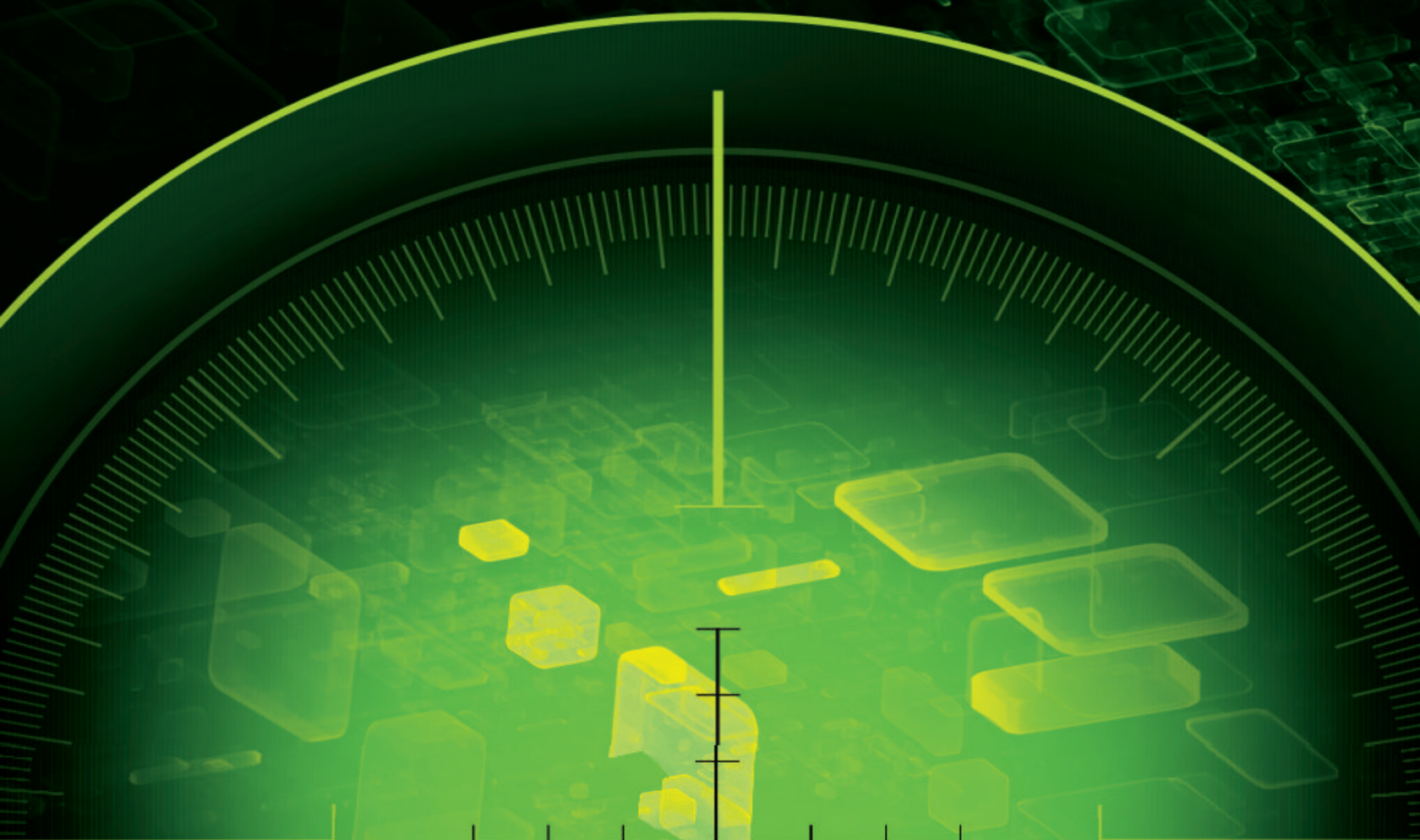
eScan™

Anti-Virus & Content Security

Internet Security Suite

with Cloud Security for SMB

User Guide



www.escanav.com

sales@escanav.com

Document Number: 5BUG/2013/14.1

Current Software Version: 14.1

Technical Support:	support@escanav.com
Sales:	sales@escanav.com
Forums:	http://forums.escanav.com
eScan Wiki:	http://www.escanav.com/wiki
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld
Date:	October, 2013

Contents

A Note to the Reader

Dear Reader,

The eScan family of products has been classified to cater to the requirements of user segments, such as home users, business users, and enterprise users. This document deals with the eScan Web Console, which is included in the eScan ISS for SMB Edition for Windows®. It is for your convenience, eScan ISS for SMB Edition is referred as eScan throughout this document. The names of other eScan products are spelled out, wherever they appear in this document to avoid ambiguity.

The eScan Team

Preface

In the past few years, there has been a sudden increase in the number of IT related crimes. Almost every other day, one gets to hear reports of hackers stealing trade secrets or viruses bringing down entire networks. Because of this, organizations are turning to Anti-Virus and content security solutions for keeping their data safe from security threats.

This guide provides you with an overview of eScan Web Console, which is a management tool in the eScan Corporate Edition that helps system administrators, manage the eScan client computers on their networks.

Contents

Who Should Read this Guide?

This guide has been designed for the use of System administrator, users, dealers, and support engineers.

Before You Read this Guide

Before reading this guide, you should familiarize yourself with eScan Web Console's user interface.

How this Guide Is Organized?

This guide is organized into several sections for your convenience and ease of access.

Chapter 1: Introduction to eScan Web Console

This chapter provides you with an introduction to eScan Web Console, its availability, features, benefits, structure, hardware requirements, and software requirements.

Chapter 2: Deployment Schemes

This chapter lists the different deployment schemes and the considerations for choosing deployment schemes.

Chapter 3: eScan Web Console's GUI

This chapter provides you detailed information about the GUI of the eScan Web Console.

Chapter 4: Managing Computers and Computer Groups

This chapter provides you with information on how to manage network computers and computer groups by using the eScan Web Console.

Chapter 5: Managing Tasks For Computers and Groups

This chapter provides you with information on how to schedule management tasks to run on computers and computer groups.

Chapter 6: Managing Policies

This chapter provides you with information on creating, modifying, and deploying policies to computers.

Chapter 7: Configuring Outbreak Notification Settings

This chapter provides you with information on how to configure Virus outbreak alert notifications.

Chapter 8: Managing Reports

This chapter provides you with information on how to manage reports.

Chapter 9: Scheduling Reports

This chapter provides you with information on how to schedule the creation of reports.

Chapter 10: Managing Events & Computers

This chapter provides you with information on how to monitor various activities performed on client's computer and enables you to save, edit settings, and view log of all events based on certain criteria's and settings defined

Chapter 11: Asset Management

This chapter gives you Information related to the Softwares and Hardware's installed on all the Managed Computers.

Chapter 12: Printing Activity

It gives you a brief on Monitoring Printing activity of all the Managed computers through any Printer connected to the network.

Chapter 13: Unmanaged Computers

This chapter provides you with information on how to move computers from unmanaged computers to Managed Computers. How to search them through hostname and IP address? And many more.

Chapter 14: Configuring the Settings

This chapter provides you with information on how to configure the settings for EMC, the eScan Web Console, and Updater.

Chapter 15: Managing User Accounts

This chapter provides you with information on how to manage local and active directory user accounts.

Chapter 16: Export and Import Settings

This chapter provides you with information on how to import and export the settings and policies of WMC and database.

Chapter 17: License

This chapter provides you with information on how to add, activate, and manage license of users.

Accessing Online Documentation

MicroWorld provides you with several resources to assist you in installing, buying, activating, or using eScan. Depending on your requirements, you can obtain information about eScan Web Console from any of the following sources.

- Online documentation and knowledgebase

To access eScan's online documentation and knowledgebase, visit the following Web site.

http://www.escanav.com/wiki/

- Other documentation

The eScan Product Installation CD with bootable Rescue Disk comes with documentation about eScan products. These documents are in the PDF format.

- eScan 14 User Guide describes the basic concepts and features of the eScan Web Console and the steps for installing on local computers and remote computers. In addition, it describes the use of the components of console's user interface, and provides detailed steps on performing management tasks.
- eScan 14 Quick Reference Guide provides an overview of eScan features and includes detailed instructions and steps for installing it.

 You can also obtain these documents from eScan's Knowledgebase by visiting the following link.

http://download1.mwti.net/wiki/index.php/User_Guides

Technical Assistance

MicroWorld is committed to provide a safe and secure computing environment for all eScan users. It offers 24x7 FREE Online Technical Support to all its customers via e-mail and Live Chat. In addition, it provides FREE Telephonic Support to its customers during business hours.

If you have any queries regarding any eScan product, you can contact the eScan Technical Support team via any of the following ways.

- Telephone

The eScan Technical Support team provides FREE Telephonic Support to its customers during business hours.

- Chat

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

- E-mail

If you have any queries, suggestions, and comments about eScan products, you can write to support@escanav.com.

- Forums

You can join the MicroWorld Forum to discuss all your eScan related problems with eScan experts. In addition, you can view threads, create new posts, and participate in online discussions regarding eScan products.

To check the online forum, visit the following link.

http://forums.escanav.com

- Support Request Form on the eScan Web site

If for some reason you are unable to contact the eScan Technical Support team, you can send a Technical Support Request by visiting the following link and filling out a form.

http://www.escanav.com/english/content/support_training/support/escan_tech_support.asp

The form contains three mandatory fields: name, e-mail address, and the description of the problem. When you submit a request, a ticket number is automatically generated and sent to your e-mail address. The eScan Support personnel will then get in touch with you and provide you with assistance.

 In case you are a registered user, you need to provide your license key to receive technical assistance via telephone or Live Chat.

If you have not yet registered your product, you can do so by visiting the following link.

http://www.escanav.com/mwscnew/getactivationcode.asp

Thank you for choosing eScan.

The eScan Team

Chapter 1: Introduction to eScan Web Console

The eScan Web Console is a centralized server management console that is available only when you install eScan as a server. This console functions as a control panel that helps system administrators remotely manage all the eScan client computers in a network.

Availability of the Application

eScan Web Console is available in the small and medium business (SMB) editions and the corporate/enterprise editions of eScan.

The enterprise edition comes bundled with eScan Edition and MailScan.

Benefits for Registered Users

MicroWorld provides registered users of eScan with several benefits during the license period. These benefits include:

- Automatic download of virus updates
- Free download of hotfixes
- Free product upgrades during the registration period
- Free telephone, e-mail, and Live Chat support
- Notifications about new viruses (Requires an eScan Alerts Subscription.)
- Notifications about eScan products (Requires an eScan Alerts Subscription.)

To subscribe to eScan Alerts, visit the following link.

http://www.escanav.com/english/content/company/news/escan_subscription.asp

Features of the Application

The new eScan Web Console provides administrators with a convenient mechanism of managing the eScan server and eScan client computers in a network. Some of its salient features are as follows:

- Web-based User Interface

The new eScan Web Console is a Web-based application that can be accessed via a Web browser from any computer in a network. It has a pleasing user interface and is extremely easy to use. In addition, it provides clear instructions for performing configuration and management tasks.

- Remote Management of Computers

The eScan Web Console is a Web-based application that is hosted on the server and can be accessed via a Web browser from any computer in the network. This feature is especially beneficial to administrators of large networks as they can centrally access the console and perform the management tasks remotely from anywhere in the network.

- Remote Installation and Uninstallation of eScan

With the help of the new eScan Web Console, administrators can install or uninstall eScan remotely on any computer in the network.

- Management of Computer Groups

Administrators often have to configure the same settings on multiple computers. Performing these tasks manually is often time-consuming and laborious. eScan eliminates the need for configuring computers individually by allowing the creation of computer groups. Administrators can create groups and add computers to those groups, delete groups, and view the properties of groups.

- Administrative Management

The eScan Web Console helps administrators centrally manage user accounts of local and active directory users, user roles with permissions to access the menus, and export and import the settings and policies of WMC and database.

- Management of User Accounts

The eScan Web Console helps administrators centrally manage user accounts of local and active directory users. It allows the addition, creation, and deletion of such accounts. In addition, it also allows administrators to enable or disable accounts based on the requirements.

- Report Generation and Scheduling

The eScan Web Console also allows administrators to create and view reports that are based on a given module. Administrators can either create reports based on predefined templates or customize them based on their requirements. Administrators can also specify whether they want eScan to create and send reports to specific recipients on specific days at a given time.

- Schedule Tasks on Computers or Groups

With the help of the eScan Web Console, administrators can create tasks and schedule them to run on specific computers or computer groups on specific days at a given time. These may involve the enabling or disabling of specific eScan modules, starting or stopping a server, setting up an update server; performing scans on the memory, system drive, and local drives; and forcing clients to download updates based on the settings defined in the tasks.

- Send Virus Outbreak Alerts and Notifications Regarding Security Violations

Administrators can configure the eScan Web Console to send notifications to specific recipients from specified senders when the number of viruses detected by eScan crosses a defined threshold.

- Events & Computers

This feature enables you to monitor various activities performed on client's computer and allows you to view log of all events.

- Policies for Specific Computers

This feature enables you to create and deploy policy on specific client computers without violating group policy, based on certain settings. There is also an option to delete policy and view properties of policy whenever required and you can add other computers if required.

Thus, eScan Web Console simplifies the task of managing the eScan client computers in a network.

- 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 you requirement. It also allows you to Export the entire system information available through this module in PDF, Excel or HTML formats.

- Print Activity

It monitors and Logs printing tasks done by all the Managed computers, it gives you a report of all Printing Jobs done by Managed computers through any Printer connected to the network. It also gives you a report of all PDF conversions done on individual Machine connected to the network.

Structure of the Application

The eScan Web Console comprises the following components.

- eScan Server allows you to manage and configure the eScan client computers. It stores the configuration information and log files about the client computers which are present in the network.
- MWAgent manages the connection between the eScan server and a client computer.
- eScan Web Console is a Web-based application hosted on the eScan Server. It allows administrators to manage the eScan servers and eScan client computers in the network.
- Microsoft SQL Express 2005/2008 for storing events and logs, Already included in the eScan Setup file
- Apache for running eScan Web Console. Already included in the eScan Setup file

All these components are installed when you install a version of eScan 14 that contains the eScan Web Console. eScan Web Console runs on Apache Server.

Minimum Requirements

Before installing, please make sure that your system meets the following requirements:

CPU:

- Windows Server 2012 - 1.4GHz (recommended 3.1GHz)
- Windows Server 2008 (32 bit)/Windows Server 2008 (64 bit) - 1.4 GHz (recommended 2GHz)
- Windows Server 2008 R2 - 1.4 GHz (64 bit) (recommended 3.1GHz)
- Windows Server 2003 (32 bit) - 550 MHz (recommended 1GHz) Windows Server 2003 (64 bit) - 1.4 GHz (recommended 2.1GHz)
- Windows 8, Windows 7, Windows Vista - 1 Ghz (recommended 2.1GHz)
- Windows XP/Windows 2000 - 450 MHZ (recommended 1GHz)

Memory:

- Windows Server 2012 – 4 GB
- Windows Server 2008 (32 bit)/Windows Server 2008 (64 bit) – 4 GB
- Windows Server 2008 R2 – 4 GB
- Windows Server 2003 (32 bit/64 bit) – 4 GB
- Windows 8, Windows 7, Windows Vista – 4 GB
- Windows XP/Windows 2000 - 512MB (recommended 2GB)

Disk Space:

- 8 GB (recommended more than 8 GB) for all Operating systems

Minimum Software Requirements for Server

Before you begin **with the installation, ensure you meet the following requirements:**

Operating Systems:

- Windows Server 2012, Windows Server 2008, Windows Server 2008 R2, Windows Server 2003
- Windows 8 (32 bit/64 bit), Windows 7 Enterprise/Professional/Ultimate (32 bit/64 bit)
- Windows Vista Business/Enterprise/Professional (32 bit/64 bit)
- Windows XP Professional Service Pack 2 or higher
- Windows 2000 with Service pack 4 with Rollup patch 1

Other Requirements:

- Web Browser: Microsoft Internet Explorer 7.0 & 8.0
- Display: High-colour display with a resolution of 640x480 pixels or higher recommended

Chapter 2: Deployment Schemes

Before you can deploy eScan on the computers in your network, you need to evaluate the deployment schemes and consider the factors for selecting a deployment scheme. This section discusses the deployment schemes available in eScan.

> Although, eScan uninstalls the other anti-virus software with few of its versions, it does not warranty its complete un-installation from your computer.
>
> In case, if eScan does not uninstall the other anti-virus software, please write to us at support@escanav.com along with name and version of the concerned software. eScan will definitely try its best to provide a solution at the earliest.

- **Schemes for Deploying eScan**
- **Considerations for Selecting a Deployment Scheme**

Schemes for Deploying eScan

You can deploy eScan on your network using any one of the following deployment schemes.

- **Installing eScan Manually**
- **Pre-requisites for Installing eScan Remotely on Client Computers**
- **Installing eScan Remotely on Client Computers**
- **Installing eScan using MWAgent**

Installing eScan Manually

You can install eScan on the local computer manually. This type of installation is done when it is not possible to deploy eScan remotely. This can be achieved using web link provided by eScan Web Console.

Pre-requisites for Installing eScan Remotely on Client Computers

There are settings that are required to be configured on the client system before deploying eScan remotely. You have to ensure that the following pre-requisites are met:

> If you have the domain environment or active directory login available, then you do not need to change the following settings, instead you can provide the administrator username and password for active directory or domain.

- For Windows 2000/2003 Operating system:

You have to provide administrator username and password in Set Host Configuration. For more information on how to add the login information, refer Setting the Host Configuration section.

- For Windows XP Professional systems:

1. Click **Start**, and then click **Control Panel**.
   The **Control Panel** window appears.
2. Double-click the **Administrative Tools** icon.
   The **Administrative Tools** window appears.
3. Double-click the **Local Security Policy** icon.
   The **Local Security Settings** window appears.
4. On the navigation pane, click **Local Policies** folder, and then click **Security Options** folder.
   The **security policy** appears.
5. Double-click the Network Access: Sharing and Security Model for Local accounts policy.
   The Network Access: Sharing and Security Model for Local accounts… dialog box appears.
6. Select Classic - Local user authenticate as themselves option from the drop-down list.
7. Click **Apply**, and then click the **OK** button.
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 the **Disabled** option.
10. Click **Apply**, and then click the **OK** button.
    If the firewall is enabled, you have to select the **File and Printer Sharing** check box, under **Exceptions** tab.

- For Windows XP Home:

Since, Mwagent is not a network operating system; it should be installed on your personal computer. You can download MWAGENT from eScan Web Console.

11. Turn off the firewall
12. Turn off the UAC
13. Enable Administrator account and set password for the same

Installing eScan Remotely on Client Computers

You can also install eScan remotely on a computer or a group by using the eScan Web Console. This uses Windows RPC technology, before pushing remote installation you need to go through below link

http://wiki.escanav.com/wiki/index.php/Escan/english/eScan-FAQ/Configuration#anchor10

Installing eScan using MWAgent

In large corporate environments, you can achieve 88% of remote deployment through eScan Web Console, rest of the system are either located over the WAN or some of the systems are not in the network when the actual

deployment take place. For this kind of scenarios Administrator's can either install MWAgent on those systems or manually install the eScan client setup. To access the MWAgent setup file follow the below steps:

Access MWAgent setup file and install eScan client

- Access eScan Management Console and login with username and password.
- Then click on Settings > Web Console Settings
- Under Login Page settings enable tick mark for "Show Agent setup link"
- Save the settings
- Logoff from the console and on the login page see if you can see the agent link..
- Click the http://<IP/hostnameofserver>:10443/Agent_Setup.exe link.
  A **File Download** window appears.
- Click the **Save** button, to save or click **Run** to run and install the file.

To test MWAgent you can run following command

telnet <ipaddress> 2222

MWAgent listen on port 2222, all the data transfers from the agent to server is encrypted. If you still not get access to the system on which you have installed MWAgent, please make sure your firewall is turned off or you allow MWAgent port in your firewall. On windows Firewall, MWAgent puts itself in the Exception list when it gets installed.

Considerations for Selecting a Deployment Scheme

Before you can select a scheme for deploying eScan, you need to consider the following factors.

- Number of domains in the organization's network.
- Number of server computers required for managing the computers.
- Number of client computers on which eScan needs to be deployed.
- Hardware resources that need to be allocated to computers for installing eScan.
- Network bandwidth and the number of client computers in each domain.
- Number of technicians involved in the maintenance and administration of the client computers, such as updating operating system components, tuning of databases, and deploying policies.
- Time required for implementing the policies and updating the eScan client computers.

Chapter 3: eScan Web Console's GUI

The eScan Web Console has a simple and easy-to-use user interface. It allows for easy navigation and simplifies the task of managing the eScan client computers in the network.

Accessing the eScan Web Console

You can access the eScan Web Console via a Web browser from any computer in the network.

The steps to open the eScan Web Console are as follows:

Method 1:

On the desktop, on the taskbar, in the notification area, Single-click  .

Method 2:

14. Open a browser window and in the Address bar, type the following URL:
    http://<IP address>**:10443**
    Here,
    <IP address> is the IP address of the eScan server.
    10443 is the default port number on which the eScan Web Console is running.
15. In the **eScan Management Console** page, under **WEB CONSOLE LOGON**, in the **User name** box, type the user name, in the **Password** box, type the password, and then click **Login**.

Overview of the User Interface

The eScan Web Console page is divided into two panes: the left pane, which contains a navigation bar called the **Dashboard** and the right pane (also called task pane), which displays the page corresponding to the link selected on the navigation bar.

In addition, a **Help** link is displayed at the top right corner of the eScan Web Console. To log off from the console, one needs to click the **Log Off** link.

Navigation Bar

The navigation bar is the mechanism that links all the pages together. It contains the following links:

- Dashboard
- Setup Wizard
- Managed Computers
- Unmanaged Computers
- Report Templates
- Report Scheduler
- Events & Computers
- Tasks for Specific Computers
- Policies for Specific Computers
- Asset Management
- Print Activity
- Outbreak Notification
- Settings
- Administration
- License

Dashboard

Dashboard is a special page that contains tabs, which display the eScan **Deployment Status**, **Protection Status**, and **Protection Statistics** and **Summary Top 10** graphically in the form of pie charts.

You have an option to decide, which charts you want to view on the dashboard through **Configure Dashboard Display** window. For more information, refer Configuring Dashboard section.

Setup Wizard

The **Setup wizard** page enables you to create groups, assign computers, and install eScan on respective computers. You also have an option to add new computers and unassigned computers to groups.

Managed Computers

The **Managed Computers** page contains a file explorer-like interface. The page is divided into two panes. The left pane contains a console tree while the right pane is the task pane, which displays information about the node selected in the console tree. This page allows you to create groups, add and remove computers from groups, create tasks, install and uninstall eScan application, install other applications, and view properties of policy and configure the policy details of client computers.

Unmanaged Computers

The **Unmanaged Computers** menu item has four sub-items: **Network Computers**, **IP range**, **Active Directory**, and **New Computers Found** each of which is linked to a corresponding page. Each of these pages has a file explorer-like interface. Each page is divided into two panes. The left pane contains a console tree and the right pane is the task pane, which displays more information about the selected node in the console tree.

- The Network Computers page displays the computers in the network.
- The IP range page displays the list of IP range in the network.
- The Active Directory page displays the computers in the active directory if configured.
- The New Computers Found page displays the computers which do not have eScan installed on them.

Reports Templates

The **Reports Template** page allows you to create and view customized reports based on a given template, for a given period; sorted by date, computer, or action taken; and for a selected condition or target group. It also contains options for configuring reports, viewing report properties, and refreshing or deleting existing reports.

Report Scheduler

The **Report Scheduler** page allows you to create a new scheduled task, run selected tasks, view the result of running a task, and view the properties of an existing task.

Events & Computers

The Events & Computers page enables you to monitor various activities performed on client's computer. You can view log of all events based on certain criteria's and settings defined in **Settings** button.

Tasks for Specific Computers

The Tasks for Specific Computers page helps you to create and run tasks on given computers, view the properties of selected tasks, view the results of running a task, and delete tasks.

Policies for Specific Computers

The **Policies for Specific Computers** page enables you to create and deploy policy on specific client computer same as for groups, based on certain settings. There is also an option to delete policy and view properties and add and remove additional systems whenever required.

Asset Management

Provides you an 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 you requirement. It also allows you to Export the entire system information available through this module in PDF, Ms Excel or HTML formats.

Print Activity

It monitors and Logs printing tasks done by all the Managed computers, it gives you a report of all Printing Jobs done by Managed computers through any Printer connected to the network. It also gives you a report of all PDF conversions done on individual Machine connected to the network.

Outbreak Notification

The **Outbreak Notification** page enables you to configure the eScan server to send virus outbreak notifications to administrator in an event of the number of viruses detected exceeds a user defined threshold.

Settings

The **Settings** menu contains the following sub-menus:

- The EMC settings page allows you to configure the FTP and LOG settings. The FTP settings section enables you to define the maximum number of FTP download sessions that has to be allowed by server for clients. The LOG settings section enables you to delete user settings and logs files after uninstallation of eScan client. In addition you can group the clients and configure client connection settings
- The Web Console Settings page allows you to configure the eScan Web Console Timeout Setting, Dashboard Setting, Login page Setting, SQL Server Connection Setting, and SQL Database Compression Settings.
- The Update Settings page allows you to configure the general, update notification, and update scheduling settings.

Administration

The **Administration** menu enables you to maintain the user account, and export and import the settings.

License

The **License** page enables you to add, activate, manage, and view the license record.

User Interface Links

The following sections describe UI of each of the links on the left navigation bar in detail.

Dashboard

Dashboard is a special page that contains tabs, which display the status of deployment, protection, licenses, and statistics for eScan modules in the form of pie charts. It is displayed when you click the Dashboard menu item in the navigation bar. This page contains the **Deployment Status**, **Protection Status**, **Protection Statistics** and **Summary Top 10 tabs**, apart from the **Configure Dashboard Display** link.

- **Deployment Status**
- **Protection Status**
- **Protection Statistics**
- **Summary Top 10**
- **Configuring Dashboard**

Deployment Status

This tab displays information regarding the status of eScan installation on client computers, the version of eScan installed, and the number of licenses available or deployed. This information is represented graphically in the form of pie charts. Each pie chart has a legend next to it. The legend displays the color associated with a data label and the value associated with the label. In case of the eScan Status and eScan Version, the values displayed in the legends are clickable. Refer

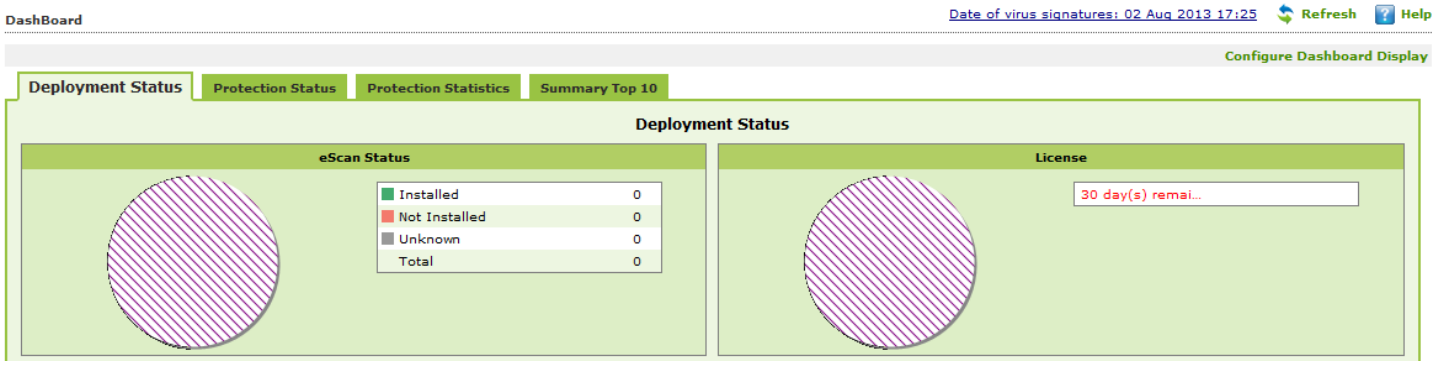


Figure 1.

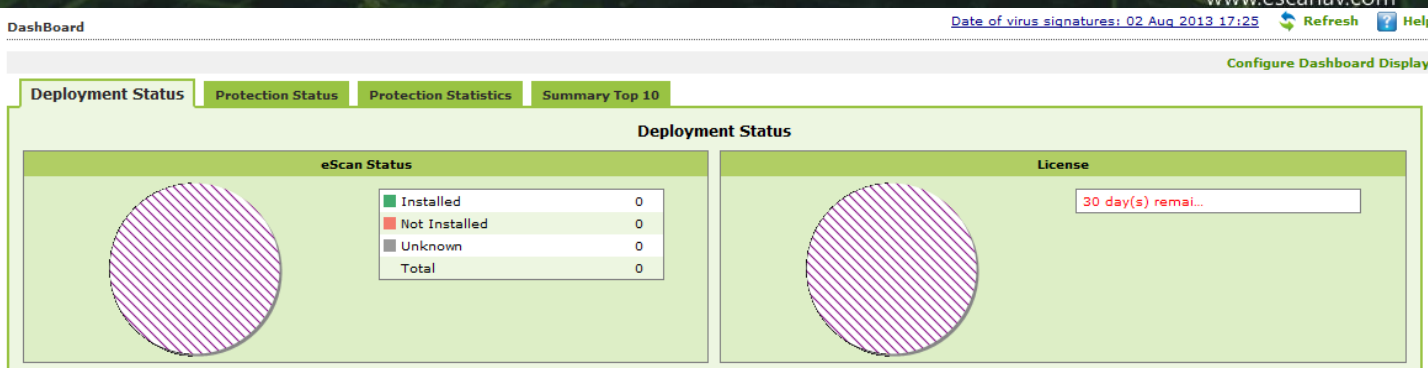


Figure 1

The following charts are displayed on this tab.

- The eScan Status pie chart displays the status of installation on eScan client computers. The status can be “Installed,” “Not Installed,” or “Unknown.” The legend displays the number of computers belonging to each category in the Value column. You can click a value to view the names of the computers and their status.
  - Unknown status indicates that the eScan client is either out of the network or not reachable to the eScan server.
- The License pie chart displays the rows depicting the total number of licenses available for deployment, the number of licenses deployed, and the number of licenses remaining and their corresponding values.

  Refer the Manage License section in order to manage licenses.

Protection Status

This tab shows pie charts that depict the protection status of eScan on the client computers in the network. This status can be “Started”, “Stopped”, or “Unknown”. Each pie chart is accompanied by a legend, which shows the color code for each status data label and its corresponding value. You can click the value to view the computer name, its status and group in a popup window. Refer

Figure 2.

Figure 2

- File Anti-Virus
- Proactive

- Mail Anti-Virus
- Anti-Spam
- Web Anti-Phishing
- Mail Anti-Phishing
- Web Protection
- Firewall
- End Point Security
- Privacy

The legend displays the number of computers on which the corresponding mode is active. You can click the number next to each mode to view a popup that displays the names of the computers and the status of the mode.

Since Last X Days

This section displays the update and scan status of the eScan client computers in the network in the form of pie charts. These charts are described as follows:

Update Status

The **Update Status** shows update status of eScan client computers in a network. Perform the following steps to view more details:

- In Update Status section, click an appropriate number link. For example, click Updated to view number of updated eScan client computers, click Not Updated to view number of not updated eScan client computers, click Unknown to view number of unknown eScan client computers, and click Total link to view all updated, not updated, and unknown records.

  A window appears displaying Machine name, Status, Update Date (MM/DD/YYY), Update Time, and Group in a tabular format. Where,

  - **Machine name:** It indicates name of the machine.
  - **Status:** It indicates status whether client computer is updated or not updated.
  - **Update Date (MM/DD/YYY):** It indicates the date when client computer is updated.
  - **Update Time:** It indicates the time when client computer is updated.
  - **Group:** It indicates name of the group.

Scan Status

The Scan Status shows status of virus scan operations conducted on eScan client computers in the network. Perform the following steps to view more details:

- In Scan Status section, click an appropriate number link. For example, click Scanned to view number of scanned eScan client computers, click Not Scanned to view number of eScan client computers that are not scanned, click Unknown to view number of unknown eScan client computers, and click Total link to view all scanned, not scanned, and unknown records.

A window appears displaying Machine name, Status, Scan Date (MM/DD/YYYY), Scan Time, and Group in a tabular format. Where,

- **Machine name:** It indicates name of the machine.
  - Click the machine name link.
    A window appears displaying **Date/Time**, **Scan Type**, and **Name**.
    Where,
  - **Date/Time:** It indicates the date and time when client computer is scanned.
  - **Scan Type:** It indicates the scan type. For example, Schedule and Manual.
    - Click an appropriate scan type to view the scan log.
  - **Name:** It indicates the job name. A job name specific to the scan appears for schedule scan and for manual scan N/A appears.
- **Status:** It indicates status whether client computer is scanned or not scanned.
- **Scan Date (MM/DD/YYY):** It indicates the date when client computer is scanned.
- **Scan Time:** It indicates the time when client computer is scanned.
- **Group:** It indicates name of the group.

Protection Statistics

This tab shows the protection statistics for the File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Endpoint Security-USB, and Endpoint Security-Application modules for the specified number of days in the form of pie charts. Each pie chart is accompanied by a legend, which displays the color code for each data label and the value associated with that label. Refer

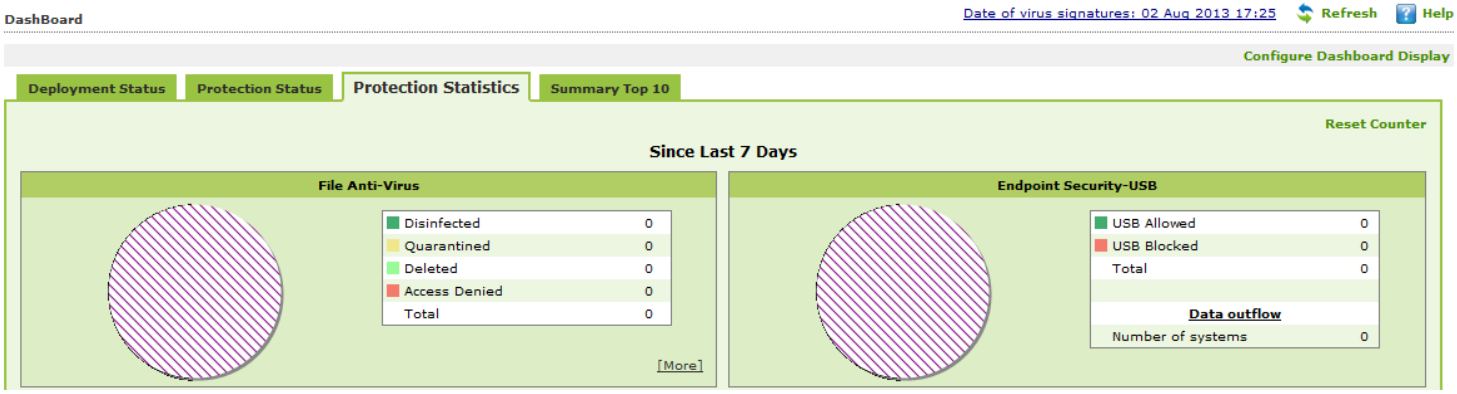


Figure 3.

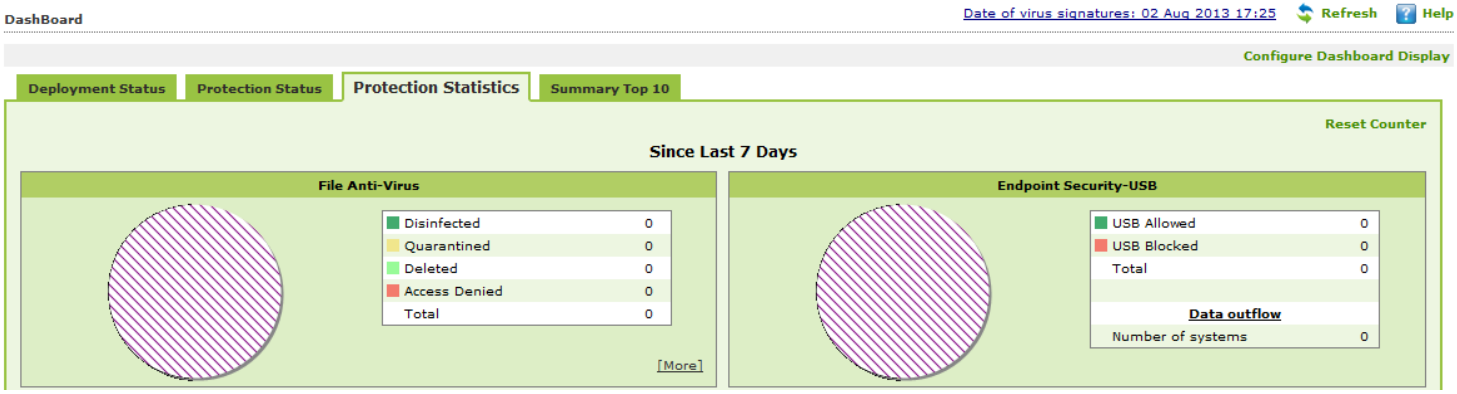


Figure 3

- The File Anti-Virus chart shows the number of files disinfected, quarantined, deleted, and access denied by the File Anti-Virus module. There is a **More** link where you can view more results on file anti-virus. Following are the details on links and how to access it:

Malware URL blocked: It indicates number of malware URL's blocked.

- To access the link, click an appropriate number link.
  A window appears displaying Machine name, Status, and Group in a tabular format. Where,
  - **Machine name:** It indicates name of the machine.
  - **Status:** It indicates number of malware URL's blocked. When you click number link. A window appears displaying Date/Time, URL Name, Action, and Description and User Name in a tabular format. Where,
    - **Date/Time:** It indicates date and time of when malware URL is accessed.
    - **URL Name:** It indicates name of the malware URL accessed.
    - **Action:** It indicates type of action taken. For example, allowed or blocked.

- **Description:** It indicates description of the blocked malware URL.
- **User Name:** It indicates the user name of the system.

- **Group:** It indicates name of the group.

Autorun blocked: It indicates number of autorun.inf files blocked.

- To access the link, click an appropriate number link.
  A window appears displaying Machine name, Status, and Group in a tabular format. Where,

  - **Machine name:** It indicates name of the machine.
  - **Status:** It indicates number of autorun.inf files blocked. When you click number link. A window appears displaying Date/Time, File Name, Action, and Description in a tabular format. Where,
    - **Date/Time:** It indicates date and time of when malware URL is accessed.
    - **File Name:** It indicates the name and location from where the autorun.inf was blocked.
    - **Action:** It indicates type of action taken. For example, allowed or blocked.
    - **Description:** It indicates description of the blocked autorun.inf file.
    - **User Name:** It indicates the user name of the system.
  - **Group:** It indicates name of the group.

Executable block USB: It indicates number of executable USB's blocked.

- To access the link, click an appropriate number link.
  A window appears displaying Machine name, Status, and Group in a tabular format. Where,

  - **Machine name:** It indicates name of the machine.
  - **Status:** It indicates number of executable USB's blocked. When you click number link. A window appears displaying Date/Time, File Name, Action, and Description in a tabular format. Where,
    - **Date/Time:** It indicates date and time of when blocked USB is accessed.
    - **File Name:** It indicates name of the file accessed.
    - **Action:** It indicates type of action taken.
    - **Description:** It indicates description of the blocked USB.
    - **User Name:** It indicates the user name of the system.
  - **Group:** It indicates name of the group.

Executable block network: It indicates number of executable blocked in a network.

- To access the link, click an appropriate number link.

  A window appears displaying Machine name, Status, and Group in a tabular format. Where,

  - **Machine name:** It indicates name of the machine.

- **Status:** It indicates number of executable blocked in a network. When you click number link. A window appears displaying Date/Time, File Name, Action, and Description in a tabular format. Where,
  - **Date/Time:** It indicates date and time of when blocked executable in a network is accessed.
  - **File Name:** It indicates name of the file accessed.
  - **Action:** It indicates type of action taken.
  - **Description:** It indicates description of the blocked executable in a network.
- **Group:** It indicates name of the group.

Executable block user based: It indicates number of user based blocked executable.

- To access the link, click an appropriate number link.

  A window appears displaying Machine name, Status, and Group in a tabular format. Where,

  - **Machine name:** It indicates name of the machine.
  - **Status:** It indicates number of user based blocked executable. When you click number link. A window appears displaying Date/Time, File Name, Action, and Description in a tabular format. Where,
    - **Date/Time:** It indicates date and time of when user based blocked executable is accessed.
    - **File Name:** It indicates name of the file accessed.
    - **Action:** It indicates type of action taken.
    - **Description:** It indicates description of the user based blocked executable.
  - **Group:** It indicates name of the group.

Proactive statistics: allow: It indicates number of executables allowed by the proactive scanner.

- To access the link, click an appropriate number link.

  A window appears displaying Machine name, Status, and Group in a tabular format. Where,

  - **Machine name:** It indicates name of the machine.
  - **Status:** It indicates number of executables allowed by the proactive scanner. When you click number link. A window appears displaying Date/Time, File Name, and Description in a tabular format. Where,
    - **Date/Time:** It indicates date and time of when allowed executable is accessed.
    - **File Name:** It indicates name of the file accessed.
    - **Description:** It indicates description of executable allowed by the proactive scanner.
  - **Group:** It indicates name of the group.

Proactive statistics: block: It indicates number of executables blocked by the proactive scanner.

- To access the link, click an appropriate number link.
  A window appears displaying Machine name, Status, and Group in a tabular format. Where,
  - **Machine name:** It indicates name of the machine.

- **Status:** It indicates number of executables blocked by the proactive scanner. When you click number link. A window appears displaying Date/Time, File Name, and Description in a tabular format. Where,
  - **Date/Time:** It indicates date and time of when blocked executable is accessed.
  - **File Name:** It indicates name of the file accessed.
  - **Description:** It indicates description of executable blocked by the proactive scanner.
- **Group:** It indicates name of the group.

- **Total:** Click this link, if you want to view all the details of additional protection statistics in one window.

- The Mail Anti-Virus chart shows the number of quarantined, deleted, and disinfected e-mails detected by the Mail Anti-Virus module.
- The Anti-Spam chart shows the number of e-mails deleted and quarantined by the Anti-Spam module.
- The Web Protection chart shows the number of Web sites allowed and blocked by the Web Protection module.

  The Suspected Phishing Site link enables you to view the list of suspected phishing sites on system.
- The Endpoint Security – USB chart shows the number of USB's allowed or blocked by endpoint security.

  Perform the following steps to view more details:

1. In **Endpoint Security – USB** section, click an appropriate number link. For example, click USB allowed to view number of USB's allowed, click USB blocked to view number of USB's blocked, and click Total link to view both USB allowed and USB blocked records.

   A window appears displaying **Machine name**, **Status**, and **Group** in a tabular format. Where,

   - **Machine name:** It indicates name of the machine.
   - **Status:** It indicates whether USB allowed or USB blocked.
   - **Group:** It indicates the group name to which the machine belongs
2. Under **Status** column, click an appropriate link. For example, USB allowed (X) and USB blocked (X), X as number of USB's allowed and blocked.

   A window appears displaying **Date/Time**, **Serial No**, and **Description** in a tabular format.
   Where,

   - **Date/Time:** It indicates date and time when USB is accessed.
   - **Serial No:** It indicates serial number of the USB.
   - **Description:** It indicates detailed description of the USB.
   - **User name:** It indicates the user name of the system where the USB was accessed.

   - **Group:** It indicates name of the group.

The **Data outflow** link enables you to view data of all the files that are copied from computer to USB drive.

- The Endpoint Security-Application shows the number of applications allowed or blocked by endpoint security.

Summary Top 10

The Summary Top 10 tab displays a graph of the following entities listed below which are populated as per – Since Last (X) days:

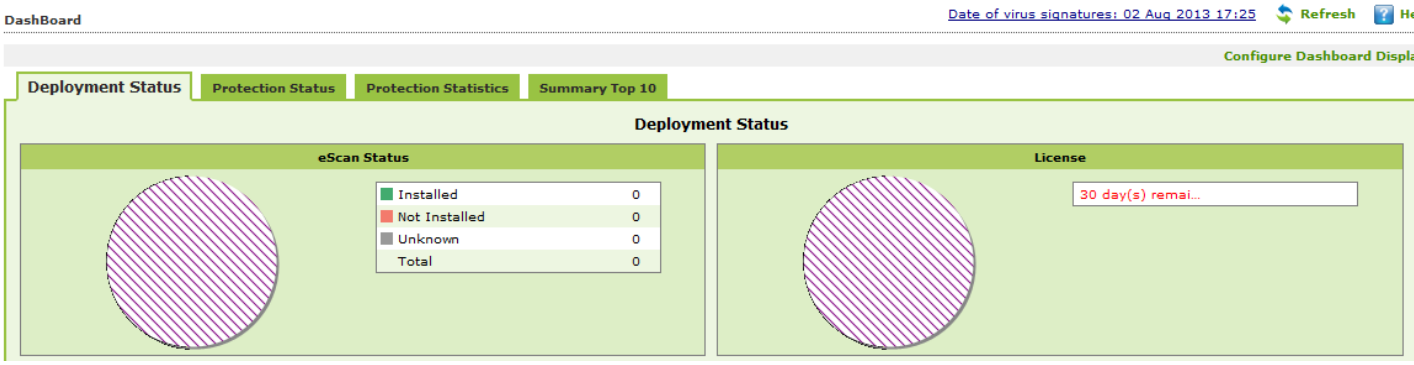
- Machine Infected
- USB Blocked
- Application Allowed by Computer
- Application Blocked by Computer
- Website Blocked by Computer
- Website Allowed by Computer
- Application Blocked by App Name
- Application Allowed by App Name
- Website Blocked by Sites
- Website Allowed by Sites
- Infected Emails
- Spam Emails
- Virus Blocked

Configuring Dashboard

Dashboard enables you to configure the charts appearing on each tab, as per your requirement.

To configure dashboard

3. On the navigation pane, click **Dashboard**.
   The **Dashboard** screen appears. Refer



4. Figure 1.

5. Click the **Configure Dashboard Display** link, at upper-right corner of the screen. The **Configure Dashboard Display** window appears. Refer Figure 4.

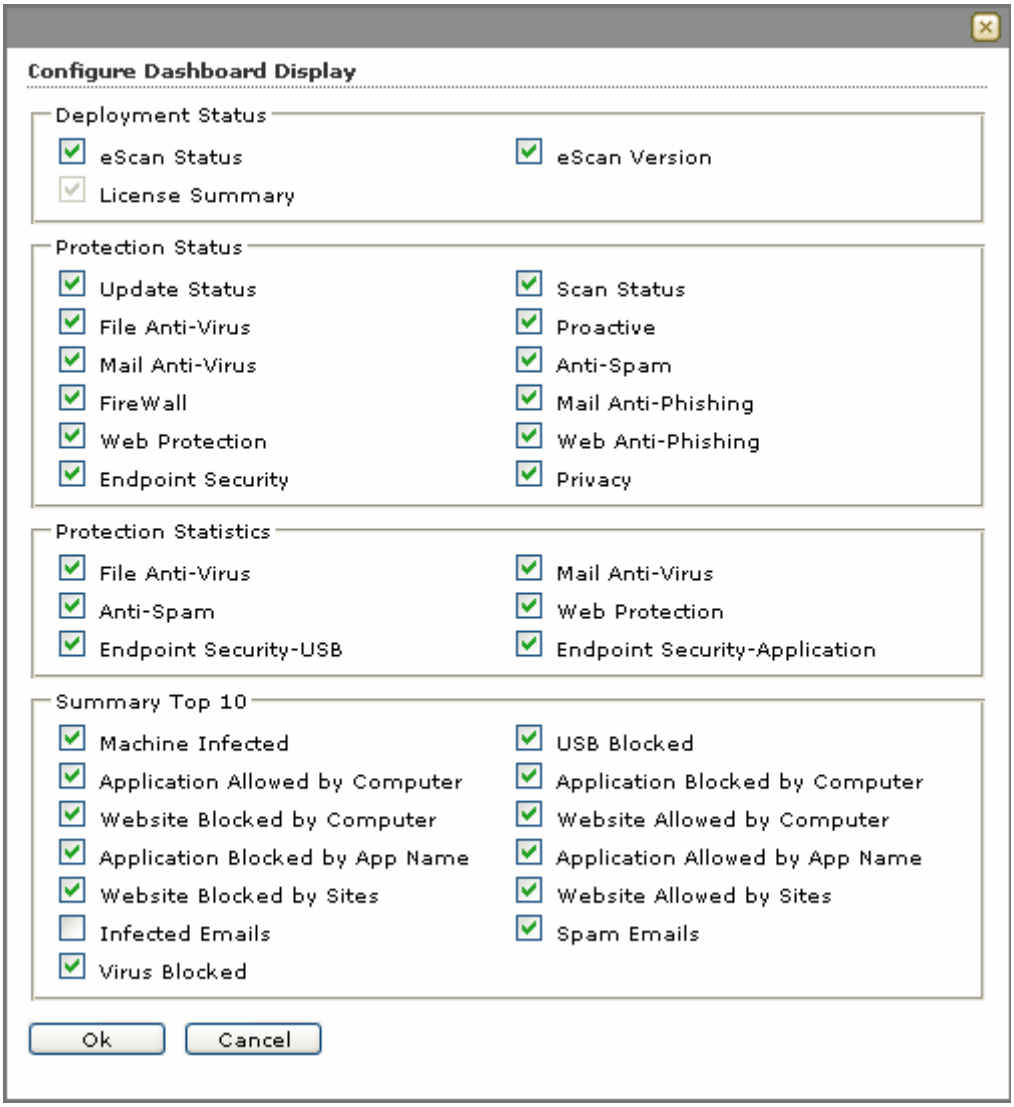


Figure 4

6. Select an appropriate check box from all sections that you want to configure on the dashboard.
7. Click the **Ok** button.
   The charts get configured on the **DashBoard** screen.

Setup Wizard

This is a first page that appears by default when you log on to the application for the first time. It is recommended that you create groups, assign computers, and install eScan on respective computers before proceeding to the other modules.

Alternatively, on the navigation pane, click **Setup Wizard** module, to view the **Setup Wizard** screen.

You can do the following activities:

- Adding IP/Host
- Adding Host from the unassigned Computer

Adding IP/Host

It enables you to add client to respective groups through IP/Host. Perform the following steps to add client.

1. On the **Welcome to the Setup Wizard** screen. Refer Figure 5.

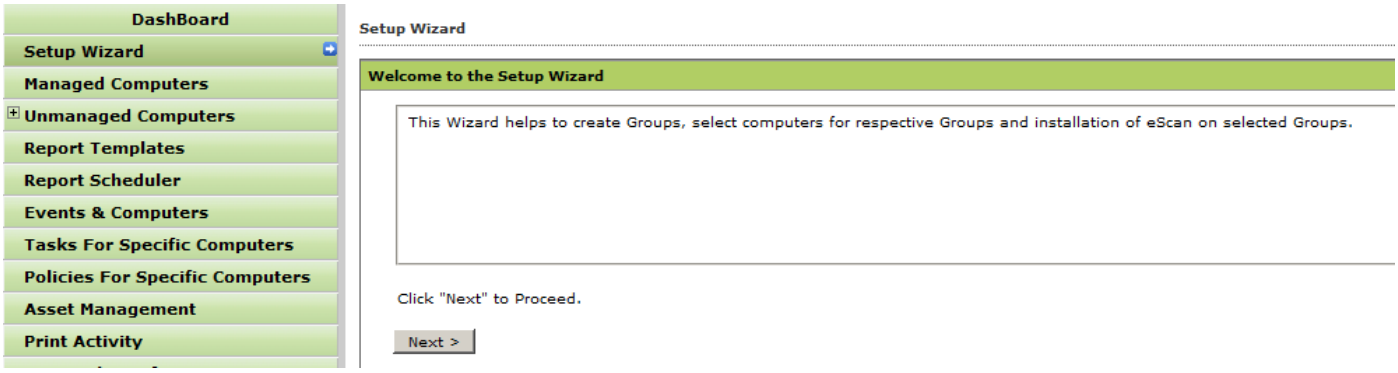


Figure 5

2. Click the **Next >** button.
   The **Create Group to Manage Computers.** Screen appears. Refer Figure 6.

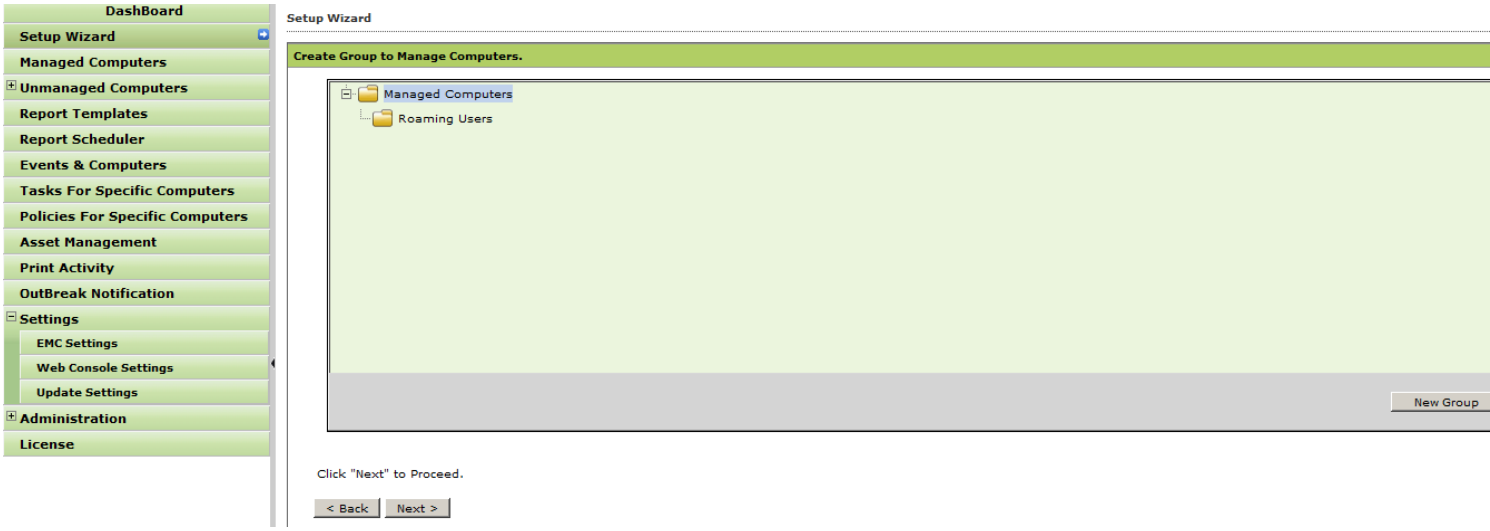
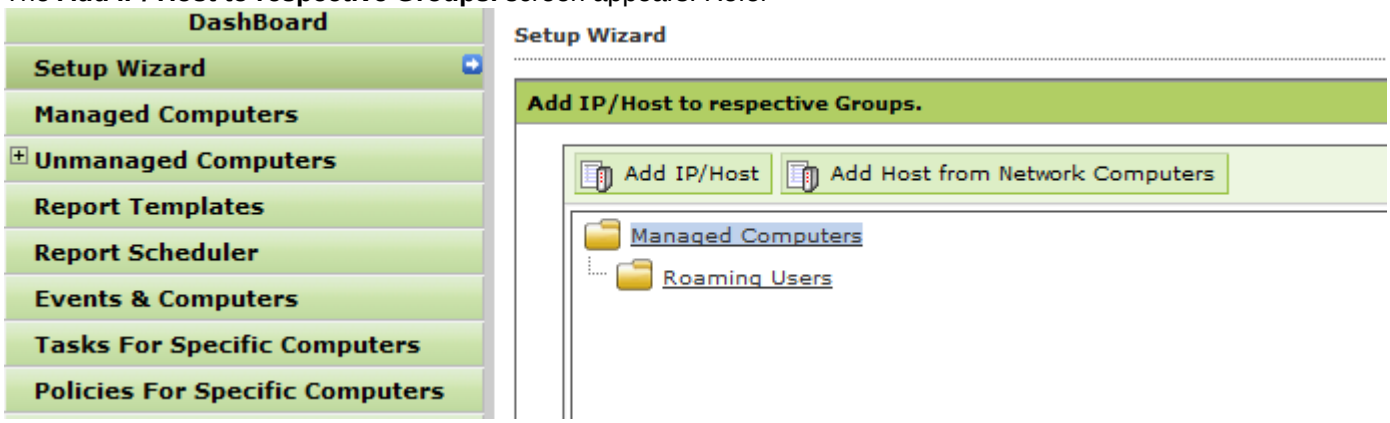


Figure 6

3. Click the **New Group** button to create a new group with the name you wish to create.
4. If you want to delete group, right-click the new group, and then click **Delete**.

> You can modify or delete only the newly created groups before proceeding to the next step. You cannot modify or delete the groups that appear by default.

5. Click the **Next >** button.
   The **Add IP/ Host to respective Groups.** screen appears. Refer



6. Figure 7.

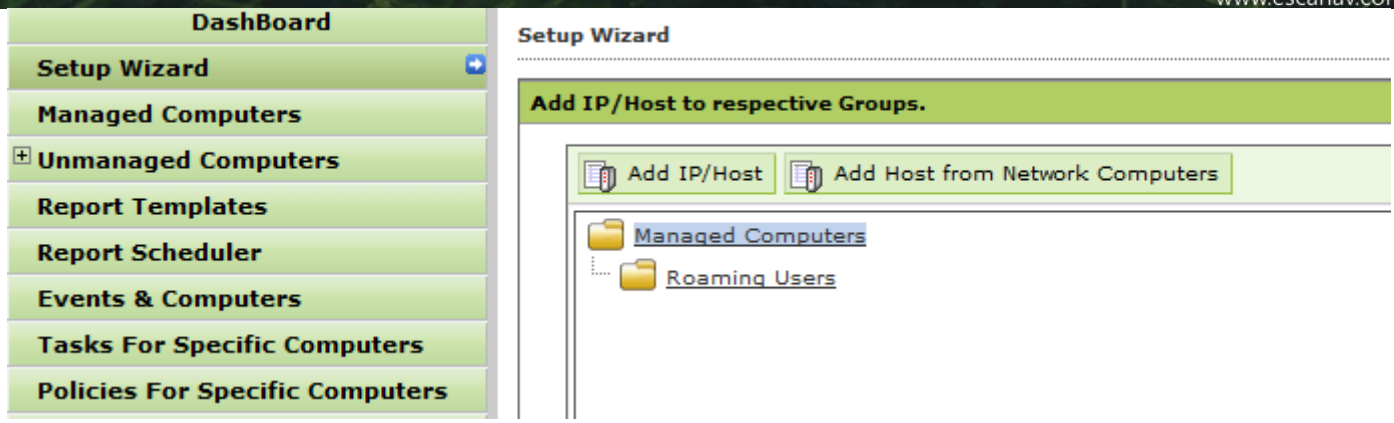


Figure 7

7. By default, the Add IP/Host and Add Host from the Network Computers button appears dimmed.

To add client, click group name for which you want to add client, and then click Add IP/Host **button. A window appears where you can add computers through host name, IP range, and also you can remove the added computers. Refer**

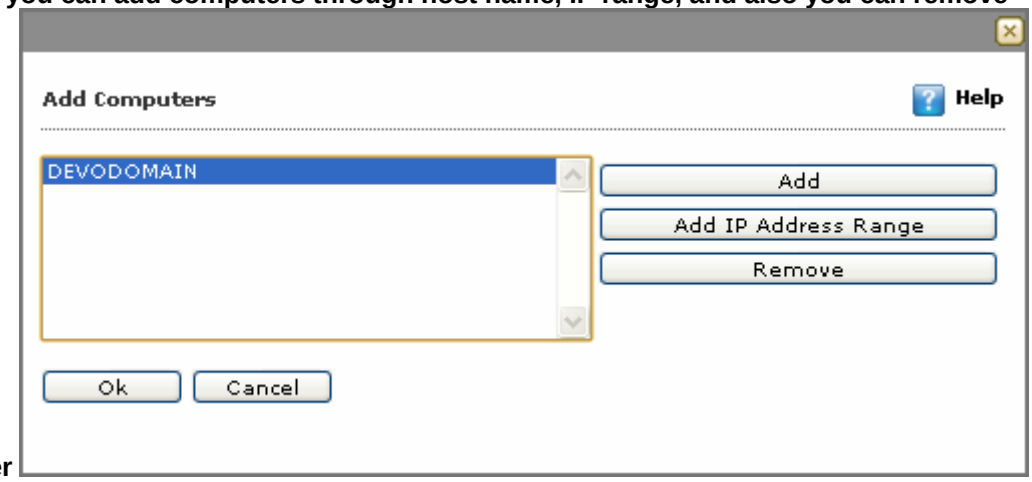


Figure 8.

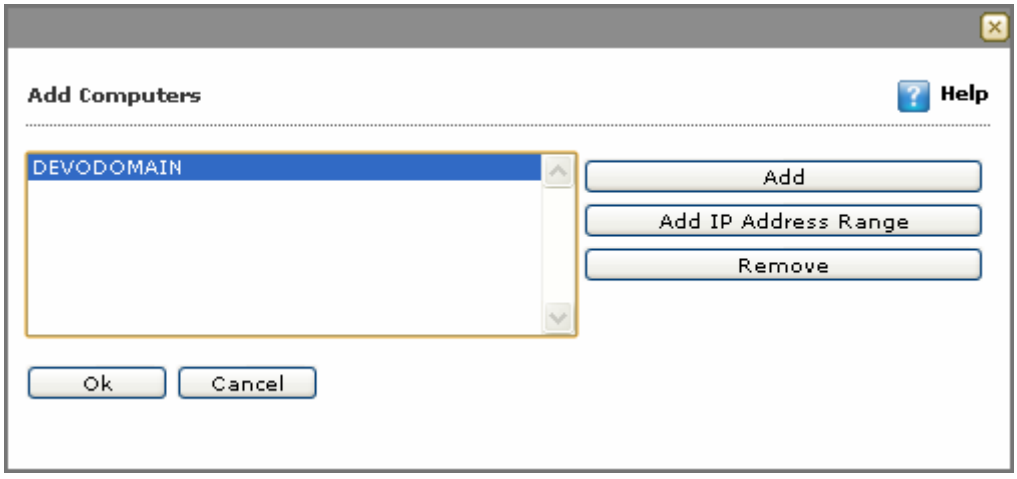


Figure 8

9. Click the **Add** button.
   A window appears. Refer Figure 9.

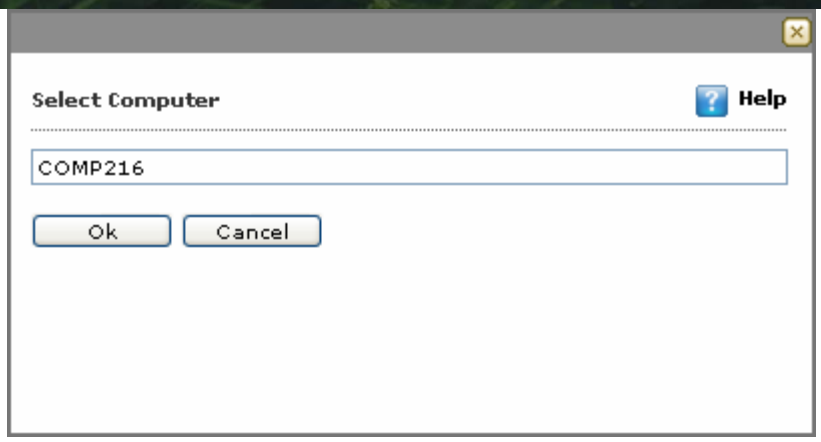


Figure 9

10. In the **Select Computer** field, type the host name that you want to add.
11. Click the **Ok** button.
    The added computer appears in **Add Computers** list.
12. Click the **Add IP Address Range** button.
    A window appears where you can add IP addresses of computers that you want to add. Refer Figure 10.

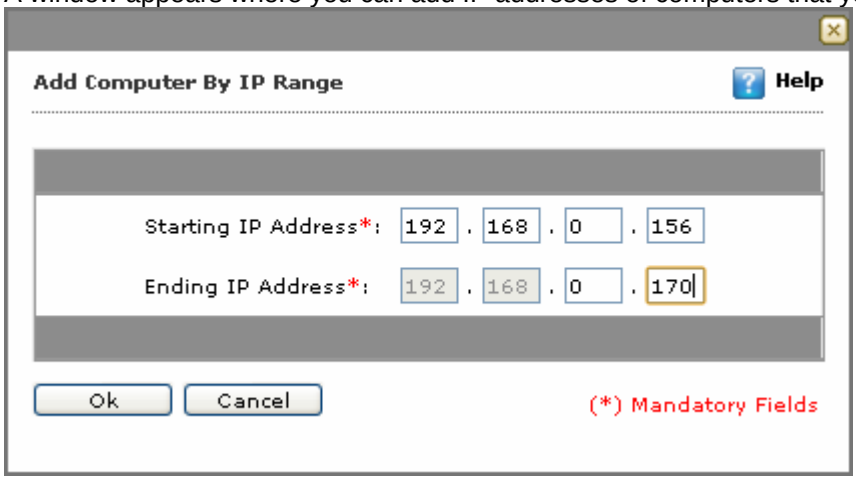


Figure 10

13. In the **Starting IP Address** field, type IP address of the computer from which range you want to add. It is a mandatory field.
14. In the **Ending IP Address** field, type IP address of the computer till which range you want to add. It is a mandatory field.
15. Click the **Ok** button.
    The added computer appears in **Add Computers** list.
16. If you want to cancel the action, click the **Cancel** button.
17. If you want to remove added computers, click the appropriate computer from the **Add Computers** list, and then click **Remove**.
    The computer gets removed from **Add Computers** list.
18. Click the **Ok** button.
    The computers get added in their respective group.

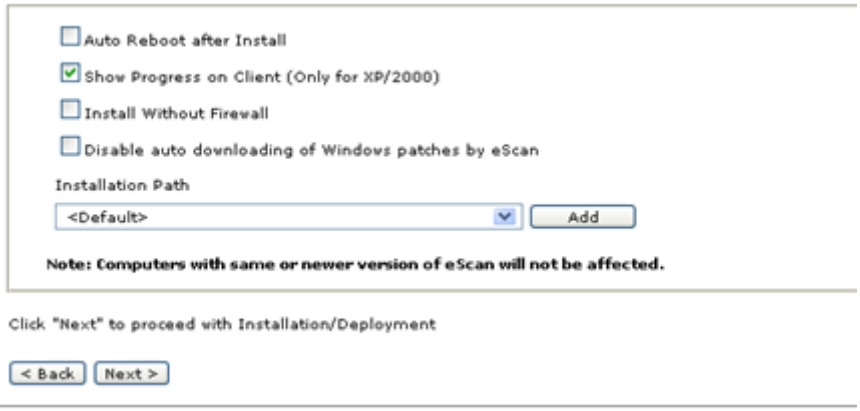
Click the Next > **button.**

The Select Groups for Installation/Deployment **screen appears. Refer**

19. Figure 11.

Figure 11

Select the appropriate check box, group on which you want to install/deploy, and then click Next > **button. It is mandatory to select at least one group.**
The Client Configuration **screen appears. Refer**



20. Figure 12.

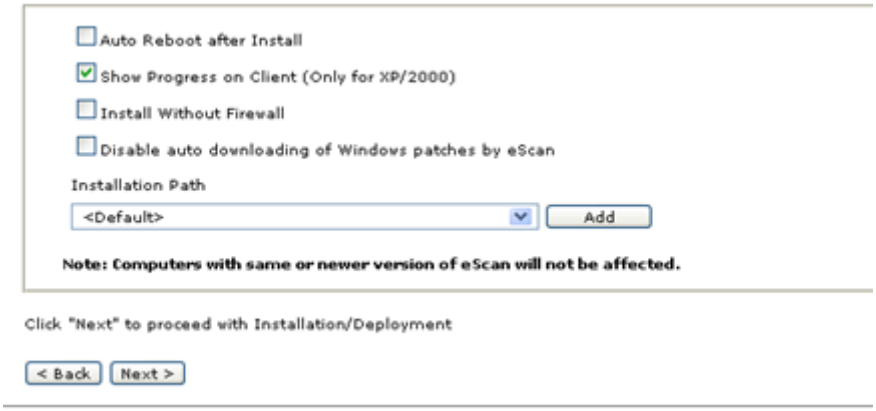


Figure 12

21. Select the **Auto Reboot after Install** check box, if you want to auto restart the client system after installation.
22. Select the **Show Progress On Client (Only for XP/2000)** check box, if you want to view installation progress on client system.

The option to view progress is available only on Windows **XP/2000** version, operating system.

23. Select the **Install Without Firewall** check box, if you want to view install eScan without Firewall module.
24. Select the **Disable auto downloading of Windows patches by eScan** check box, if you do not want eScan to auto download the windows patches.
25. In the **Installation Path** drop-down list, default path appears.
26. To change path, click the **Add** button.
    A window appears.
27. In the **Add folder** field, type folder path where you want to install, and then click **Add** button.
    The added path appears in the **Installation Path** drop-down list.
28. If you want to cancel the action, click the **Cancel** button.
29. Click the **Next >**button, to install/deploy.
    The **Client Installation** screen appears.

The computers having same or newer version of eScan are not affected. And eScan will not install eScan firewall if Server operating system is found

During the process of installation, in case any error occurs in connecting the login information details. In such a situation, you can set host configuration details for both client and group by clicking the following two options:

- **Set Host Configuration for Client(X):** Click this link if you want to add the login information details for the host computer of a client. For example, X indicates the machine name. For more information on how to add the login information, refer setting the Host Configuration section.

- **Set Host Configuration for group(X):** Click this link if you want to add the login information details for the host computer of a group. For example, X indicates the machine name. For more information on how to add the login information, refer setting the Host Configuration section.

