

eScanTM

Anti-Virus & Content Security

eScan Endpoint Security (with MDM & Hybrid Network Support) **User Guide**

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

Document Number: 5BUG/23.06.2014/14.1

Current Software Version: 14.1

Copyright Notice: Copyright © 2014. All rights reserved.

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

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

Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of MicroWorld.

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

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

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

Technical Support:	support@escanav.com
Sales:	sales@escanav.com
Forums:	http://forums.escanav.com
eScan Wiki:	http://www.escanav.com/wiki
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld
Date:	June, 2014

Table of Contents

1. eScan Management Console	4
2. Pre-requisites for eScan Server.....	5
3. System Requirements	6
4. Installing eScan Endpoint Security Server	7
5. Components of eScan Server.....	16
6. User Interface of eScan Management Console	17
7. Managed Computers	34
8. Managing Installations.....	51
9. Managing Policies and Tasks for the Group	75
10. Managing Tasks and Policies for Specific Computers.....	91
11. Managing and Scheduling Reports	97
12. Asset Management	100
13. Print Activity.....	104
14. Defining Settings	109
15. Export and Import Settings	115
16. Managing Licenses	118
17. Introduction - eScan Mobile Device Management.....	121
18. Getting started with eScan Mobile Device Management	127
19. Working with eScan Mobile Device Management Console	129
20. Backup Management	146
21. Lost Device Protection through Anti-Theft.....	148
22. Mobile Endpoints- Asset Management	150
23. Customizing and Scheduling Reports.....	155
24. Report Scheduler	159
25. Events and Devices	163
26. Settings.....	165
27. App Store	166
28. Getting started with eScan Mobile Security.....	168
29. Contact Details.....	174
30. Registered Offices.....	175

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 has Windows, Mac or Linux Operating System.
- Create and Manage policies or tasks for computers on your network.
- 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.
- 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:

- | |
|---|
| <ul style="list-style-type: none">• You require a user name and password to send emails, if authentication for the mail server is mandatory for accepting emails. |
|---|

3. System Requirements

Windows	Linux	Mac	Android
<ul style="list-style-type: none"> (Windows server & workstations) Platforms Supported <p>Microsoft® Windows® 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)</p>	<ul style="list-style-type: none"> (Linux Endpoints) Platforms Supported <p>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)</p>	<ul style="list-style-type: none"> (Mac Endpoints) Platforms Supported <p>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</p>	<p>(Android Endpoints) Platforms Supported</p> <p>Android Version 2.2 & above</p>
<p>Hardware for Clients and Server (Server) CPU - 2GHz Intel™ Core™ Duo processor or equivalent. Memory - 4 GB & above Disk Space – 8 GB & above</p> <p>(Endpoints) 1.4 Ghz minimum (2.0 Ghz recommended) Intel Pentium or equivalent 1.0 GB minimum (1.5GB recommended) Disk Space – 800 MB and more</p>	<p>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</p>	<p>Hardware Requirements (Endpoints) CPU - Intel based Macintosh Memory – 1 GB and More recommended Disk Space – 500 MB and above</p>	<p>Hardware Requirements (Endpoints) Android 2.2 & above devices</p>
<p>eScan Console can be accessed by using below browsers:</p> <p>Internet Explorer 7 / 8 / 9 / 10 Firefox 14 & above Google Chrome latest version</p>			

4. Installing eScan Endpoint Security Server

- **Installing eScan from CD/DVD**

Installing eScan Endpoint Security for Windows 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 Ewn2ksmk.exe on CD Rom, this will open the wizard based setup of eScan Endpoint Security for Windows on your computer. To complete the installation follow the instructions on screen. Denote

- **Downloading and installing eScan Endpoint Security 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 Ewn2ksmk.exe and follow the instructions on screen to complete the installation process.

Note: Before deploying eScan on any endpoint where any third party antivirus is already installed, please make sure to exclude following folders of eScan from real time scanning -

- For 32 bit computer - C:\Program Files\eScan
C:\Program Files\Common Files\Microworld
- For 64 bit Computer - C:\Program Files(x86)\eScan
C:\Program Files\Common Files(x86)\Microworld

- **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**

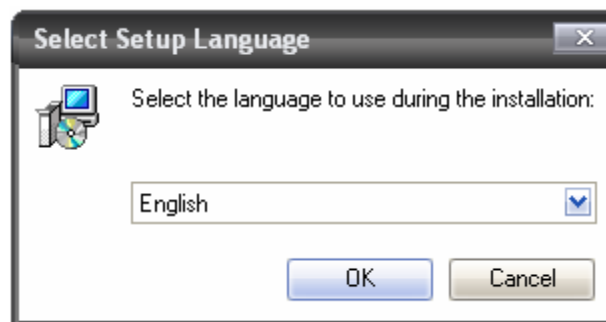


Figure 4.1

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 only English and Japanese.

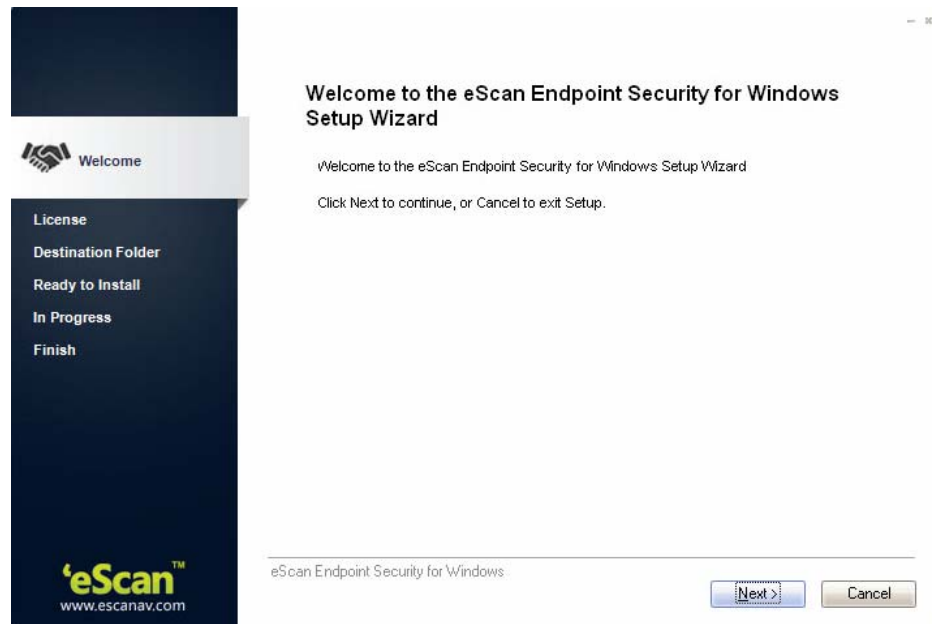


Figure 4.2

- **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.

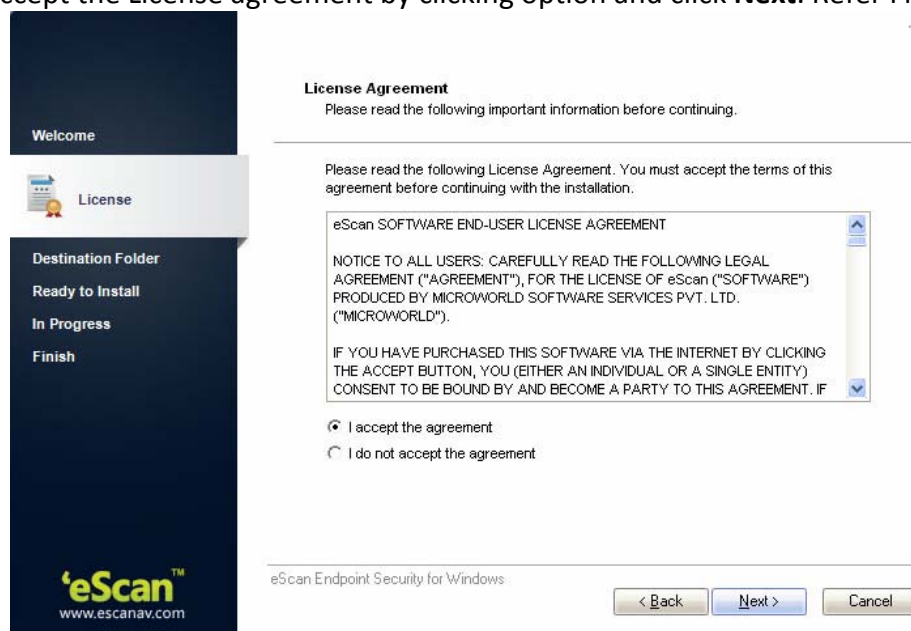


Figure 4.3

- **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

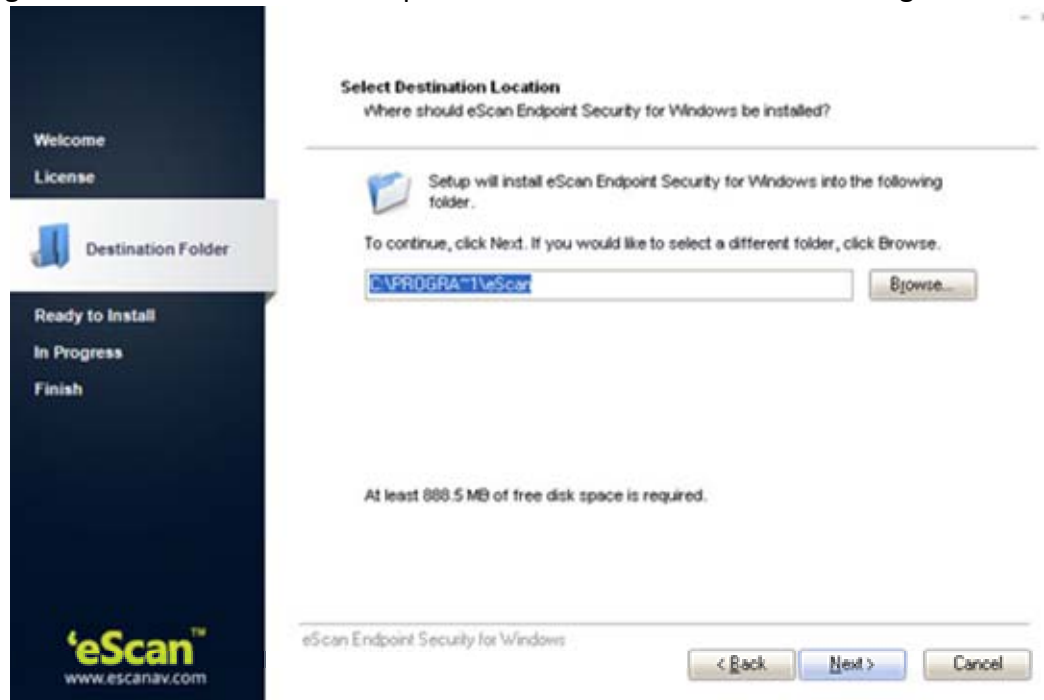


Figure 4.4

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

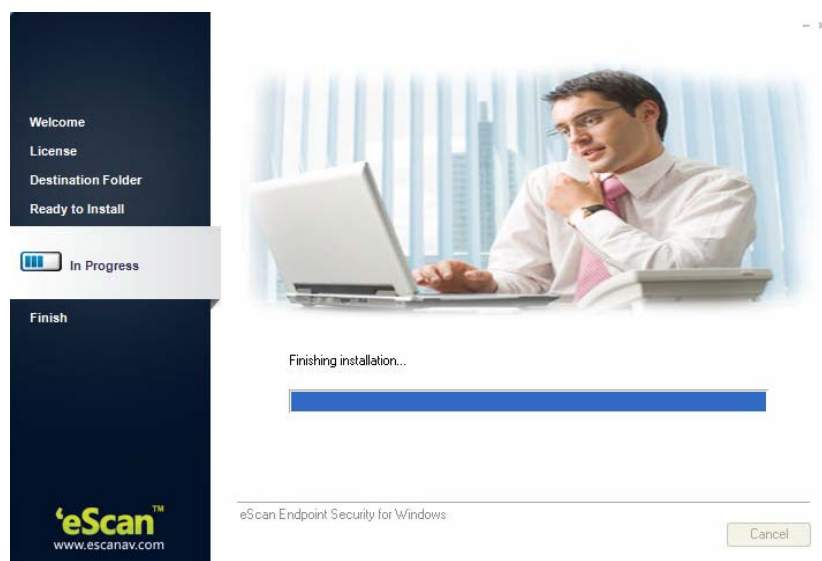


Figure 4.6

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

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

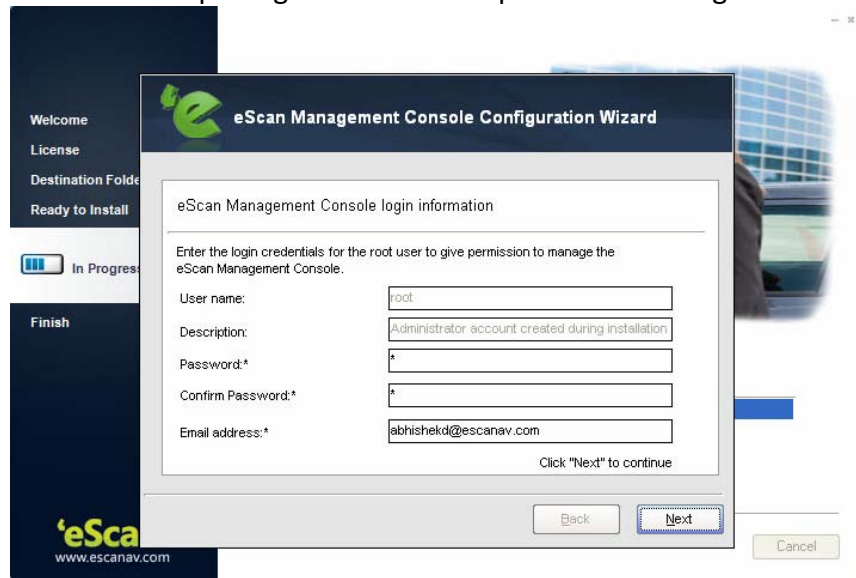


Figure 4.7

- **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

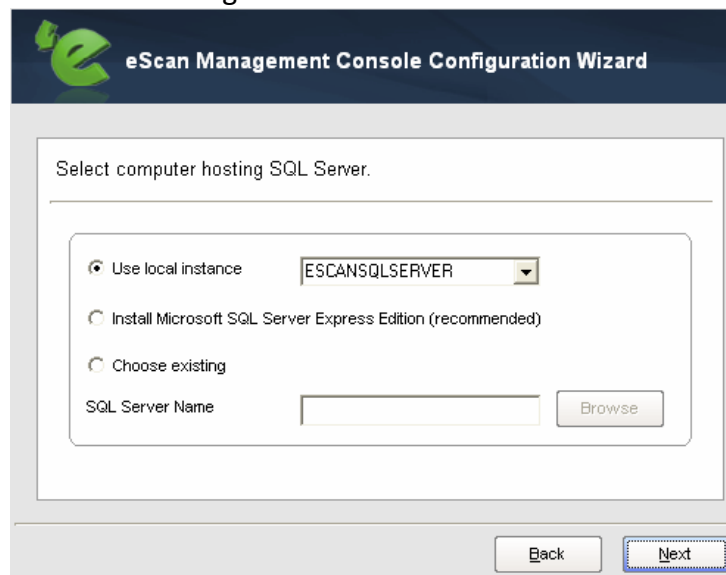


Figure 4.8

Options	Description
Use Local Instance	[Radio button] Use the drop down to select the desired instance for Hosting the SQL Server. It displays a list of 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. 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.

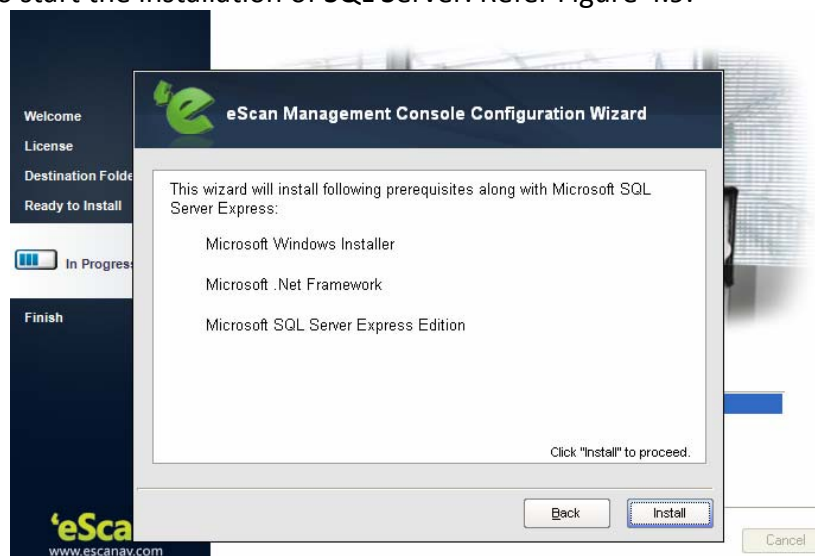


Figure 4.9

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

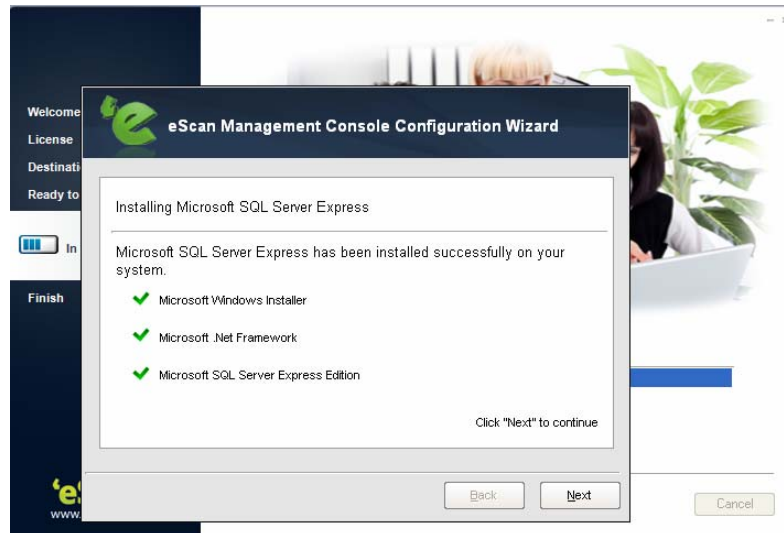


Figure 4.10

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.

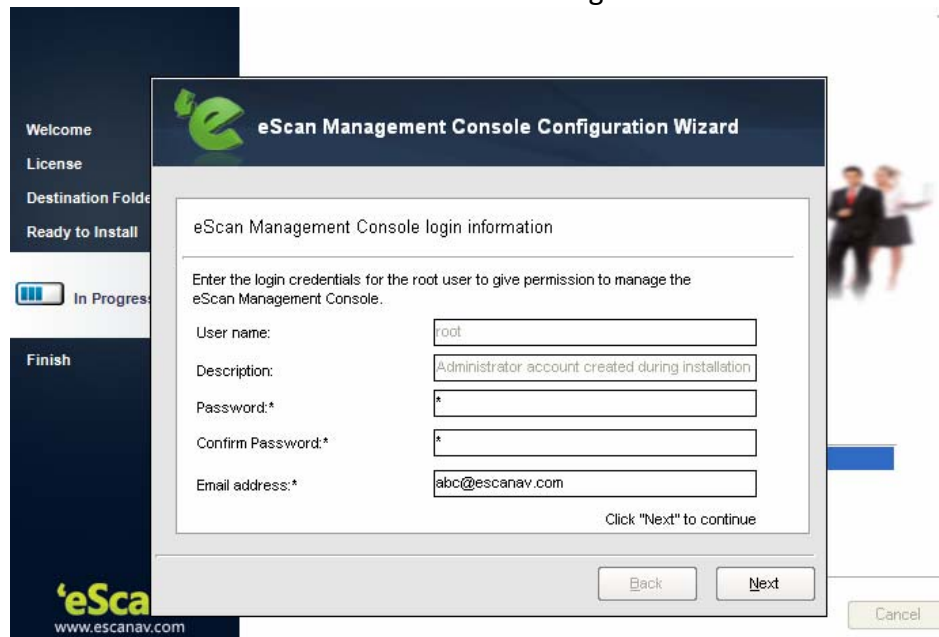


Figure 4.11

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

For completing the Configuration of eScan Management Console, click Finish. It will start installing the necessary files as per the configuration being done, It will take few minutes to complete with the installation. **Refer Figure 4.12**



Figure 4.12

Once the scanning is complete or the scanning is cancelled, you will be forwarded to the **Finish** window. Click **Finish** to complete the installation process.

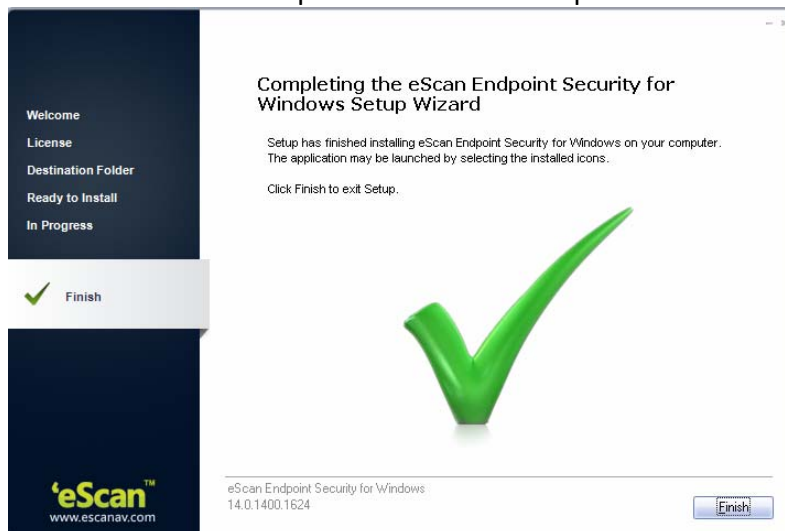


Figure 4.13

Note:

- eScan Endpoint security client as well as server can be installed on any computer where any other antivirus software is already installed.

5. Components of eScan Server

The eScan Server comprises the following components.

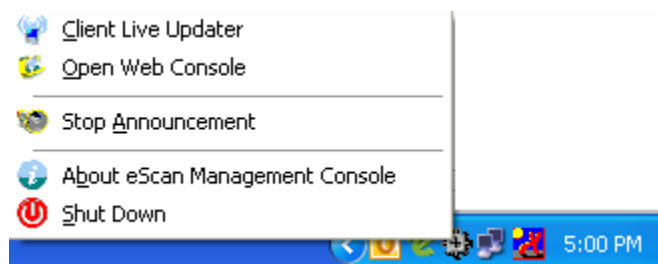
- **eScan Server** - This is a core component which allows you to manage, deploy and configure eScan on Endpoints. It stores the configuration information and log files about the Endpoints which are present in the network. It also communicates with other components mentioned below.
- **Agent** – It manages 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 Endpoint Security to Login to the **eScan Management Console**. Refer **Figure 6.1**

WEB CONSOLE LOGIN

Please type your User name and Password to access the Web Console.

User name:
For Active Directory account: domain\username

Password:

You can provide users the following link(s):

eScan Client Setup [+]
http://DANNY:10443/Setup/eScan_Client.exe

eScan Agent Setup (Windows) [+]
http://DANNY:10443/Setup/Agent_Setup.exe

eScan Agent Setup (Linux) [-]
http://DANNY:10443/Setup/Agent_Setup.deb
http://192.168.0.60:10443/Setup/Agent_Setup.deb
http://DANNY:10443/Setup/Agent_Setup.rpm
http://192.168.0.60:10443/Setup/Agent_Setup.rpm

eScan Agent Setup (MAC) [-]
http://DANNY:10443/Setup/Agent_Setup.dmg
http://192.168.0.60:10443/Setup/Agent_Setup.dmg

Copyright © 2010 MicroWorld Technologies Inc. All rights reserved.

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

	<p>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.</p>
<p>eScan Agent Setup Link</p>	<p>[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.</p>

- Main Interface - eScan Management Console - Refer Figure 6.2

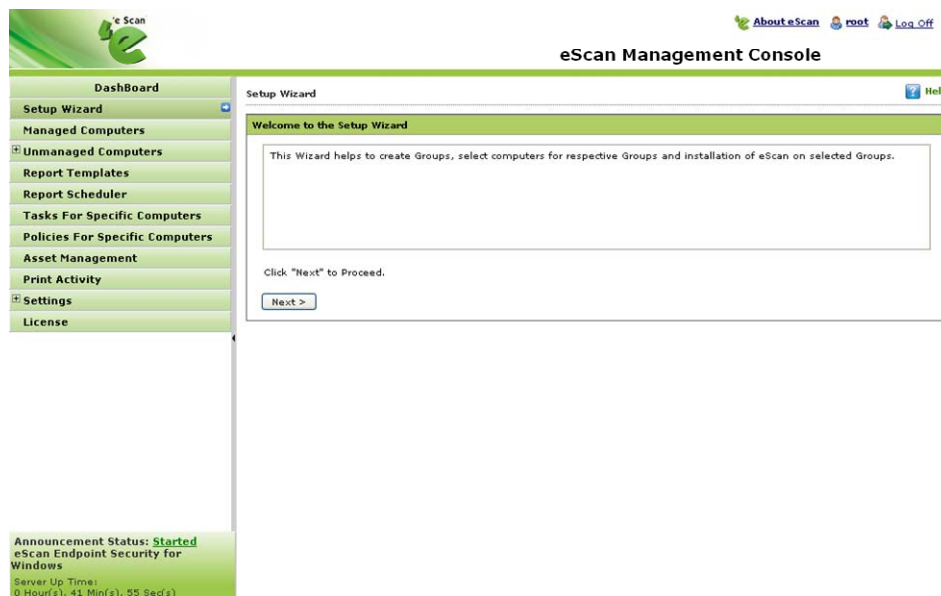





Figure 6.2

Note:

➡ Icons on every status Label denotes 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.
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. **Refer - Figure 6.3**

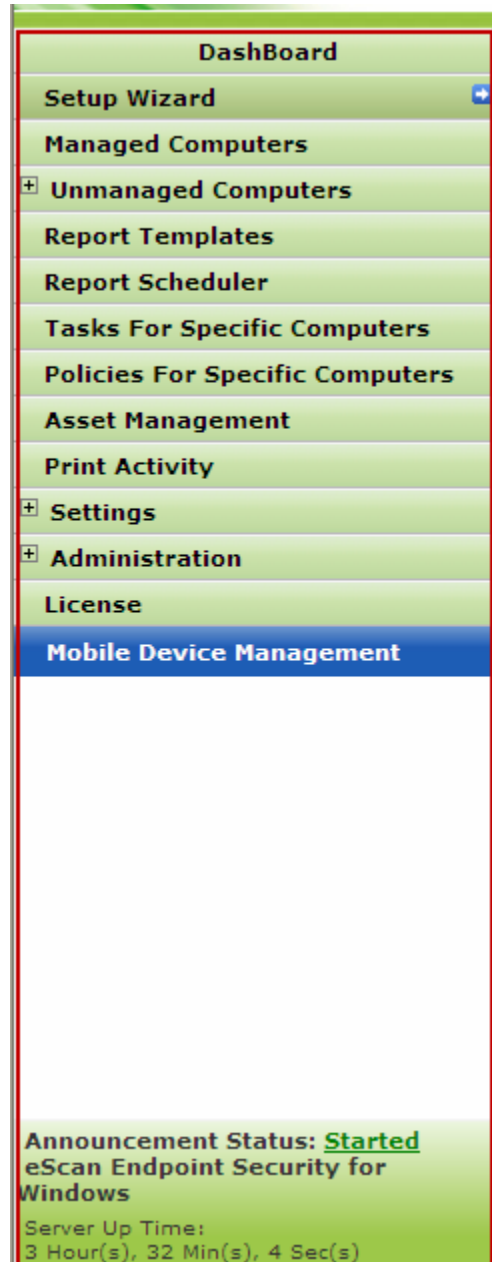


Figure 6.3

- **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 Web protection and application control. For [more details click here](#). Refer - Figure 6.4

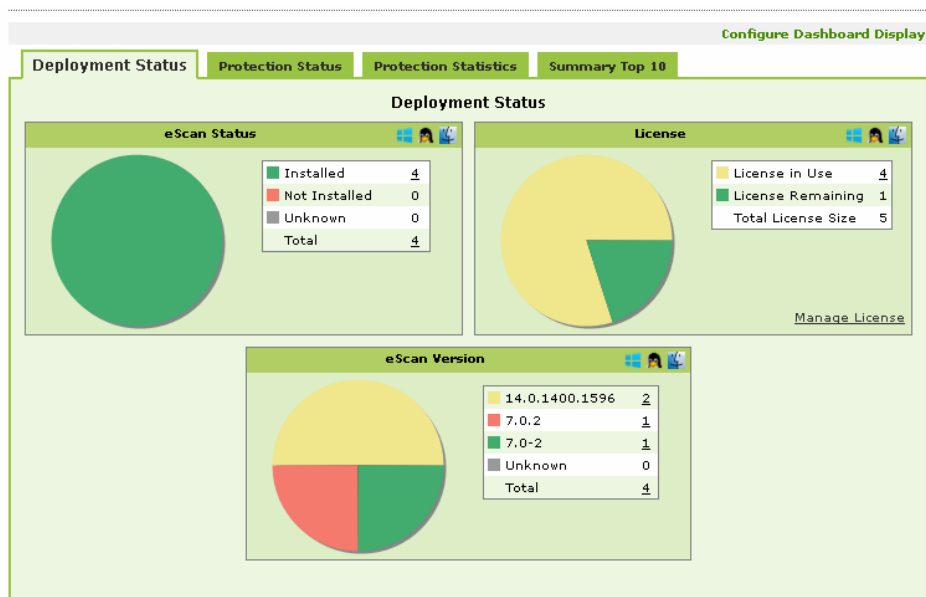


Figure 6.4

Note:

➡ Icons on every status Label denotes 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. Refer - Figure 6.5

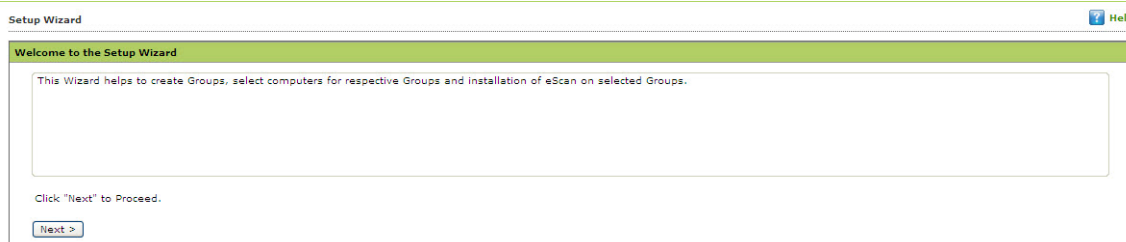


Figure 6.5

- **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

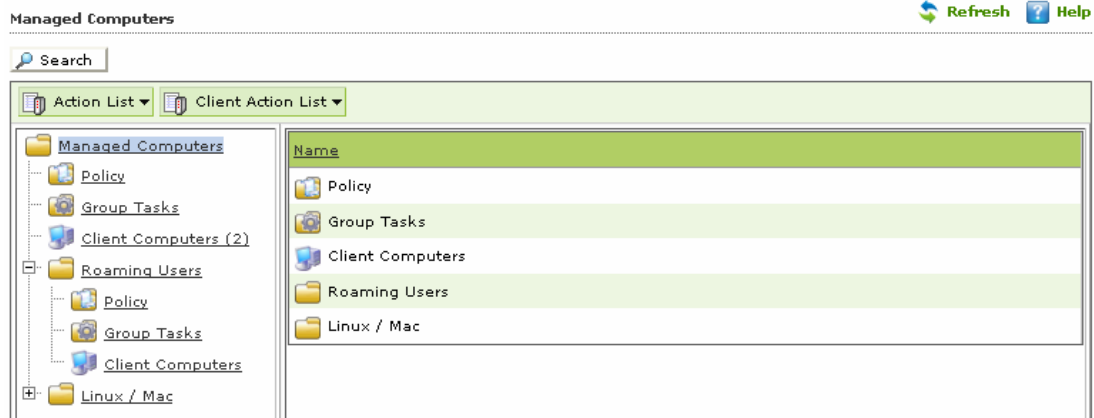


Figure 6.6

- 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

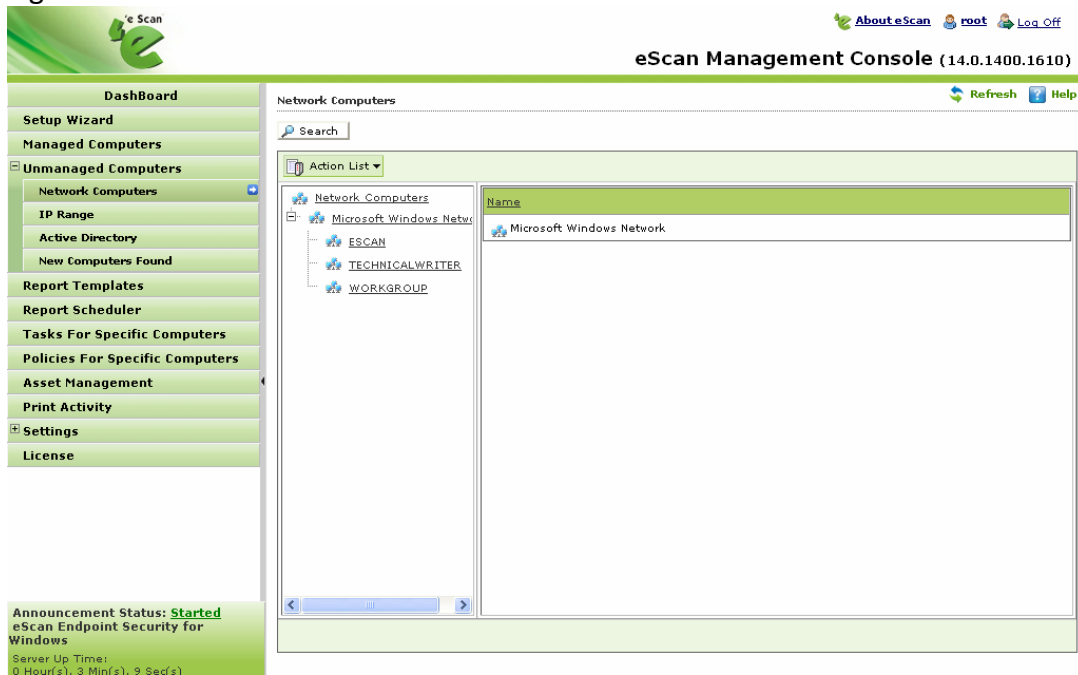


Figure 6.7

- Report Templates** - The **Report 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

