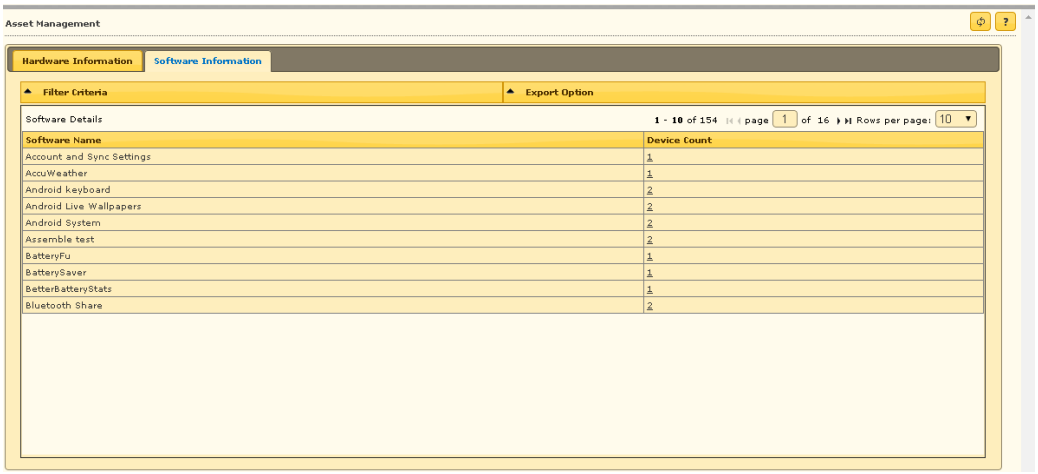


Figure 27.4

This tab displays the list of software installed on Managed devices as well as the device count for every installed software.

Asset Management – Software Information – Filter Criteria

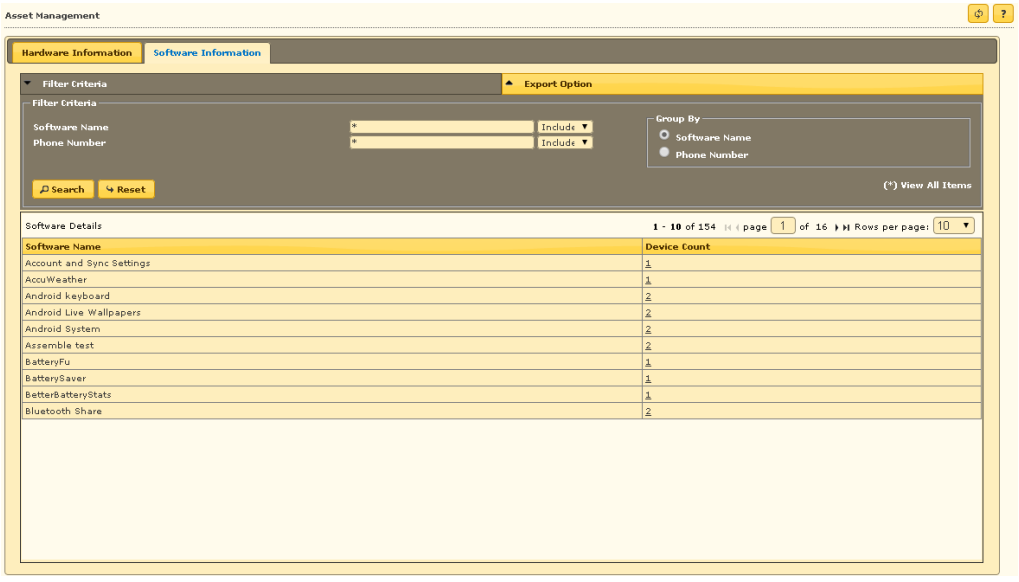


Figure 27.5

All the information captured from the devices can be filtered on the basis of including the software name or the Phone number associated with the device.

Asset Management – Export Options for the Generated Reports

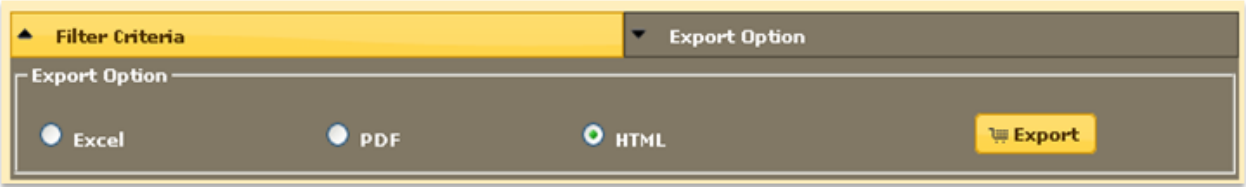


Figure 27.6

eScan's MDM supports export of All reports generated for the hardware as well as software inventory to **Excel**, **PDF** or **HTML** formats, as desired by you.

Steps for Exporting a Report

1. Click **Export** option present on the interface.
2. Now select the desired export option.
3. Click **Export** button present on the interface, report will be exported in the selected format and you will be informed through following message –

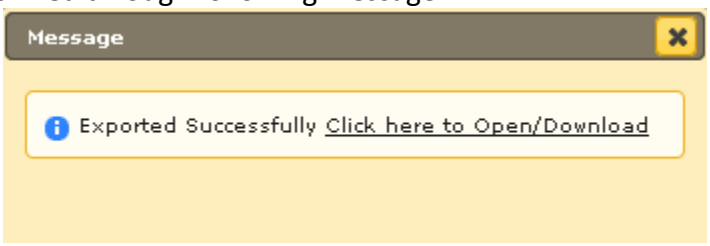


Figure 27.7

4. Click on the link to open/download the report in selected format.

28. Customizing and Scheduling Reports

28.1. Report Templates

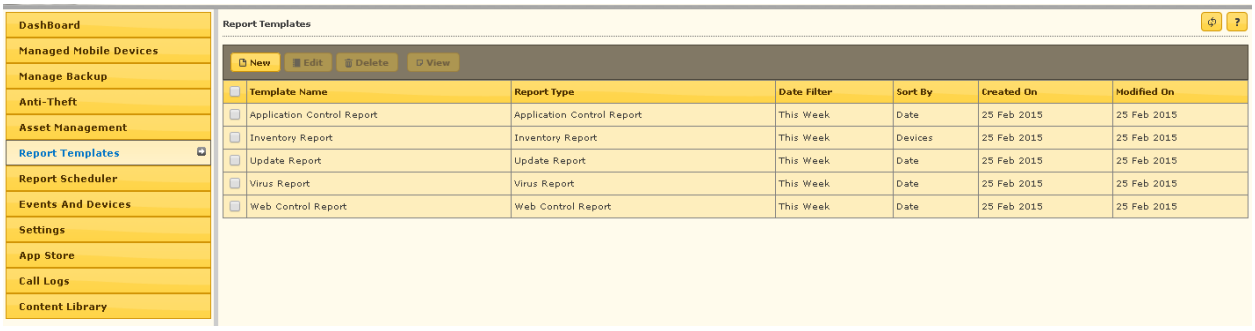


Figure 28.1

Using this Module you can generate / Edit (Customize) any pre-defined Report Template for any eScan Module. You can also create your own customized report template for desired period of time and for desired module.