30. Click the **Finish** button.
    The **Dashboard** appears.

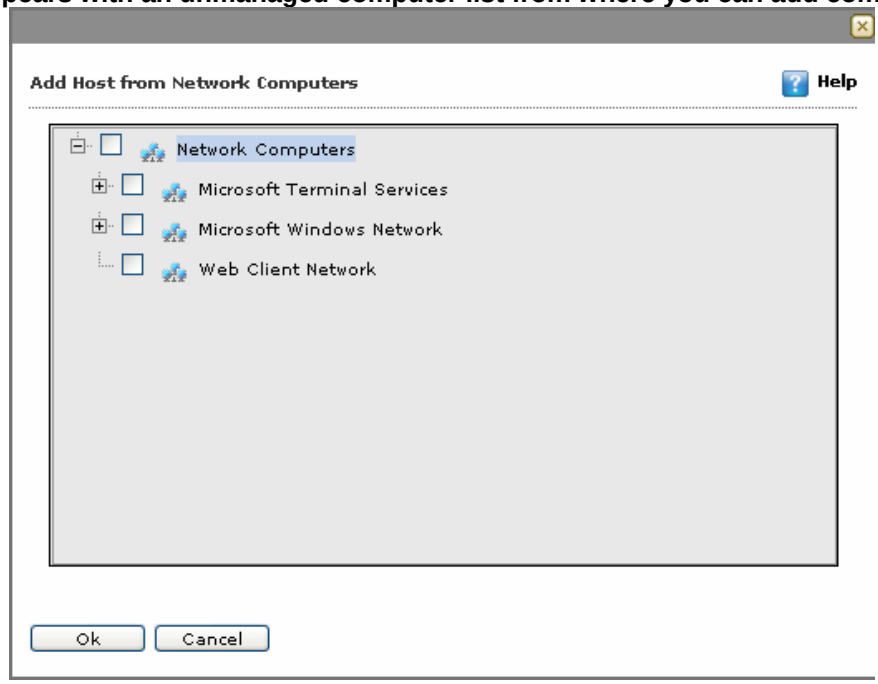
Adding Host from Network Computers

It enables you to add computers from domain to respective groups. Perform the following steps to add client.

1. Repeat the steps from 1 to 6 as given in Adding IP/Host section.

To add computer from domain, click the group name for which you want to add host, and then click the Add Host from Network Computers **button.**

A window appears with an unmanaged computer list from where you can add computers. Refer



2. Figure 13.

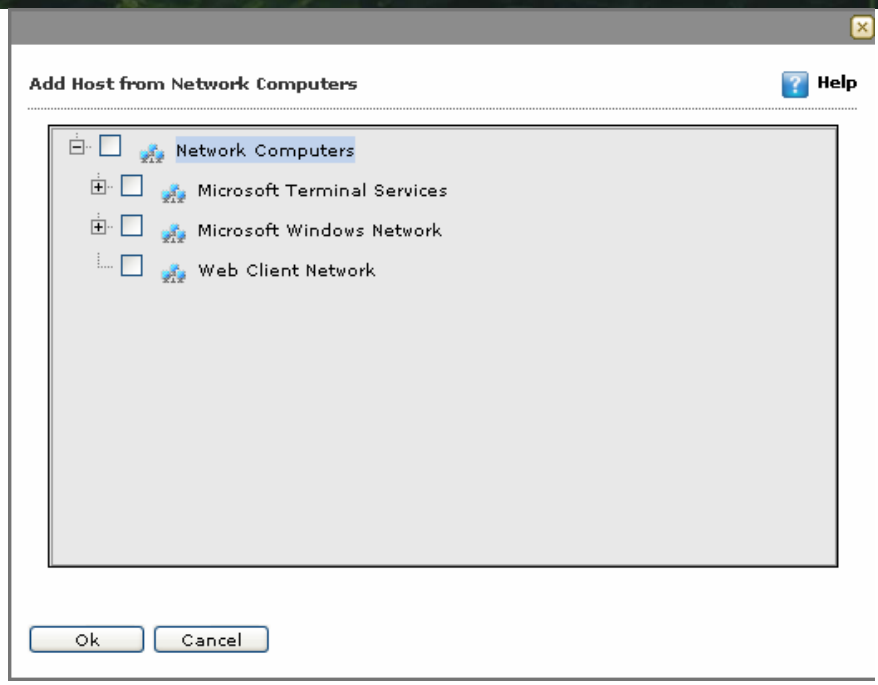


Figure 13

3. Select an appropriate check box, groups that you want to add, and then click **Ok** button. The computers get added in their respective group.
4. Repeat the steps from 18 to 29 as given in Adding IP/Host section.

Managed Computers

The **Managed Computers** page allows you to perform management tasks such as creating and removing groups; installing and uninstalling applications; and viewing the properties of client computers.

This page is organized like a file explorer window; it is divided into two panes. The left pane shows a console tree and the right pane, which is the task pane, shows the information about the selected node in the tree.

This page also displays a **Search** button, which allows you to search for computers and add them to the Client Computers group or any other user-defined group.

Console Tree

The console tree displays the hierarchical structure of the eScan servers and client computers in the eScan network.

The root node in the console tree is **Managed Computers**. It stores and displays the configuration information of groups, group policies, group tasks, and client computers in the eScan network. Its three sub-nodes are **Policies**, **Group Tasks**, and **Client Computers**. You cannot delete root node that is Managed Computers.

- The Policies page enables you to configure various policy details as per your requirement.
- The Group Tasks page lists the tasks that can be applied to a particular group of computers. However, to use this feature, first you need to create computer groups. These groups appear as separate nodes under Managed Computers.
- The Client Computers page lists all the client computers on the eScan network. You can add computers to this list by using the Unmanaged Computers link on the navigation bar.

Task Pane

Whenever you select a node in the console tree, the corresponding information is displayed in the task pane. The task pane usually displays information in a tabular format. On some pages, it may also display additional buttons or menus.

Policies Pane

A policy or a rule-set is a collection of eScan rules that can be executed on an individual computer or computer group.

The **Properties** button in the policy screen is divided in to two tabs - **General** and **Policy Details**. In **General** tab, you can view the general policy details and in **Policy Details** tab, you can configure the policy details.
The **Copy Policy** button helps to copy the policy to a group.

Group Tasks Pane

The **Group Task** pane allows you to create and view the tasks that apply to a group of computers. This pane shows the **New Task**, **Start Task**, **Properties**, **Results**, and **Delete** buttons.

You can create a task and enable it to run at a specific time by configuring the options in the New Task Template window. This window is displayed when you click **New Task** in the **Group Tasks** pane. You can then specify a name for the task, and then select the actions in the **Assigned Tasks** section. In this section, you can choose to view the status of modules, start or stop servers, set an update server, perform scans, or force computers to download updates. You can also run the task on subgroups by selecting the **Apply for subgroups** check box.

You can configure the task to run either manually or automatically. The tasks can be scheduled to run at a specific time either on a daily or monthly basis or on certain days of the week.

Client Computers Pane

The **Client Computer** pane lists all the managed computers that have not yet been assigned to any particular computer group. You can add computers to this pane with the help of the **Network Computers** link on the navigation bar.

Accessing the Search Feature

At times, you may need to add a particular computer to a group, but you may not have a clear idea of the workgroup to which it belongs. The Search feature of the eScan Web Console comes handy in such situations.

To access search feature

1. On the navigation pane, click **Managed Computers**.

   The **Managed Computers** screen appears. Refer Figure 14.

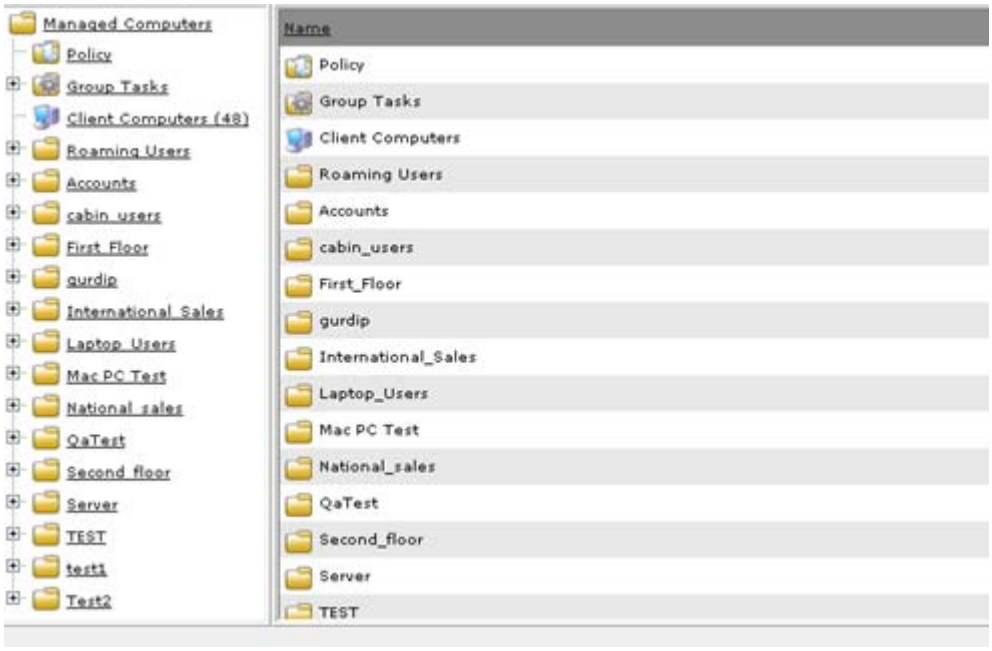


Figure 14

2. At the upper left side, click the **Search** button.

The Search for Computers **window appears. Refer**

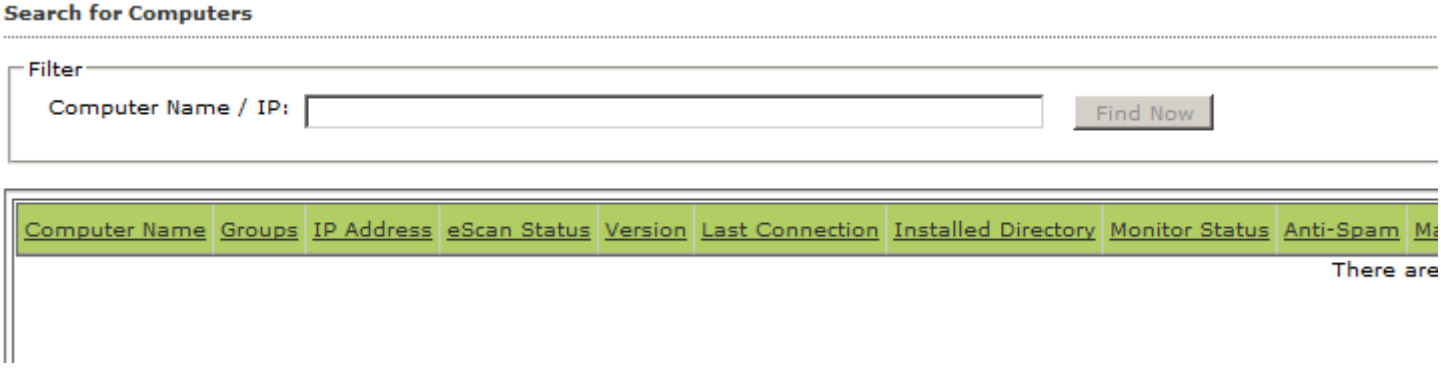


Figure 15.

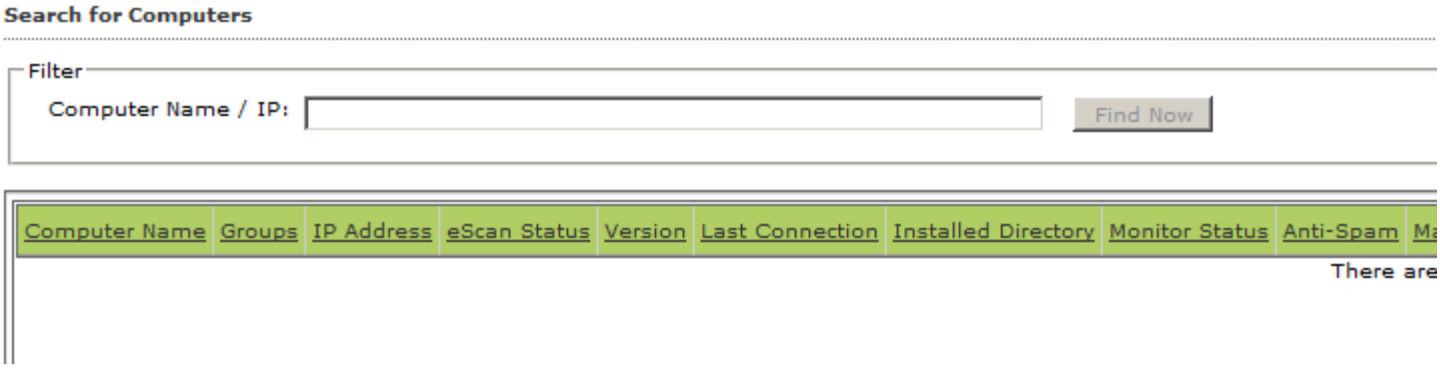


Figure 15

3. Under **Filter** section, in the **Computer Name** field, type the computer name that you want to search.

For example, if you are searching for a computer named “Comp20” in your network, you can specify **Comp20** in the **Computer Name** field. However, if you want to find all computers whose names begin with text string “Comp,” you need to specify only **Comp*** in the **Computer Name** field.

4. Click the **Find Now** button.
   The following field details appear in a tabular format.

- The name of the computer
- The name of the group
- The IP address of the computer
- The status of eScan, whether it is installed on the computer or not
- The version of eScan
- Last connection
- The directory in which eScan is installed on the computer
- The status of the eScan monitor
- The status of the Anti-Spam, Mail Anti-Virus, Web Protection, Endpoint Security, and Firewall modules
- The timestamp of the last update
- The name of the update server
- The operating system installed on the computer
- The status of the eScan installation, whether it has all the critical patches and hotfixes installed on it or not

The symbol indicates status as protected, symbol indicates status as not installed/critical, and symbol indicates status as unknown.

You can sort the rows in the table by any of the above criteria by clicking on the corresponding heading.

Menus

In addition, the window shows you two menus: **Action List** and **Client Action List**.

The **Action List** menu under **Managed Computers** has the following options: Refer Figure 16.

Figure 16

- New Group: It enables you to create new group and sub-group for maintaining policies and tasks of various clients.
- Set Group Configuration: It enables you to set basic login information for the group.
- Deploy / Upgrade Client: It enables you to install eScan application on the client machine.
- Uninstall eScan Client: It enables you to uninstall eScan application that is installed on the managed computer.
- Create Groups and Tasks: It enables you to create group structures and tasks based on Active Directory and Workgroup. If you want the same structure which is present in ADS or Workgroup, you can use this option.
- Properties: The properties enable you to create update agent who plays an important role in providing latest updates to its clients. You can change the properties of normal and roaming user.

The **Action List** menu under **Unmanaged Computers** has the following options: Refer Figure 17.

Figure 17

- Set Host Configuration: It enables you to set basic login information for the host computer.
- Move to Group: It enables you to move computers to a managed computer group or any of its sub-groups.
- **Properties:** It enables you to view properties of the selected computer. The properties are divided in to three sections – **General**, **AV-Status**, and **Protection**.
- Refresh Client: It enables you to refresh the client details in case, if you have made any kind of changes on the Managed Computers screen.

The **Client Action List** menu has the following options: Refer Figure 18.

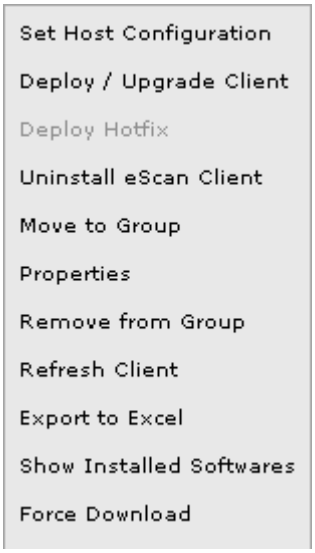


Figure 18

- Set Host Configuration: It enables you to set basic login information for the host computer.
- Deploy / upgrade Client: It enables you to install eScan application and other software on the client machine.
- Deploy Hotfix: It enables you to deploy hotfix on the client machine.

The **Deploy Hotfix** option is available only when you download it on the eScan server from the **eScan Protection Center**, by clicking the **Download Latest Hotfix** link, under **Tools** module.

- Uninstall eScan Client: It enables you to uninstall eScan application that is installed on the client machine.
- Move to Group: It enables you to move computers to a managed computer group or any of its sub-groups.
- Properties: It enables you to view properties of the selected computer. The properties are divided in to three sections – General, AV-Status, and Protection.

- Remove from Group: It enables you to remove client from the managed computer group.
- Refresh Client: It enables you to refresh the client details in case, if you have made any kind of changes on the Managed Computers screen.
- Export to Excel: It enables you to export the managed client computer details into an excel sheet.

You can access the **Export to Excel** option, only if Microsoft Excel software is installed on the server, on which the eScan Management Console is installed.

- Show Installed Softwares: It enables you to view the name and total number of software programs installed on a specific computer.
- Force Download: Click on this option to forcefully download eScan Client application on a machine connected to the network

Managing Unmanaged Computers

The **Unmanaged Computers** section allows you to view the network computers, IP range, or Active Directory domains that have not been assigned to any computer group. You can use this page to discover the computers on your network and then add them to groups depending on the organization's structure and your requirements.

The **Unmanaged Computers** node in the navigation bar has four sub-nodes: **Network Computers**, **IP range**, **Active Directory** and **New Computers Found**. When you click a sub-node, the corresponding page is displayed.

Each page is organized like a file explorer window. It is divided into two panes with the left pane showing a console tree and the right pane (the task pane), showing the information about the selected node in the console tree.

Each page also shows an **Action List** menu, which allows you to set the host configuration, move the selected computer to a computer group, view the properties of the computer or group, and refresh the client computer. Initially, on all these pages, the **Action List** menu is disabled. To enable it, you must select a computer name in the task pane.

Reports Template

The **Reports Template** page provides you with predefined reports based on eScan modules. It provides you an option to create custom reports based on certain criteria.

This page is displayed when you click **Reports Template** in the navigation bar. You can click this option to view the corresponding report. The page provides you with options to create new reports, view the properties of reports, configure and schedule reports, and delete only those reports that are created by you.

Report Scheduler

The **Report Scheduler** page allows you to schedule the creation and sending of reports based on your requirements.

This page is displayed when you click **Report Scheduler** in the navigation bar. This page displays the details of user defined scheduled tasks in a tabular format. The page displays a table containing report names and a **View** link next to each name. The table shows information like the name of the schedule, the name of the report recipient, and the scheduler type. In addition, it has options that allow you to create a new schedule, run a task manually, view the status of tasks, and view the properties of the selected scheduled task.

Events & Computers

The **Events & Computers** module enables you to monitor various activities performed on client's computer. You can view log of all events based on certain criteria's and settings defined in **Settings** button.

The **Events & Computers Settings** window is divided in to three tabs - Event Status, Computer Selection, and Software/ Hardware Changes.

The **Edit Selection** enables you to edit various computer selections.

Tasks for Specific Computers

The Tasks for Specific Computers page allows you to create tasks that you want to run on specific computers or computer groups at a specific time on specific days.

When you click the Tasks for Specific Computers node in the navigation bar, its corresponding page appears in the right pane. This pane displays a table that contains information such as the name of the task, the status of the task performed, the computer to which the task has been assigned, and the type of schedule. In addition, the pane displays options for creating a new task, starting a task, viewing its properties, viewing the results of the task, and deleting an existing task.

Policies for Specific Computers

The **Policies for Specific Computers** page enables you to create and deploy policy on specific client computer same as for groups, based on certain settings. There is also an option to delete policy and view properties of policy whenever required. This is an alternative method, the reason being every Managed group will have the default policies, if a system which is present in that Managed Group does not want to have that default policies applied, and then this feature comes in the picture. Otherwise you can make use of Policies from Managed Computers. Policy for specific computers will take precedence over group policies.

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 you requirement. It also allows you to Export the entire system information available through this module in PDF, Ms Excel or HTML formats.

Print Activity

It monitors and Logs printing tasks done by all the Managed computers, it gives you a report of all Printing Jobs done by Managed computers through any Printer connected to the network. It also gives you a report of all PDF conversions done on individual Machine connected to the network.

Outbreak Notifications

The **Outbreak Notifications** page allows you to configure to notify you whenever there is a virus outbreak in the network. This page is displayed when you click **Outbreak Notification** in the navigation bar. This page displays the settings for controlling the number of times eScan should send e mail alerts during the specified number of days or hours.

Configuring the EMC, Web Console, and Updater

The **Settings** page allows you to configure the settings related to EMC, Web Console, and Updater.

Administration

The **Administration** menu enables you to maintain the user account, user role, and export and import the settings. It contains the following sub-menus:

- The User Accounts enables you to add custom accounts or active directory users or groups.
- The Export and Import Settings enables you to export and import the settings and policies of WMC and database.

License

The **License** page enables you to add, activate, and manage licenses. In manage licenses, you can 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.

Chapter 4: Managing Computers and Computer Groups

The eScan Web Console simplifies the management of eScan client computers in a network by providing you with options for creating, modifying, deleting, and moving computer groups. In addition, it also allows you to install and uninstall eScan and other software in the network.

- Managing Individual Hosts
- Managing Computer Groups
- Creating Groups and Tasks
- Installing and Uninstalling Applications

Managing Individual Hosts

Administrators may often have to perform management tasks such as assigning authentication information to host computers, checking the properties of host computers, removing host computers from the console tree, or obtaining the latest information about computers from the network.

- Setting the Host Configuration
- Viewing the Properties of a Host Computer
- Deploying Hotfix
- Moving Computers to Group
- Refreshing Clients

Setting the Host Configuration

It enables you to set basic login information for the host computer.

> If the computer that you want to log on is part of a domain, then you must specify the domain name along with the user name while logging in. For example, if the computer **Mrktng1** is within the **Marketing** domain and you want to log on as an Administrator, you must specify the user name as **Marketing\Administrator** when you log on to the computer using EMC.

To set host configuration

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 19.

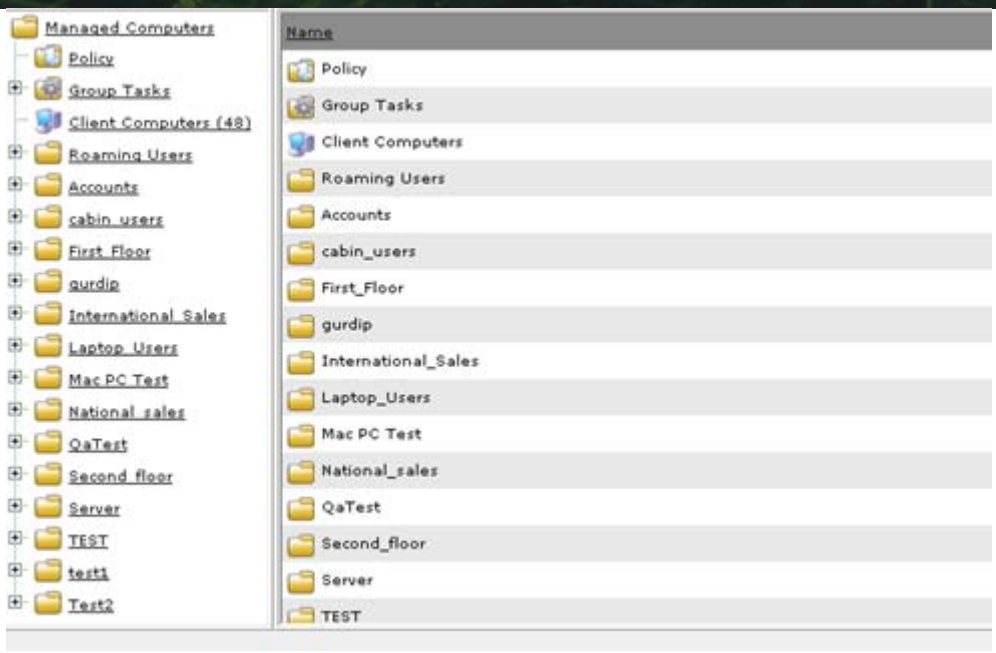
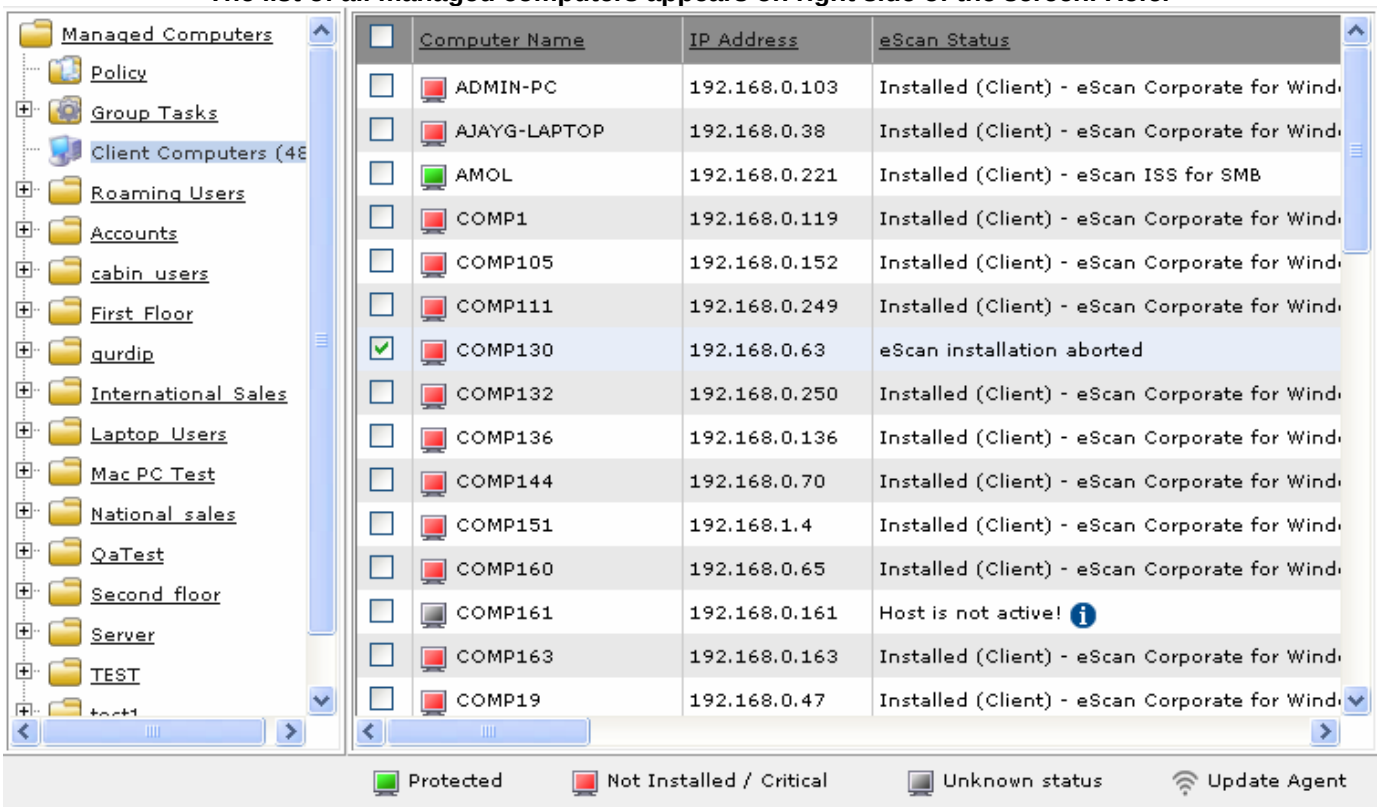

Managed Computers
Policy
Group Tasks
Client Computers (48)
Roaming Users
Accounts
cabin_users
First_Floor
gurdip
International_Sales
Laptop_Users
Mac PC Test
National_sales
QaTest
Second_floor
Server
TEST
test1
Test2
Name
Policy
Group Tasks
Client Computers
Roaming Users
Accounts
cabin_users
First_Floor
gurdip
International_Sales
Laptop_Users
Mac PC Test
National_sales
QaTest
Second_floor
Server
TEST

Figure 19

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

On the left pane, under an appropriate managed computers folder, click Client Computers**. The list of all managed computers appears on right side of the screen. Refer**



2. Figure 20.

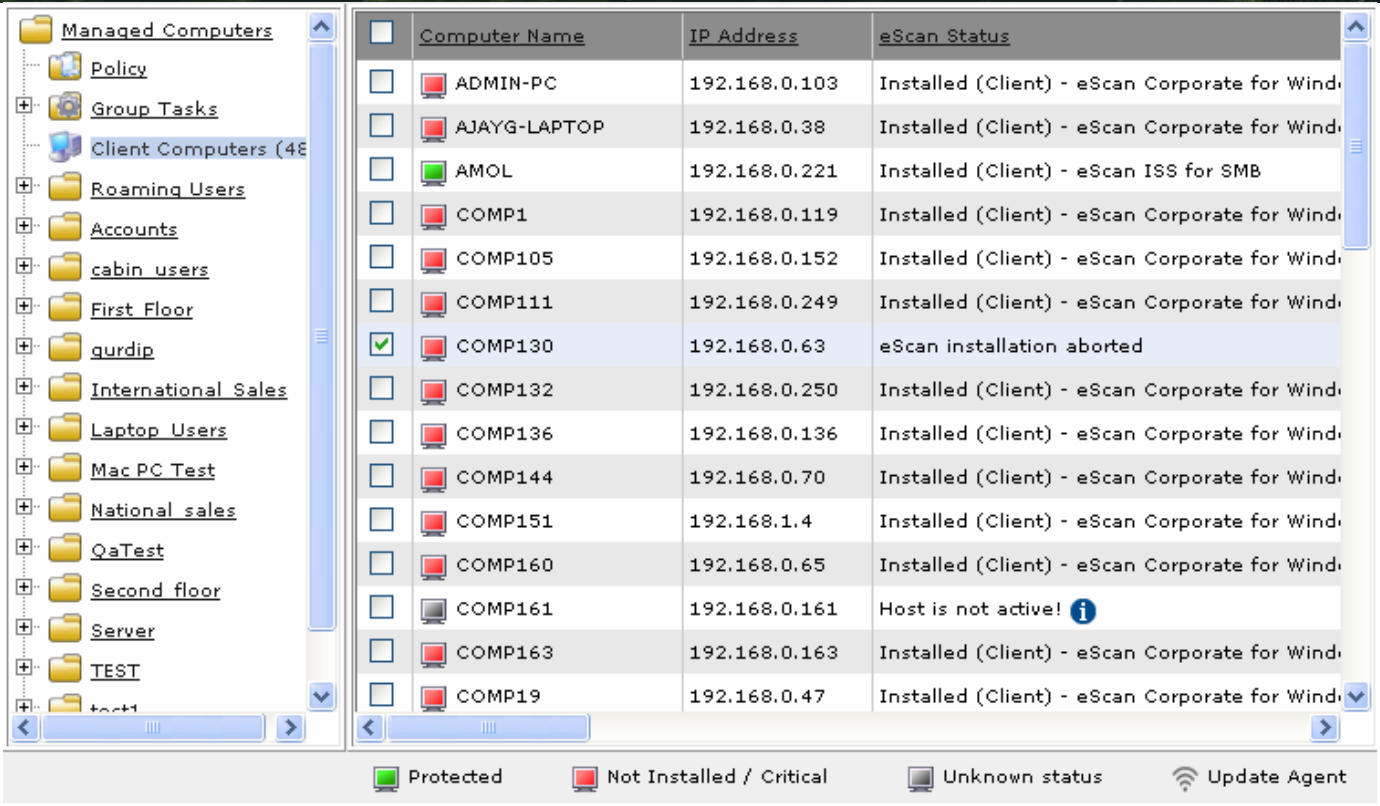


Figure 20

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box for which you want to set configuration.

The **Set Host Configuration** menu and **Refresh Client** button is available, only when you select an appropriate computer name check box from the list.

Click the Client Action List **drop-down menu, and then click** Set Host Configuration**.**
The Set Host Configuration **window appears. Refer**

4. Figure 21.

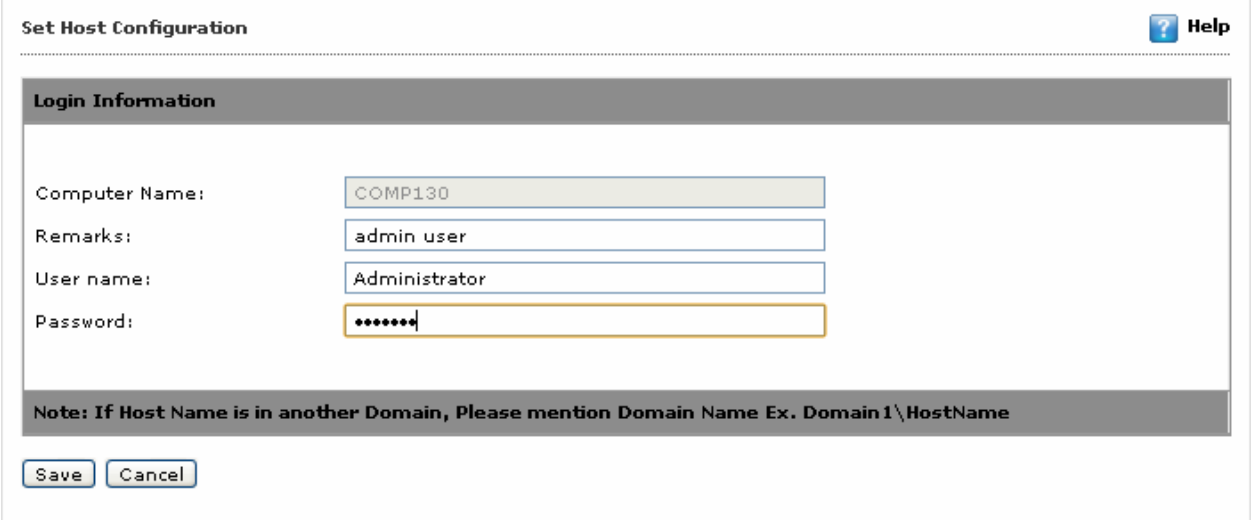


Figure 21

5. Specify the following field details.

Field	Description
Login Information	
Computer Name	It displays the name of selected group. It appears dimmed.
Remarks	Type the remarks, if any.
User name	Type the login user name of selected group.
Password	Type the password of selected group.

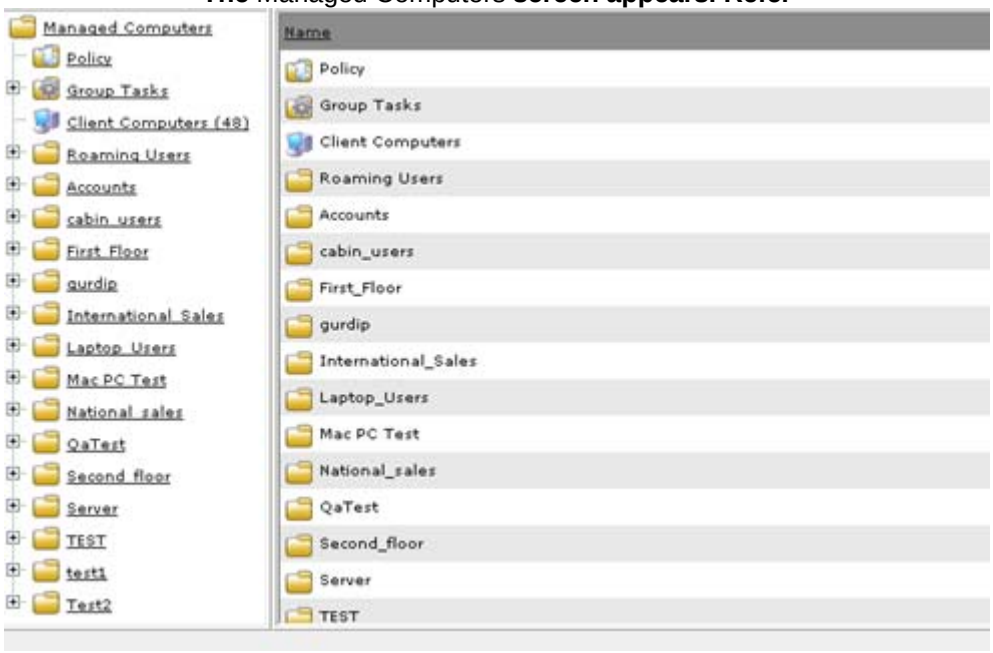
6. Click the **Save** button.
   The login information gets saved.

Viewing the Properties of a Host Computer

It enables you to view properties of the selected computer. The properties are divided in to three sections – **General**, **AV-Status**, and **Protection**.

To view the properties

On the navigation pane, click Managed Computers**.**
The Managed Computers **screen appears. Refer**



1. Figure 22.

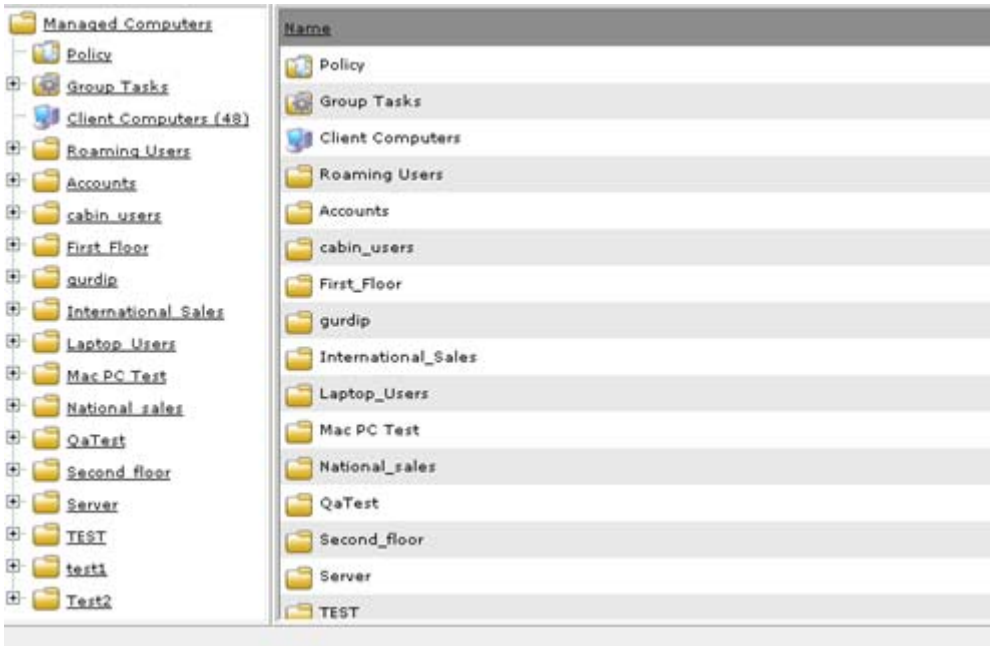
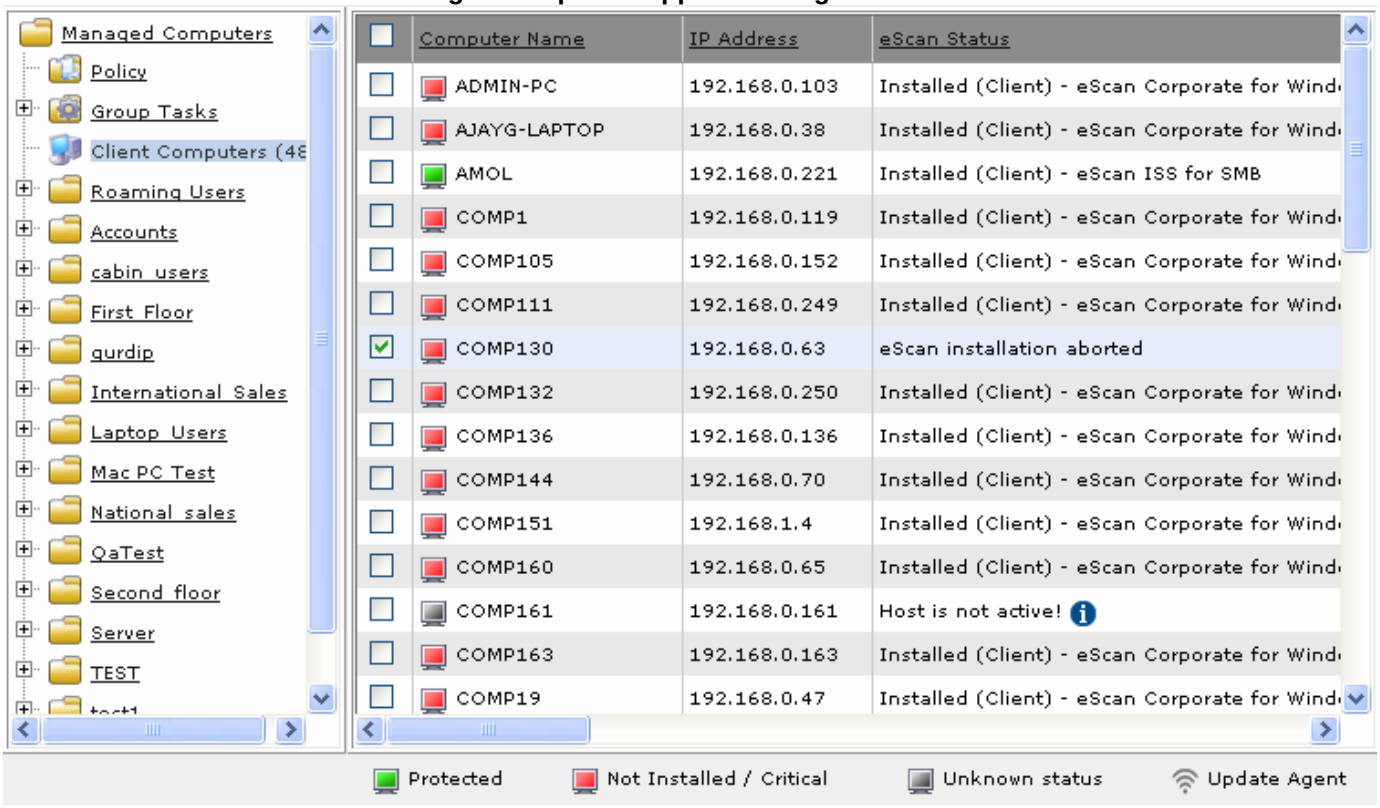


Figure 22

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

On the left pane, under the appropriate managed computers folder, click Client Computers**.**
The list of all managed computers appears on right side of the screen. Refer



2. Figure 23.

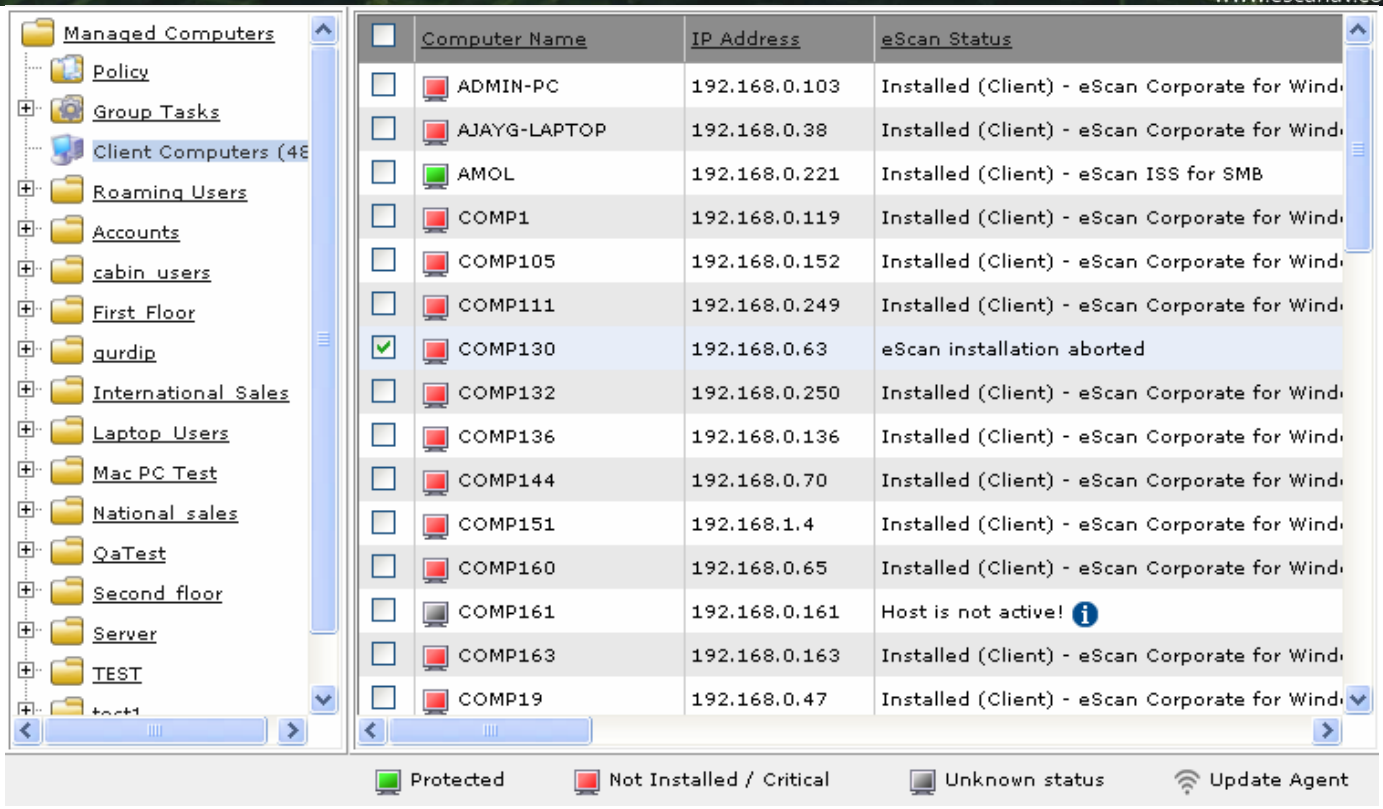


Figure 23

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box for which you want to view properties.

The **Properties** menu and **Refresh Client** button is available, only when you select the appropriate computer name check box from the list.

Click the Client Action List **drop-down menu, and then click** Properties**.**
The Properties **window appears. Refer**

4. Figure 24.

Properties Help

COMP111	
General	
Computer Name	COMP111
IP Address	192.168.0.249
User name	Administrator
Operating System	Windows XP
AV-Status	
Anti-Virus Installed	Installed (Client) - eScan Corporate for Windows
Version	11.0.1139.1239
Installed Directory	C:\Program Files\eScan
Update Server	qa30
Last Update	2013/03/28 07:43
Protection	
File Anti-Virus	Enabled
Mail Anti-Virus	Disabled
Anti-Spam	Enabled
Web Protection	Enabled
Firewall	Enabled (Limited Filter)
Endpoint Security	Enabled

Close

Figure 24

5. View the following details as required:

The status N/A appears incase if eScan is not installed on selected computer and when the selected host details are not available on eScan server.

Field	Description
General	
This section provides you the following basic details: • Computer Name • IP Address • User name • Operating System	
AV – Status	
Anti-Virus Installed	It indicates status whether eScan is installed or not, and also version name of eScan installed on the selected computer.
Version	It indicates version of eScan installed.
Installed Directory	It indicates installation path of eScan.
Update Server	It indicates IP address of the update server or internet address. In case, if the selected computer downloads the virus signature updates directly from the internet.
Last Update	It indicates the date when selected computer was last updated.
Protection	
This section provides you the status details of following eScan modules whether they are enabled or disabled on the client machine: • File Anti-Virus • Mail Anti-Virus • Anti-Spam • Web Protection • Firewall • Endpoint Security	

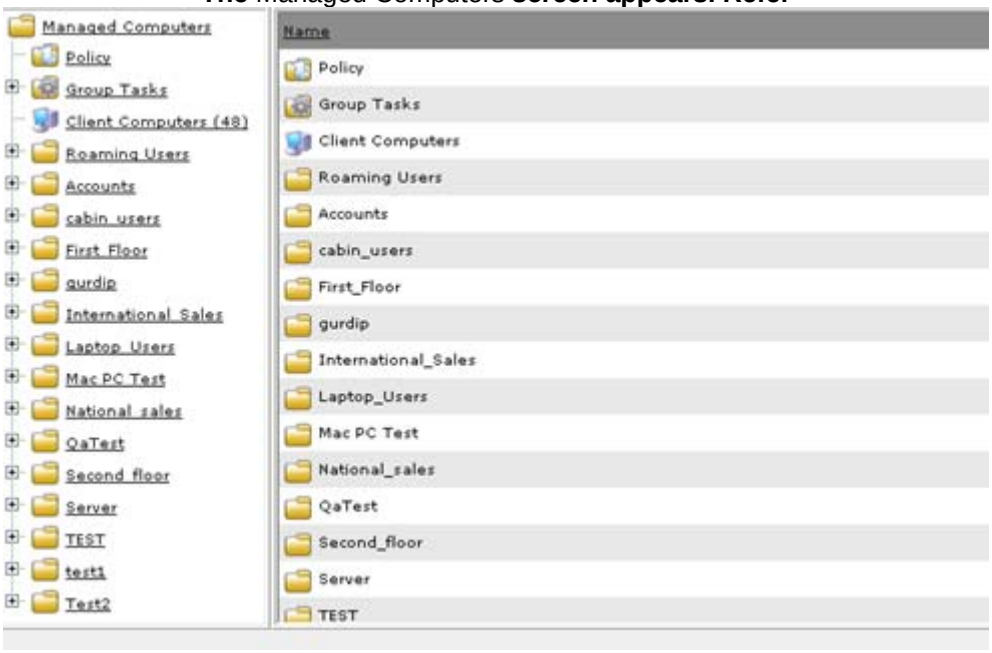
Deploying Hotfix

It enables you to deploy hotfix on the client machine.

> The **Deploy Hotfix** option is available only when you download it on the eScan server from the **eScan Protection Center**, by clicking the **Download Latest Hotfix** link, under **Tools** module.

To deploy hotfix

On the navigation pane, click Managed Computers**.**
The Managed Computers **screen appears. Refer**



1. Figure 25.

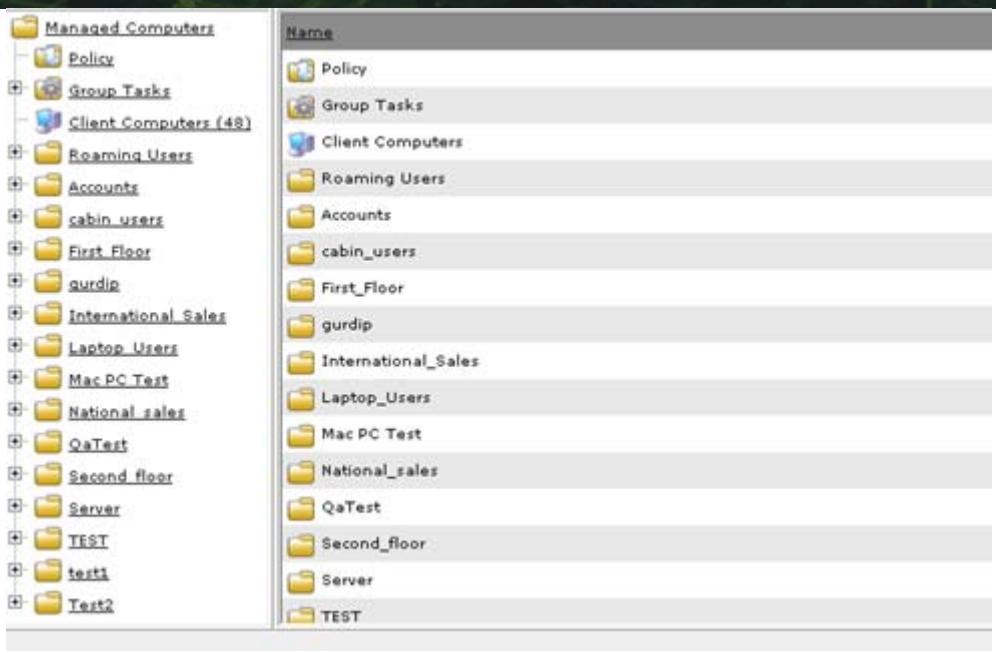
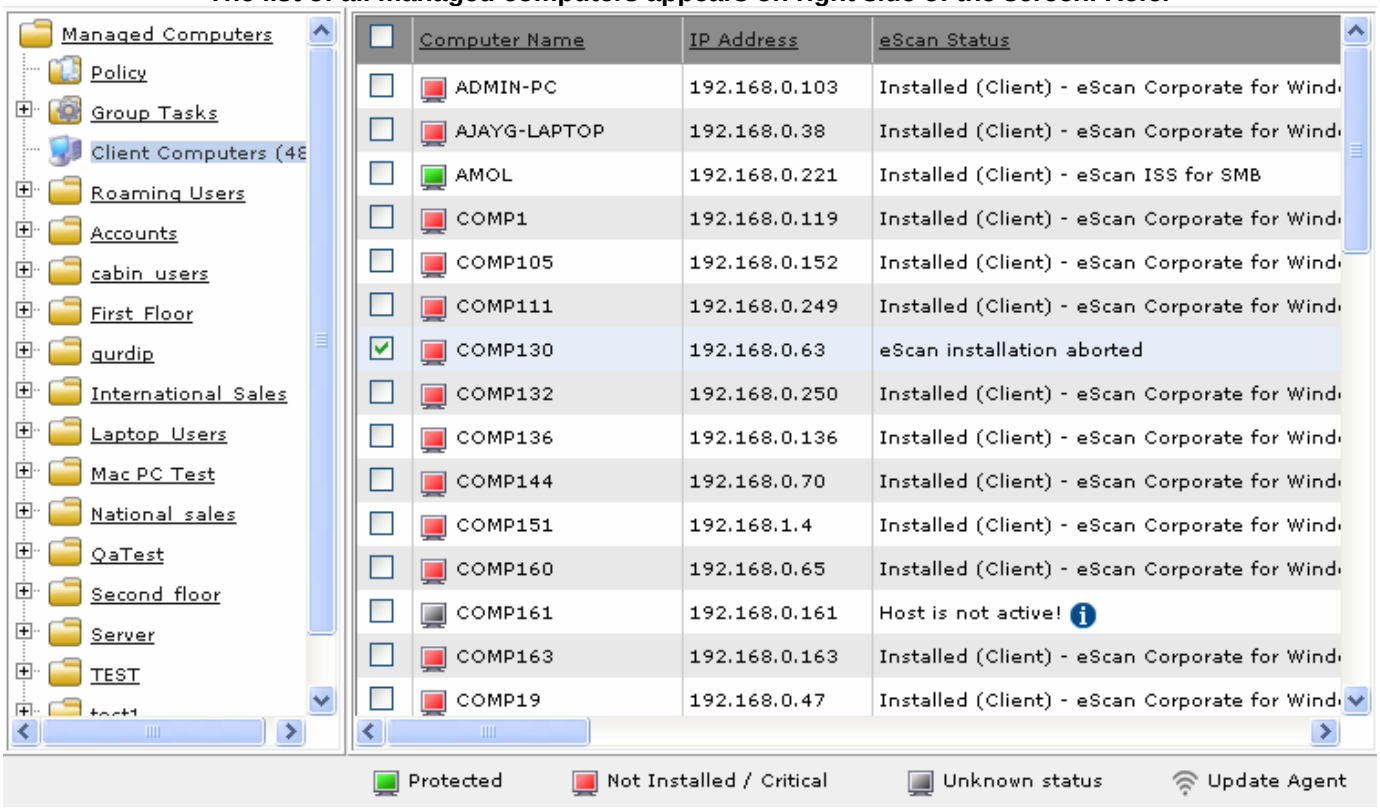

Managed Computers
Policy
Group Tasks
Client Computers (48)
Roaming Users
Accounts
cabin_users
First_Floor
gurdip
International_Sales
Laptop_Users
Mac PC Test
National_sales
QaTest
Second_floor
Server
TEST
test1
Test2
Name
Policy
Group Tasks
Client Computers
Roaming Users
Accounts
cabin_users
First_Floor
gurdip
International_Sales
Laptop_Users
Mac PC Test
National_sales
QaTest
Second_floor
Server
TEST

Figure 25

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

On the left pane, under the appropriate managed computers folder, click Client Computers**.**
The list of all managed computers appears on right side of the screen. Refer



2. Figure 26.

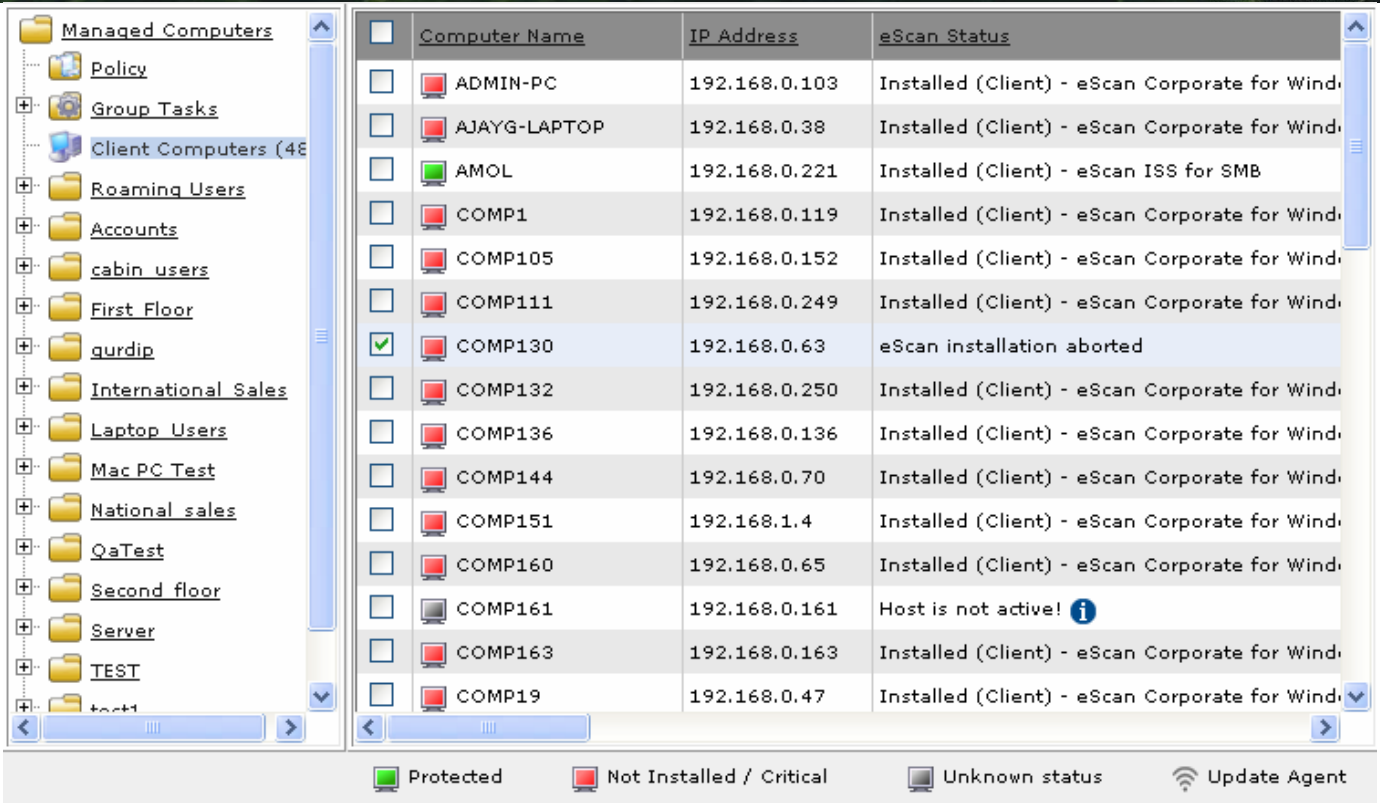


Figure 26

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box for which you want to deploy hotfix.

The **Deploy Hotfix** menu and **Refresh Client** button is available, only when you select the appropriate computer name check box from the list.

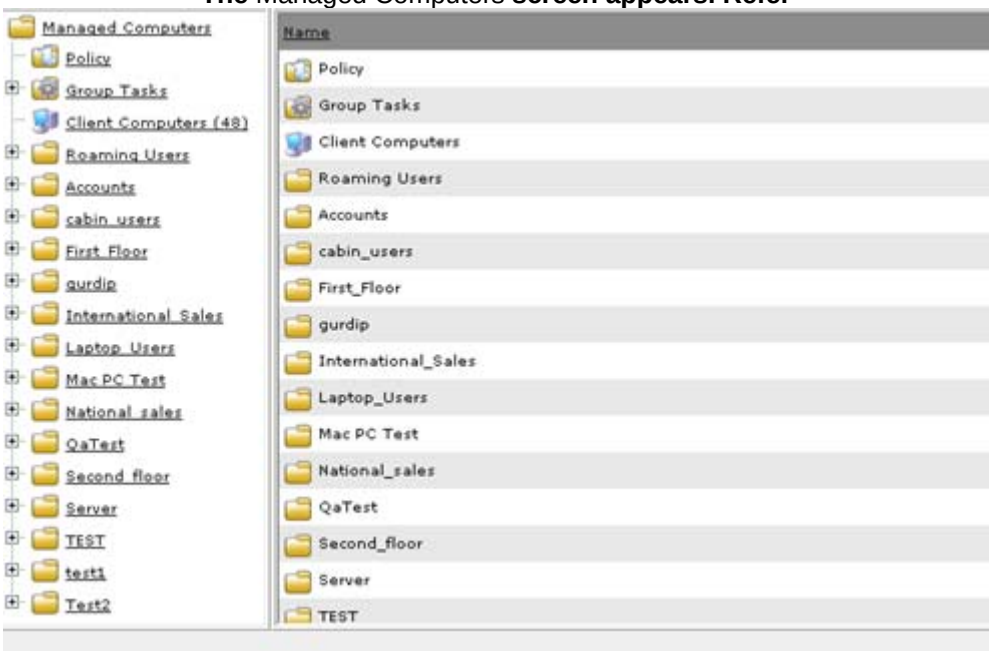
4. Click the **Client Action List** drop-down menu, and then click **Deploy Hotfix**.
   The **Client Installation** window appears and hotfix gets deployed.

Moving Computers to Group

It enables you to move computers to a managed computer group or any of its sub-groups.

To move computers to group

On the navigation pane, click Managed Computers**.**
The Managed Computers **screen appears. Refer**



1. Figure 27.

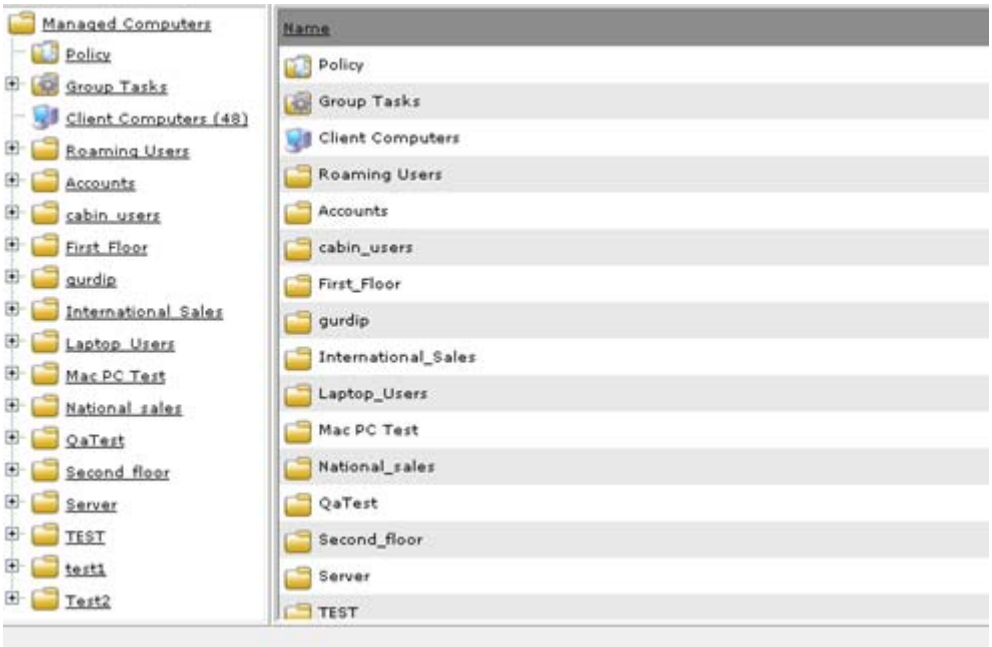
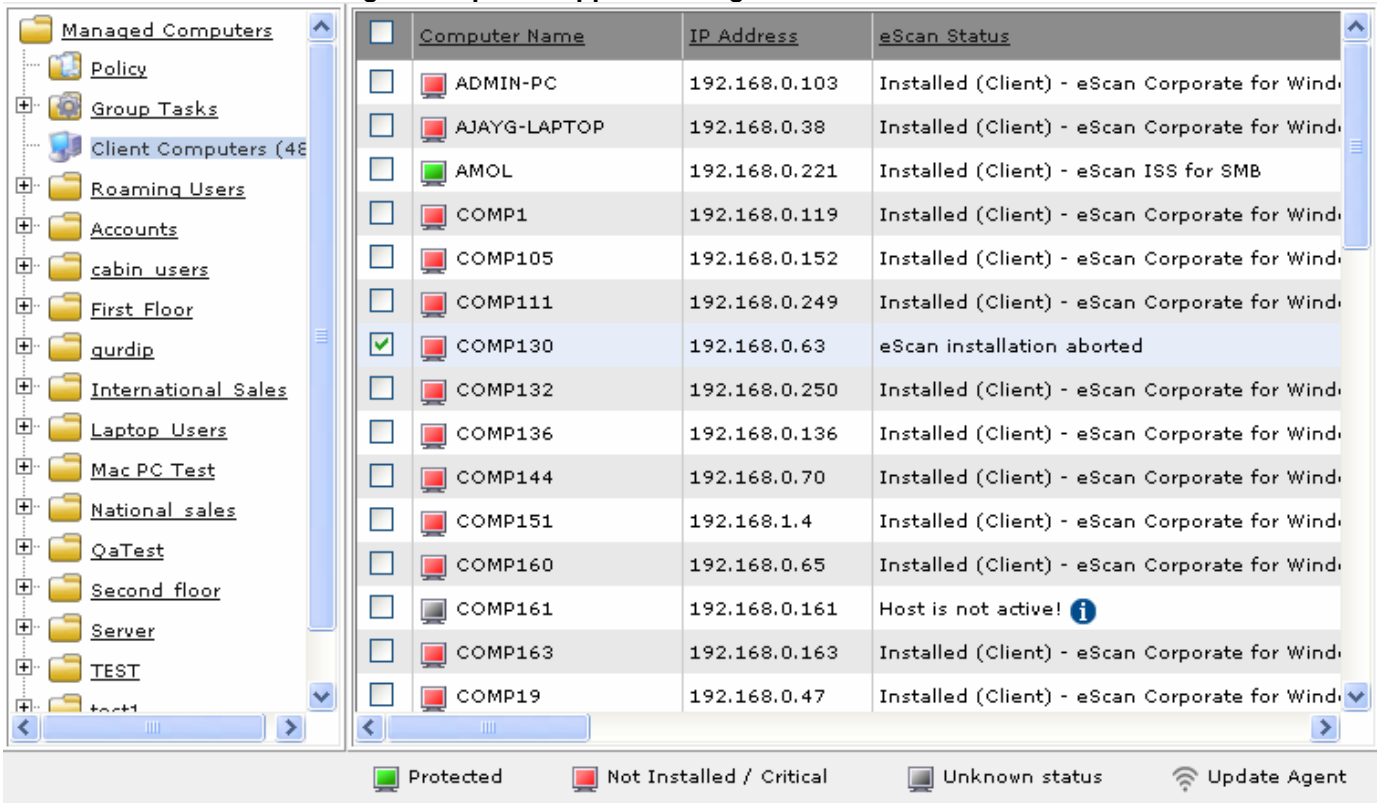


Figure 27

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

On the left pane, under an appropriate managed computers folder, click Client Computers**. The list of all managed computers appears on right side of the screen. Refer**



2. Figure 28.

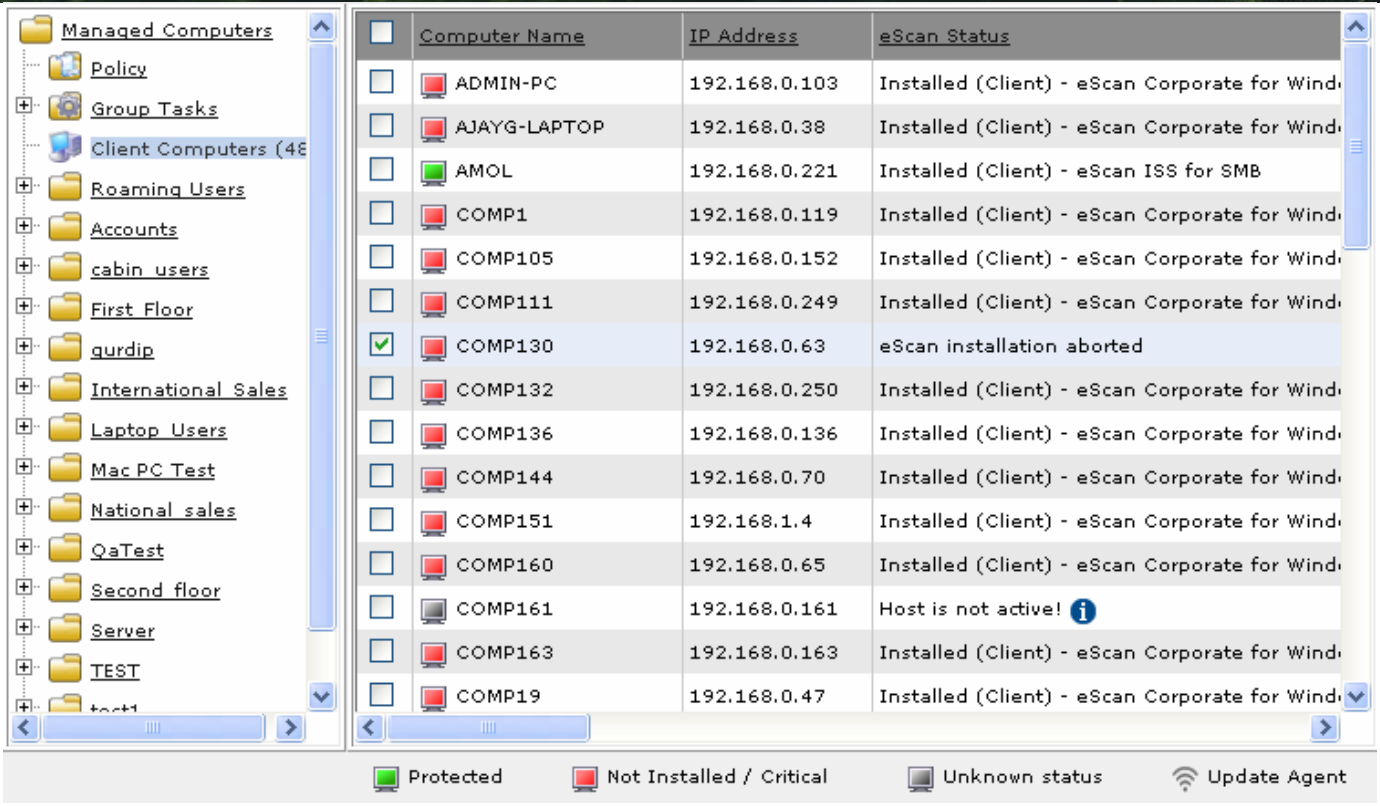


Figure 28

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box that you want to move to group.