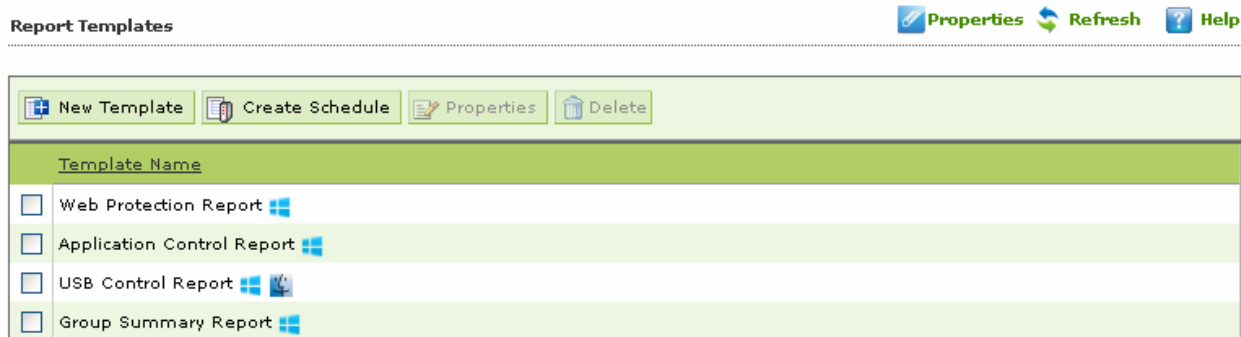





Figure 6.8

Note:

➡ *Icons on every status Label denotes that the status is displayed for the computers having operating system as  **Windows**,  **MAC OS X** 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

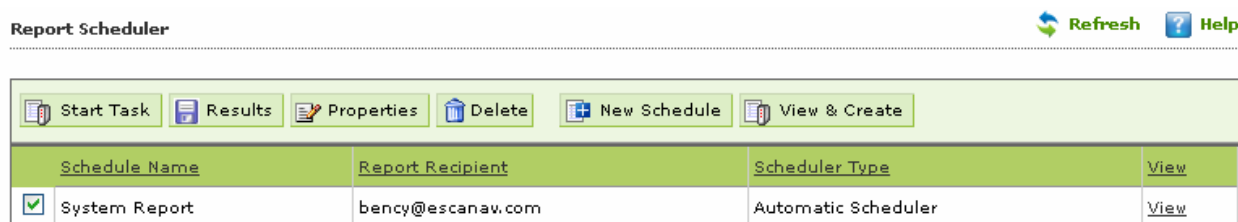


Figure 6.9

- **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 6.10

Tasks For Specific Computers

Refresh Help

<input type="button" value="New Task"/> <input type="button" value="Start Task"/> <input type="button" value="Properties"/> <input type="button" value="Results"/> <input type="button" value="Delete"/>				
Task Name	Pending	Completed	Schedule Type	Task Status
<input type="checkbox"/> Virus Scanning	1	0	Automatic Scheduler	

Figure 6.10

- 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 6.11

Policies For Specific Computers

Refresh Help

<input type="button" value="New Policy"/> <input type="button" value="Properties"/> <input type="button" value="Delete"/>		
Name of Policy	Last Deployed	Last Deployed To Whom
<input type="checkbox"/> No Facebook	Jun 29 2013 04:28:59 PM	COMP 134
<input type="checkbox"/> USB Allowed	Jun 08 2012 03:45:35 PM	COMP167
<input type="checkbox"/> No USB Access	Jul 25 2012 04:15:50 PM	COMP 145
<input type="checkbox"/> full internet blocked	Jul 09 2012 06:00:31 PM	COMP180
<input type="checkbox"/> USB Allowed	Jun 18 2012 06:30:35 PM	COMP92
<input type="checkbox"/> safari-include	Aug 02 2012 02:37:46 PM	COMP74, QA75-PC

Figure 6.11

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 6.12

Asset Management Refresh Help

Hardware Report Software Report

Filter Criteria Export Option

Computer Details 1 - 5 of 5 | page 1 of 1 | Rows per page: 100

Computer Name	Group	IP Address	User name	Operating System	Service Pack
qas-Mac-10-9	Mac	192.168.1.60	root	Mac OS X 10.9 64-Bit	13.0.0
qasmac1-212	Managed Computers	192.168.1.212	root	Mac OS X 10.7.1 64-Bit	11.0.1
qas-Mac-Pro	Mac	192.168.1.156	root	Mac OS X 10.6 32-Bit	10.2.0
QA-TEST-XP	Mac	192.168.2.43	SYSTEM	Windows XP	Service Pack 3, v
QA-WIN-155	Managed Computers	192.168.5.82,192.168.1.155	SYSTEM	Windows XP	Service Pack 3 (B

Figure 6.12

- **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 6.13

Print Activity Refresh Help

Filter Criteria Export Option

1 - 32 of 32 | page 1 of 1 | Rows per page: 100

Printer Name	Copies
Brother HL-2140	1
Canon LBP3300	335
doPDF v7	2
HP Deskjet F2400 series	4
HP Deskjet F4200 series	164
HP Deskjet Ink Advant K209a-z	46300

Figure 6.13

- **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](#)
- **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 6.14

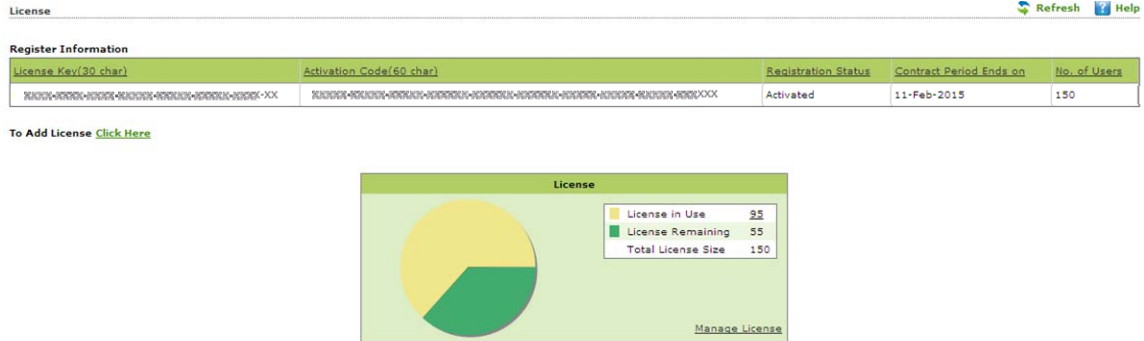


Figure 6.14

- **Server Status info** – It displays the Announcement 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 its 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 -**

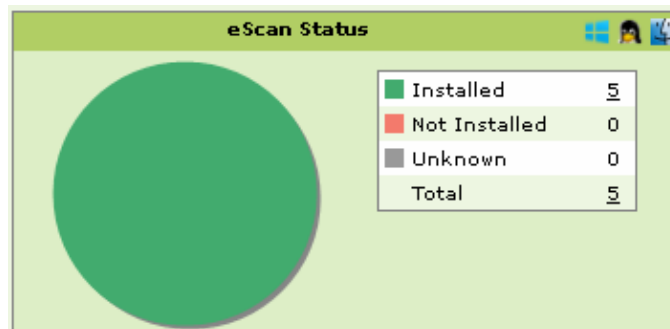


Figure 6.15

- **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 –**

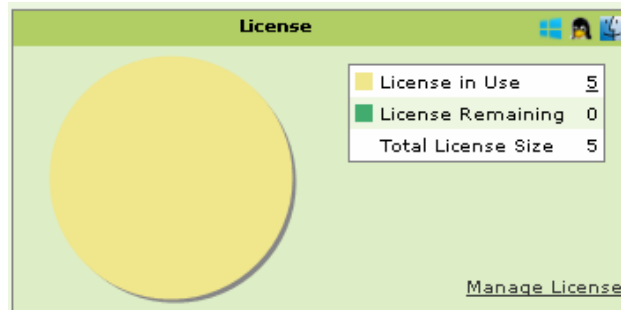


Figure 6.16

- **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.

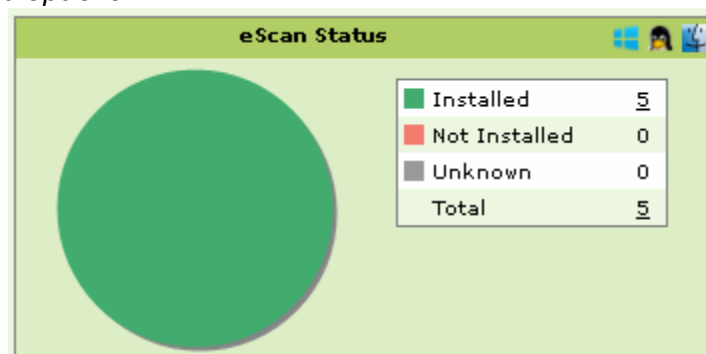
- **eScan Version -**

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.
- **Web Anti –Phishing –**

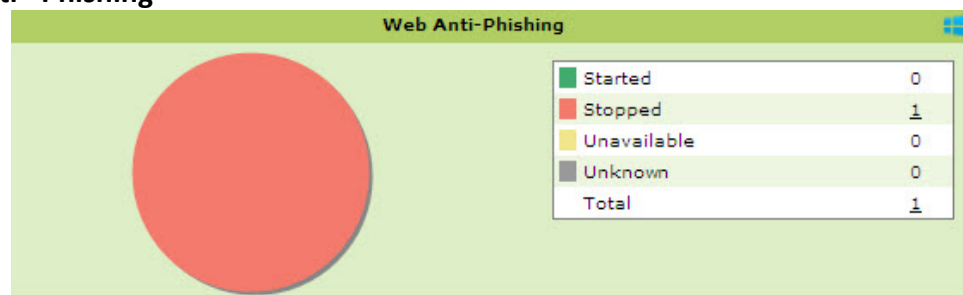


Figure 6.17

- **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.

- **Web Protection**

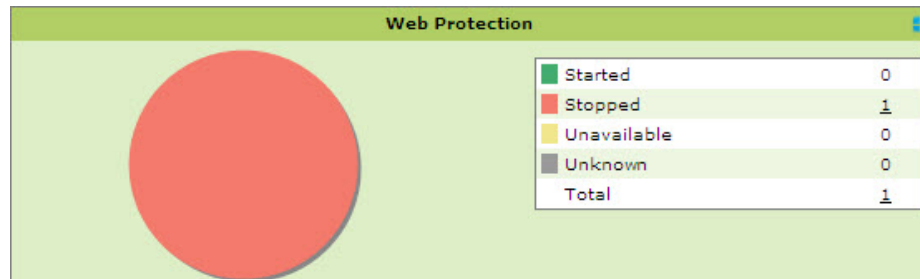


Figure 6.18

- **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.
- **Endpoint Security**

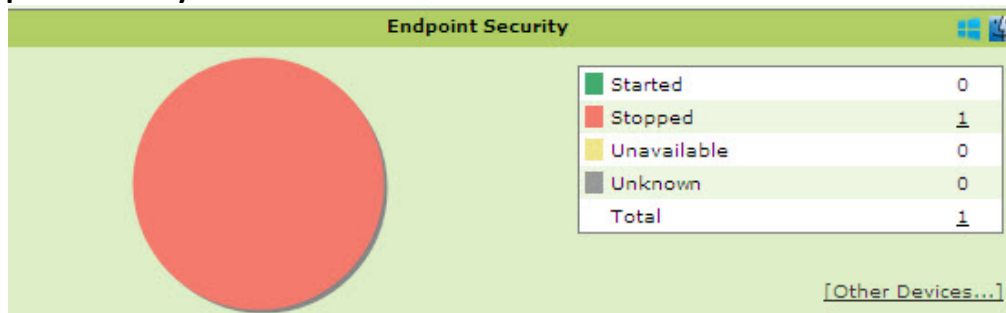





Figure 6.19

- **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 are 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.

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.

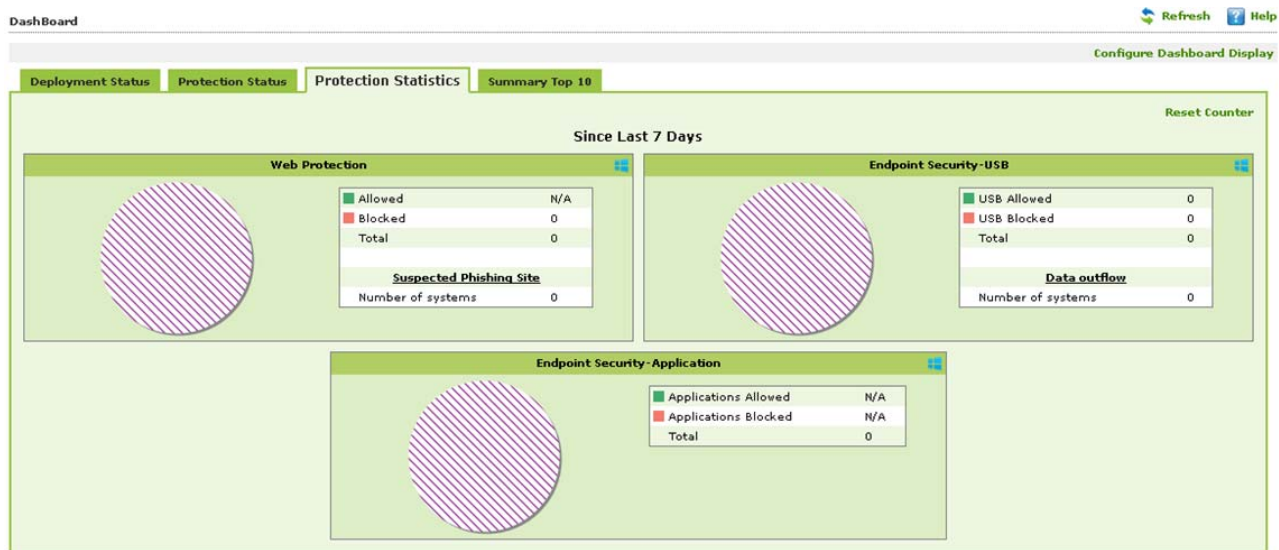


Figure 6.20

- **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.

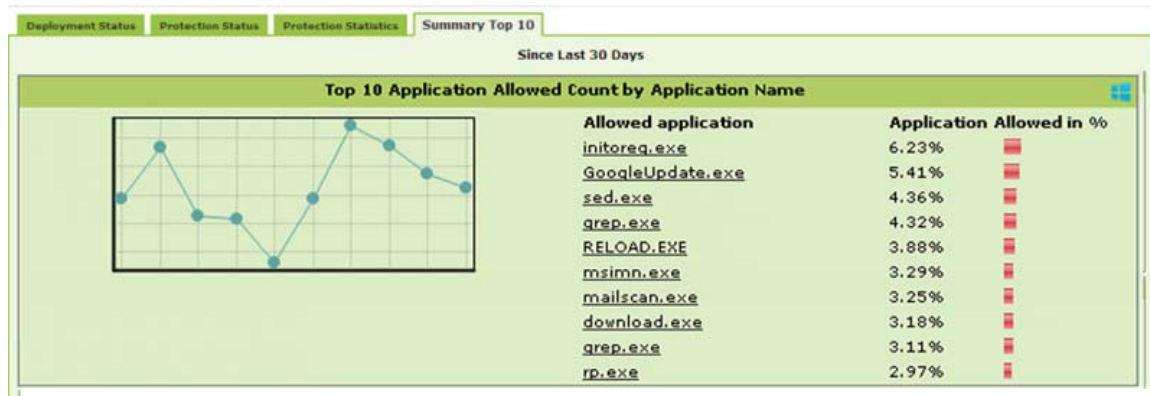


Figure 6.21

- **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 – 6.22

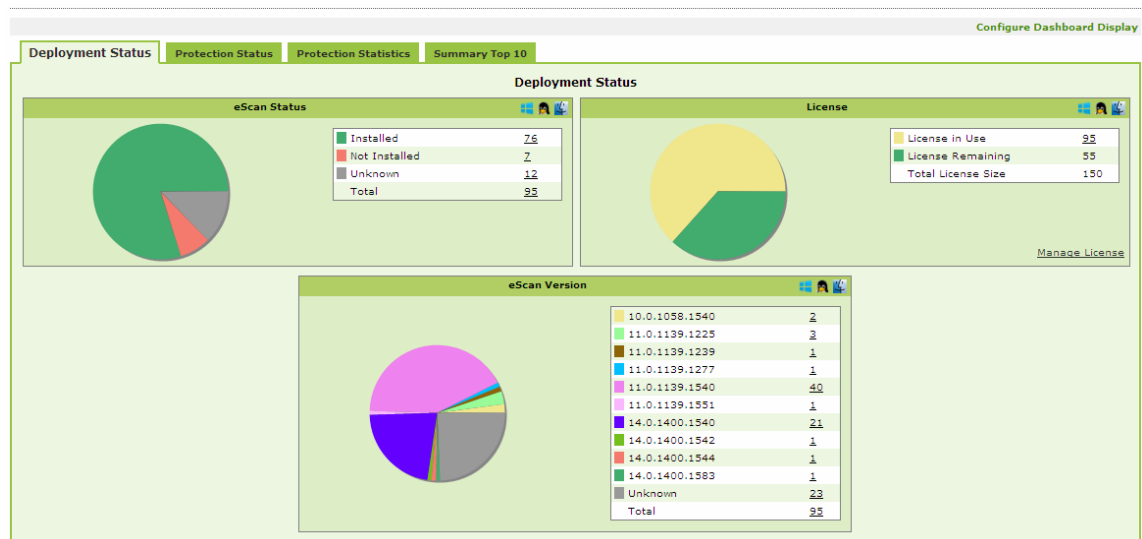


Figure – 6.22

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

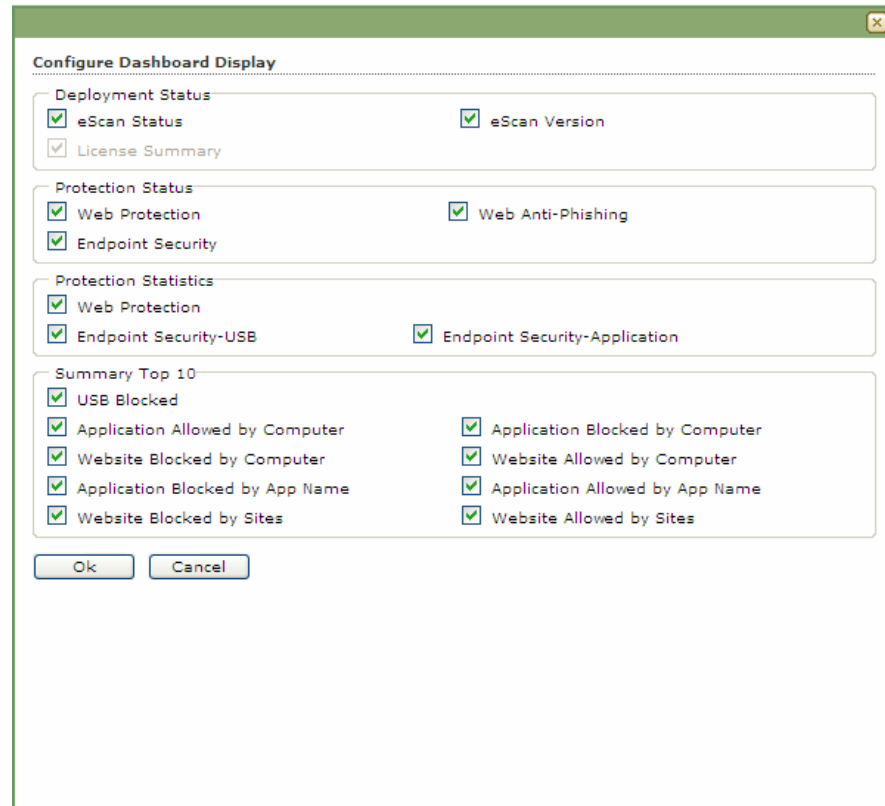





Figure 6.23

- 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. Managed 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

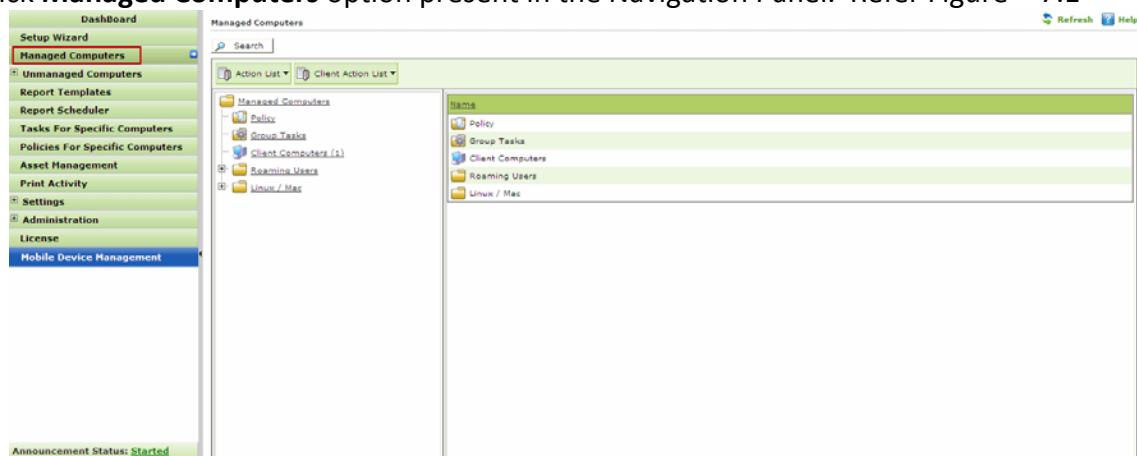


Figure - 7.1

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

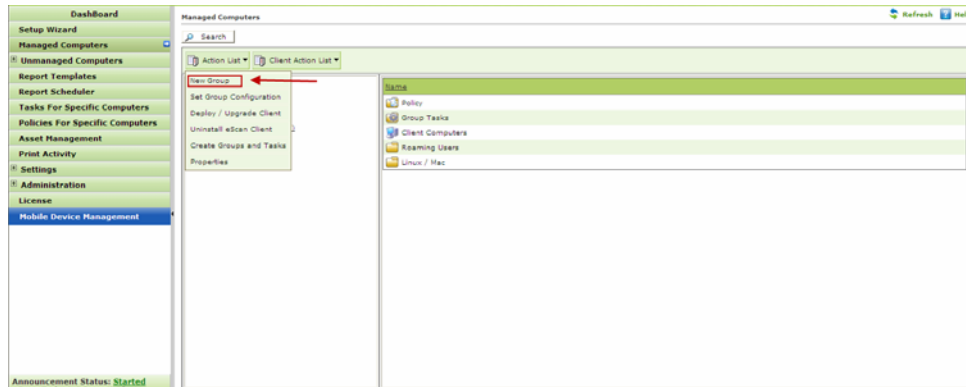


Figure -7.2

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.

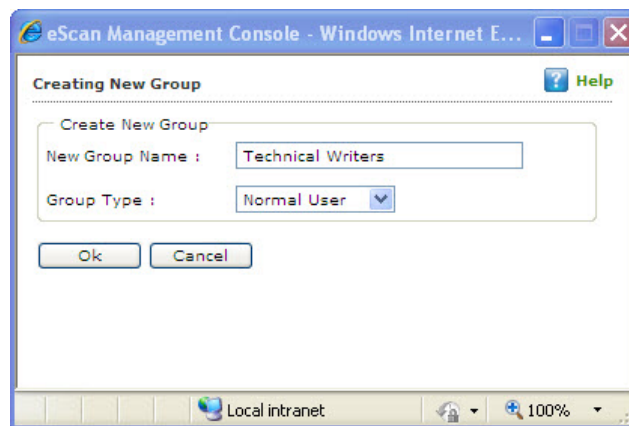


Figure 7.3

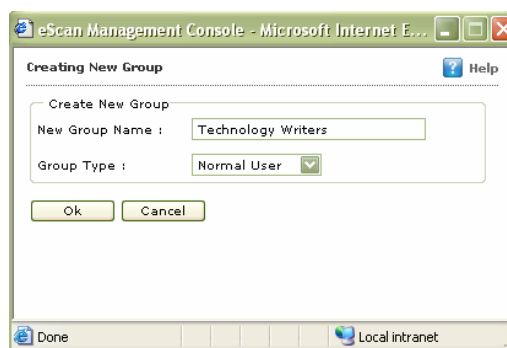


Figure -7.4

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

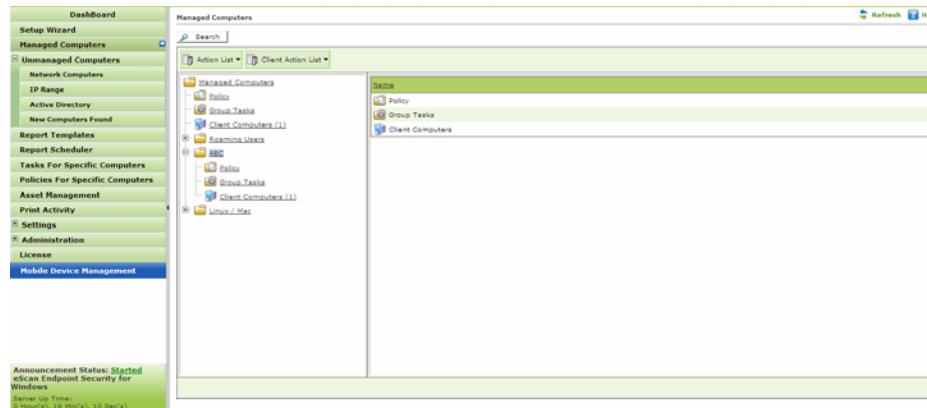


Figure – 7.5

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

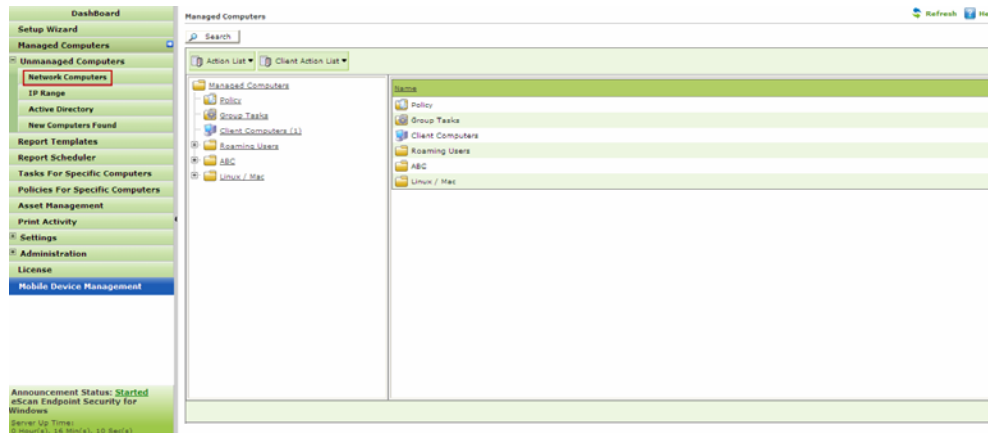


Figure -7.6

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

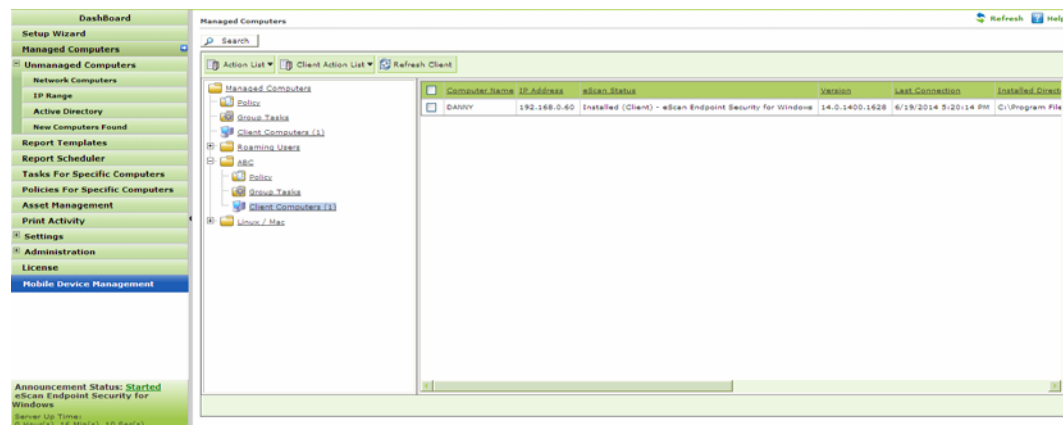


Figure -7.7

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

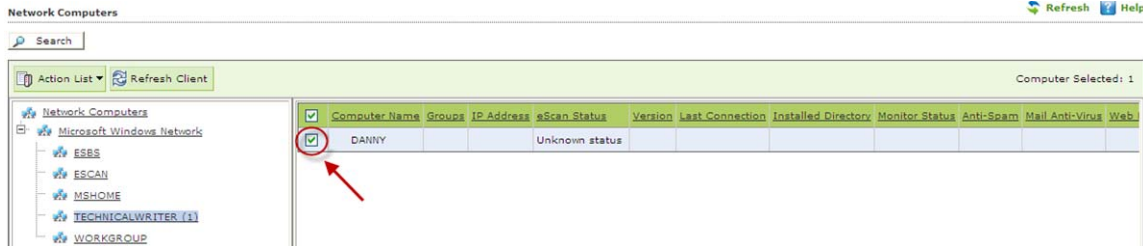


Figure -7.8

Also see [Viewing Properties](#) and [Setting Host Configuration](#)