Creating a New Report Template

Based on your requirement, select the desired Report Type for Creating a New Report Template.

Steps for Creating a New Report Template

1. Click **New** option present in Report Template Module of Mobile Device Management of eScan.
2. You will be forwarded to the **New Report Template** window, as shown below --

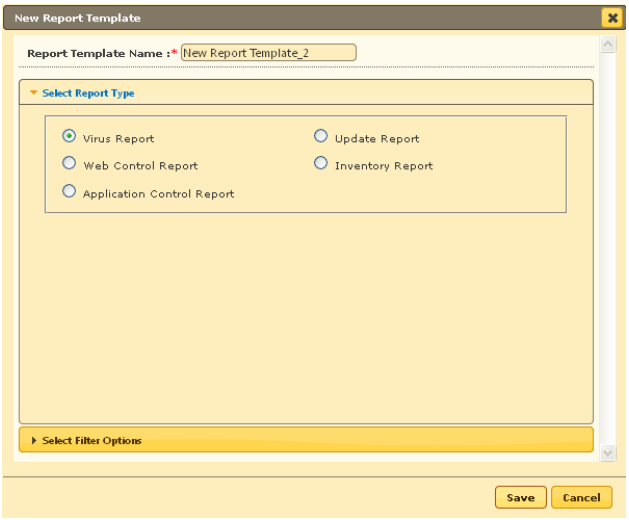


Figure 28.2

3. Type the desired Report Template Name in the respective field present on the interface.
4. Select the Report type that you wish to generate using the respective Radio buttons present on the interface under Select Report type section.
5. Select the **Filter** and **Sort** option using the respective Radio buttons and click **Save.**

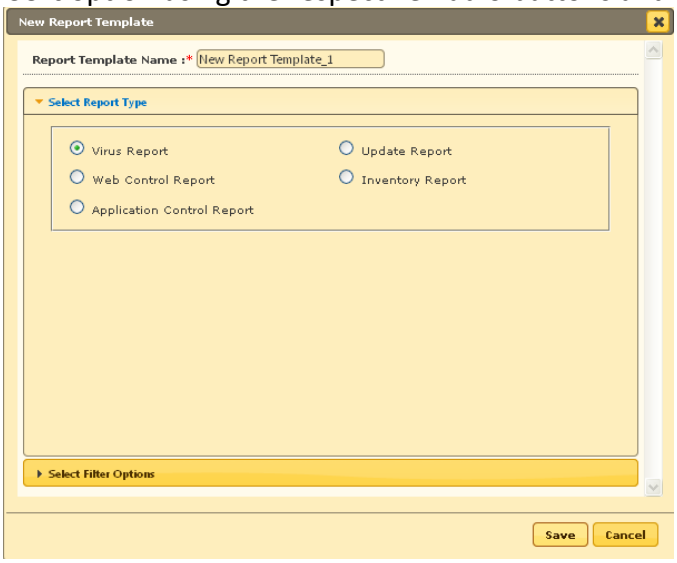


Figure 28.3

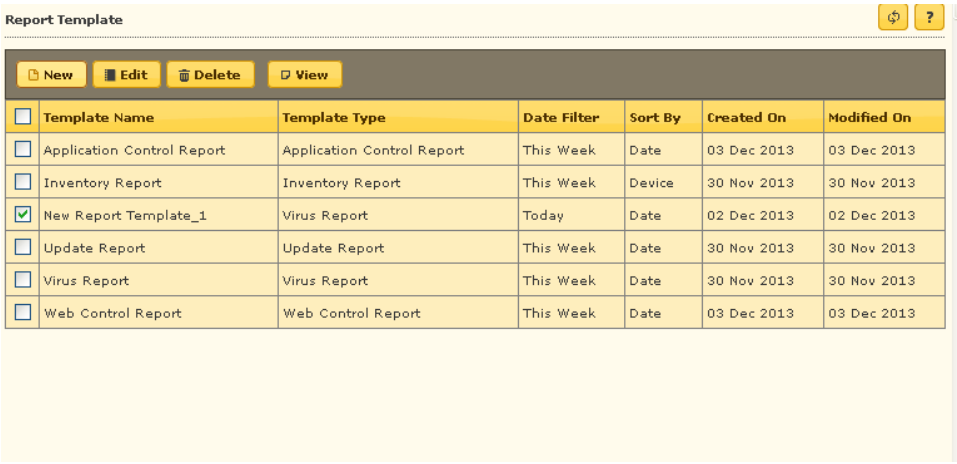
6. Report Template will be created instantly.

Editing an Existing Report Template

You can **Edit / Customize** any existing Report Template as per your requirement using the Edit option present on the interface, under Report Template module of eScan's Mobile Device Management.

Steps for Editing an Existing Report Template

1. Select the desired report template that you wish to Edit/Customize from the list using the respective checkbox, as shown below –



	Template Name	Template Type	Date Filter	Sort By	Created On	Modified On
☐	Application Control Report	Application Control Report	This Week	Date	03 Dec 2013	03 Dec 2013
☐	Inventory Report	Inventory Report	This Week	Device	30 Nov 2013	30 Nov 2013
☑	New Report Template_1	Virus Report	Today	Date	02 Dec 2013	02 Dec 2013
☐	Update Report	Update Report	This Week	Date	30 Nov 2013	30 Nov 2013
☐	Virus Report	Virus Report	This Week	Date	30 Nov 2013	30 Nov 2013
☐	Web Control Report	Web Control Report	This Week	Date	03 Dec 2013	03 Dec 2013

Figure 28.4

2. Now click **Edit** button present at the top of interface. You will be forwarded to **Edit Report Template** Window.
3. Make desired changes and click **Save**.