The **Move to Group** menu and **Refresh Client** button is available, only when you select the appropriate computer name check box from the list.

Click the Client Action List **drop-down menu, and then click** Move to Group**.**
The Select Group **window appears. Refer**

4. Figure 29.

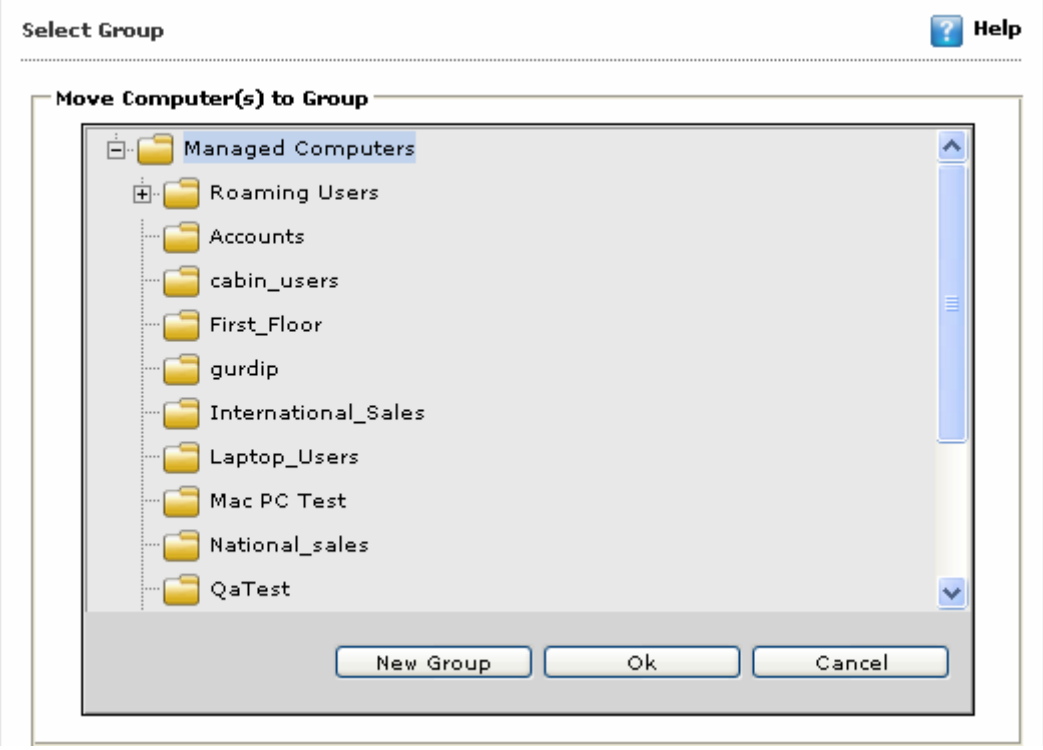


Figure 29

5. Under **Move Computer(s) to Group** section, click the group in which you want to move, and then click **Ok** button.
6. If you want to create new group, click **New Group** button, and then specify name to a group. You can either create a New Group under Managed computers or any of its sub-groups.

Refreshing Clients

In case, if you have made any kind of changes on the Managed Computers screen, you can refresh the details by clicking the **Refresh Client** button.

The Refresh Client button is available, only when you select the appropriate computer name check box from the list.

To refresh client

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 30.

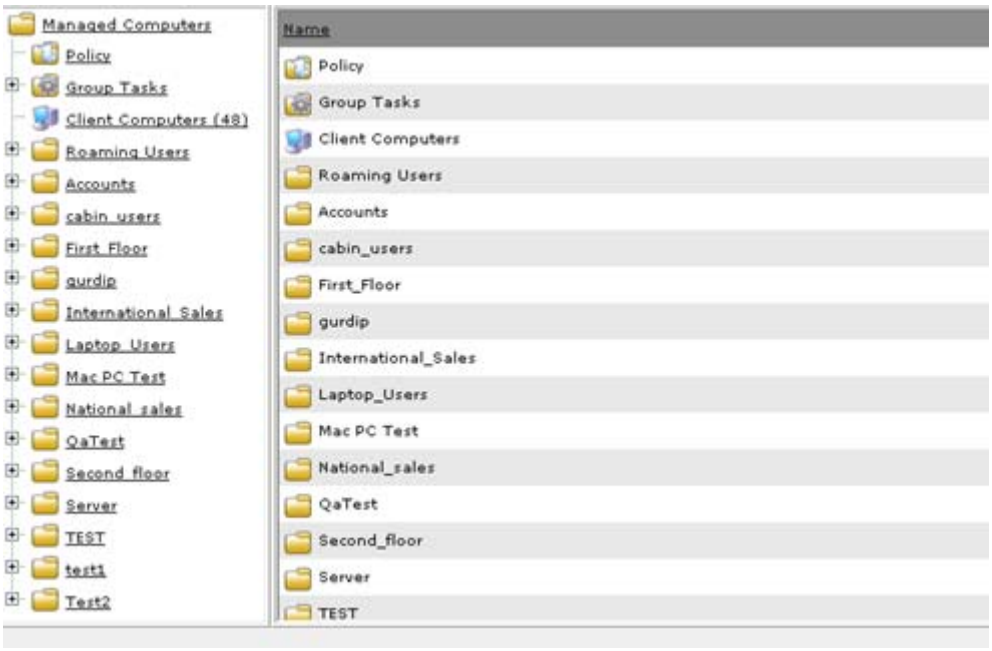


Figure 30

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

2. On the left pane, under the appropriate managed computers folder, click **Client Computers**.
   The list of all managed computers appears on right side of the screen. Refer Figure 31.

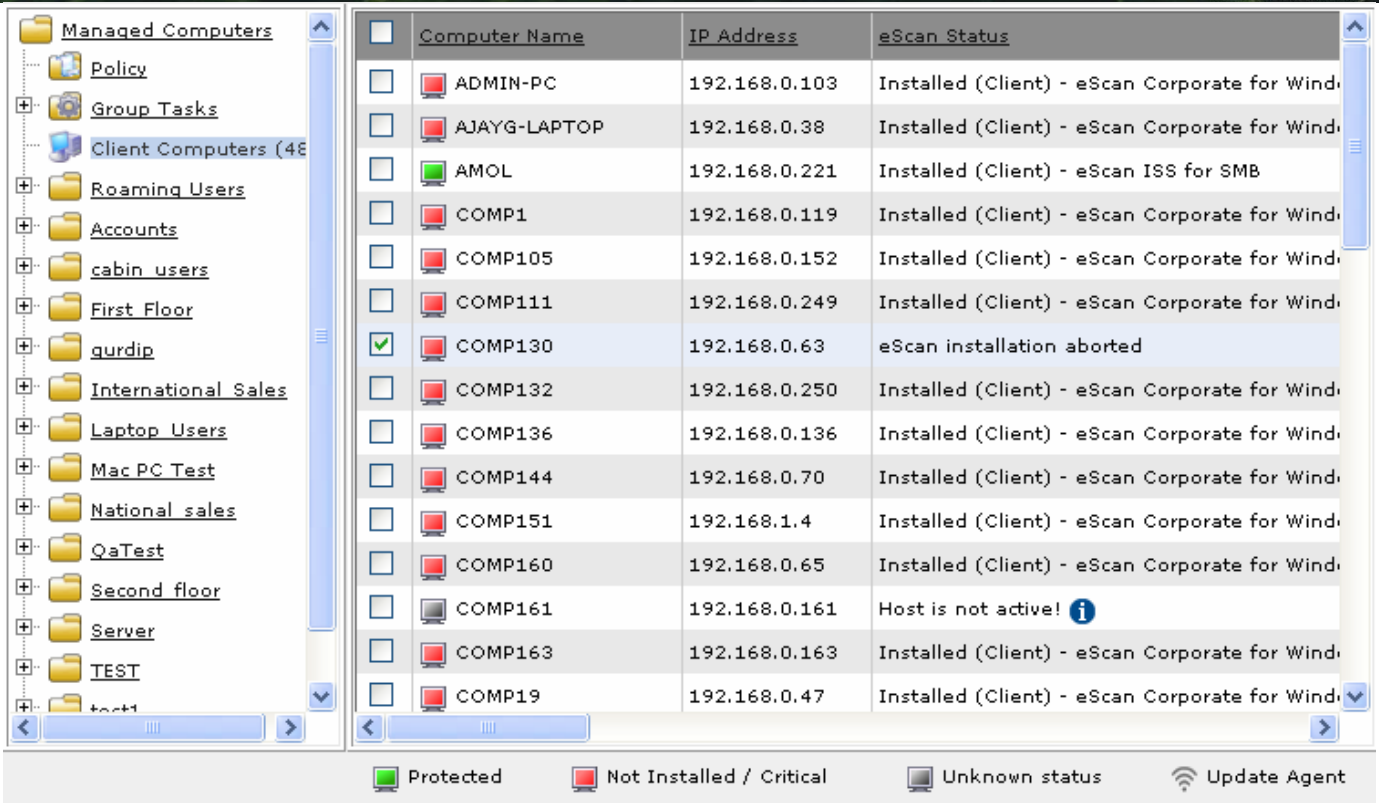


Figure 31

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box, and then click **Refresh Client** button, to refresh all details of the selected client.
   The details in the table gets refresh.

Managing Computer Groups

System administrators often need to perform the same set of tasks on different computers. These tasks may involve deploying policies; installing hotfixes and updates; and installing software. eScan helps you simplify management tasks by allowing you to create groups of computers.

- Creating New Group
- Remove a Host Computer from the Group
- Deleting a Computer Group
- Viewing the properties of a group
- Setting the Group Configuration
- Creating Groups and Tasks
- Installing and Uninstalling Applications

Creating New Group

Suppose you are a system administrator of a network that has 50 computers, out of which 25 belong to the Marketing department, 5 belong to the Accounts department, 15 belong to the Sales department, and the remaining belong to Administration department. In this case, each department has its own set of software requirements. For example, the Accounts department will rely heavily on accounting software. Now, if you need to manage each of the computers in the Accounts department the task will become difficult. If the number of computers in each department increases, the task of managing each computer separately will become very difficult.

In such cases, the eScan Web Console provides you with the facility to create computer groups that allows you to group together computers on which you want to perform the same administrative tasks.

It enables you to create new group and sub-group for maintaining policies and tasks of various clients.

To create new group

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 32.

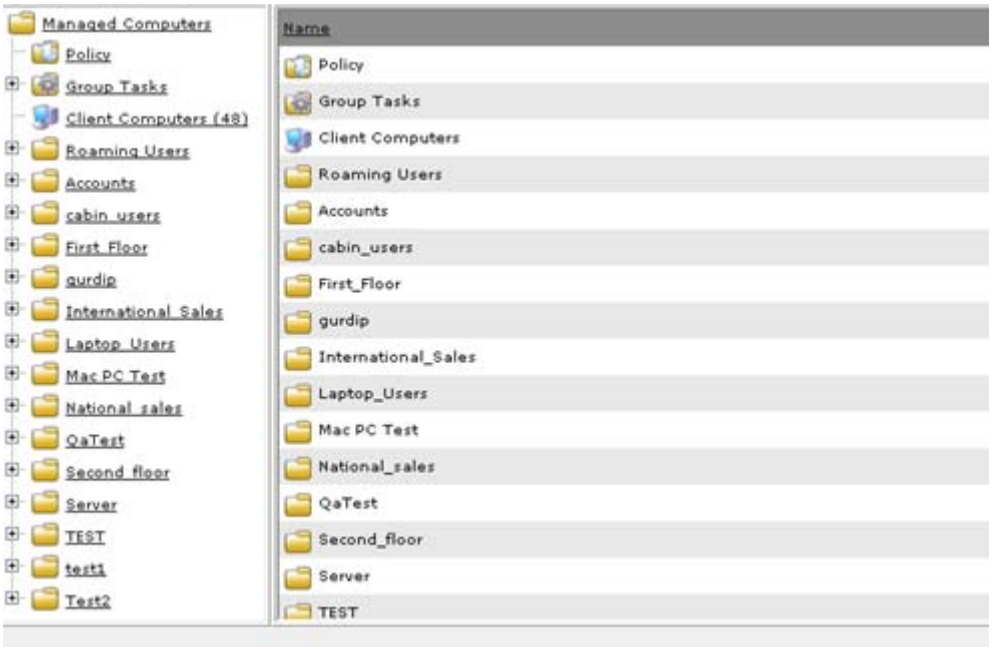


Figure 32

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

2. Click the **Action List** drop-down menu, and then click **New Group**.
   The **Creating New Group** window appears. Refer Figure 33.

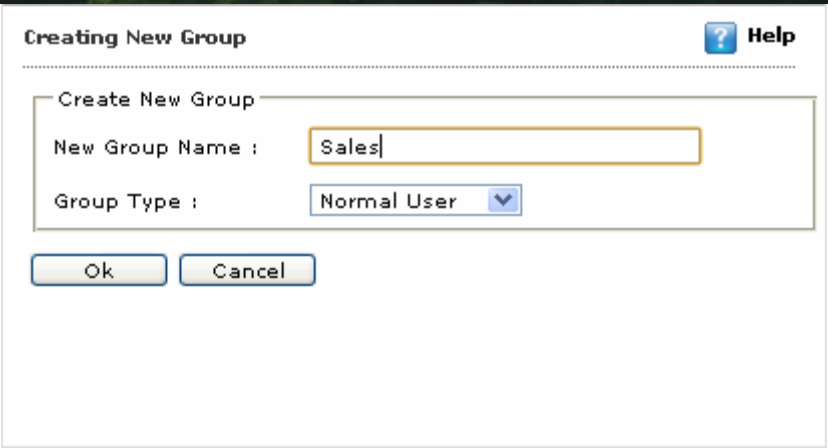


Figure 33

3. Type group name in the **New Group Name** field.
4. Select an appropriate type of group from the **Group Type** drop-down list.
5. Click the **Ok** button.
   The group gets created.
6. If you want to create sub-group under any group, perform the following steps:
   1.1 On the left pane, click an appropriate managed group folder.
   2.1 Click the Action List drop-down menu, and then click New Sub Group.
   The Creating New Group window appears.
   3.1 Type group name in the **New Group Name** field.
   4.1 Select an appropriate type of group from the **Group Type** drop-down list.
   5.1 Click the **Ok** button.
   The sub-group gets created.

Remove a Host Computer from the Group

Sometimes, as a result of changes within the organization or due to the shuffling of computers in a network, you may need to remove a computer from a group.

For this, you must visit the **Client Computers** node of the group in the console tree, and then click the **Remove from group** option on the **Client Action List** menu.

The steps to remove a computer are as follows:

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears.
2. On the left pane, under an appropriate managed computers folder, and then click **Client Computers** folder.
   The list of computer appears on right side of the screen. Refer Figure 34.

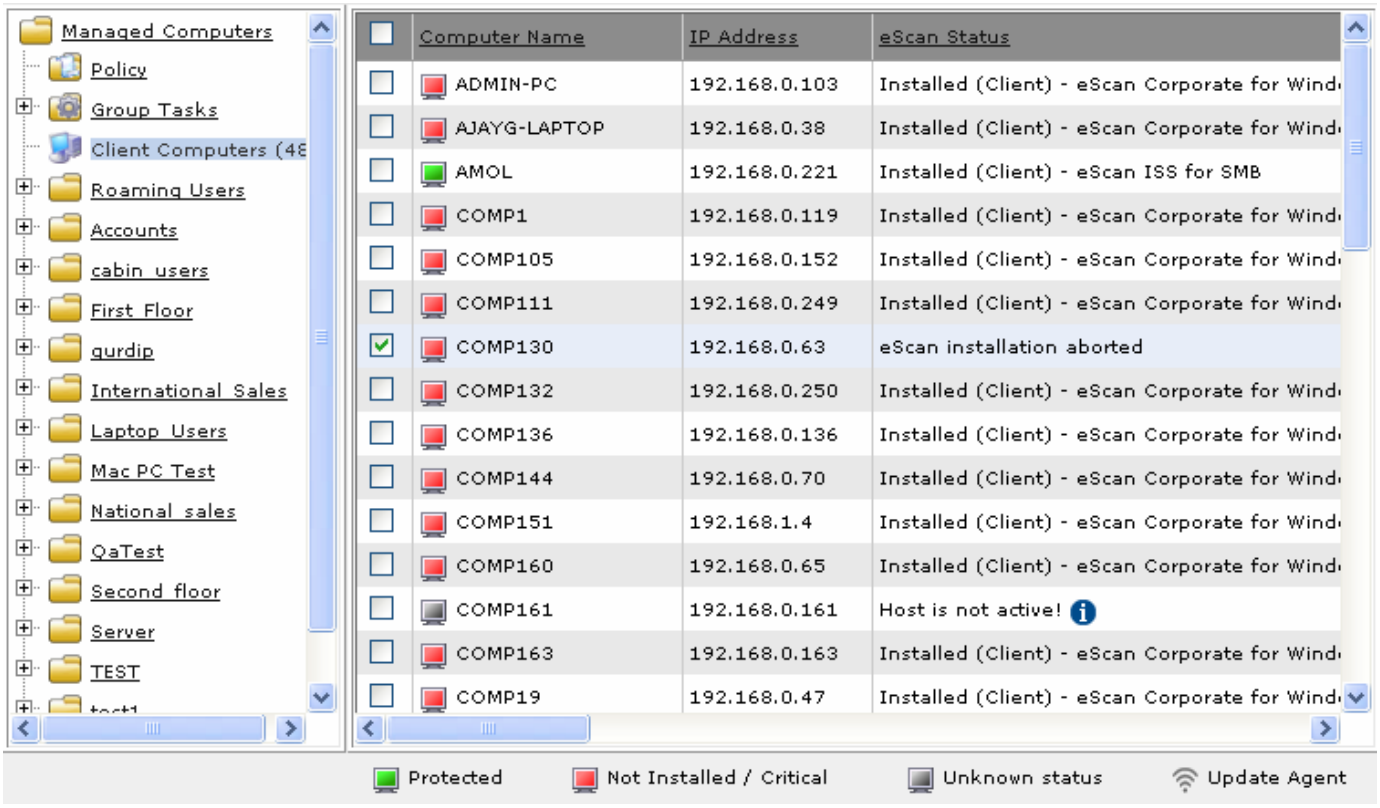


Figure 34

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box, which you want to remove from the group.
4. Click the **Client Action List** drop-down menu, and then click **Remove from Group**.
   The following window appears. Refer Figure 35.

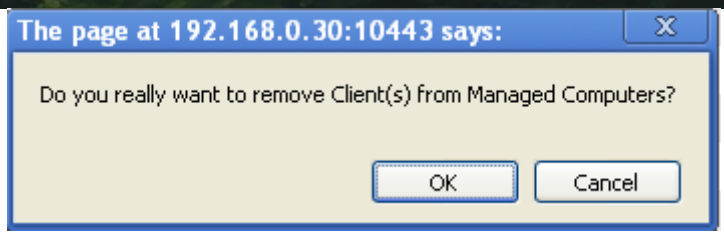


Figure 35

5. Click the **OK** button.
   The client gets deleted from the list.

Deleting a Computer Group

At times, you may need to remove an entire computer group. In such cases, you need to use select the group in the console tree and then use the **Delete** menu item in the **Action List** menu to remove the node.

The steps to delete a computer group are as follows:

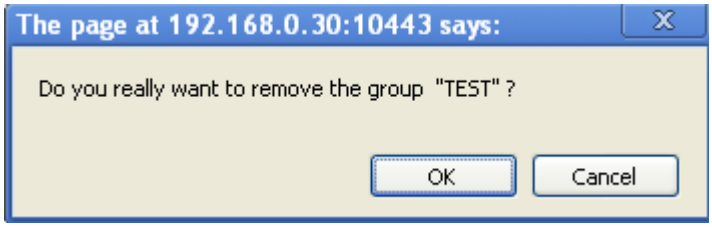
1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 32.
2. On the left pane, click an appropriate group that you want to remove.
3. Click the **Action List** drop-down menu, and then click **Remove Group**.
   The following window appears. Refer Figure 36.
4. 

Figure 36

5. Click the **OK** button.
   The group gets deleted from the list.

Viewing the Properties of a Group

The properties enable you to create update agent which plays an important role in providing latest updates to its clients. You can do the following activities:

Update Agent concept is taken from eScan child servers. You can simply install eScan as client in all branch systems. And from EMC you can choose which machine or system can act as Update agent. Once you set the system as Update Agent it will act like Update server for other Clients in the branch. Update Agent will download the updates from the Primary server and will distribute it to branch clients. This saves your bandwidth as well as an effort of making other client servers if one goes down. You can set as many Update Agents as you want.

Viewing General Properties

It enables you to view the general properties of the managed computers groups and sub-groups.

To view general properties

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 37.

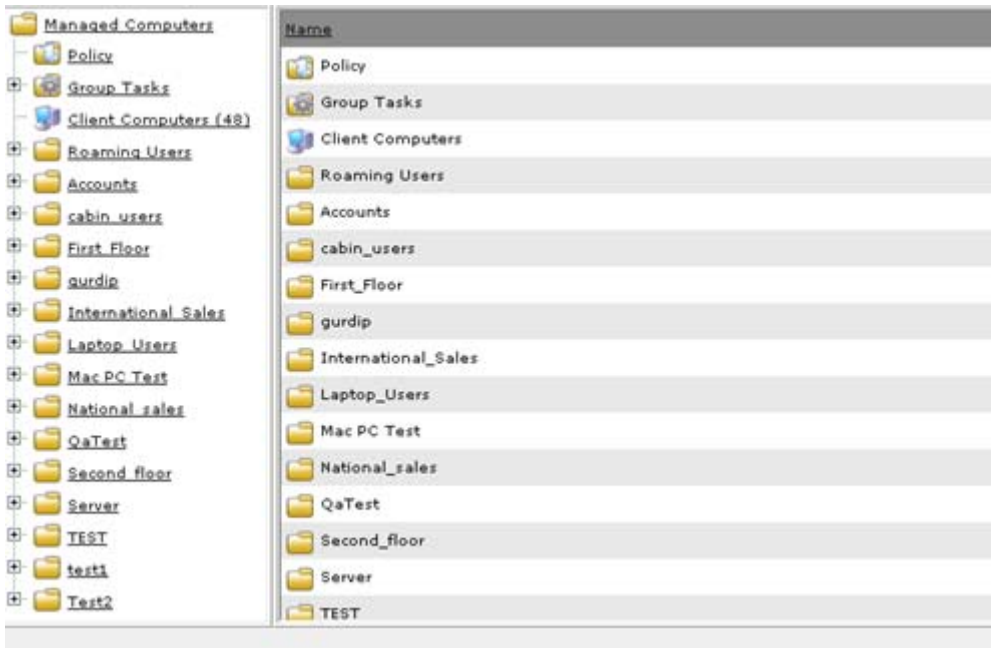


Figure 37

Click the (+) sign to expand the folder and view the sub-folders and click the (-) sign to collapse the required folder.

2. On the left pane, under an appropriate managed computers folder, click an appropriate managed computer sub-folder for which you want to view properties.

Click the Action List **drop-down menu, and then click** Properties**.**
The Properties (X) **window appears. For example, X as name of the managed computers sub-folder. Refer**

3. Figure 38.

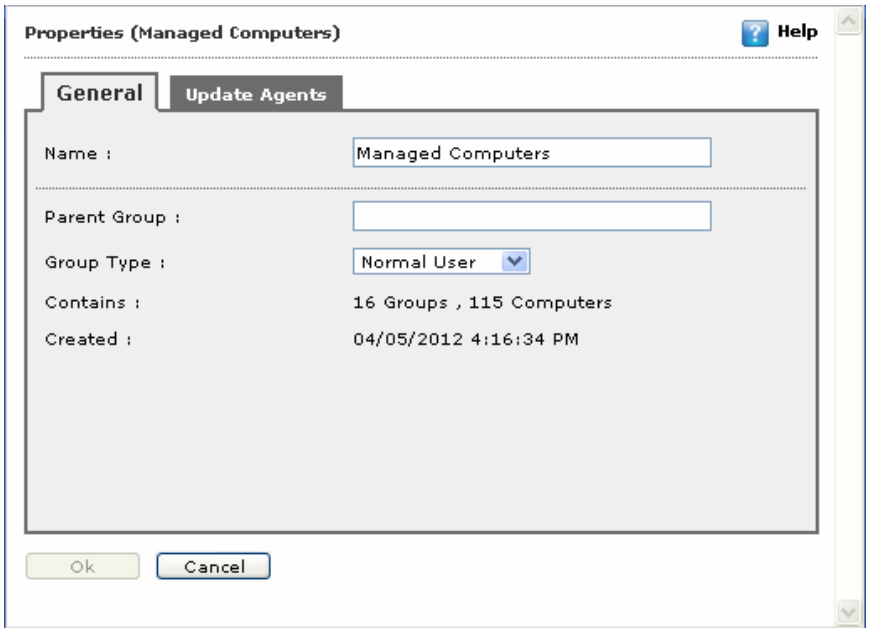


Figure 38

Click the General **tab.**
The General **tab appears. Refer**

4. Figure 38.
5. View the following field details as required.

Field	Description
Name	It indicates the name of managed computer sub-folder.
Parent Group	It indicates the name of parent managed computer folder.
Group Type	It indicates the type of group. For example, normal or roaming user.
Contains	It indicates the total number of groups and computers. For example, 4 groups, 19 computers.
Created	It indicates the date and time when managed computer group is created.

Creating Update Agent

An update agent plays an important role in providing latest updates to its clients. The clients can take updates from an update agent instead of from the main server. It enables you to create update agent for managed computer. You can create as many update agents as you want, herein one agent can act as a subsidiary to another agent. For example, Agent “B” can provide update in the absence of Agent “A”

To create update agent

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 39.

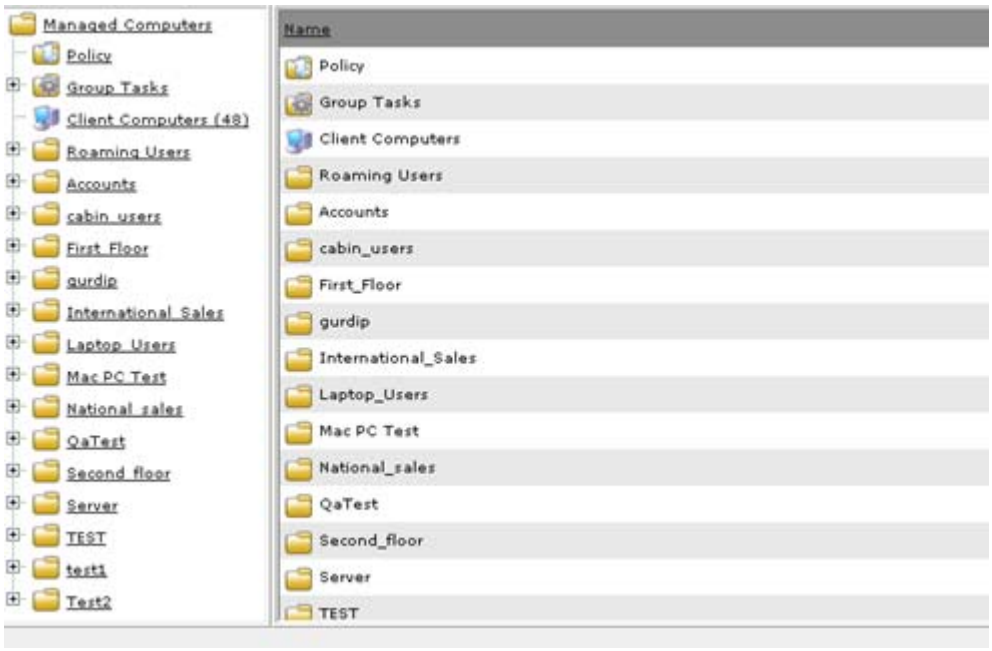


Figure 39

Click the (+) sign to expand the folder and view the sub-folders and click the (-) sign to collapse the required folder.

2. On the left pane, under an appropriate managed computers folder, click an appropriate managed computer sub-folder for which you want to create update agent.

Click the Action List **drop-down menu, and then click** Properties**.**
The Properties (a) **window appears. Refer**

3. Figure 40.

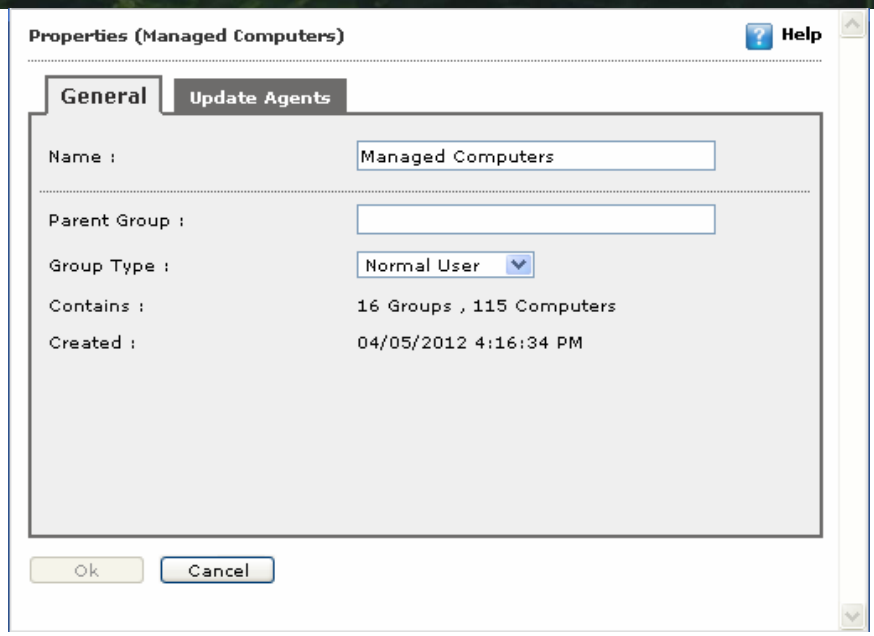


Figure 40

4. Click the **Update Agents** tab.
   The **Update Agents** tab appears. Refer Figure 41.

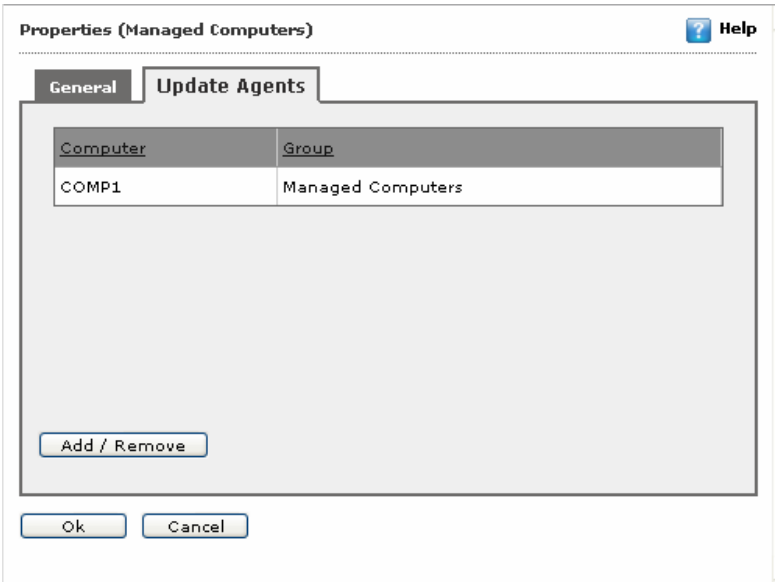


Figure 41

5. Click the **Add/Remove** button.
   A window appears displaying selected sub-group with its client machine. Refer Figure 42.

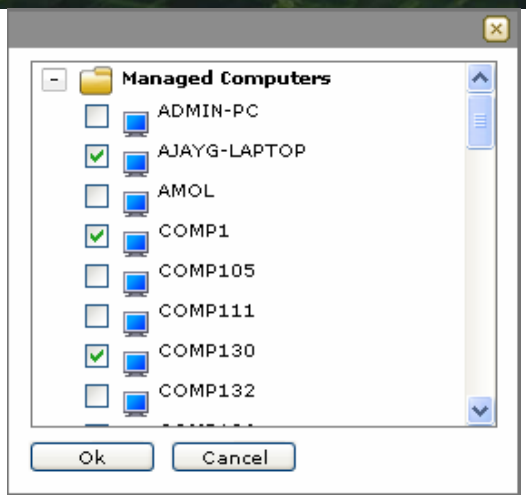


Figure 42

6. Select an appropriate client machine check box, and then click the **Ok** button.
   The selected client machine gets added to the list.

Removing Update Agent

It also enables you to remove the added update agent from managed computer sub-group.

To remove update agent

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 39.

Click the (+) sign to expand the folder and view the sub-folders and click the (-) sign to collapse the required folder.

2. On the left pane, under an appropriate managed computers folder, click an appropriate managed computer sub-folder for which you want to create update agent.

Click the Action List **drop-down menu, and then click** Properties**.**
The Properties (a) **window appears. Refer**

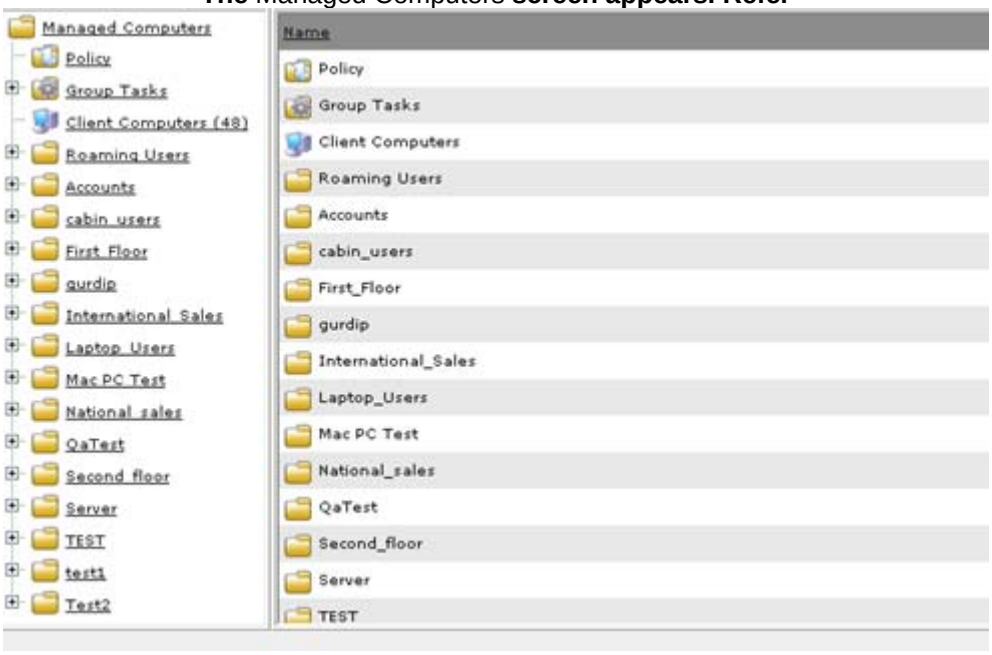
3. Figure 40.
4. Click the **Update Agents** tab.
   The **Update Agents** tab appears. Refer Figure 41.
5. Click the **Add/Remove** button.
   A window appears displaying selected sub-group with its client machine. Refer Figure 42.
6. Click to clear the selected client machine check box, and then click the **Ok** button.
   The selected client machine gets removed from the list.

Setting the Group Configuration

It enables you to set basic login information for the group.

To set group configuration

On the navigation pane, click Managed Computers**.**
The Managed Computers **screen appears. Refer**



1. Figure 43.

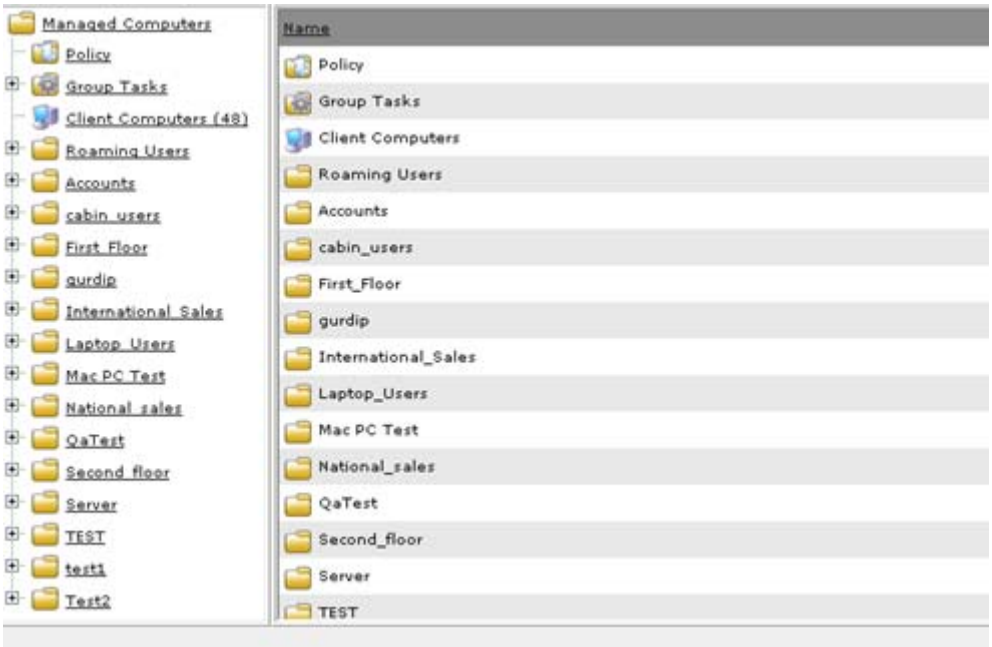


Figure 43

Click the Action List **drop-down menu, and then click** Set Group Configuration**.**
The Set Group Configuration **window appears. Refer**

2. Figure 44.

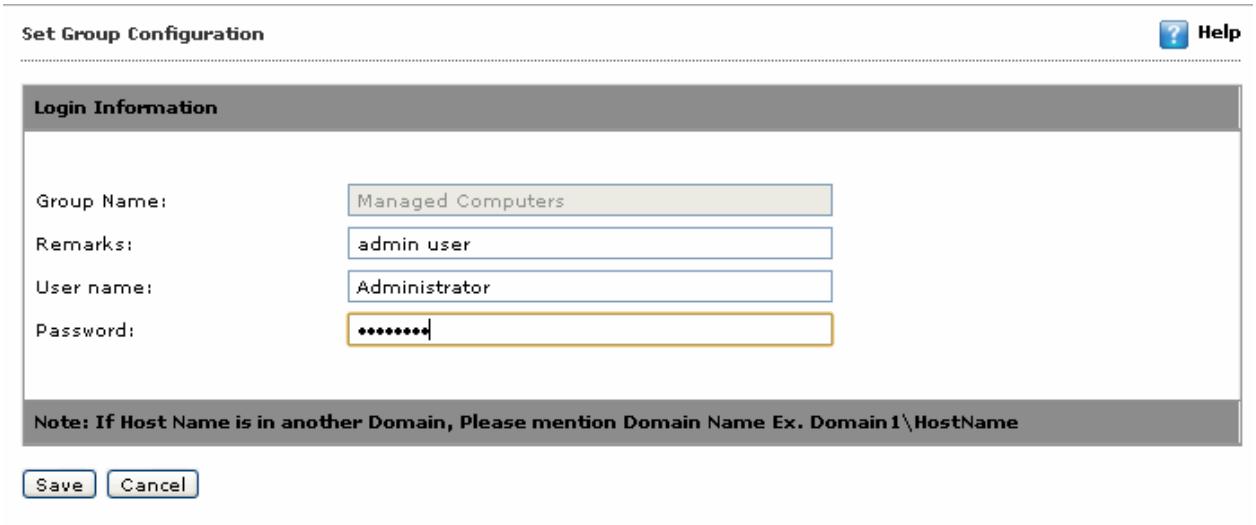


Figure 44

3. Specify the following field details.

Field	Description
Login Information	
Group Name	It displays the name of selected group. It appears dimmed.
Remarks	Type the remarks, if any.
User name	Type the login user name of selected group.
Password	Type the password of selected group.

4. Click the **Save** button.
The login information gets saved.

Creating Groups and Tasks

It enables you to create group structures and tasks based on the following two options:

- Creating Groups for Microsoft Windows Domains and Workgroups
- Creating Groups for Active Directory

Creating Groups for Microsoft Windows Domains and Workgroups

Perform the following steps to create group structure for Microsoft windows domains and workgroups:

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 45.

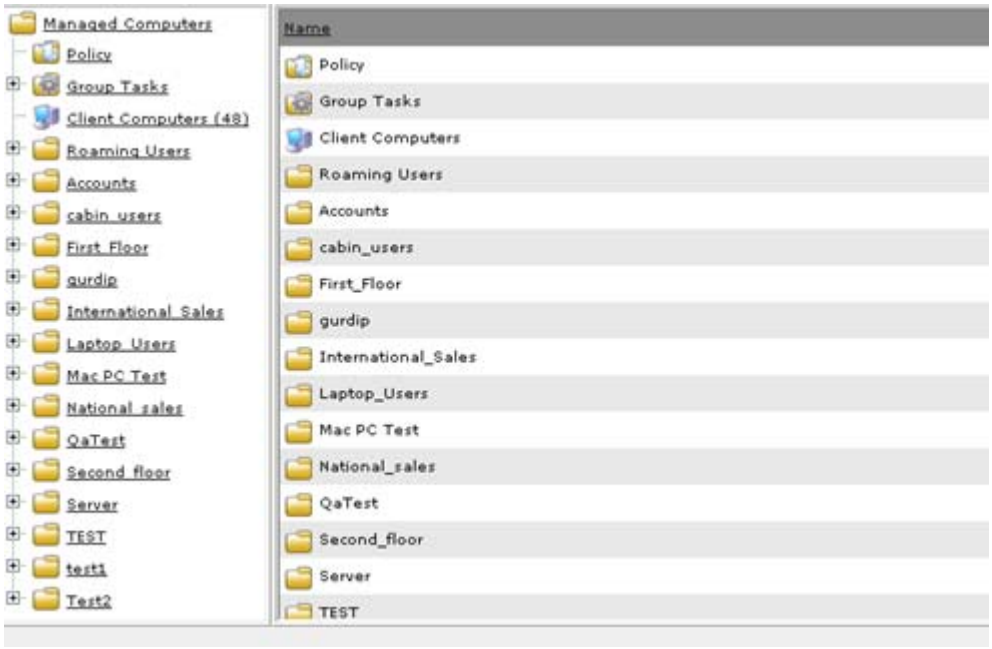


Figure 45

Click the Action List **drop-down menu, and then click** Create Groups and Tasks**.**
The Group Structure Wizard **window appears. Refer**

2. Figure 46.

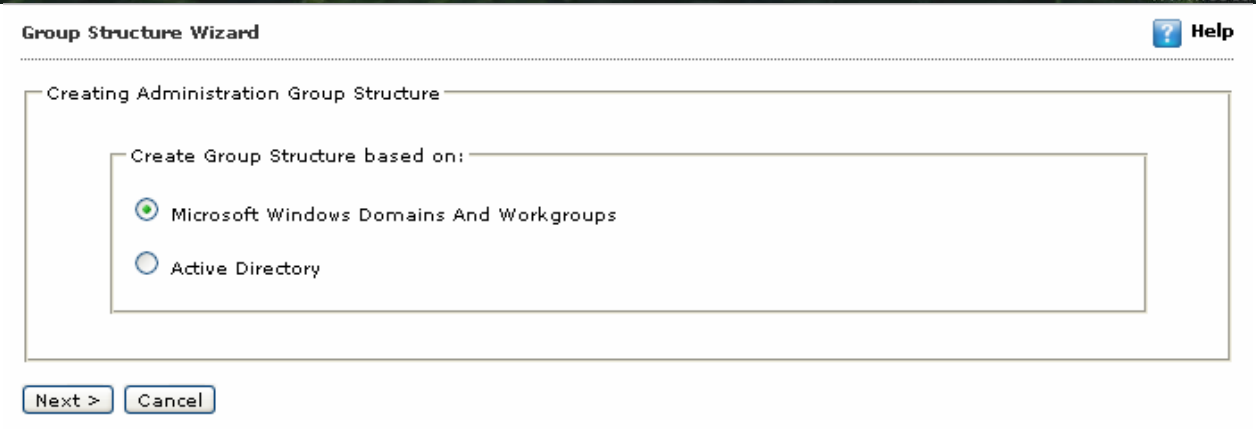


Figure 46

Under Create Group Structure based on **section, click the** Microsoft Windows Domains and Workgroups **option, and then click the** Next > **button.**
The following window appears. Refer

3. Figure 47.

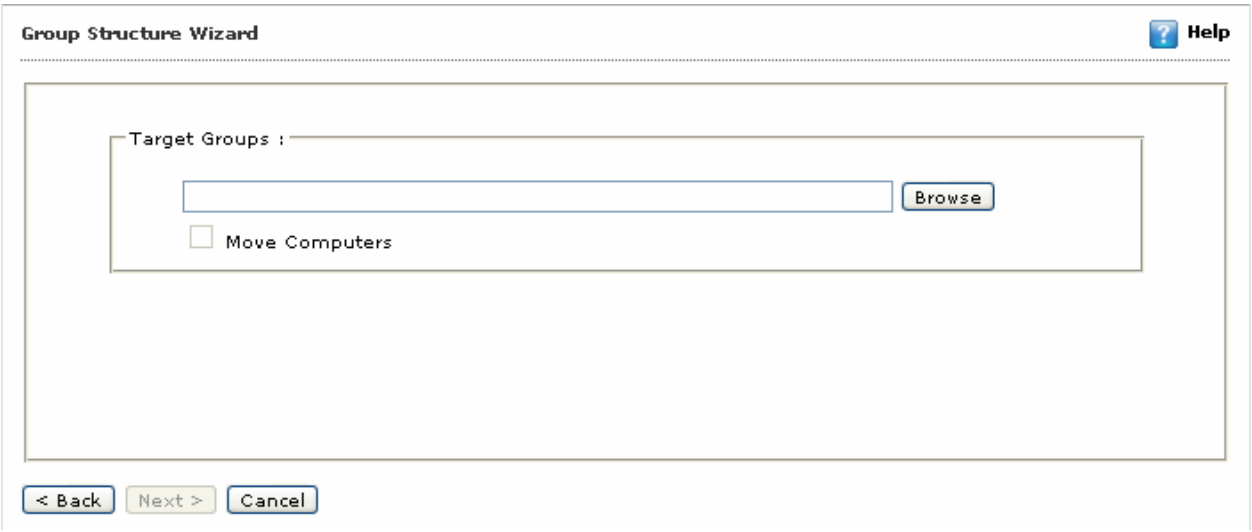


Figure 47

Under Target Groups section, click the Browse **button.**
The Select Group **window appears. Refer**

4. Figure 48.

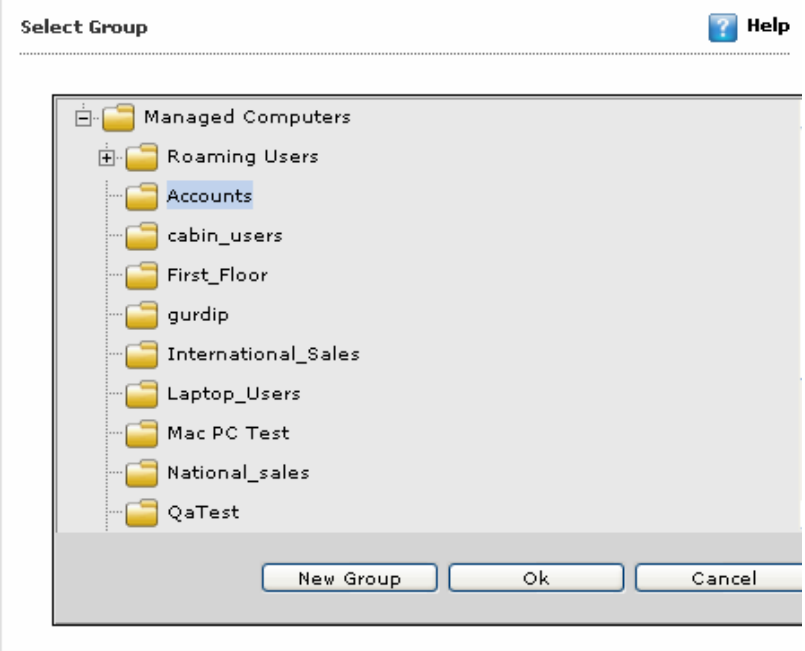


Figure 48

Click the (+) sign to expand the folder and view the options and click the (-) sign to collapse the required folder.

5. Click an appropriate group that you want to add, and then click **Ok** button.
6. If you want to create new group, click **New Group** button, and then specify name to a group. You can either create a New Group under Managed computers or any of its sub-groups.

The **Move Computers** check box is available only when you browse and select an appropriate group.

Select Move Computers **check box, if you want to move the computers to the selected group. Refer**

7. Figure 47.
8. Click the **Next >** button.
   A message of creating the group wizard appears.
9. Click the **Finish** button.

Creating Groups for Active Directory

Perform the following steps to create group structure for active directory:

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 45.
2. Click the **Action List** drop-down menu, and then click **Create Groups and Tasks**.
   The **Group Structure Wizard** window appears. Refer Figure 49.

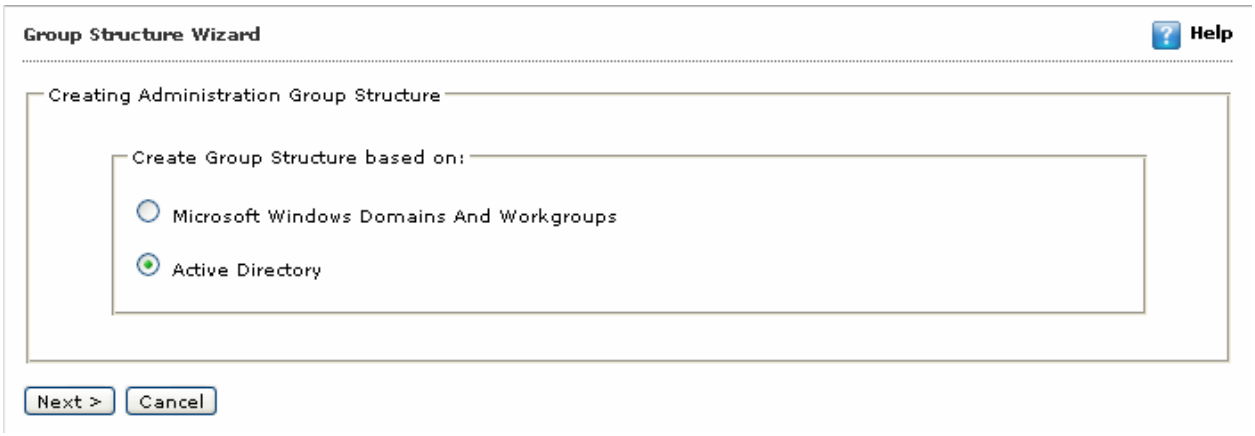


Figure 49

3. Under **Create Group Structure** based on section, click the **Active Directory** option, and then click the **Next >** button.
   The following window appears. Refer Figure 50.
4.

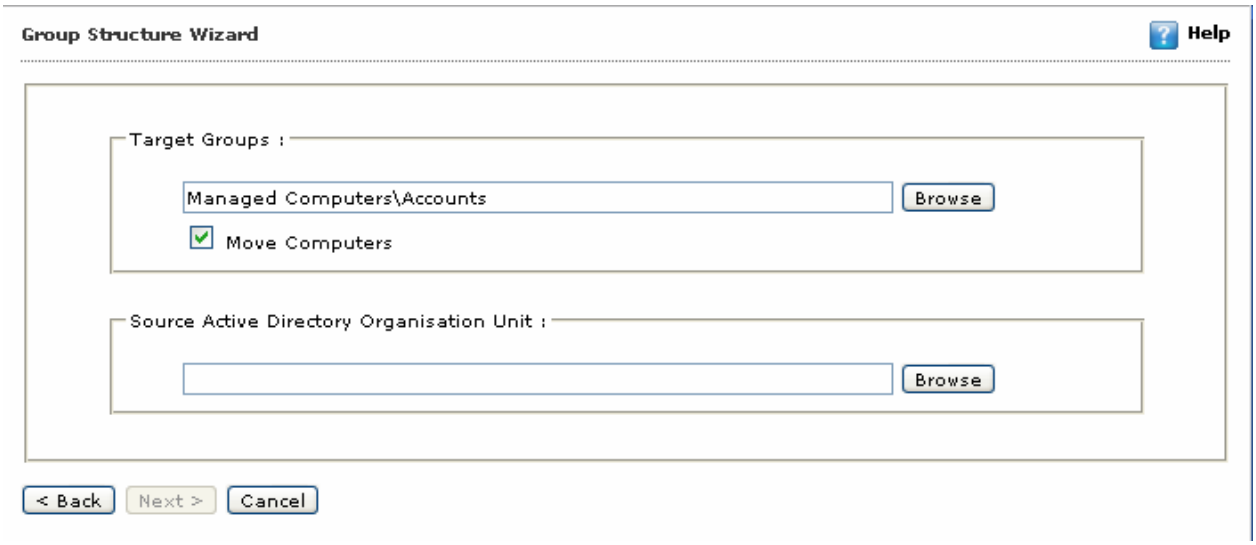
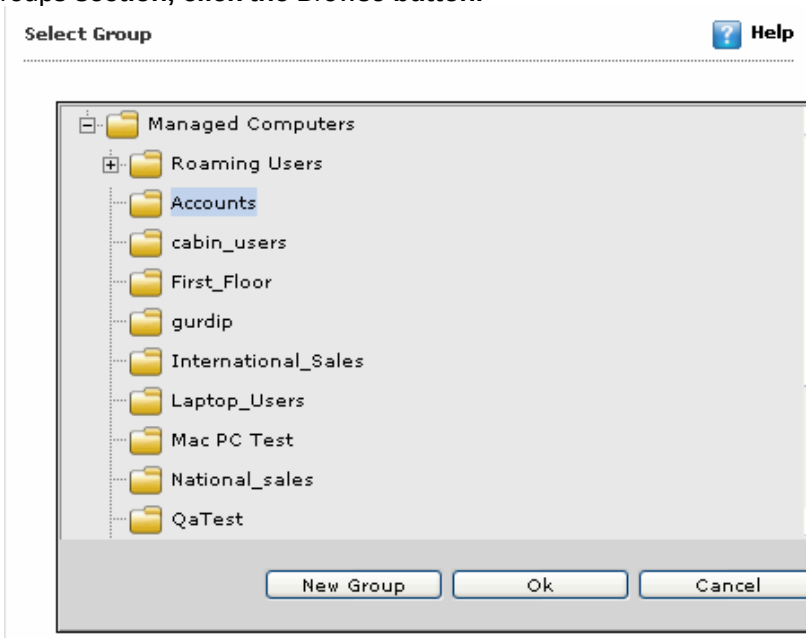


Figure 50

Under Target Groups **section, click the** Browse **button.**



The Select Group **window appears. Refer**

5. Figure 51.

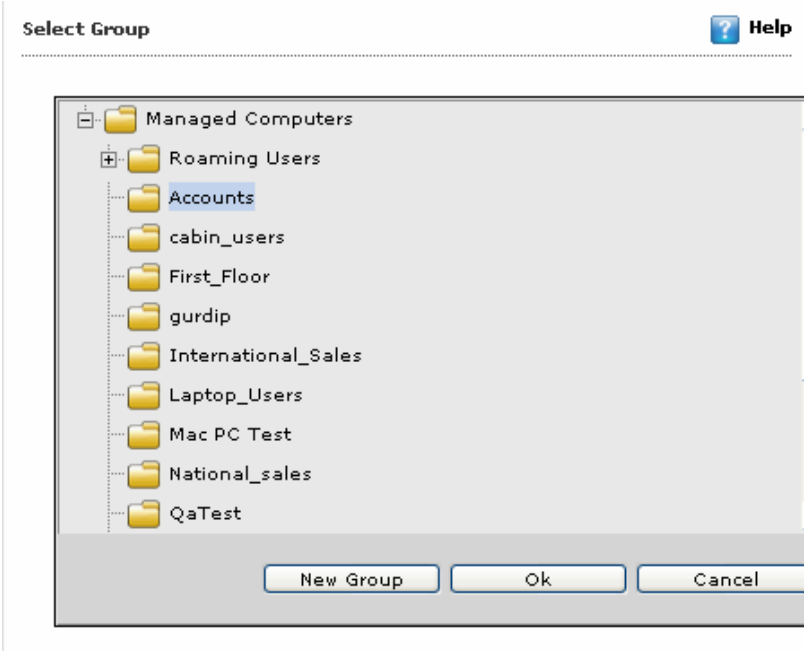


Figure 51

Click the (+) sign to expand the folder and view the options and click the (-) sign to collapse the required folder.

6. Click an appropriate group that you want to add, and then click **Ok** button.
   The selected group path appears in the **Browse** field. Refer Figure 50.
7. If you want to create new group, click **New Group** button, and then specify name to a group. You can either create a New Group under Managed computers or any of its sub-groups.

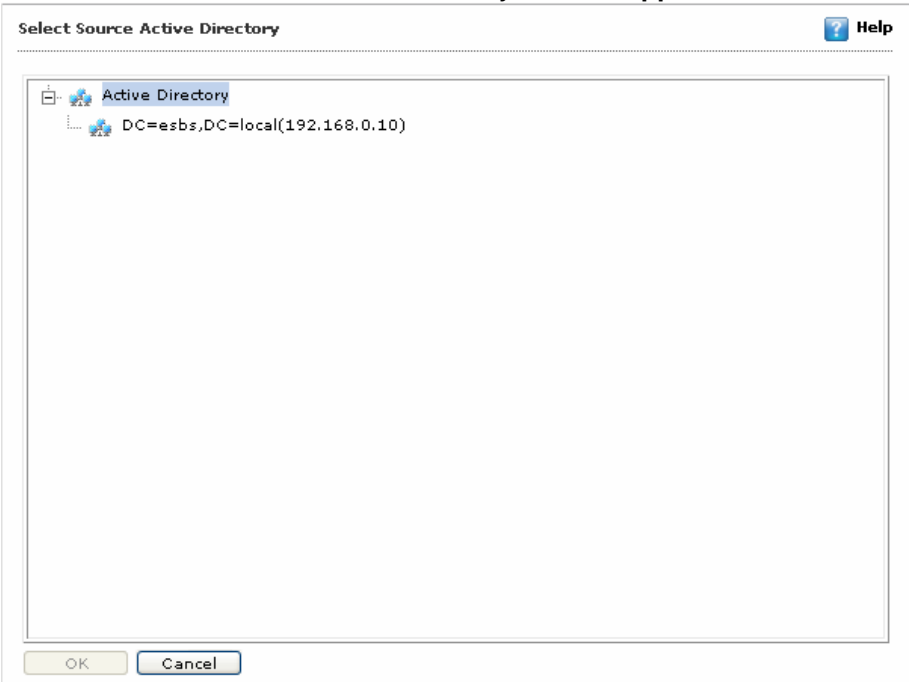
The **Move Computers** check box is available only when you browse and select an appropriate computer.

8. Select **Move Computers** check box, if you want to move computers to the selected group.

The **Next >** button is available only when you select path from both **Target Groups** and **Source Active Directory Organisation Unit** sections.

9. Under Source Active Directory Organization Unit section, click the Browse button.

The Select Source Active Directory **window appears. Refer**



10. Figure 52.

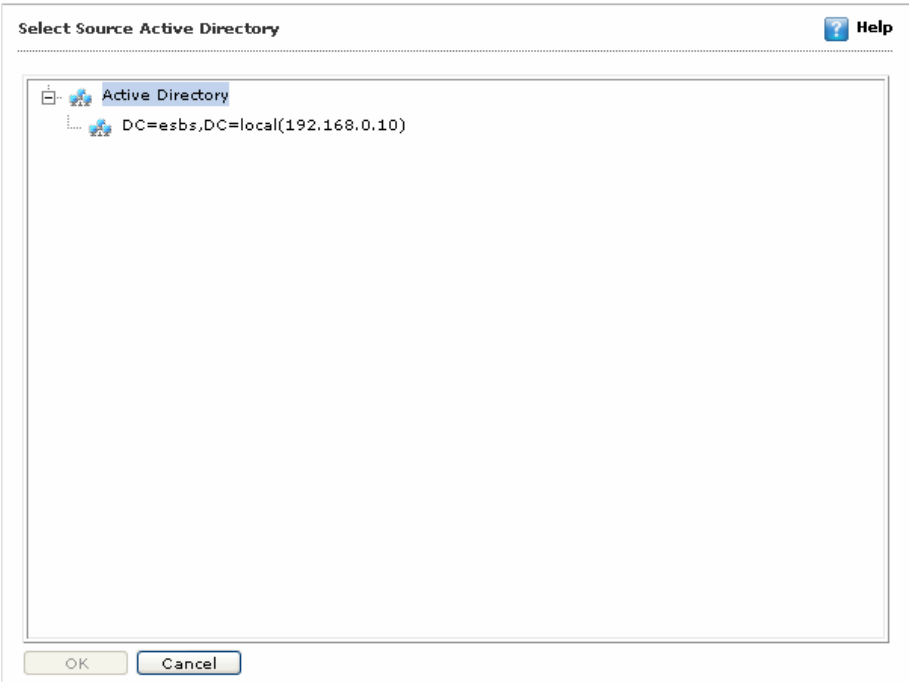


Figure 52

Click the (+) sign to expand the folder and view the options and click the (-) sign to collapse the required folder.

11. Click an appropriate active directory source that you want to add, and then click **Ok** button.
12. Click the **Next >** button. Refer Figure 50.
13. A message of creating the group wizard appears.
14. Click the **Finish** button.
    The window gets close.

Installing and Uninstalling Applications

It enables you to install and uninstall eScan application on the client machine. You also have an option to install other software, if required.

You can do the following activities:

- Installing eScan
- Installing Other Software
- Uninstalling eScan

Installing eScan

Perform the following steps to install eScan.

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 53.

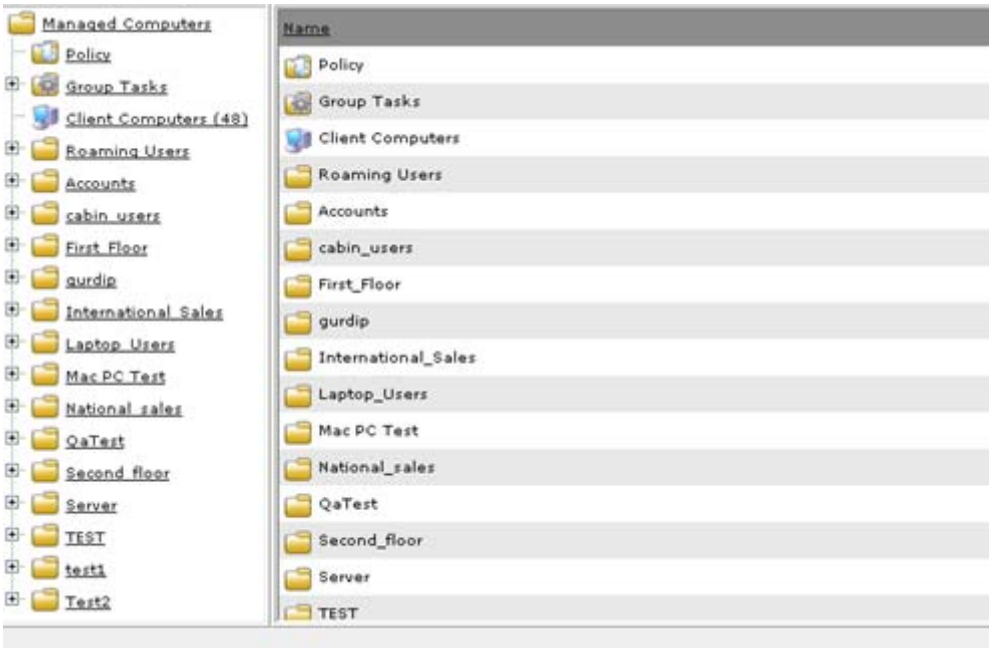


Figure 53

2. Click the **Action List** drop-down menu, and then click **Deploy/Upgrade Client**. The **Client Installation** window appears. Refer Figure 54.

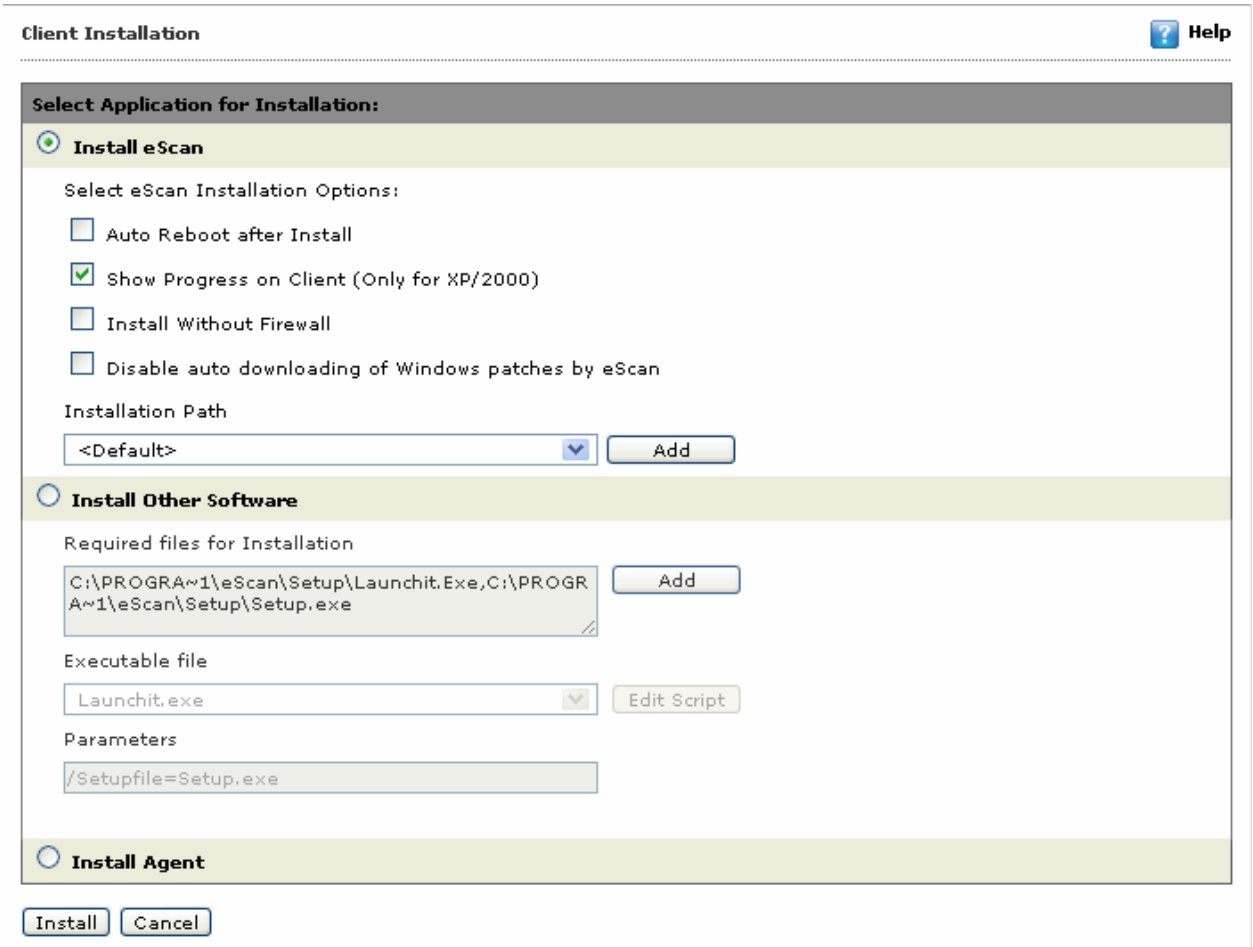


Figure 54

3. Click **Install eScan** option, if you want to install eScan application.

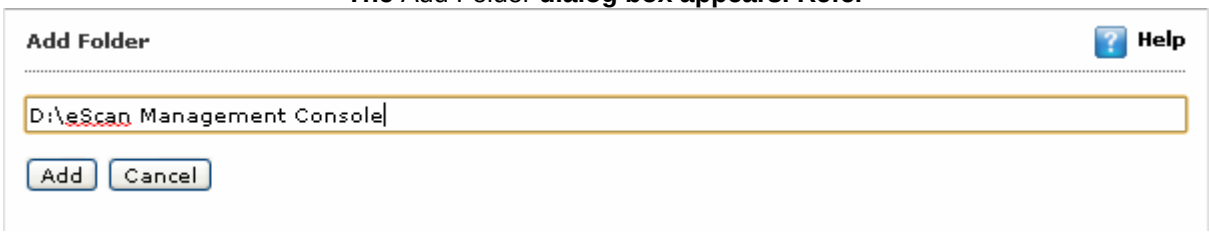
When you select **Install eScan** option, the options under **Install Other Software** option becomes unavailable.

4. Specify the following field details:

Field	Description
Select eScan Installation Options:	
Auto Reboot after install	Select this check box if you want to auto reboot your computer after installation.
Show Progress on Client (Only for XP/2000)	Select this check box if you want to view the installation progress on client machine. This option is available only for windows XP and 2000 version of operating system.
Install without Firewall	Select this check box if you do not want to install eScan Firewall.
Disable auto downloading of Windows patches by eScan	Select this check box if you do not want to install Windows patches from eScan server

5. In the **Installation Path** drop-down list, by default <Default> appears, which installs eScan in "%systemroot%/programfiles/eScan" folder.

Click the Add **button.**
The Add Folder **dialog box appears. Refer**



6. Figure 55.

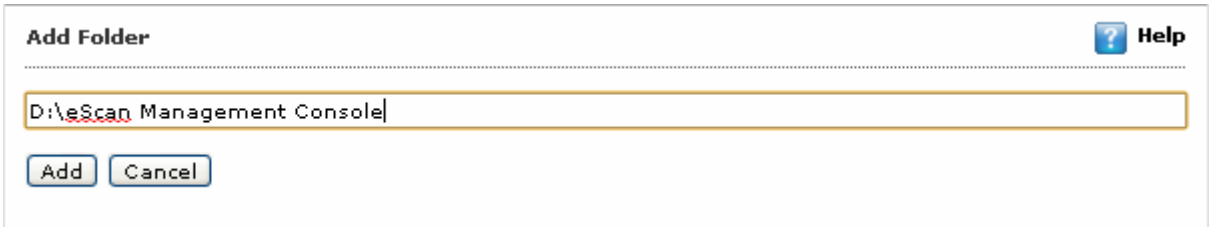


Figure 55

Please ensure that you specify valid and complete path for installation, else eScan gets installed on default path.