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

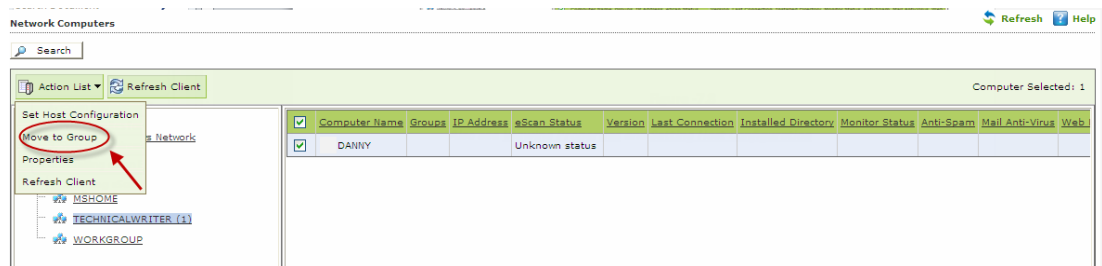


Figure – 7.9

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

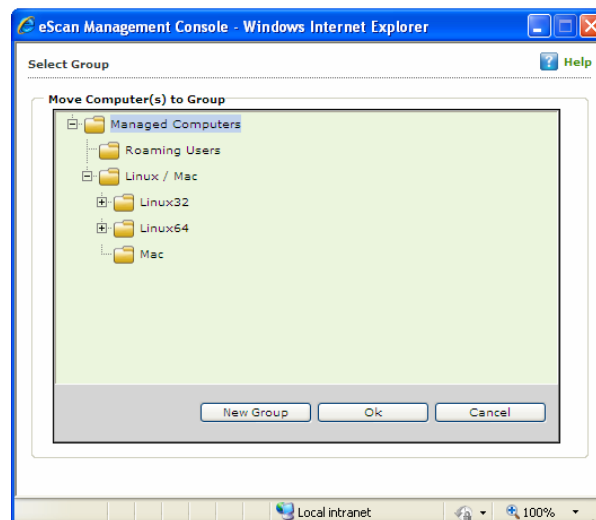


Figure – 7.10

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

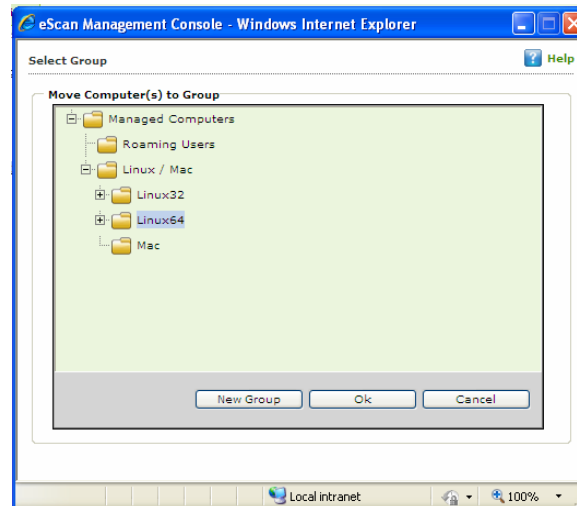


Figure – 7.11

- 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 –

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

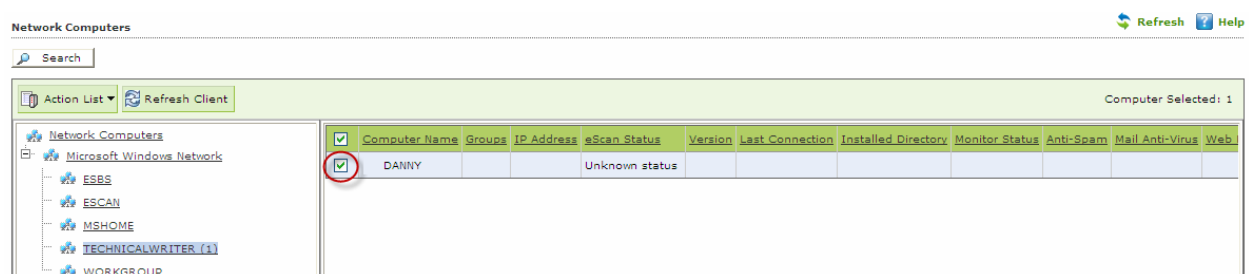


Figure -7.12

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

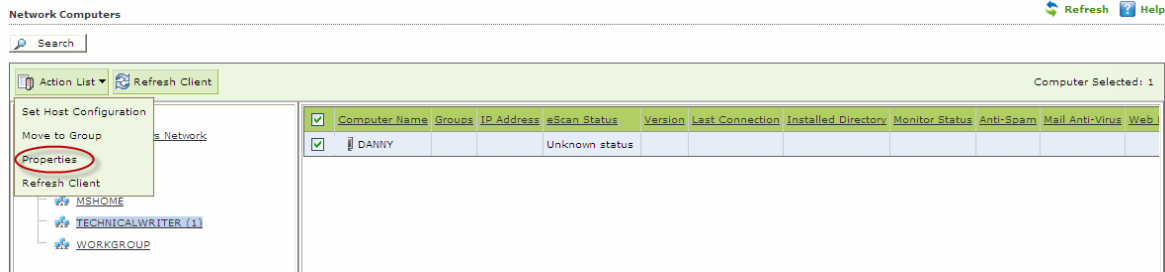


Figure – 7.13

- 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 its version and update summary. Refer **Figure – 7.14**

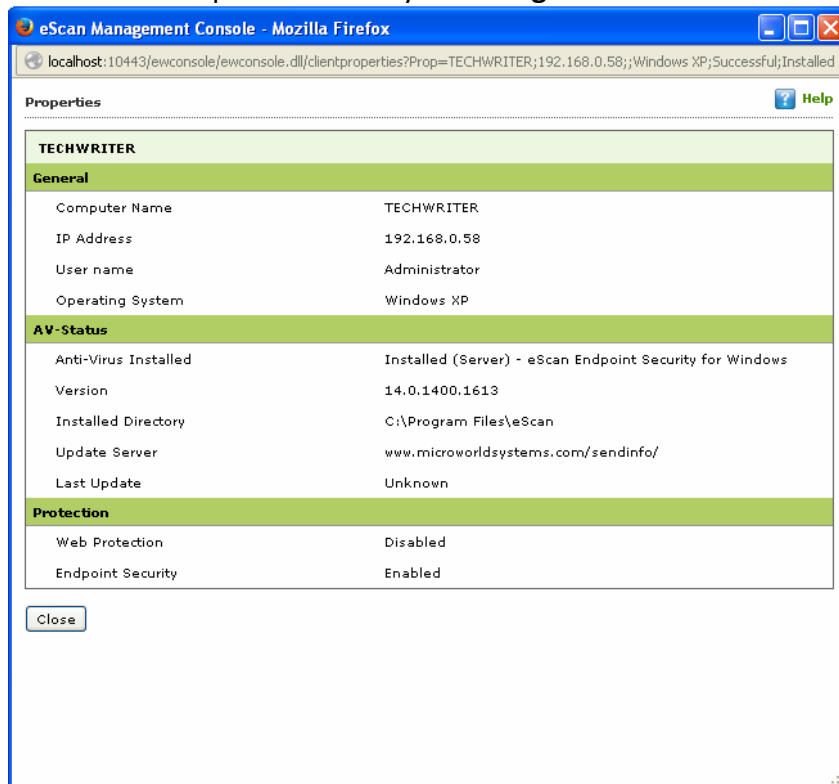


Figure – 7.14

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**

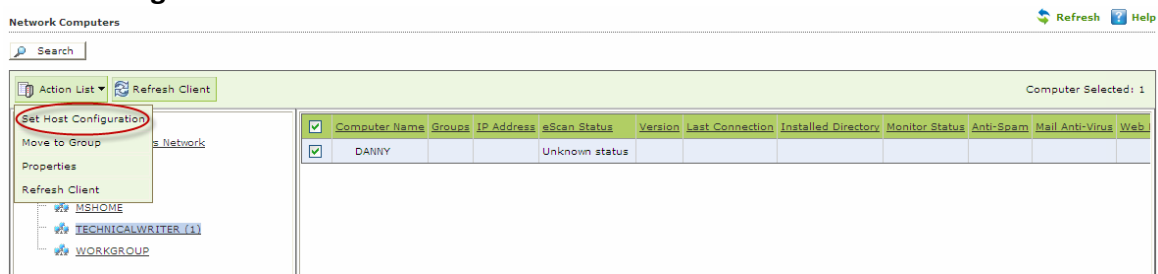


Figure – 7.15

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

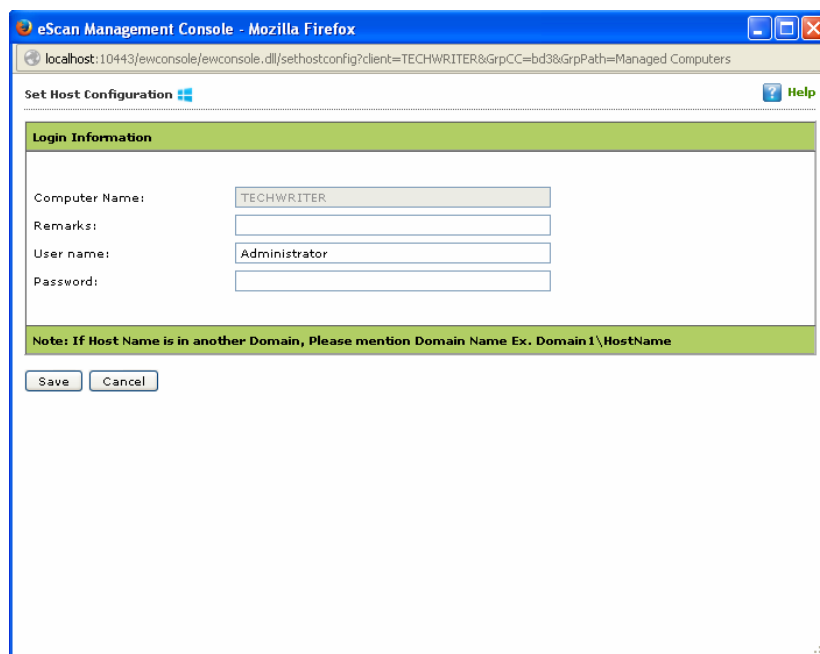


Figure - 7.16

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**

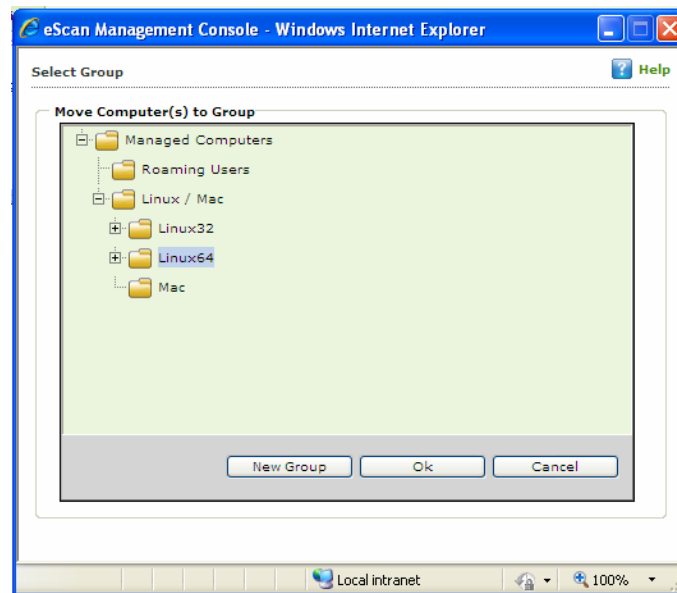


Figure - 7.17

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**

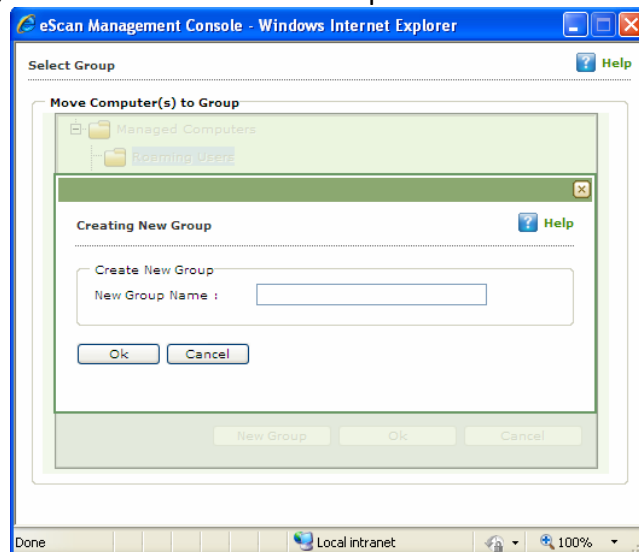


Figure – 7.18

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

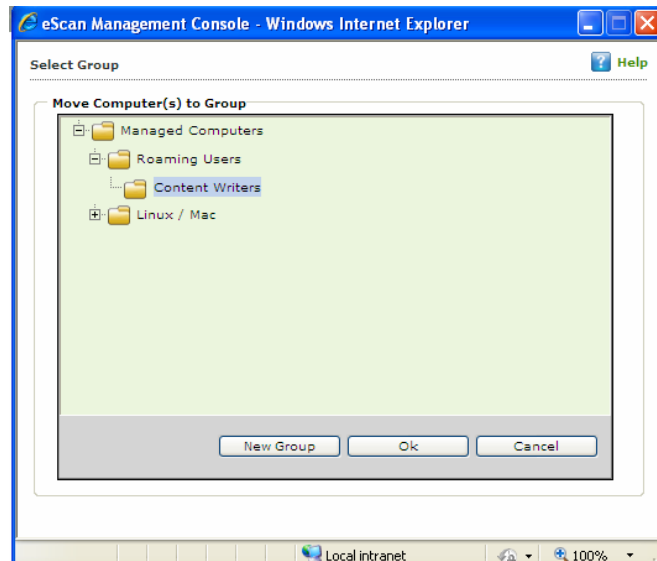


Figure – 7.19

- **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**

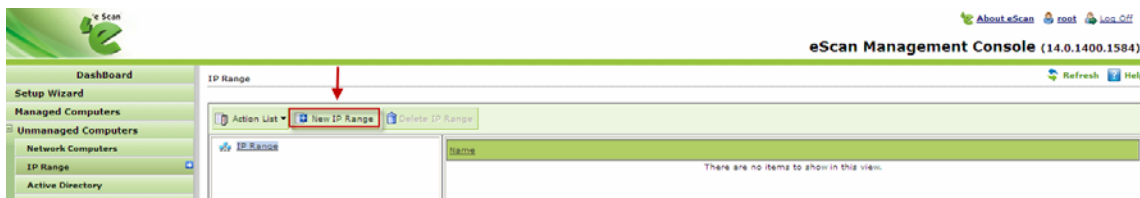


Figure - 7.20

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

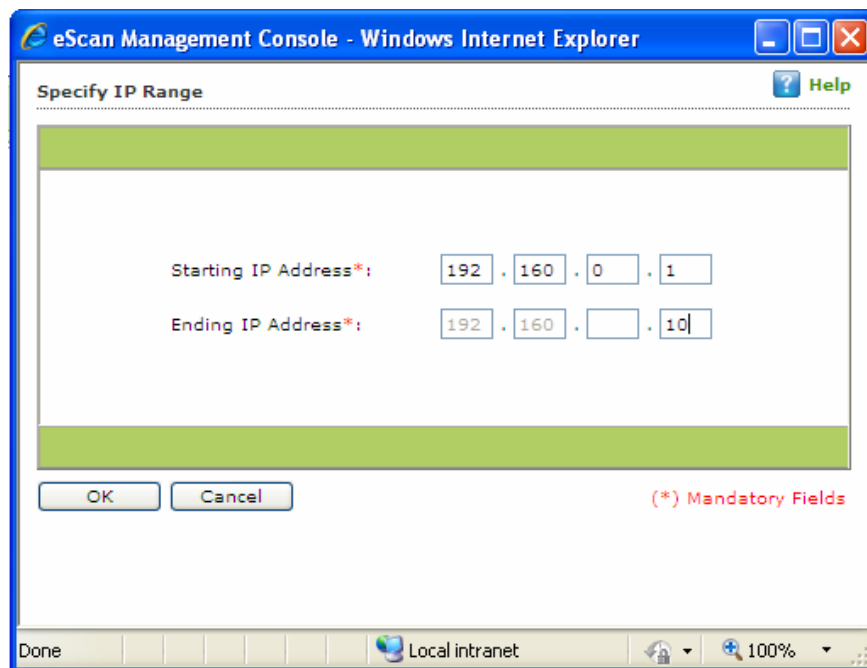


Figure – 7.21

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**.

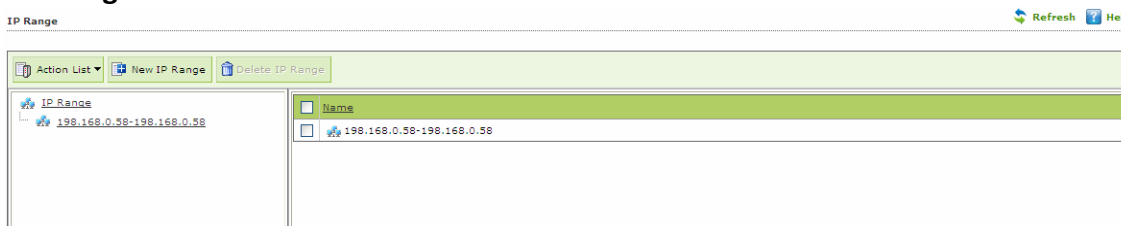


Figure – 7.22

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**

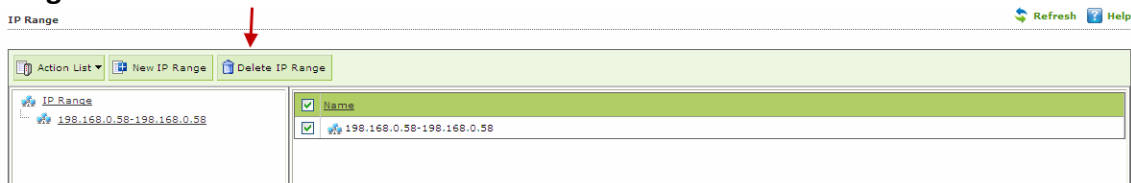


Figure – 7.23

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

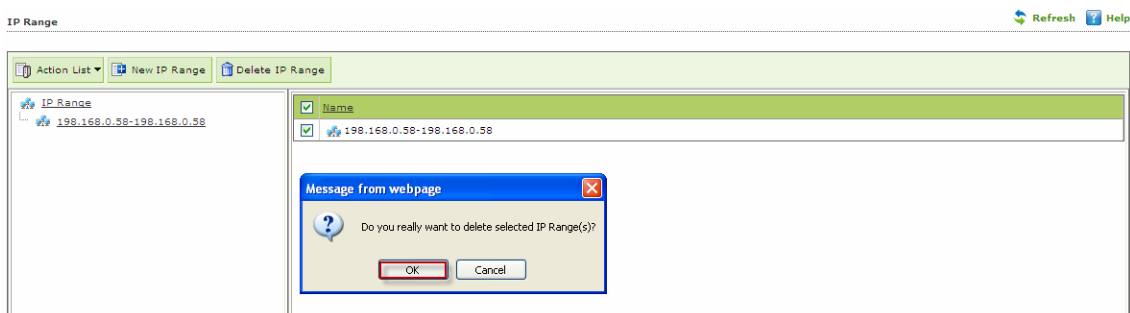


Figure – 7.24

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**

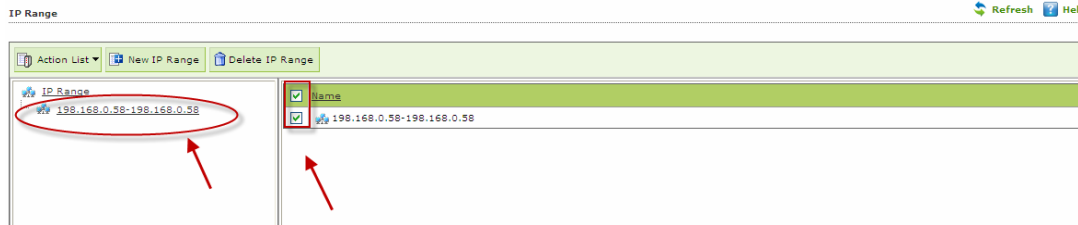


Figure – 7.25

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

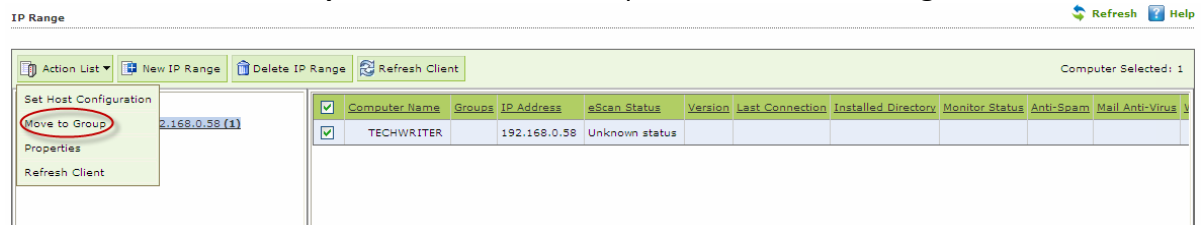


Figure – 7.26

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**

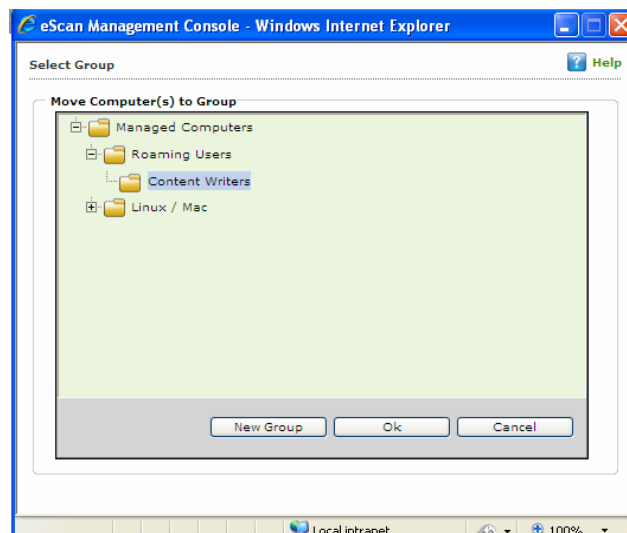


Figure – 7.27

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

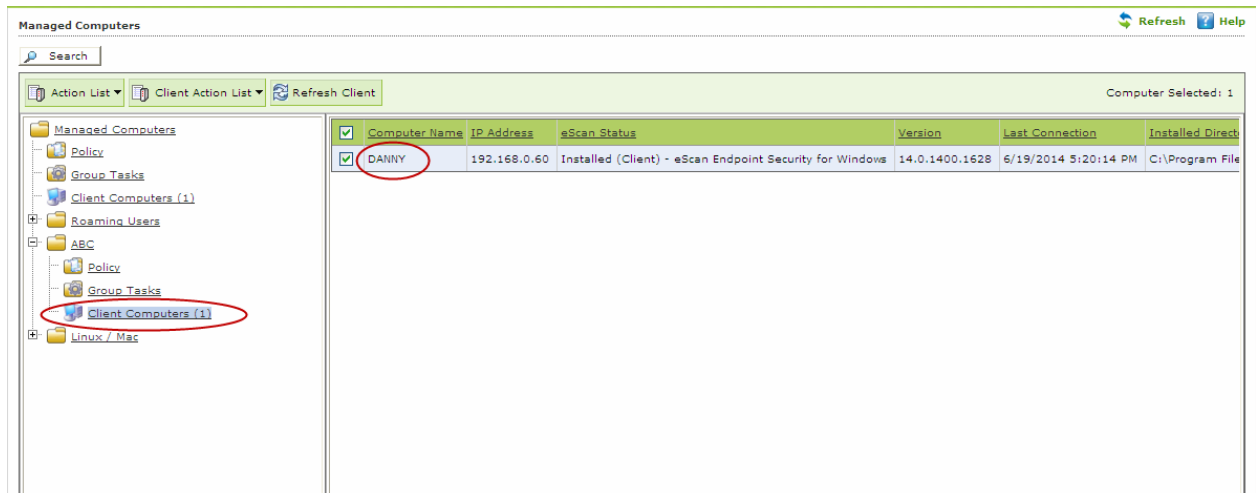


Figure – 7.28

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**

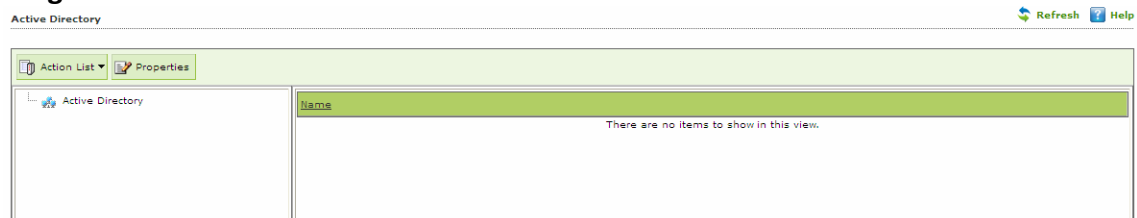


Figure – 7.29

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

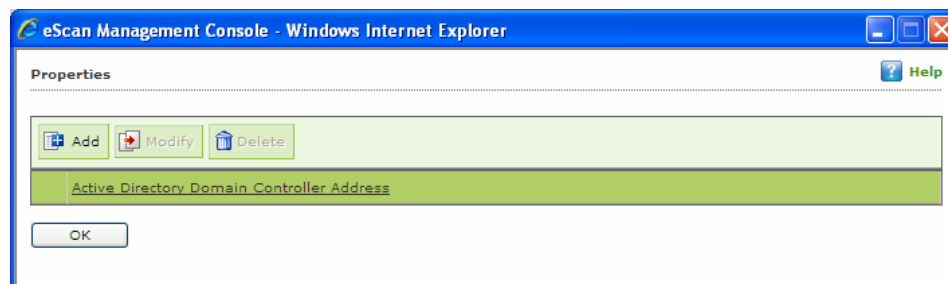


Figure 7.30

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**

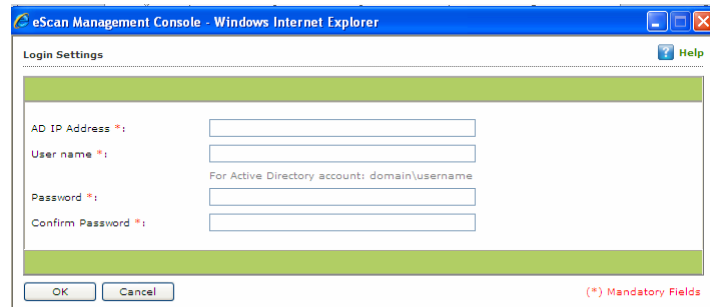


Figure 7.31

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

Properties

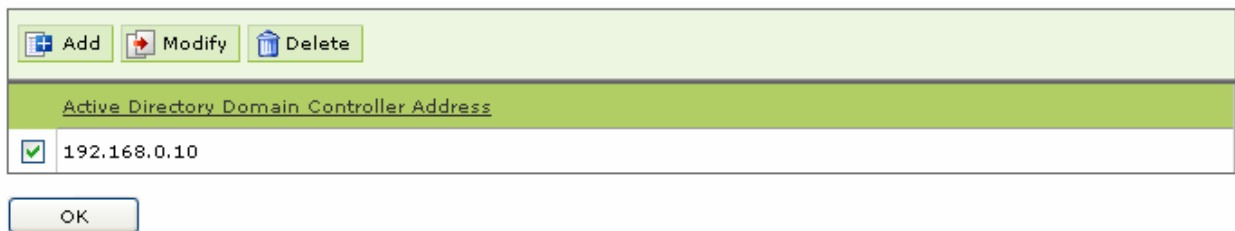


Figure 7.32

- 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**

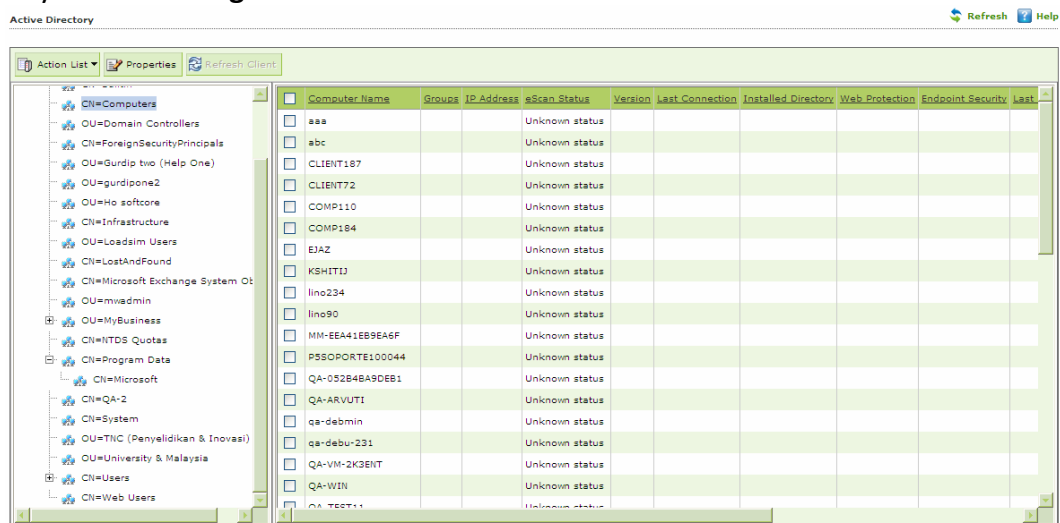


Figure 7.33

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

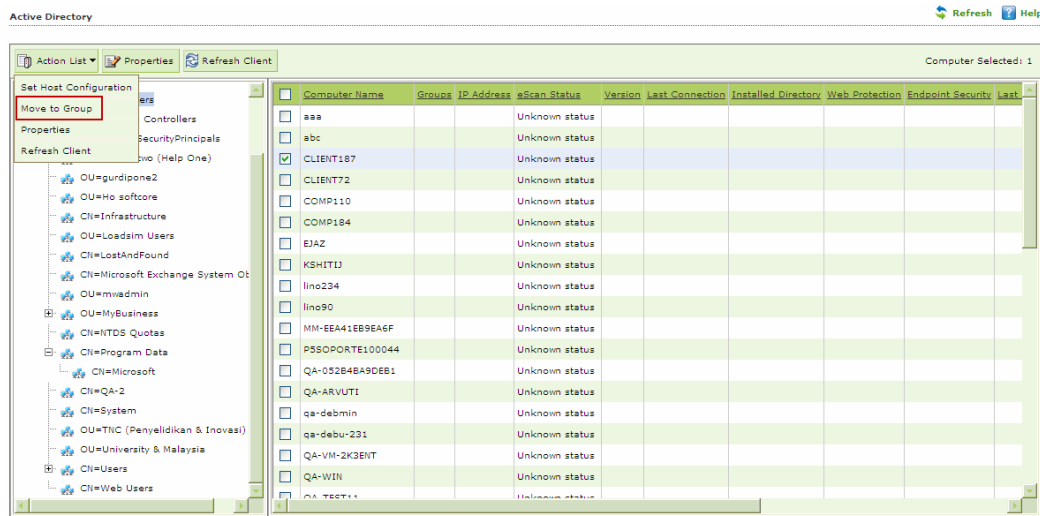


Figure 7.34

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

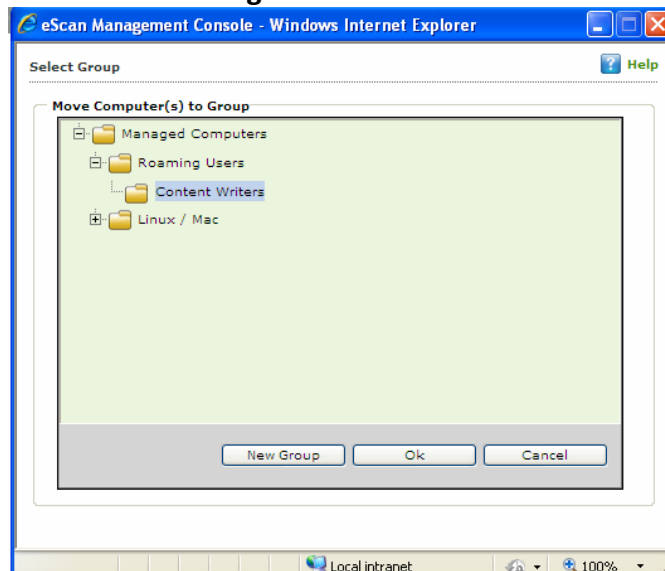


Figure 7.35

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.

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.