Viewing a Report

You can View the results captured in the report by selecting the Report and then click on View option present on the top of Report Template module. Results of the selected report will be displayed, as shown below –

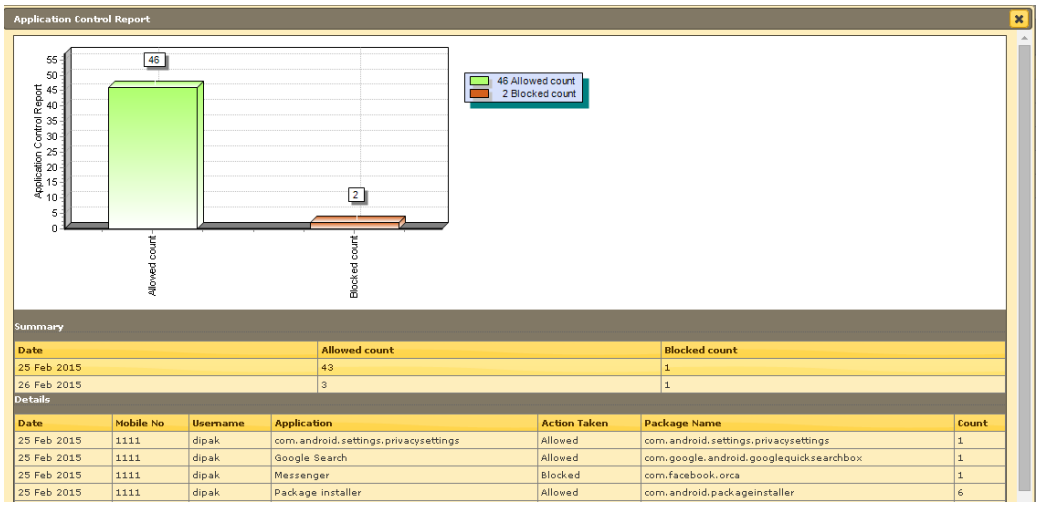


Figure 28.5

Deleting a Report Template

Select the Report Template that you wish to delete using the respective checkbox and click **Delete**.

29. Report Scheduler

Creating a Report Schedule

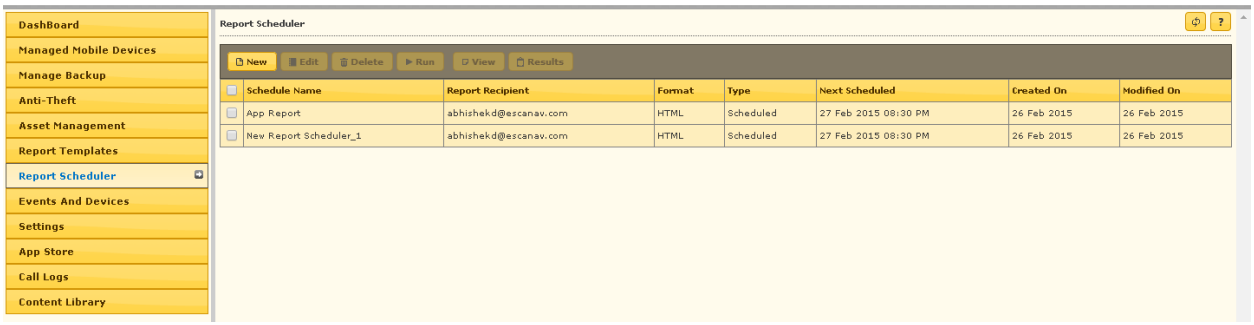


Figure 29.1

Following options will be displayed

Sr.No.	Options	Description
1.	New	Use this option create a New Report Schedule
2.	Edit	Use this option to Edit an Existing Report Schedule
3.	Delete	Use this option to delete an existing Report Schedule
4.	Run	Use this option to Run an already created Report schedule
5.	View	Use this option to View an already created Report Schedule
6.	Result	Use this option to view results of previously deployed report schedule

Steps for Creating a New Report Schedule

1. Click **New**.
2. Select the desired report templates that you wish to schedule and Filter the criteria, as shown below --

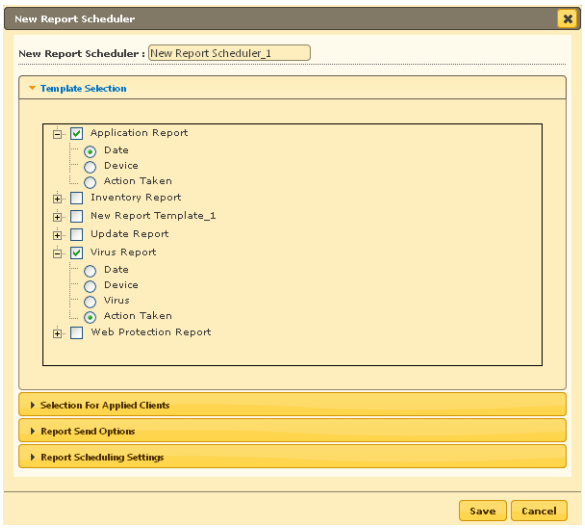


Figure 29.2

3. Select the **Groups or Devices** for which you wish to Schedule the Report.

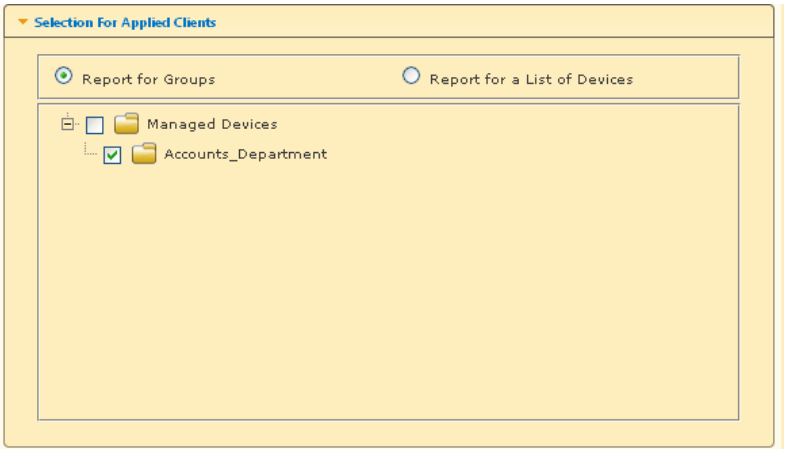


Figure 29.3

4. Configure the options for Sending the Report on Email using **Report Send Options**.
5. Also select the Format for sending the Report on Mail. Excel, HTML and PDF formats are supported.