7. In the **Add folder** field, type the complete path of the folder on which you want to install eScan on the client machine, and then click **Add** button.
   The installation path gets added to the **Installation Path** drop-down list.

Installing Other Software

Perform the following steps to install other software.

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 56.

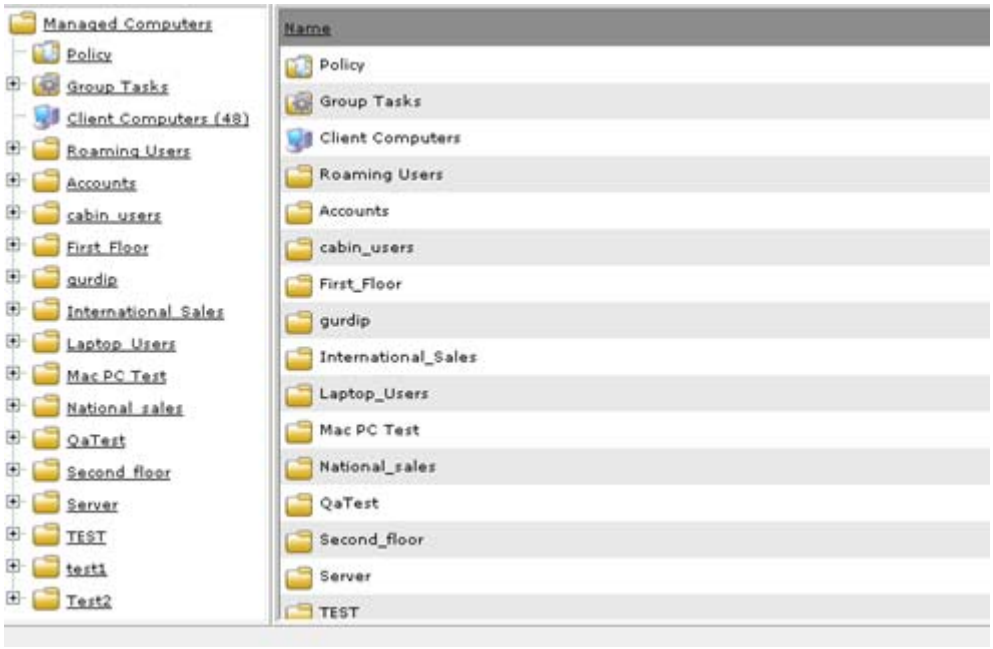
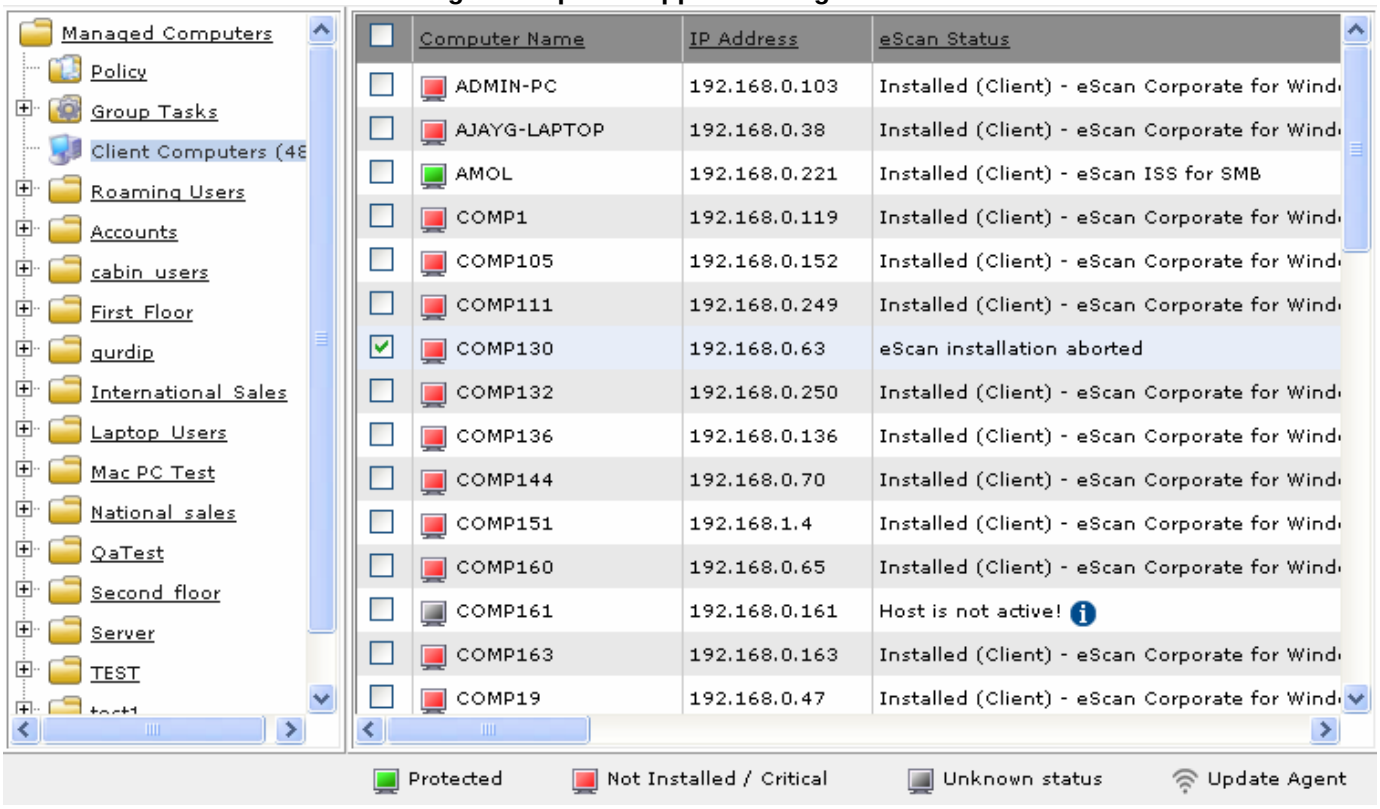


Figure 56

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

On the left pane, under the appropriate managed computers folder, click Client Computers**.**
The list of all managed computers appears on right side of the screen. Refer



2. Figure 57.

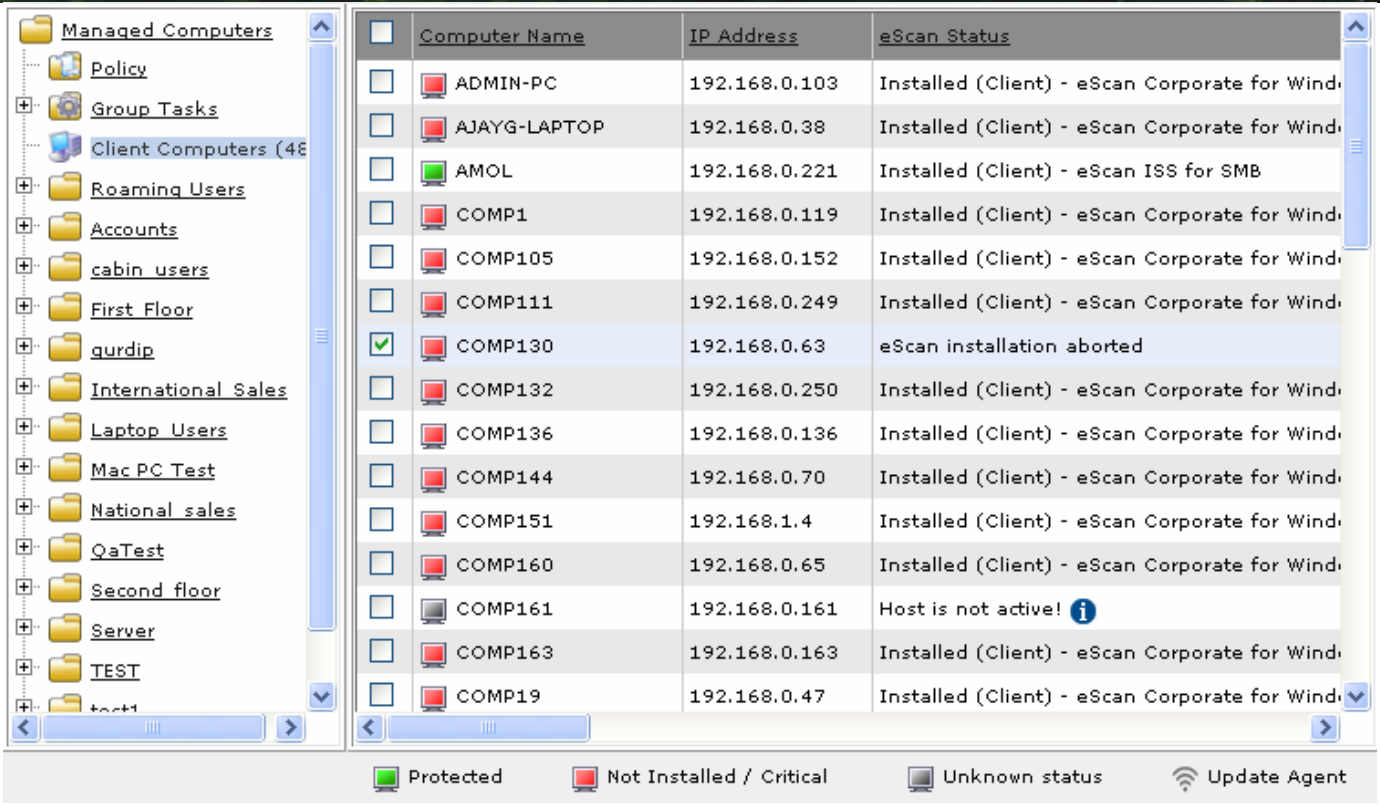


Figure 57

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box on which you want to install other software.

The **Deploy/Upgrade Client** menu and **Refresh Client** button is available, only when you select the appropriate computer name check box from the list.

Click the Client Action List **drop-down menu, and then click** Deploy/Upgrade Client**.**
The Client Installation **window appears. Refer**

4. Figure 58.

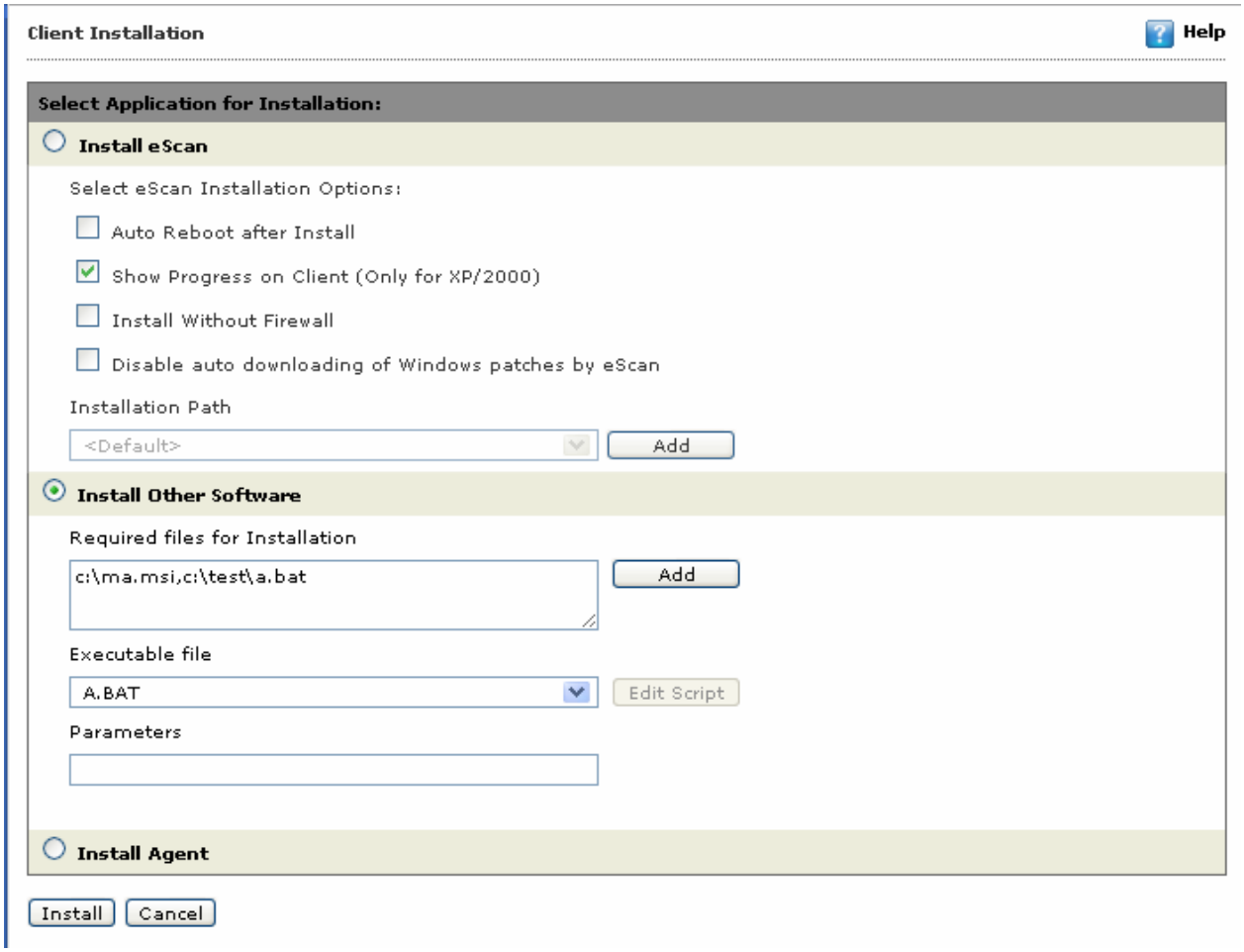


Figure 58

5. Click **Install Other Software** option, if you want to install other software.

When you select **Install Other Software** option, the options under **Install eScan** option becomes unavailable.

6. In **Required files for Installation** field, type the file path or click the **Add** button.
The **Add Files** dialog box appears. Refer Figure 59.

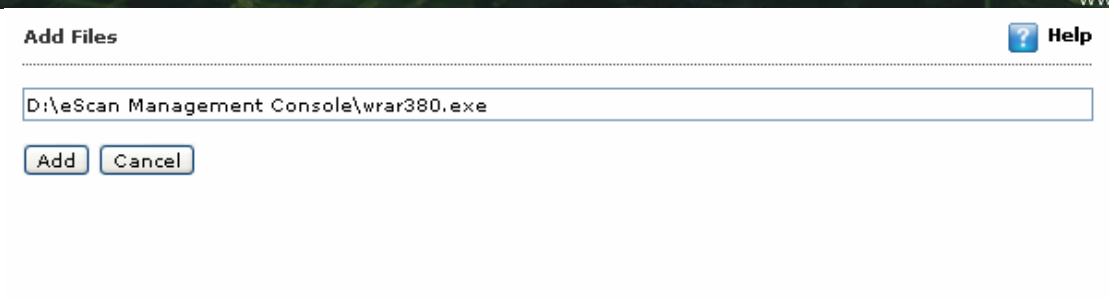


Figure 59

7. In the **Add Files** field, type the file path that you want to add, and then click the **Add** button.

In Executable file **drop-down list, click the file that you want to execute on client machine. Refer**

8. Figure 58.

In Parameters **field, type the parameters using which you want to execute the executable file. Refer**

9. Figure 58.

10. Click the **Install** button.
A message of successful installation of eScan appears.

Installing Agent

This option will enable to install only the eScan agent on the machine selected.

Uninstalling eScan

It is a very easy process to uninstall eScan application from your client machine, whenever required. You can uninstall eScan application from your specific client machine as well as from the computers in the group.

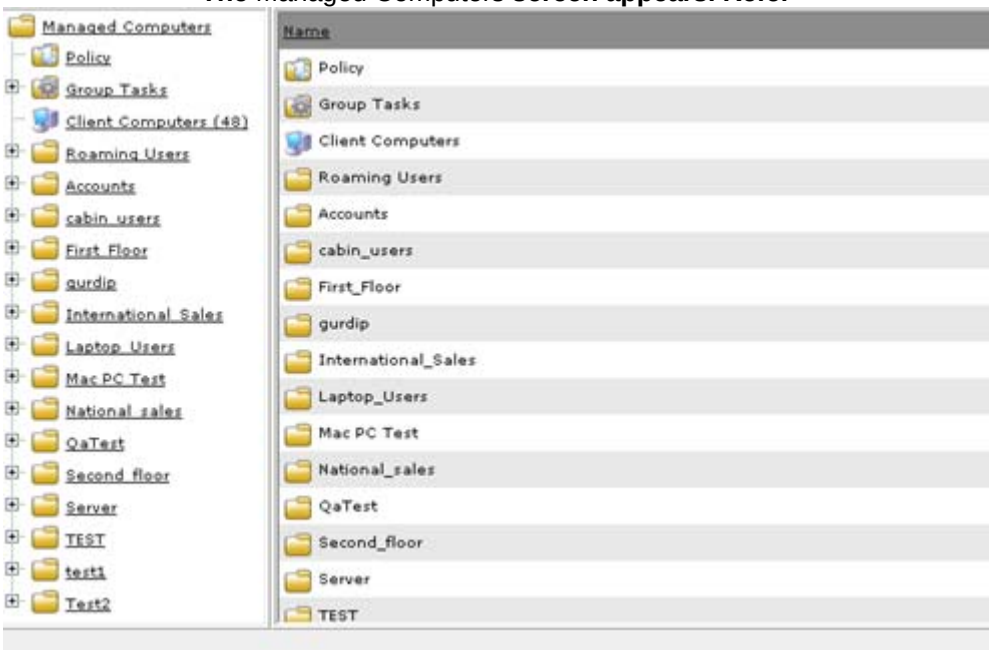
You can perform the following activities:

- Uninstalling eScan from Group
- Uninstalling eScan on Specific Client Machine

Uninstalling eScan from Group

Perform the following activities to uninstall eScan from a computer in the group, from the **Action List**.

On the navigation pane, click Managed Computers**.**
The Managed Computers **screen appears. Refer**



1. Figure 60.

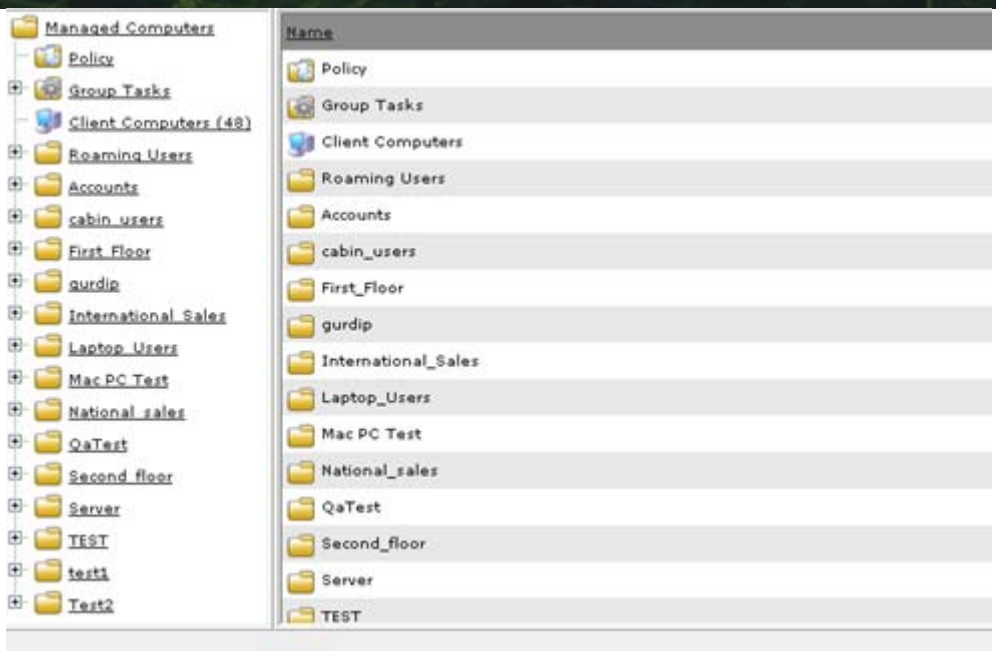


Figure 60

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

2. Click the **Action List** drop-down menu, and then click **Uninstall eScan Client**.
   The **Client Uninstallation** window appears. Refer Figure 61.

Figure 61

3. Click the **Uninstall** button.
   It displays uninstallation status on the selected client computer.

Uninstalling eScan on Specific Client Machine

Perform the following activities to uninstall eScan on specific client machine from the **Client Action List**.

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 62.

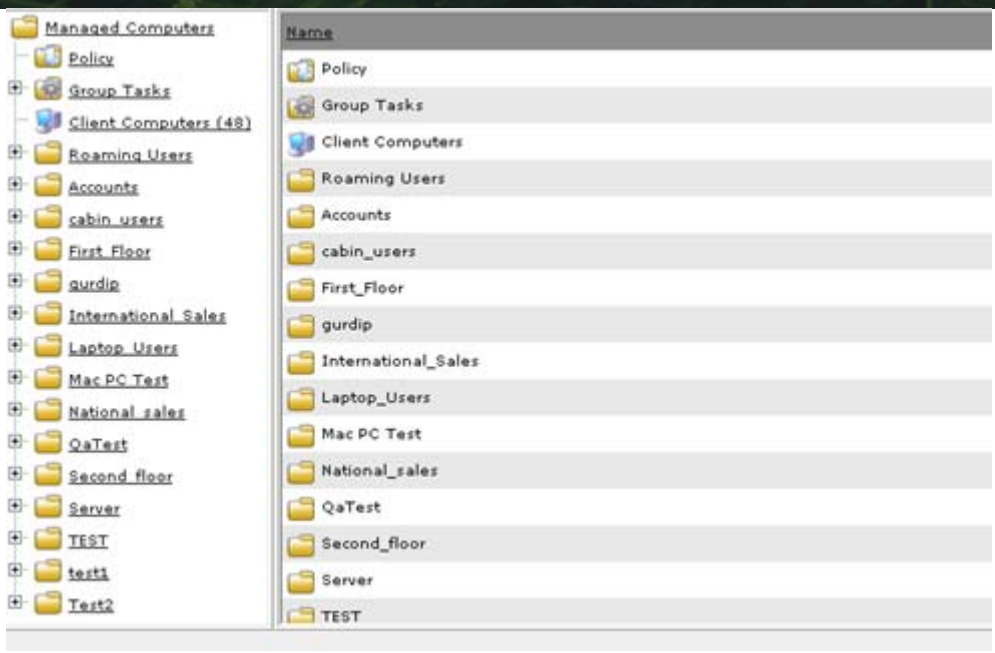


Figure 62

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

2. On the left pane, under an appropriate managed computers folder, click **Client Computers**. The list of all managed computers appears on right side of the screen. Refer Figure 63.

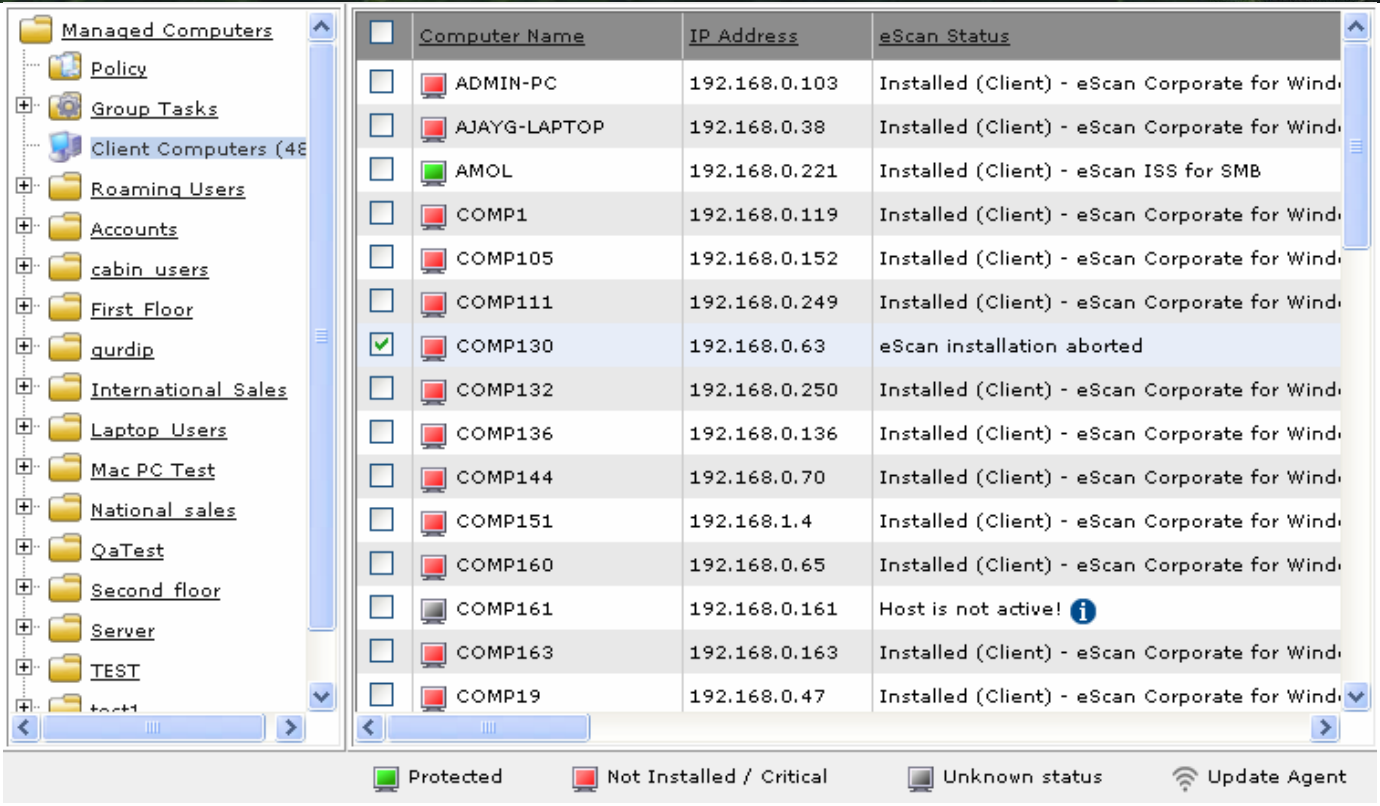


Figure 63

The symbol indicates status as protected, symbol indicates status as not installed/critical, symbol indicates status as unknown, and symbol indicates status as update agent.

3. Select an appropriate computer name check box on which you want to uninstall eScan.

4. Click the **Client Action List** drop-down menu, and then click **Uninstall eScan Client**.
   The **Client Uninstallation** window appears. Refer Figure 64.

Figure 64

5. Click the **Uninstall** button.
   It displays uninstallation status on the selected client computer.

Chapter 5: Managing Tasks for Computers and Groups

The eScan Web Console comes with several handy features such as the ability to schedule eScan tasks to run at specific intervals.

The eScan Web Console manages the computers and computer groups on a network by using tasks. A task may comprise the enabling or disabling or modules, filter; starting and stopping of a server; specifying an update server; performing scans on the memory, system drives, or local drives, and forcing the client computer to download updates or forcing them to upgrade.

A task can be applied to a selected computer or computer group and can be configured to either run on a schedule or to be started manually. The **Tasks For Specific Computers** page of the eScan Web Console allows you to create and manage tasks and view the properties of existing tasks.

Creating a Task

You can configure eScan to run specific modules at specific times on specific computers or computer groups by creating tasks.

For example, you can create a task for enabling the Web Protection module on a given computer group at a given time on say, every Wednesday and Saturday. On the other hand, you can create a task to run a memory scan on a computer group on a monthly basis.

These were a couple of examples. Nevertheless, the possibilities are endless.

To create a new task, you should click the **Create New Task** button on the **Tasks For Specific Computers** page of the eScan Web Console. This opens up the **New Task Template** page. On this page, you need to specify a name for the task, and then select the actions that should be executed when you run the task by selecting the appropriate options and check boxes.

Once you have selected the actions, you need to choose the computers and computer groups on which you want to run these tasks.

You must be careful while selecting groups because when you select a group in the **Select Computers/Groups** list, its subgroups are selected automatically.

You can also configure a task to run automatically at a given time on a specified day or week or month by selecting **Enable Scheduler** in the **Task scheduling settings** section. If you want to run the task manually, you can do so by selecting the **Manual Start** option and then clicking **Save**. After you have created a task, you can run it manually by clicking **Start Task** on the **Tasks For Specific Computers** page.

When you create a new task, a new row is added to the table on the **Tasks For Specific Computers** page. This table contains information such as the name of the task; status of the task, whether it has been performed or not; the computer to which this task has been assigned, and the schedule type.

In addition, a **View** link for the row is created and added to the table. When you click this link, the result of running the task is displayed in the form a pie chart and a summary of this information is displayed below the chart.

Perform the following steps to create a new task:

1. On the navigation pane, click **Tasks For Specific Computers**.
   The **Tasks For Specific Computers** screen appears. Refer Figure 65.

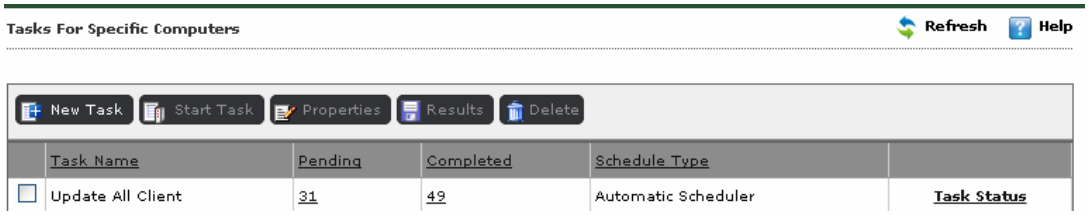
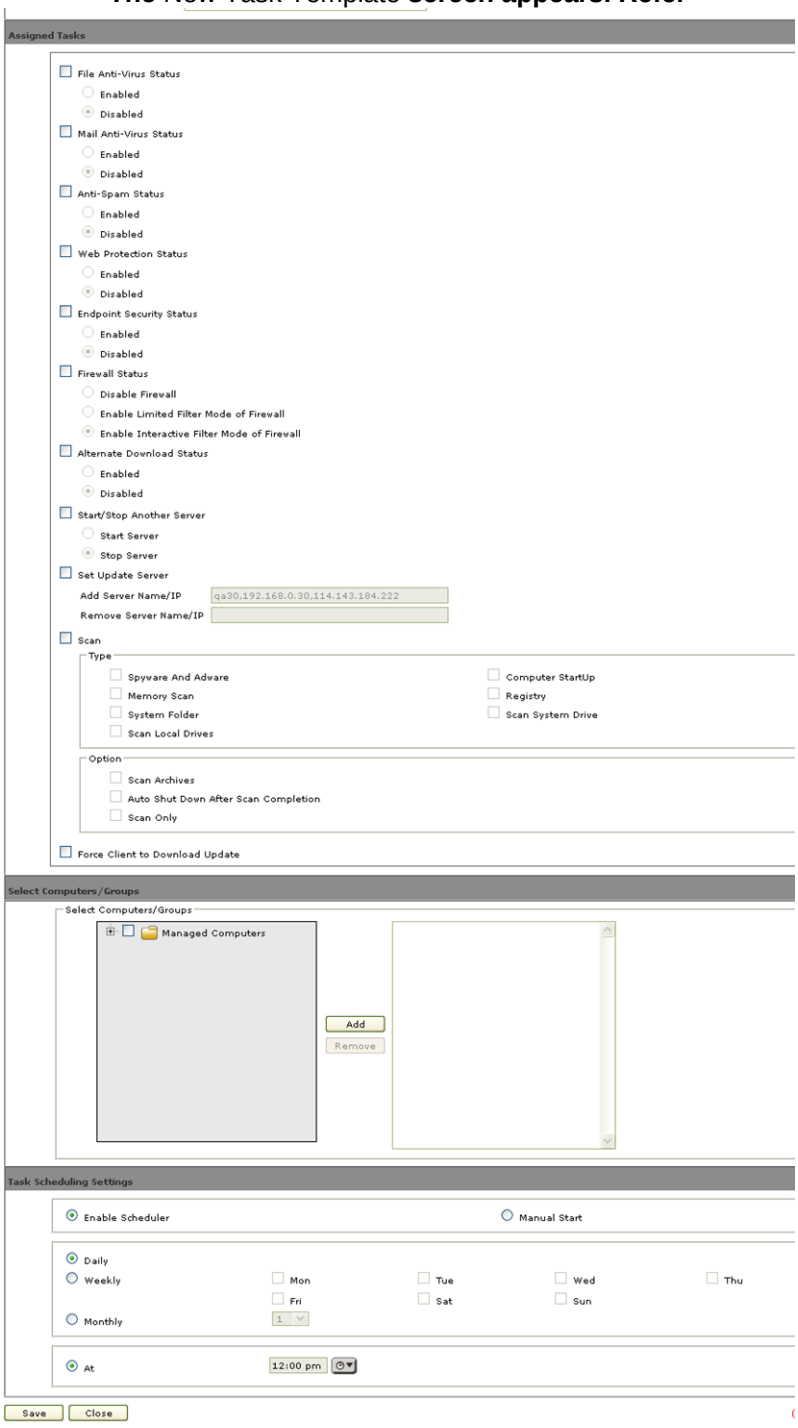


Figure 65

Click the New Task **button.**
The New Task Template **screen appears. Refer**



2. Figure 66.

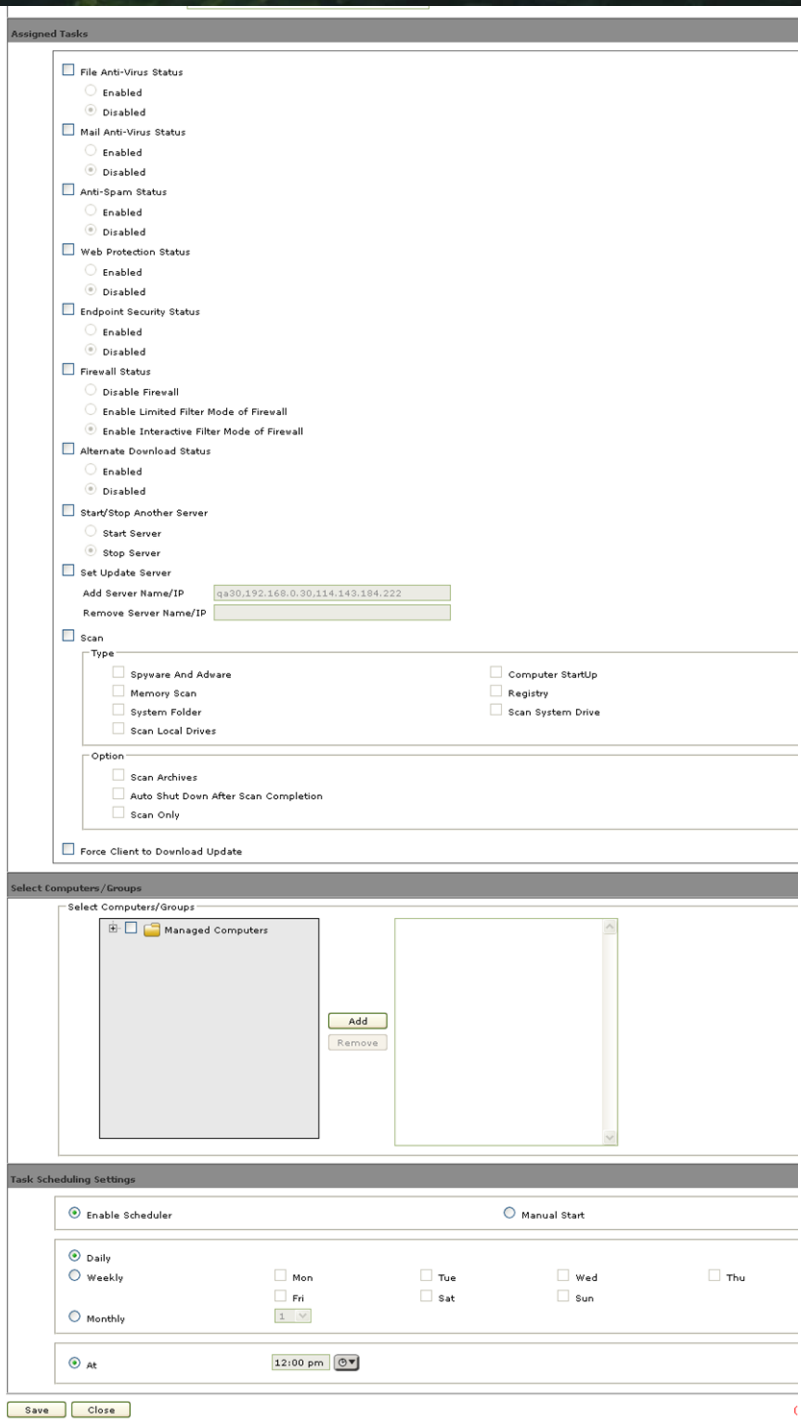


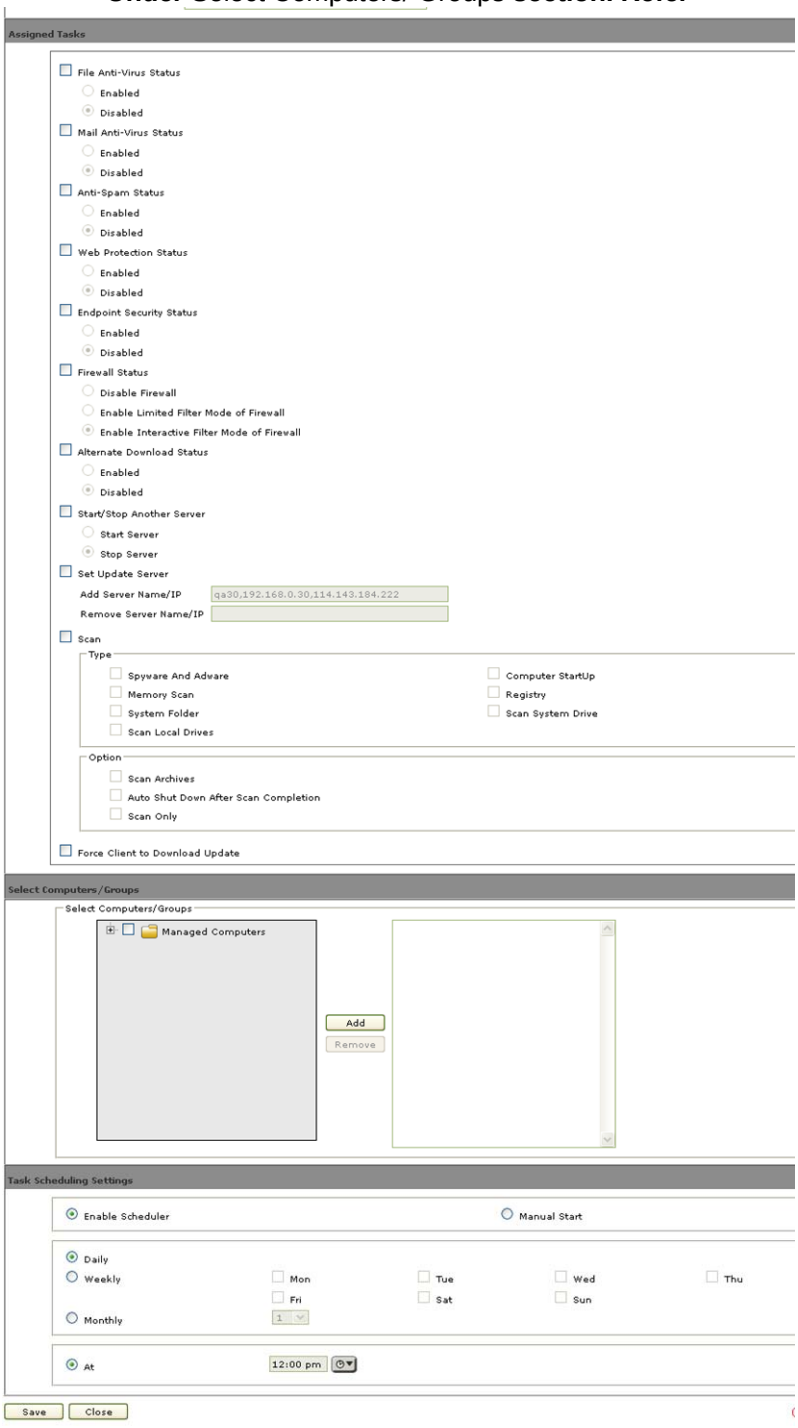
Figure 66

3. Under **Task Name** section, in the **Task Name** field, type name for the task.
4. Under **Assigned Tasks** section, specify the following field details.

Field	Description
File Anti-Virus Status	Select this check box, and click an appropriate option. • Click **Enabled**, if you want to start **File Anti-virus** module. • Click **Disabled**, if you want to stop **File Anti-virus** module.
Mail Anti-Virus Status	Select this check box, and click an appropriate option. • Click **Enabled**, if you want to start **Mail Anti-Virus** module. • Click **Disabled**, if you want to stop **Mail Anti-Virus** module.
Anti-Spam Status	Select this check box, and click an appropriate option. • Click **Enabled**, if you want to start **Anti-Spam** module. • Click **Disabled**, if you want to stop **Anti-Spam** module.
Web Protection Status	Select this check box, and click an appropriate option. • Click **Enabled**, if you want to start **Web Protection** module. • Click **Disabled**, if you want to stop **Web Protection** module.
Endpoint Security Status	Select this check box, and click an appropriate option. • Click **Enabled**, if you want to start **Endpoint Security** module. • Click **Disabled**, if you want to stop **Endpoint Security** module.
Firewall Status	Select this check box, and click an appropriate option. • Click **Disable Firewall**, if you want to start Firewall module. • Click **Enable Limited Filter Mode of Firewall**, if you want to start only limited filter modes of **Firewall** module. • Click **Enable Interactive Filter Mode of Firewall**, if you want to start only interactive filter modes of **Firewall** module.
Alternate Download Status	Select this check box, and click an appropriate option. • Click **Enabled**, if you want to take direct updates and view the status of alternate download. • Click **Disabled**, if you want do not want to view status of the updates.

Start/Stop Another Server	Select this check box, and click an appropriate option. • Click **Start Server**, if you want to start announcement of another server. • Click **Stop Server**, if you want to stop announcement of another server.
Set Update Server	Select this check box if you want to set update server. • **Add Server Name/IP:** This field is available only when you select **Set Update Server** check box. Type the server name or IP address that you want to add. • **Remove Server Name/IP:** This field is available only when you select **Set Update Server** check box. Type the server name or IP address that you want to remove.
Scan	Select this check box if you want to do scanning through the following options: • Select **Memory Scan** check box, if you want to scan memory. • Select **Scan System Drive** check box, if you want to scan system drive. • Select **Scan Local Drives** check box, if you want to scan all local drives.
Force Client to Download Update	Select this check box, if you want to force clients to take download updates.

Under Select Computers/ Groups **section. Refer**

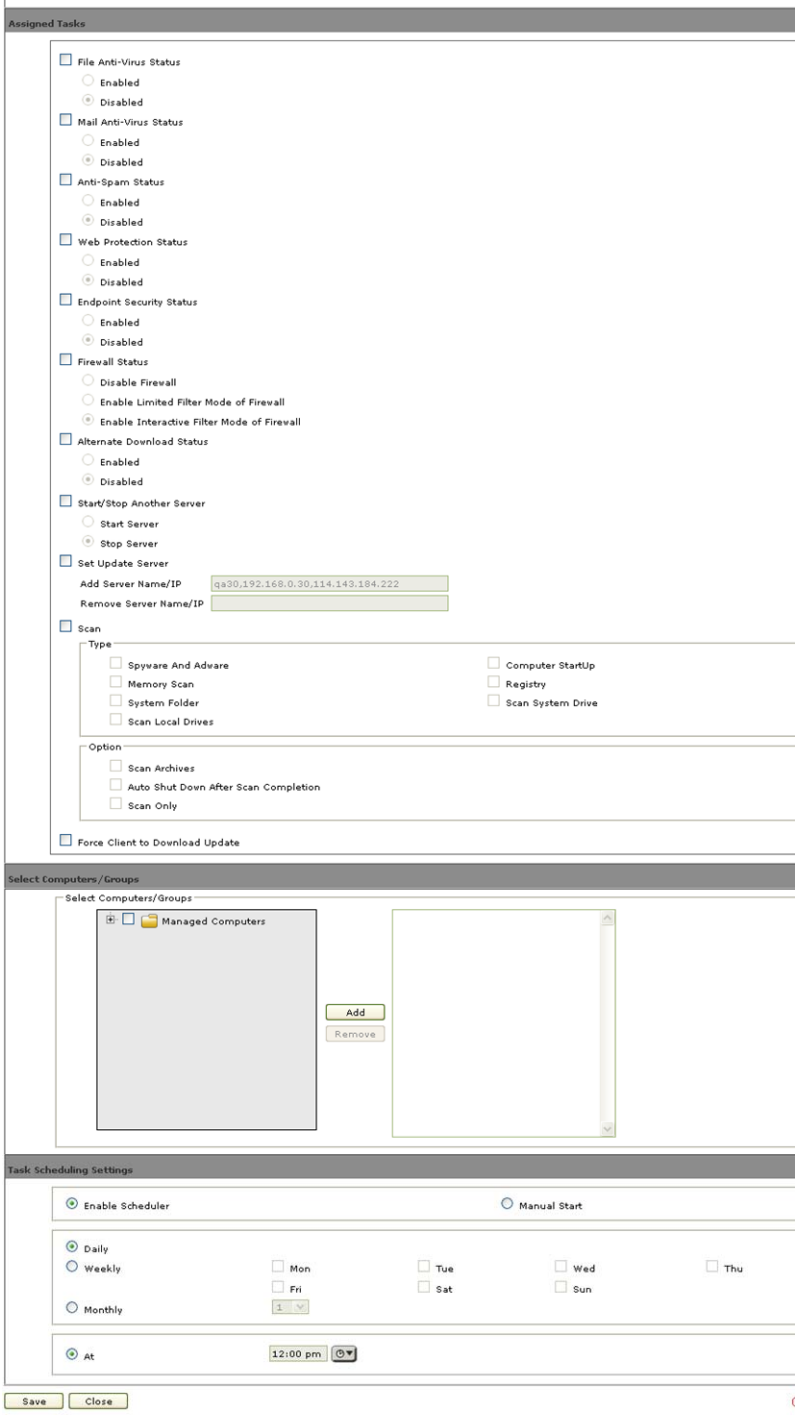


5. Figure 66.

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

6. Select an appropriate check box, the computer or group that you want to add for creating the task.
7. Click the **Add** button, to add selected computer or group to the list on right side.
8. To remove added computer or group from the list on right side, select an appropriate computer or group name, and then click the **Remove** button.

Under Task Scheduling Settings **section, specify the following field details. Refer**



9. Figure 66.

Field	Description
Enable Scheduler	Click this option, if you want to schedule the tasks to run automatically. When you click this option, **Daily**, **Weekly**, **Monthly**, and **At** option becomes available.
Daily	Click this option, if you want to schedule the tasks to run daily.
Weekly	Click this option, if you want to schedule the tasks to run weekly, and then select an appropriate check box. For example, Mon, Tue, Wed, and so on.
Monthly	Click this option, if you want to schedule the tasks to run monthly. Select appropriate number of days in a month for which you want to run task.
At	Perform the following steps to select time: • Click the Time  icon. The Timer appears. • Click the A.M. tab to view the before noon time and P.M. 0tab to view the afternoon time, and then select an appropriate time from the list.
Manual Start	Click this option, if you want to schedule the task manually. When you click this option, **Daily**, **Weekly**, **Monthly**, and **At** option becomes unavailable.

10. Click the **Save** button.
    The task gets created.

Start an Existing Task

It may so happen that you have already created a task to run on a group of computers at a scheduled time but for some reason, you may need to shut the computers down for some maintenance work. In such a situation, you can either modify the task, which means that you will have to change it back to the original settings once it has finished executing. Another problem here is that you need to remember all the settings. This is not practically possible.

This is an example of a situation where you need to run tasks manually. Fortunately, the eScan Web Console provides you with the Start Task option. To run an existing task, all you have to do is select the task in the **Tasks For Specific Computers** page and then click **Start Task**.

The steps to run an existing task manually are as follows:

1. **In the eScan Web Console, in the left pane, click** Tasks for Specific Computers**. Refer** Figure 67.

Figure 67

2. On the **Tasks for Specific Computers** page, on the right pane, in the table, select the check box next to the name of the task that you want to run, and then click **Start Task**.

3. A window appears displaying status of the running task. To close the status window, click **Close**. Refer Figure 68.

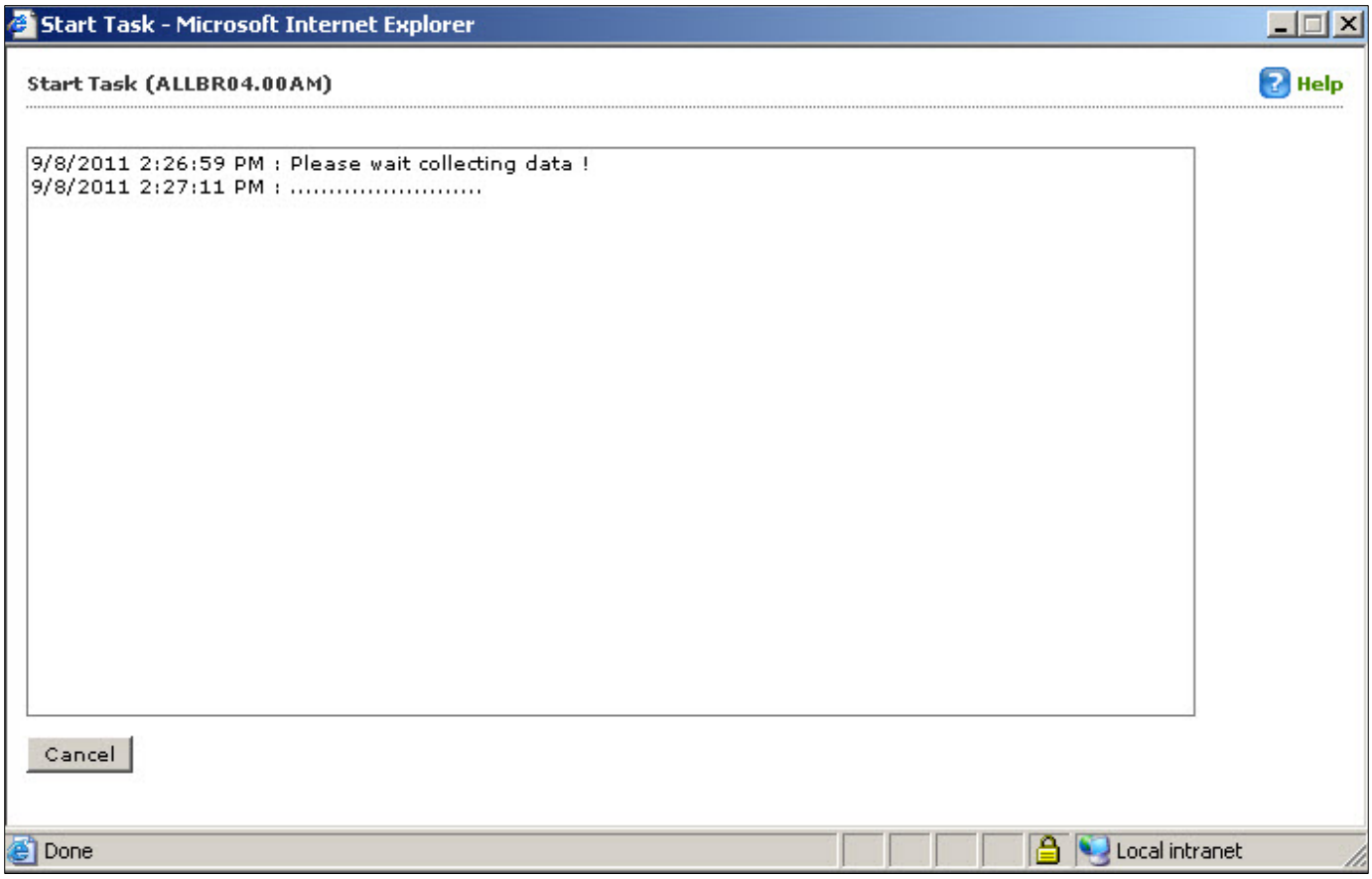


Figure 68

View the Status of Tasks

You can view the status of both manual and scheduled task. The table shows you the list of task performed, list of computers to whom the task is assigned, type of schedule, and status of the task. In addition, you can view a pie chart representing summary of the task.

To view the status of task

In the eScan Web Console, in the left pane, click Tasks for Specific Computers**.**
The Tasks for Specific Computers **screen appears. Refer**

1. Figure 69.

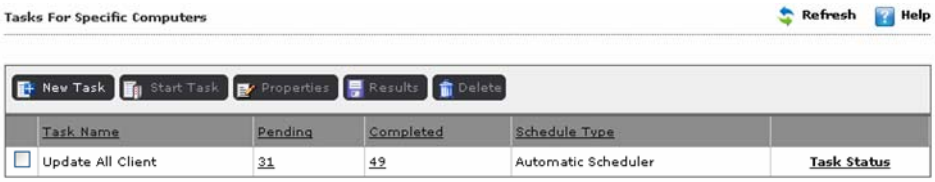
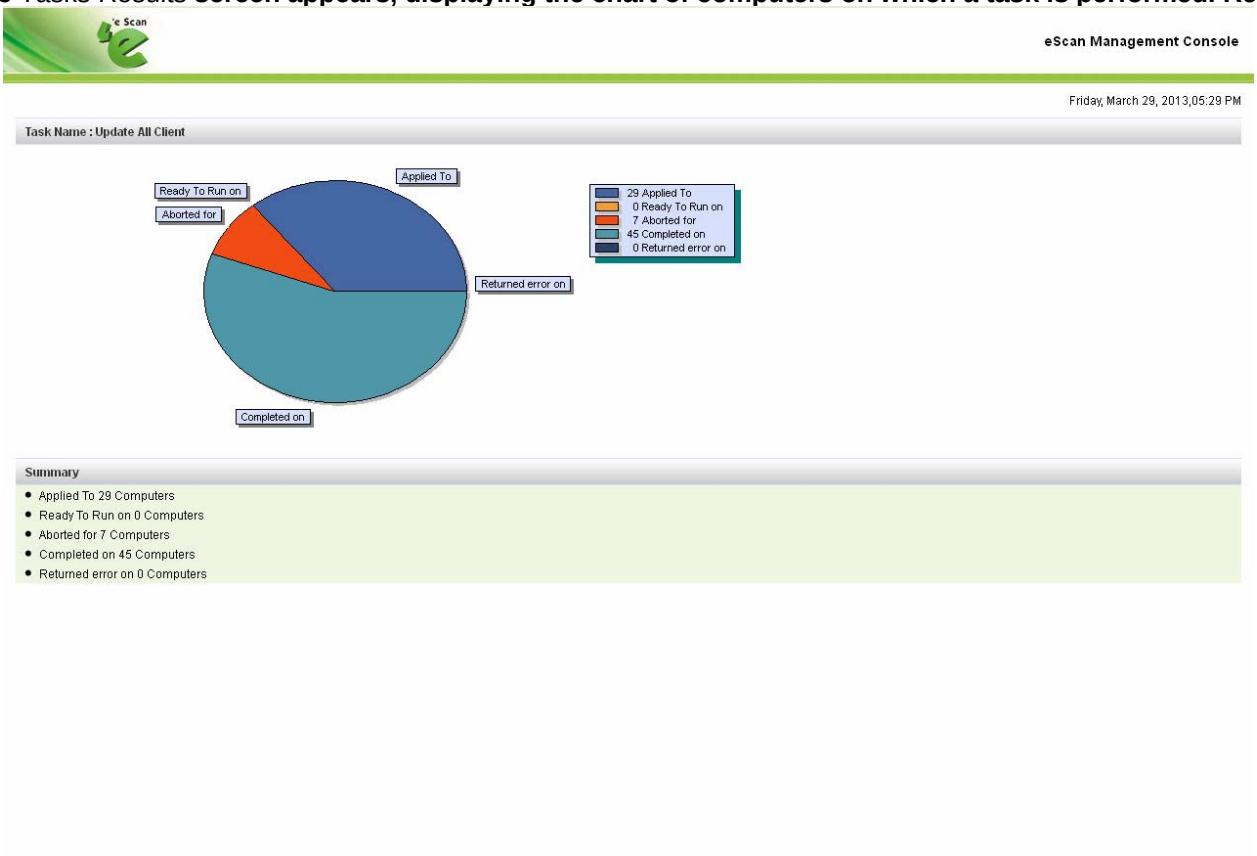


Figure 69

2. On the **Tasks for Specific Computers** page, on the right pane, in the table, select the check box next to the name of the task whose results you want to view, and then click **Results**.

The Tasks Results **screen appears, displaying the chart of computers on which a task is performed. Refer**



3. Figure 70.

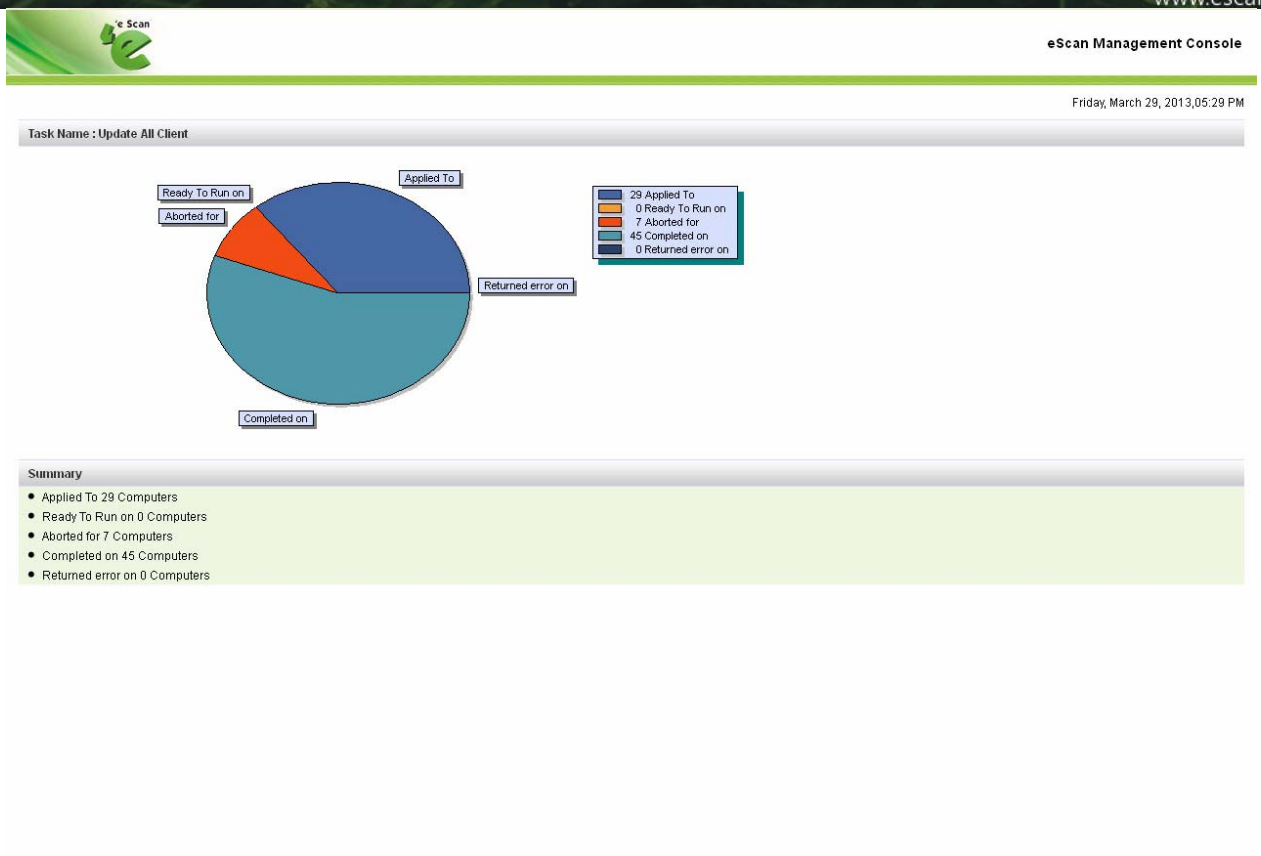

eScan Management Console
Friday, March 29, 2013,05:29 PM
Task Name : Update All Client
Ready To Run on
Aborted for
Applied To
Returned error on
Completed on
29 Applied To
0 Ready To Run on
7 Aborted for
45 Completed on
0 Returned error on
Summary
Applied To 29 Computers
Ready To Run on 0 Computers
Aborted for 7 Computers
Completed on 45 Computers
Returned error on 0 Computers

Figure 70

4. View the details as required.

On the Tasks for Specific Computers **screen, click the** Task Status **link, to view the summary of the task. The following window appears. Refer**

5. Figure 711.

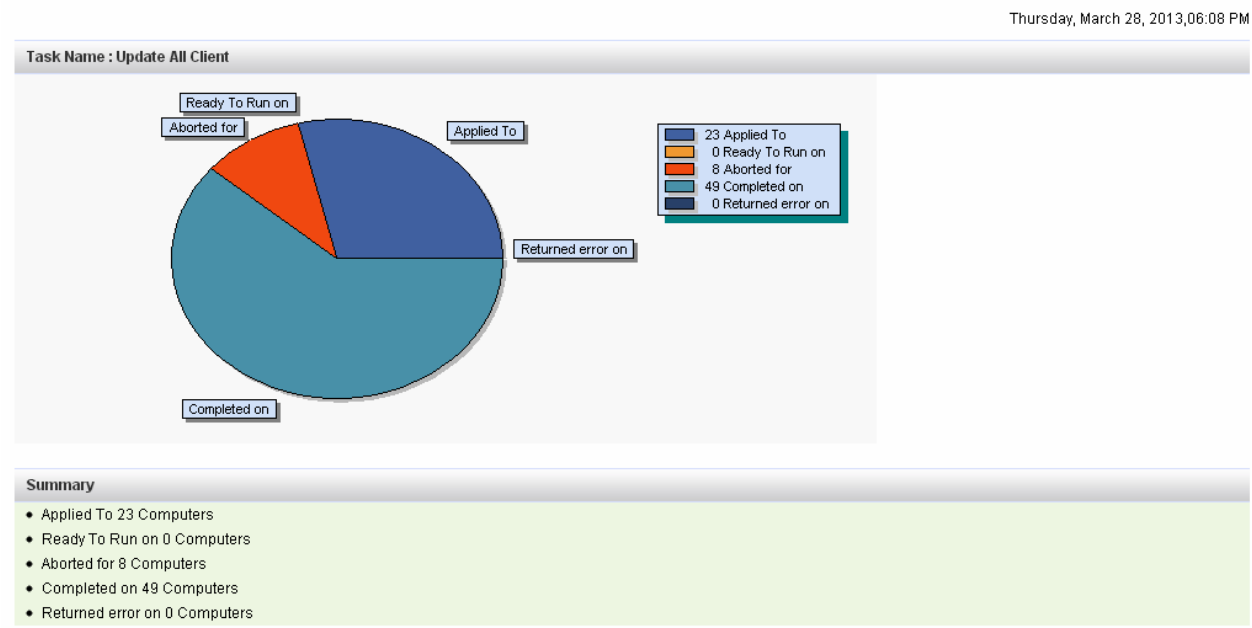


Figure 71

6. View the report summary details as required.

View the Properties of an Existing Task

You can view the properties of existing task by selecting an appropriate task name check box, and then clicking **Properties**. These properties include the name of the task, the date of creation, date of modification, sort criteria, and the available groups.

The steps to configure an existing task are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Tasks for Specific Computers**.

   Refer

   Figure 67.

2. On the **Tasks for Specific Computers** page, on the right pane, in the table, select the check box next to the name of the report that you want to configure, and then click **Properties**.
3. On the **Properties** page:
   - The **General** tab, shows you the name of the task, and details regarding the report such as the date of creation, its status, whether the task is complete, completion status, and time stamp of completion. Refer **Error! Reference source not found.**2.

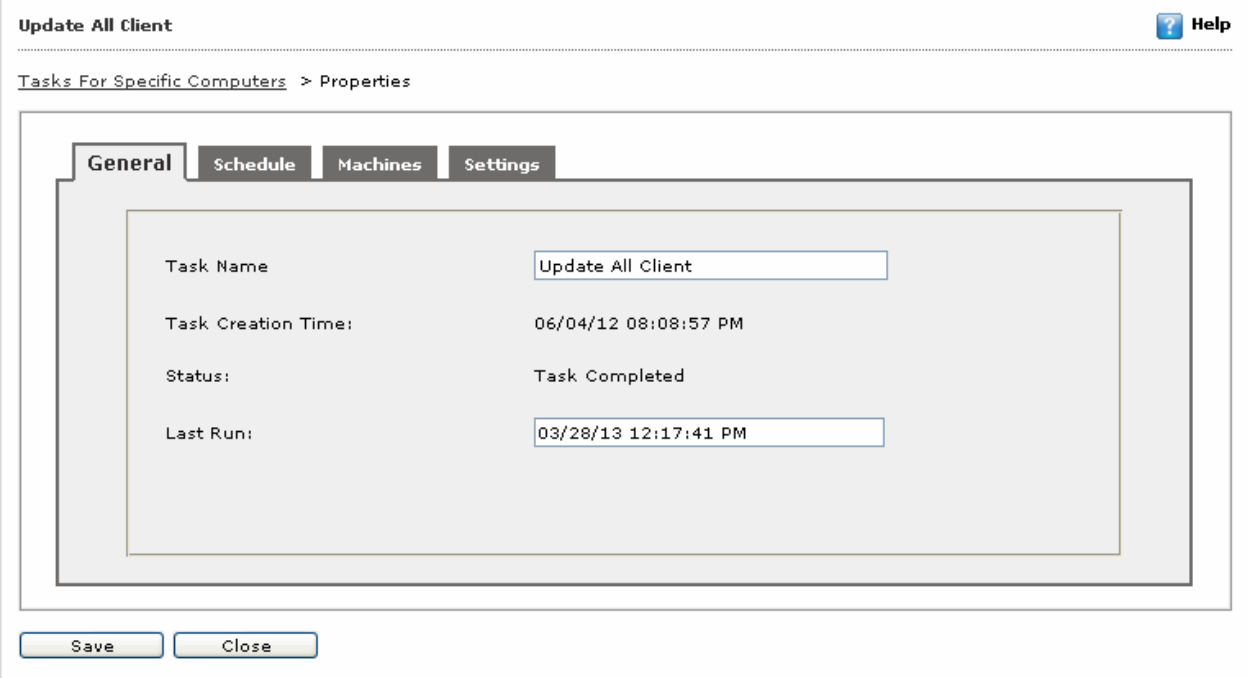


Figure 72

The Schedule **tab displays the date options. Refer**

- Figure 73.

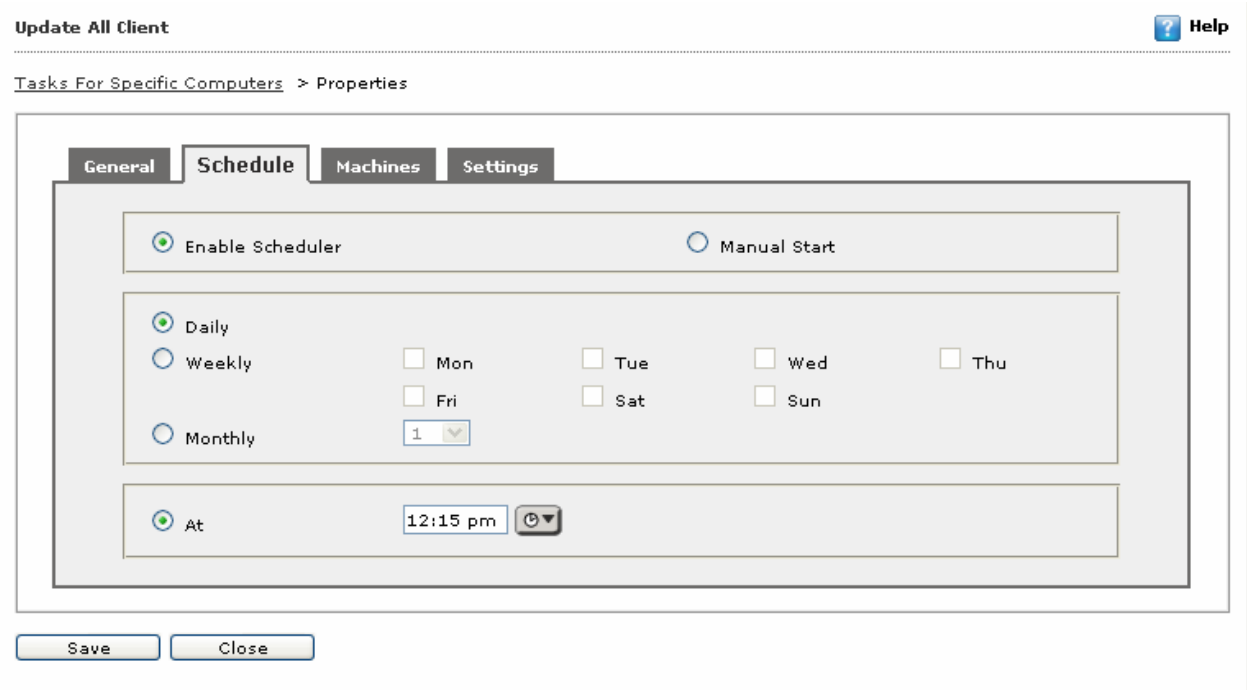


Figure 73

The Machines **tab displays all the groups as well as managed computers in the network. Refer**

- Figure 74.