- **Remote Installation of eScan Client –**

- **Preparing Client Computer for Remote Deployment**

To install eScan Endpoint Security for Windows 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**

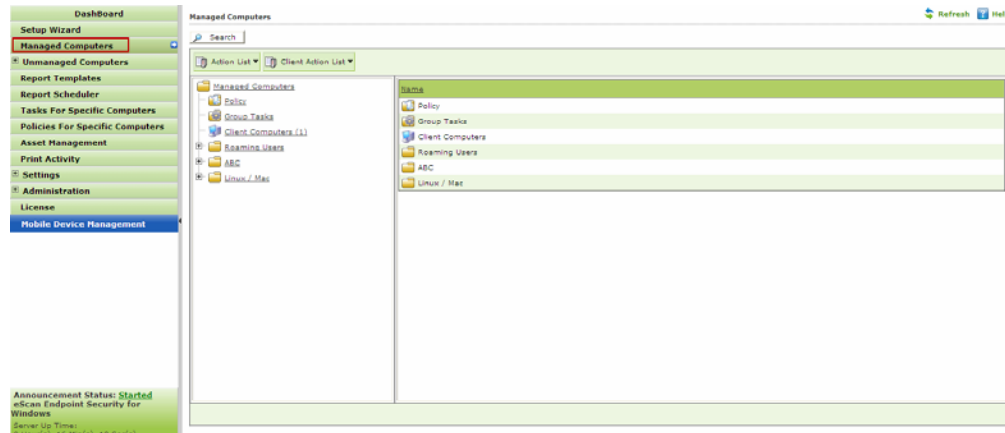


Figure 8.1

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

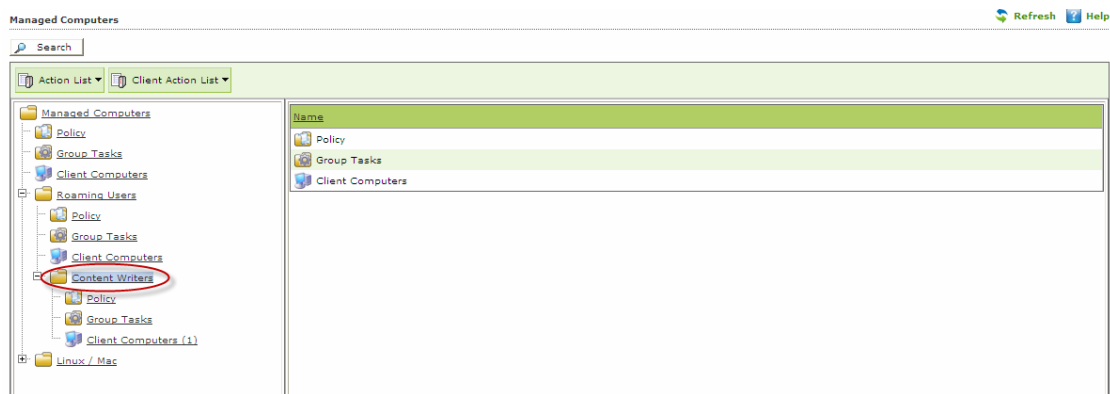


Figure 8.2

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

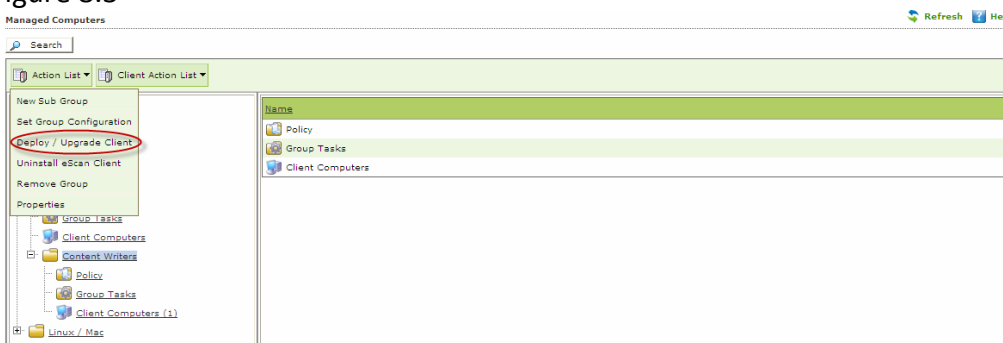


Figure 8.3

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**

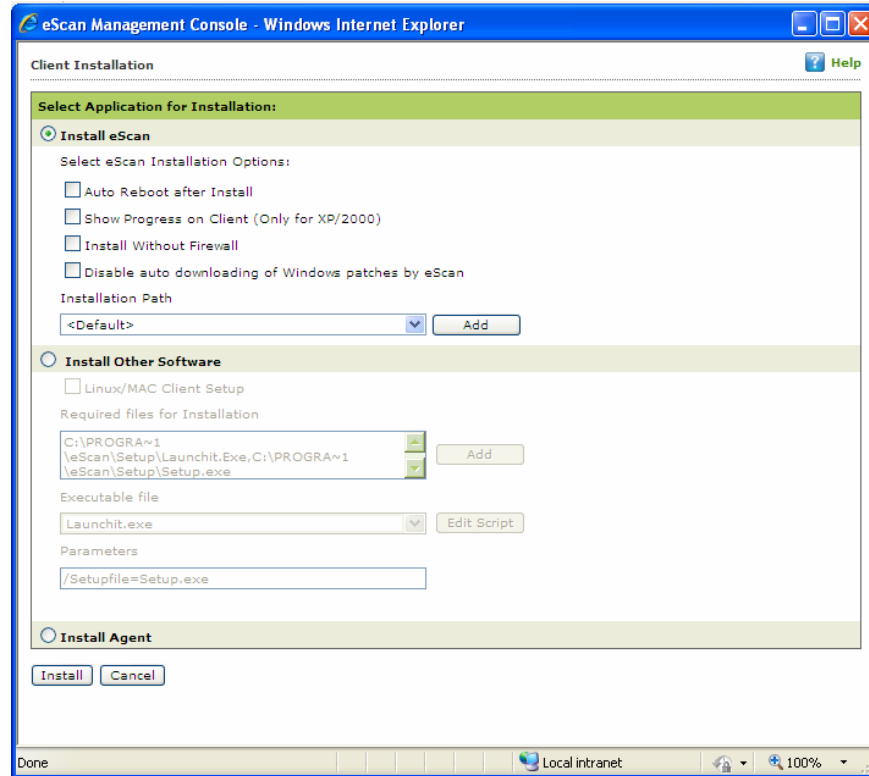


Figure 8.4

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**

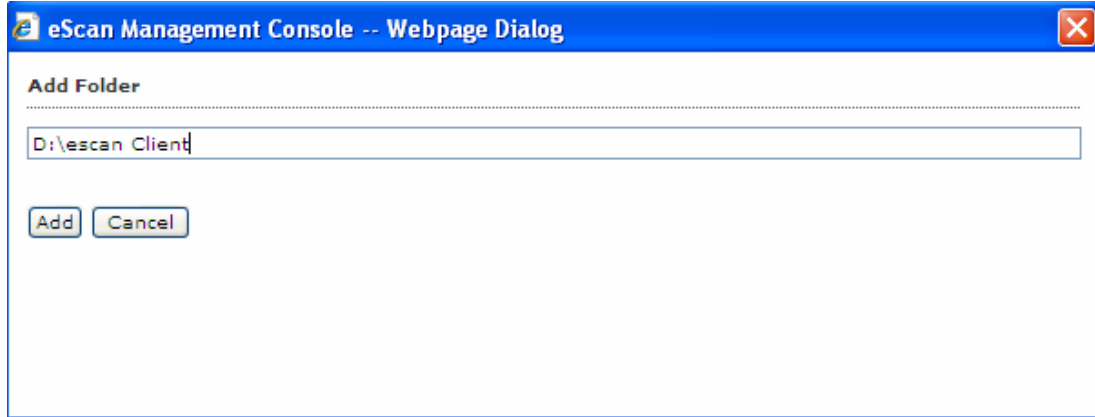


Figure 8.5

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**

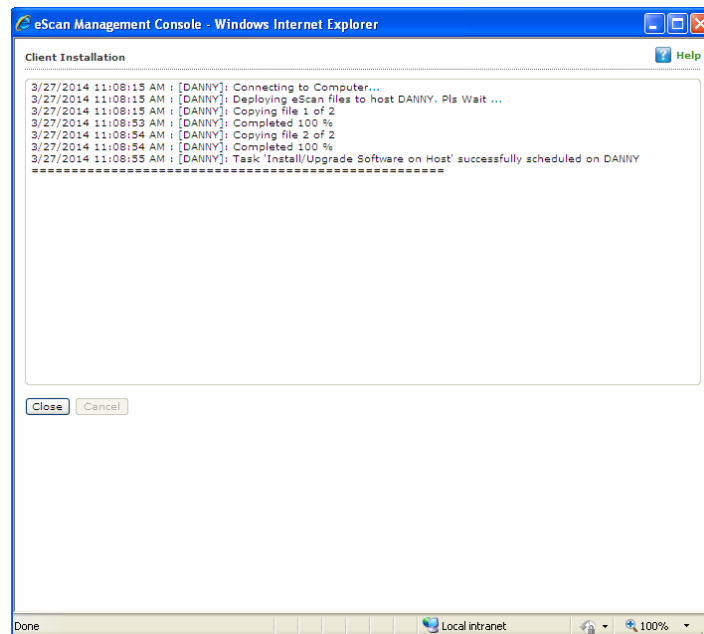


Figure 8.6

11. After Installation the eScan status will be updated in Managed Computers list “**Installed (Client)** - eScan Endpoint Security for Windows”.

<input type="checkbox"/>	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory
<input type="checkbox"/>	DANNY	192.168.0.60	Installed (Client) - eScan Endpoint Security for Windows	14.0.1400.1628	6/19/2014 5:28:48 PM	C:\Program File

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**

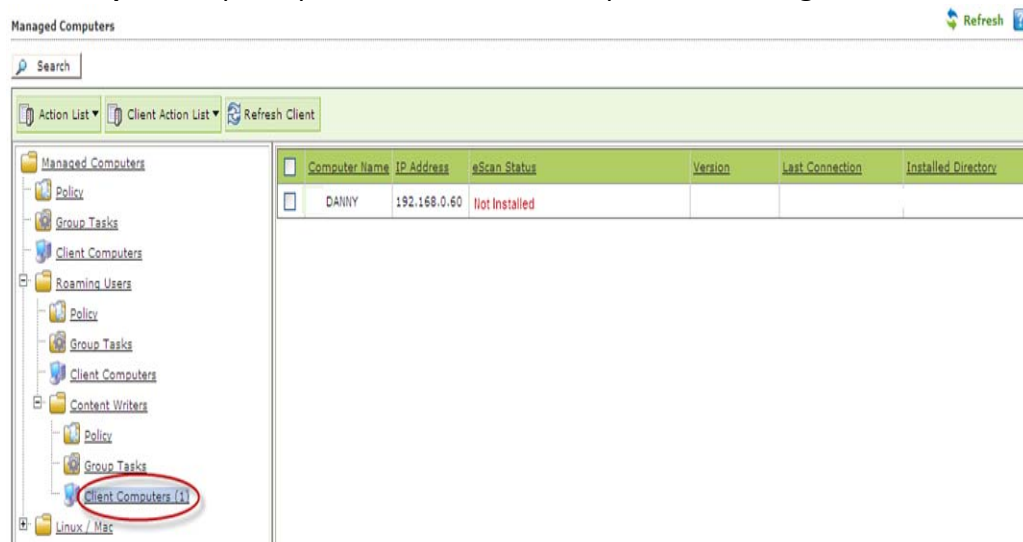


Figure 8.8

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**

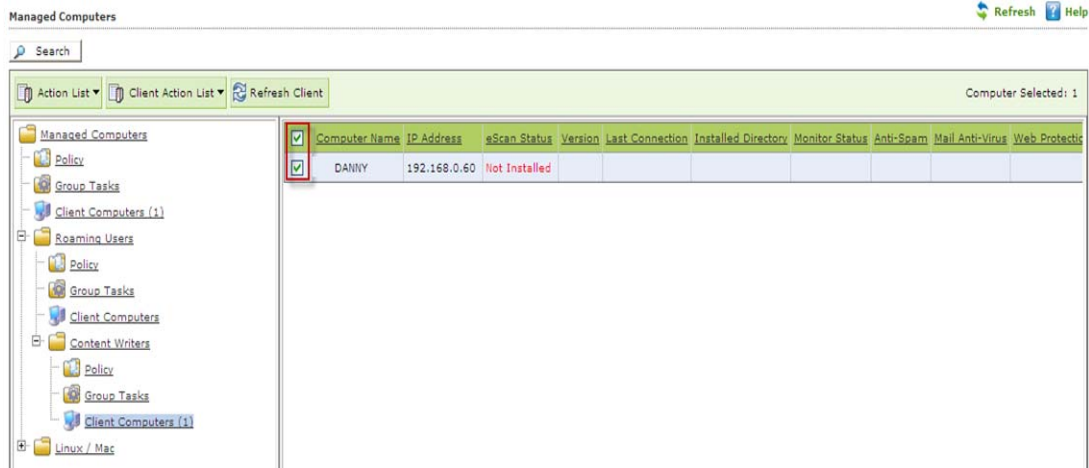


Figure – 8.9

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



Figure – 8.10

- You will be forwarded to the Client Installation window.
- Now Select Install eScan option and also select the desired eScan installation option using the respective checkboxes present on the interface.
- 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 Endpoint Security for Windows”.

<input type="checkbox"/>	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Direct
<input type="checkbox"/>	DANNY	192.168.0.60	Installed (Client) - eScan Endpoint Security for Windows	14.0.1400.1628	6/19/2014 5:28:48 PM	C:\Program File

Figure – 8.11

- **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**

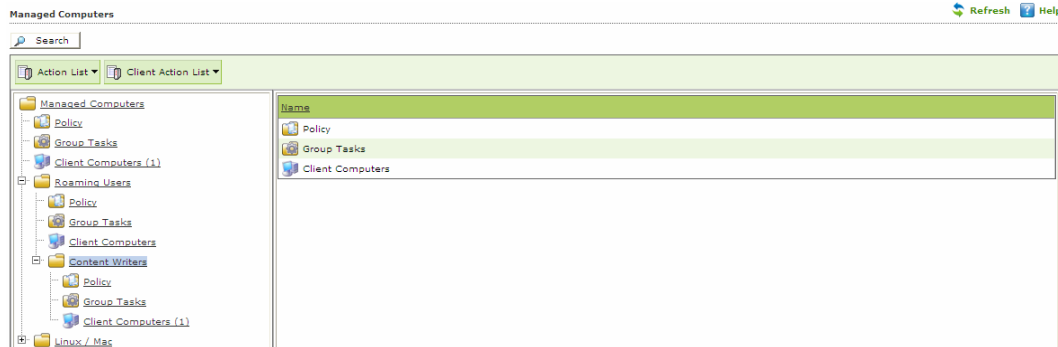


Figure – 8.12

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

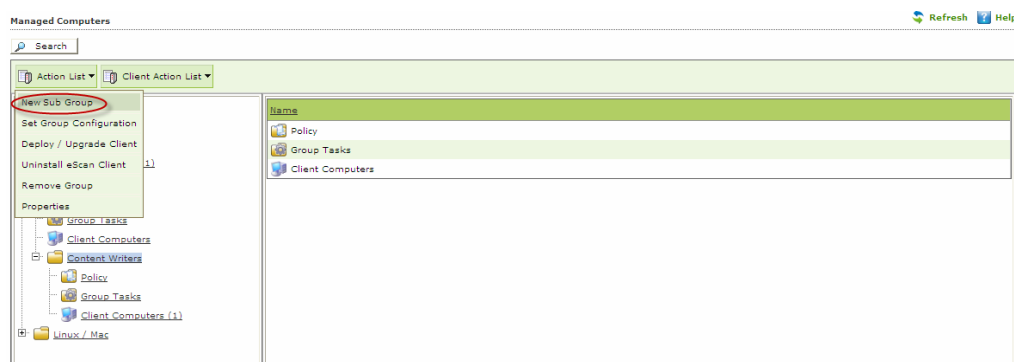


Figure – 8.13

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**

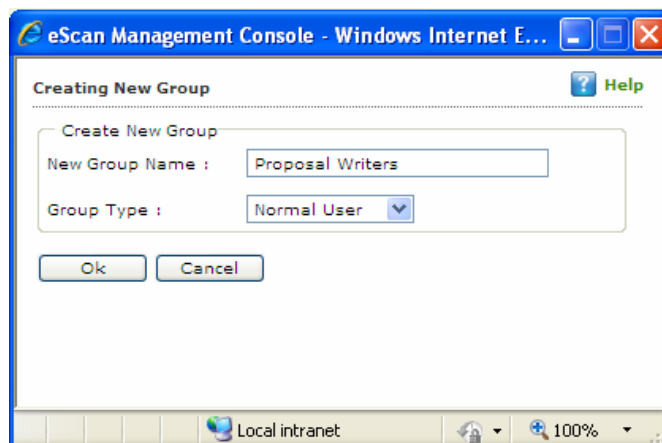


Figure – 8.14

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**

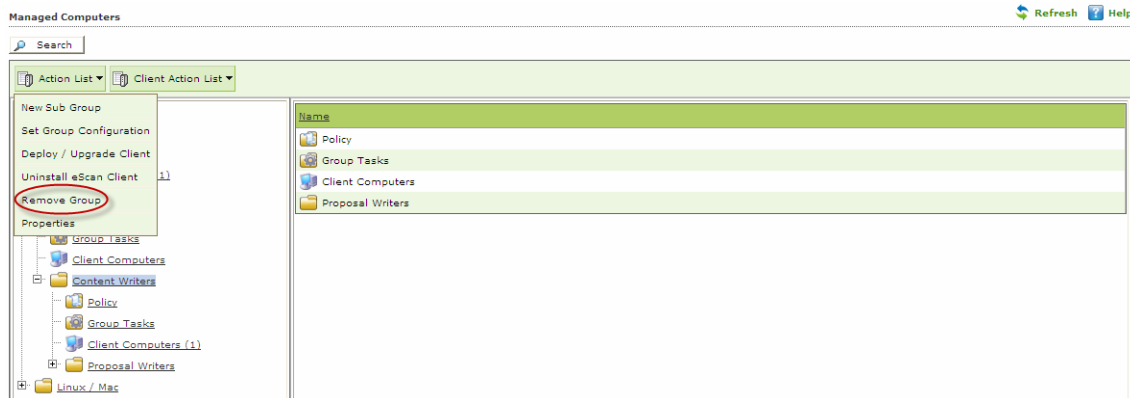


Figure – 8.15

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

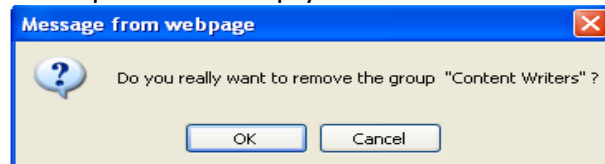


Figure – 8.16

- **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.

<input checked="" type="checkbox"/>	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Direct
<input checked="" type="checkbox"/>	DANNY	192.168.0.60	Installed (Client) - eScan Endpoint Security for Windows	14.0.1400.1628	6/19/2014 5:28:48 PM	C:\Program File

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**

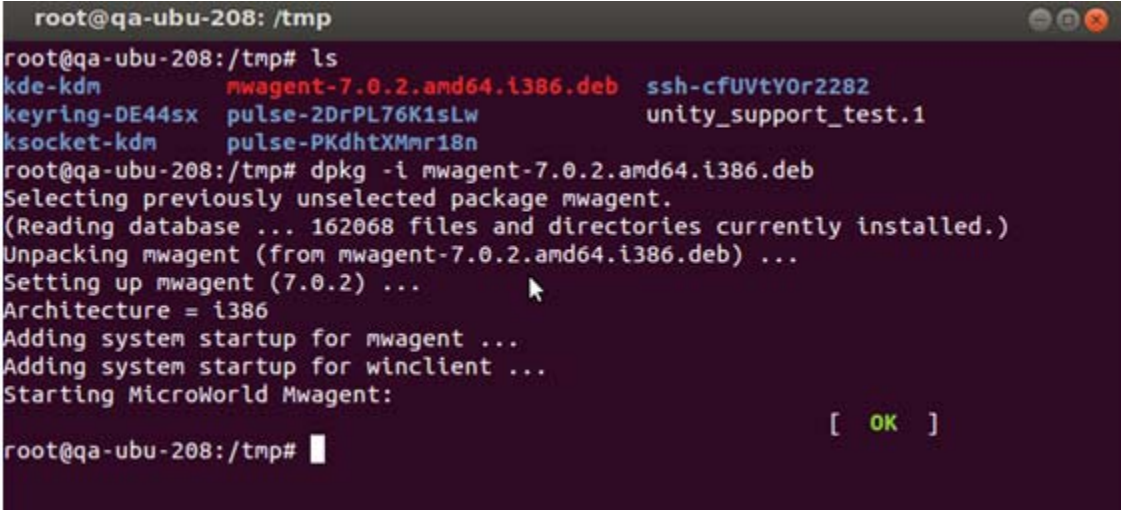
For installing eScan on Linux or Mac computer please install the Agent on the Linux or Mac computers and then proceed to install eScan, it can be done with the following simple steps –

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**



```
root@qa-ubu-208: /tmp
root@qa-ubu-208:/tmp# ls
kde-kdm          mwagent-7.0.2.amd64.i386.deb  ssh-cfUVtY0r2282
keyring-DE44sx  pulse-2DrPL76K1sLw          unity_support_test.1
ksocket-kdm     pulse-PKdhtXMmr18n
root@qa-ubu-208:/tmp# dpkg -i mwagent-7.0.2.amd64.i386.deb
Selecting previously unselected package mwagent.
(Reading database ... 162068 files and directories currently installed.)
Unpacking mwagent (from mwagent-7.0.2.amd64.i386.deb) ...
Setting up mwagent (7.0.2) ...
Architecture = i386
Adding system startup for mwagent ...
Adding system startup for winclient ...
Starting MicroWorld Mwagent:
[ OK ]
root@qa-ubu-208:/tmp#
```

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 on Continue button to continue the installation process . Refer **Figure 8.20**

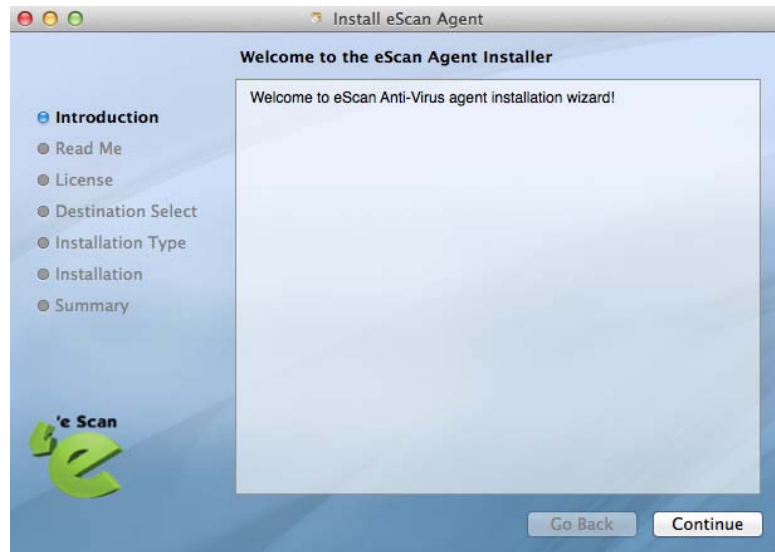


Figure 8.20

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

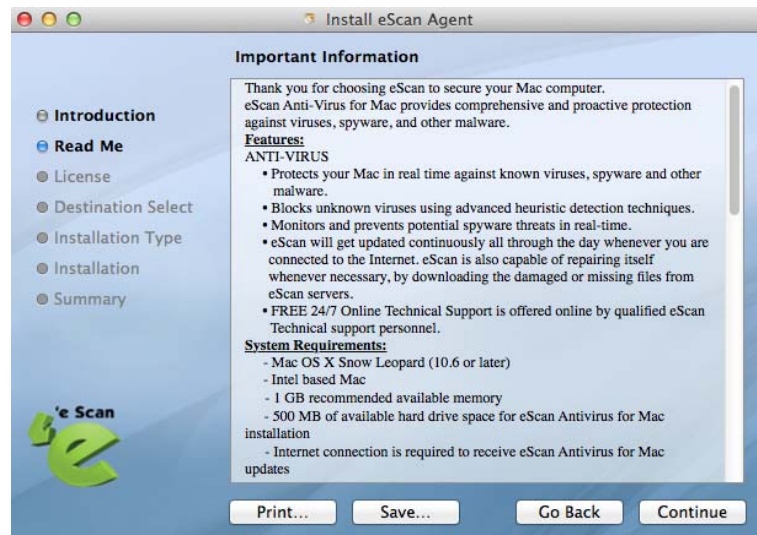


Figure 8.21

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

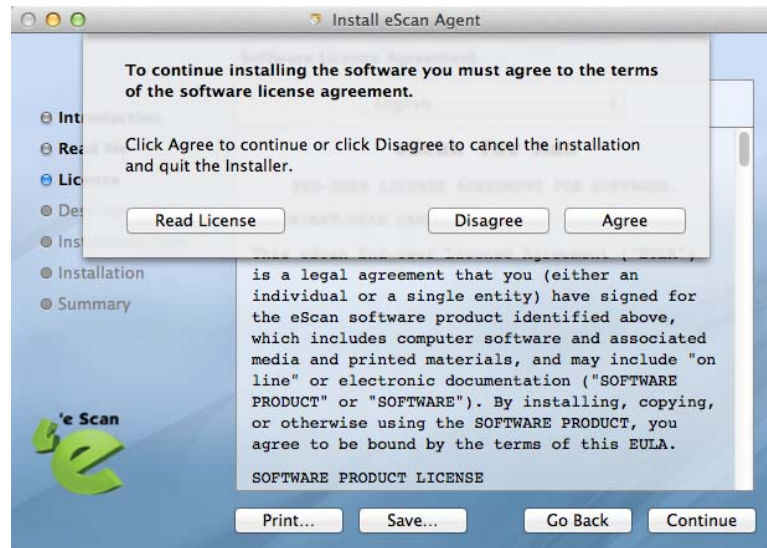


Figure 8.22

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

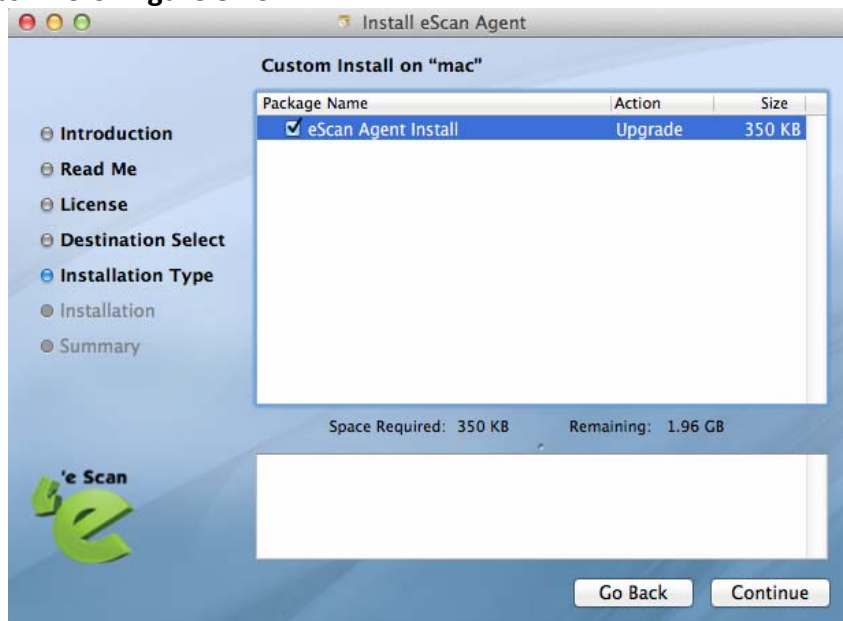


Figure 8.23

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

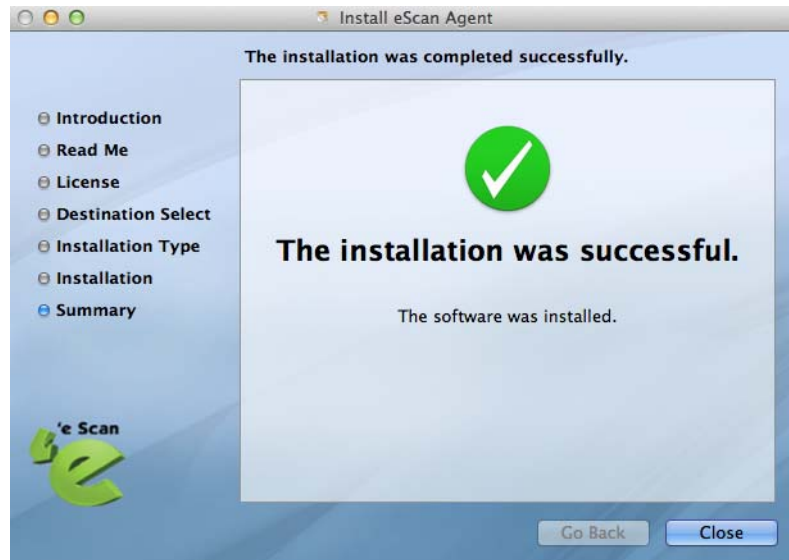


Figure 8.24

- **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

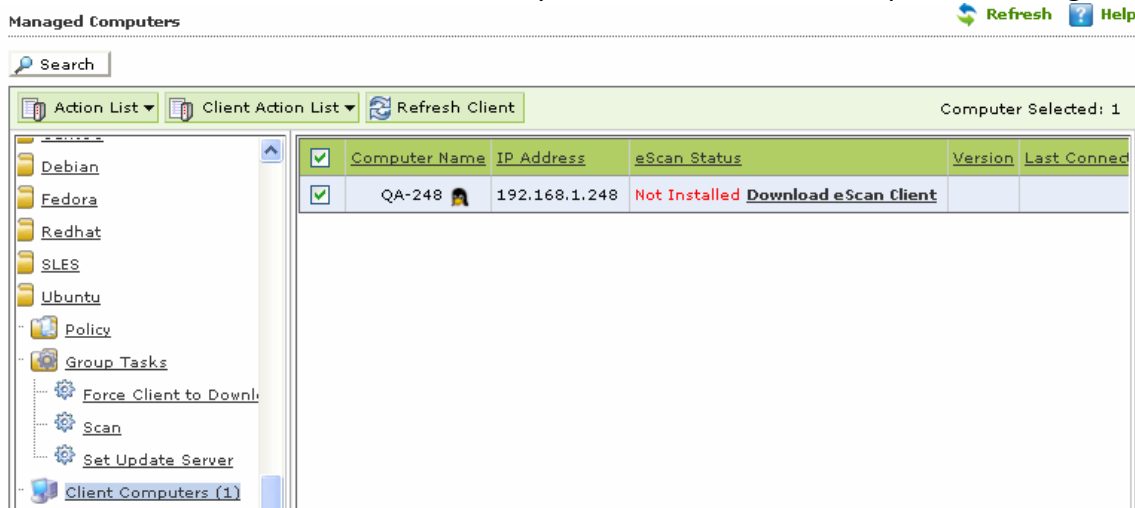


Figure 8.25

4. Download the client Setup from the link on the computer where eScan Endpoint Security server is installed.

- 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

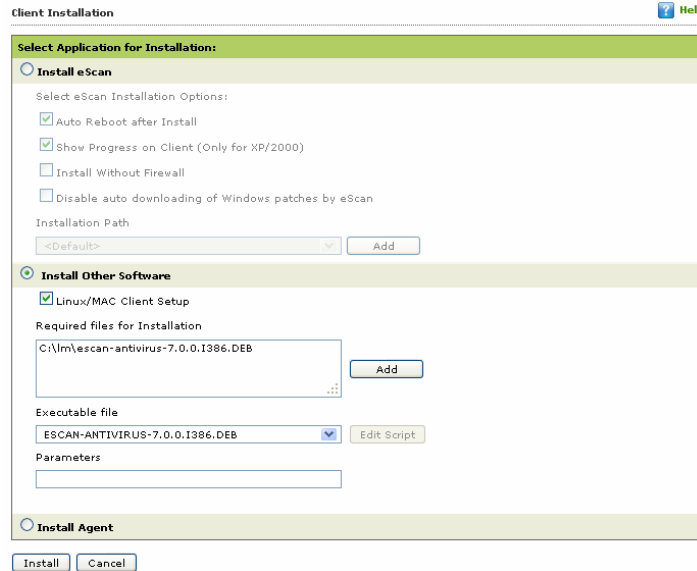


Figure 8.26

- Click on Install button to initiate the installation process.
- 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**

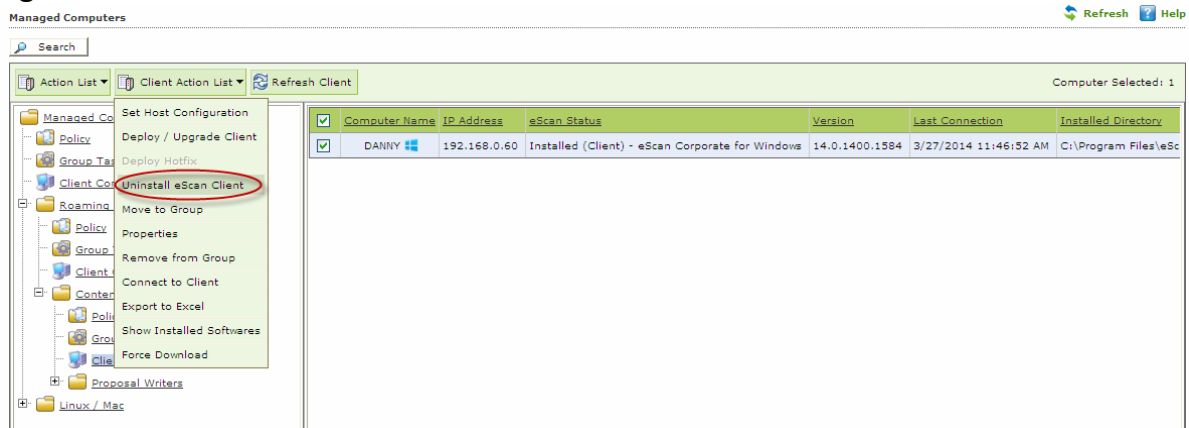


Figure – 8.27

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

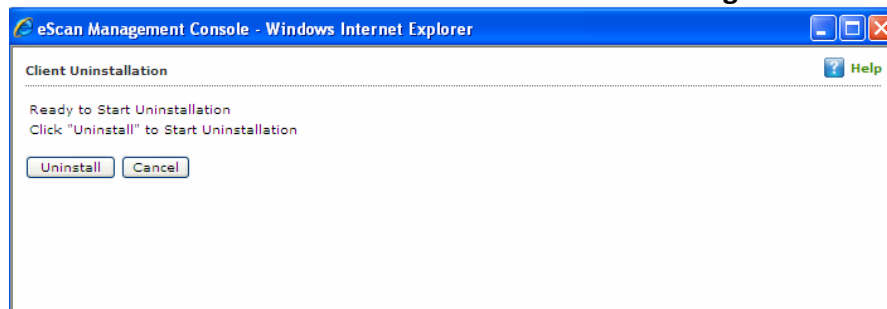


Figure – 8.28

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

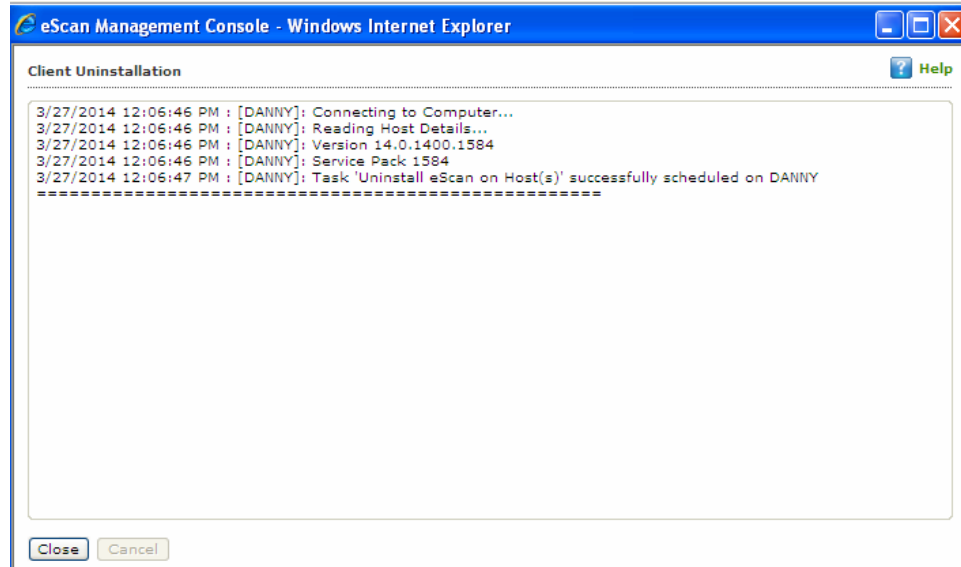


Figure – 8.29

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**

WEB CONSOLE LOGIN

Please type your User name and Password to access the Web Console.