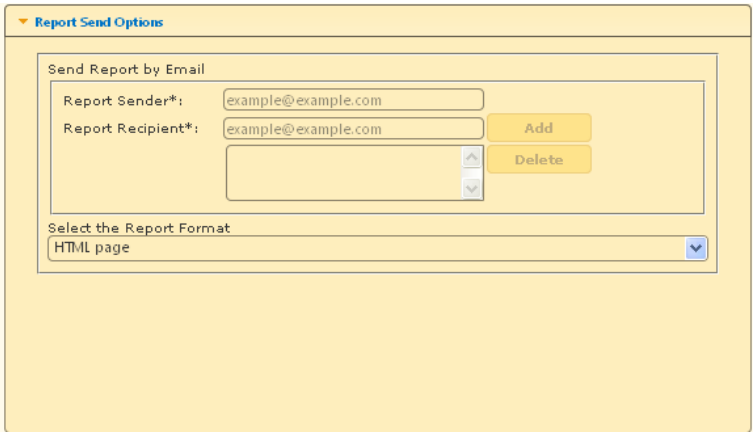


Figure 29.4

6. Schedule the report as per your requirement and click **Save**.

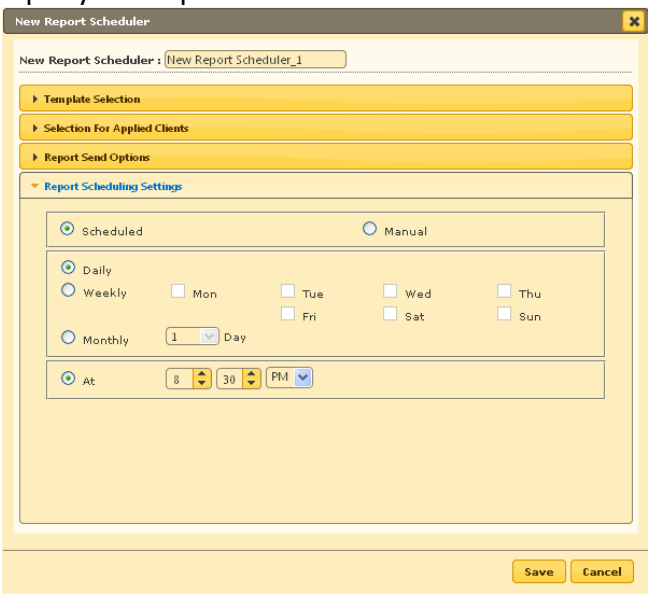


Figure 29.5

7. Report Schedule will be created instantly.
8. Select the Report Schedule and click **Run** to manually run the Created Report Schedule.

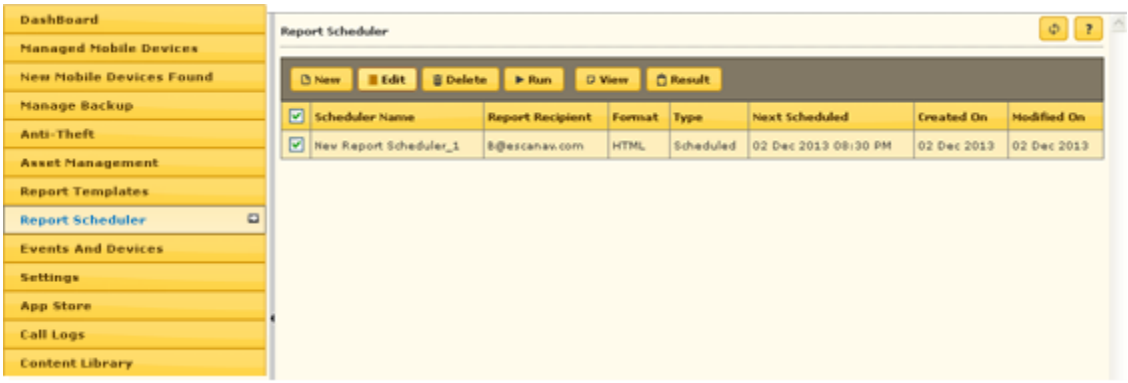


Figure 29.6

9. You can View the Data of the Report by clicking **View** button present on the interface.

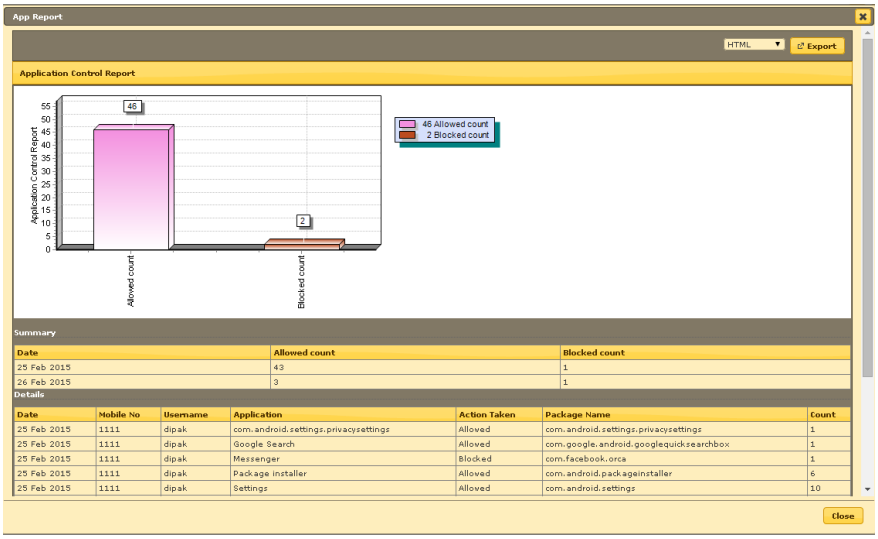


Figure 29.7

10. To View the Status of Scheduled Report click **Result**.

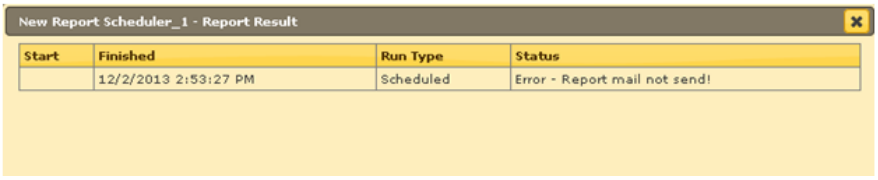


Figure 29.8

30. Events and Devices

30.1. Viewing Events

Events captured from the devices are categorized and displayed in this module. This will give a real – time status of security and eScan update on all the devices.