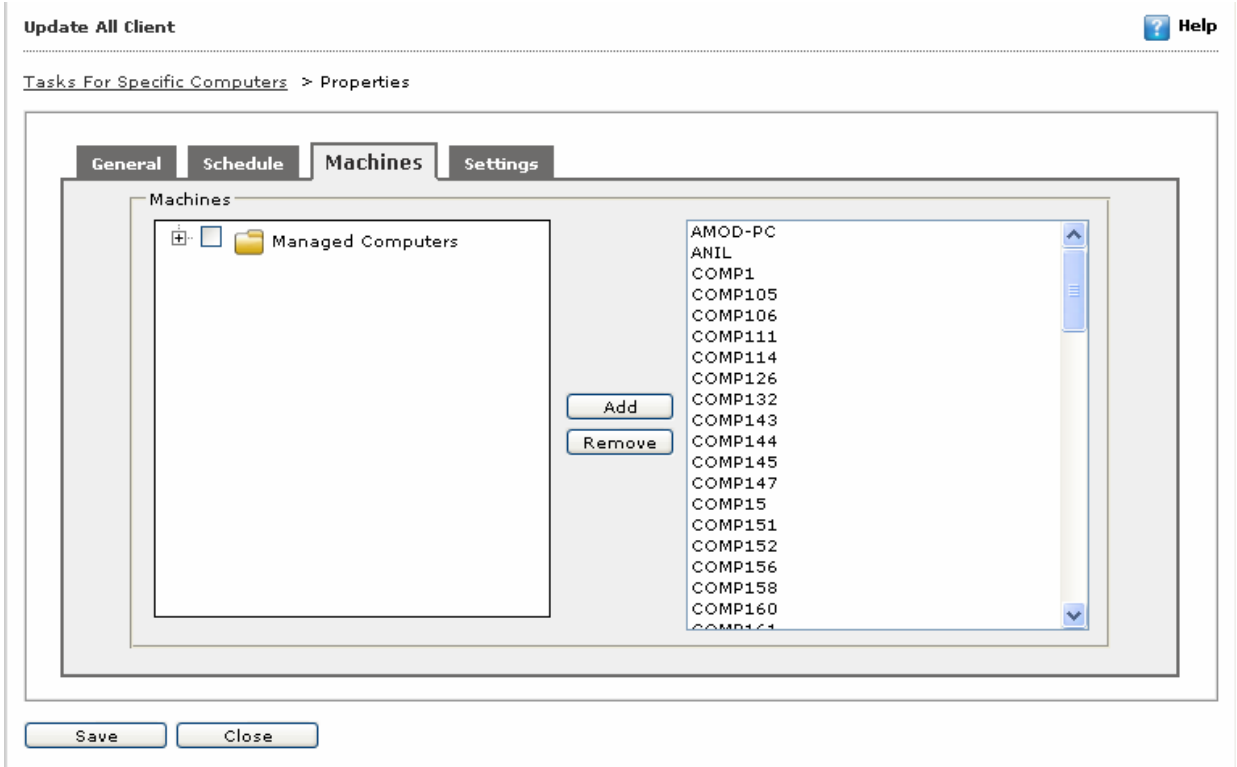


Figure 74

The **Settings** tab displays the template used for creating the task. You can make changes to the settings, if required. Refer

- Figure 75

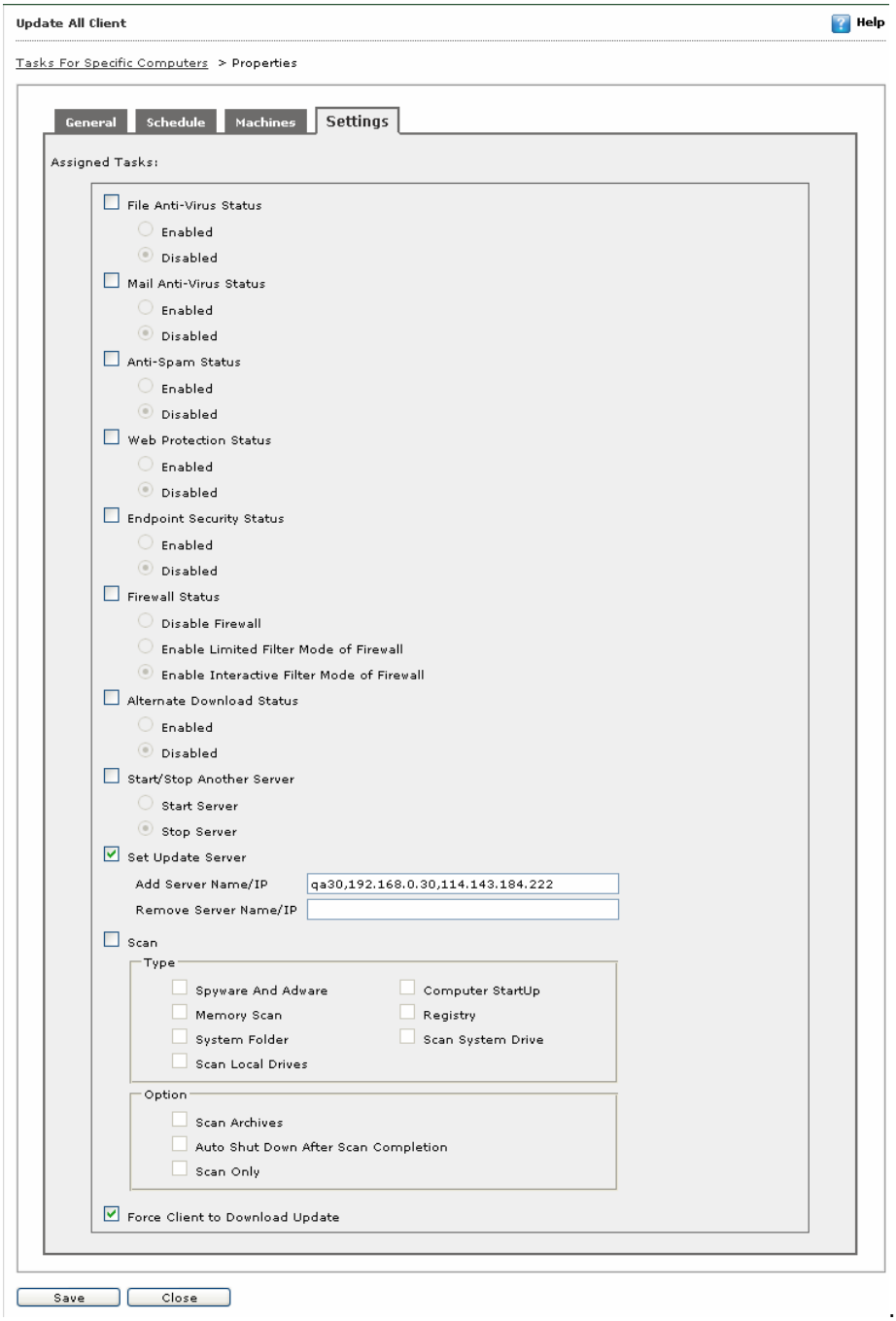


Figure 75

4. To save and close the **Properties** page, click **Ok**.

Delete an Existing Task

If a task is no longer required, you can delete it from the tasks list by selecting the task and then clicking **Delete**.

The steps to configure an existing task are as follows:

1. **In the eScan Web Console, in the left pane, click** Tasks for Specific Computers. **Refer** Figure 67.

   On the **Tasks for Specific Computers** page, on the right pane, in the table, select the check box next to the name of the task that you want to delete, and then click **Delete**.

Chapter 6: Managing Policies

A policy or a rule-set is a collection of eScan rules that can be executed on an individual computer or computer group.

In **Policies For Specific Computers**, you also have an option to create policy for specific computer same as for groups. You can create policy by setting various rule-sets and deploy it on the specific client computer. If you want you can also delete policy and view properties of policy whenever required. You can do the following activities:

Policies are also available in **Managed Computers**, which is divided in to two tabs - **General** and **Policy Details**. In **General** tab, you can view the general policy details and in **Policy Details** tab, you can configure the policy details.

Creating and Deploying New Policy

It enables you to create new policy and deploy it on specific client computer.

To create and deploy new policy

1. On the navigation pane, click **Policies For Specific Computers**.

   The Policies For Specific Computers screen appears. Refer Figure 766.

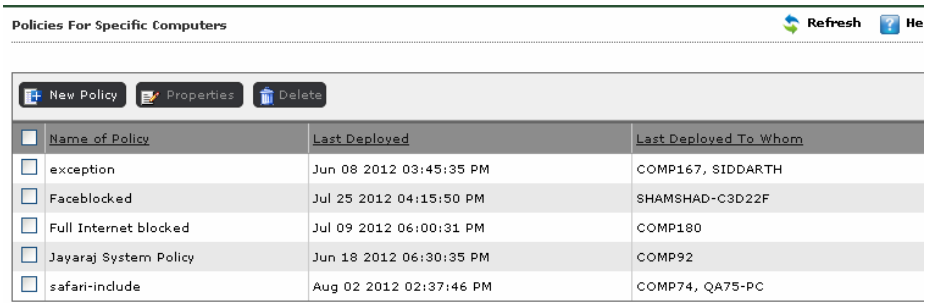


Figure 76

2. Click the **New Policy** button.

   The New Policy **screen appears. Refer** Figure 777.

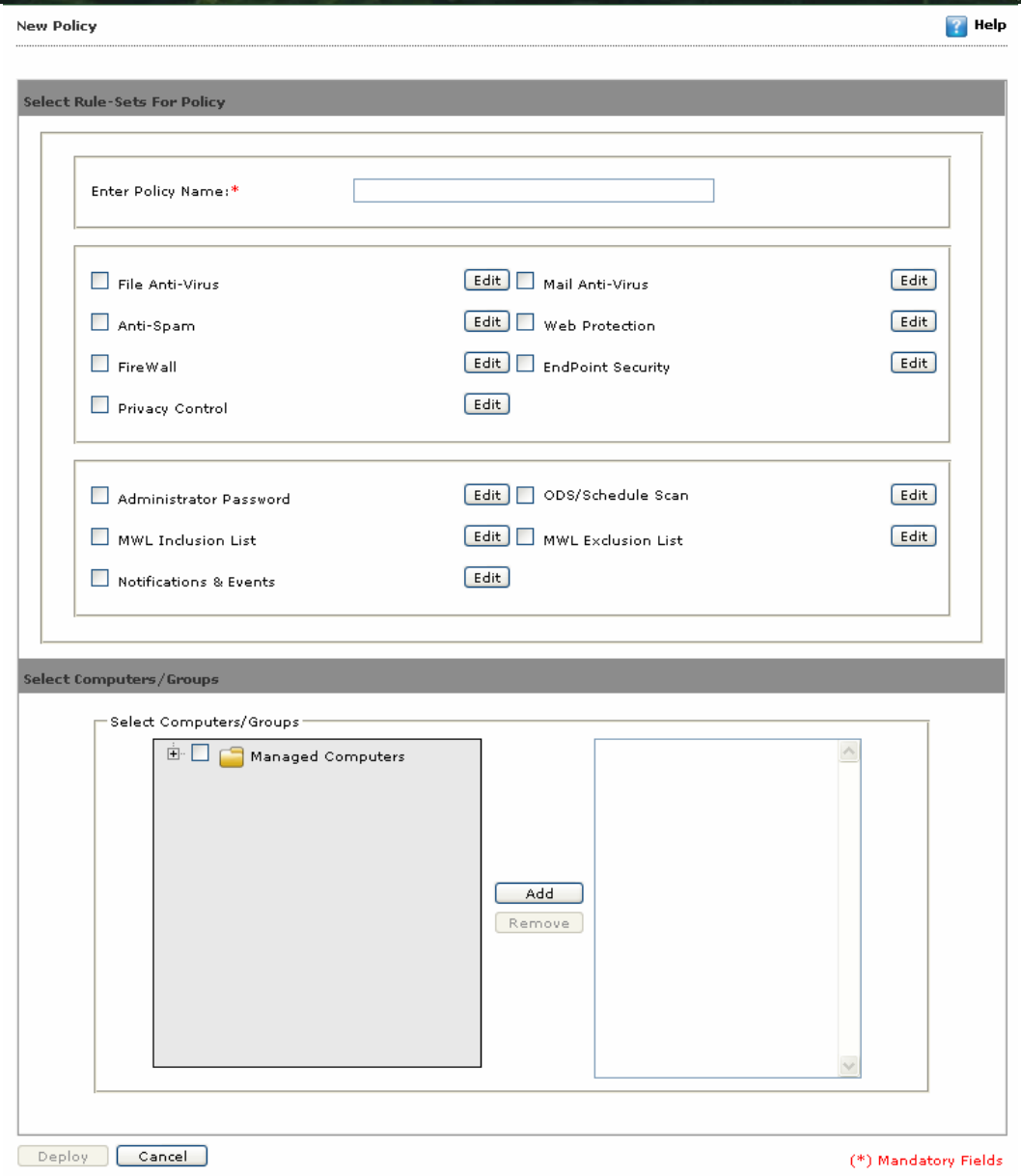


Figure 77

3. Under Select **Rules-Sets For Policy** section, in the **Enter Policy Name** field, type the policy name.
4. Select an appropriate check box, and then click the Edit icon, if you want to view and configure settings.
5. Under Select Computers/ Groups section.

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

6. Select an appropriate check box, the computer or group on which you want to deploy the policy.

7. Click the **Add** button, to add selected computer or group to the list on right side.
8. To remove added computer or group from the list on right side, select an appropriate computer or group name, and then click the **Remove** button.
9. Click the **Deploy** button.
   The policy gets deployed.

Viewing Policy Properties

It enables you to view the list of created policy and its properties.

To view policy property

1. On the navigation pane, click Policies For Specific Computers.
   The Policies For Specific Computers screen appears. Refer Figure 78.

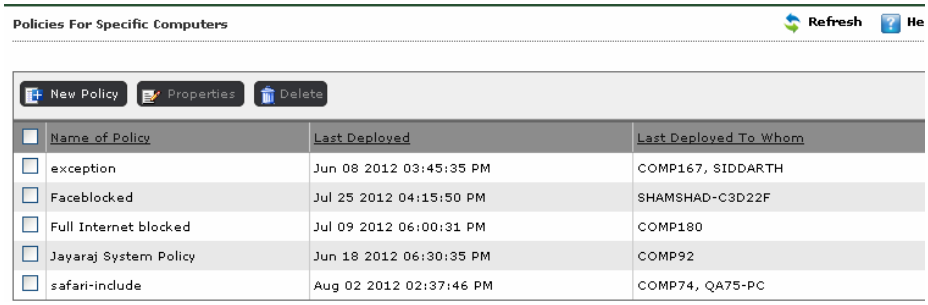


Figure 78

The **Properties** button is available only when you select an appropriate policy check box for which you want to view properties.

To view properties, you can select only one check box at a time.

2. Select an appropriate policy check box, and then click the **Properties** button.

The Properties **screen appears. Refer**

Figure .

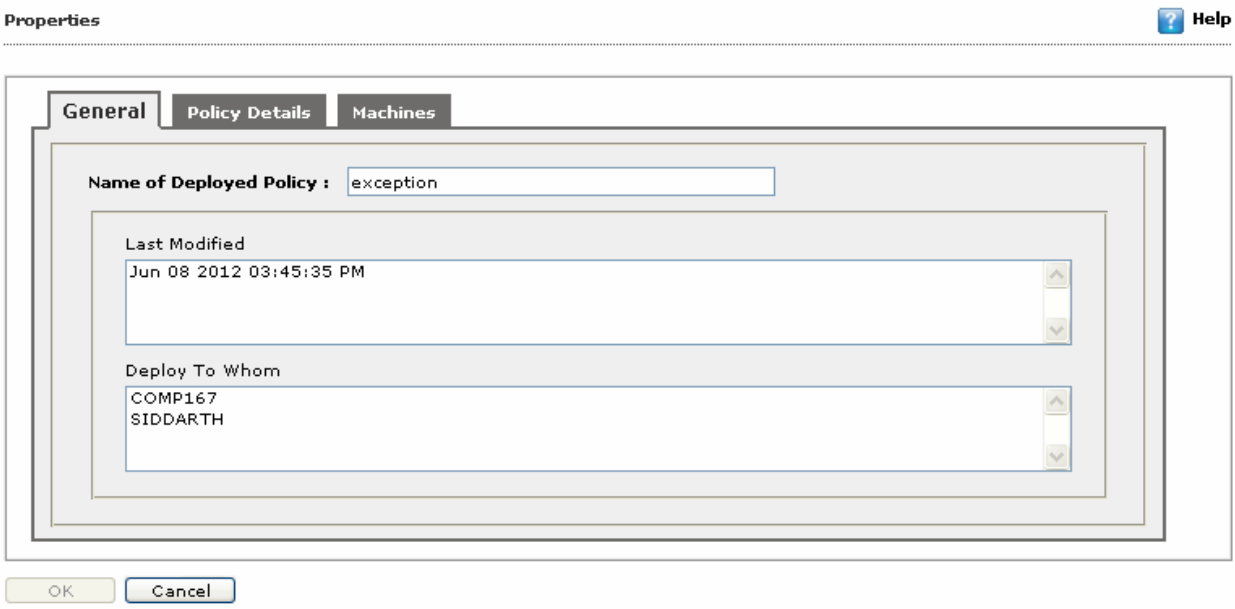


Figure 79

3. The **General** tab appears as the default tab.
4. View the field details as required.
5. Click the **Policy Details** tab.

The **Policy Details** tab appears. Refer

Figure .

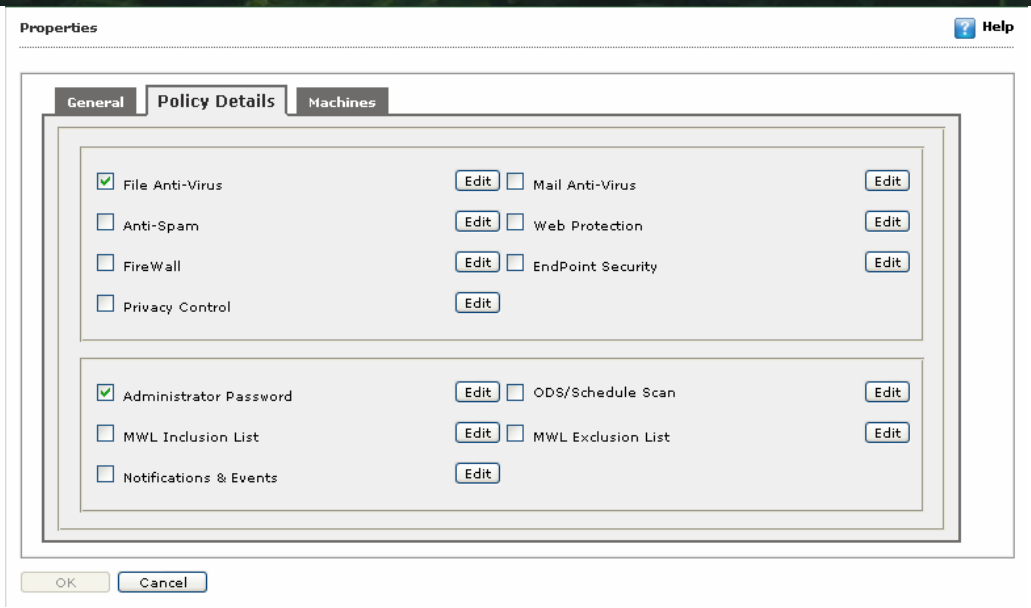


Figure 80

6. Select an appropriate check box, and then click the Edit icon, if you want to view settings.
7. View the field details as required.

Click the Machines **tab.**
The Machines **tab appears. Refer**

8. Figure .

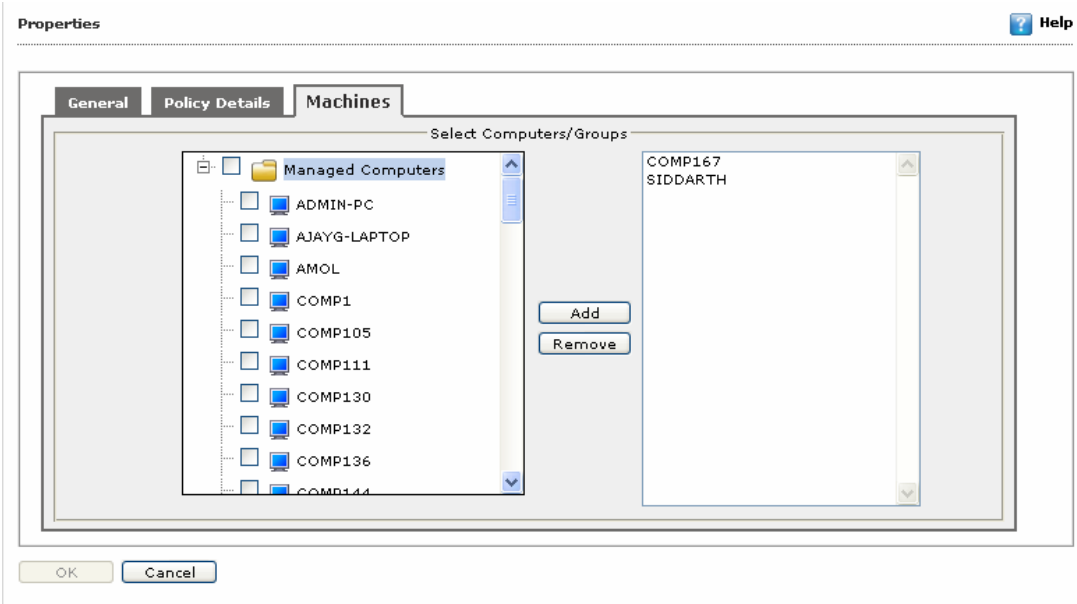


Figure 81

9. View the field details as required.

Deleting Policy

It enables you to delete policy from the list.

To delete policy

1. On the navigation pane, click Policies For Specific Computers.
   The Policies For Specific Computers screen appears.
2. Select an appropriate policy check box, and then click the **Delete** button.
   The policy gets deleted from the list.

Viewing General Policy Settings

The **General** tab enables you to view general policy settings for managed computers.

To view general policy settings

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 79.

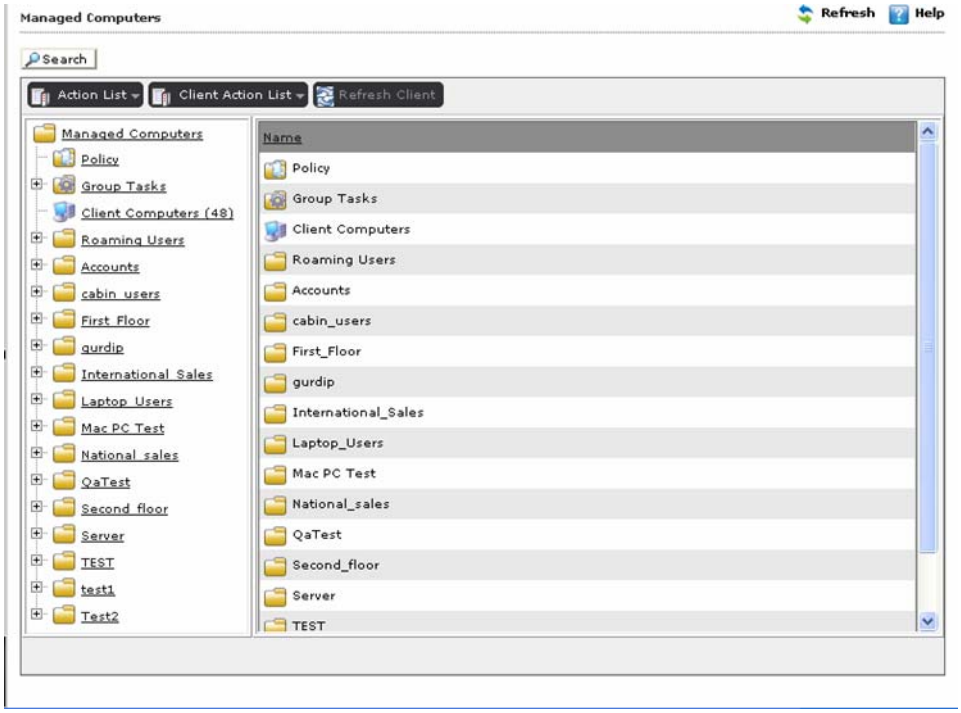


Figure 79

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

2. On the left pane, under an appropriate managed computers folder, click **Policy**.

The Policy **screen appears. Refer**

3. Figure 80.

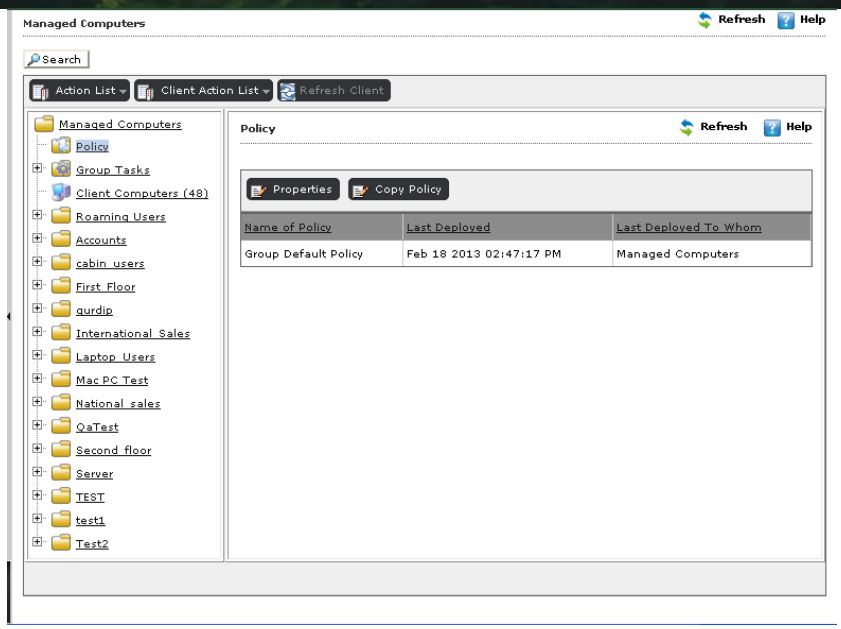


Figure 80

4. Click the **Properties** button.

The Properties **window appears. Refer**

5. Figure 81.

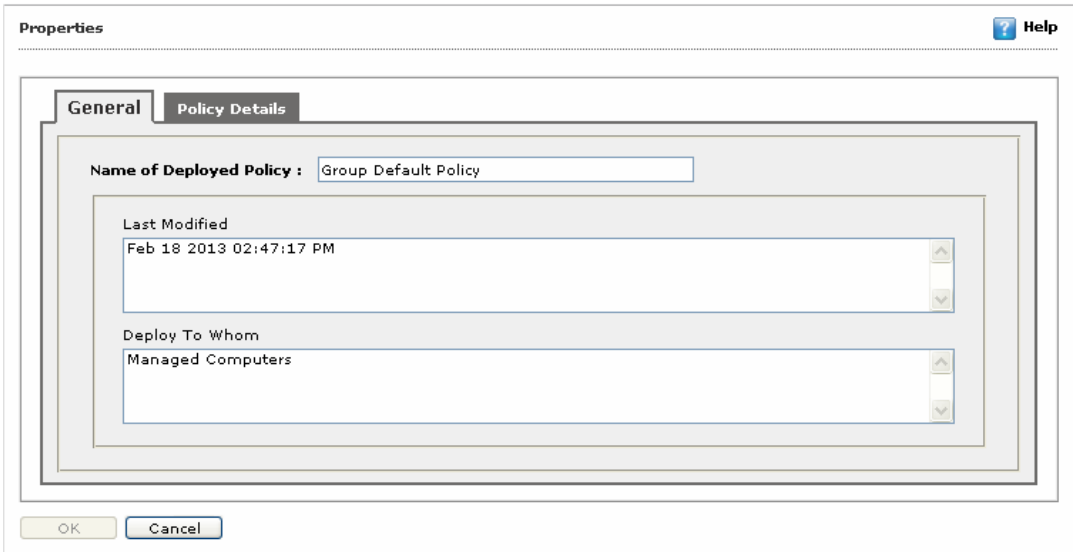


Figure 81

6. The **General** tab appears by default.
7. By default, Group Default Policy appears in the **Name of Deployed Policy** field, it indicates name of the policy.
8. In the **Last Modified** section, you can view the details of when and at what time the last policy is deployed.
9. In the **Deploy To Whom** section you can view the name of the group on which the policy is deployed.
10. View the details as required.

Configuring Policy Details

The Policy Details tab enables you to configure policy details for managed computers. You can modify and configure settings for all the available modules by selecting the appropriate check boxes.

To configure policy details

1. On the navigation pane, click **Managed Computers**.
   The **Managed Computers** screen appears. Refer Figure 79.

   Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

2. On the left pane, under an appropriate managed computers folder, click **Policy**.

   The Policy **screen appears. Refer**

   Figure 80.

3. Click the **Properties** button.

   The **Properties** window appears. By default, **General** tab appears.

4. Click the **Policy Details** tab.

   The **Policy Details** tab appears. Refer Figure 82.

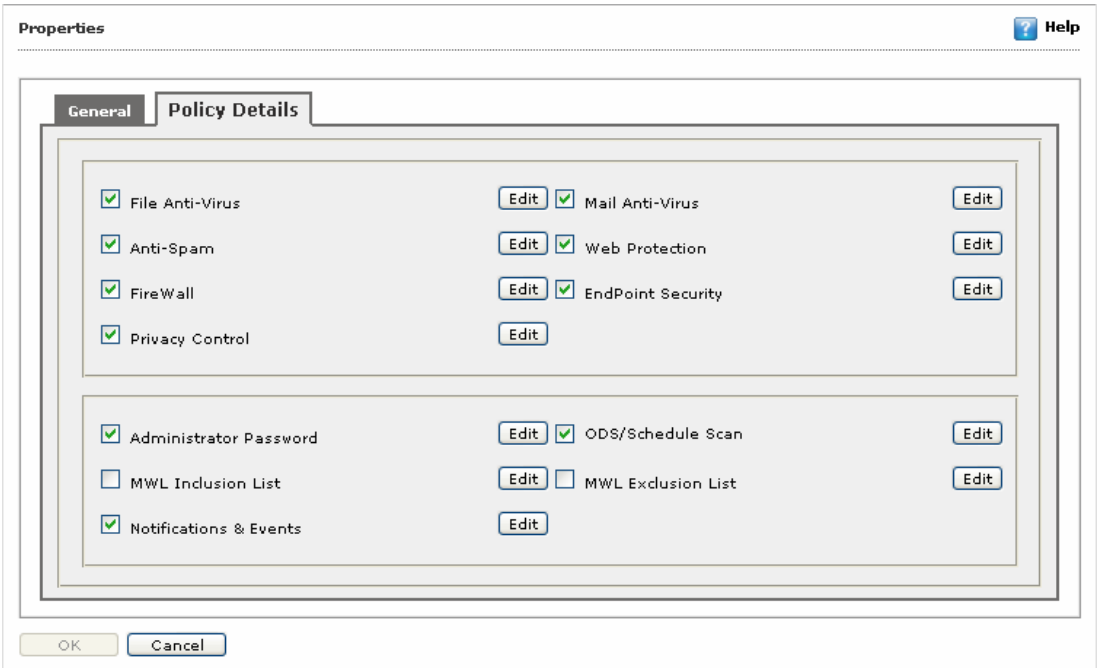


Figure 82

5. Select an appropriate check box, and then click the **Edit** icon, if you want to view and configure settings.
6. Select the **Apply for all subgroups** check box, if you want to apply settings to all subgroups.
7. Click the **OK** button.

Chapter 7: Configuring Outbreak Notification Settings

You can use the **Outbreak Notifications** page to configure the frequency of outbreak alert notifications. To enable alerts, you should ensure that the **Send notification for viruses detected exceed the following number within the shown time** check box is enabled. If the virus occurrence exceed than the number specified an alert will be generated and will be sent to the specified email address.

The steps to configure the outbreak notification settings are as follows:

1. To send notifications when the number of viruses detected exceeds a given threshold, on the Outbreak Notification page, under Outbreak Alert Settings, select the Send notification for viruses detected exceed the following number within the shown time check box. Refer Figure 83.

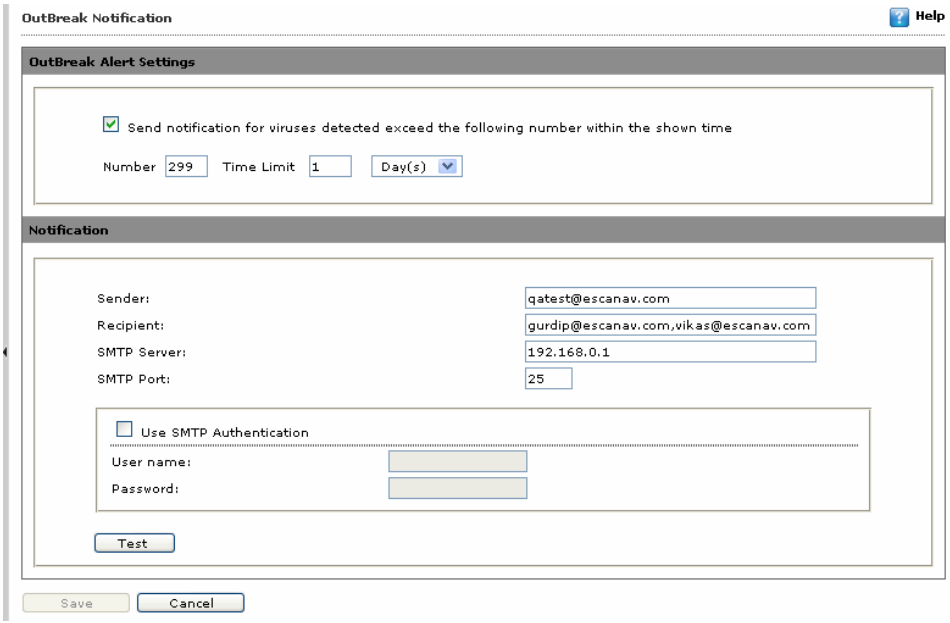


Figure 836

2. To specify the number, in the **Number** box, type the number.
3. In the **Time Limit** box, specify the value, and in the drop-down list, select either **Day(s)** or **Hour(s)** based on your requirements.

4. Under **Notification** section, specify the following field details.

Field	Description
Notification	
This section is available only when you select **Send notification for viruses detected exceed the following number within the shown time** check box.	
Sender	Type email ID of the sender.
Recipient	Type email ID of the recipient.
SMTP Server	Type name of the SMTP server.
SMTP Port	Type the SMTP port number.
Use SMTP Authentication	Select this check box, if you want to mention authentication details.
User name	This field is available only when you select **Use SMTP Authentication** check box. Type the user name.
Password	This field is available only when you select **Use SMTP Authentication** check box. Type the password.
Test	Click this button to test the connection. And send a test email

5. Click the **Save** button.

   The settings get saved.

Chapter 8: Managing Reports & Notifications

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 existing reports based on predefined reports, and customize existing reports for computers or for a group of computers. You can do the following activities:

- Creating New Template for Report
- Viewing the Properties of a Report
- Creating Notification Settings

Creating New Template for Report

It enables you to create new template for reports. There are various types of report, and every report has different options to schedule. The options under Report Period & Sort By section changes depending upon the report type that you select under Report Template section. You can generate report for both groups and computers.

To create new template for report

On the navigation pane, click Report Templates**.**
The Report Templates **screen appears. Refer**

1. Figure 84.

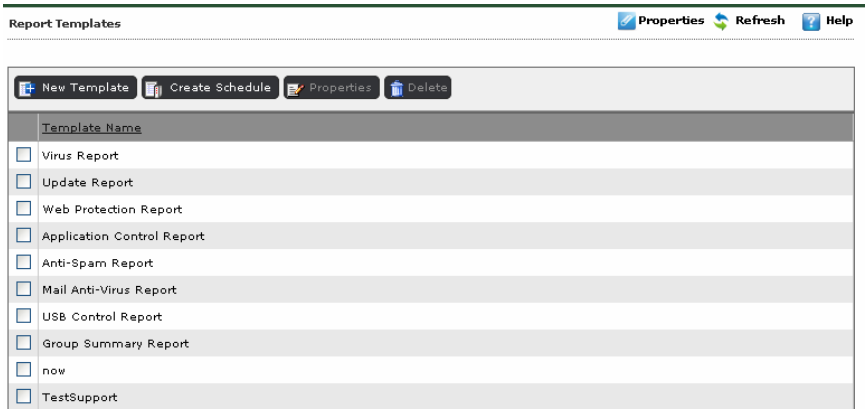


Figure 84

2. Click the **New Template** button.

The New Template **screen appears. Refer**

Figure 85.

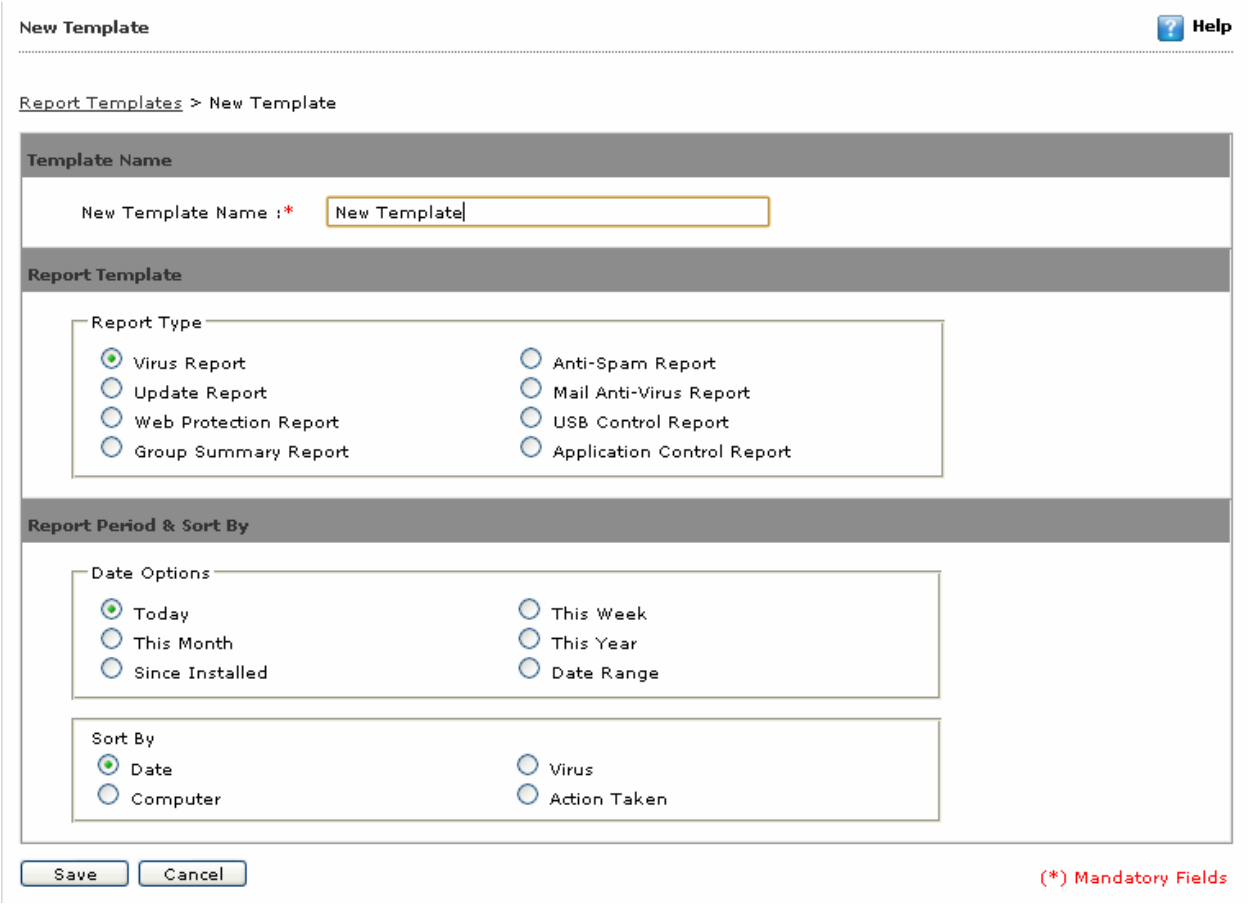


Figure 85

3. Under **Template Name** section, in the **New Template Name** field, type the template name.

4. Under **Report Template** section, specify the following field details.

Field	Description
Report Type	
Virus Report	Click this option, if you want to create template for virus report. When you click this option, under **Report Period & Sort By** section. • **Date Options** section: These options are available – **Today**, **This Week**, **This Month**, **This Year**, **Since Installed**, and **Date Range**. • **Sort By** section: These options are available – **Date**, **Virus**, **Computer**, and **Action Taken**.
Anti-Spam Report	Click this option, if you want to create template for Anti-Spam report. When you click this option, under **Report Period & Sort By** section. • **Date Options** section: These options are available – **Today**, **This Week**, **This Month**, **This Year**, **Since Installed**, and **Date Range**. • **Sort By** section: These options are available – **Date**, **Action Taken**, and **Computer**.
Update Report	Click this option, if you want to create template for update report. When you click this option, the **Report Period & Sort By** section becomes unavailable.
Main Anti-Virus Report	Click this option, if you want to create template for Anti-Spam report. When you click this option, under **Report Period & Sort By** section. • **Date Options** section: These options are available – **Today**, **This Week**, **This Month**, **This Year**, **Since Installed**, and **Date Range**. • **Sort By** section: These options are available – **Date**, **Action Taken**, and **Computer**.
Web Protection Report	Click this option, if you want to create template for virus report. When you click this option, under **Report Period & Sort By** section.

Field	Description
	• **Date Options** section: These options are available – **Today**, **This Week**, **This Month**, **This Year**, **Since Installed**, and **Date Range**. • **Sort By** section: These options are available – **Date**, **Websites**, **Computer**, and **Action Taken**.
USB Control Report	Click this option, if you want to create template for Anti-Spam report. When you click this option, under **Report Period & Sort By** section. • **Date Options** section: These options are available – **Today**, **This Week**, **This Month**, **This Year**, **Since Installed**, and **Date Range**. • **Sort By** section: These options are available – **Date**, **Action Taken**, and **Computer**.
Application control Report	Click this option, if you want to create template for virus report. When you click this option, under **Report Period & Sort By** section. • **Date Options** section: These options are available – **Today**, **This Week**, **This Month**, **This Year**, **Since Installed**, and **Date Range**. • **Sort By** section: These options are available – **Date**, **Application**, **Computer**, and **Action Taken**.
Report Period & Sort By	
Date Options	Click an appropriate option. For example, Today, This Week, This Month, and so on. The options changes depending upon the report type.
Sort By	Click an appropriate option. For example, Date, computer, and so on. The options changes depending upon the report type.

5. Click the **Save** button. The template gets created.

Viewing the Properties of a Report

You can view all the properties of a report. In addition, you can also view summary of the report depending on the report type, in a graphical format, showing the number of viruses found in a virus report, number of times the updates done on a specific computer in a update report, and so on.

To view the properties of a report

1. On the navigation pane, click **Report Templates**.The **Report Templates** screen appears. Refer Figure .

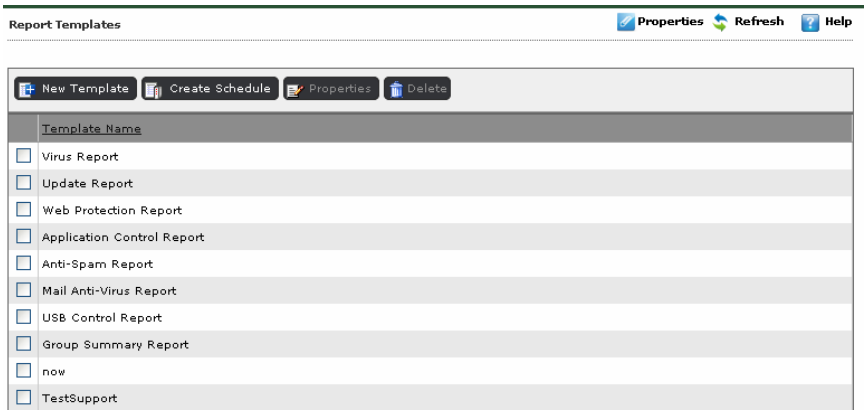


Figure 89

2. On the **Report Template** screen, select an appropriate template check box of which you want to view the properties, and then click **Properties**.The **Properties** screen appears. Refer Figure 90.

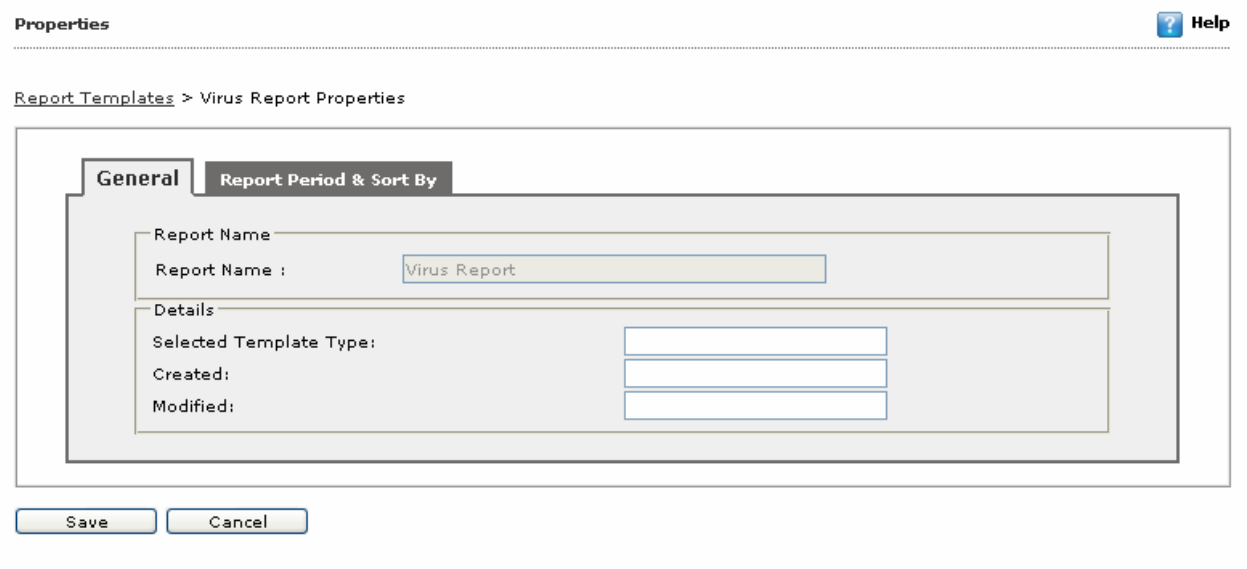


Figure 90

3. The **General** tab appears by default.
4. Click the Report Period & Sort By tab.

   The Report Period & Sort By tab appears.

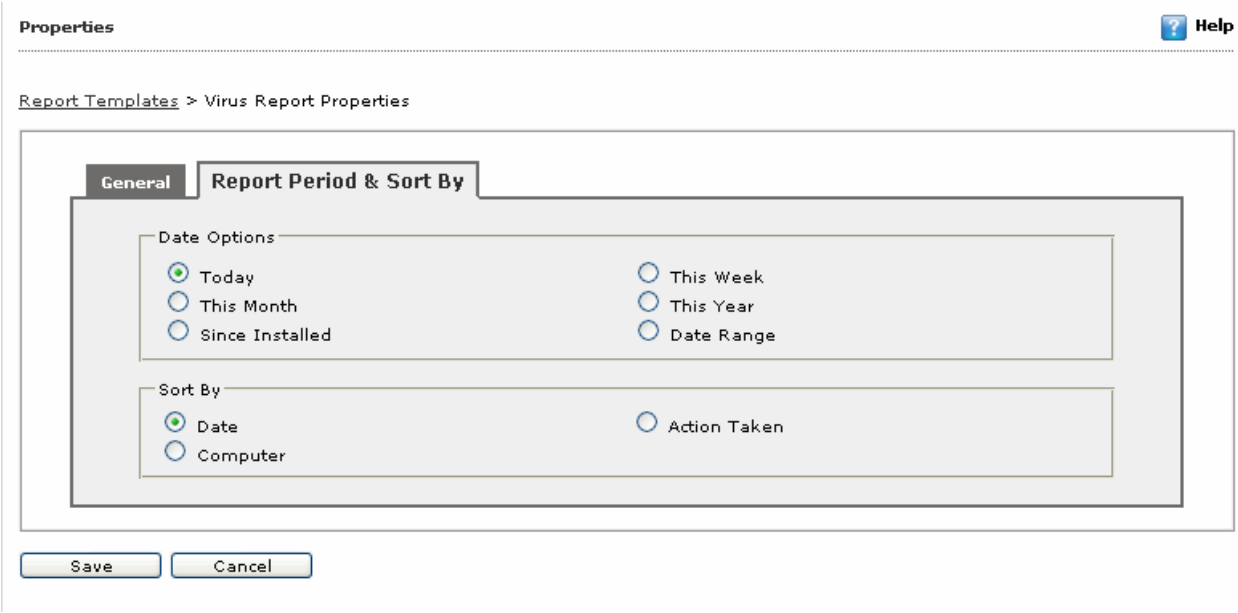


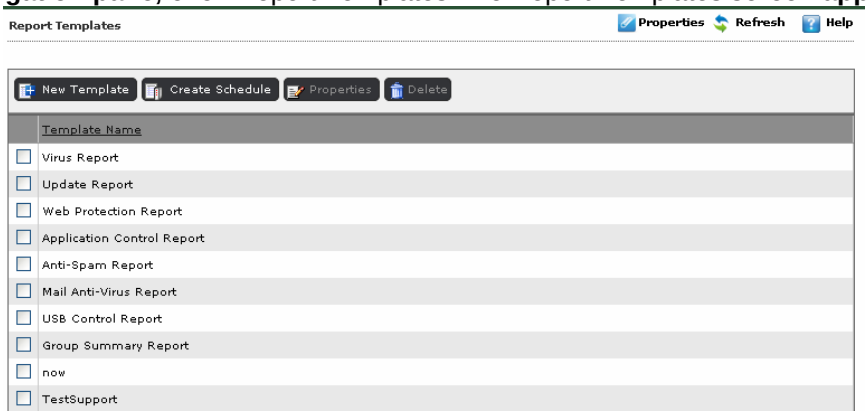
Figure 91

5. View the details as required, and you can also modify the details, if required.
6. Click the **Save** button.

Creating Notification Settings

It enables you to create and save notification settings, which helps you to send reports to the recipient. Perform the following steps:

On the navigation pane, click Report Templates**.The** Report Templates s**creen appears. Refer**



1. Figure .

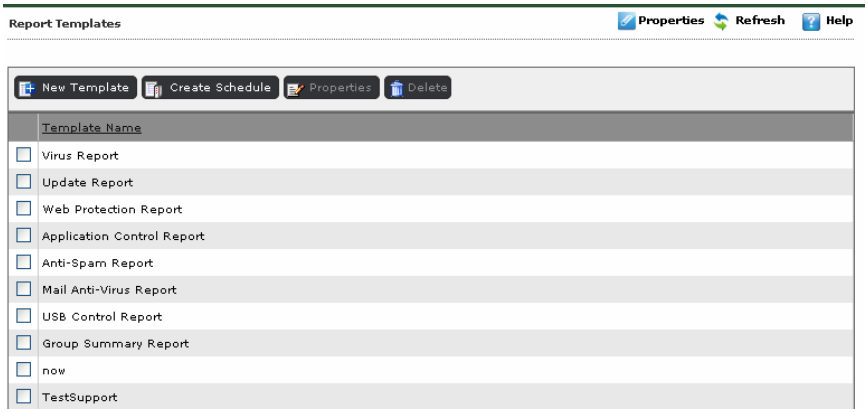


Figure 92

2. Click the 

button, on upper-right side of the screen.

The Properties **screen appears. Refer**

3. Figure .

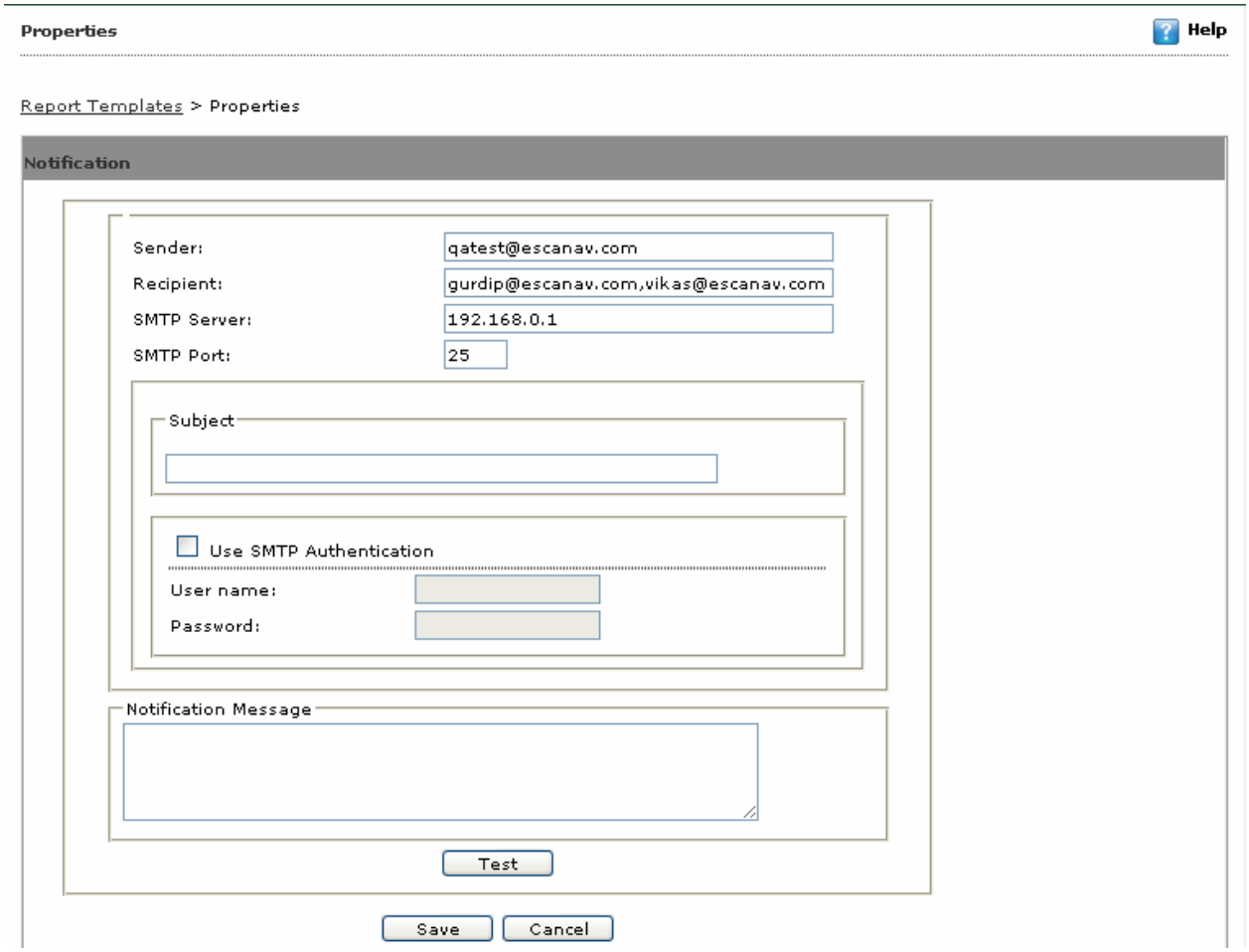


Figure 96

4. Specify the following field details.

Field	Description
Notification	
Sender	Type email ID of the sender.
Recipient	Type email ID of the recipient.
SMTP Server	Type name of the SMTP server.
SMTP Port	Type the SMTP port number.
Subject	Type subject of the email.
Use SMTP Authentication	Select this check box, if you want to mention authentication details.
User name	This field is available only when you select **Use SMTP Authentication** check box. Type the user name.
Password	This field is available only when you select **Use SMTP Authentication** check box. Type the password.
Notification Message	Type the notification message, if any.

5. Click the **Test** button, to test the connection.

   A message of successful connection and sending of notification appears.

6. Click the **Save** button. The settings get saved.

Chapter 9: Scheduling Reports

The new eScan Web Console not only has a comprehensive reporting feature but it also supports the scheduling of reports.

This means that administrators can automate the task of creating reports by simply creating a report generation schedule on the eScan Web Console. Based on the settings, the eScan Web Console will generate the report on the specific day and time and then send it to the specified recipients or save the reports to a shared folder for easy access.

Create a New Report Creation Schedule

With the eScan Web Console, you can easily set up a report creation schedule either for a list of computers or for a computer group.

When you are a creating a new report, you must specify a name in the **New Report Name** box. This task is not the same as the one given in the **Tasks For Specific Computers** section.

There are several pre-existing reports templates available for creating reports. These are Virus Report, Web Protection Report, Anti-Spam Report, Mail Anti-Virus Report, Application Control Report, USB Control Report, and Update Report. Based on your requirements, you can choose any one of these templates.

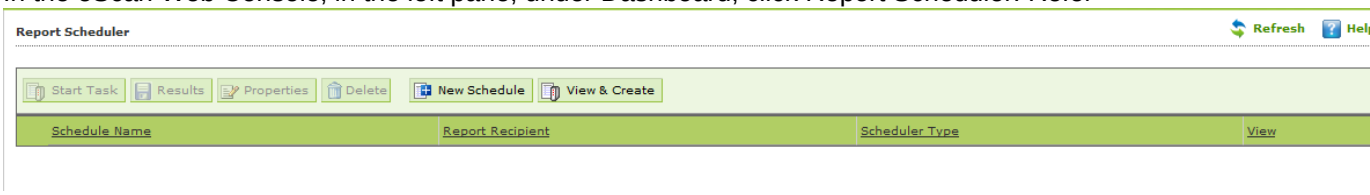
You can also create a combined report that contains information about multiple modules. For example, if you want to create a combined report for the Web Protection and Anti-Spam modules, you can do so by selecting both modules in the **Select a template for creating a report** list.

As in the case of scheduling tasks for computers, you can opt to either let the scheduler run automatically or start it manually. You can configure a task to run automatically at a given time on a specified day or week or month by selecting **Enable Scheduler** in the **Task scheduling settings** section. If you want to run the task manually, you can do so by selecting the Manual Start option and then clicking **Save**. After you have created a task, you can run it manually by clicking **Start Task** on the **Report Scheduler** page.

The details regarding newly created report schedule, such as the name of the schedule, the e-mail address of the recipient and the schedule type appears in a table on the **Report Scheduler** page.

The steps to configure a report are as follows:

In the eScan Web Console, in the left pane, under Dashboard, click Report Scheduler. Refer



1. Figure 86.

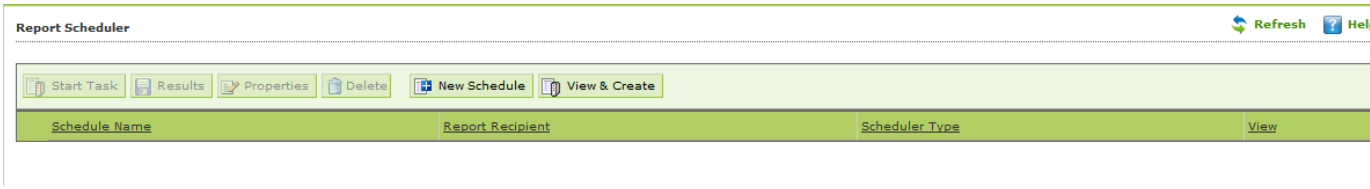
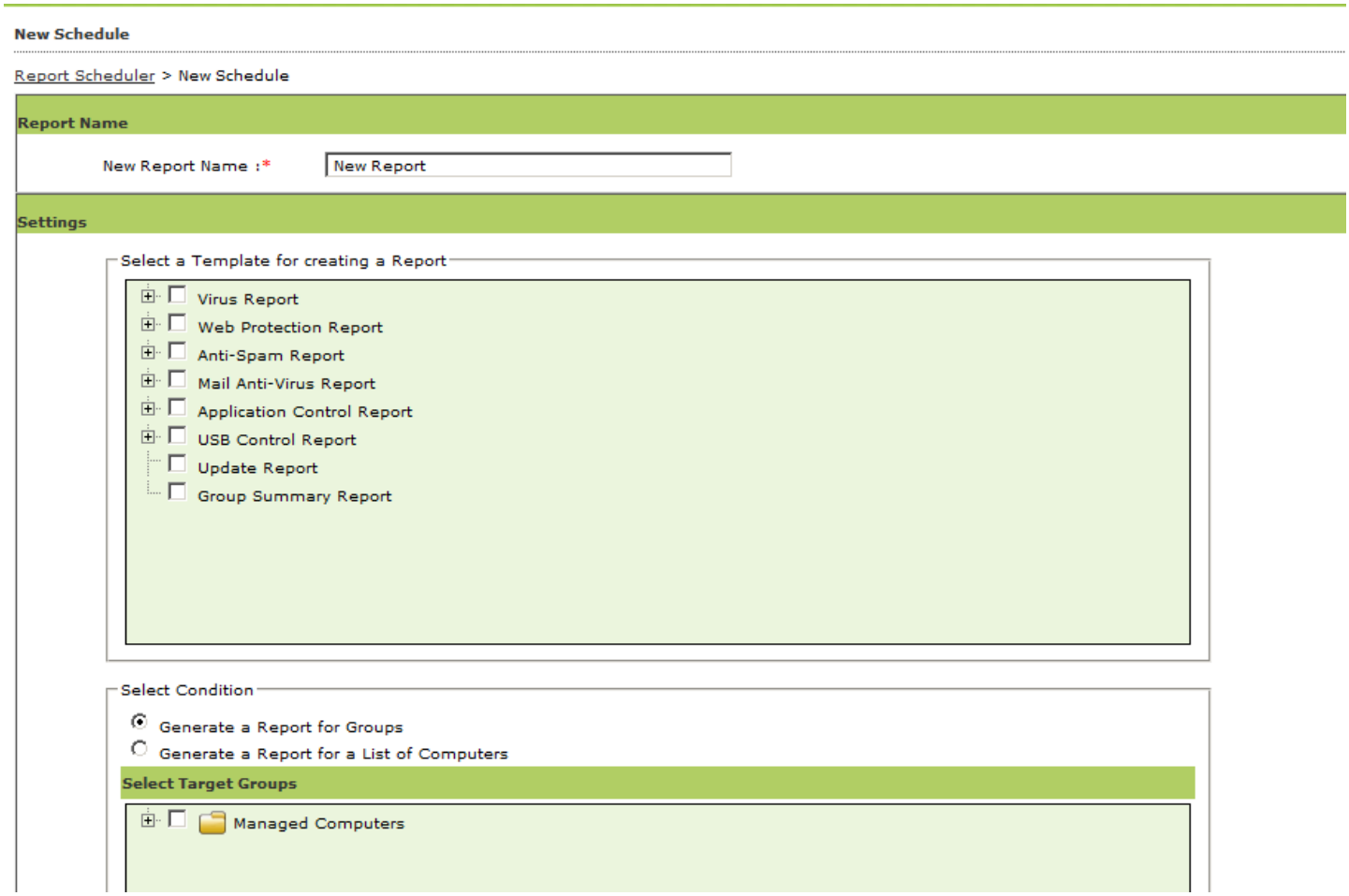


Figure 86

2. On the **Report Scheduler** page, on the right pane, click **New Schedule**.

3. The **New Schedule** screen appears. Refer



4. Figure .

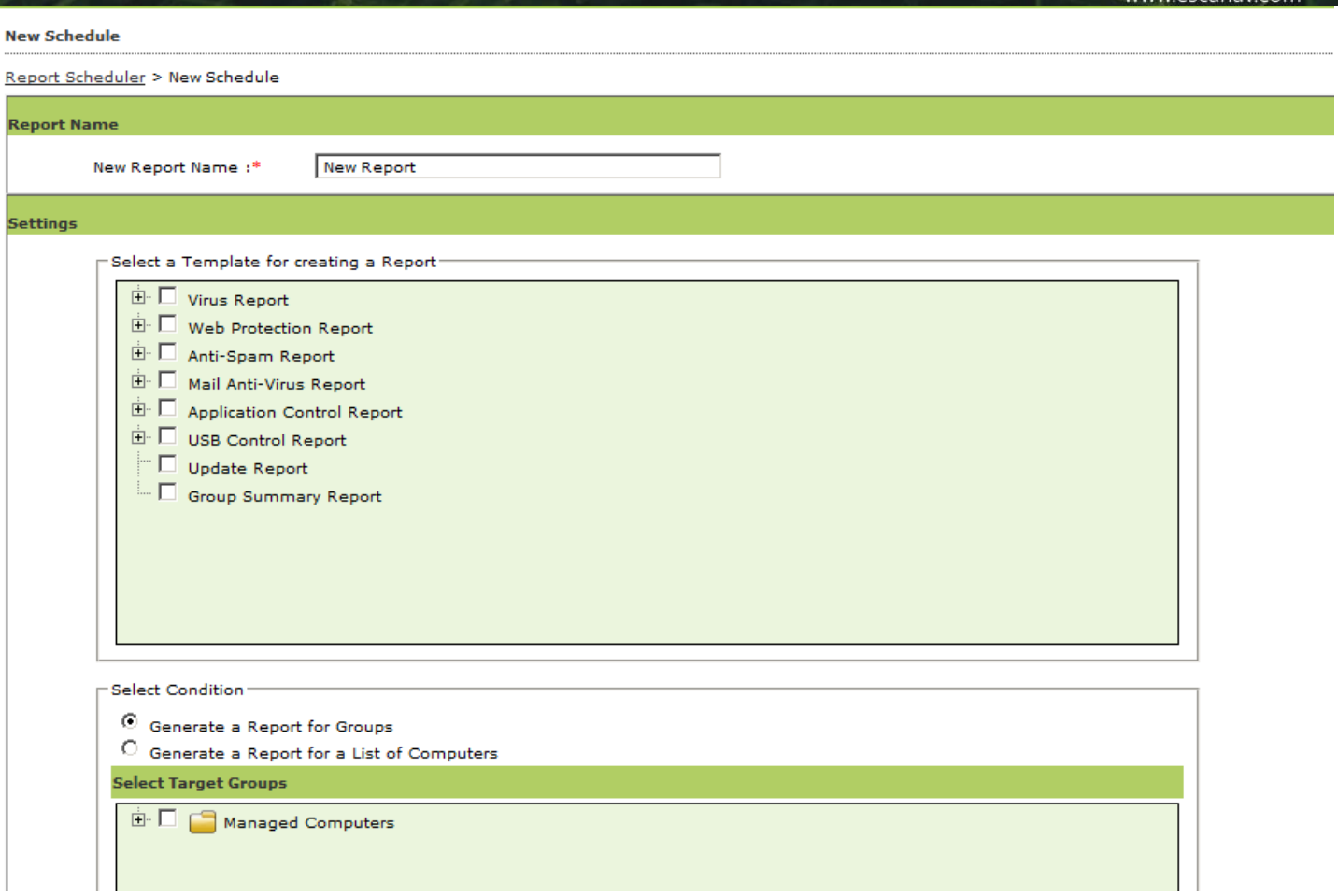

New Schedule
Report Scheduler > New Schedule
Report Name
New Report Name :*
New Report
Settings
Select a Template for creating a Report
Virus Report
Web Protection Report
Anti-Spam Report
Mail Anti-Virus Report
Application Control Report
USB Control Report
Update Report
Group Summary Report
Select Condition
Generate a Report for Groups
Generate a Report for a List of Computers
Select Target Groups
Managed Computers

Figure 98

5. On the **New Schedule** page, under **Report Name**, in the **New Report Name** box, type a name for the task, under **Settings**, in the **Select a template for creating a report** box, select the appropriate options.

- To send the report by e-mail, select the Send report by email check box. When you select this check box, the following settings are displayed below it.
  - **Report Sender:** This box should be filled in with the e-mail address of the sender.
  - **Report Recipient:** This box should be filled in with the e-mail address of the recipients. You can use the **Add** button to add e-mail addresses as required and use the **Delete** button to remove the addresses that are not required.
  - **Mail Server IP Address:** This box should be filled in with the IP address of your mail server.
  - **Mail Server Port:** This box should be filled in with the port number used by your mail server to send e-mails. The default port is **25**.
  - **User Authentication:** This box allows you to specify the user name of the administrator.
  - **Password Authentication:** This box allows you to specify the password of the administrator.

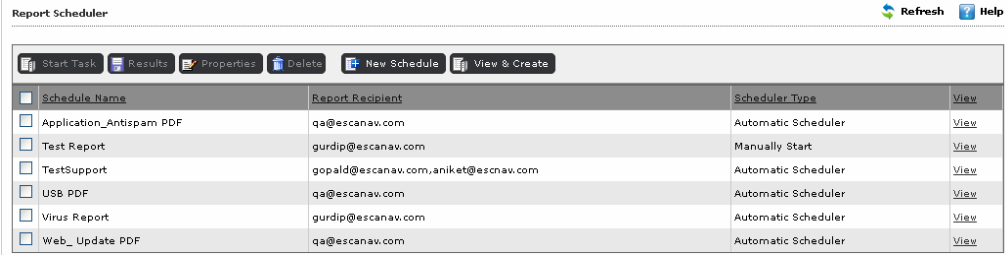
6. Select an appropriate option from the **Select the Report Format** drop-down list. For example, HTML page and Adobe PDF. (PDF is available in English Language only, and will be added to the later versions.)
7. To enable the scheduler, under **Task scheduling settings**, click **Enable Scheduler**. Alternately, you can start the scheduler manually by clicking **Manual Start**.
8. To generate reports on a daily basis, click **Daily**, else to generate report monthly, click **Weekly**, and then select the appropriate day of the week.
9. To generate reports on a monthly basis, click **Monthly**, and then select the number of months from the drop-down list.
10. Click the Time  icon.
11. The Timer appears.
    - Click the A.M. tab to view the before noon time and P.M. tab to view the afternoon time, and then select an appropriate time from the list.
    - To save the report and create a scheduled task, click **Save**.

Start an Existing Report Generation Task

Sometimes, you may need to view a report for a given module or multiple modules. And, it may also happen that you have already created a task for generating that report. In such case, you do not need to wait until the report gets generated. All you have to do is, run the report generation task manually by clicking Start Task.

The steps to run an existing task manually are as follows:

In the eScan Web Console, in the left pane, under Dashboard**, click** Report Scheduler**. Refer**



1. Figure 87.

Figure 879

2. On the **Report Scheduler** page, on the right pane, in the table, select the check box next to the name of the task that you want to run, and then click **Start Task**.