User name:
For Active Directory account: domain\username

Password:

You can provide users the following link(s):

eScan Client Setup	
http://DANNY:10443/Setup/eScan_Client.exe	[+]
eScan Agent Setup (Windows)	
http://DANNY:10443/Setup/Agent_Setup.exe	[+]
eScan Agent Setup (Linux)	
http://DANNY:10443/Setup/Agent_Setup.deb	
http://192.168.0.60:10443/Setup/Agent_Setup.deb	
http://DANNY:10443/Setup/Agent_Setup.rpm	
http://192.168.0.60:10443/Setup/Agent_Setup.rpm	
eScan Agent Setup (MAC)	
http://DANNY:10443/Setup/Agent_Setup.dmg	
http://192.168.0.60:10443/Setup/Agent_Setup.dmg	

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**

WEB CONSOLE LOGIN

Please type your User name and Password to access the Web Console.

User name:
For Active Directory account: domain\username

Password:

You can provide users the following link(s):

eScan Client Setup	[+]
http://DANNY:10443/Setup/eScan_Client.exe	
eScan Agent Setup (Windows)	[+]
http://DANNY:10443/Setup/Agent_Setup.exe	
eScan Agent Setup (Linux)	[-]
http://DANNY:10443/Setup/Agent_Setup.deb	
http://192.168.0.60:10443/Setup/Agent_Setup.deb	
http://DANNY:10443/Setup/Agent_Setup.rpm	
http://192.168.0.60:10443/Setup/Agent_Setup.rpm	
eScan Agent Setup (MAC)	[-]
http://DANNY:10443/Setup/Agent_Setup.dmg	
http://192.168.0.60:10443/Setup/Agent_Setup.dmg	

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**

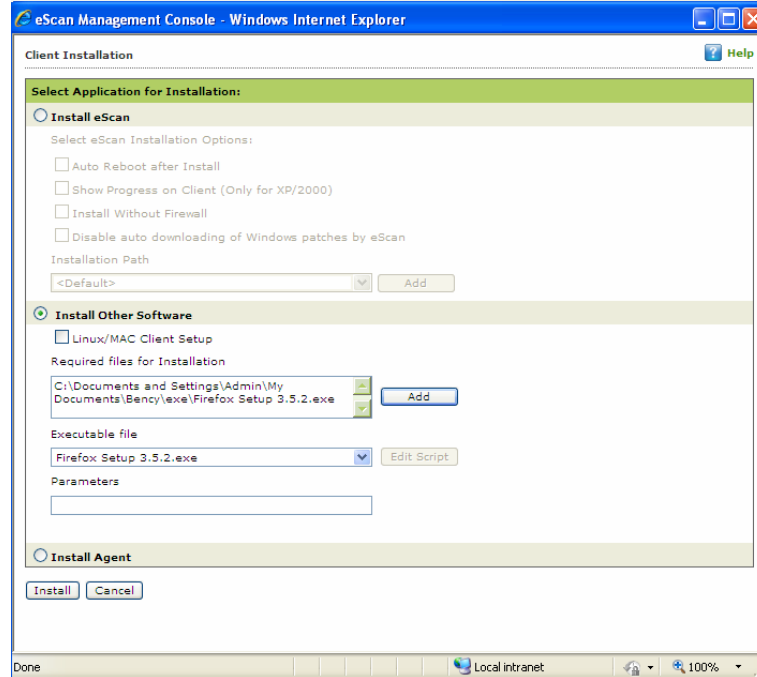


Figure - 8.32

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**

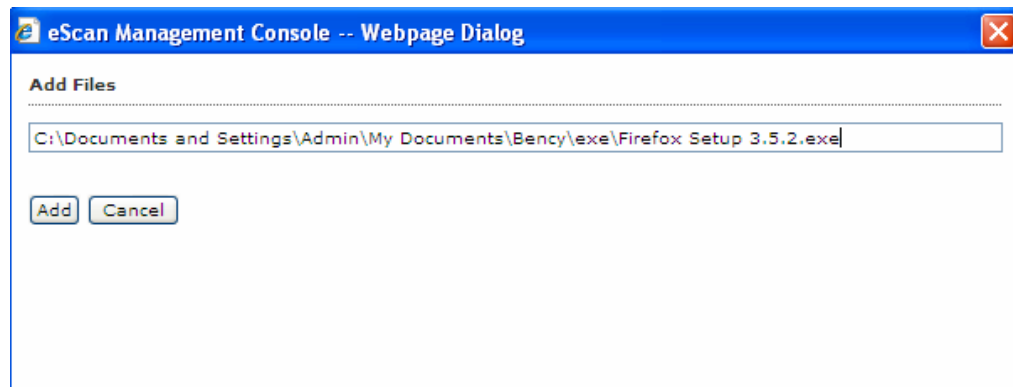


Figure - 8.33

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

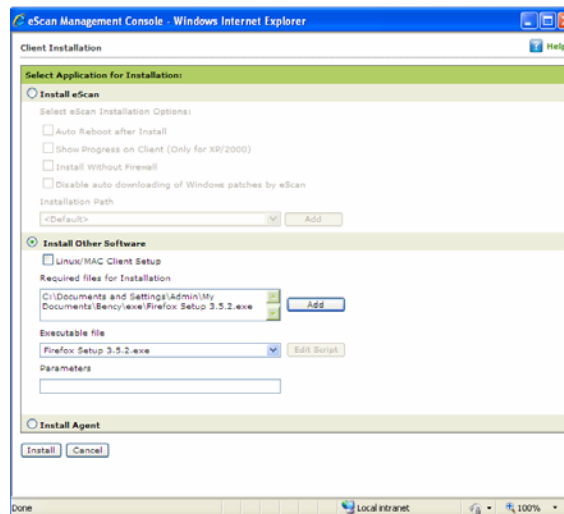


Figure - 8.34

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**

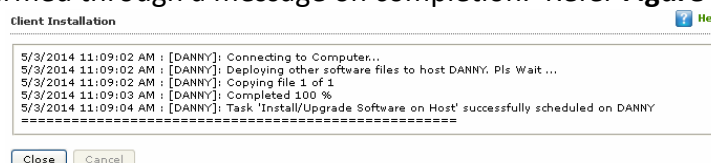


Figure 8.35

“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 Policies and creating tasks through eScan Management Console.

Defining Policies for the Group - Using the policies 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
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.
Administrator Password	This will allow you to set password to enter into eScan Protection Center.
Notifications & Events	This will allow you to stop receiving the events and notification for all the executable and websites that are allowed.

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

Modules	Description
Endpoint Security  <i>Block USB storage device - This option is present in settings under Protection Module in eScan for Mac</i>	This will allow you to block USB storage device from accessing your computer. This option is available only in Mac computers.

Steps for Defining Policies for the group

1. Click **Managed Computers**.
2. Select the desired group name from the tree

3. Now click **Policy**. Refer **Figure – 9.1**

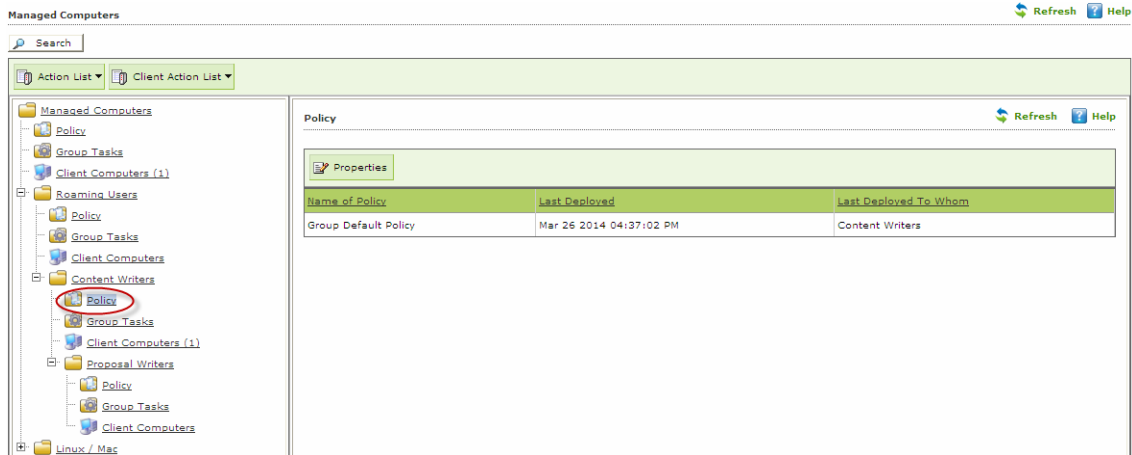


Figure – 9.1

4. Click **Properties**.

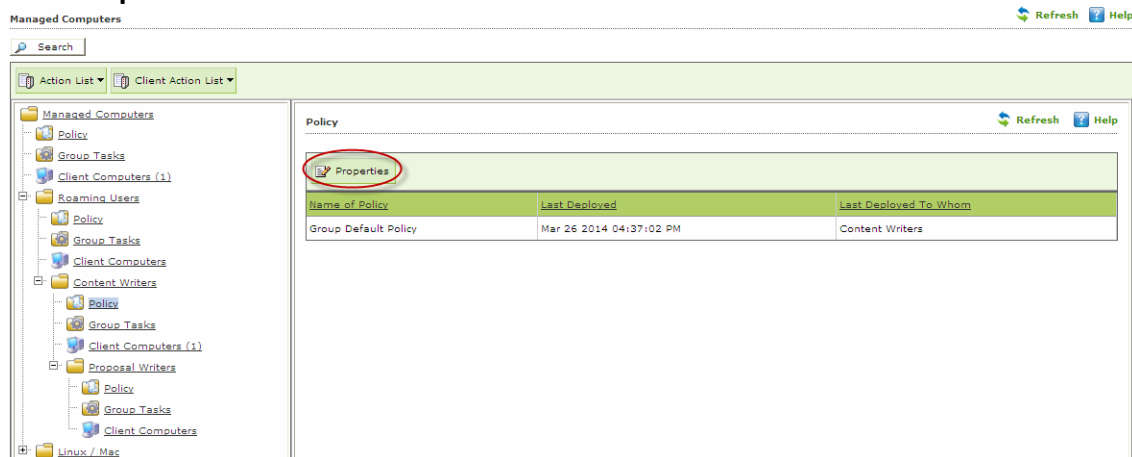


Figure – 9.2

5. You will be forwarded to the **Properties** window.

6. Now click **Policy Details** tab to re-define policies for the group. Refer **Figure – 9.3**.

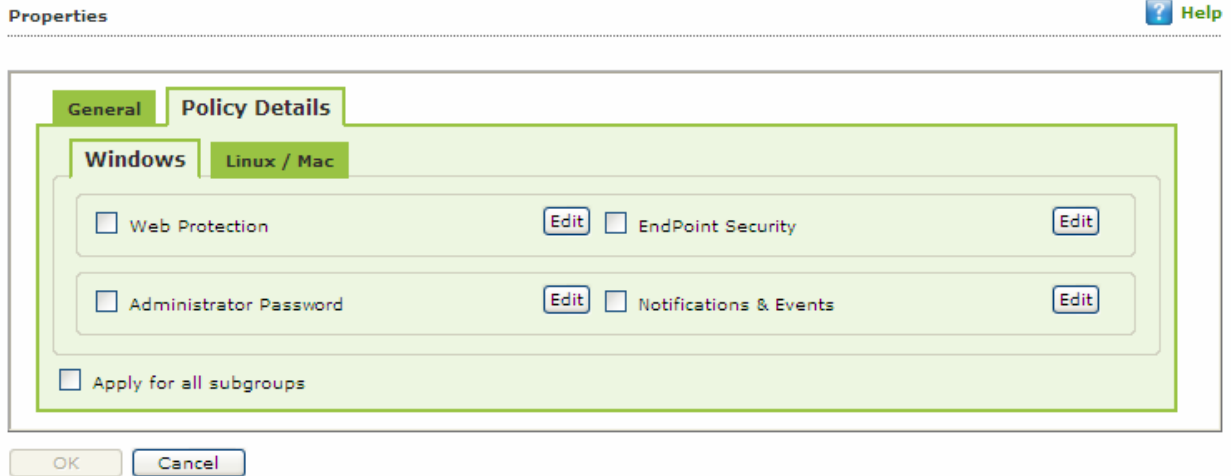


Figure – 9.3

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

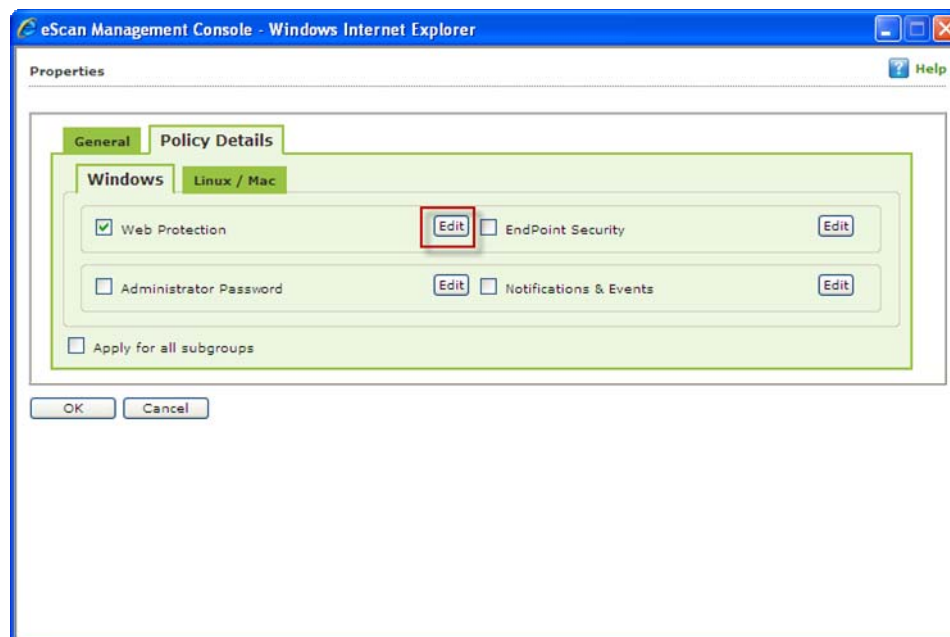




Figure – 9.4

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**

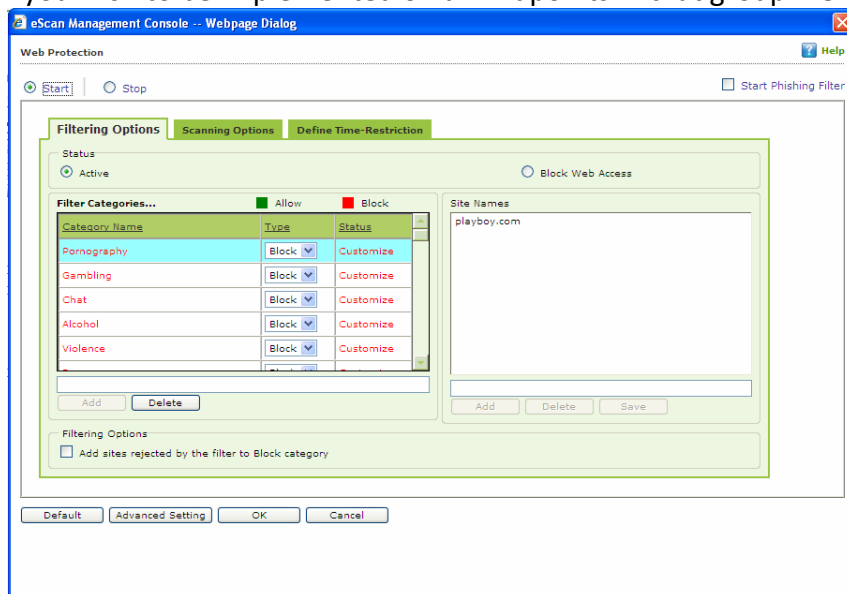


Figure 9.5

- eScan Management Console** allows you to define policies 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**

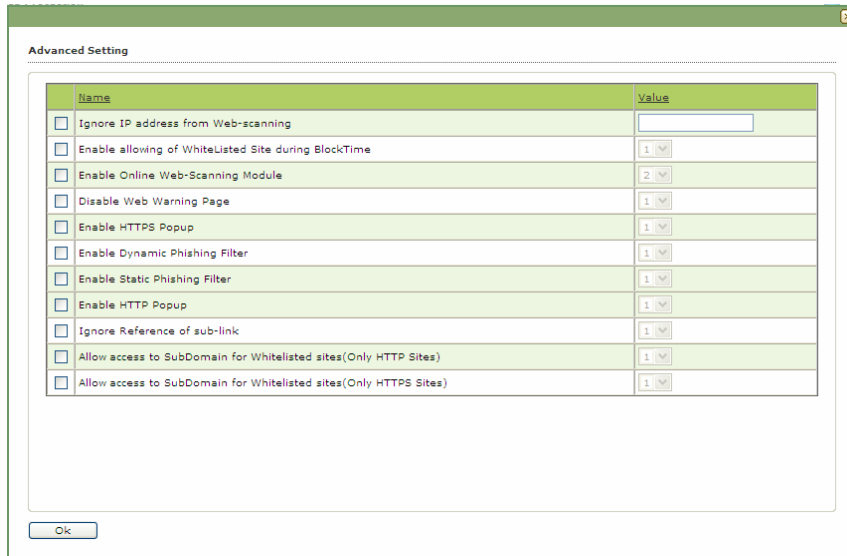


Figure – 9.6

➤ **Configurable eScan Policies for Windows Computers**

1. Web Protection

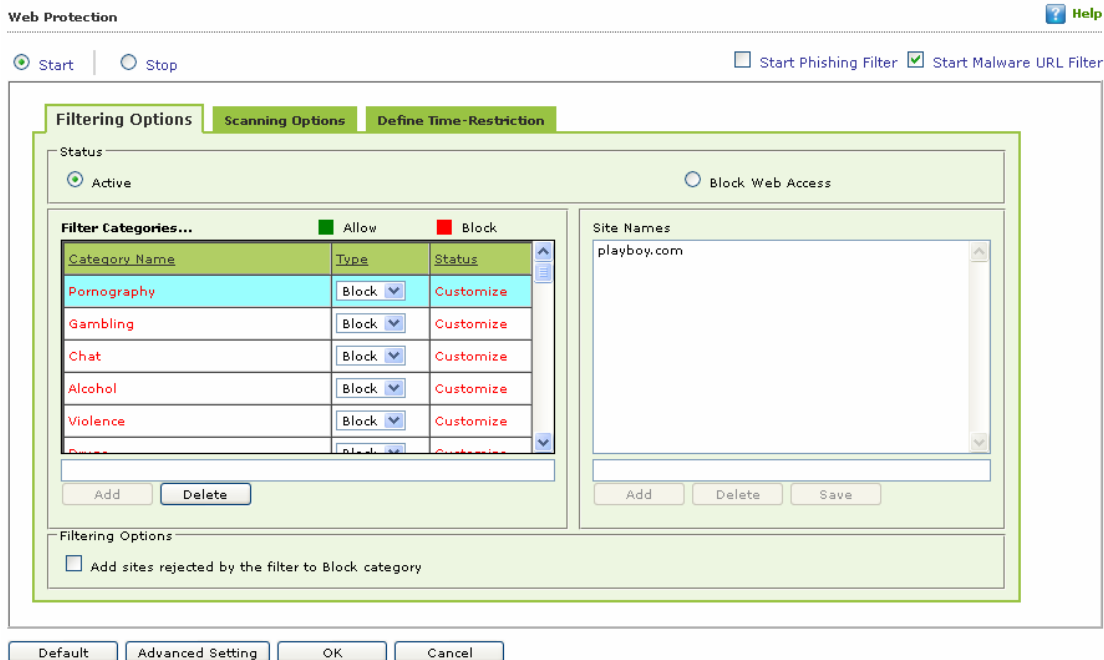


Figure – 9.7

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 to 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.
- **Block Images:** Select this check box to block download of any kind of images on managed endpoints.
- **Block Applications:** Select this check box to block the download of any applications on managed endpoints.
- **Block Emails:** Select this check box to block download of **RFC 822** type emails.
- **Block Audio files:** You should select this option if you want to block all audio files.
- **Block Video files:** you should be selecting this option if you want to block all video files.

2. Endpoint Security

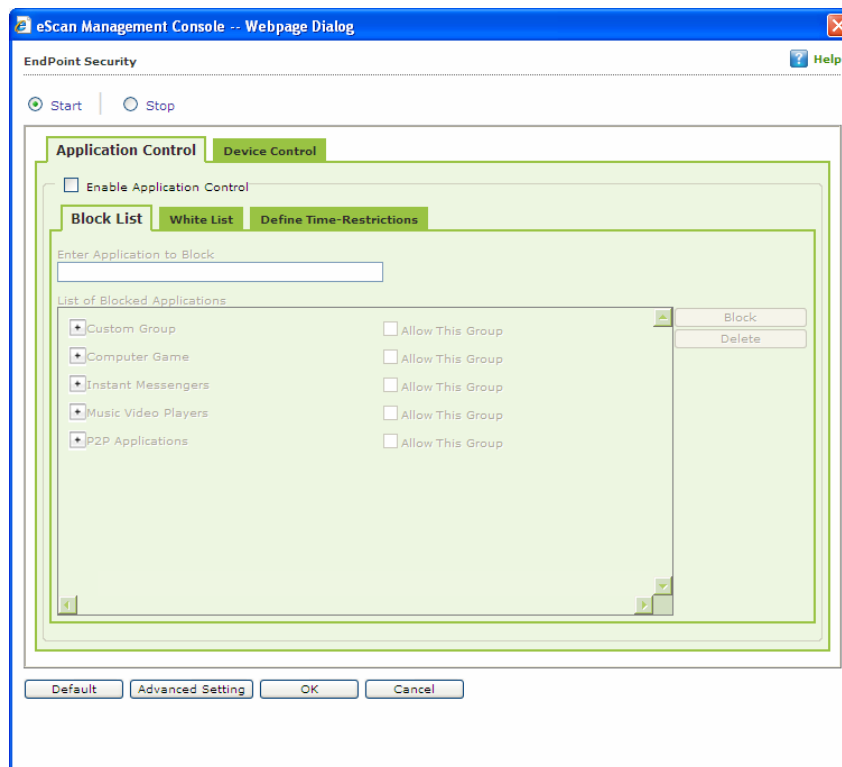


Figure – 9.8

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. Device 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 Device Control: [Default]** You should select this check box if you need to monitor all the USB storage 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.
 - **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.

- 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.
- **Disable Web Cam:** You should select this option, if you want eScan to disable Web Cam.
- **Disable Bluetooth:** You should select this option, if you want eScan to disable Bluetooth.
- **Disable SD cards:** You should select this option, if you want eScan to disable SD Cards.
- **CD/DVD Settings:** You should select this check box if you need to block any CD/ DVD or allow read only access to CD/ DVD.
 - **Block CD/DVD:** You should select this option, if you want eScan to block CD/DVD.
 - **Read only CD/DVD:** You should select this option, if you want eScan to disable CD / DVD.

Advanced Settings

Name	Value
<input type="checkbox"/> Allow Composite USB Device	1
<input type="checkbox"/> Allow USB Modem	1
<input type="checkbox"/> Enable Predefined USB Exclusion for Data Outflow	1
<input type="checkbox"/> Enable USB Whitelisting option on prompt for eScan clients	1
<input type="checkbox"/> Enable USB on Terminal Client	1
<input type="checkbox"/> Enable Domain Password for USB	1
<input type="checkbox"/> Show System Files Execution Events	1
<input type="checkbox"/> Allow execution of Microsoft Signed Application	1
<input type="checkbox"/> Allow mounting of Imaging device	1
<input type="checkbox"/> Block File Transfer from IM	1
<input type="checkbox"/> Allow WIFI Network	1
<input type="checkbox"/> Whitelisted WIFI SSID (Comma Separated)	
<input type="checkbox"/> Allow Network Printer	1
<input type="checkbox"/> Whitelisted Network Printer list(Comma Separated)	
<input type="checkbox"/> Disable Print Screen	0

Ok

Figure – 9.9

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 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.

3. Notifications and Events

Events

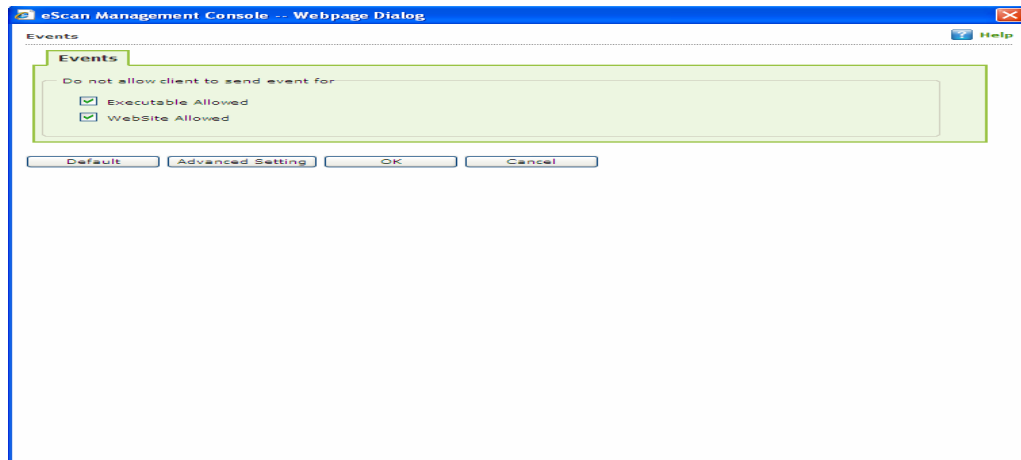


Figure – 9.10

Define settings to stop client from sending Event of certain types as per your selection.

➤ Configurable eScan Policies for Linux and Mac Computers

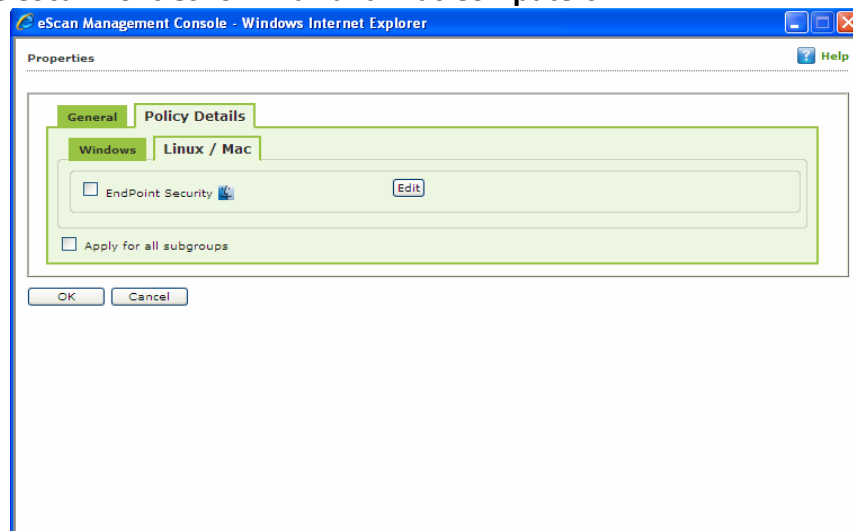


Figure – 9.11

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 Endpoint Security for 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**

- **Endpoint Security** – Settings valid for eScan client on **Mac** systems only.