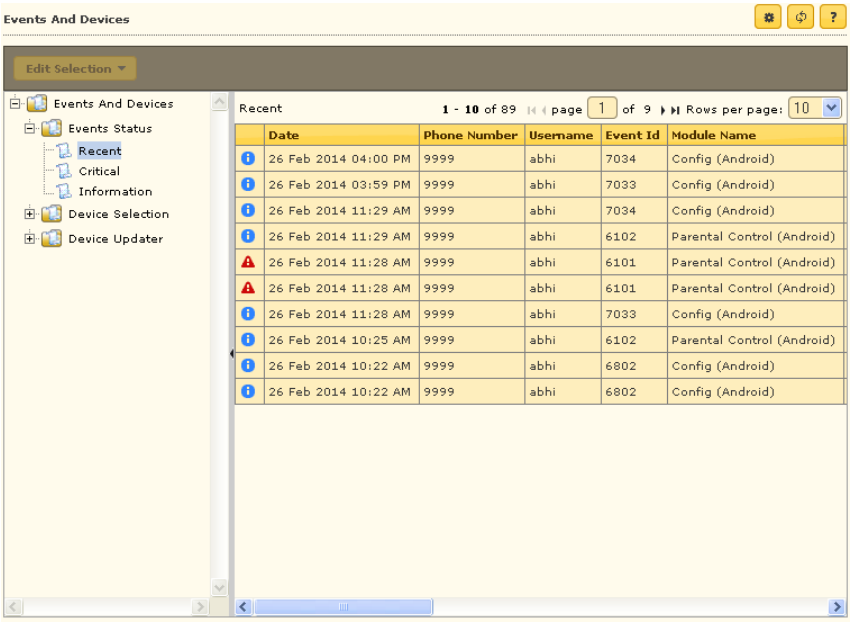


Figure 30.1

Types of Event Status

On the basis of severity, that is, the level of importance, events are categorized in to the following three types.

- **Recent**: It displays both critical and information events that occurred recently on managed devices
- **Critical**: It displays all critical events occurred on managed devices, such as virus detection, monitor disabled status etc.
- **Information**: It displays all informative type of events, such as virus database update, status.

Device Selection

The **Device Selection** tab enables you to select and save the computer status settings. This module enables you to do the following activities:

Define Criteria's for Filtering of Device Status on the basis of following-

- Device with the "Critical Status"
- Device with the "Warning Status"
- Database are Outdated
- Many viruses Detected
- Not connected for a long time
- Not scanned for a long time
- Protection off

Hardware / Software Updates

Capture Events on the basis of Software Changes, Hardware Changes or existing Device Information.

Type of Updates

The lists of updates are as follows:

- Software Changes: It displays the list of managed devices on which software related changes are made. For example, Installation/Uninstallation of other software.
- Hardware Changes: It displays the list of managed devices on which hardware related changes are made.

Events and Devices settings

Defining Settings for Events and Devices

Event Status: You can define settings for the Events and Devices for Event Status, Device Selection, as well as Hardware and Software changes. By defining these settings you can define number of Records to show for Events, capture events, Information related to Events for Hardware and Software Changes for desired number of days and desired number of records to show.

Device Selection: The following actions can be performed using this option.

Option	Description
Check for Monitor Status	Select this check box if you wish to generate Events related to eScan Monitor enable/ disable status on managed devices.
Check for Not Scanned	Select this check box if you want to view the list of devices which has not been scanned.
Check for Database Not Updated	Select this check box if you want to view the list of devices on which database has not been updated.
Check for Not Connected	Select this check box if you want to view the list of devices that have not communicated with eScan MDM server.

- Existing System Info: It displays device information of the existing devices.

Events and Devices settings

The Software/Hardware changes: The following actions can be performed using this option

Field	Description
Software/Hardware Changes	Select from the drop down to generate Events related to the selected option.
Number of Days	Type the number of days, to view changes made within the specified days. For example, if you have typed 2 days, then you can view the list of devices on which any software/hardware changes have been made in the last 2 days.
Number of Records	Type the number of devices that you want to view in the list.

31. Settings

Using this module, you can Save Server details for sending Email notifications to the Device user email addresses.

Figure 31.1

32. App Store

Using the App Store you can **Add** apps that will be of use to the Mobile Device users accessing your network. After adding the apps to the App Store you can push these apps to the managed devices through policy deployment.

For more information on Policy Deployment, click here

Steps for adding an App to the App store

1. Click **Add** under the App Store module of eScan's Mobile Device Management Console.

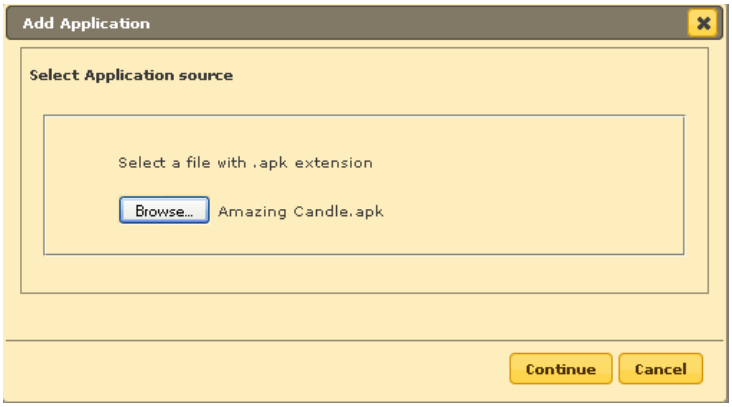


Figure 32.1

2. Now **browse** the path where the .apk file for the app is saved and click **Continue**.
3. You will be forwarded to the **Edit Application** window, write a brief description for the App and click **Save**.