The Task **window appears displaying the status of running task. Refer**

3. Figure .

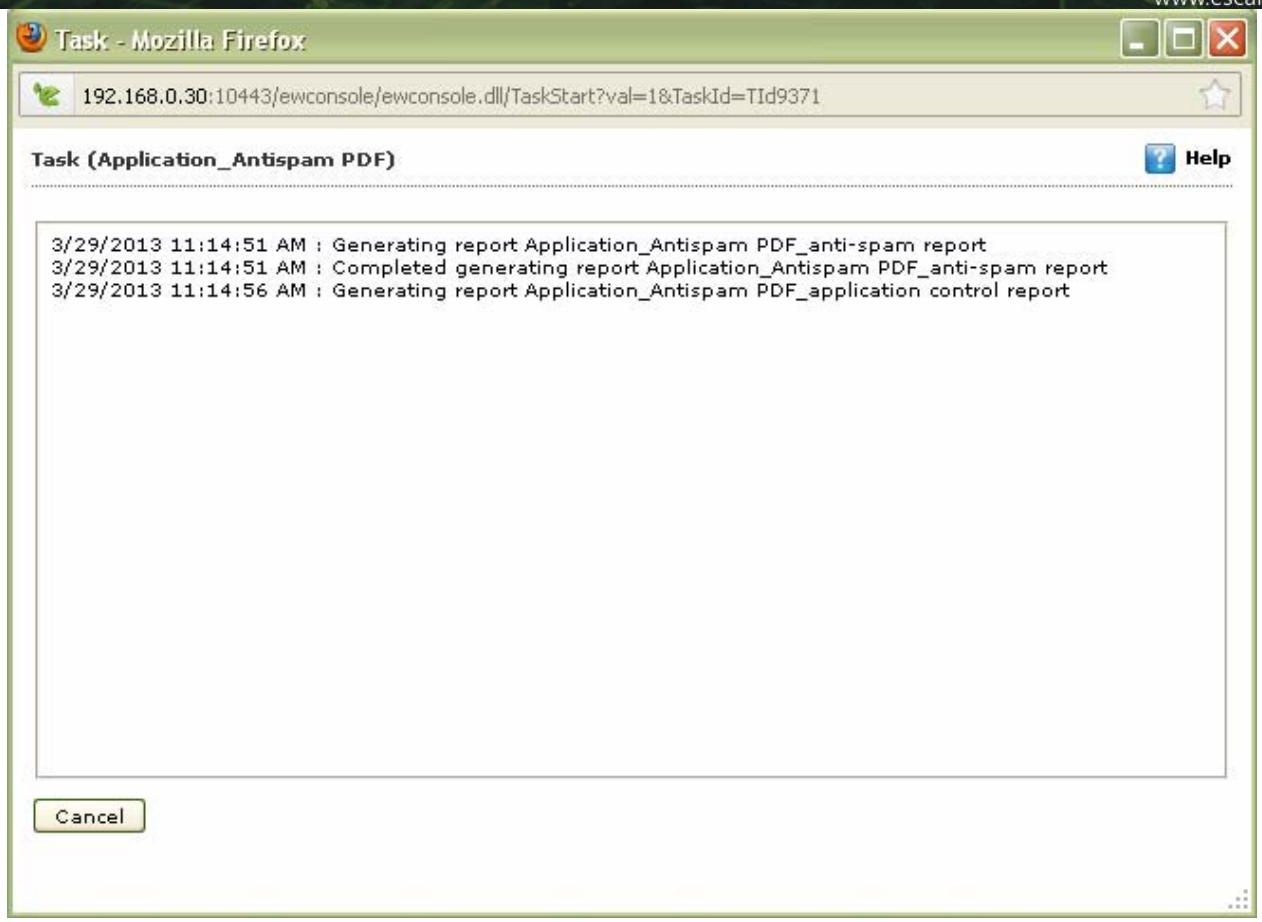


Figure 100

4. Click **Close** button, to close the window.

View the Status of Report Creation Schedules

You can view the status of scheduled tasks or the tasks that you have run manually by clicking **Results**. This opens the **Results** page, which displays the details of the client computer, the group to which it belongs, the status of completion of tasks on it, and the timestamp. In addition, it also displays the status and timestamp of the tasks that have been executed on it in a tabular format.

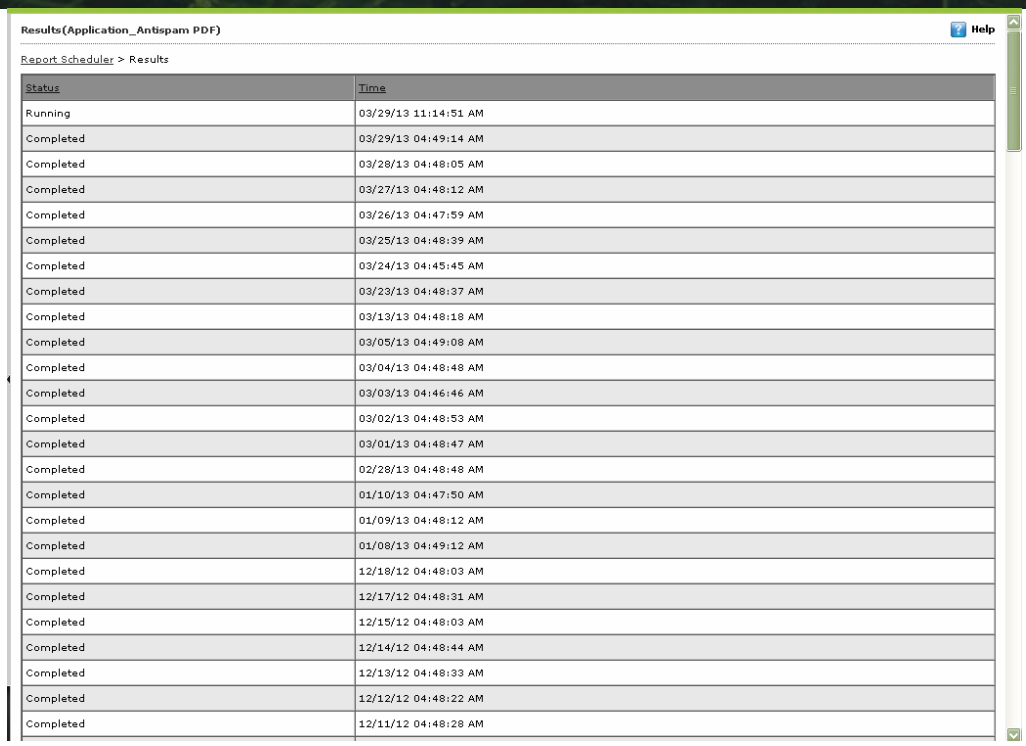
The steps to view the result of running a task are as follows:

In the eScan Web Console, in the left pane, under Dashboard**, click** Report Scheduler**. Refer**

1. Figure 87.

On the Report Scheduler**, on the right pane, in the table, select the check box next to the name of the task whose results you want to view, and then click** Results**.**
The Results **screen appears. Refer**

2. Figure .



Status	Time
Running	03/29/13 11:14:51 AM
Completed	03/29/13 04:49:14 AM
Completed	03/28/13 04:48:05 AM
Completed	03/27/13 04:48:12 AM
Completed	03/26/13 04:47:59 AM
Completed	03/25/13 04:48:39 AM
Completed	03/24/13 04:45:45 AM
Completed	03/23/13 04:48:37 AM
Completed	03/13/13 04:48:18 AM
Completed	03/05/13 04:49:08 AM
Completed	03/04/13 04:48:48 AM
Completed	03/03/13 04:46:46 AM
Completed	03/02/13 04:48:53 AM
Completed	03/01/13 04:48:47 AM
Completed	02/28/13 04:48:48 AM
Completed	01/10/13 04:47:50 AM
Completed	01/09/13 04:48:12 AM
Completed	01/08/13 04:49:12 AM
Completed	12/18/12 04:48:03 AM
Completed	12/17/12 04:48:31 AM
Completed	12/15/12 04:48:03 AM
Completed	12/14/12 04:48:44 AM
Completed	12/13/12 04:48:33 AM
Completed	12/12/12 04:48:22 AM
Completed	12/11/12 04:48:28 AM

Figure 101

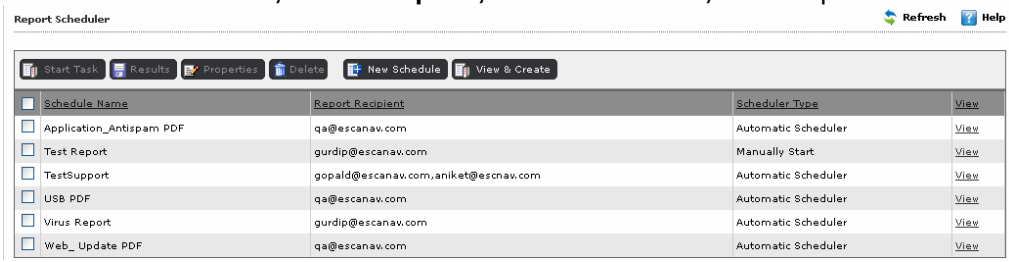
3. View the details as required.

Configure the Properties of an Existing Report Creation Task

You can configure the properties of existing task by clicking the task name and then clicking Properties. These properties include the name of the report, the date of creation, date of modification, sort criteria, and the available groups.

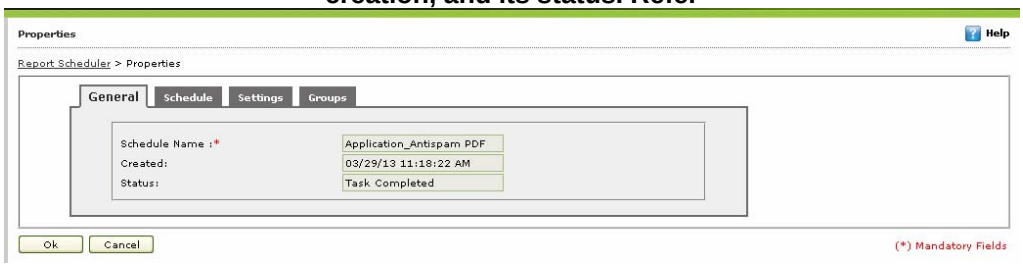
The steps to configure the properties of an existing report creation task are as follows:

In the eScan Web Console, in the left pane, under Dashboard**, click** Report Scheduler**. Refer**



1. Figure 87.
2. On the **Report Scheduler** page, on the right pane, in the table, select the check box next to the name of the report that you want to configure, and then click **Properties**.
3. On the **Properties** page:

The General tab, shows you the name of the schedule, and details regarding the report such as the date of creation, and its status. Refer



- Figure .

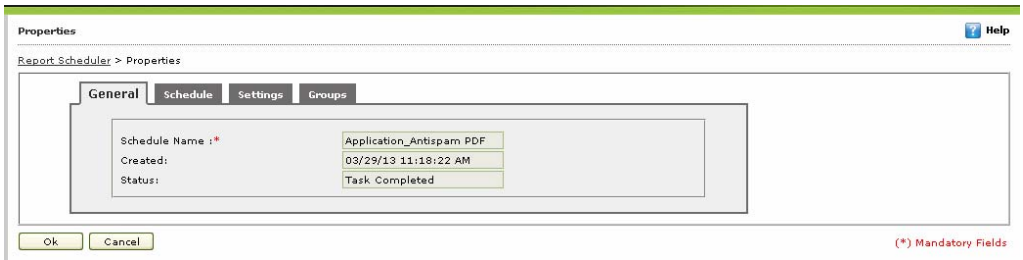
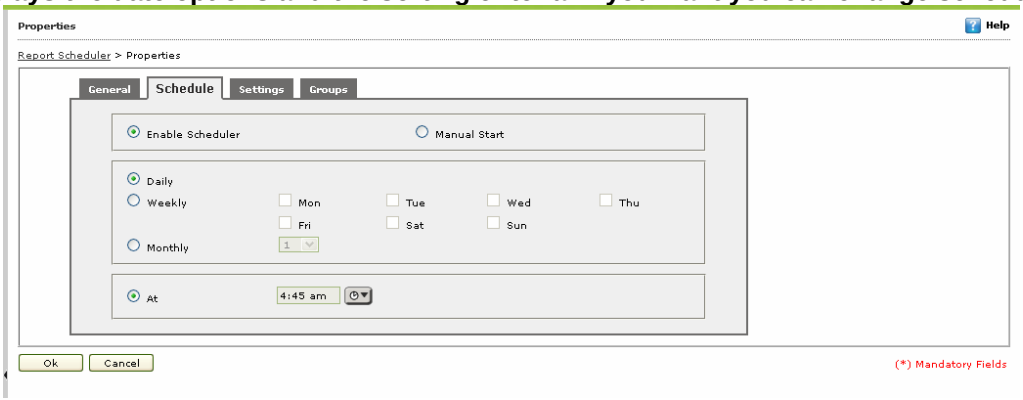


Figure 102

The Schedule tab displays the date options and the sorting criteria. If you want you can change schedule of the report. Refer



- Figure .

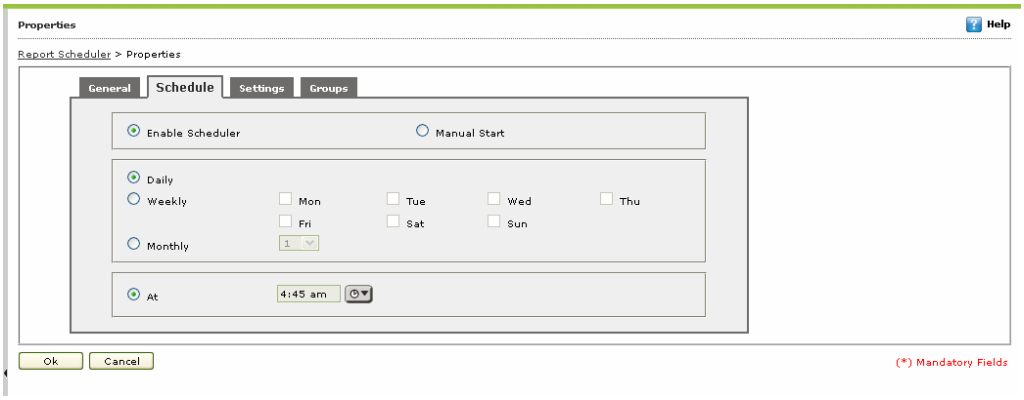
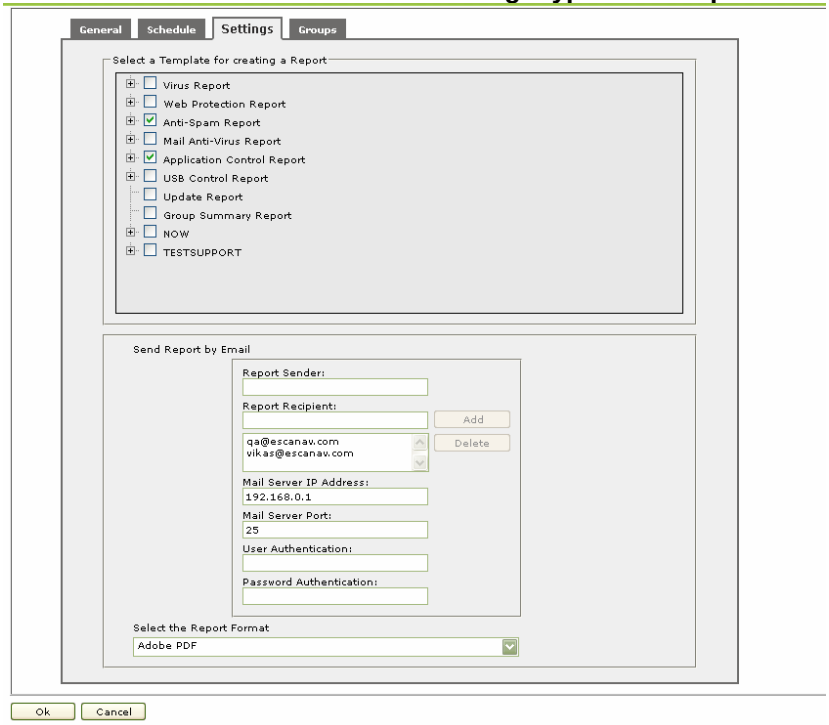


Figure 103

The Settings tab displays the template used for creating the report, the settings required for sending the report via e-mail such as the e-mail addresses of the sender and the recipients; the IP address and port of the mail server; and authentication information. This tab also displays the path of the shared folder in which

the report needs to be saved. You can also change type of the report format. Refer



- Figure .

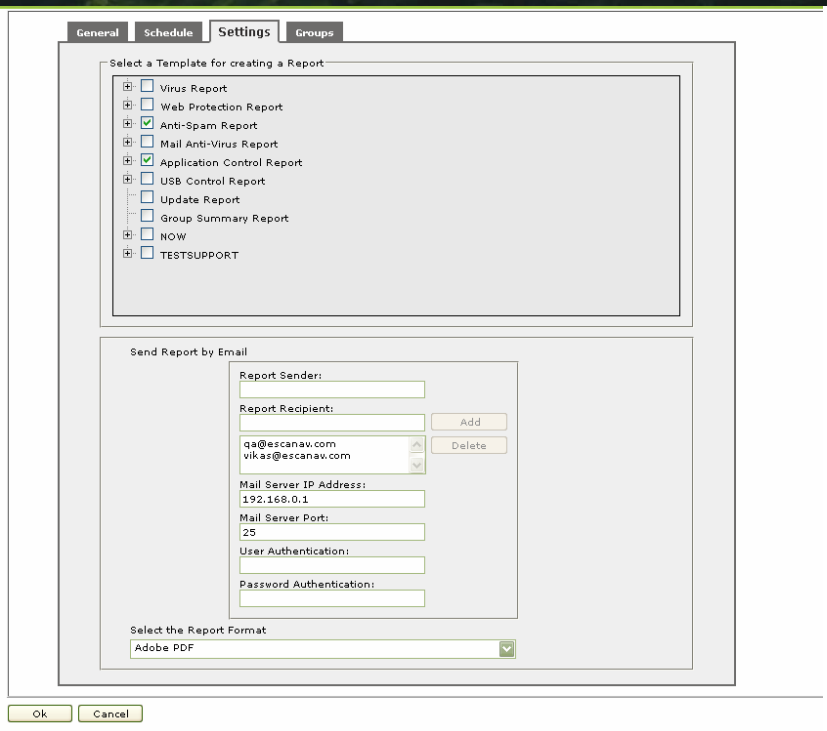


Figure 104

- The **Groups** tab helps you to Add Managed Computers for scheduling Task for Report Creation on the basis of the created groups**. See Figure 105**

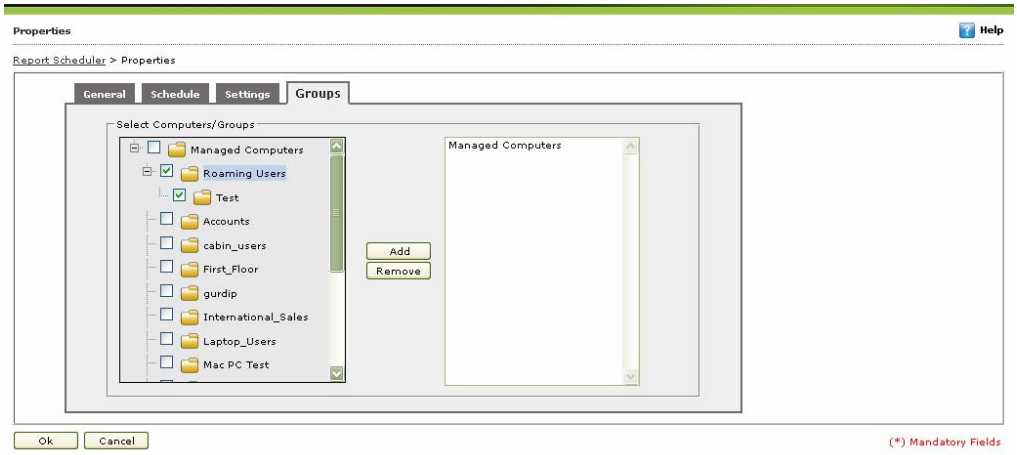


Figure 105

4. To save and close the **Properties** page, click **Ok**.

Chapter 10: Managing Events & Computers

The **Events & Computers** page enables you to monitor various activities performed on client's computer. You can save, edit settings, and also can view log of all events based on certain criteria's and settings defined. You can do the following activities:

- Settings
- Edit Selection
- Viewing Event List

Settings

The Settings enables you to create and save settings of events, computer selection as per different criteria's, and making certain settings in software/ hardware for getting updates, in case if any changes are made related to software, hardware, or existing system. You can change the following settings:

- Event Status
- Computer Selection
- Software/ Hardware Changes

Event Status

Basically, events are activities performed on client's computer. There are three types of event status – Recent, Critical, and Information. You can select the status as per your requirement. The Events Status tab enables you to do the following activities:

- Types of Event Status
- Saving Event Status Settings

Types of Event Status

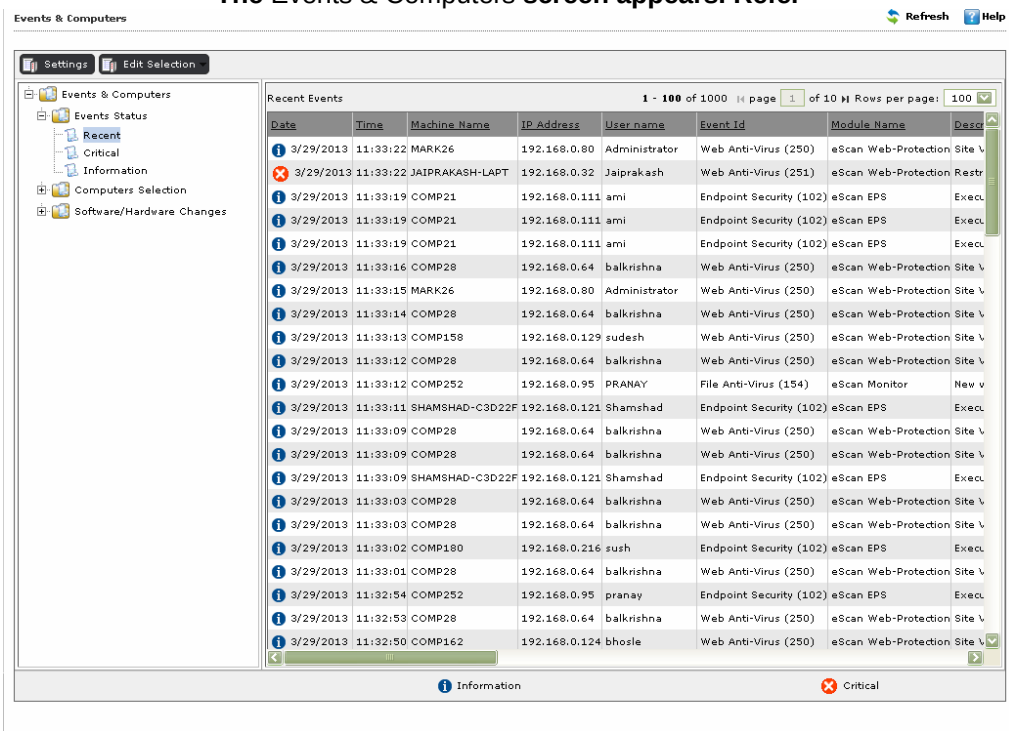
On the basis of severity, that is, the level of importance, events are categorized in to the following three types:

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

Saving Event Status Settings

Perform the following steps to save the event status settings:

On the navigation pane, click Events & Computers**.**
The Events & Computers **screen appears. Refer**



1. Figure 10688.

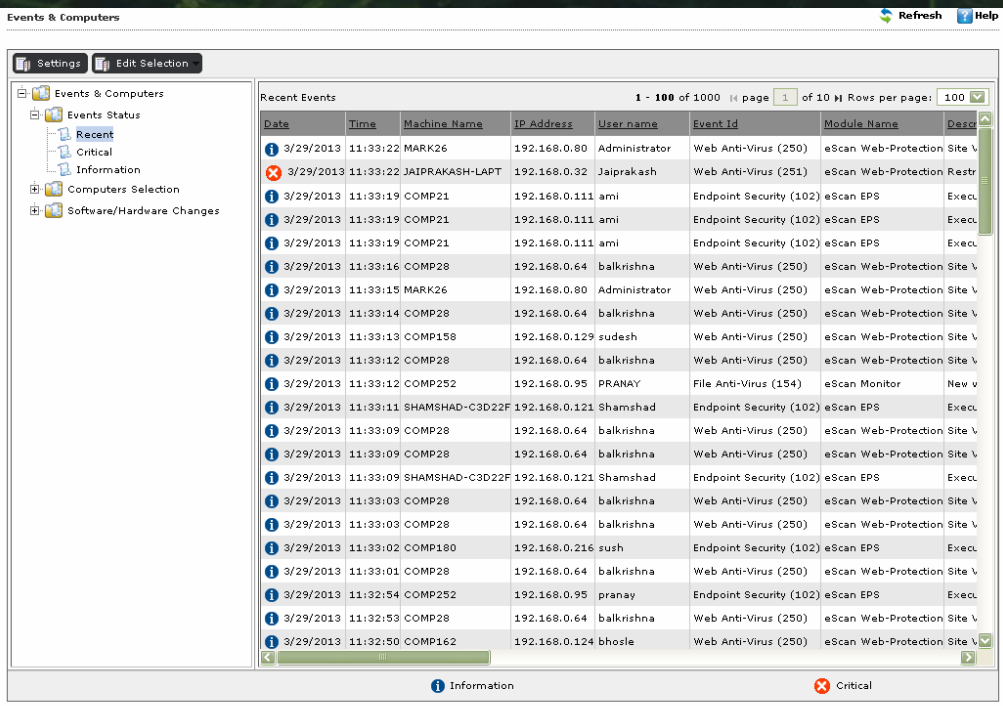
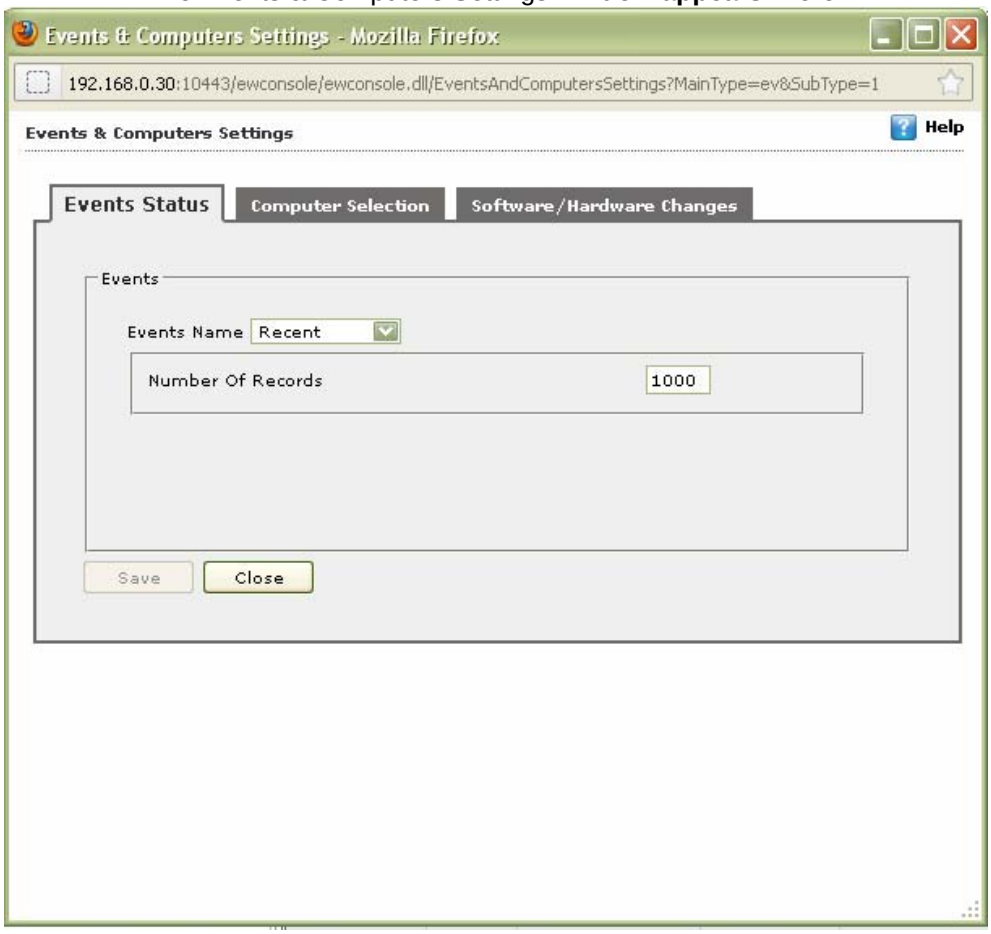


Figure 10688

Click the Settings **button.**
The Events & Computers Settings **window appears. Refer**



2. Figure .

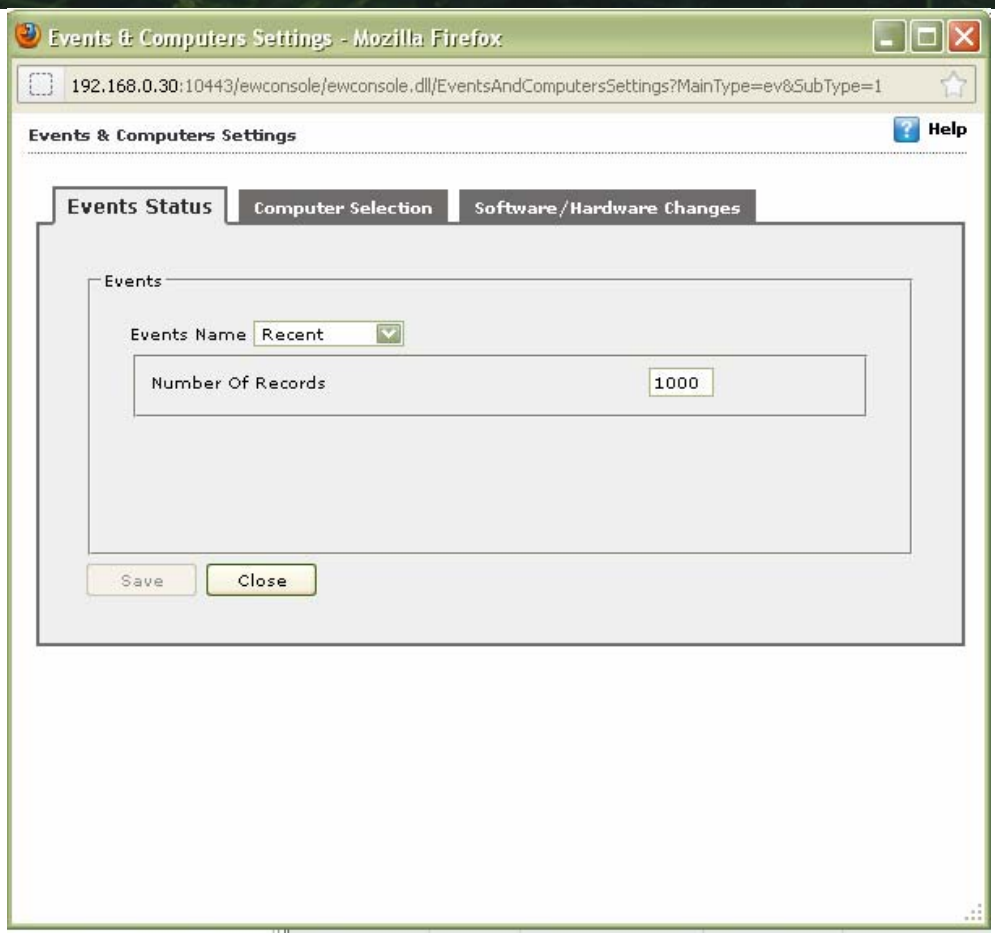


Figure 107

3. Select type of event from the **Event Name** drop-down list.
4. Type the number of events that you want to view in a list, in the **Number of Records** field.
5. Click the **Save** button.
   The settings get saved.

Computer Selection

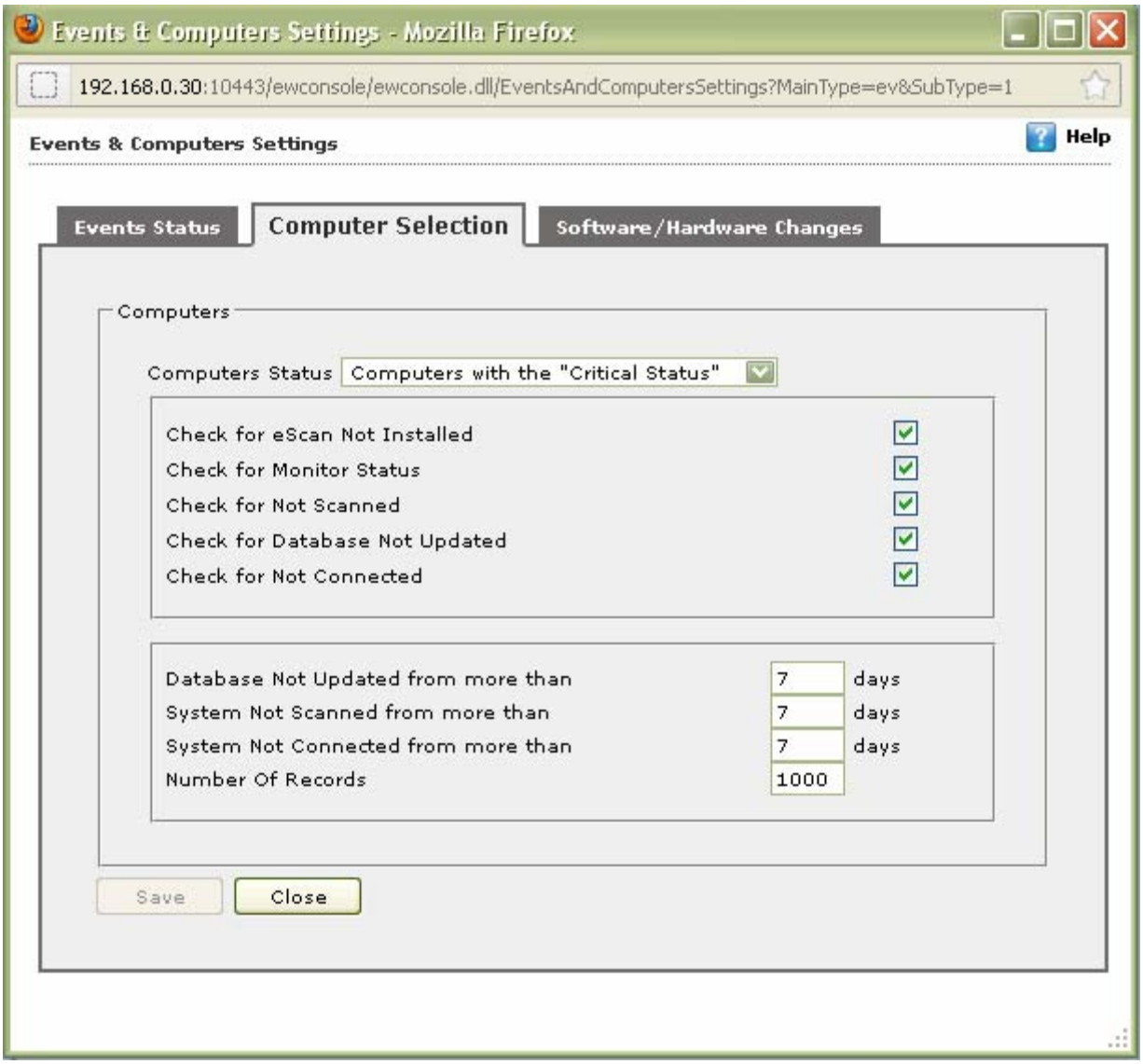
The **Computer Selection** tab enables you to select and save the computer status settings. This module enables you to do the following activities:

- Types and Criteria's of Computer Status
  - Computers with the "Critical Status"
  - Computers with the "Warning Status"
  - Database are Outdated
  - Many viruses Detected
  - No eScan Antivirus Installed
  - Not connected for a long time
  - Not scanned for a long time
  - Protection is off
- Saving Computer Settings

Types and Criteria's of Computer Status

Each computer status has different criteria's, which you can set according to your requirement. The lists of computer status with its criteria are as follows:

Computers with the "Critical Status": It displays the list of systems which are critical in status, as per the criteria's selected in computer settings. Refer



- Figure .

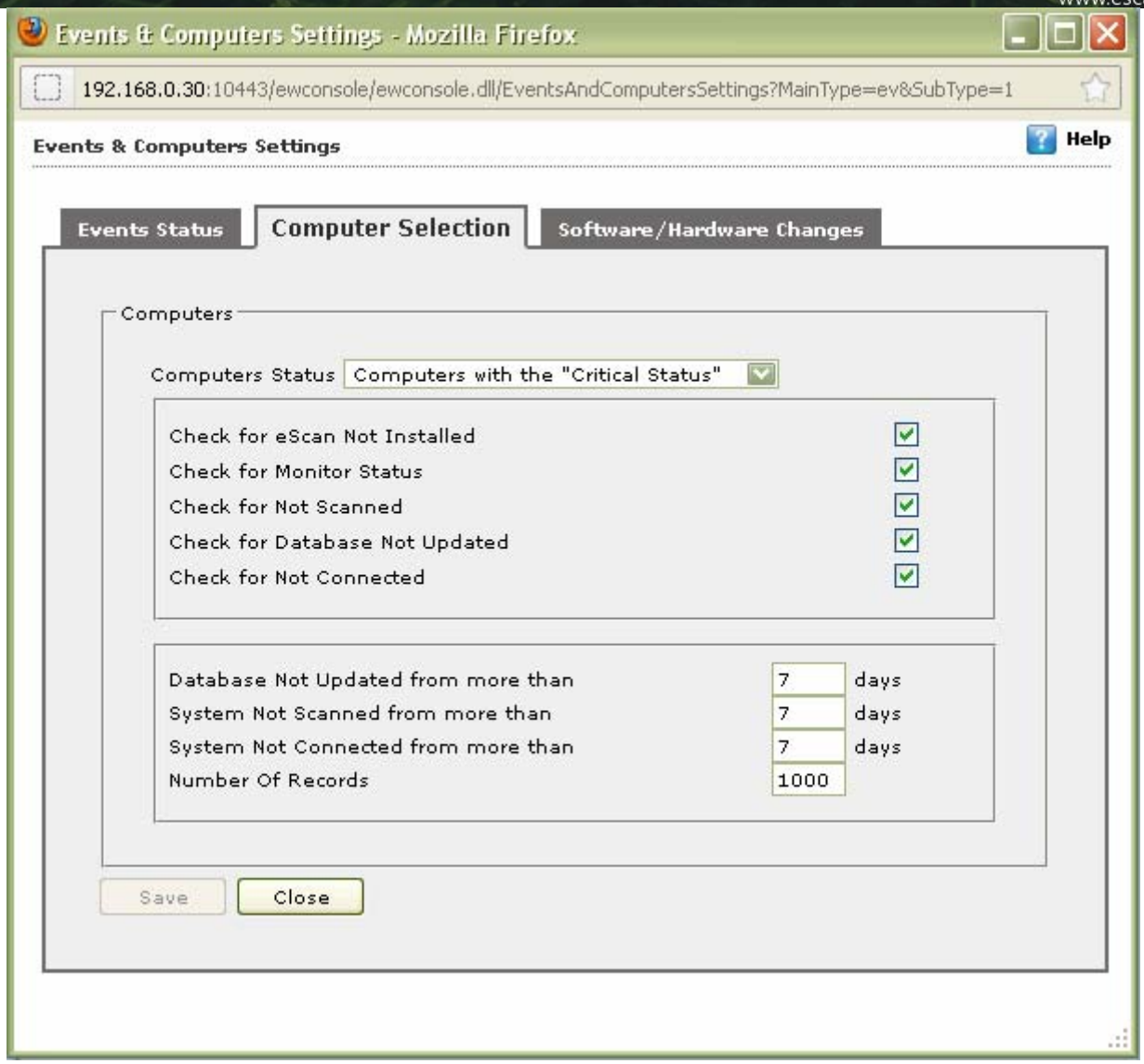
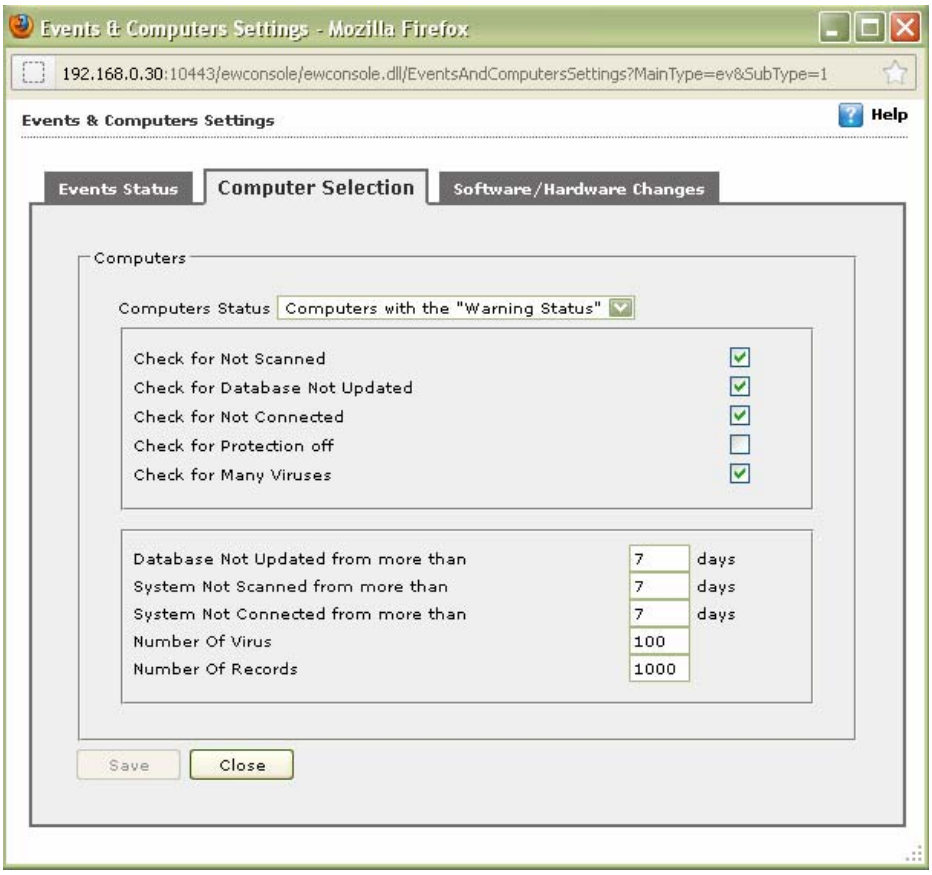

Events & Computers Settings - Mozilla Firefox
192.168.0.30:10443/ewconsole/ewconsole.dll/EventsAndComputersSettings?MainType=ev&SubType=1
Events & Computers Settings
Help
Events Status
Computer Selection
Software/Hardware Changes
Computers
Computers Status
Computers with the "Critical Status"
Check for eScan Not Installed
Check for Monitor Status
Check for Not Scanned
Check for Database Not Updated
Check for Not Connected
Database Not Updated from more than
7
days
System Not Scanned from more than
7
days
System Not Connected from more than
7
days
Number Of Records
1000
Save
Close

Figure 108

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

Computers with the “Warning Status”: It displays the list of systems which are warning in status, as per the criteria’s selected in computer settings. Refer



- Figure 89.

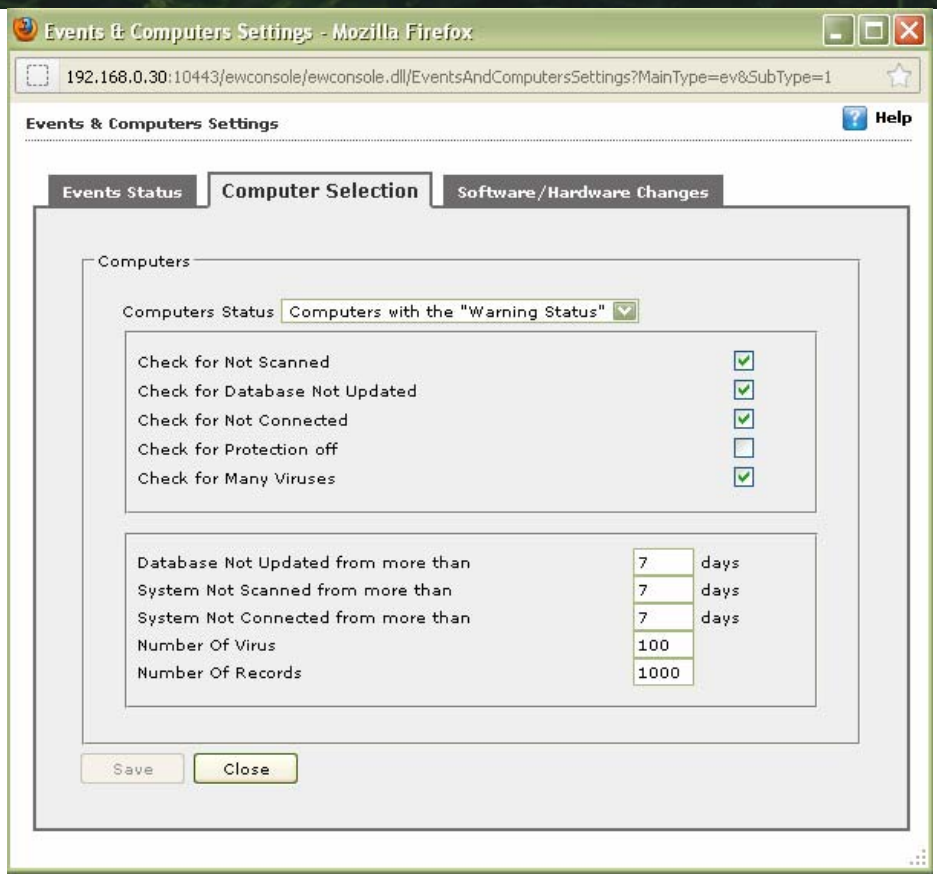
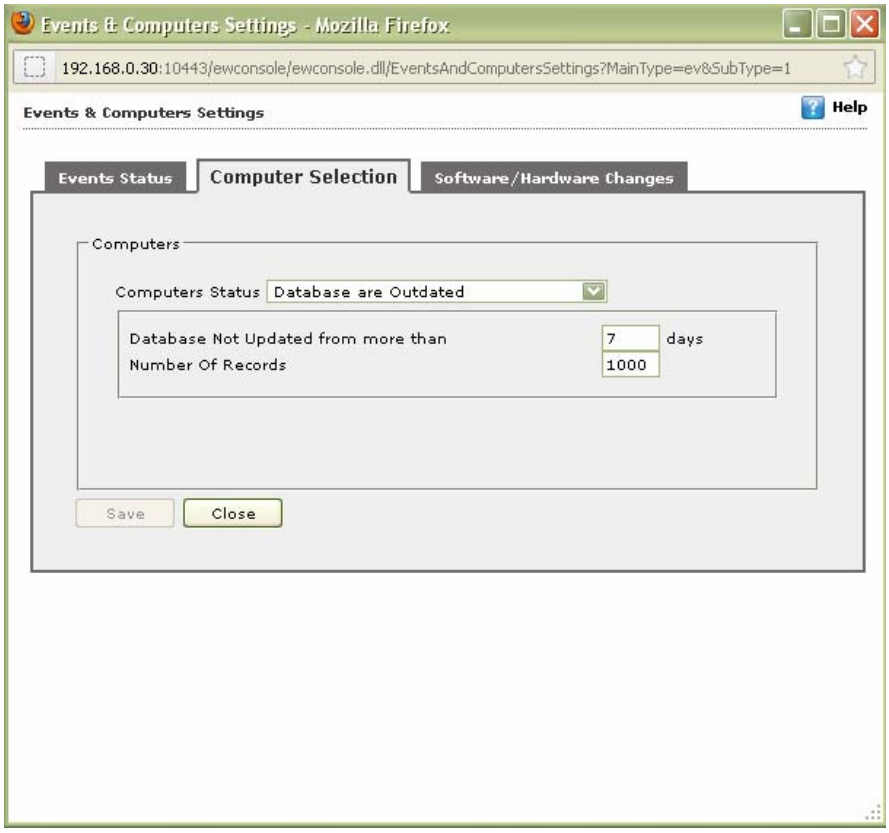

Events & Computers Settings - Mozilla Firefox
192.168.0.30:10443/ewconsole/ewconsole.dll/EventsAndComputersSettings?MainType=ev&SubType=1
Events & Computers Settings
Help
Events Status
Computer Selection
Software/Hardware Changes
Computers
Computers Status
Computers with the "Warning Status"
Check for Not Scanned
Check for Database Not Updated
Check for Not Connected
Check for Protection off
Check for Many Viruses
Database Not Updated from more than
7
days
System Not Scanned from more than
7
days
System Not Connected from more than
7
days
Number Of Virus
100
Number Of Records
1000
Save
Close

Figure 89

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

- Database are Outdated: It displays the list of systems on which virus database is outdated. Refer



- **Figure 90.**

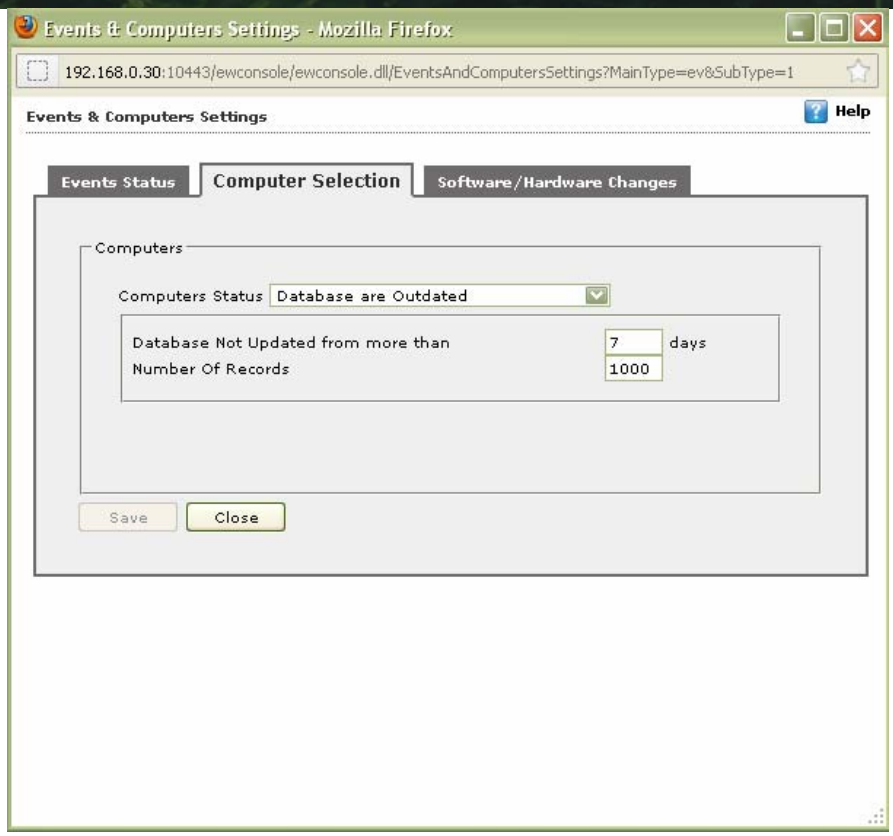
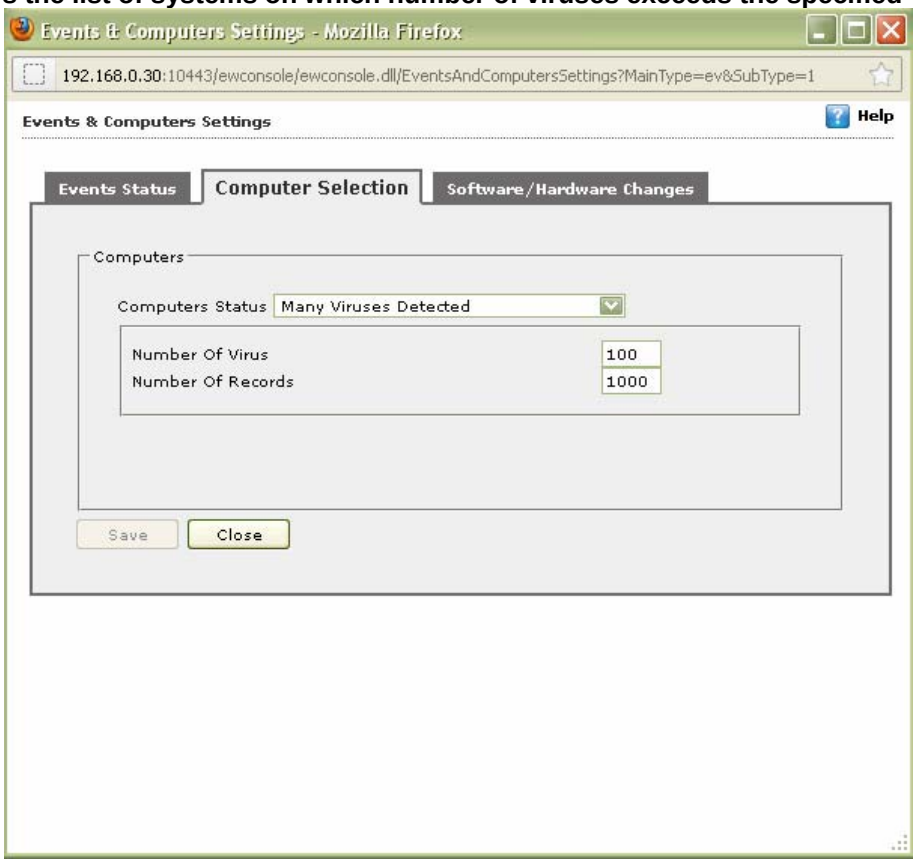


Figure 90

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

Many viruses Detected: It displays the list of systems on which number of viruses exceeds the specified count in computer settings. Refer



- Figure 91.

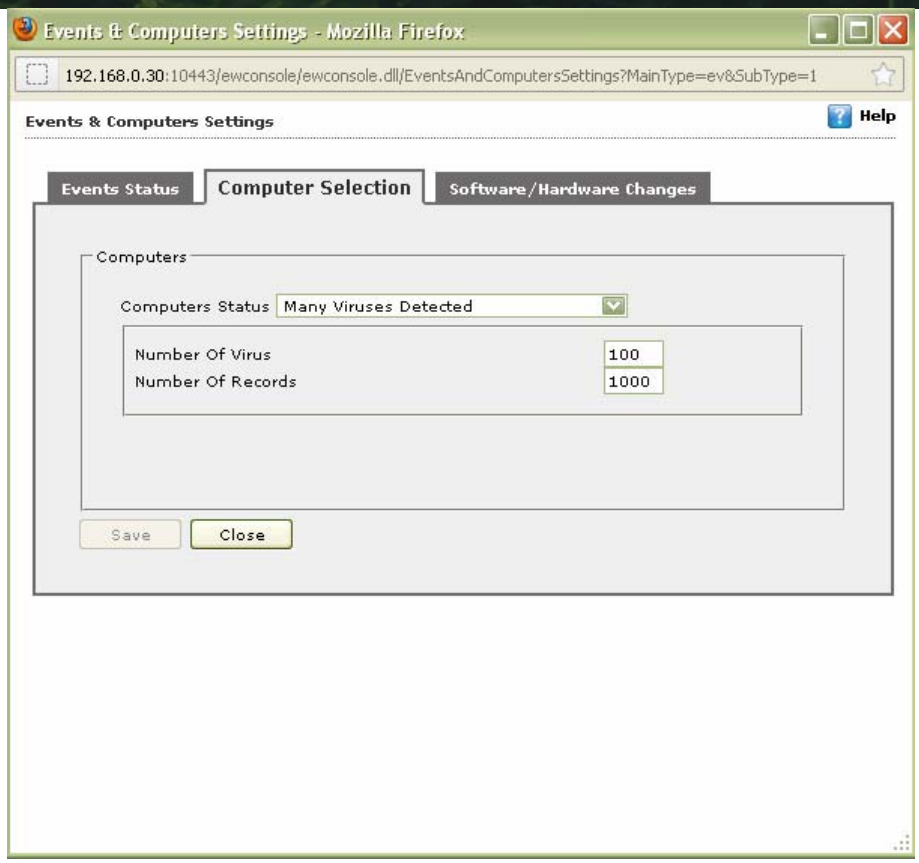
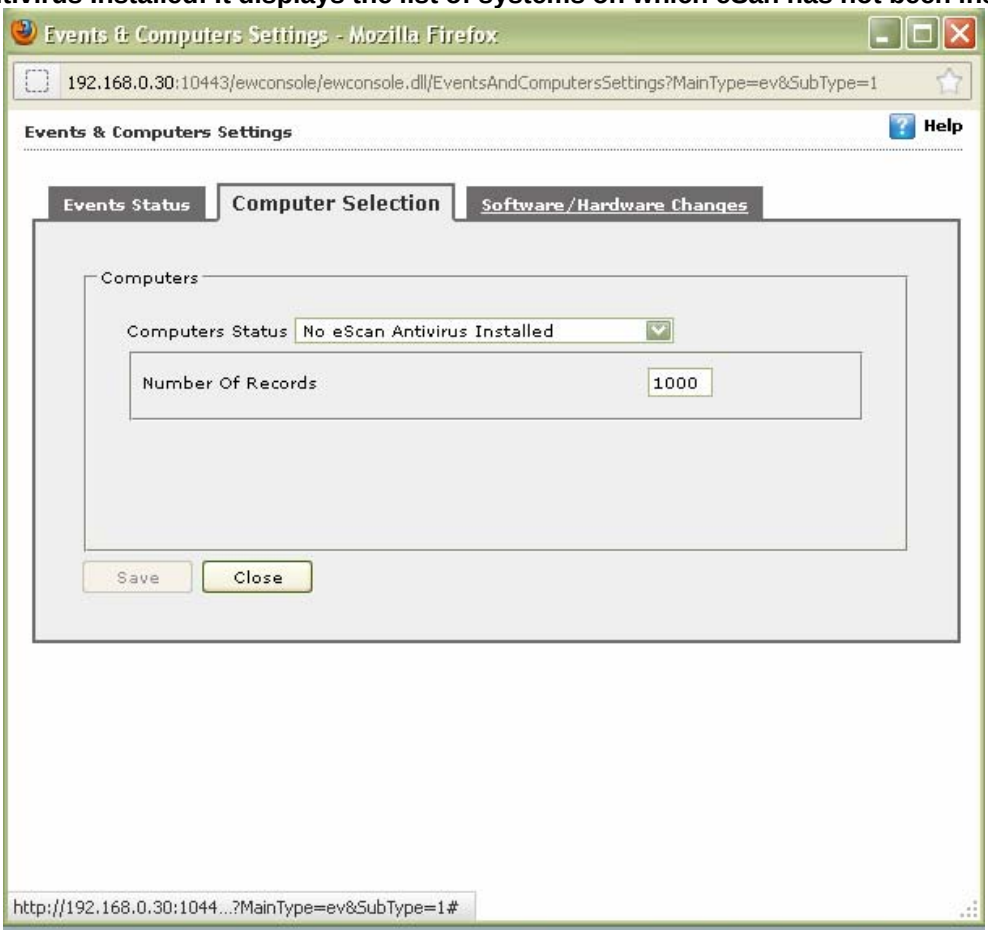


Figure 91

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

No eScan Antivirus Installed: It displays the list of systems on which eSan has not been installed. Refer



- Figure 92.

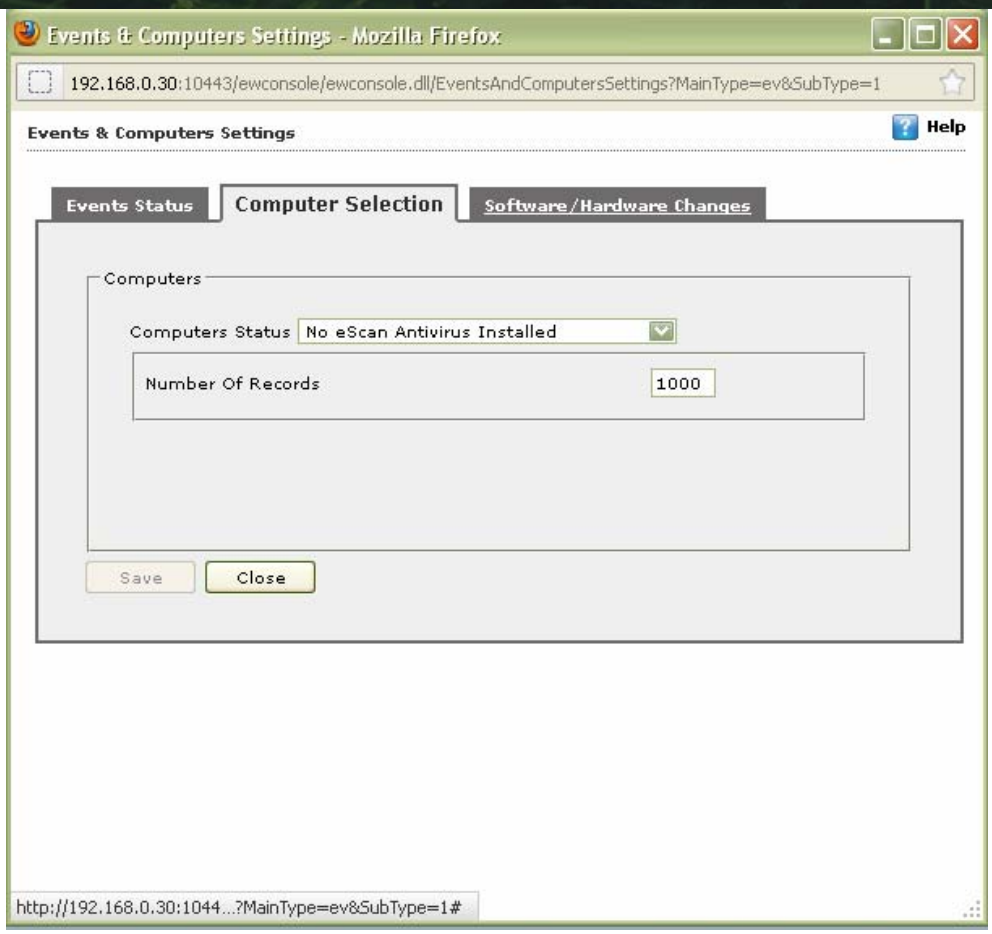
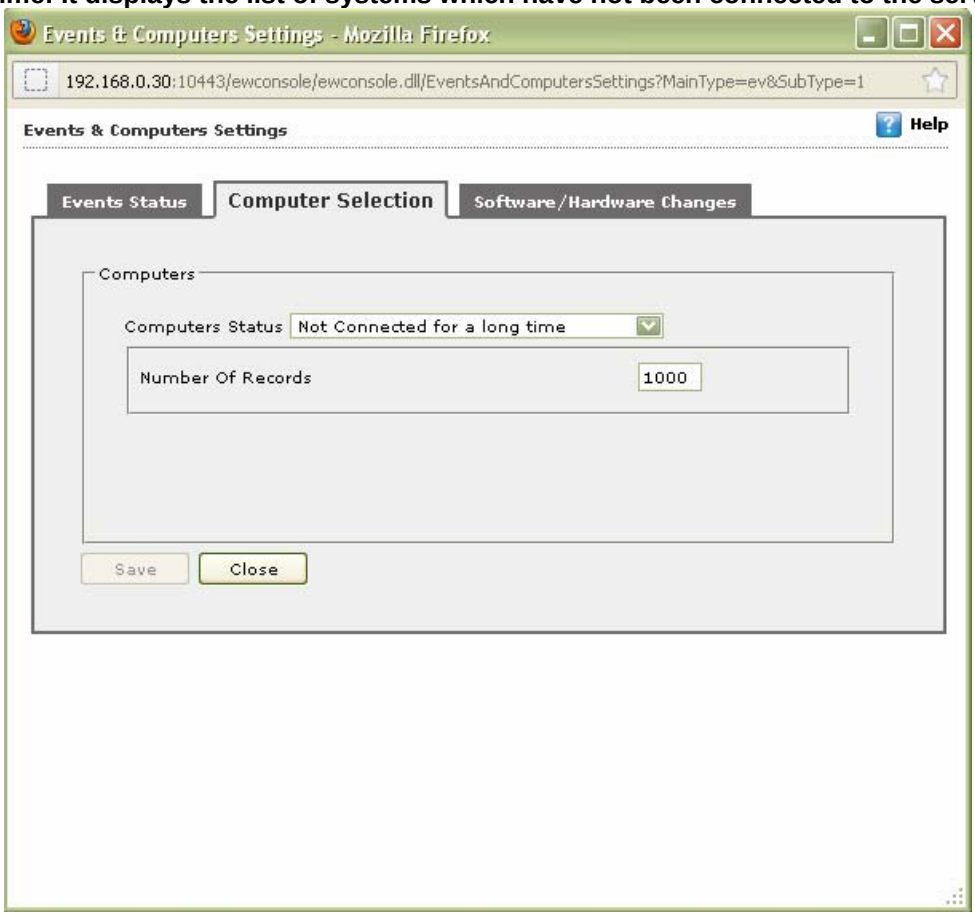


Figure 92

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

Not connected for a long time: It displays the list of systems which have not been connected to the server from a long time. Refer



- Figure 93.

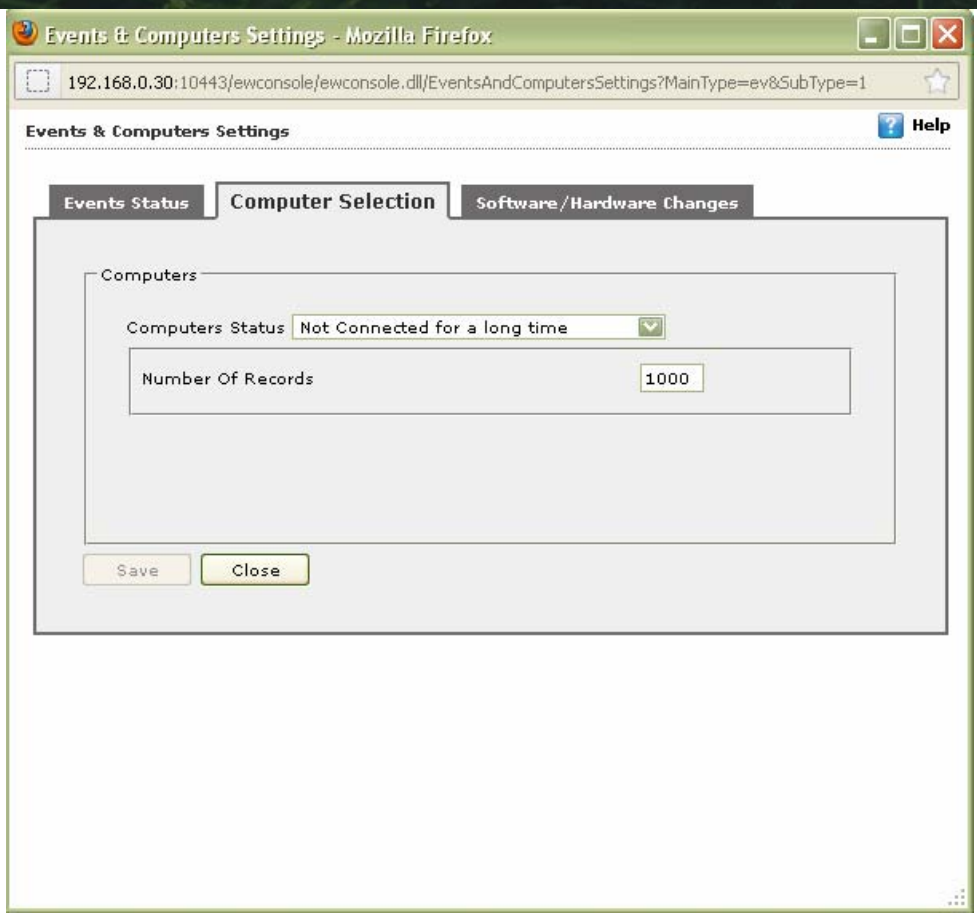
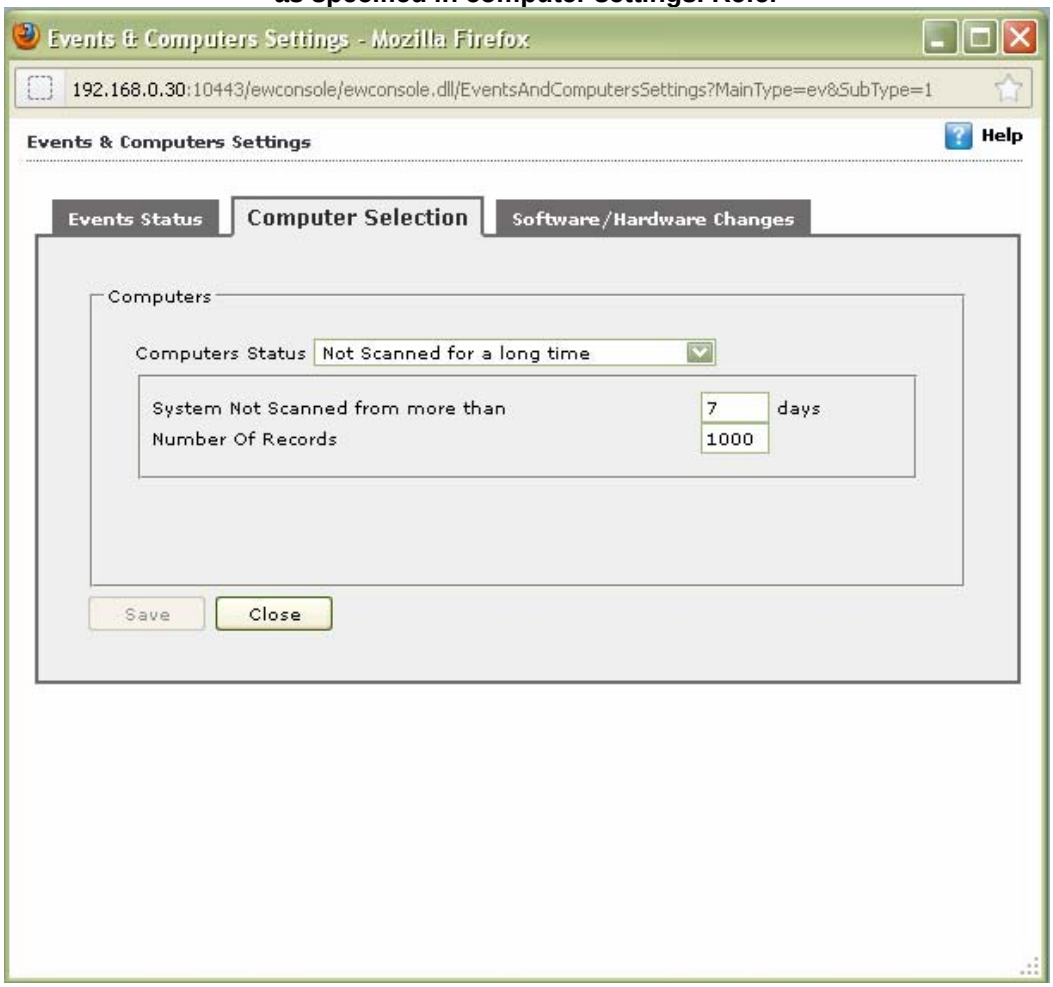


Figure 93

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

Not scanned for a long time: It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Refer



- Figure 94.