Figure – 9.12

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

7. **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 – 9.13**

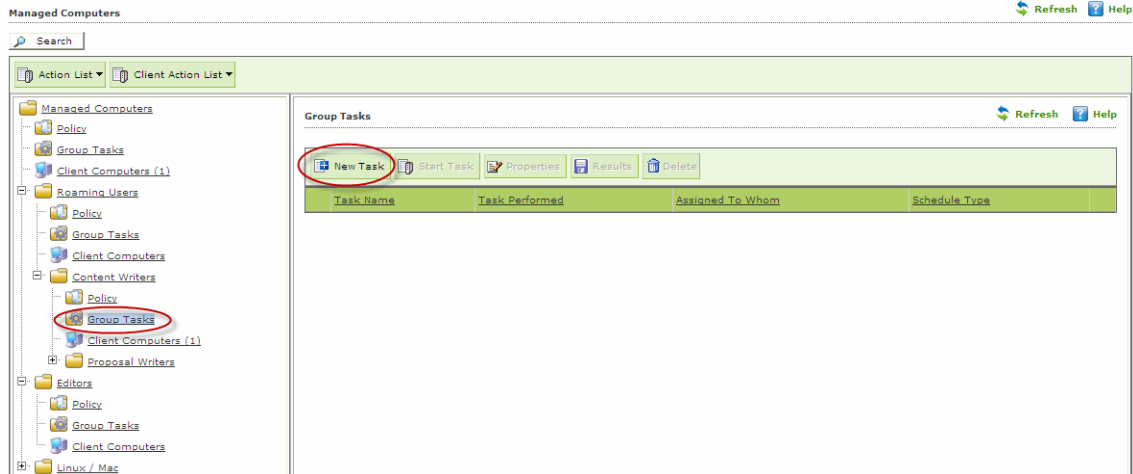


Figure – 9.13

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 – 9.14**

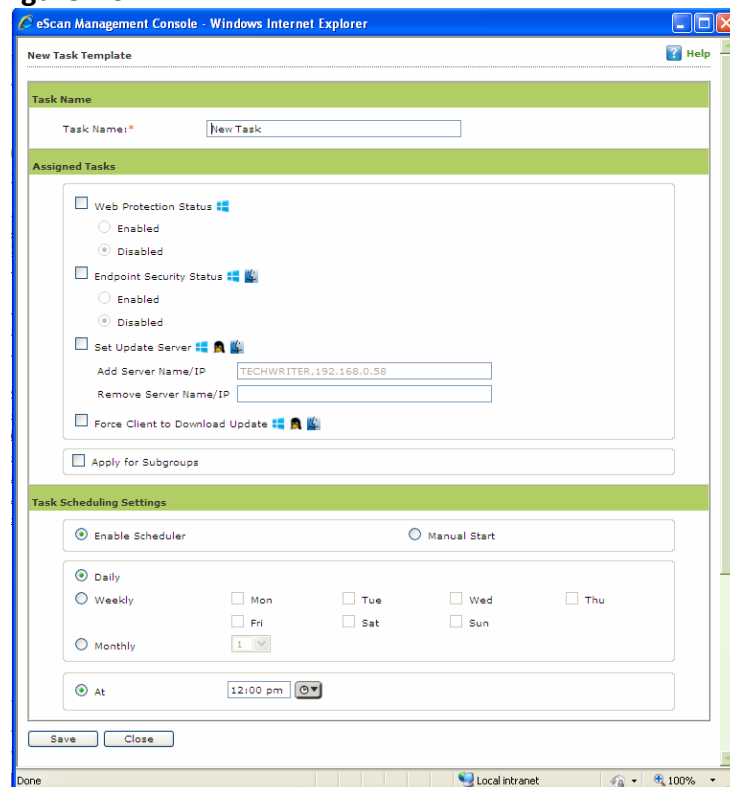






Figure – 9.14

Note:  Windows, ,  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 – 9.15**

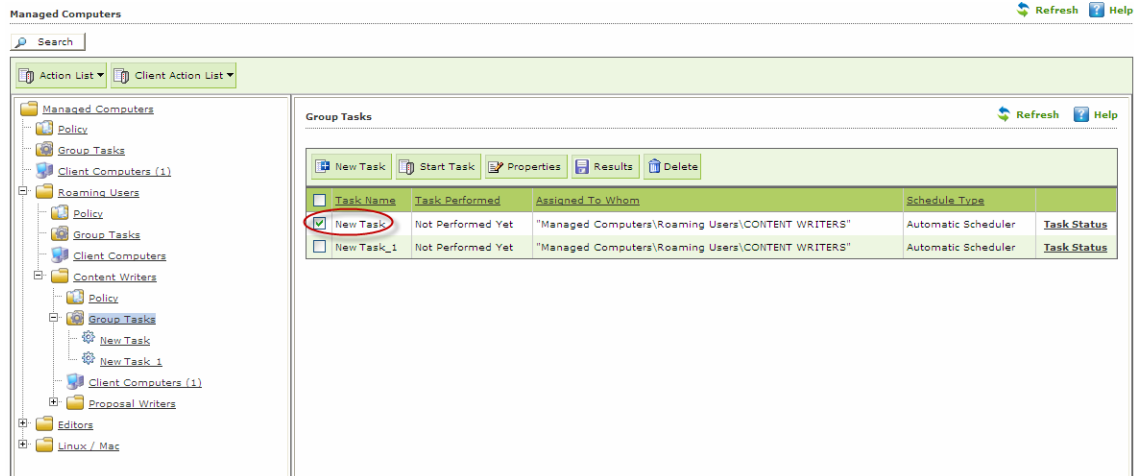


Figure – 9.15

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 – 9.16**

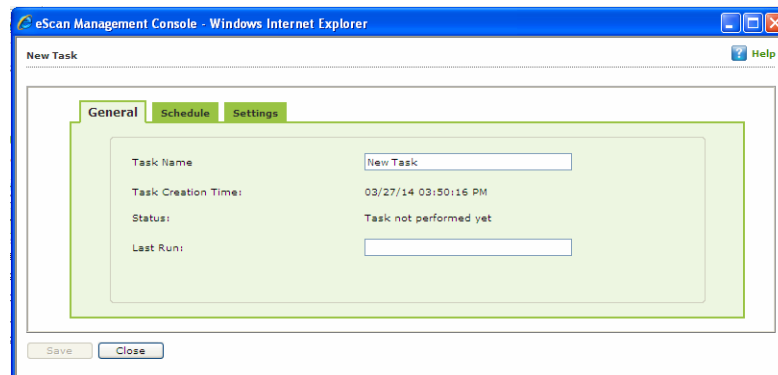


Figure – 9.16

- Using the **Start Task** option you can initiate the selected task on the Endpoints in the Group. Refer **Figure – 9.17**

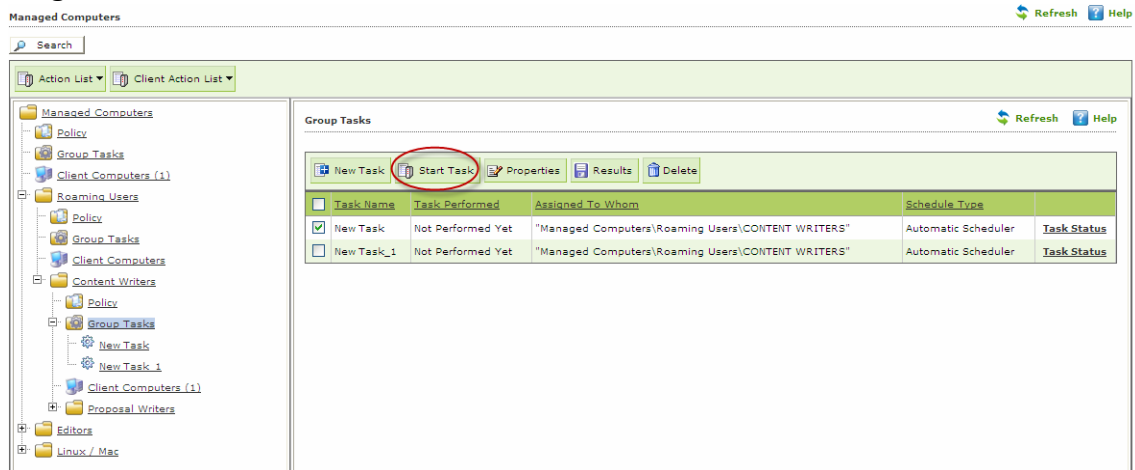


Figure – 9.17

- Click **Results** to view the details of recently executed tasks.
- Click **Task Status** Link to view the status of the listed tasks. It gives you a brief summary of the selected task. Refer **Figure - 9.18**

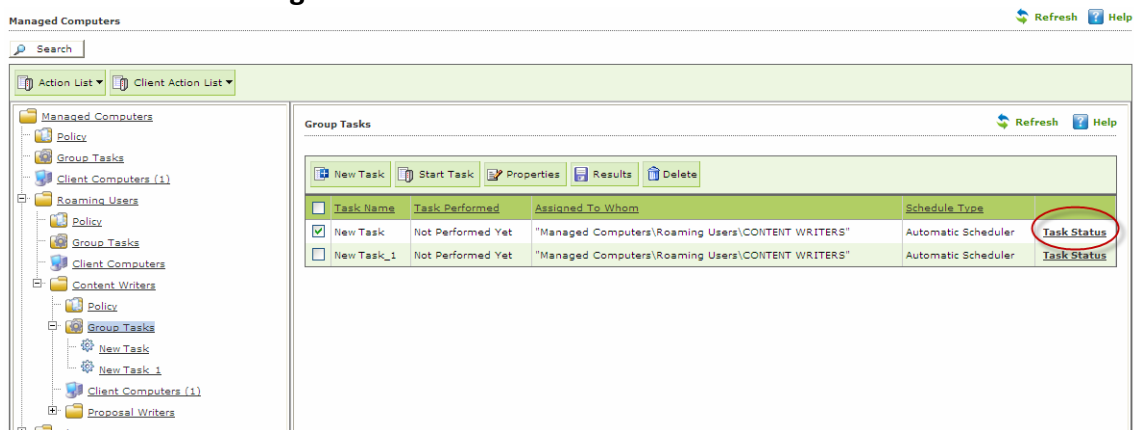


Figure – 9.18

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**

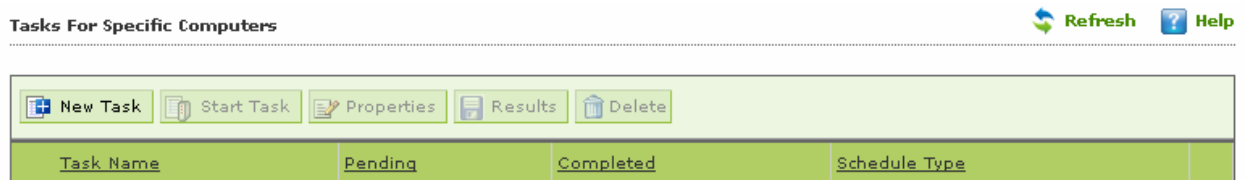


Figure 10.1

3. You will be forwarded to **New Task Template** Window.

1. Define the **Task Name** in the text field. Refer **Figure 10.2**

[Tasks For Specific Computers](#) > [New Task Template](#)

Task Name: *

Figure 10.2

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

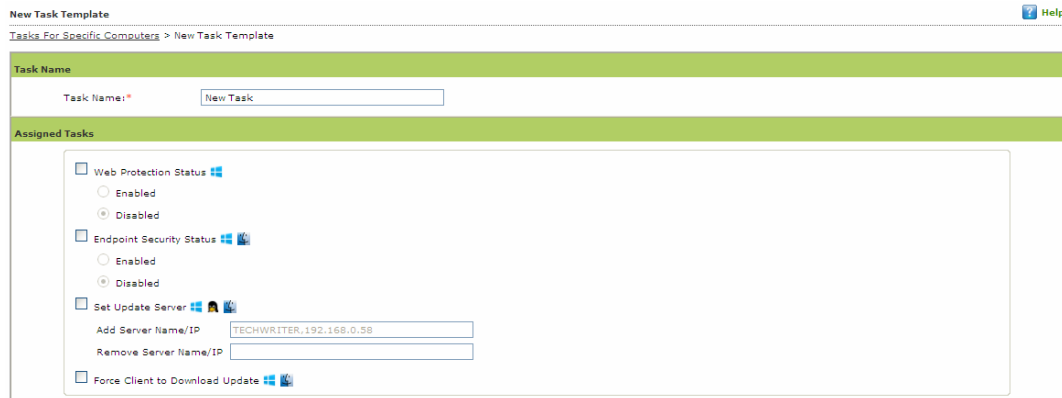






Figure 10.3

Note:  Windows, ,  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**

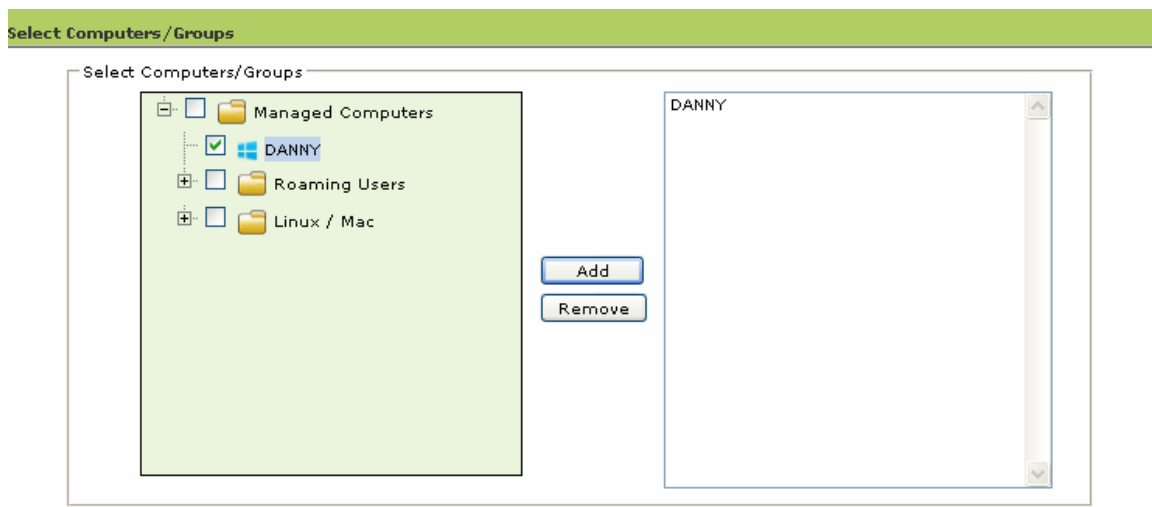
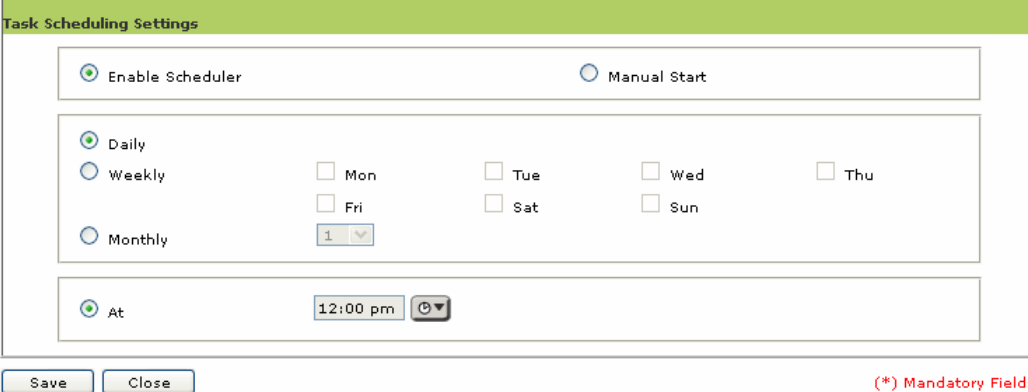


Figure 10.4

4. **Schedule the Task** as desired. Refer **Figure 10.5**



The 'Task Scheduling Settings' dialog box contains the following elements:

- Radio buttons for 'Enable Scheduler' (selected) and 'Manual Start'.
- Radio buttons for 'Daily' (selected), 'Weekly', and 'Monthly'.
 - Under 'Weekly', there are checkboxes for 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun', all of which are currently unchecked.
 - Under 'Monthly', there is a dropdown menu showing the number '1'.
- Radio button for 'At' (selected), followed by a time input field set to '12:00 pm' and a clock icon.
- 'Save' and 'Close' buttons at the bottom left.
- A red note at the bottom right: '(*) Mandatory Fields'.

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**

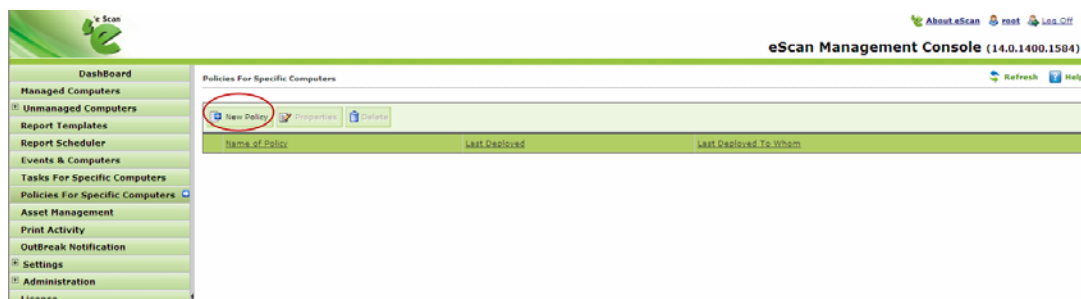


Figure 10.6

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**

New Policy Help

Select Rule-Sets For Policy

Enter Policy Name:*

Web Protection Edit EndPoint Security Edit

Administrator Password Edit Notifications & Events Edit

EndPoint Security Edit

Select Computers/Groups

Select Computers/Groups

Managed Computers

Add
Remove

Deploy Cancel

(*) Mandatory Fields

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

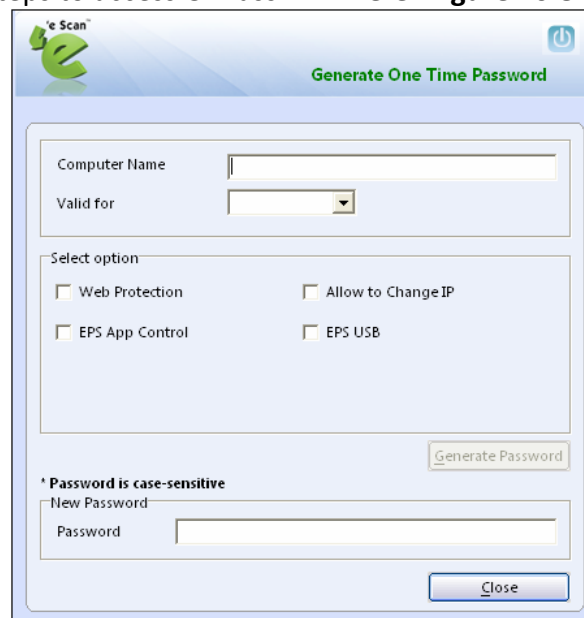


Figure 10.8

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

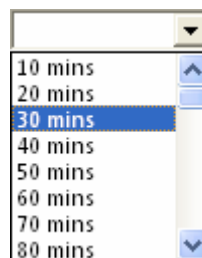


Figure 10.9

7. Select the Module that you wish to enable or disable using check boxes present on the interface and click on Generate Password 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 Endpoint Security for Windows Client using right click on eScan Endpoint Security for Windows icon and click on Pause Protection from the task bar. **Refer Figure 10.11**

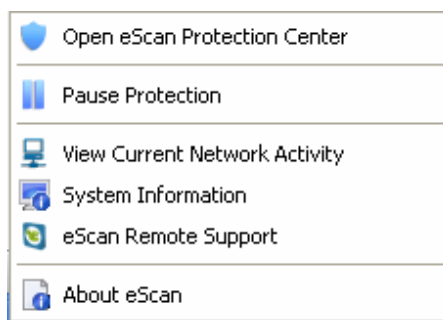


Figure 10.11

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**

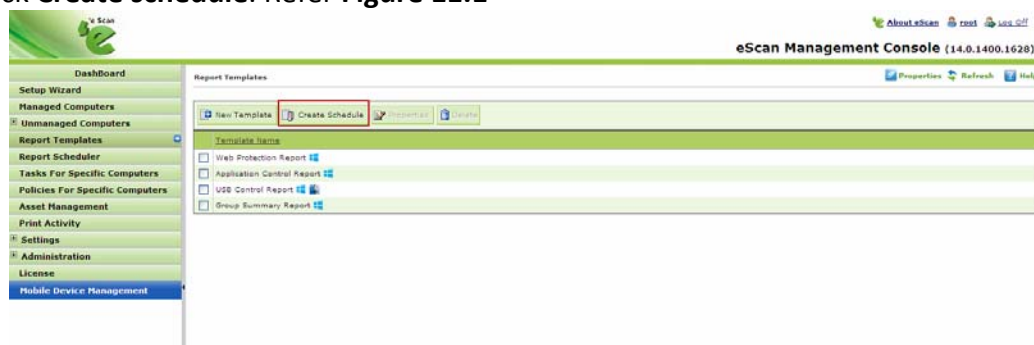


Figure 11.1

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

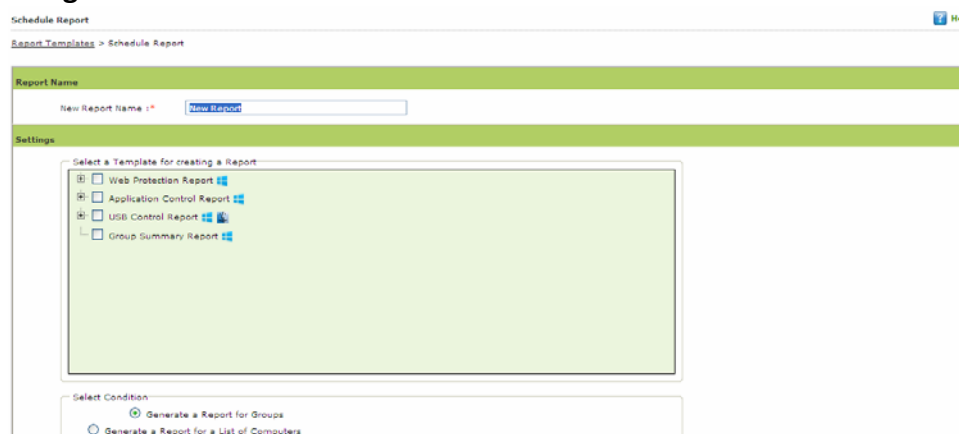


Figure 11.2

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

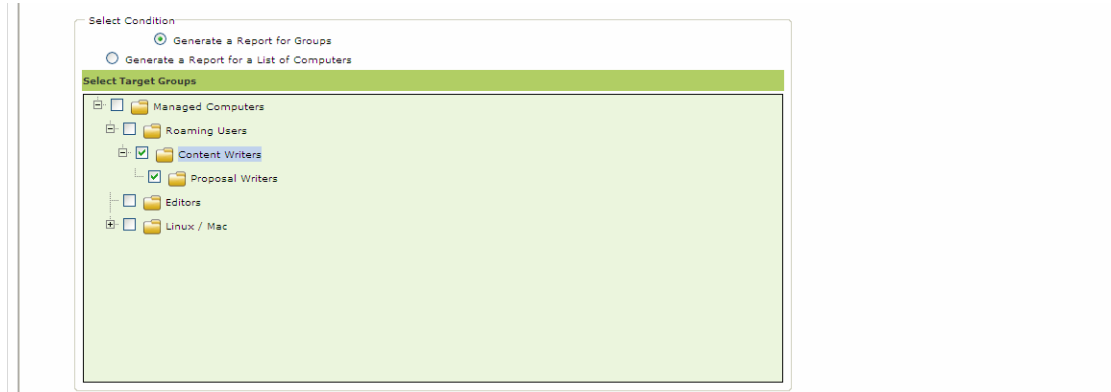


Figure 11.3

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. Refer **Figure - 11.4**.

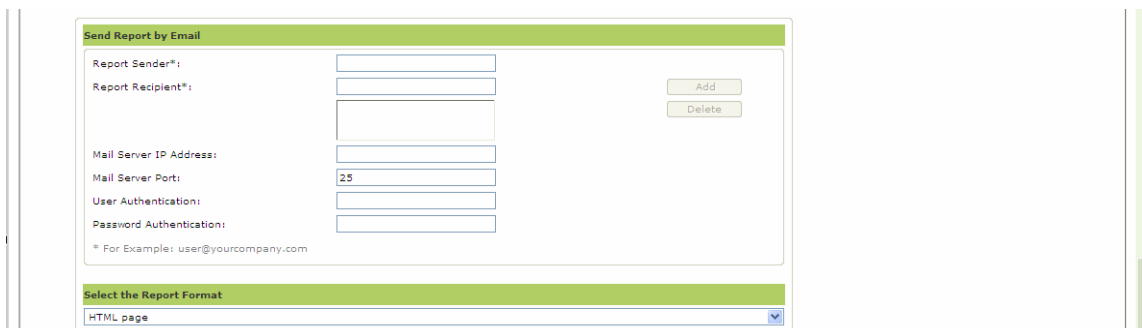


Figure - 11.4

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

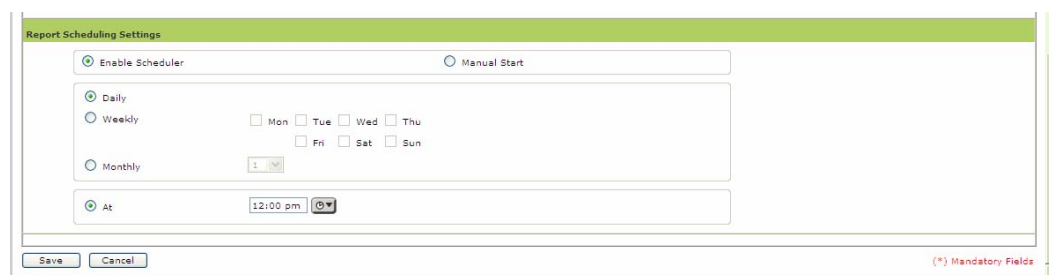


Figure 11.5

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

Report Scheduler

 Refresh  Help







 Start Task	 Results	 Properties	 Delete	 New Schedule	 View & Create
<u>Schedule Name</u>	<u>Report Recipient</u>	<u>Scheduler Type</u>	<u>View</u>		
<input checked="" type="checkbox"/> New Report	abhishek@escanav.com	Automatic Scheduler	View		

Figure 11.6

Note:

- You can Options to create and schedule reports are also present in Report Scheduler section of **eScan Management Console**.

12. 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 on the Managed 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.	PC Identifying umber	It displays the unique Identification number of each Managed Endpoint.
16.	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 **▲ Filter Criteria** in **Asset Management** section. The Hardware report can be filtered on the basis of following Criteria. Refer **Figure 12.1**

Figure 12.1

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 **▲ Filter Criteria** in Asset Management Section. The Software report can be filtered on the basis of following Criteria.

Figure 12.2

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

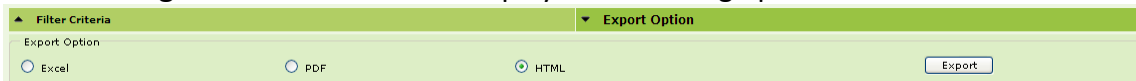


Figure 12.3

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 12.4

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

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.
 - 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.
 -
 - 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.
- **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 13.1**

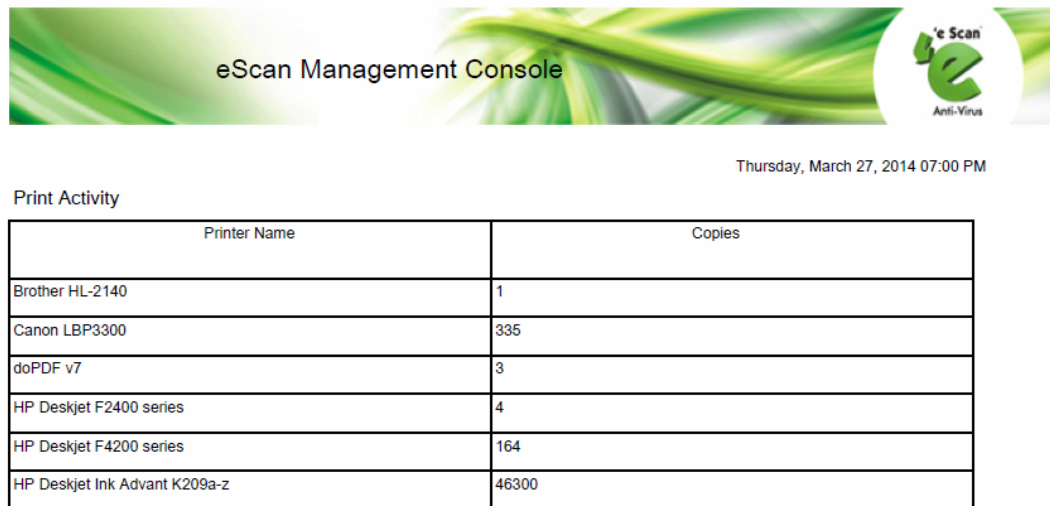


Printer Name	Copies
Brother HL-2140	1
Canon LBP3200	232
60PDF v7	2
HP Deskjet F2400 series	4
HP Deskjet F4200 series	164
HP Deskjet Ink Advant K209anz	46200
HP Deskjet Ink Advant K209anz (Copy 1)	4533
HP Fax/Print Ink Advant K209anz (Copy 1)	1840

Figure 13.1

● **Viewing the Print Logs**

For viewing the Print log of a Printer listed in the Printing Activity table, click on the number of Copies under copies column, this will forward you to the Print Activity window. Refer **Figure 14.2**



The screenshot shows the eScan Management Console interface. At the top, there is a header with the text "eScan Management Console" and the eScan logo. Below the header, the date and time "Thursday, March 27, 2014 07:00 PM" are displayed. The main content area is titled "Print Activity" and contains a table with two columns: "Printer Name" and "Copies". The table lists several printers and their corresponding copy counts.

Printer Name	Copies
Brother HL-2140	1
Canon LBP3300	335
doPDF v7	3
HP Deskjet F2400 series	4
HP Deskjet F4200 series	164
HP Deskjet Ink Advant K209a-z	46300

Figure 13.2

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.

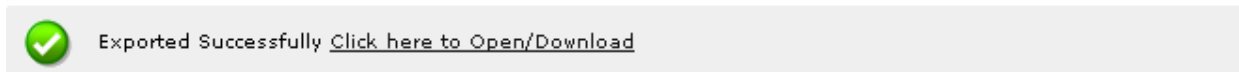


Figure 13.3

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

• **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**

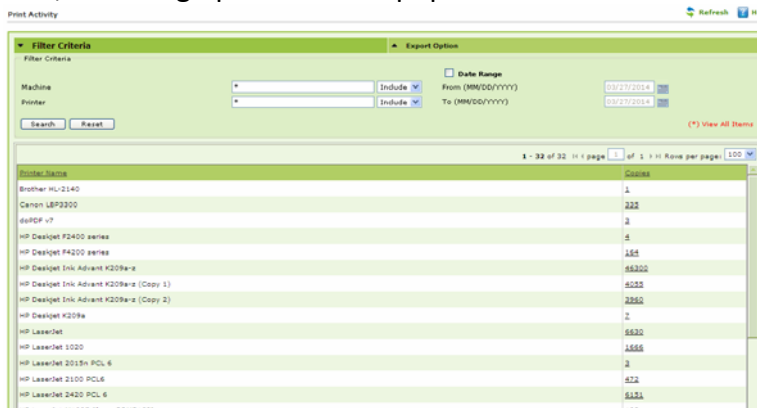


Figure 13.4

S.No.	Option	Description
1.	Machine	Type the desired machine name that you wish to exclude or include in your Log.
2.	Not	Tick on this checkbox, if you wish to exclude a machine in the log report.
3.	Printer	Type the desired printer name that you wish to exclude or include in your log.
4.	Not	Tick on this checkbox, if you wish to exclude a printer to in the log report.
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 **Export Option** in Print Activity Section. It will display the following options.



Figure 13.5

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 –



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

14. 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.

14.1. 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 14.1**

Figure 14.1

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.

14.2. 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.

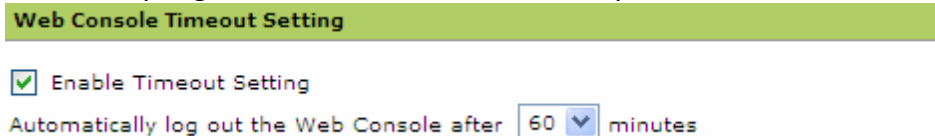


Figure 14.2

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.

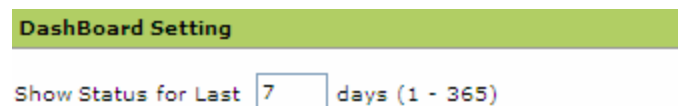


Figure 14.3

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.

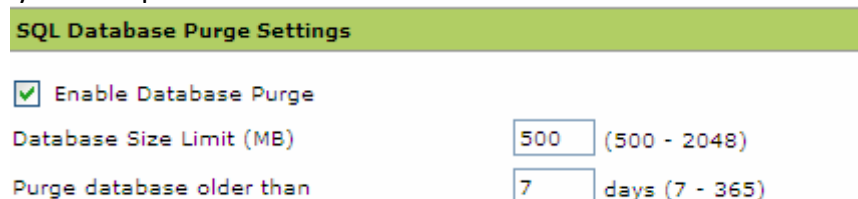


Figure 14.4

Click **Save** to save the defined settings

14.3. Update Settings

The Update module allows you to 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. Refer **Figure 14.5**

Update Settings [Help](#)

General Config
Update Notification
Scheduling

Select Mode

FTP HTTP

Proxy Settings

Download via Proxy

HTTP

HTTP Proxy Server IP : Port:

Login Name : Password :

FTP

FTP Proxy Server IP: Port:

Login Name : Password :

Logon Type

User@siteaddress

OPEN siteaddress

PASV Mode

Socks

Save
Cancel
Update

Figure 14.5

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 updaters downloads the eScan updates. Refer **Figure 16.6**

Update Settings [Help](#)

General Config | **Update Notification** | **Scheduling**

Update Notification

Sender:

Recipient:

SMTP Server: SMTP Port:

Use SMTP Authentication

User name:

Password:

Figure 14.6

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. Refer **Figure 14.7**

Update Settings Help

General Config | **Update Notification** | **Scheduling**

Automatic Download

Query Interval: minutes

Schedule Download

Daily

Weekly

Monthly

At

Mon Tue Wed Thu
Fri Sat Sun

1 of the month

1:50 PM

Save Cancel Update

Figure 14.7

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.