Figure 32.2

4. The App will be added in the store instantly.

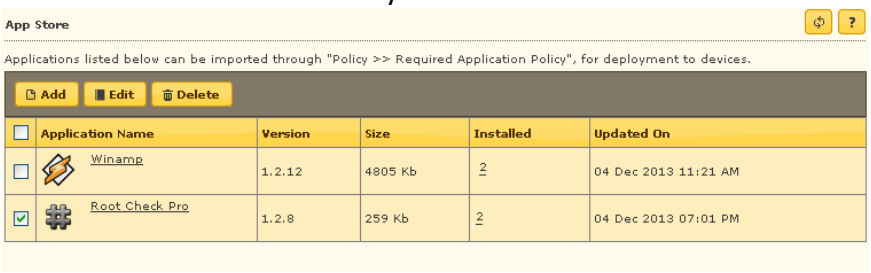


Figure 32.3

5. Click on the Numeric Value present in Installed Column to view the list of devices where the application is installed, initially before policy deployment it will be 0. If the app with the same version number is installed on the devices the count will be shown accordingly.

33. Call Logs

33.1. Call Logs

Allows you to maintain incoming as well as Outgoing Call logs of all enrolled endpoints along with the call duration in hours, minutes and seconds format.

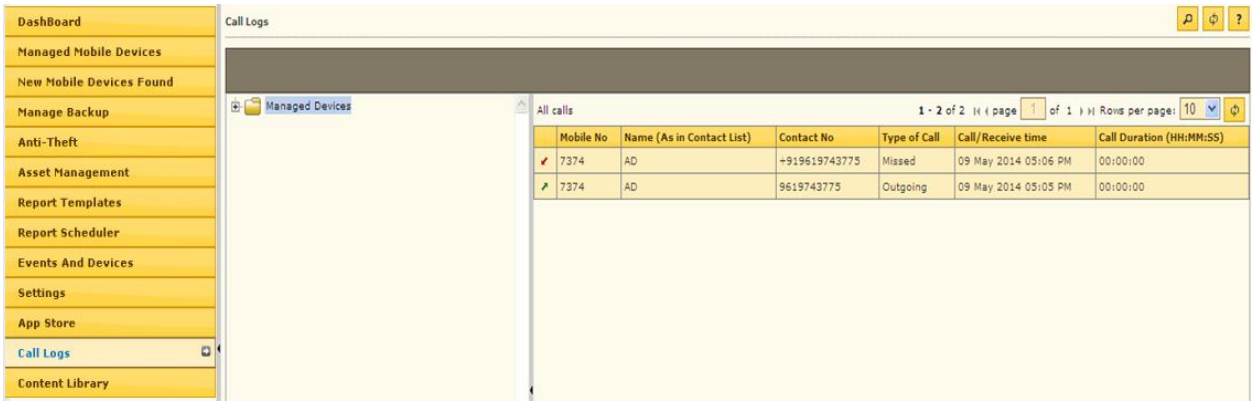


Figure 33.1

This module will display the list of all the incoming and outgoing calls.

It will display the following details

Sr. No.	Captured Information	Description
1	Mobile no.	It will display the managed Mobile Device number
2	Name (As in Contact List)	It will display the name of the Contact as in the contact list of the managed device.
3	Contact No.	The Contact number to which the call was made or the call was received from.
4	Type of Call	It will display whether the call was incoming or outgoing.
5	Call/ Receive time	It will display the specific time when the call was made or received.
6	Call Duration	It will display the time duration of each call (incoming and outgoing) of the managed mobile device.

34. Content Library

34.1 Content Library

This will allow the administrator to deploy documents through the web console. The document types that can be deployed are .PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, TXT, JPG, JPEG, PNG, and BMP. This feature is used by the administrator to share any kind of information.

Steps for adding a document to the App store

1. Click **Add** under the content Library module of eScan's Mobile Device Management Console.

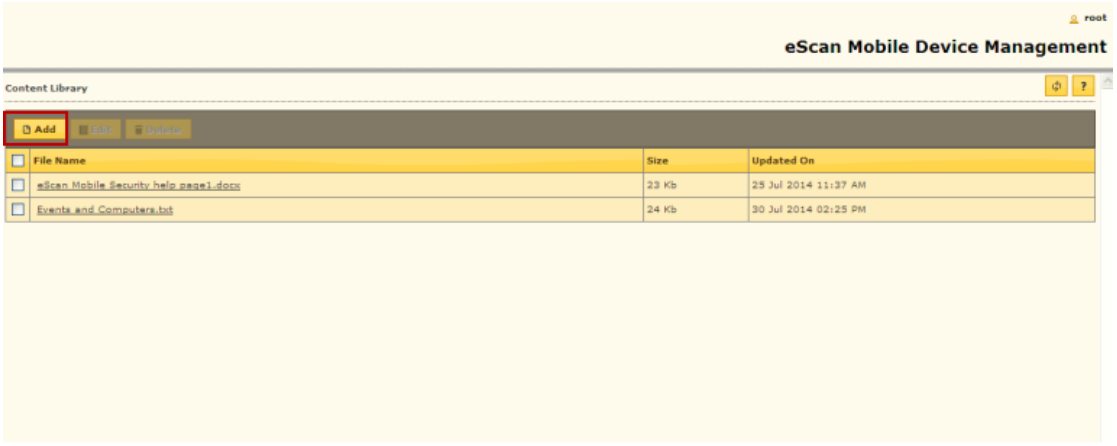


Figure 34.1

2. Now **browse** the path where the file is saved and click **Continue**.

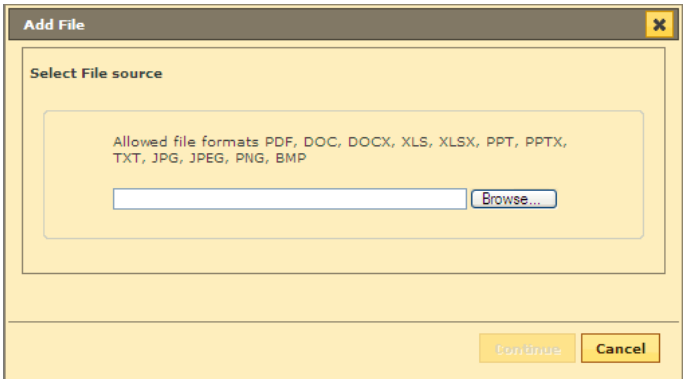


Figure 34.2

3. You will be forwarded to the next window, write a brief description for the document and click **Save**.

35. Getting started with eScan Mobile Security

35.1 Introduction

eScan Mobile Security is specifically designed for Android devices. It helps you secure and protect smart phones and tablet connected to your network against viruses, malwares, Trojans, and secures enterprise data accessed from devices.

It enables you to white list/black list contacts and messages, backup/restore contacts and messages, blocks applications and websites, which ensure security to the devices.