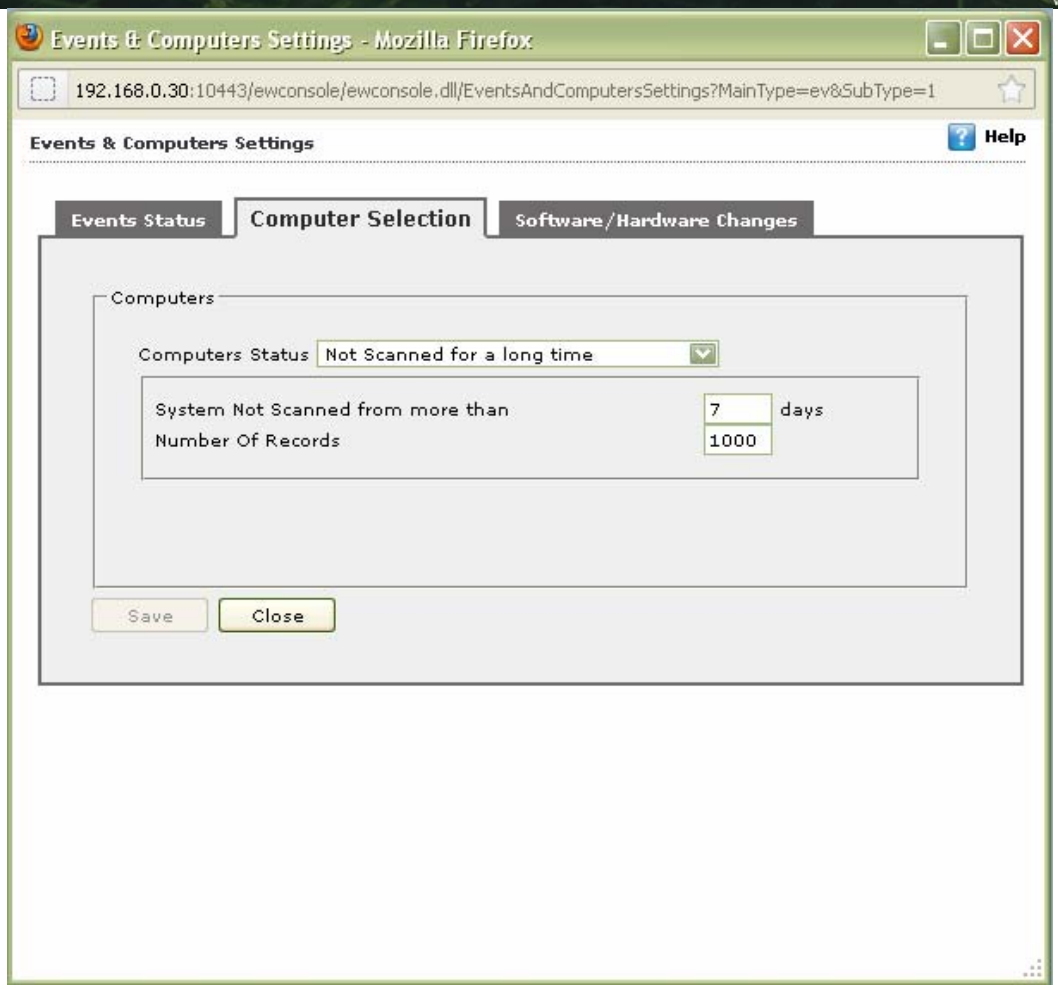
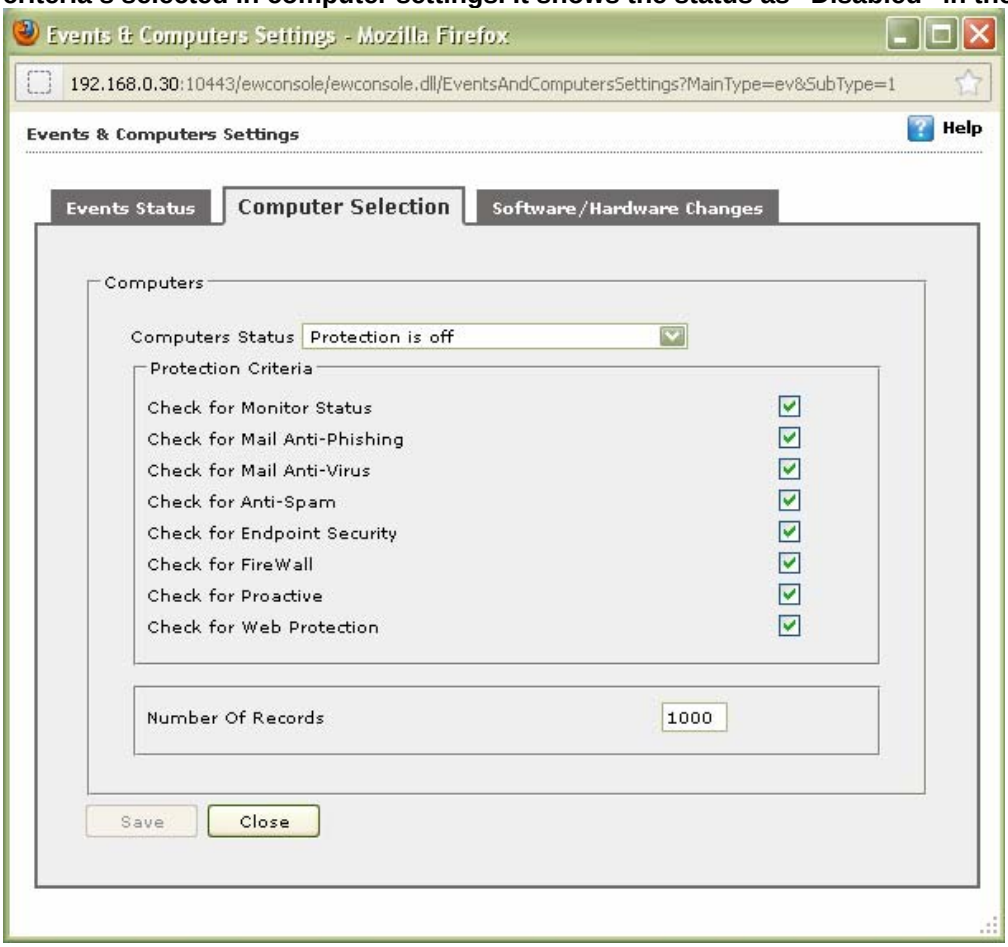


Figure 94

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

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



- Figure 95.

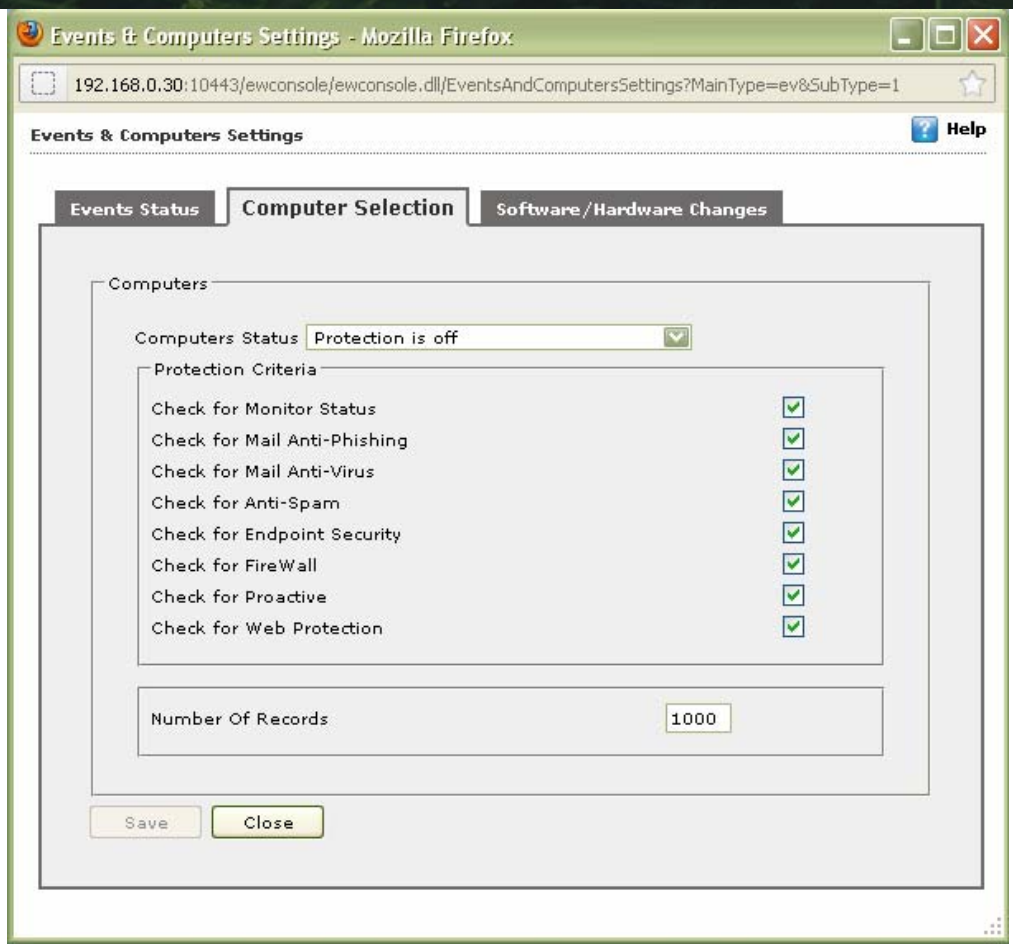


Figure 95

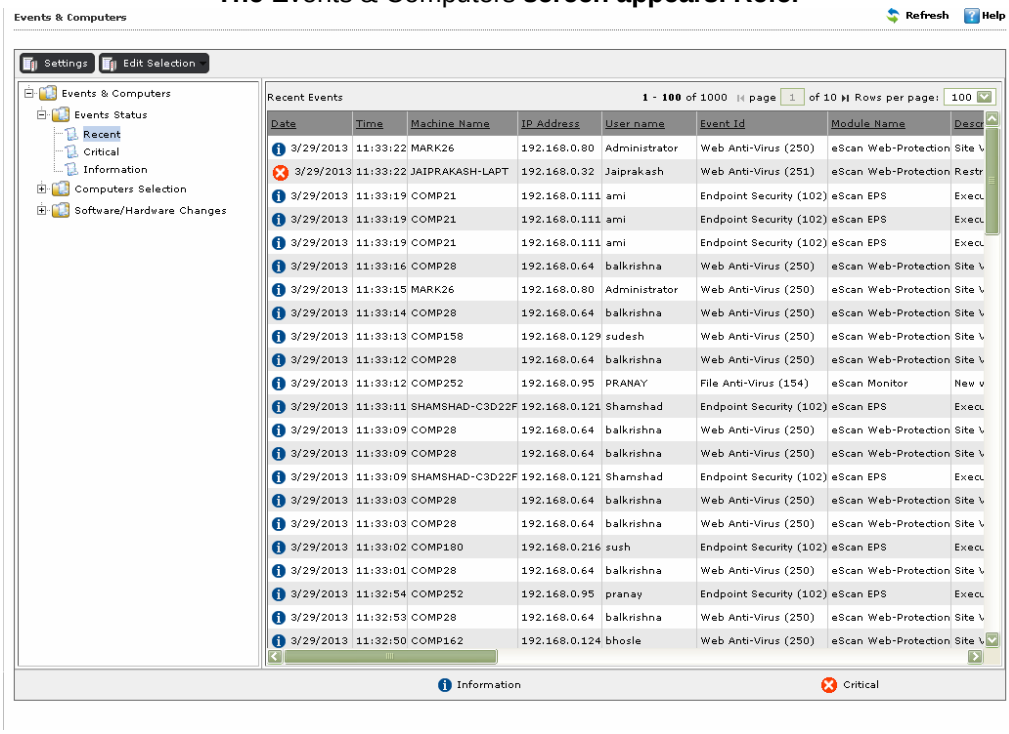
Field	Description
Protection Criteria	
Check for Monitor Status	Select this check box if you want to view the client systems on which eScan monitor is not enabled.
Check for Mail Anti-Phishing	Select this check box if you want to view the list of client systems on which **Mail Anti-Phishing** protection is inactive, that is disabled.
Check for Mail Anti-Virus	Select this check box if you want to view the list of client systems on which **Mail Anti-Virus** protection is inactive, that is disabled.
Check for Mail Anti-Spam	Select this check box if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive, that is disabled.
Check for Endpoint Security	Select this check box if you want to view the list of client systems on which **Endpoint Security** protection is inactive, that is disabled.
Check for Firewall	Select this check box if you want to view the list of client systems on which **Firewall** protection is inactive, that is disabled.

Field	Description
Check for Proactive	Select this check box if you want to view the list of client systems on which **Proactive** protection is inactive, that is disabled.
Check for Web Protection	Select this check box if you want to view the list of client systems on which protection of **Web Protection** module is inactive, that is disabled.
Number Of Records	Type the number of client system that you want to view in the list.

Saving Computer Settings

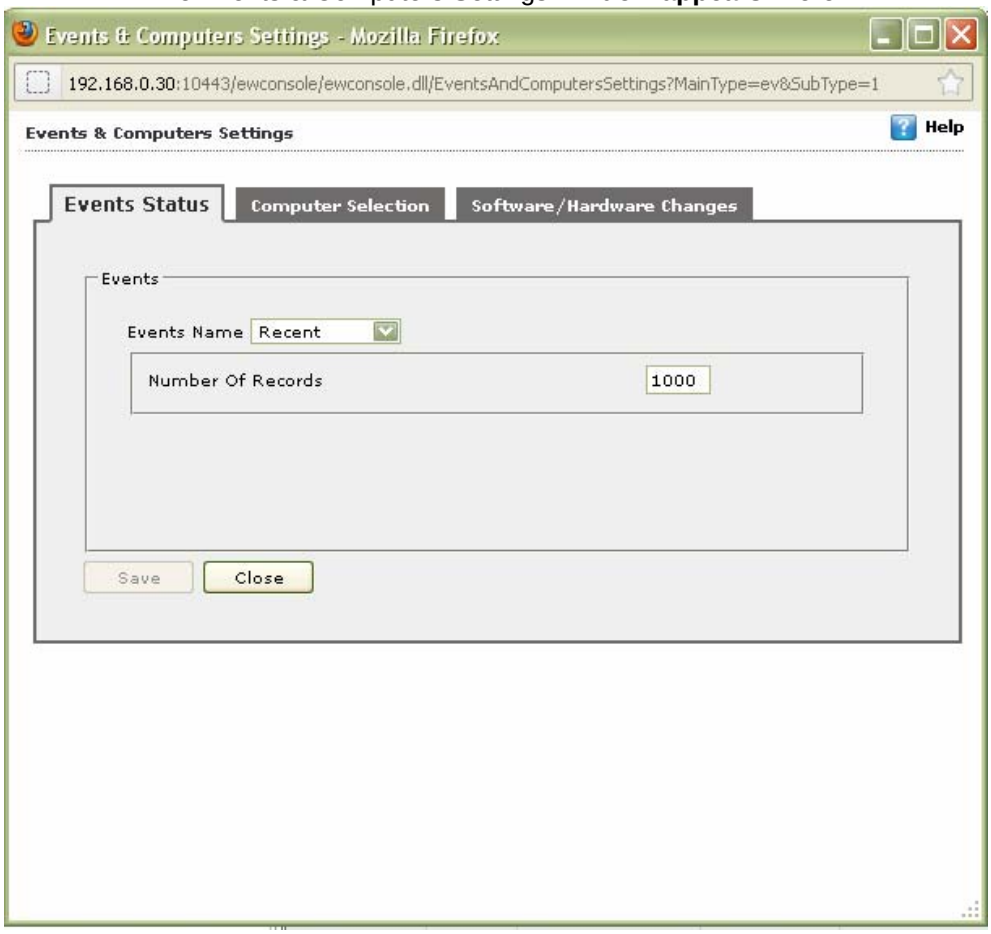
Perform the following steps to save the computer settings:

On the navigation pane, click Events & Computers**.**
The Events & Computers **screen appears. Refer**



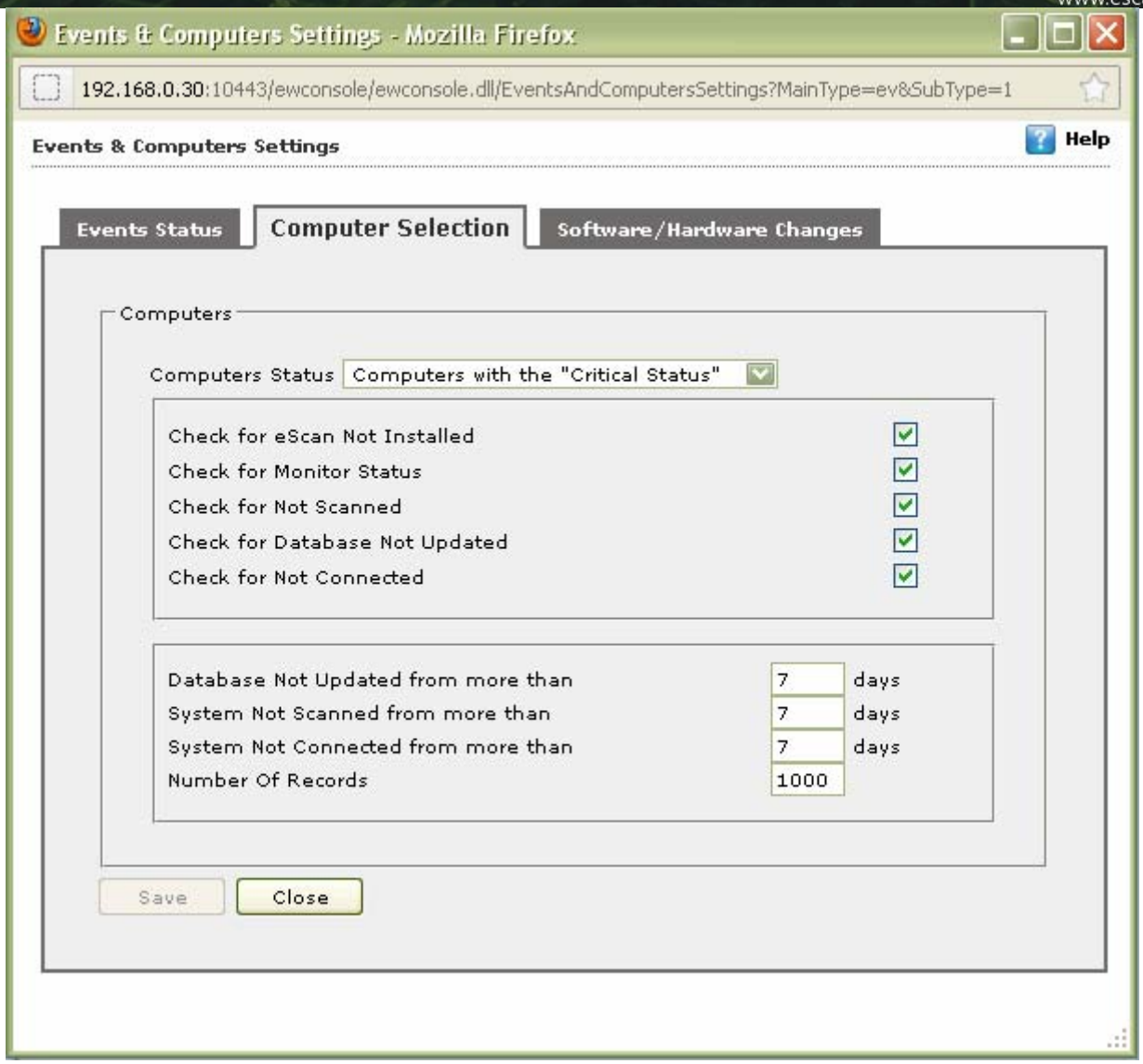
1. Figure 106886.

Click the Settings **button.**
The Events & Computers Settings **window appears. Refer**



2. Figure 7.
3. By default, the **Events Status** window appears.

Click the Computers Selection **tab.**
The Computers Selection **window appears. Refer**



4. Figure 8.
5. Select type of status for which you want to set criteria, from the **Computer status** drop-down list.
6. Select the appropriate check boxes, and then type field details in the available fields. For more information, refer Types and Criteria's of Computer Status section.
7. Click the **Save** button.
   The settings get saved.

Software/ Hardware Changes

If you want to get updates on any changes made in the software, hardware, and to existing system, you have to make certain settings for it. The Software/ Hardware Changes tab enables you to do the following activities:

- Type of Updates
  - Software Changes
  - Hardware Changes
  - Existing System Info
- Changing Software/Hardware Settings

Type of Updates

The lists of updates are as follows:

- Software Changes: It displays the list of managed client systems on which software related changes are made. For example, Installation/Uninstallation of other softwares.
- Hardware Changes: It displays the list of managed client systems on which hardware related changes are made. For example, change in the IP address.
- Existing System Info: It displays the information of an existing system.

Changing Software/Hardware Settings

Perform the following steps to change the software/hardware settings:

1. On the navigation pane, click **Events & Computers**.
   The **Events & Computers** screen appears..
2. Click the Settings button.
   The Events & Computers Settings window appears.
3. By default, the **Events Status** window appears.

   Click the **Software/Hardware Changes** tab.
   The **Software/Hardware Changes** window appears. Refer
4. Figure 96.

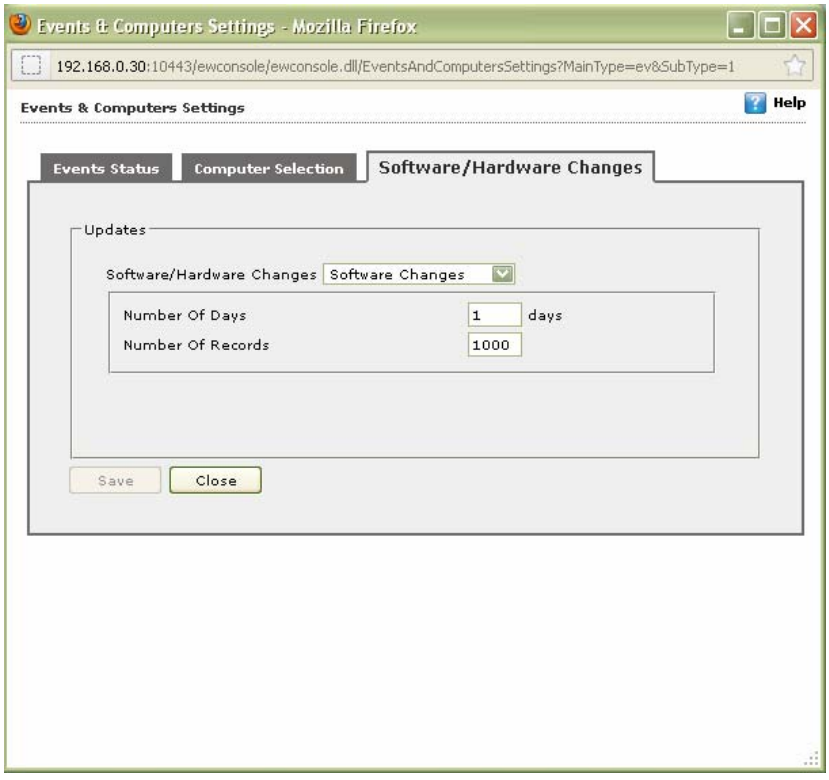


Figure 96

5. Specify the following field details.

Field	Description
Software/Hardware Changes	Select the type of update made in the system from the drop-down list.
Number of Days	Type the number of days, to view changes made within the specified days. For example, if you have typed 2 days, then you can view the list of client systems on which any software/hardware changes have been made in the 2 days.
Number of Records	Type the number of client systems that you want to view in the list.

6. Click the **Save** button.

   The settings get saved.

Edit selection

> The properties of **Edit Selection** drop-down menu appears dimmed, it is available only when you select the appropriate client system check box available under **Machine Name** column. For more information, refer Editing Properties section.
>
> Click the (+) sign to expand the folder and view the sub-folders and click the (-) sign to collapse the required folder.

The **Edit Selection** enables you to edit the computer selections that have already been made by you. You can do the following activities:

- Tabs under Edit Selection
  - Protection
  - Events
  - Deploy/Upgrade Client
  - Check Connection
  - Connect to Client
  - Properties
- Editing Properties

Tabs under Edit Selection

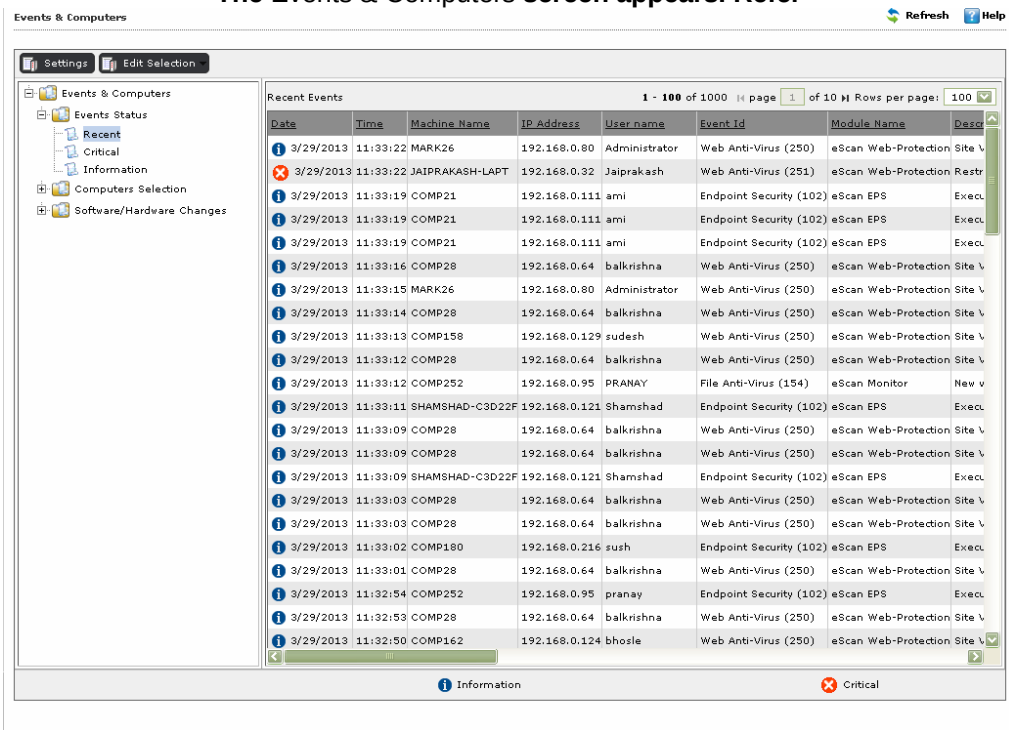
The different tabs under edit selection are as follows:

- Protection: It displays the computer protection status.
- Events: It displays both critical and information events that occurred recently on managed client computers.
- Deploy/Upgrade Client: It enables you to deploy/upgrade eScan on client system.
- Check Connection: It displays the connection status between server and client.
- Connect to Client: It enables you to take a remote desktop connection to client system.
- Properties: It displays the properties of a specific client system.

Editing Properties

Perform the following steps to edit the properties:

On the navigation pane, click Events & Computers**.**
The Events & Computers **screen appears. Refer**



1. Figure 10688.
2. On the left pane, click the **Computer Selection** folder, and then click the computer status for which you want to edit.

The list of selected computer status records appear on right side of the screen. Refer

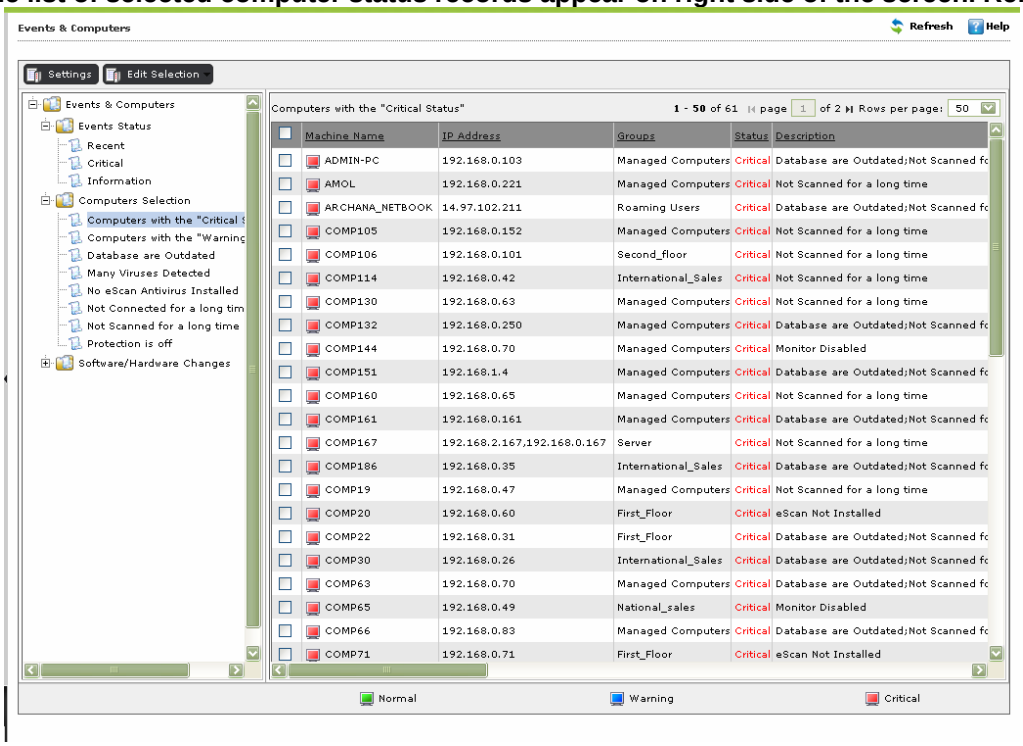


Figure 97.

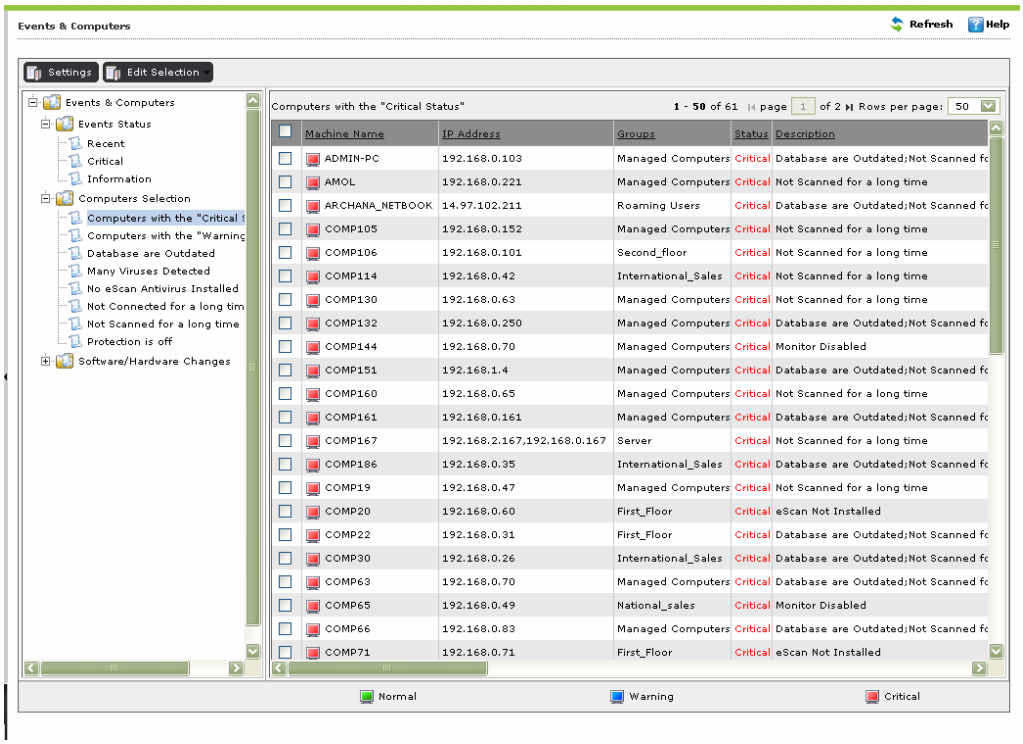


Figure 97

3. Select the appropriate check box, the client system for which you to edit the properties, and then click the

4. **Edit Selection** drop-down menu.

   The list of properties appears. For more information, refer Tabs Under Edit Selection section.

5. Click the appropriate property, which you want to edit and save the settings.

Viewing Event List

The **Events and Computers** module enables you to view log of the following events occurred.

- Viewing Event Status List
  - Recent
  - Critical
  - Information
- Viewing Computer Selection List
  - Computers with the “Critical Status”
  - Computers with the “Warning Status”
  - Database are Outdated
  - Many viruses Detected
  - No eScan Antivirus Installed
  - Not connected for a long time
  - Not scanned for a long time
  - Protection is off
- Viewing Software/ Hardware Changes
  - Software Changes
  - Hardware Changes
  - Existing System Info

Viewing Event Status List

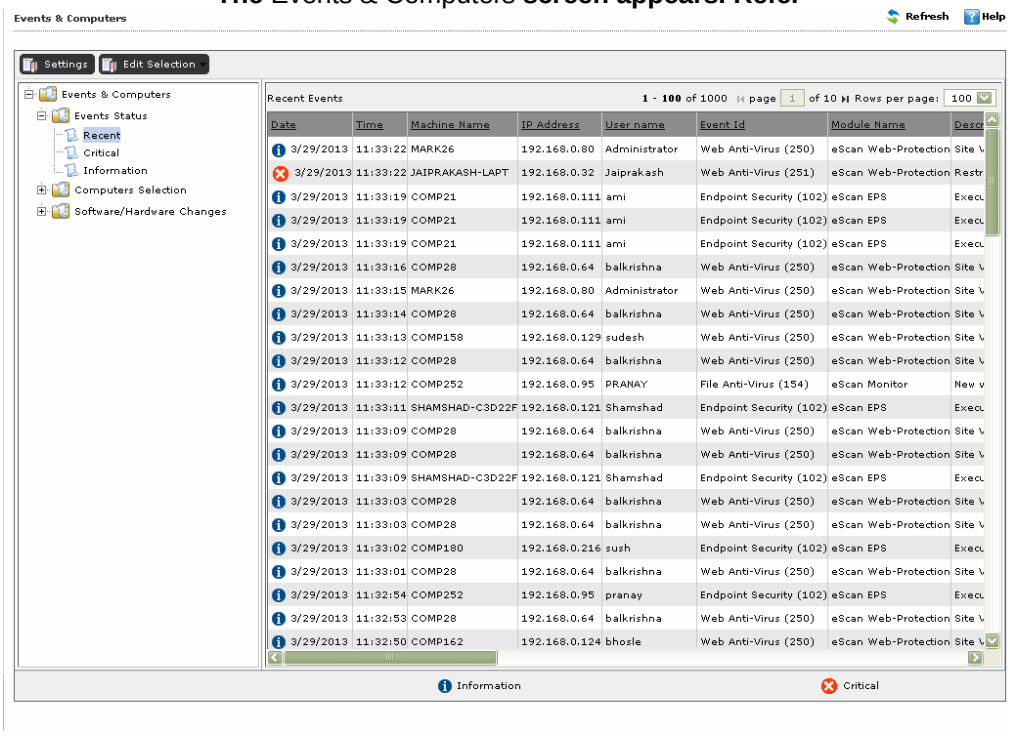
It enables you to view the list of recent, critical, and information type of events occurred on managed client computers. For more information, refer Types of Event Status section. The  symbol indicates information events and  symbol indicates critical events.

 Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

 If you want to view limited events at a time, you can select the number of records from the **Row per page** drop-down list. Click ⏮ and ⏭ to navigate to the previous and next page respectively.

To view event status list

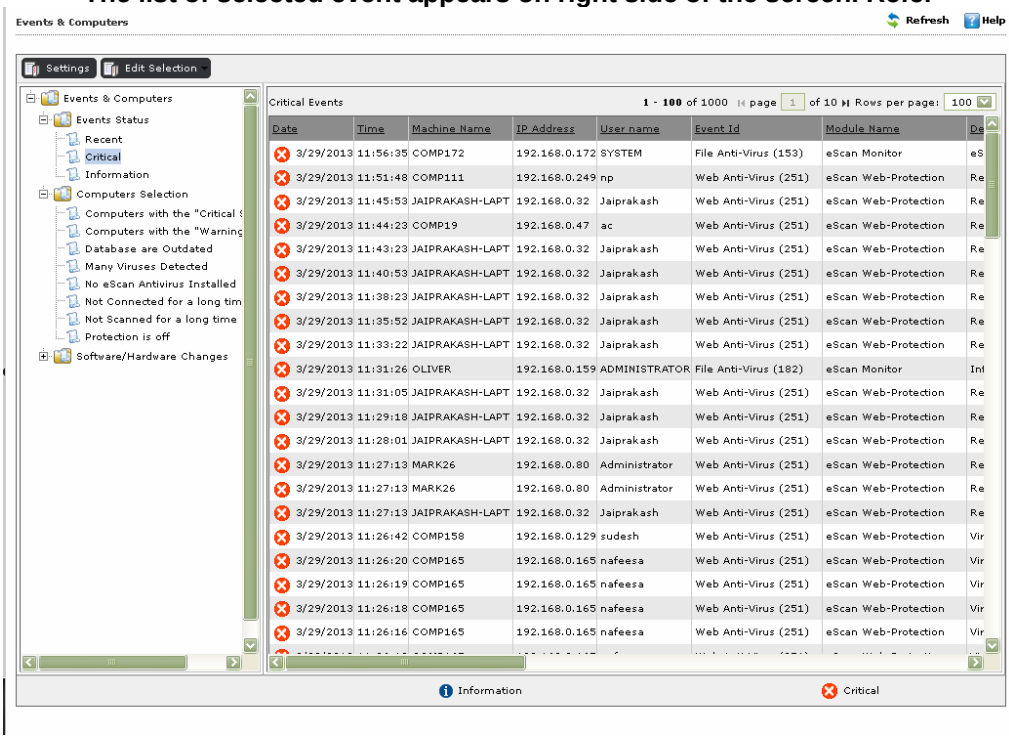
On the navigation pane, click Events & Computers**.**
The Events & Computers **screen appears. Refer**



1. Figure 10688.

On the left pane, click Events Status **folder, and then click an appropriate option to view the recent, critical, and information events log.**

The list of selected event appears on right side of the screen. Refer



2. Figure 98.

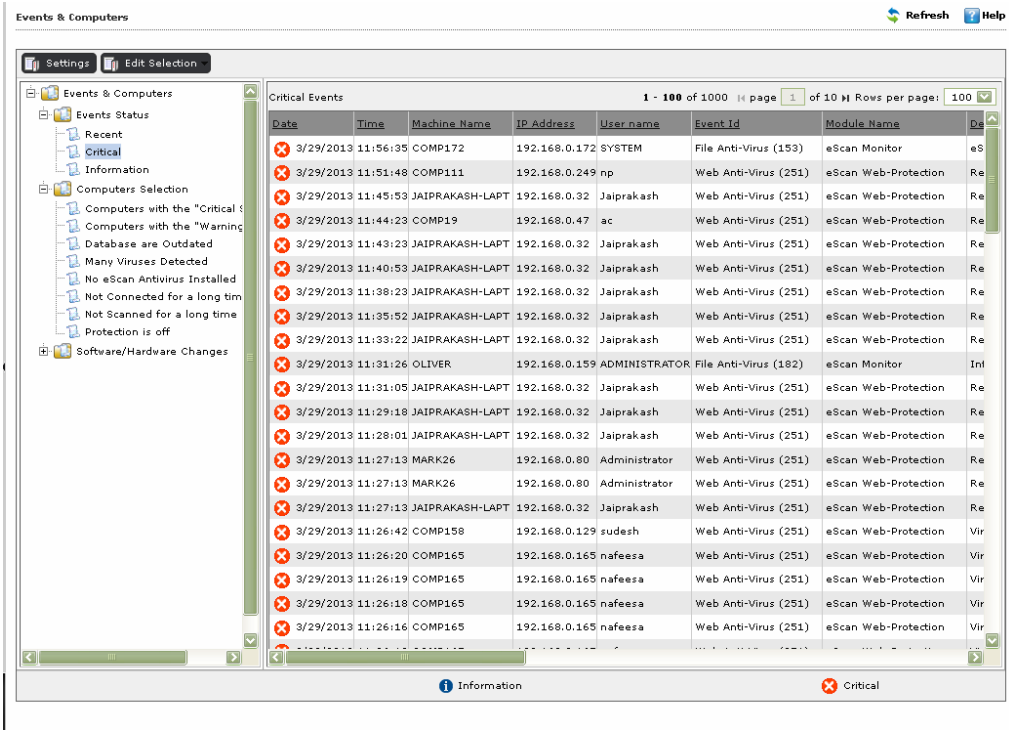


Figure 98

3. The event list appears in a tabular format, and the table contains following columns:

Column heading	Description
Date	It indicates the date when client has accessed machine with type of event symbol. For example, 4/14/2011
Time	It indicates the time when client has accessed machine.
Machine Name	It indicates client machine name.
IP Address	It indicates IP address of client machine.
User name	It indicates user name of the system.
Event Id	It indicates type of event name with its ID.
Module Name	It indicates type of module name under events.
Description	It indicates description of event occurred.
Client Action	It indicates type of action taken by client.
Site Programme Name	It indicates name of the programme accessed.

4. View the details as required.

Viewing Computer Selection List

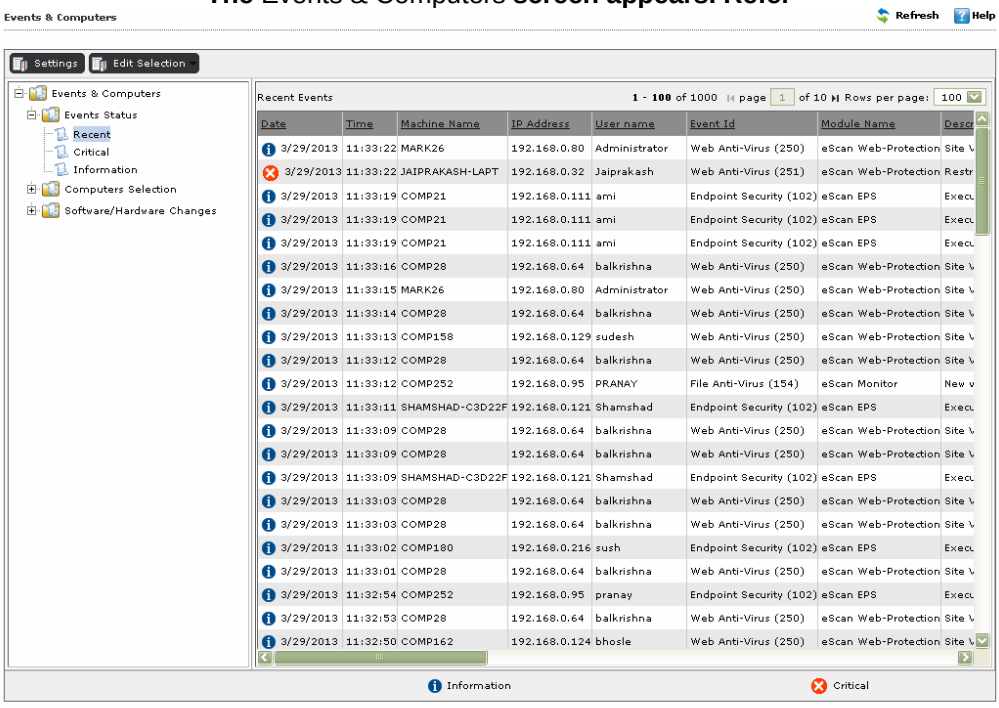
There are different types of computer status with different criteria's. For more information, refer Types and Criteria's of Computer Status section. It enables you to view the log of all types of computer status. The symbol indicates normal status, symbol indicates warning status, and symbol indicates critical status.

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

If you want to view limited events at a time, you can select the number of records from the **Row per page** drop-down list. Click and to navigate to the previous and next page respectively.

To view computer selection list

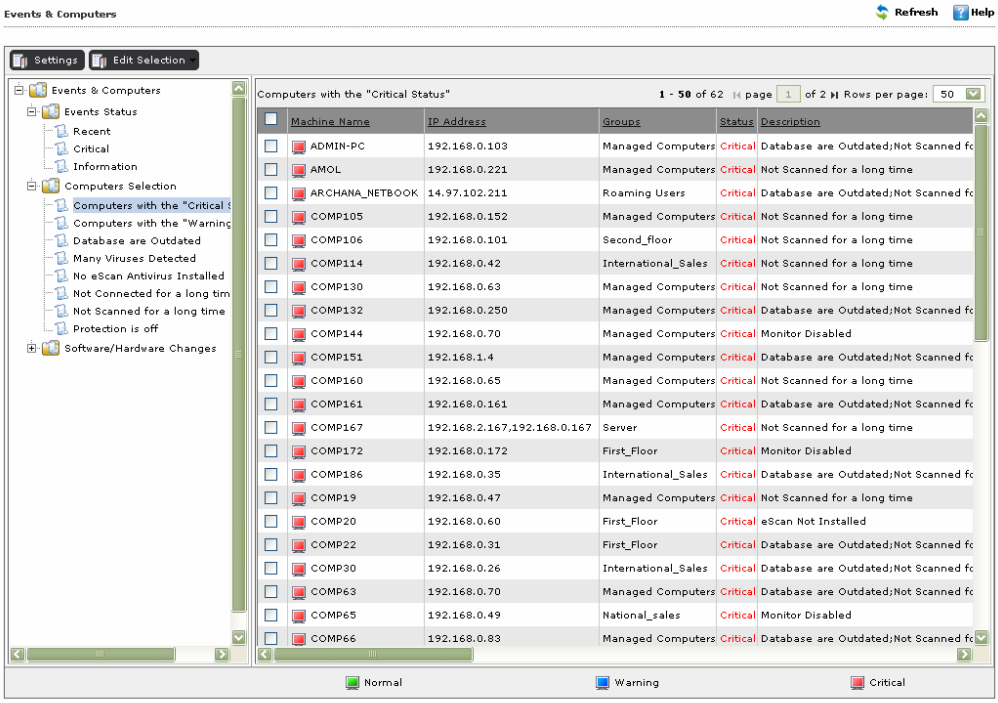
On the navigation pane, click Events & Computers**.**
The Events & Computers **screen appears. Refer**



1. Figure 10688.

On the left pane, click Computer Selection **folder, and then click an appropriate option for which you want to view status log.**

The list of selected computer status appears on right side of the screen. Refer



2. Figure 99.

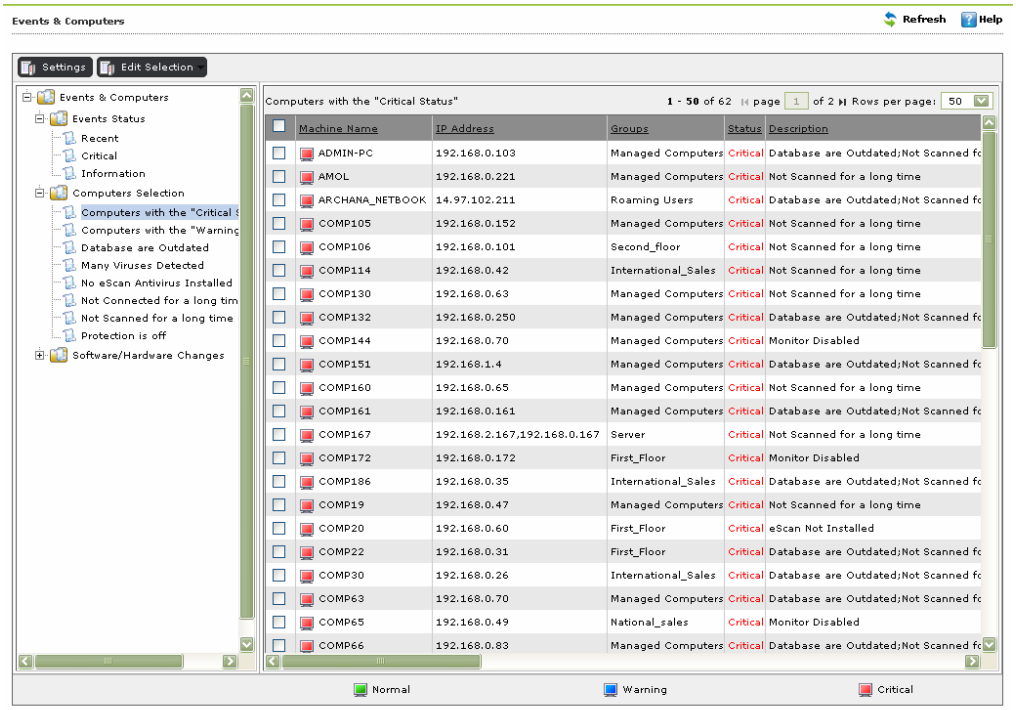


Figure 99

3. The computer status list appears in a tabular format, and the table contains following columns:

Column heading	Description
Machine Name	It indicates client machine name with type of status symbol. For example, COMP104.
IP Address	It indicates IP address of client machine.
Groups	It indicates group name.
Status	It indicates type of status. For example, Normal, warning, and critical
Description	It indicates detailed description of event occurred.
eScan Installed	It indicates status whether eScan is installed or not.
Last Connection	It indicates the date when eScan is lastly connected to machine.
Last Update	It indicates the date when eScan is lastly updated.
Last Scanned	It indicates the date when scanning occurred.
Monitor Status	It indicates monitor status. For example, enabled or disabled if eScan installed and unknown if eScan is not installed.
Proactive	It indicates proactive status. For example, enabled or disabled and unknown if eScan is not installed.
Mail Anti-Virus	It indicates the mail anti-virus status. For example, enabled or disabled and unknown if eScan is not installed.
Anti- Spam	It indicates the anti-spam status. For example, enabled or disabled and unknown if eScan is not installed.
Mail Anti-Phishing	It indicates the mail anti-phishing status. For example, enabled or disabled and unknown if eScan is not installed.
Web Protection	It indicates the web protection status. For example, enabled or disabled and unknown if eScan is not installed.
Firewall	It indicates the firewall status. For example, enabled or disabled and unknown if eScan is not installed.
Endpoint Security	It indicates the endpoint security status. For example, enabled or disabled and unknown if eScan is not installed.
Virus count	It indicates the total number of infected viruses detected in a machine.

4. View the details as required.

Viewing Software/ Hardware changes list

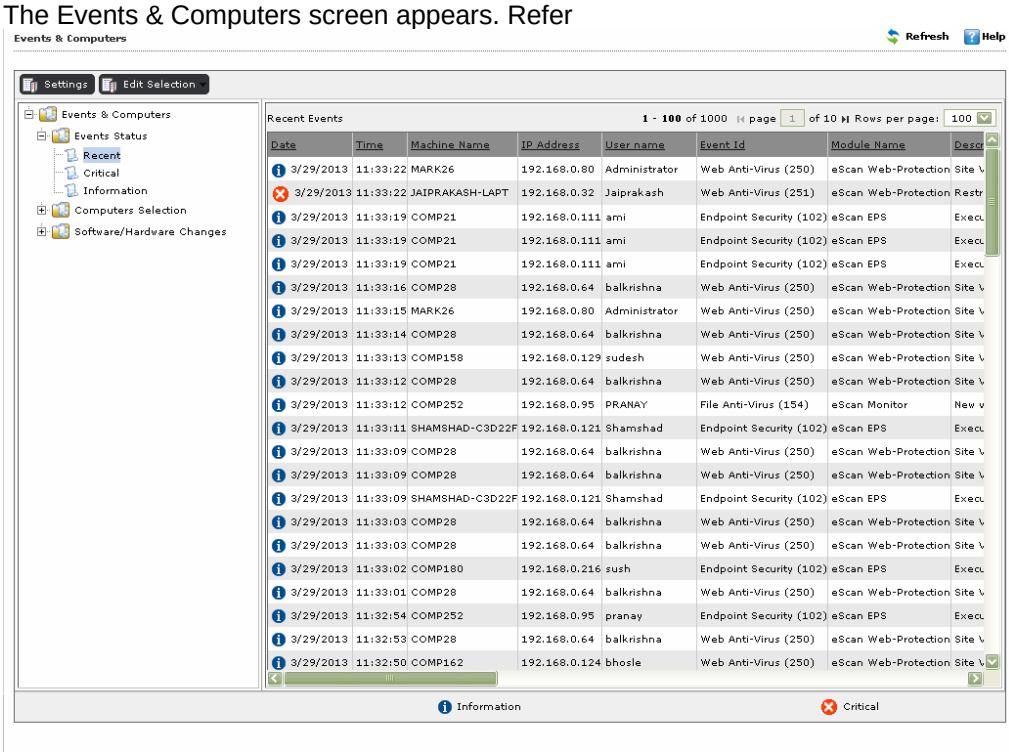
The software/ hardware changes contain three types of updates – Software, Hardware, and Existing system information. For more information, refer Type of Updates section.

Click the (+) sign to expand the folder and view options and click the (-) sign to collapse the required folder.

If you want to view limited events at a time, you can select the number of records from the **Row per page** drop-down list. Click ⏮ and ⏭ to navigate to the previous and next page respectively.

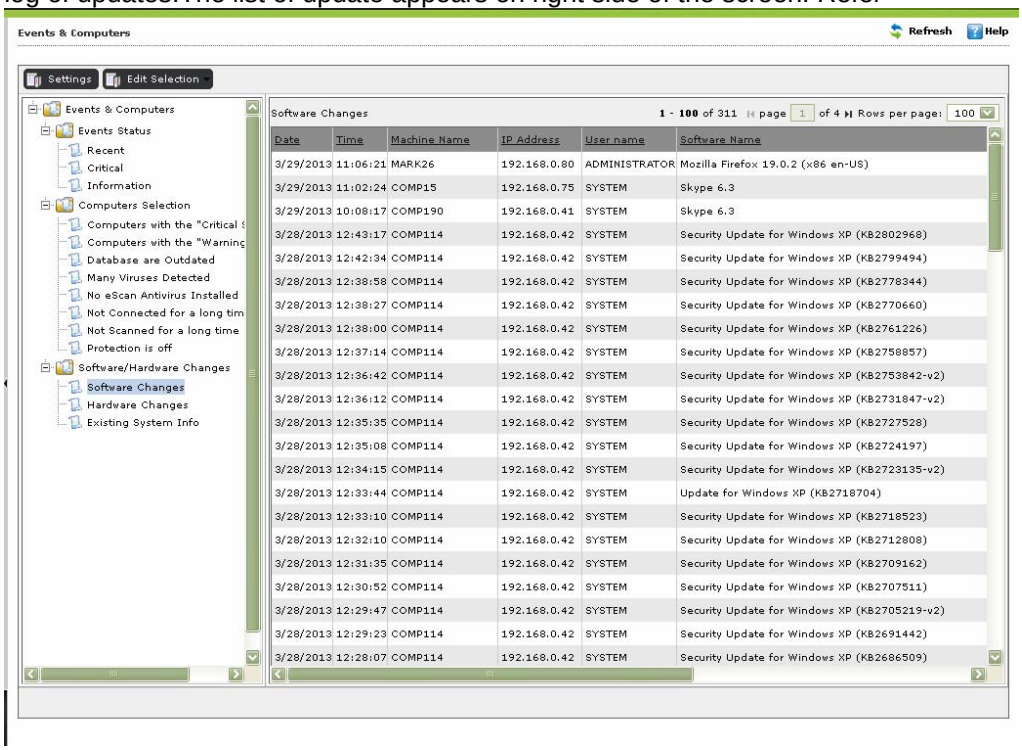
To view software/ hardware changes list

1. On the navigation pane, click Events & Computers.
   The Events & Computers screen appears. Refer



2. Figure 10688.

3. On the left pane, click Software/ Hardware Changes folder, and then click an appropriate option to view the log of updates.The list of update appears on right side of the screen. Refer



4. Figure **100**.

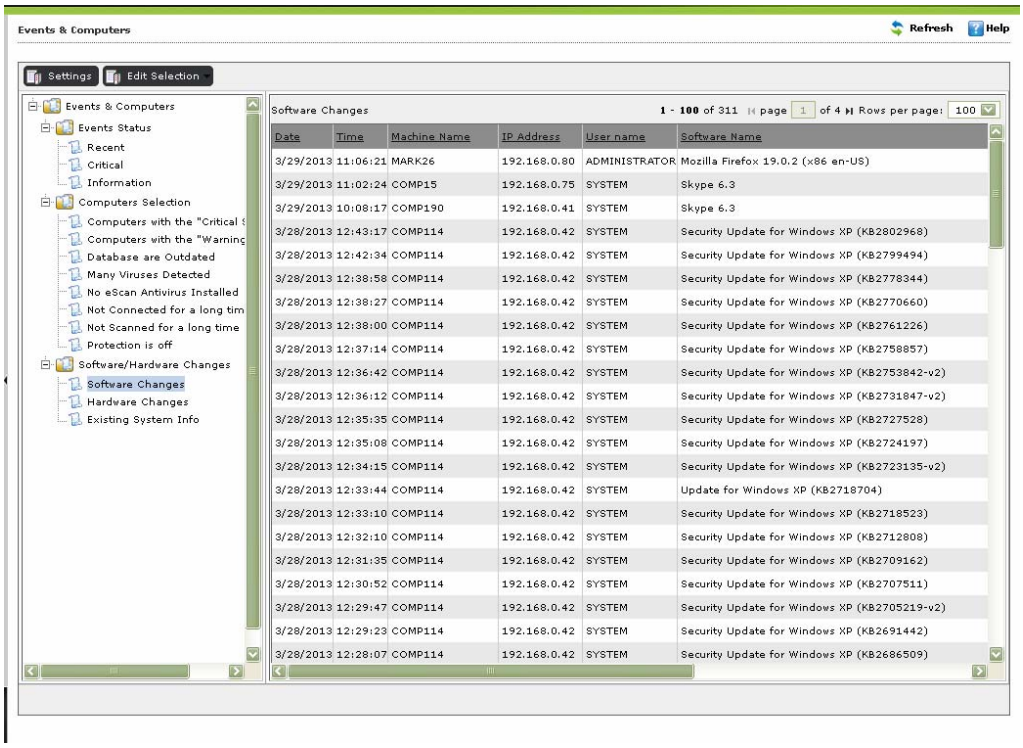


Figure 100

5. The updates list appear in a tabular format, and each type of update has specific table with different columns, which are as follows:

Software changes table

Column heading	Description
Date	It indicates the date when software changes are made.
Time	It indicates the time when software changes are made.
Machine Name	It indicates client machine name.
IP Address	It indicates IP address of client machine.
User name	It indicates user name of the system.
Software name	It indicates name of the software.
Client Action	It indicates the status, whether new software is installed or existing software is uninstalled.

6. Hardware changes table (Refer Figure 121)

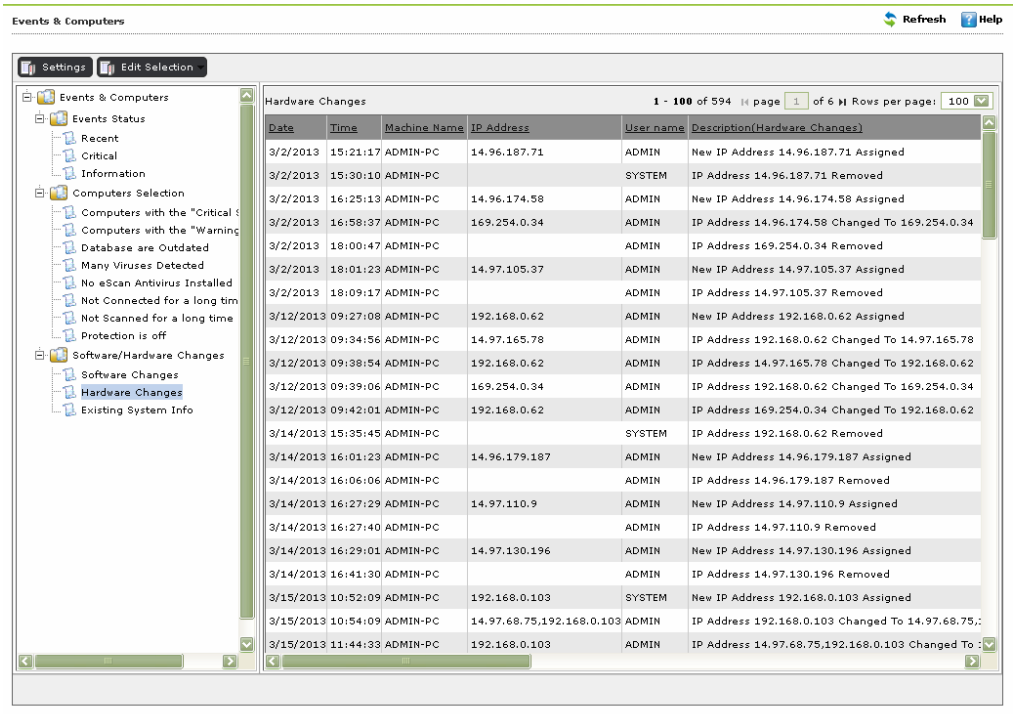
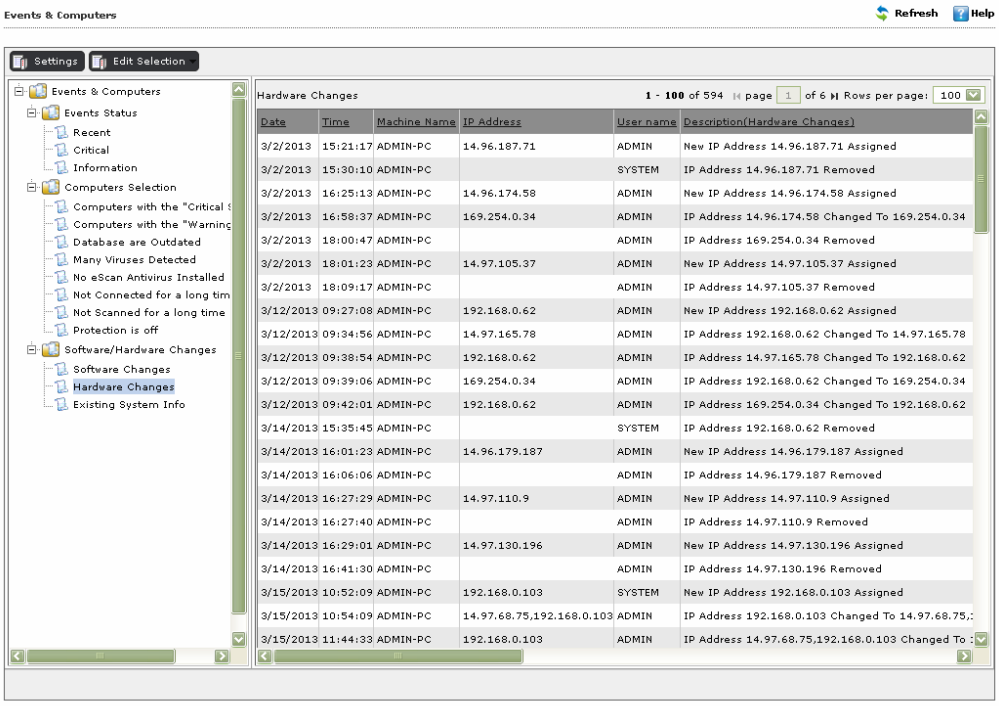


Figure 101

Column Names	Description
Date	It indicates the date when software changes are made.
Time	It indicates the time when software changes are made.
Machine Name	It indicates client machine name.
IP Address	It indicates IP address of client machine.
User name	It indicates user name of the system.
Description(Hardware changes)	It indicates the description of hardware change.
Operating System	It indicates type of operating system.
Service Pack	It indicates type and version of service pack.
Internet Explorer	It indicates type and version of internet explorer.
RAM	It indicates the capacity of RAM.
Processor	It indicates type of processor.
Motherboard	It indicates name of the motherboard.
HDD	It indicates the capacity that is, size of HDD (Hard Disk).

Existing system information table (Refer



- Figure 102)

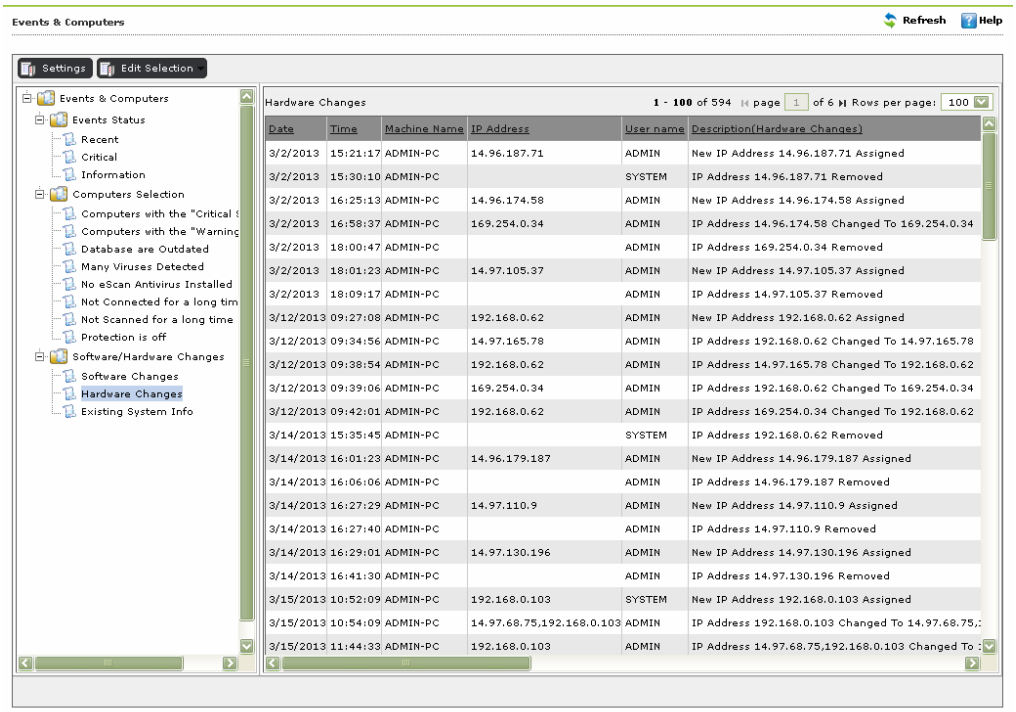


Figure 102

Column heading	Description
Date	It indicates the date when software changes are made.
Time	It indicates the time when software changes are made.
Machine Name	It indicates client machine name.
IP Address	It indicates IP address of client machine.
User name	It indicates user name of the system.
Operating System	It indicates type of operating system.
Service Pack	It indicates type and version of service pack.
Internet Explorer	It indicates type and version of internet explorer.
RAM	It indicates the capacity that is, size of RAM (Random Access Memory).
Processor	It indicates type of processor.
Motherboard	It indicates name of the motherboard.
HDD	It indicates the capacity that is, size of HDD (Hard Disk).

7. View the details as required.

Chapter 11 – 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 you requirement. It also allows you to Export the entire system information available through this module in PDF, Ms Excel or HTML formats.

All the Information related to the Softwares and Hardwares installed on all the Managed Computers is sent to eScan Web Management Console through the client application installed on them on a real time basis. This information is populated in Asset Management Section of the eScan Web Management console. This document will give you an Overview on how to View Hardware and Software Reports, Filter them as per your Criteria and Export them to the desired formats.

Viewing Hardware Reports

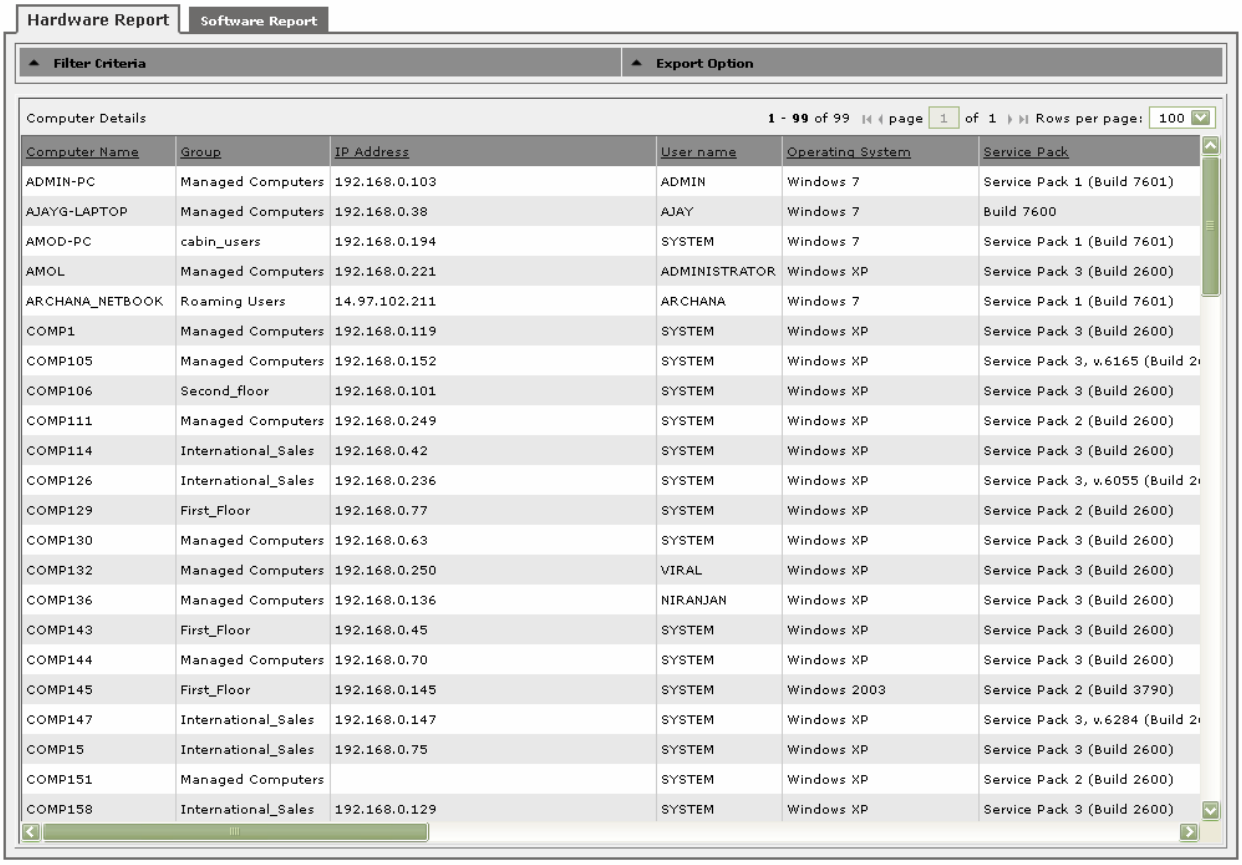
For Viewing the Hardware Configuration of all the Managed Computers connected to the Network, Click on the Asset Management section present on the Left in the eScan Web Management Console. Following Information will populate in the table on the right.