15. 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 –**

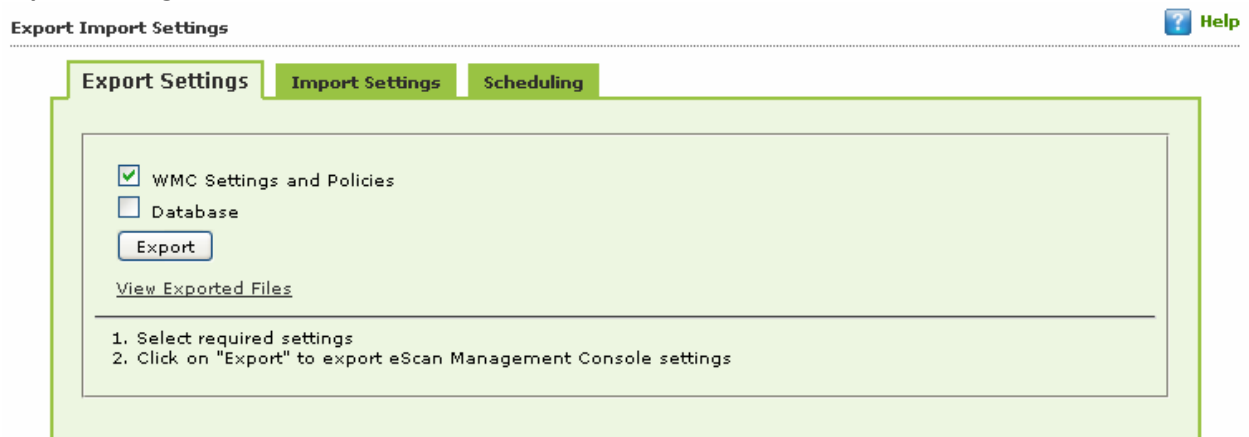


Figure 15.1

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**

Export Import Settings

Export Settings | **Import Settings** | Scheduling

File Name

WMC Settings and Policies

Database

1. Select file to import (EservConf_[YYYYMMDDhhmm]_[_SCHD].zip)
2. Select required settings
3. Click on "Import" button to import the saved settings

Figure 15.2

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**

Export Import Settings

Export Settings Import Settings **Scheduling**

Enable Export Scheduler

WMC Settings and Policies Database

Daily
 Weekly Mon Tue Wed Thu
 Fri Sat Sun
 Monthly

At

Enable Notification settings

Sender:
Recipient:
SMTP Server:
SMTP Port:

Use SMTP Authentication

User name:
Password:

Enable Optional Settings

Select how many backup files to store

Create the backup only if drive space is greater than or equal to :

[View Exported Files](#)

Last schedule status : Unknown Status

Figure 15.3

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.

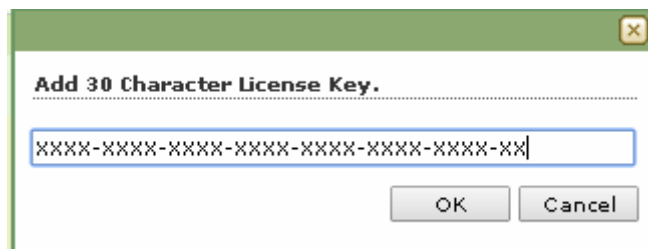


Figure 16.2

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

License [Refresh](#) [Help](#)

Register Information

License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX	Activate Now	Activate before 02-May-2014	-	150

To Add License [Click Here](#)

Figure 16.3

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 operating system**.

17. Introduction - eScan Mobile Device Management

eScan Mobile Device Management solution is specifically designed for XE "Android" Mobile or Smart Phone devices. It 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, manage all your android devices remotely. Using this solution you can control and monitor all security settings, gain real-time visibility 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 Endpoint Security	For using eScan Mobile Device Management server, you first need to install eScan Endpoint Security 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 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 will display the devices synced within the defined time period. Such as devices synced today, within last 1-2 days, 3-7 days, etc. and also devices that are not yet synced.
	Device Compliant	It will display the devices that are compliant with the policies defined, non-compliant with the policies defined and unknown.
	Protection Status	
	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 control	It displays the status of Applications blocked or started t 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	
	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 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 Data	Wipe Data feature that helps users to remotely delete contacts and SMSs from devices that are either lost or stolen.
	Block Device	Allows you to remotely block the device
	Scream	Raise an Alarm on the Device for easy location
	Send Message	Allows you to send some message to the device
	Locate Device	The Locate Device feature helps track the location of the lost device through GPS finder.
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
	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 Groups/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 events which received from 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 shows the list of all the outgoing, incoming calls, along the details such as the name of the contact as in the contact list, type of call (incoming/ outgoing), call time, date and duration.

 Features of eScan Mobile Security (Client)

S.No.	Features	Description
1.	Device Compliance	This will display the compliance status of the device as healthy or non-compliant.
2.	Call and SMS Filter	It will allow you to filter SMS on the basis of black list and whitelist created by you. It will also allow you to filter the Outgoing calls based on the white list created by you.
3.	Backup	Take a Backup of SMS and Contacts and also restores MSMS and contacts from managed device to the server.
4.	Parental Control	Block execution of Unwanted Applications as well as opening on unwanted websites on the device, as desired.

5.	Anti-Theft	Use this option to Enable Anti-theft module on the device, administrator Use this feature for locating 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.
6.	Privacy Advisor	Shows the permissions for installed applications on your device.
7.	Applications	It will allow to add apps from the console and also allows you to add the downloaded applications.
8.	Additional Settings	Configure Advanced Settings for your device for showing notifications, sound notifications, creating secret code, Write logs, and Uninstall eScan from Device, Sync with the Server, and Change Server and Port Address.

18. 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 Endpoint Security Installation. Once eScan Endpoint Security is installed, using eScan Endpoint Security 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 -

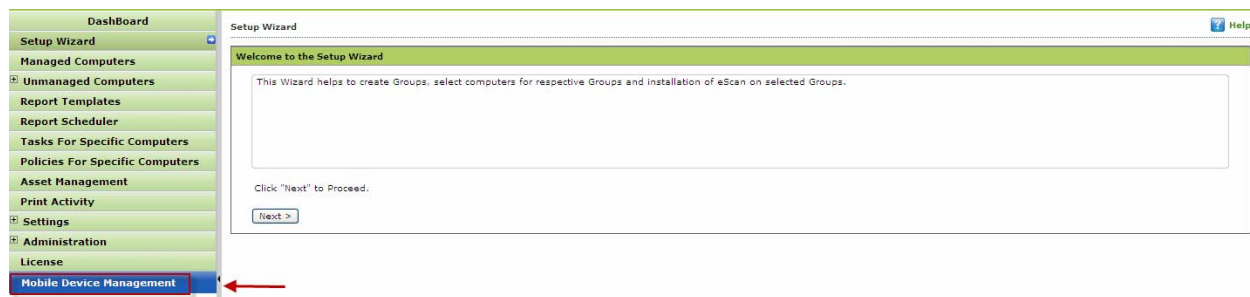



Figure 18.1

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.

19. Working with eScan Mobile Device Management Console

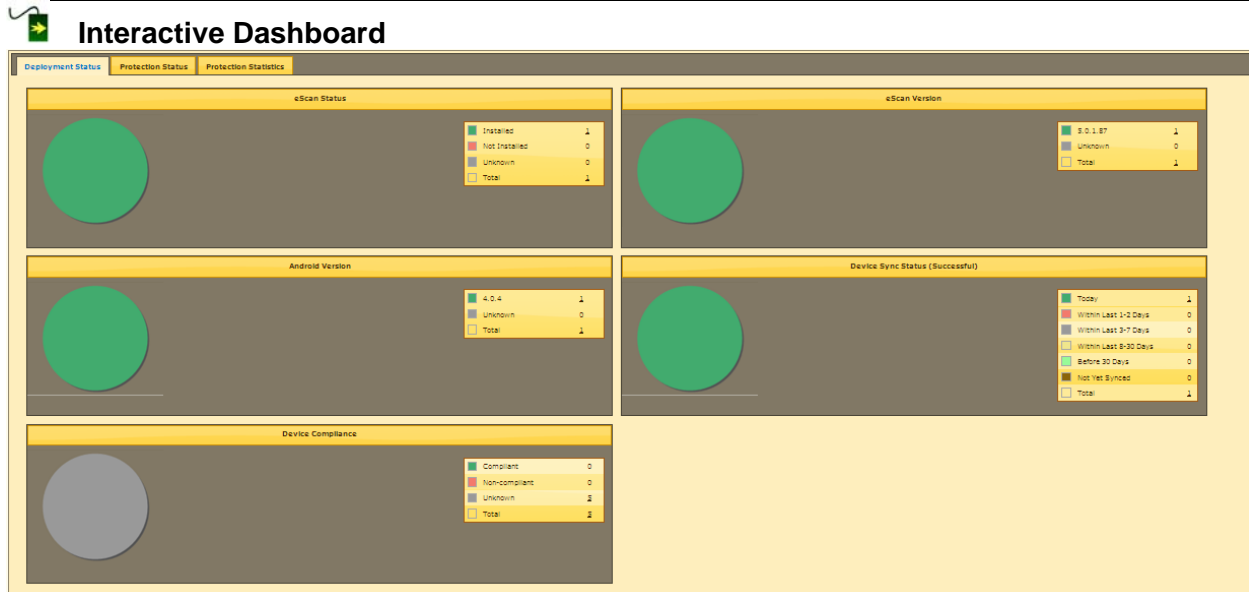


Figure 19.1

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 (Successful)** – This will display the list of devices synced with on the basis of time period and also the list of devices that are not synced. It will display the devices that are synced as of today, in the last 2 days, in last 3-7 days, within the last 8- 30 days, and before 30 days
- **Device Compliance** – This will display the compliance status of the device as healthy or non-compliant. The device is identified as healthy or non- compliant based on the policies defined for the managed group.

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

- **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.

- **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 numbers for SMS received or sent on Managed Devices. Further details can be viewed by clicking on the numeric values for respective details.

Managed Mobile Devices

- Creating Groups, Adding Devices and Uninstalling eScan

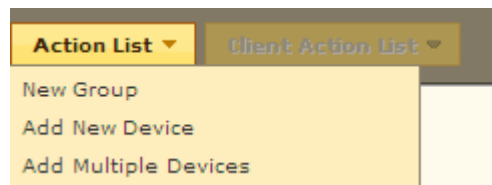


Figure 19.2

S.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.

Create New Group



Figure 19.3

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.

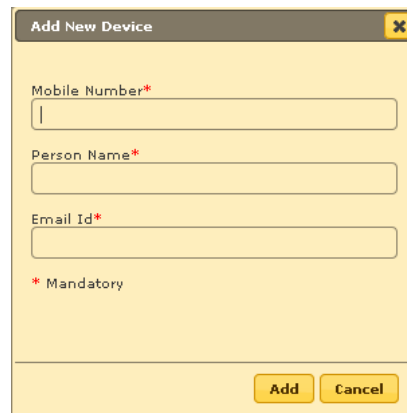


Figure 19.4

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:

Using the Same enrollment details the user should register the product from the device.

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.

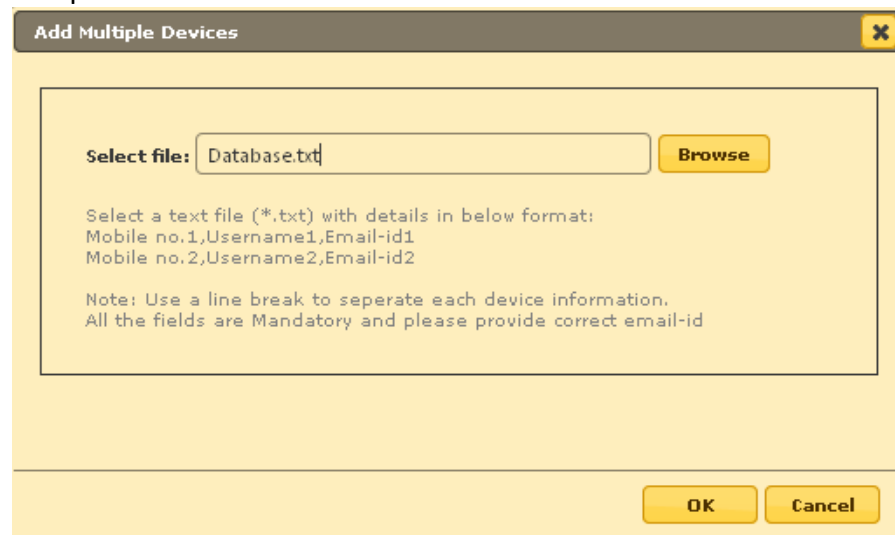


Figure 19.5

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 –

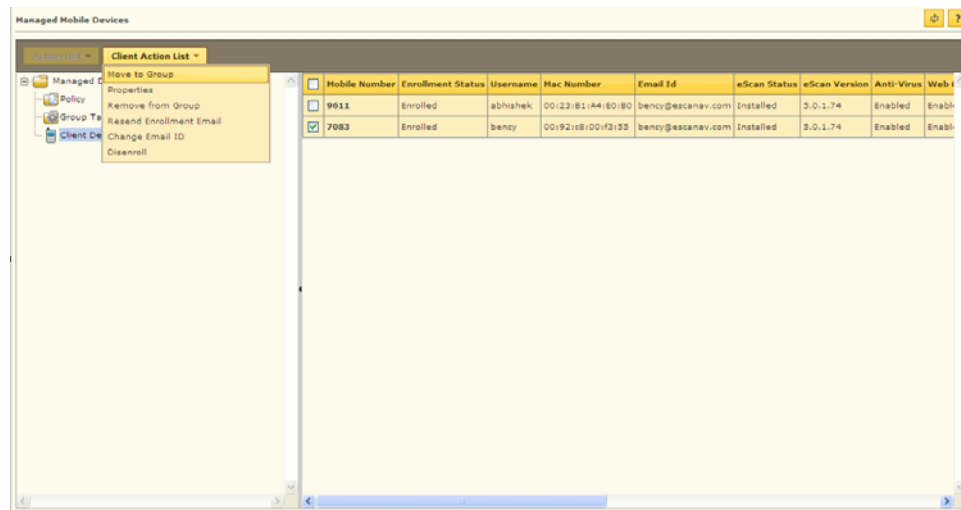


Figure 19.6

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 19.7

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 -

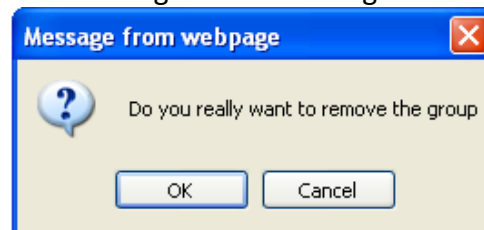


Figure 19.8

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 user 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.

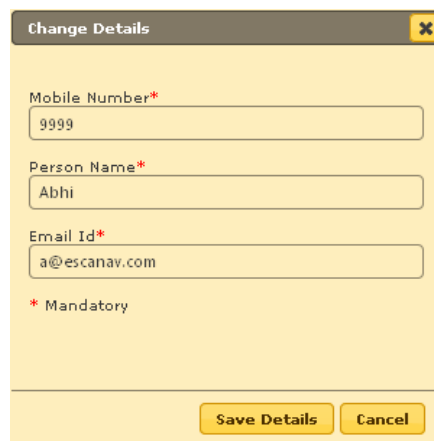
 **Resending Enrollment Email**

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 –



Change Details

Mobile Number*
9999

Person Name*
Abhi

Email Id*
a@escanav.com

* Mandatory

Save Details Cancel

Figure 19.9

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**.

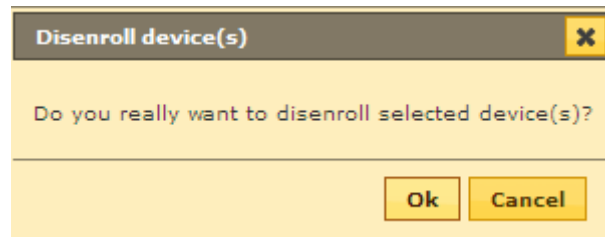


Figure 19.10

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 –

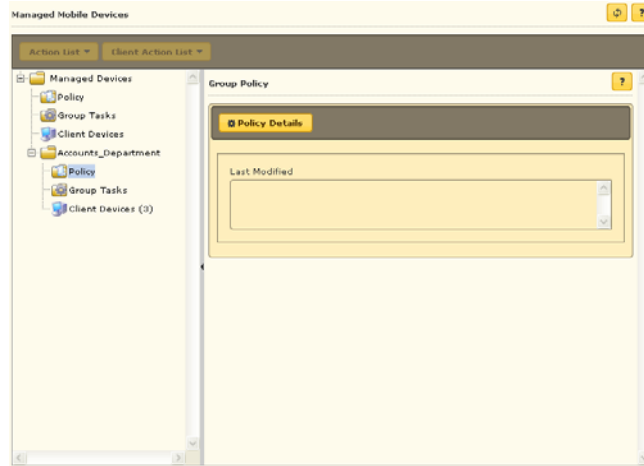


Figure 19.11

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

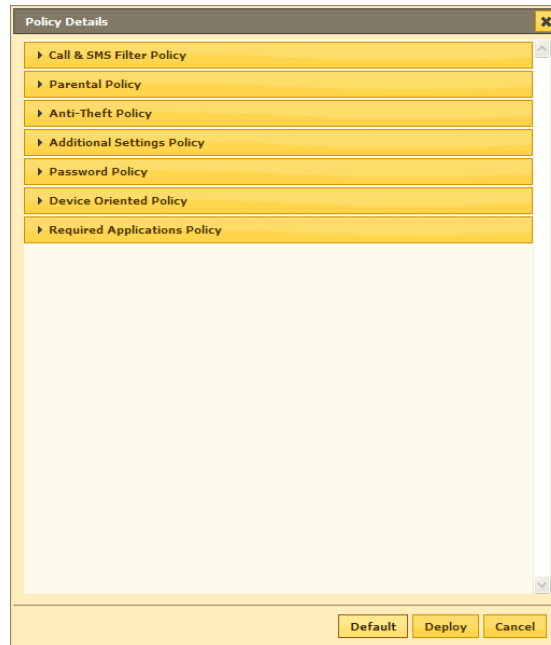


Figure 19.12

Call and SMS Filter Policy

Click **Call and SMS Filter Policy** to define policies for Filtering Calls and SMS on the basis of the whitelist and blacklist created by you. It will allow incoming calls and SMS only from the numbers in your contact list and also block SMS and calls from non-numeric numbers for all managed devices.

Figure 19.13

It includes following options –

Option	Description
Call and SMS Filter Mode	
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

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.

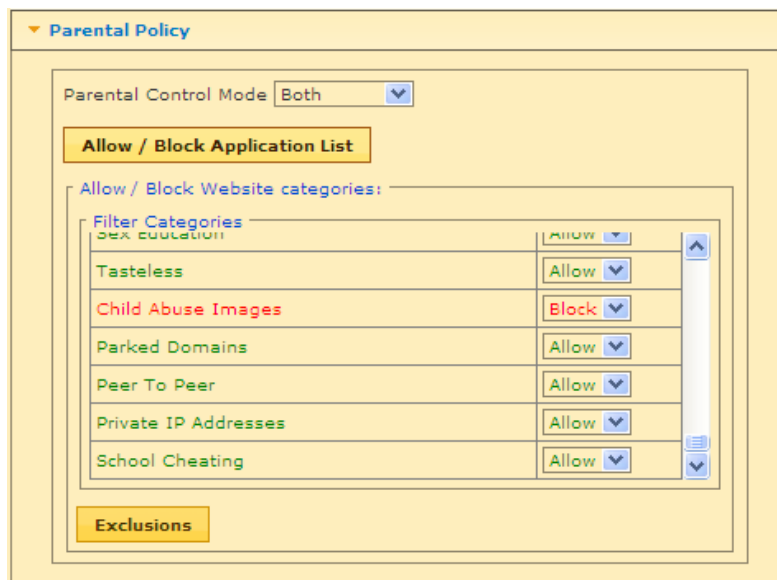


Figure 19.14

S.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	<ol style="list-style-type: none"> 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.	Exclusions	<p>You can allow user to view specified websites or web pages by adding them to exclusions.</p> <p>Web filtering allows user to view websites from the exclusion list regardless of the selected categories.</p>

 **Anti-Theft Policy**

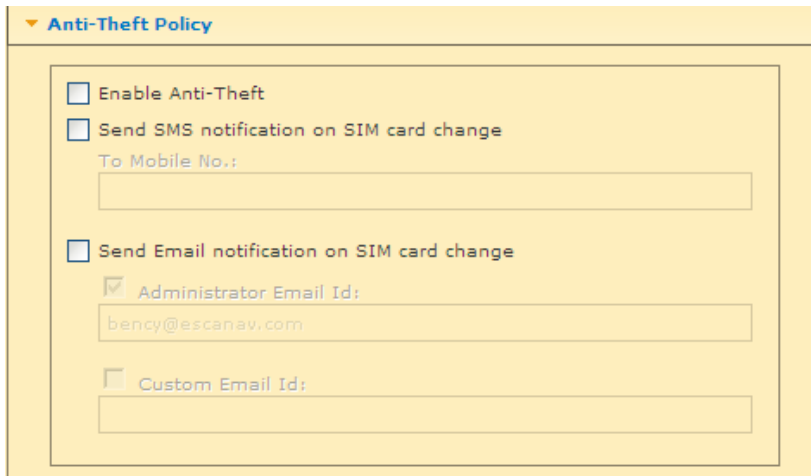


Figure 19.15

S.No.	Options	Description
1.	Enable Anti- theft	Tick this checkbox to Enable anti-theft under 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 devices is lost or stolen, even then it will receive Anti-theft messages, if connected to an internet.

 **Additional Settings**

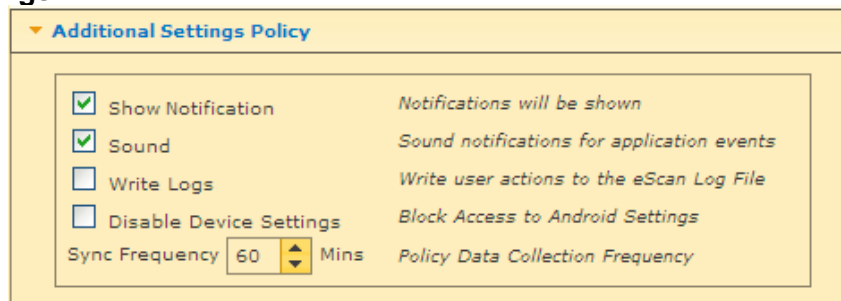


Figure 19.16

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

S.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.	Sync Frequency	Define time frequency for collecting Policy Data from devices. By default it is 60 minutes.

Password Policy

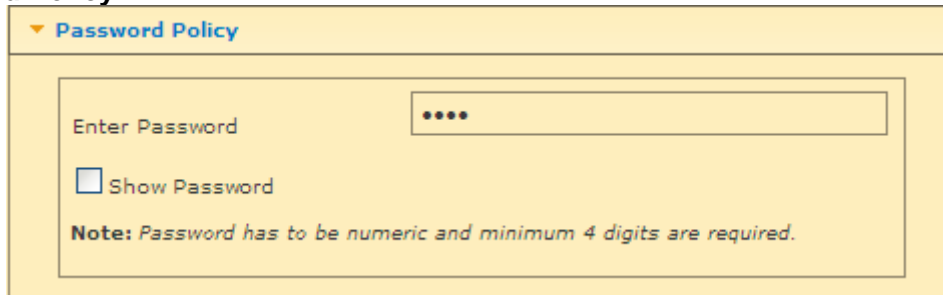


Figure 19.17

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

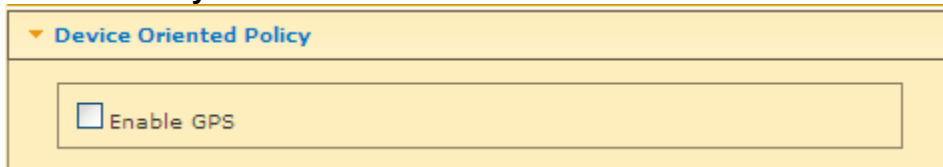


Figure 19.18

Use this option to enable/ disable 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**.

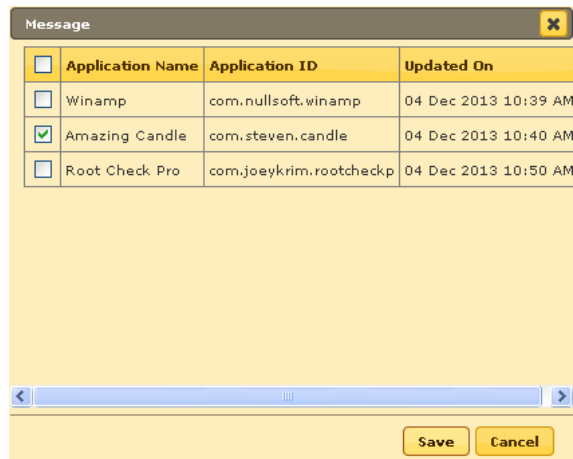


Figure 19.20

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.

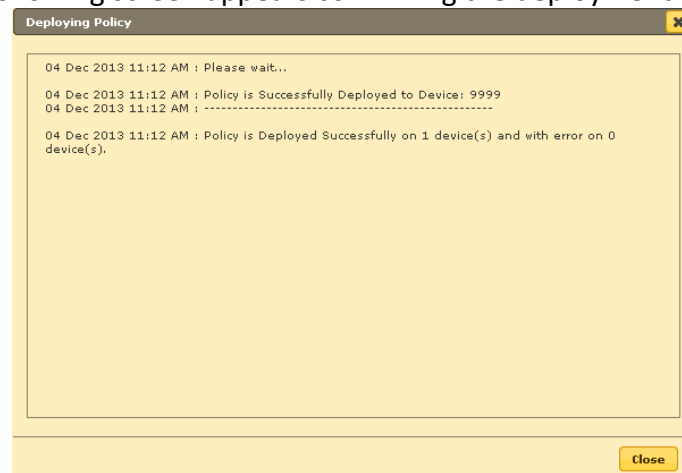


Figure 19.21

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.

Viewing Managed Client Devices

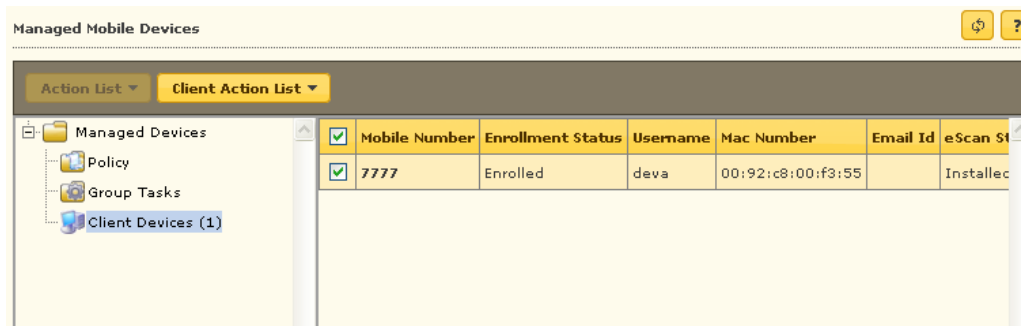


Figure 19.6

S.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 be changed 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
9.	Status for eScan modules	It displays the Enable/Disable status of eScan Modules – Web Control, Application Control, Call and SMS Filter on the device
10.	Last Connection	It displays the Last connection timing between MDM server and device
11.	Last Update	It displays the date and time when eScan was last updated on the device
12.	Last Scanned	It displays date and time of Last Scan on the device
13.	Update Server	It displays the Name / IP address of Update Server
14.	Client OS	It displays the OS Name and Version installed on the device
15.	Policy Applied Date	It displays the date and time on which the Policy is applied on the device

20. Backup Management

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.

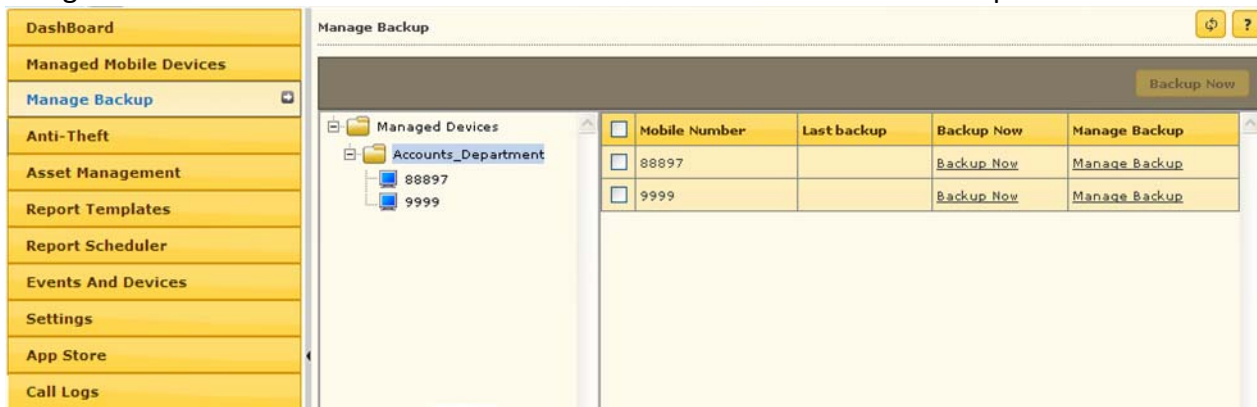


Figure 20.1

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.

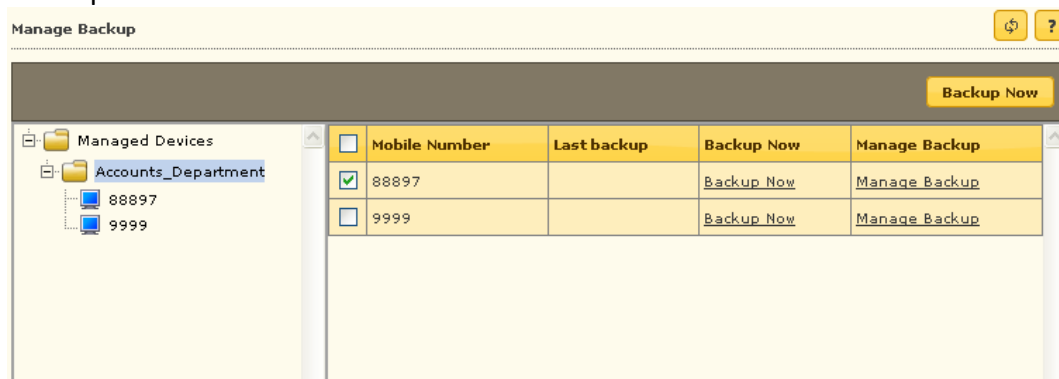


Figure 20.2

2. Now click **Backup Now** and select the desired option using respective check box to take backup.

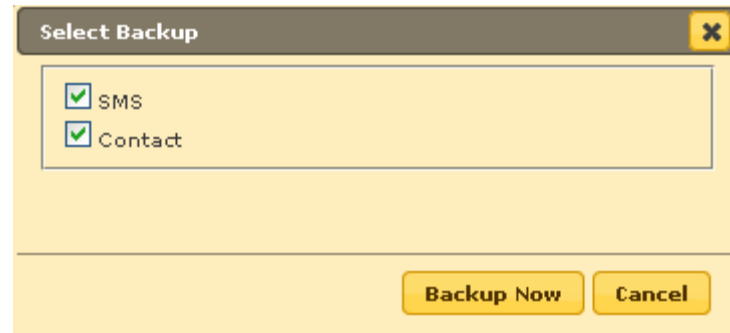


Figure 20.3

3. Click **Backup Now** option to take the Backup.

Note:

This feature will not work if there is no internet connection.

21. Lost Device Protection through Anti-Theft

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.

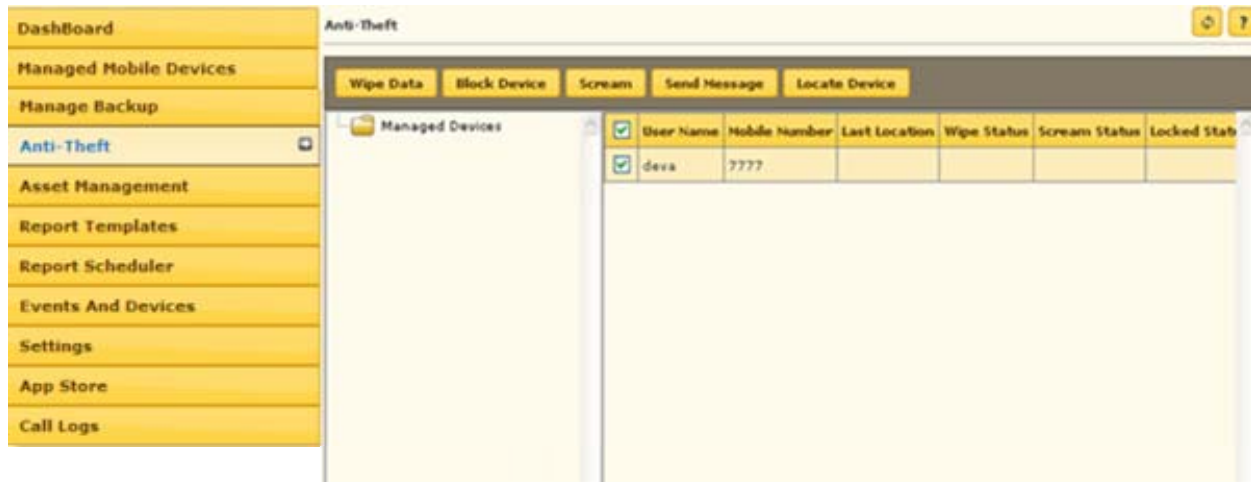


Figure 21.1

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.