Downloading and Enrolling eScan Mobile Security

As first step for enrolling the device, the administrator has to add device details to the MDM console. Once the details of the device is added to the MDM Console by the administrator, an email is automatically sent to the user's email address with a link to download eScan Mobile security on devices along with mandatory user details required for enrolling the device, the details include, Mobile Number, Server, Port number and country.

It is mandatory for the user to have internet connection on the device for downloading eScan and completing the enrollment process.

Enrolment Process

Enrolment process consist of following steps –

1. Download the .apk from the download link received on your email address.
2. Install eScan Mobile Security on the device.
3. Open eScan Mobile Security and enroll the device on MDM server by filling up Enrollment details on the device.

You can fill up the form using any of the following two procedures

- **Filling enrollment details manually**
- **Automatically filling enrollment details using QR code received in enrollment mail**

  The QR code contains user information filled by the administrator at the time of adding the device on MDM console.
  You are required to fill the same information in the Enrollment Details form from the device for enrolling the device on eScan MDM server.

Steps for filling enrollment details through QR Code

1. Open eScan Mobile Security on device after installation.
2. Enrollment Details form will open on the device, Tap on **Fill entries through QR Code**.
3. Now focus the camera towards the QR Code received in the enrollment email on your computer.
4. The Enrollment details form will automatically be filled with all the mandatory details encrypted in the QR Code.
5. Tap on Enroll Device button present at the bottom of the interface.

Steps for filling information manually

1. Open eScan Mobile Security on device after installation.
2. Enrollment Details form will open on the device.
3. Now fill in the Enrollment details form with the mandatory (*marked) details received in the enrollment email sent by the administrator.
4. Tap on **Enroll Device** button present at the bottom of the interface.
5. The device will be enrolled instantly and you will be forwarded to the Device Administrator pop up message.
6. Tap on Next button to activate device administrator permission to enable Anti-theft, Parental Control and Uninstall Protection features on the device.
7. You will be forwarded to the information window for activating device administrator. Tap on **Activate** button present at the bottom of the interface or Tap on **Cancel** to cancel the activation.
   The device will be enrolled to the MDM Server

eScan Mobile security

The following are the modules /options present on screen on the mobile interface.

- **Administrator Mode:** This will allow you to change the settings from your mobile device once you input the correct password provided on the server. Without the password you will have only a ready-only access to all the modules and won't be able to make any changes to the already defined settings.

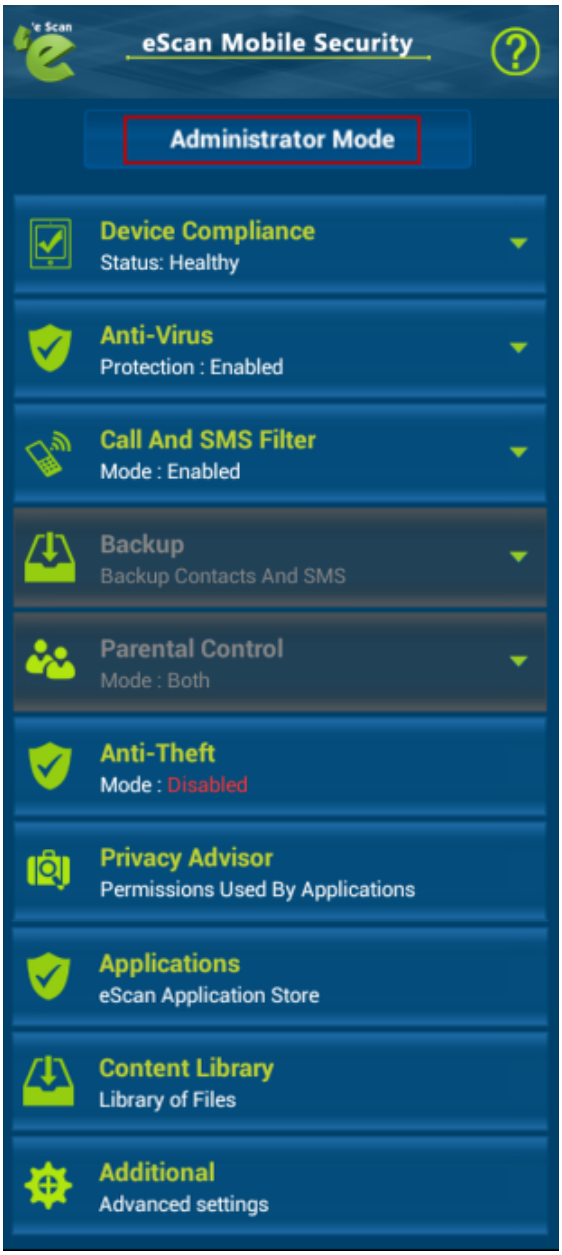


Figure 33.1

- **Device Compliance:** This will portray the compliance status of the device as healthy or non-compliant. The device is set to healthy or non- compliant based on the policies defined on the server.

Figure 33.2

- **Anti-Virus:** A real-time scanning and protection against viruses, infections, and other threats.

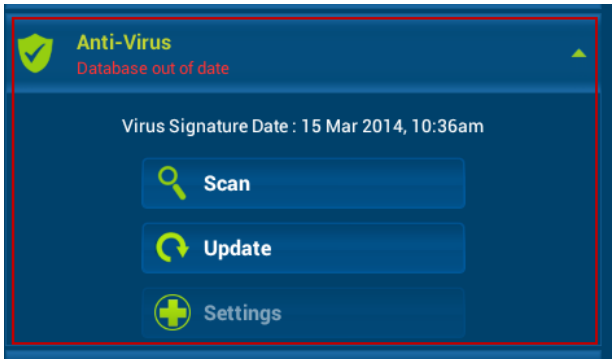


Figure 33.3

- **Call And SMS Filter:** This will allow you to filter incoming Calls and SMS on the basis of black list and whitelist created by you. This will also allow you to filter the Outgoing calls based on the white list created by you.

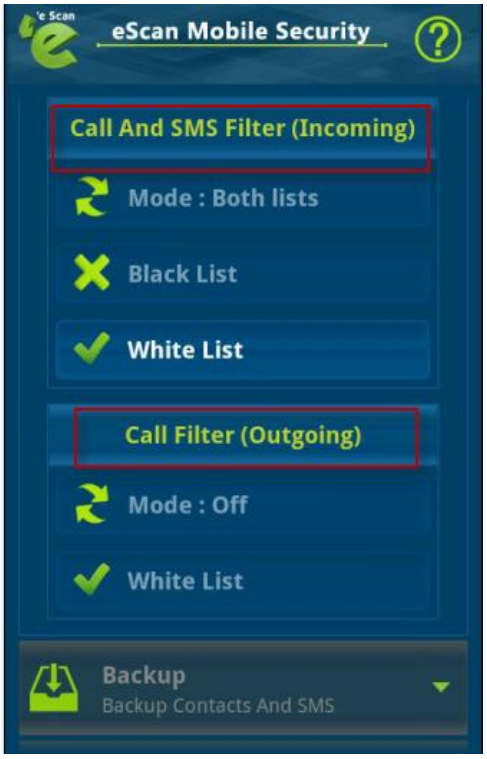


Figure 33.4

- **Backup:** This will allow you to take a backup of contacts and SMS, restore contacts and SMS and will also maintain the log for all the activities carried out.

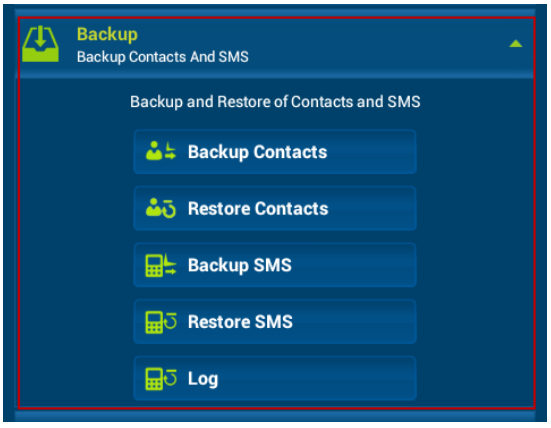


Figure 33.5

- **Parental Control:** Allowing and blocking specific websites and applications.

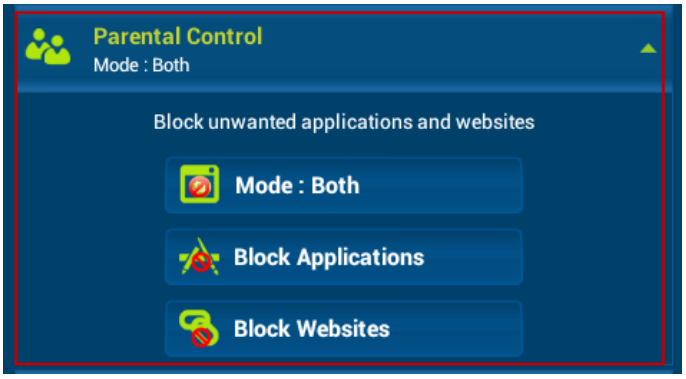


Figure 33.6

- **Anti-theft** – This section helps the user to trace, Lock, or Wipe the Data on Tablet through an online profile in case of a lost or theft of the device.

Figure 33.7

- **Privacy Advisor:** This section displays the list of applications installed on the Tablet along with the permissions used by them.

Figure 33.8

- **Applications:** You can download new apps from the app store and also displays the list of downloaded apps.

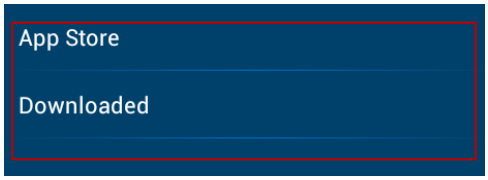


Figure 33.9

- **Content Library:** This will display the documents the administrator shared through the Mobile Device Management console. It will also allow the user to download the documents from here.

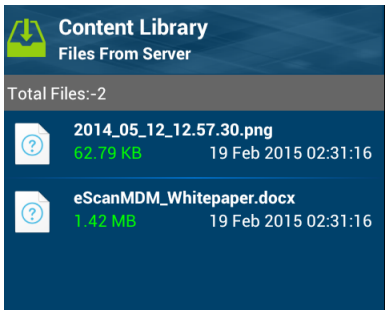


Figure 33.10

- **Additional:** Configuring additional advanced settings.

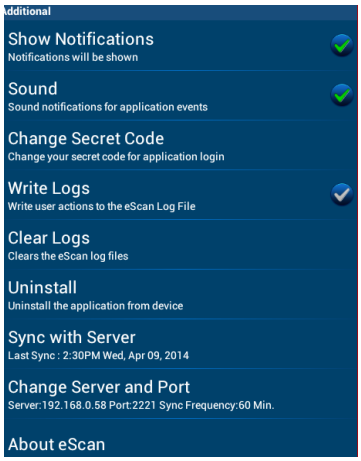


Figure 33.11

36. Contact Details

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

- **Chat Support**

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

  http://www.escanav.com/english/livechat.asp

- **Forums Support**

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

- **E-mail Support**

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

37. Registered Offices

Asia Pacific MicroWorld Software Services Pvt. Ltd. Plot No 80, Road 15, MIDC, Marol, Andheri (E), Mumbai, India Tel : (91) (22) 2826-5701 Fax: (91) (22) 2830-4750 E-mail : **sales@escanav.com** Web site: **http://www.escanav.com**
Malaysia MicroWorld Technologies Sdn.Bhd. (Co.No. 722338-A, E-8-6, Megan Avenue 1, 189, Jalan Tun Razak, 50400 Kuala Lumpur, Malaysia Tel : (603) 2333-8909 or (603) 2333-8910 Fax: (603) 2333-8911 E-mail : **sales@escanav.com** Web site: **http://www.escanav.com**
South Africa MicroWorld Technologies South Africa (PTY) Ltd. 376 Oak Avenue Block C (Entrance from 372 Oak Avenue) Ferndale, Randburg, Gauteng, South Africa Tel : Local 08610 eScan (37226) Fax: (086) 502 0482 International : (27) (11) 781-4235 E-mail : **sales@microworld.co.za** Web site: **http://www.microworld.co.za**
USA MicroWorld Technologies Inc. 31700 W 13 Mile Rd, Ste 98, Farmington Hills, MI 48334, USA Tel : (1) (248) 855 2020 Fax: (1) (248) 855 2024 E-mail : **sales@escanav.com** Web site: **http://www.escanav.com**
Germany MicroWorld Technologies GmbH Drosselweg 1, 76327 Pfinztal, Germany Tel : (49) 7240 944909 20 Fax: (49) 7240 944909 92 E-mail : **sales@escanav.de** Web site: **http://www.escanav.de**