Block 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.

Scream

Use Scream Option to raise an alarm on the device for easily locating the device.

Send Message

Use this option to send Message to desired Managed Devices.

Locate 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:

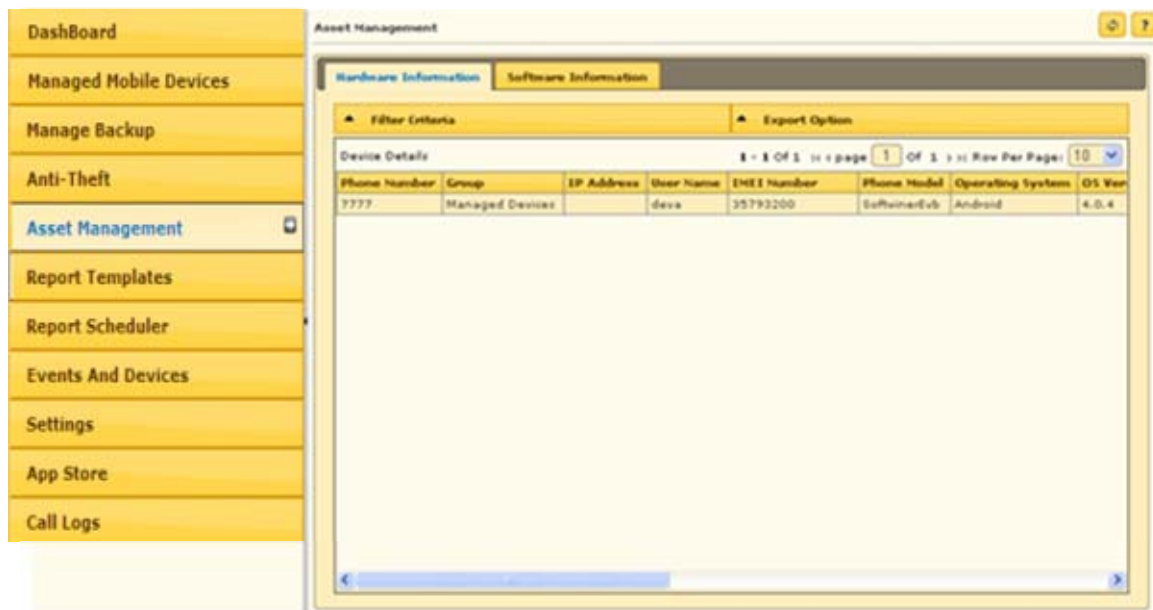
An active internet connection is required to use this feature.
--

22. Mobile Endpoints- Asset Management

Asset Management – How it Works

This Module displays detailed description of the Hardware and Software installed on the Managed Devices.

Asset Management – Hardware Information



The screenshot shows the 'Asset Management' interface. On the left is a navigation panel with options: Dashboard, Managed Mobile Devices, Manage Backup, Anti-Theft, Asset Management (highlighted), Report Templates, Report Scheduler, Events And Devices, Settings, App Store, and Call Logs. The main area is titled 'Asset Management' and has two tabs: 'Hardware Information' (selected) and 'Software Information'. Below the tabs are 'Filter Criteria' and 'Export Option' sections. A table titled 'Device Details' shows one row of data. The table has columns: Phone Number, Group, IP Address, User Name, ENEI Number, Phone Model, Operating System, and OS Ver.

Phone Number	Group	IP Address	User Name	ENEI Number	Phone Model	Operating System	OS Ver
7777	Managed Devices		deva	35793200	SoftwareEvb	Android	4.0.4

Figure 22.1

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 --

S.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(MB)	Displays the size of Phone memory of the device in MB
11.	External SD Card(MB)	Displays the size of SD Card of the device in MB
12.	Internal SD (MB)	Displays the size of Internal memory in MB
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.	WI-FI	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 22.2

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.

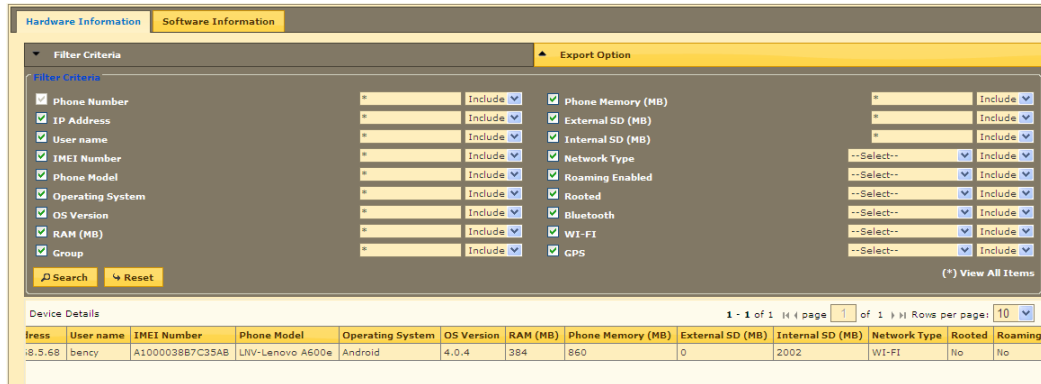


Figure 22.3

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**

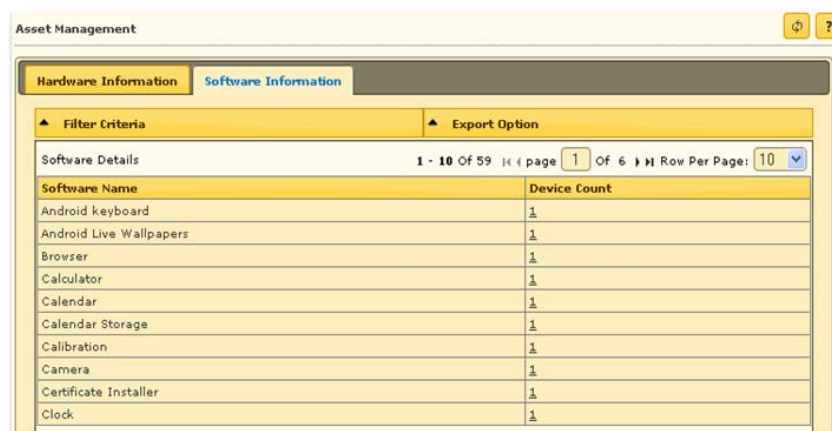


Figure 22.4

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**

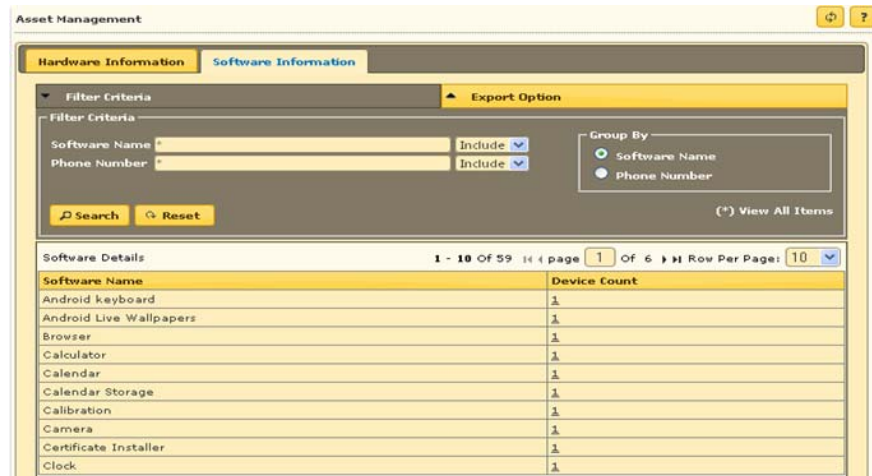


Figure 22.5

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 22.6

eScan’s MDM supports export 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 –

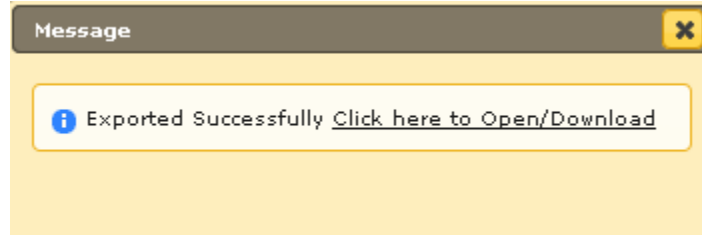


Figure 22.7

4. Click on the link to open/download the report in selected format.

23. Customizing and Scheduling Reports

Report Templates



<input type="checkbox"/>	Template Name	Report Type	Date Filter	Sort By	Created On	Modified On
<input type="checkbox"/>	Application Control Report	Application Control Report	This Week	Date	17 Jun 2014	17 Jun 2014
<input type="checkbox"/>	Inventory Report	Inventory Report	This Week	Devices	17 Jun 2014	17 Jun 2014
<input type="checkbox"/>	Web Control Report	Web Control Report	This Week	Date	17 Jun 2014	17 Jun 2014

Figure 23.1

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 --

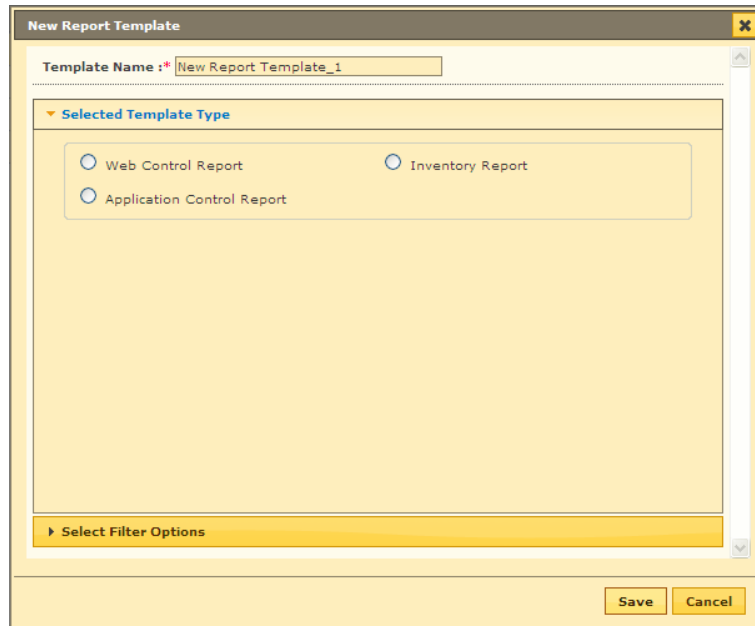


Figure 23.2

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**.

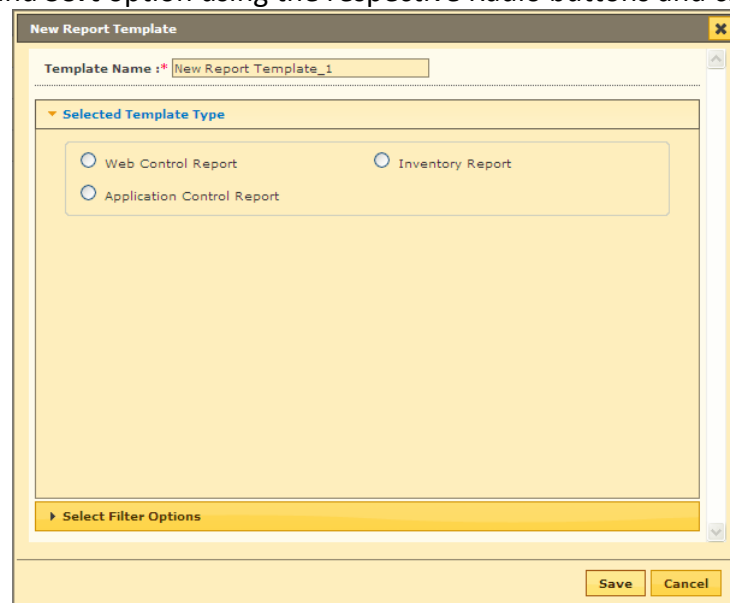


Figure 23.3

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 –



<input type="checkbox"/>	Template Name	Report Type	Date Filter	Sort By	Created On	Modified On
<input checked="" type="checkbox"/>	Application Control Report	Application Control Report	This Week	Date	17 Jun 2014	17 Jun 2014
<input type="checkbox"/>	Inventory Report	Inventory Report	This Week	Devices	17 Jun 2014	17 Jun 2014
<input type="checkbox"/>	Web Control Report	Web Control Report	This Week	Date	17 Jun 2014	17 Jun 2014

Figure 23.4

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 –

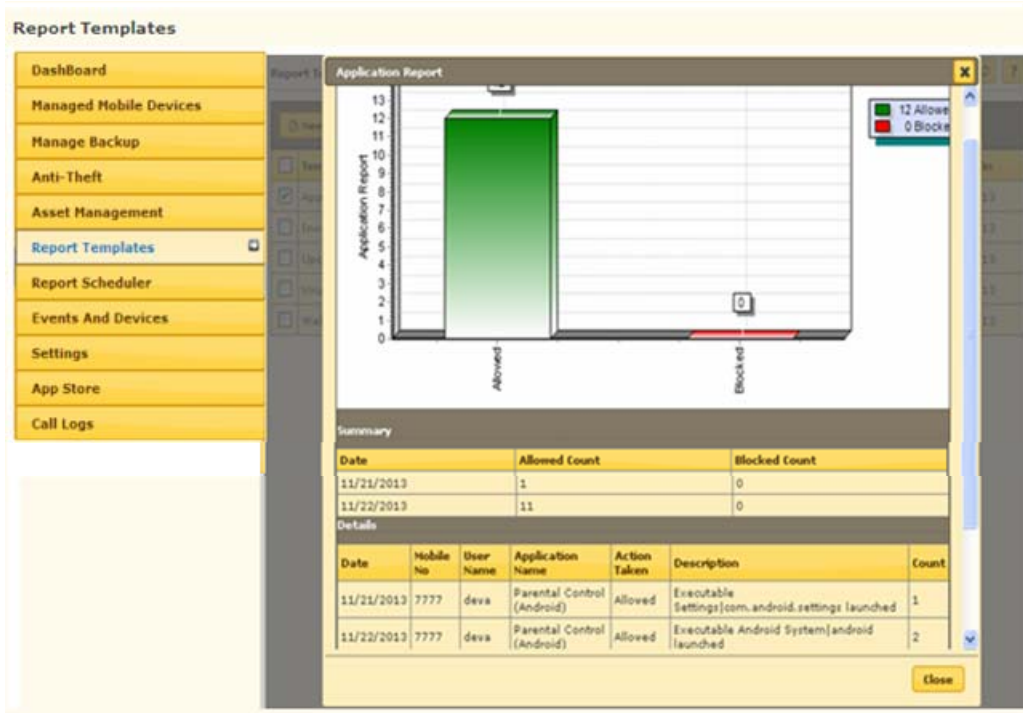


Figure 23.5

Deleting a Report Template

Select the Report Template that you wish to delete using the respective checkbox and click **Delete**.

24. Report Scheduler

Creating a Report Schedule



Figure 24.1

Following options will be displayed

S.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 --

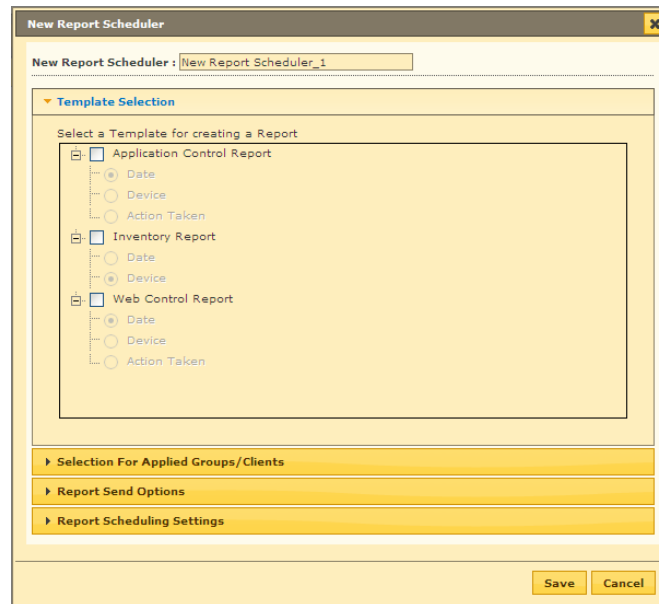


Figure 24.2

3. Select the **Groups or Devices** for which you wish to Schedule the Report.

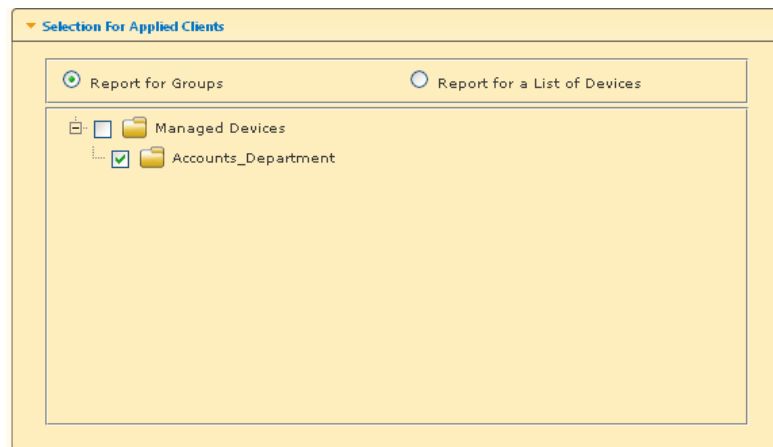


Figure 24.3

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.

New Report Scheduler

New Report Scheduler:

▶ **Template Selection**

▶ **Selection For Applied Groups/Clients**

▼ **Report Send Options**

Send Report by Email

Report Sender*:

Report Recipient*:

Mail Server IP Address: 192.168.0.1
Mail Server Port: 25

Select the Report Format

HTML page

▶ **Report Scheduling Settings**

Figure 24.4

6. Schedule the report as per your requirement and click **Save**.

New Report Scheduler

New Report Scheduler:

▶ **Template Selection**

▶ **Selection For Applied Clients**

▶ **Report Send Options**

▼ **Report Scheduling Settings**

Scheduled Manual

Daily Weekly Monthly At

Mon Tue Wed Thu Fri Sat Sun

1 Day

8 30 PM

Figure 24.5

7. Report Schedule will be created instantly.
8. Select the Report Schedule and click **Run** to manually run the Created Report Schedule.



Figure 24.6

9. You can View the Data of the Report by clicking **View** button present on the interface.

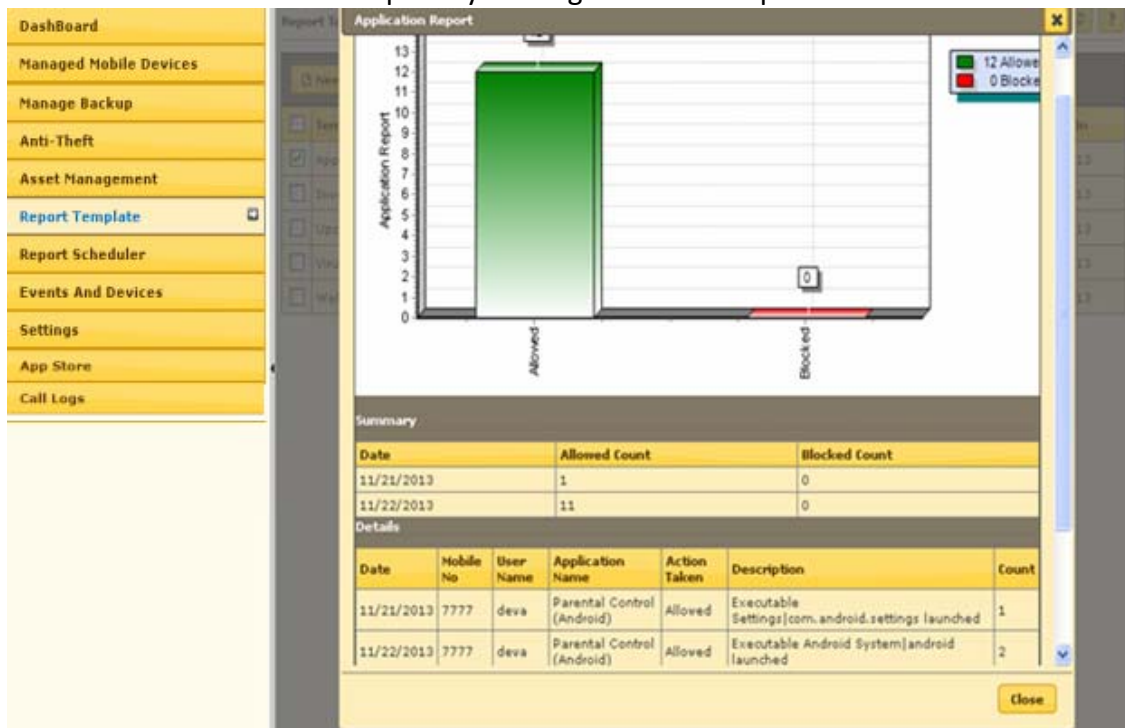


Figure 24.7

10. To View the Status of Scheduled Report click **Result**.

The screenshot shows the 'New Report Scheduler_1 - Report Result' window with the following table:

Start	Finished	Run Type	Status
	12/2/2013 2:53:27 PM	Scheduled	Error - Report mail not send!

Figure 24.8

25.Events and Devices

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.

Date	Phone Number	Username	Event Id	Module Name
26 Feb 2014 04:00 PM	9999	abhi	7034	Config (Android)
26 Feb 2014 03:59 PM	9999	abhi	7033	Config (Android)
26 Feb 2014 11:29 AM	9999	abhi	7034	Config (Android)
26 Feb 2014 11:29 AM	9999	abhi	6102	Parental Control (Android)
26 Feb 2014 11:28 AM	9999	abhi	6101	Parental Control (Android)
26 Feb 2014 11:28 AM	9999	abhi	6101	Parental Control (Android)
26 Feb 2014 11:28 AM	9999	abhi	7033	Config (Android)
26 Feb 2014 10:25 AM	9999	abhi	6102	Parental Control (Android)
26 Feb 2014 10:22 AM	9999	abhi	6802	Config (Android)
26 Feb 2014 10:22 AM	9999	abhi	6802	Config (Android)

Figure 25.1

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 such as web control status, application status etc.
- **Critical:** It displays all critical events occurred on managed devices such as anti-theft disabled etc.
- **Information:** It displays all informative type of events such as anti-theft status, manual sync status etc.

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”
- Not connected 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.

- 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.

26. Settings

Using this module, you can Save Server details for sending Email notifications to the Device user email addresses.



The screenshot displays the 'Settings' module in the eScan application. On the left is a vertical navigation menu with the following items: Dashboard, Managed Mobile Devices, Manage Backup, Anti-Theft, Asset Management, Report Template, Report Scheduler, Events And Devices, Settings (highlighted), App Store, and Call Logs. The main content area is titled 'Settings' and contains a section for 'Email Notification Settings'. This section includes five input fields for the following fields: From, SMTP Server, Server Port, Login Name, and Login Password. Below the input fields are two buttons: 'Save' (with a checkmark icon) and 'Cancel' (with an 'X' icon).

Figure 26.1

27. 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.

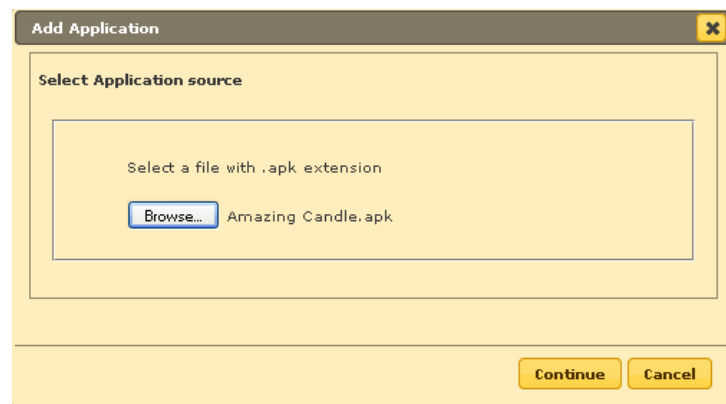


Figure 27.1

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**.

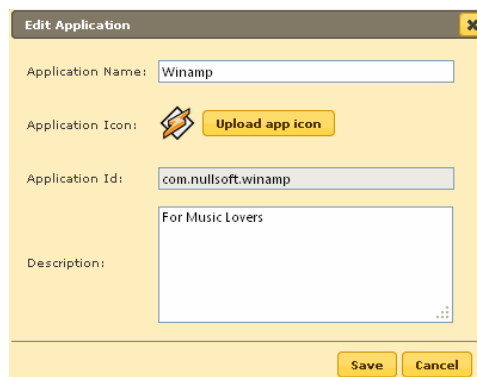


Figure 27.2

4. The App will be added in the store instantly.

App Store ⊕ ?

Applications listed below can be imported through "Policy >> Required Application Policy", for deployment to devices.

+ Add ✎ Edit ✖ Delete



<input type="checkbox"/>	Application Name	Version	Size	Installed	Updated On
<input type="checkbox"/>	 Winamp	1.2.12	4805 Kb	<u>2</u>	04 Dec 2013 11:21 AM
<input checked="" type="checkbox"/>	 Root Check Pro	1.2.0	259 kb	<u>2</u>	04 Dec 2013 07:01 PM

Figure 27.3

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.

28. Getting started with eScan Mobile Security

Introduction

eScan Mobile Security is specifically designed for Android devices. It helps you secure enterprise data accessed from smart phones and tablet connected to your network. 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 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.

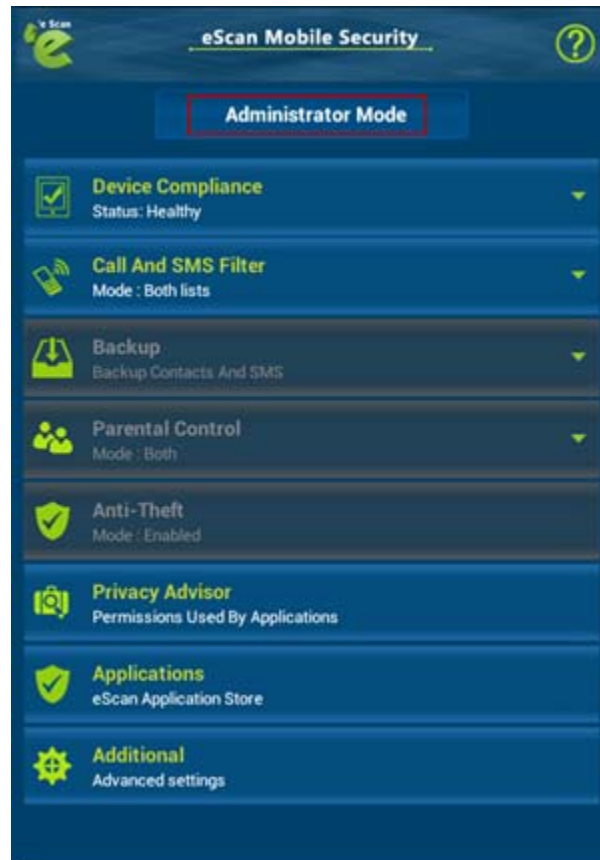


Figure 28.1

- **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 28.2

- **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.

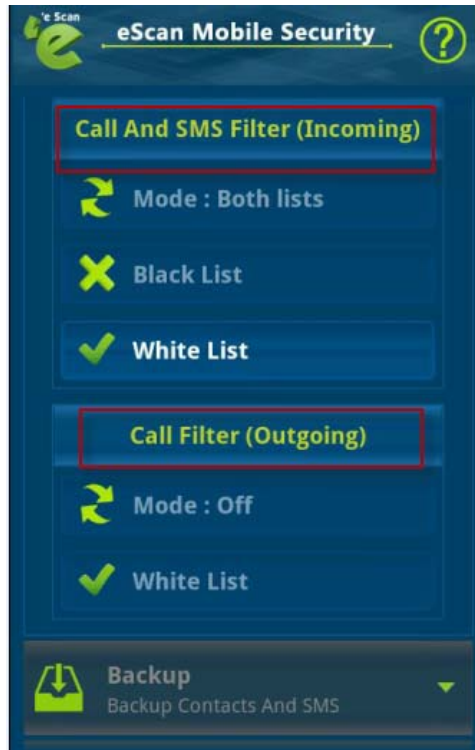


Figure 28.3

- **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.

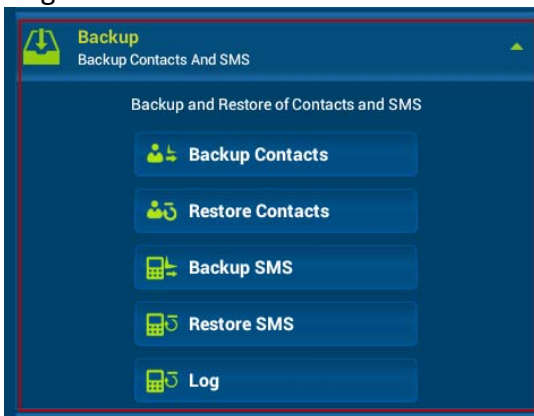


Figure 28.4

- **Parental Control:** Allowing and blocking specific websites and applications.

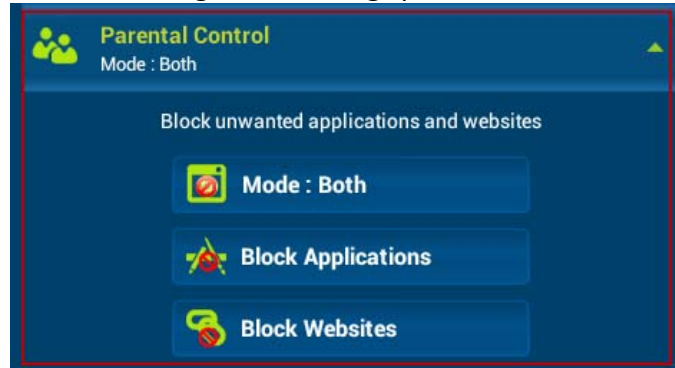


Figure 28.5

- **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.

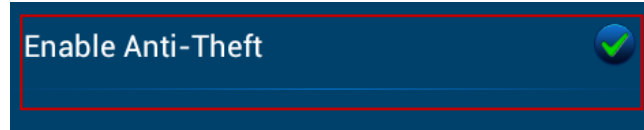


Figure 28.6

- **Privacy Advisor:** This section displays the list of applications installed on the Tablet along with the permissions used by them.

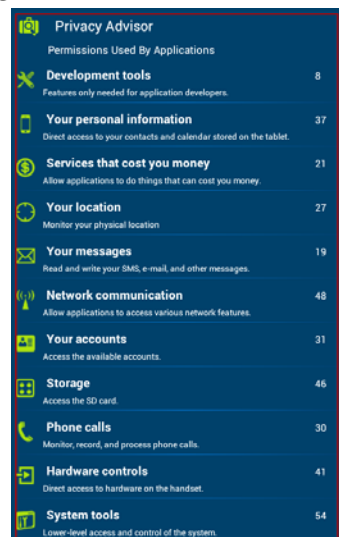


Figure 28.7

- **Applications:** You can download new apps from the app store and also portrays the list of downloaded apps.

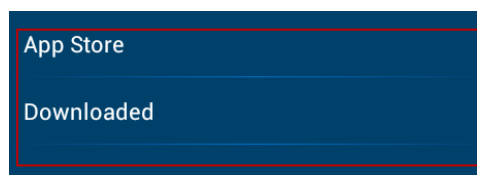


Figure 28.8

- **Additional:** Configuring additional advanced settings.

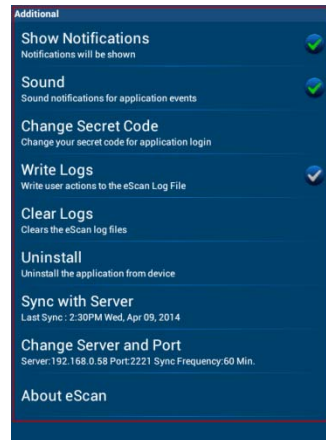


Figure 28.9

29. 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.

30. Registered Offices

<p>Asia Pacific MicroWorld Software Services Pvt. Ltd. CIN No.: U72200MH2000PTC127055 Plot No 80, Road 15, MIDC, Marol, Andheri (E), Mumbai, India Tel : (91) (22) 2826-5701 Fax: (91) (22) 2830-4750 E-mail : sales@escanav.com Web site: http://www.escanav.com</p>
<p>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</p>
<p>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</p>
<p>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</p>
<p>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</p>