S.No.	Column Name	Description
1.	Computer Name	It displays the 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 Managed Computers.
4.	User Name	It displays the Username of the Managed Computers as defined by the Administrator for system Login.

5.	Operating System	It displays the Operating system Installed on the Managed Computers.
6.	Service Pack	It displays the Service Pack Version and Build installed on the Managed Computers.
7.	OS Version	It displays the Version of the Operating system installed in the Managed Computers.
8.	OS Installed Date	It displays the Date and Time of Installation of the Operating system on the Managed Computers.
9.	Internet Explorer	It displays the Version of the Internet Explorer installed on the Managed Computers.
10.	Processor	It displays the Processor details like Processor Name, Type and Processing Speed of the Managed Computers.
11.	Motherboard	It displays the Details of the Motherboard of the Managed Computers.

12.	RAM	It displays the details of the RAM installed on the Managed Computers.
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 Managed Computers.
15.	Software	By clicking on the View link present in this Column, you can view the list of Softwares along with the installation dates on the Managed Computer.

Actual Table View (Figure 123)



Computer Name	Group	IP Address	User name	Operating System	Service Pack
ADMIN-PC	Managed Computers	192.168.0.103	ADMIN	Windows 7	Service Pack 1 (Build 7601)
AJAYG-LAPTOP	Managed Computers	192.168.0.38	AJAY	Windows 7	Build 7600
AMOD-PC	cabin_users	192.168.0.194	SYSTEM	Windows 7	Service Pack 1 (Build 7601)
AMOL	Managed Computers	192.168.0.221	ADMINISTRATOR	Windows XP	Service Pack 3 (Build 2600)
ARCHANA_NETBOOK	Roaming Users	14.97.102.211	ARCHANA	Windows 7	Service Pack 1 (Build 7601)
COMP1	Managed Computers	192.168.0.119	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP105	Managed Computers	192.168.0.152	SYSTEM	Windows XP	Service Pack 3, v.6165 (Build 2
COMP106	Second_floor	192.168.0.101	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP111	Managed Computers	192.168.0.249	SYSTEM	Windows XP	Service Pack 2 (Build 2600)
COMP114	International_Sales	192.168.0.42	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP126	International_Sales	192.168.0.236	SYSTEM	Windows XP	Service Pack 3, v.6055 (Build 2
COMP129	First_Floor	192.168.0.77	SYSTEM	Windows XP	Service Pack 2 (Build 2600)
COMP130	Managed Computers	192.168.0.63	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP132	Managed Computers	192.168.0.250	VIRAL	Windows XP	Service Pack 3 (Build 2600)
COMP136	Managed Computers	192.168.0.136	NIRANJAN	Windows XP	Service Pack 3 (Build 2600)
COMP143	First_Floor	192.168.0.45	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP144	Managed Computers	192.168.0.70	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP145	First_Floor	192.168.0.145	SYSTEM	Windows 2003	Service Pack 2 (Build 3790)
COMP147	International_Sales	192.168.0.147	SYSTEM	Windows XP	Service Pack 3, v.6284 (Build 2
COMP15	International_Sales	192.168.0.75	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP151	Managed Computers		SYSTEM	Windows XP	Service Pack 2 (Build 2600)
COMP158	International_Sales	192.168.0.129	SYSTEM	Windows XP	Service Pack 3 (Build 2600)

Figure 123

The View Link

By clicking on the **View** link present in **Software** Column, you can view the list of Softwares along with the installation dates on the Managed Computers. Refer **Figure 124**

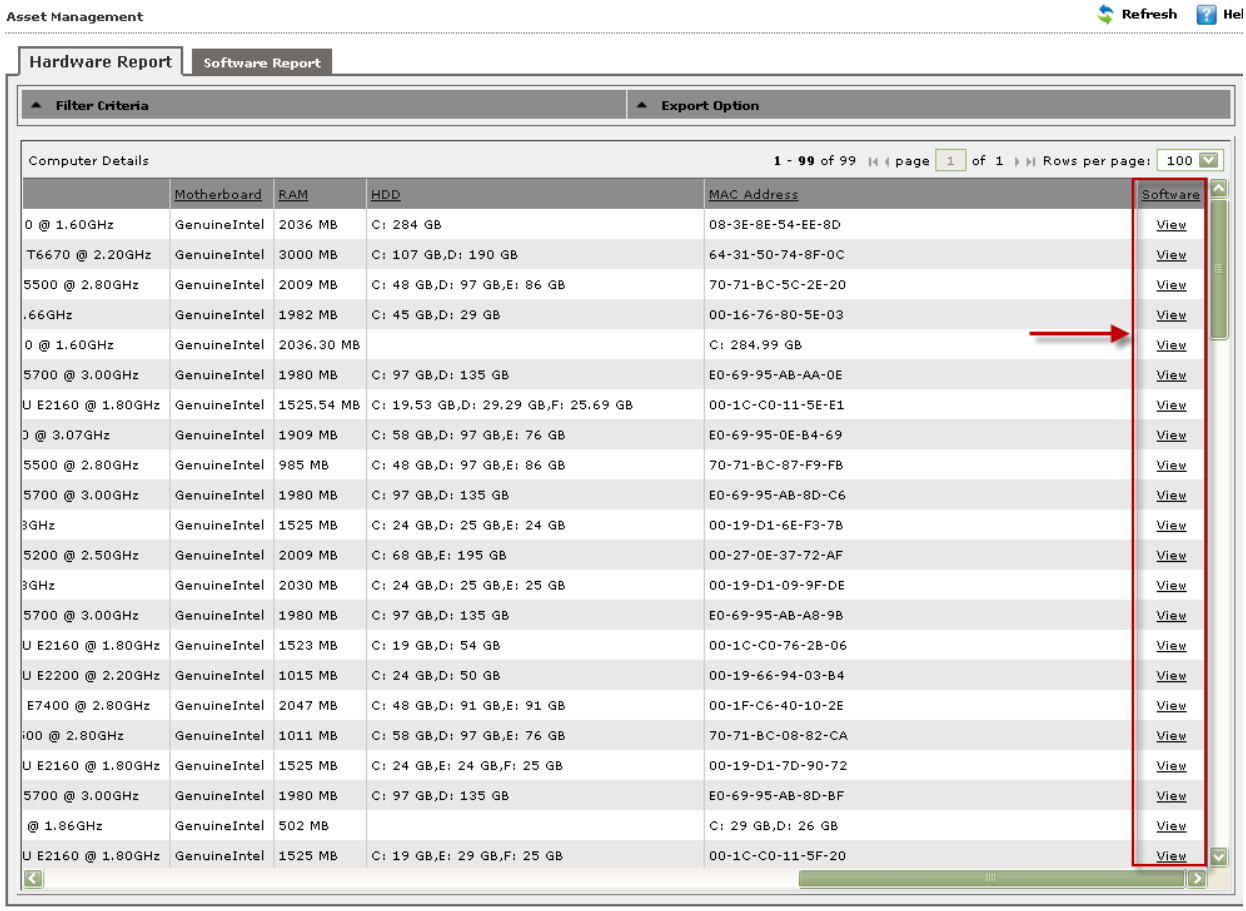


Figure 124

Software List - Refer Figure 125

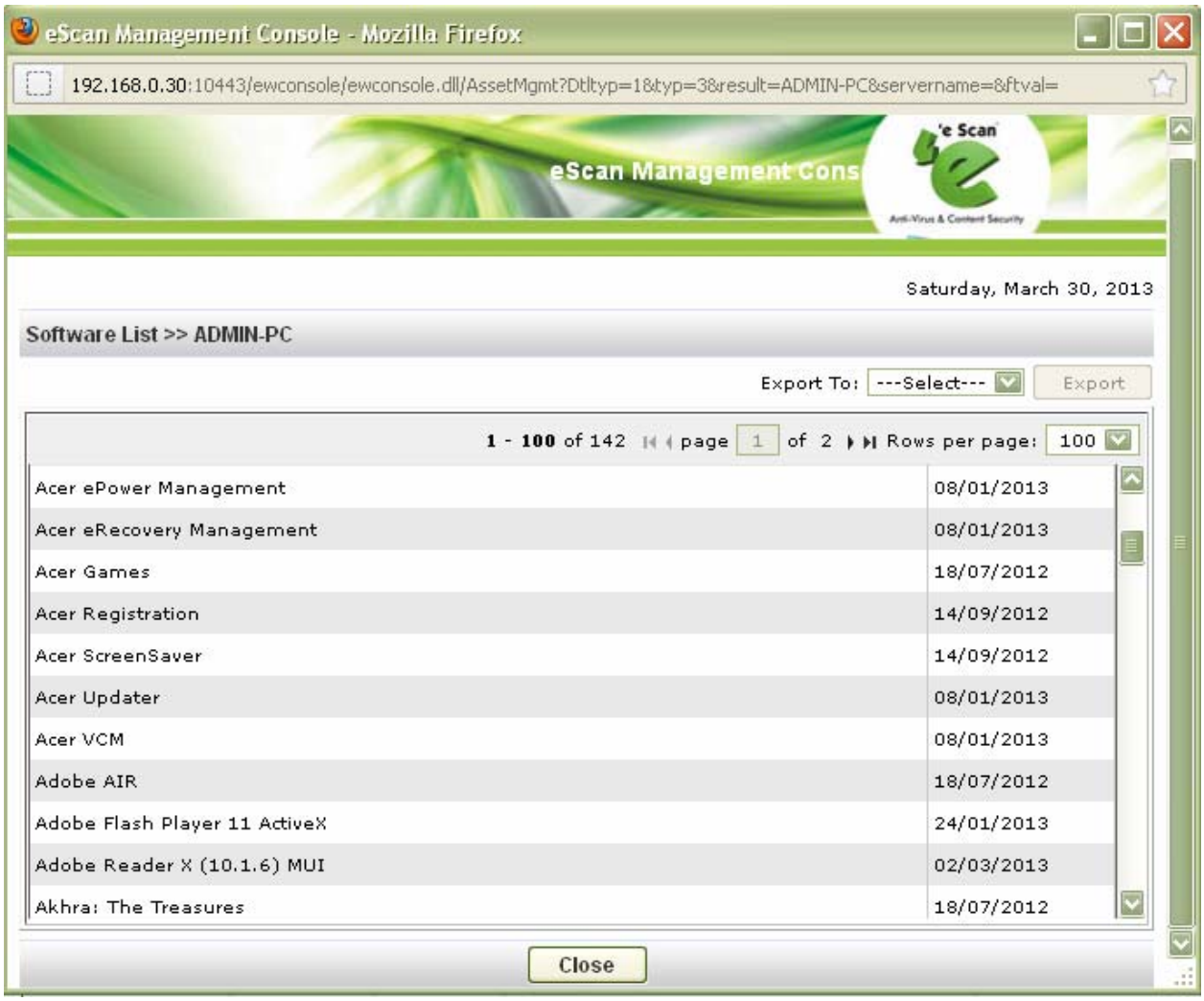
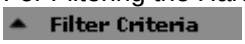


Figure 125

Filter Criteria (Filtering the Hardware Report)

For Filtering the Hardware Report as per your desire, click on the Drop Menu Link of Filter Criteria  in **Asset Management** Section. The Hardware report can be filtered on the basis of following Criteria – **Refer Figure 126**

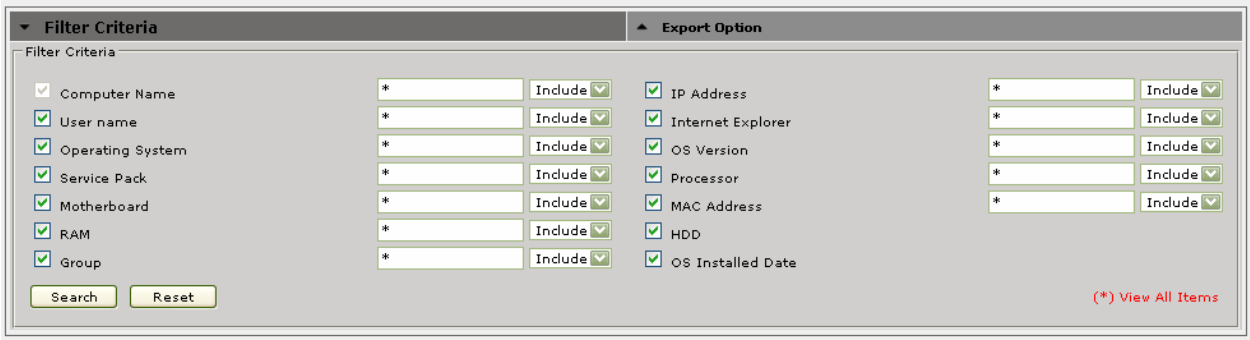


Figure 126

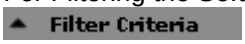
You can define criteria for the text / Column Content to be included or excluded in your Search result using the drop downs present on the interface.

Viewing the Software Report

This section displays list of Softwares along with the number of Managed Computers on which they are installed. To view the Software Report, click on Asset Management and then Click on the 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,

Filter Criteria (Filtering the Software Report)

For Filtering the Software Report as per your desire, click on the Drop Menu Link of Filter Criteria 

in Asset Management Section. The Software report can be filtered on the basis of following Criteria – **Refer Figure 127**

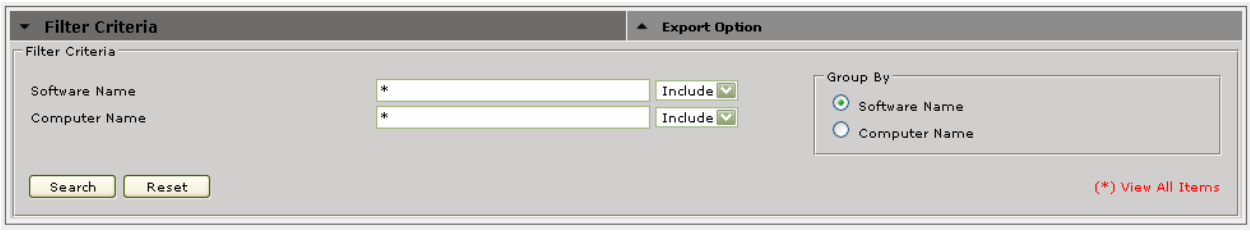


Figure 127

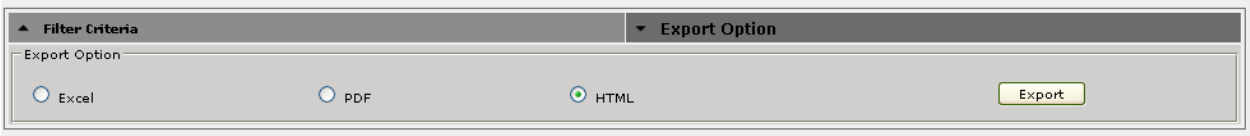
You can filter your search on the basis of Software Name or the Computer Name, using the drop down present on the interface; you can either include the search string entered by you in your search or exclude it if desired. System will populate the results accordingly

Export Options: Exporting the Hardware / Software Report

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

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

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



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 shown above.

Chapter 12 – Print Activity

It monitors and Logs printing tasks done by all the Managed computers, it gives you a report of all Printing Jobs done by Managed computers 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.

The log report generated in this section keeps the log of Number of Copies Printed through any printer, the Document 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 on the Print Activity option present 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 128**

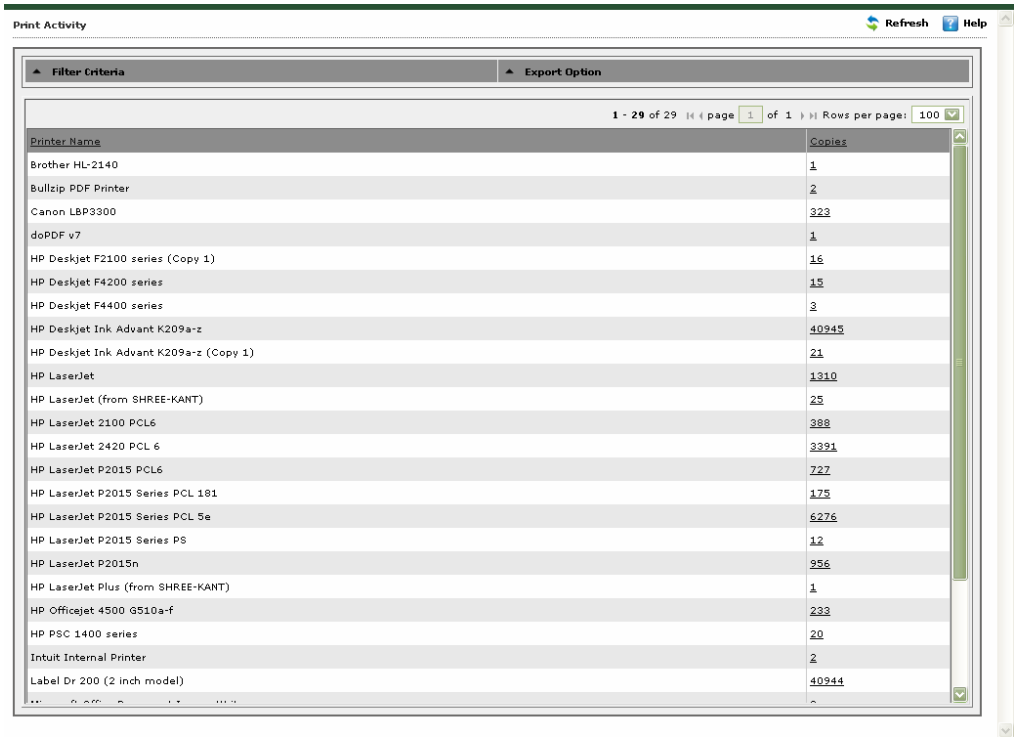


Figure 128

Viewing the Print Logs

For viewing the Printing 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 129**

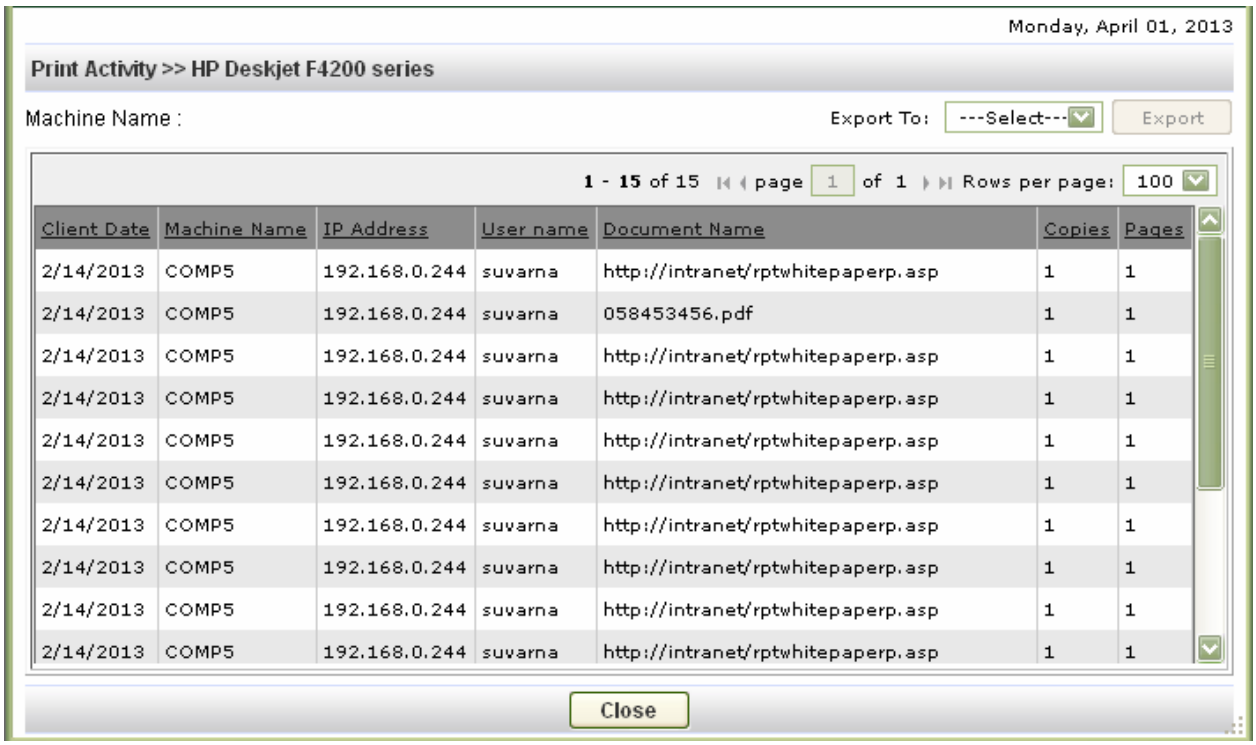
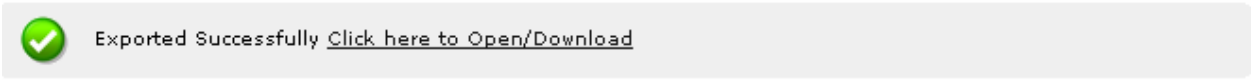


Figure 129

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 on the Export button present beside it. After the Export is complete you will be informed through the following message



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

Filter Criteria

For Filtering the Print Activity Log as desired, click on the Filter Criteria option present on the main interface of Print Activity section, following options will be populated on screen. **Refer Figure 130**

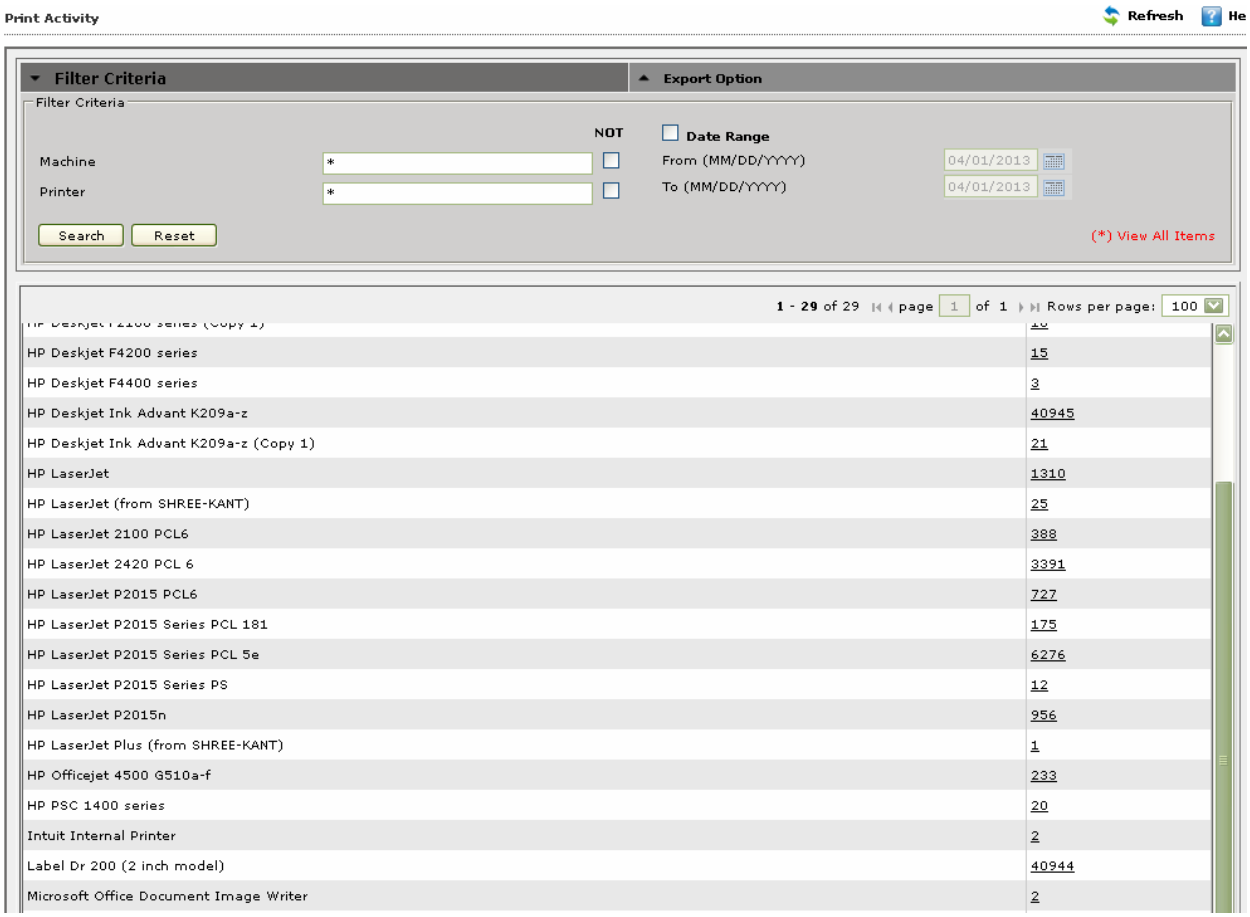


Figure 130

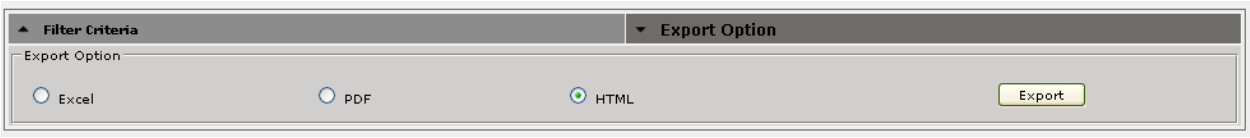
S.No.	Option	Description
1.	Machine	Type the desired Machine name that you wish to exclude or include in your Log.
2.	Not	Tick on this checkbox, if you wish to exclude a Machine in the Log report.
3.	Printer	Type the desired Printer name that you wish to exclude or include in your Log.
4.	Not	Tick on this checkbox, if you wish to exclude a Printer to be included 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 on this option top Filter the Log on the defined criteria.
9.	Reset	Click on this option to reset the defined criteria for filtering.

Exporting the Print Activity Log

eScan Management Consoles offers Exporting of Print Activity logs in PDF, Excel or HTML formats.

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

in Print Activity Section. It will display the following options.



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 shown above.

Chapter 13: Management of Unmanaged Computers

The **Unmanaged Computers** section provides you with information about the computers that have not yet been assigned to any computer group.

On the navigation bar, there are four nodes under **Unmanaged Computers: Network Computers**, **IP range**, and **Active Directory**, **New Computers found**

- The Network Computers page displays the hierarchy of the domains, workgroups, and computers in your network. The computers displayed here are not part of any computer group defined in the eScan Web Console. If you add a computer to a computer group, its entry is removed from the hierarchy.
- The IP range page shows the hierarchical structure of the IP ranges available in the network.
- The Active Directory page shows the hierarchical structure of the active directory domains in the network.

The console tree in each of the pages is updated automatically by the eScan Web Console by using a polling mechanism. You can also update the information manually by pressing the F5 key or by clicking **Refresh** on the top right corner of the page.

The eScan Web Console 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 menu appears on all the pages under **Unmanaged Computers**.

The **IP range** and the **Active Directory** pages contain menus other than the **Action List** menu. These menus allow you to perform additional management tasks, which include creating a new IP range, deleting an existing IP range, or viewing the properties of the domain controller.

You can do the following activities:

- Network Discovery
- Network Computers
- IP Range
- Active Directory

Network Discovery

The eScan Web Console periodically updates the hierarchy displayed in the console tree in the **Network Computers**, **IP range**, and **Active Directory** pages by polling mechanism. This mechanism polls the network neighbourhood, IP range, and Active Directory on a periodic basis and updates the information displayed in the console tree based on the results.

The types of polling used by the eScan Web Console are as follows:

- **Network Neighbourhood:** The eScan Web Console obtains information about all the network computers, domains and workgroups with their operating systems, IP address, status of eScan, version of eScan, and so on while polling the network neighbourhood.
- **IP range:** The eScan Web Console polls the available IP ranges by sending out ICMP packets and collects information about the computers on each IP range.
- Active Directory: The eScan Web Console polls the active directory and displays the retrieved information.

The computers which have not been assigned to any computer group are added to the **Unmanaged Computers** console tree.

Network Computers

The **Network Computers** page displays the client computers and workgroups in the network in a console tree. You can click the name of a computer or group to view its details in the task pane in the form of a table. The table displays information, such as the computer name, name of the group, IP address, eScan status, version of eScan installed, last connection, path of the installed directory, status of the monitor, status of the Anti-Spam, Mail Anti-Virus, Web Protection, Endpoint Security, and Firewall modules, status of the server, date and time when the client computer was last updated, IP address of the update server, operating system on the client computer, and the status of client computer (if eScan installed).

This page also displays a **Search** button, which allows you to search for computers and add them to the Client Computers group or any other user-defined group.

You can do the following activities:

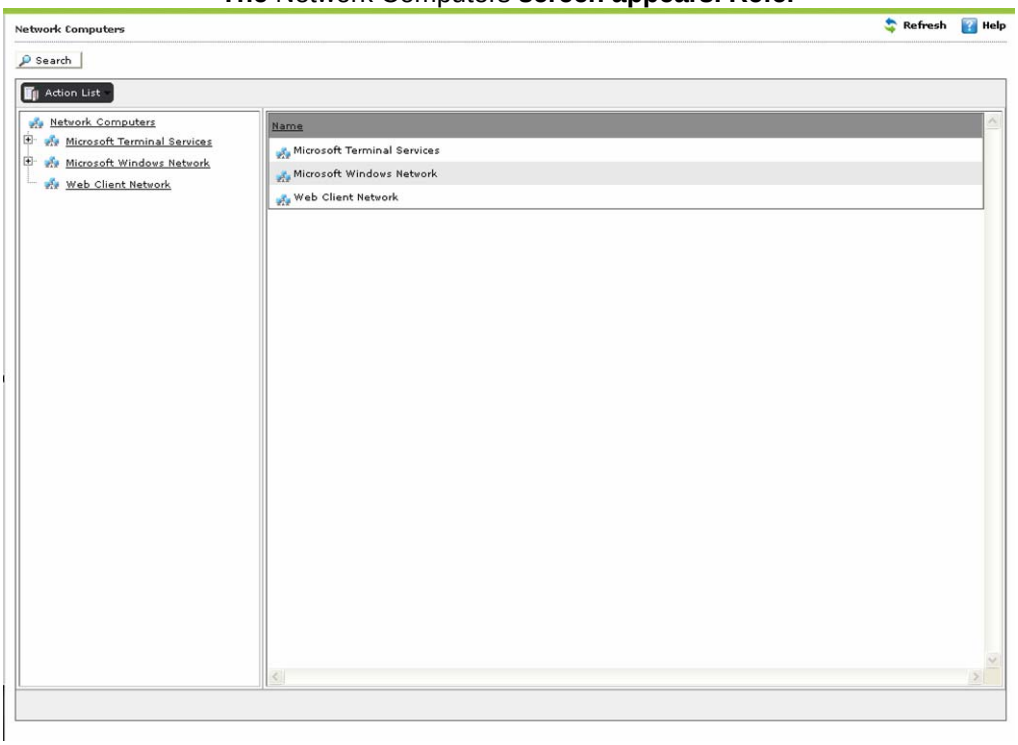
- Accessing the Search Feature
- Setting the Host Configuration
- Moving Computers to Group
- Viewing the Properties

Accessing the Search Feature

At times, you may need to add a particular computer to a group, but you may not have a clear idea of the workgroup to which it belongs. The Search feature of the eScan Web Console comes handy in such situations.

To access search feature

On the navigation pane, click Unmanaged Computers**, and then click** Network Computers**.**
The Network Computers **screen appears. Refer**



1. **Figure 103.**

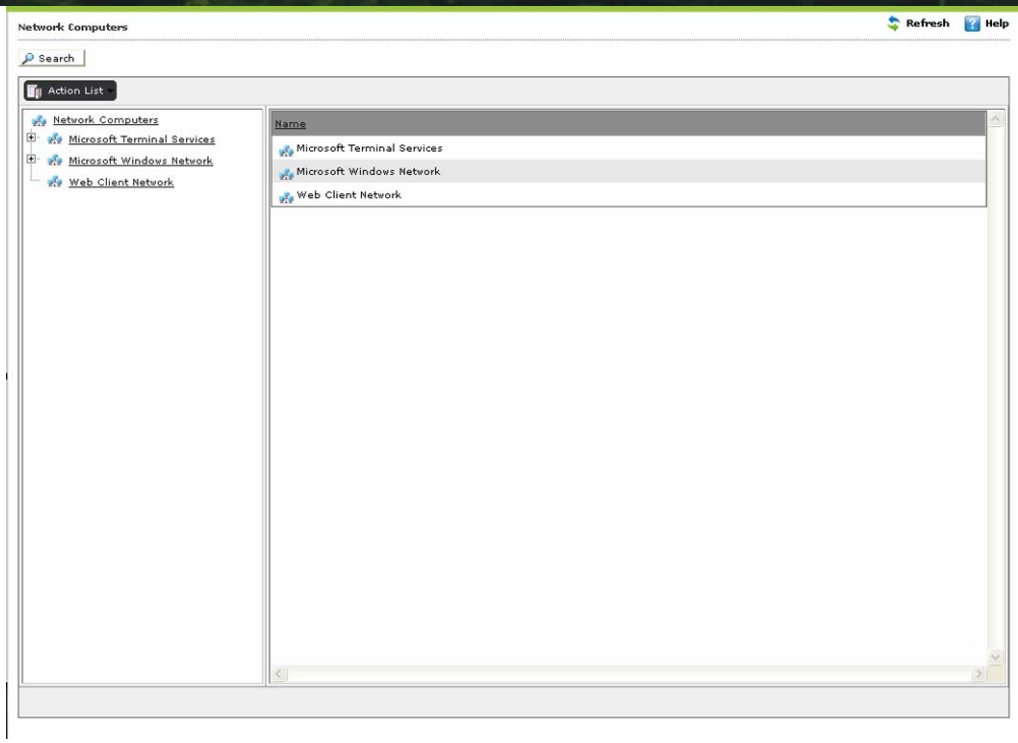
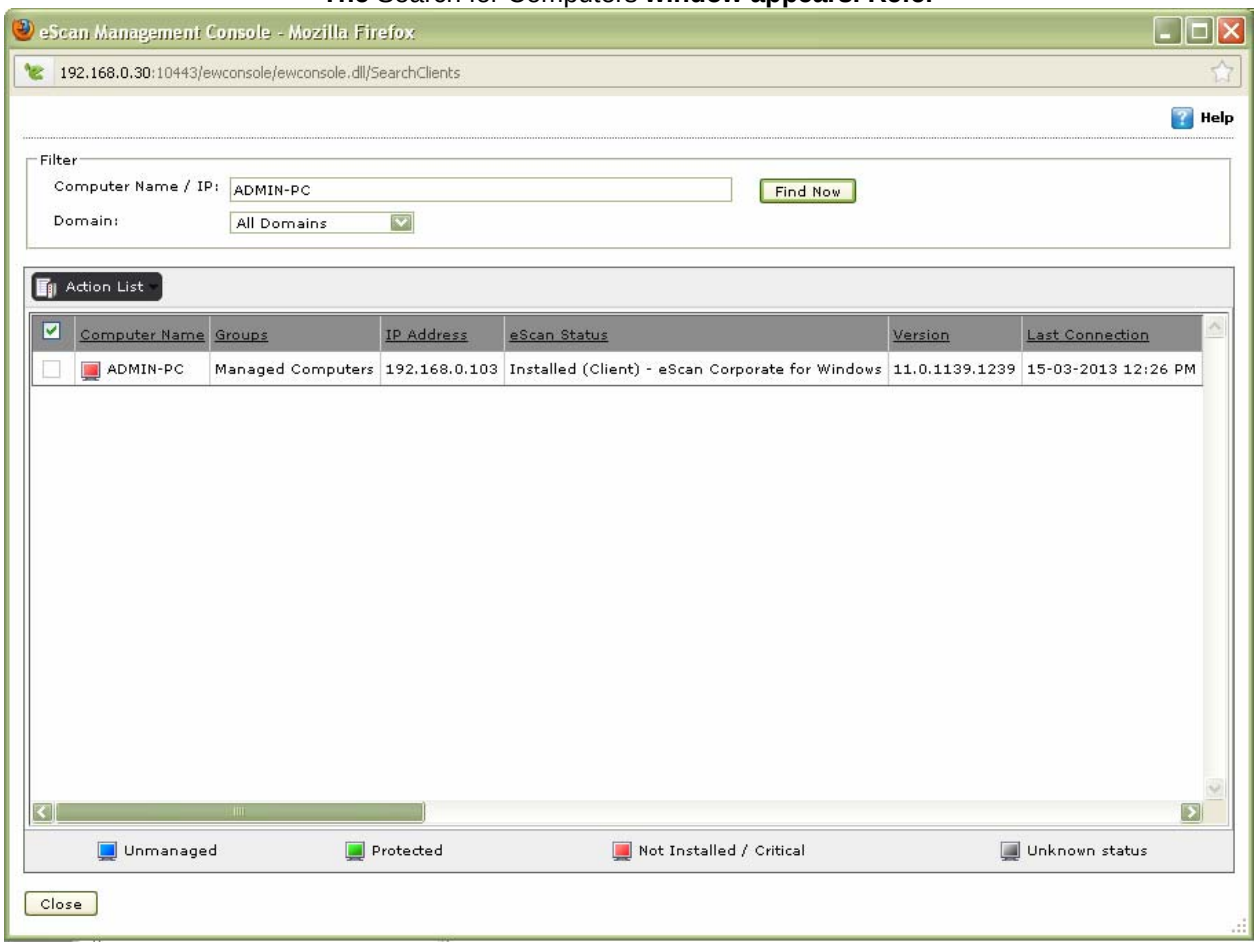

Network Computers
Refresh
Help
Search
Action List
Network Computers
Microsoft Terminal Services
Microsoft Windows Network
Web Client Network
Name
Microsoft Terminal Services
Microsoft Windows Network
Web Client Network

Figure 103

At the upper left side, click the Search **button.**
The Search for Computers **window appears. Refer**



2. Figure 104.

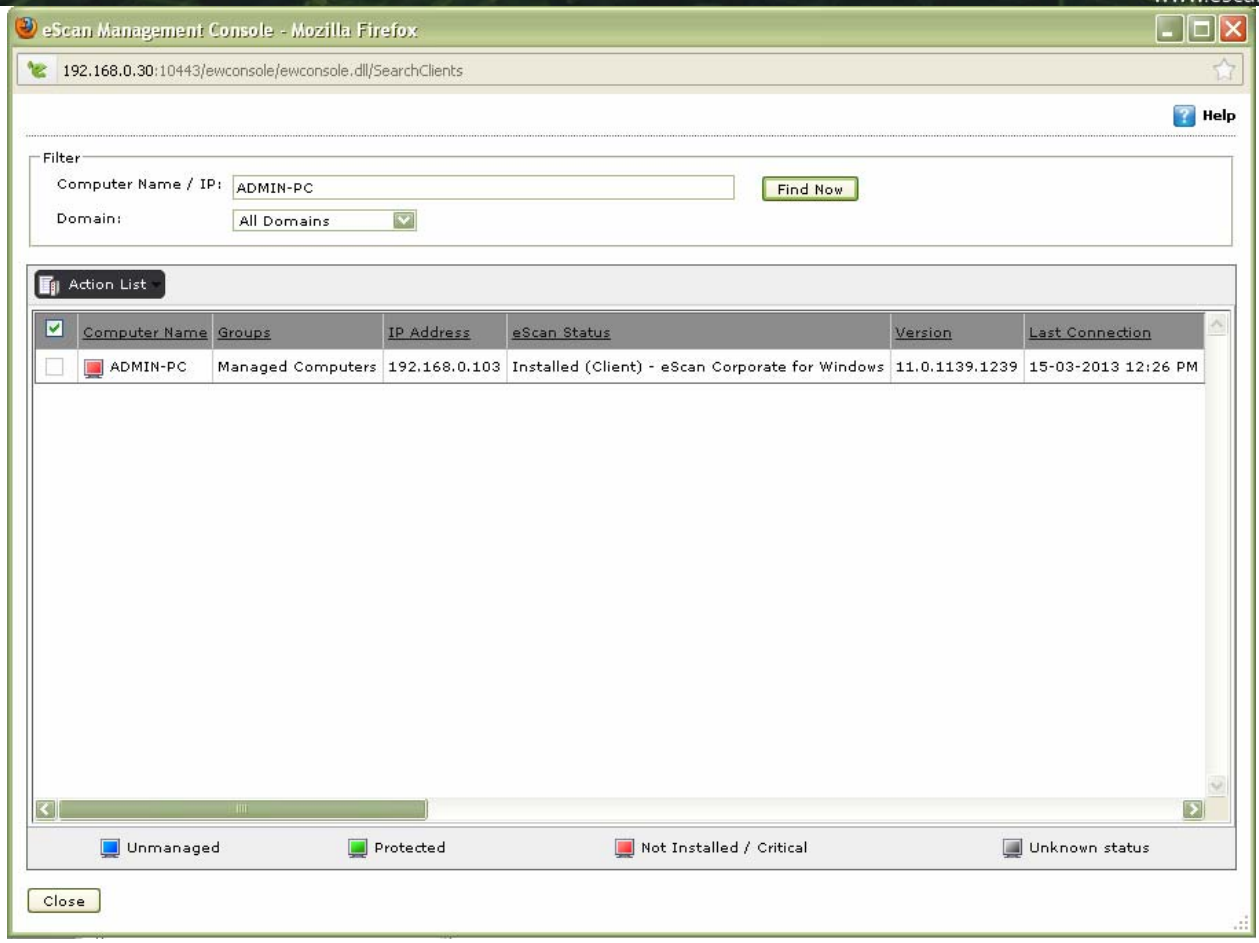


Figure 104

3. Under **Filter** section, in the **Computer Name** field, type the computer name that you want to search.

   For example, if you are searching for a computer named “Comp20” in your network, you can specify **Comp20** in the **Computer Name** field. However, if you want to find all computers whose names begin with text string “Comp,” you need to specify only **Comp*** in the **Computer Name** field.

4. Select the type of domain from the **Domain** drop-down list.

5. Click the **Find Now** button.
   The following field details appear in a tabular format.

- The name of the computer
- The name of the group
- The IP address of the computer
- The status of eScan, whether it is installed on the computer or not
- The version of eScan
- Last connection
- The directory in which eScan is installed on the computer
- The status of the eScan monitor
- The status of the Anti-Spam, Mail Anti-Virus, Web Protection, Endpoint Security, and Firewall modules

- The timestamp of the last update
- The name of the update server
- The operating system installed on the computer
- The status of the eScan installation, whether it has all the critical patches and hotfixes installed on it or not

The  symbol indicates status as unmanaged,  symbol indicates status as protected,  symbol indicates status as not installed/critical, and  symbol indicates status as unknown.

6. Click the **Action List** menu, if you want to set host configuration, move computers to group, and to view properties. For more information, refer Moving Computers to Group section.

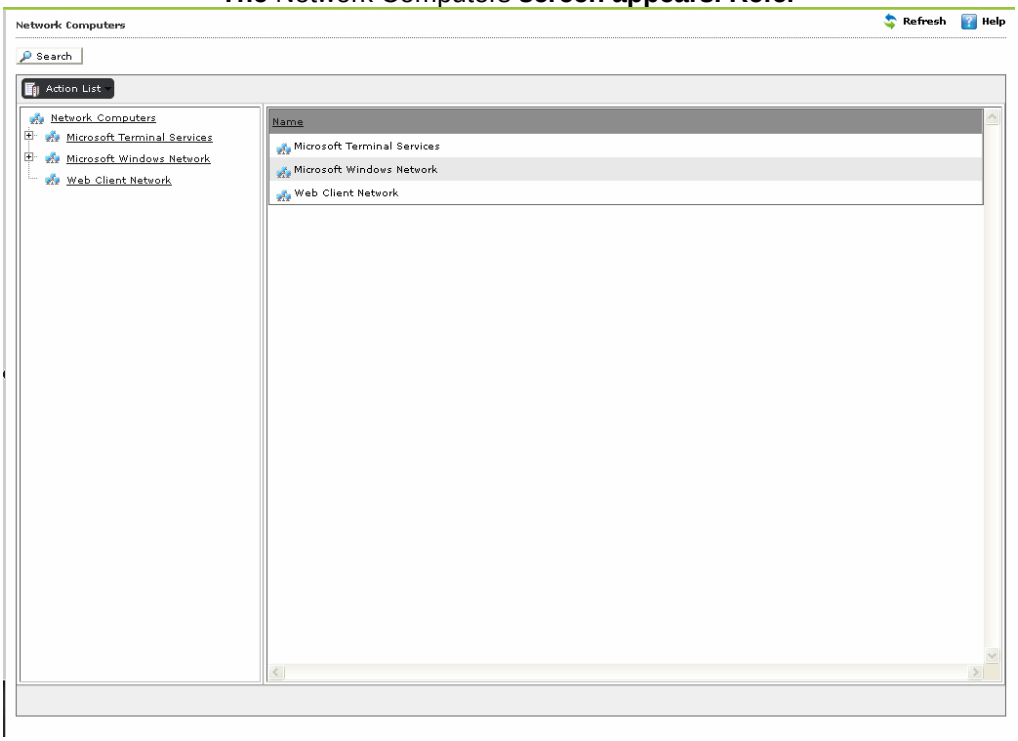
Setting the Host Configuration

It enables you to set basic login information for the host computer.

If the computer that you want to log on is part of a domain, then you must specify the domain name along with the user name while logging in. For example, if the computer **Mrktng1** is within the **Marketing** domain and you want to log on as an Administrator, you must specify the user name as **Marketing\Administrator** when you log on to the computer.

To set host configuration

On the navigation pane, click Unmanaged Computers**, and then click** Network Computers**.**
The Network Computers **screen appears. Refer**



1. Figure 105.

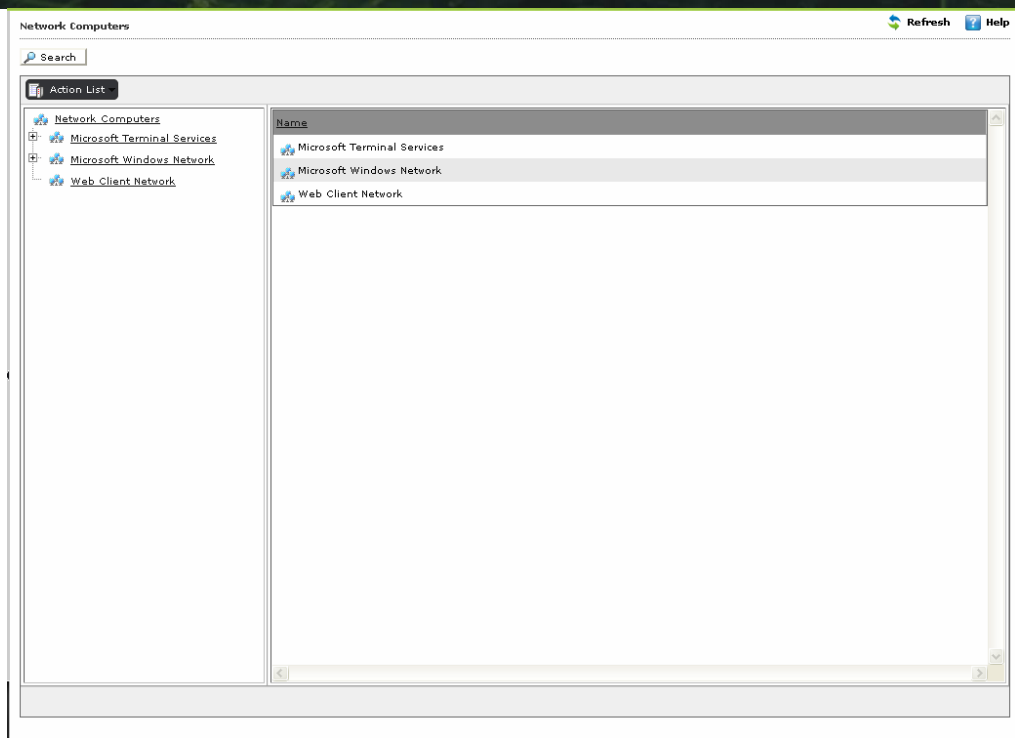
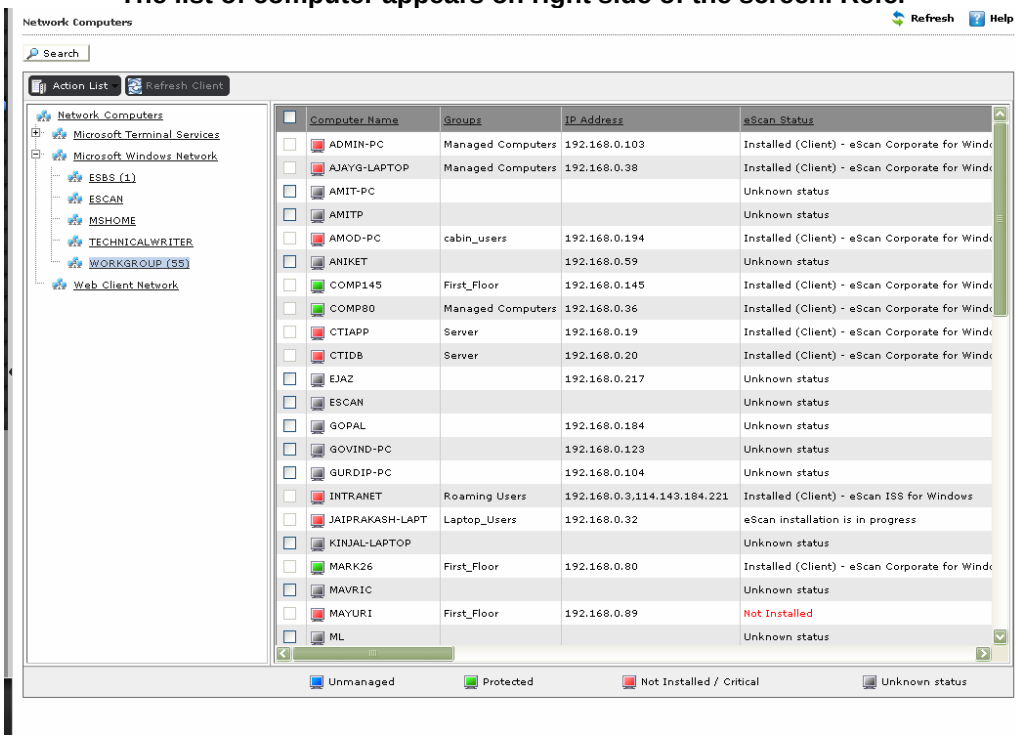

Network Computers
Refresh
Help
Search
Action List
Network Computers
Microsoft Terminal Services
Microsoft Windows Network
Web Client Network
Name
Microsoft Terminal Services
Microsoft Windows Network
Web Client Network

Figure 105

On the left pane, under Network Computer**, click an appropriate domain/workgroup. The list of computer appears on right side of the screen. Refer**



2. Figure 10634.

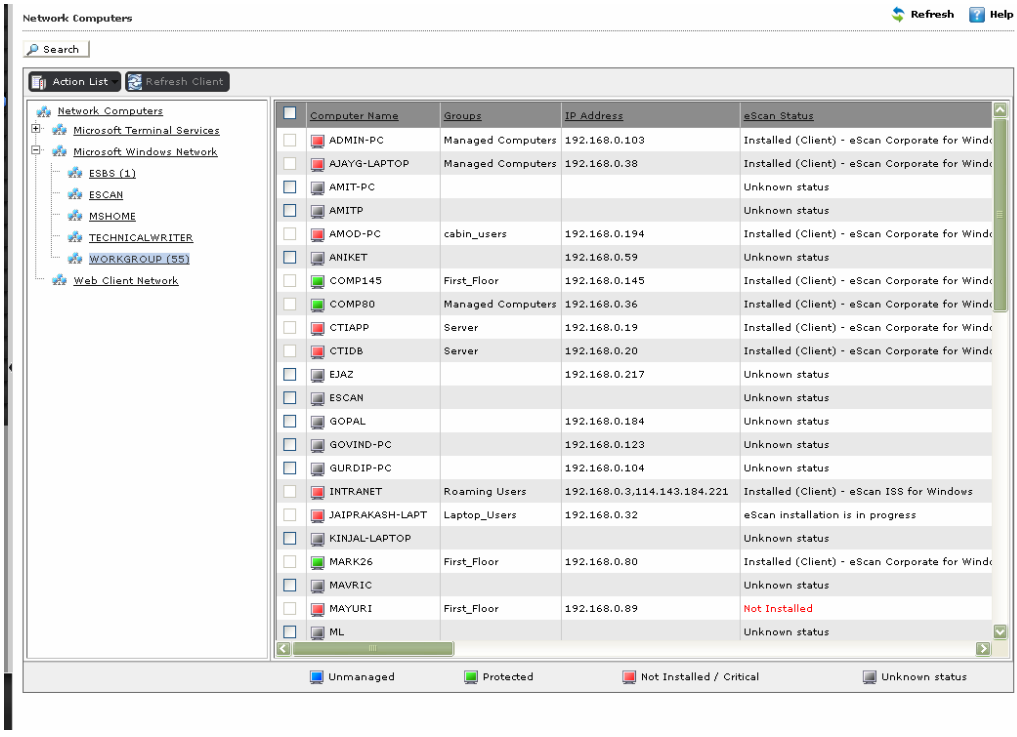


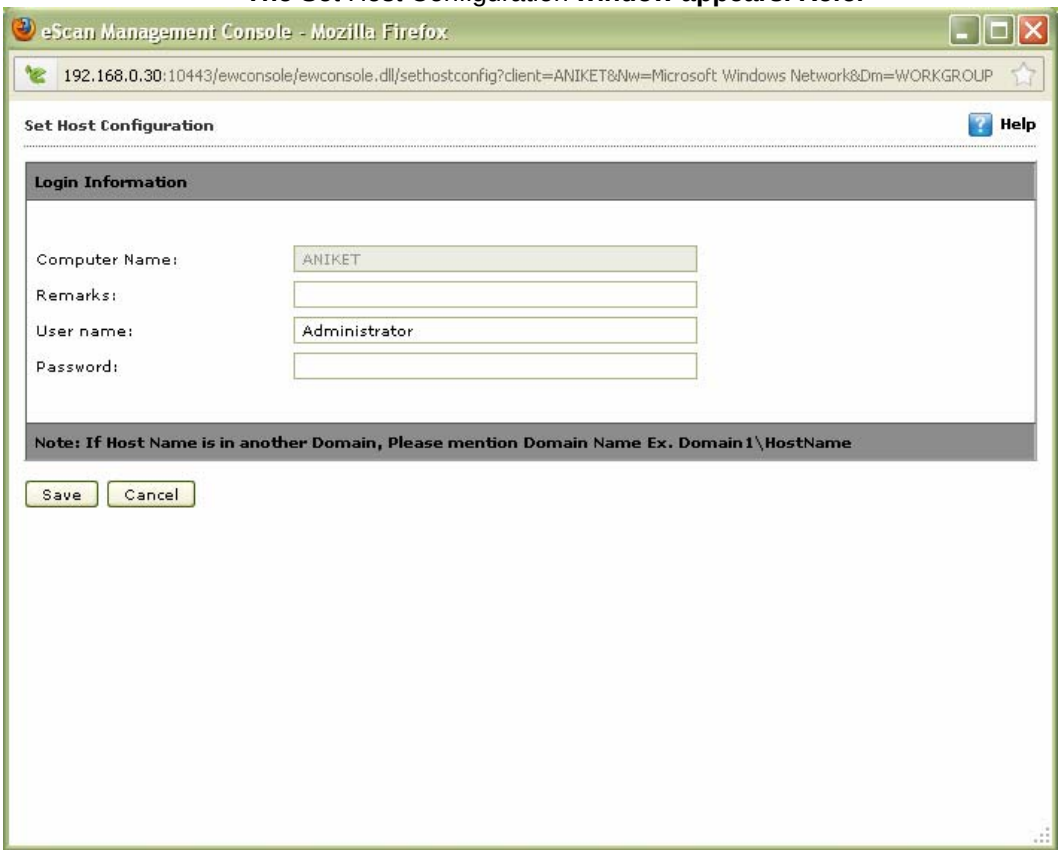
Figure 10634

The symbol indicates status as unmanaged, symbol indicates status as protected, symbol indicates status as not installed/critical, and symbol indicates status as unknown.

3. Select an appropriate computer name check box for which you want to set configuration.

The **Set Host Configuration** menu and **Refresh Client** button is available, only when you select an appropriate computer name check box from the list.

Click the Action List **drop-down menu, and then click** Set Host Configuration**.**
The Set Host Configuration **window appears. Refer**



4. Figure 10735.

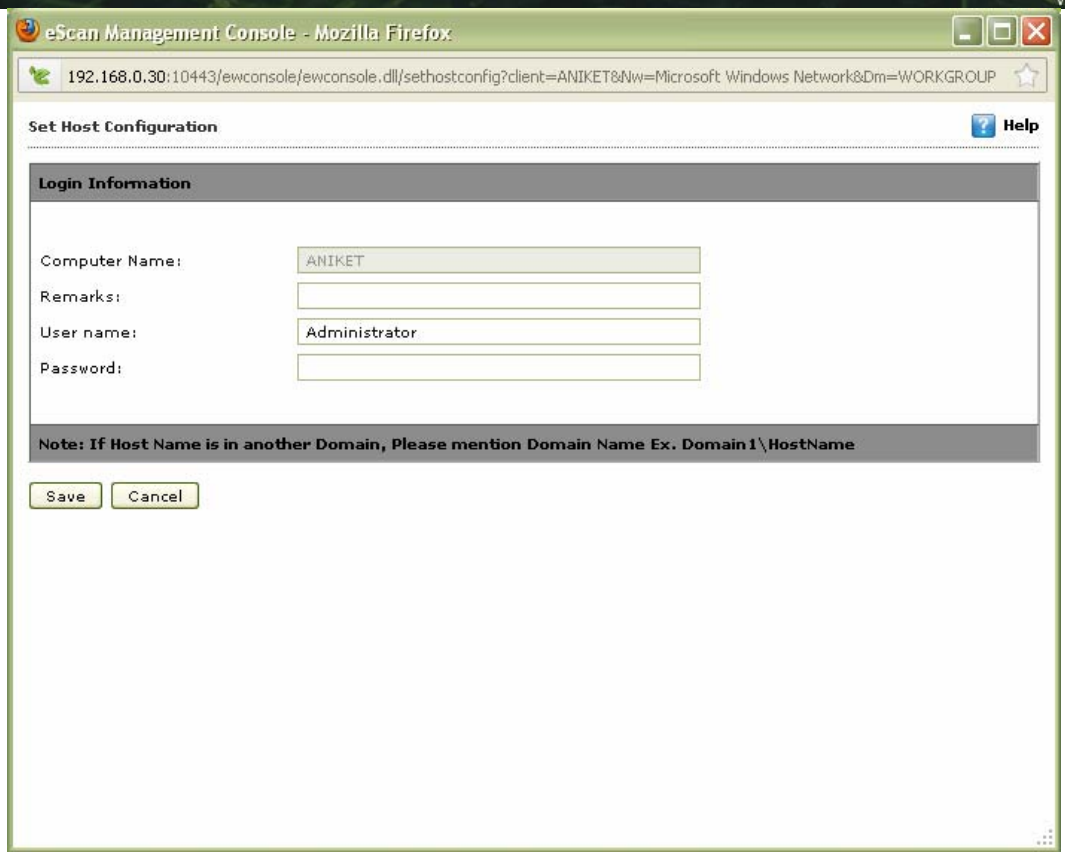


Figure 10735

5. Specify the following field details.

Field	Description
Login Information	
Computer Name	It displays the name of selected computer. It appears dimmed.
Remarks	Type the remarks, if any.
User name	Type the login user name of selected user.
Password	Type the password of selected user.

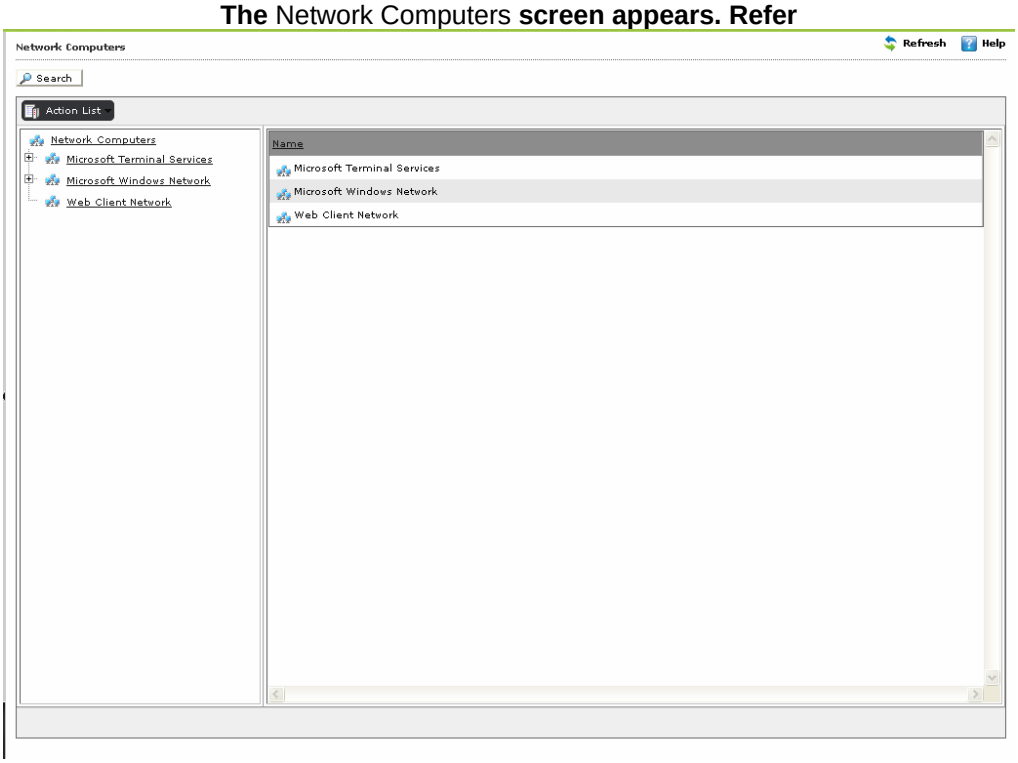
6. Click the **Save** button.
   The login information gets saved.

Moving Computers to Group

It enables you to move computers to either the managed computer group or any of its sub-groups.

To move computers to group

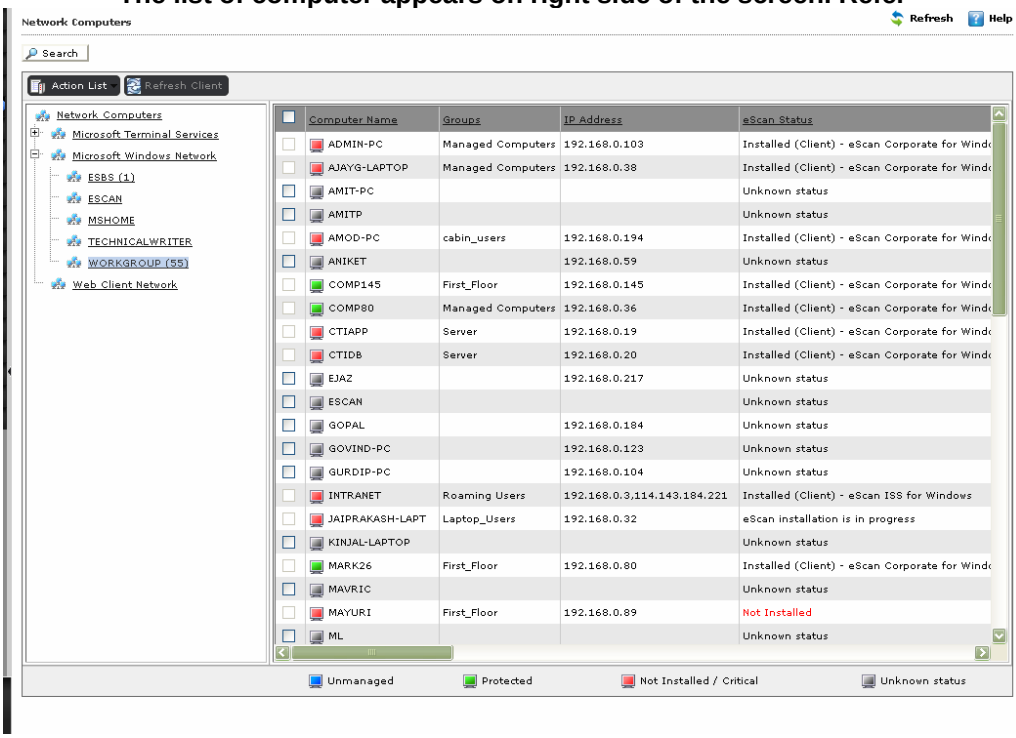
On the navigation pane, click Unmanaged Computers**, and then click** Network Computers**.**
The Network Computers **screen appears. Refer**



1. Figure 10533.

Click the (+) sign to expand the folder and view the options and click the (-) sign to collapse the required folder.

On the left pane, under Network Computers**, click an appropriate domain/workgroup. The list of computer appears on right side of the screen. Refer**



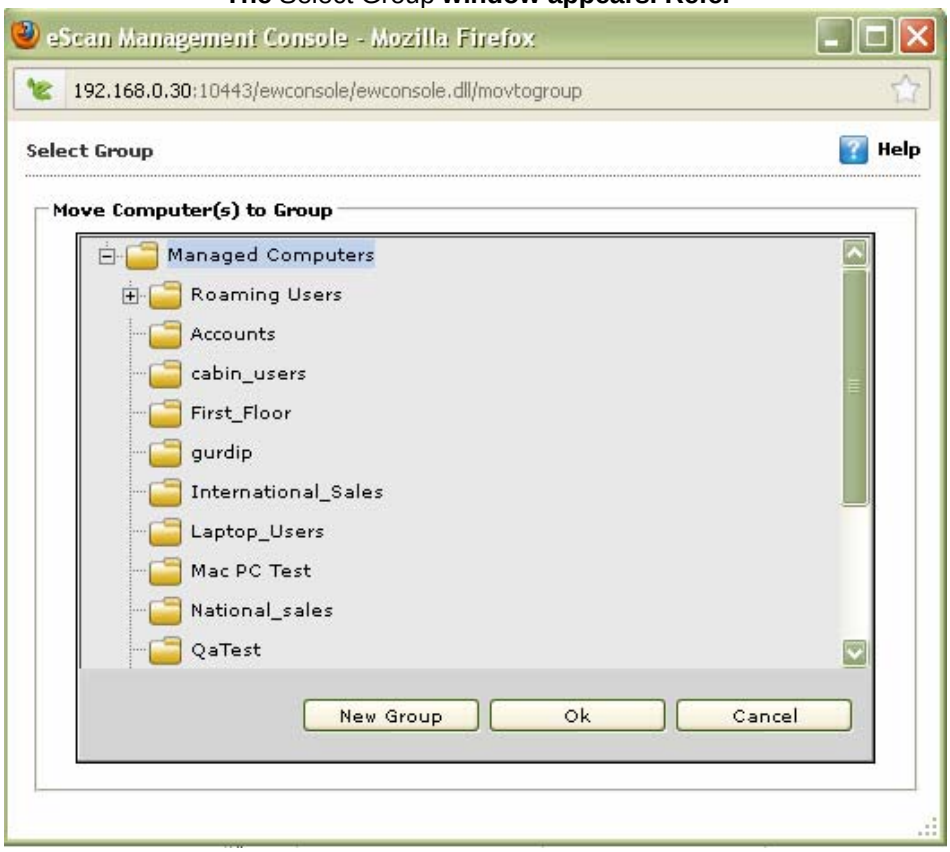
2. Figure 10634.

The symbol indicates status as unmanaged, symbol indicates status as protected, symbol indicates status as not installed/critical, and symbol indicates status as unknown.

3. Select an appropriate computer name check box that you want to move to group.

The **Move to Group** menu and **Refresh Client** button is available, only when you select an appropriate computer name check box from the list.

Click the Action List **drop-down menu, and then click** Move to Group**.**
The Select Group **window appears. Refer**



4. Figure 10836.

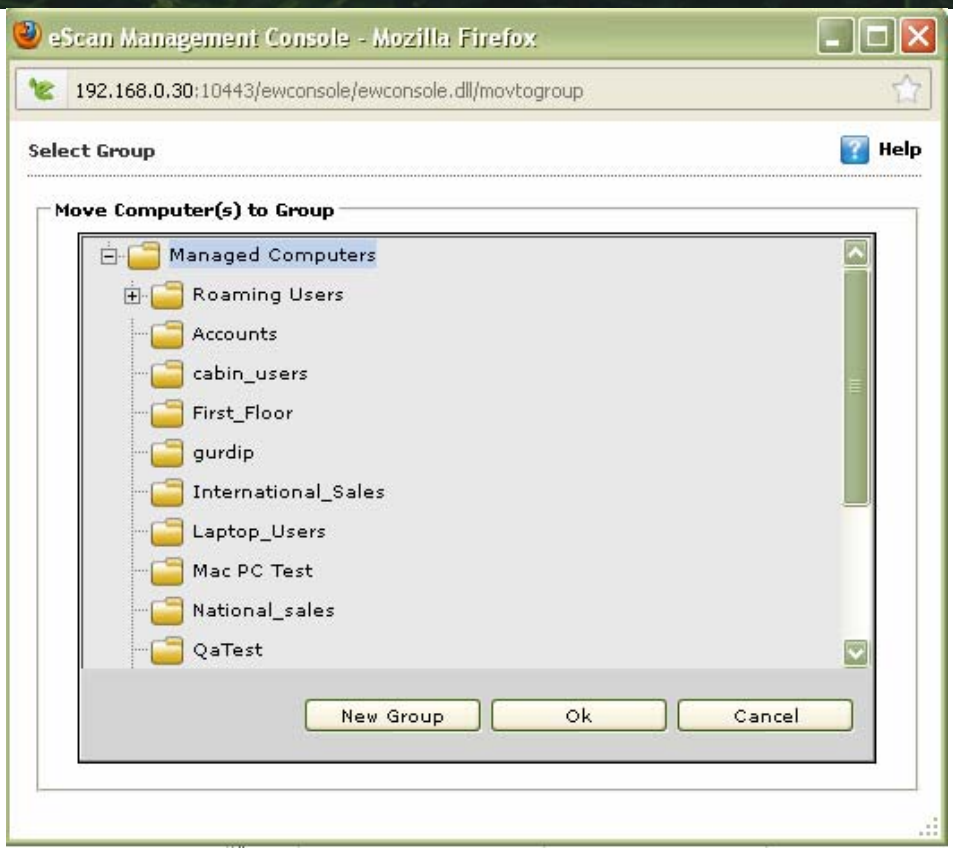


Figure 10836

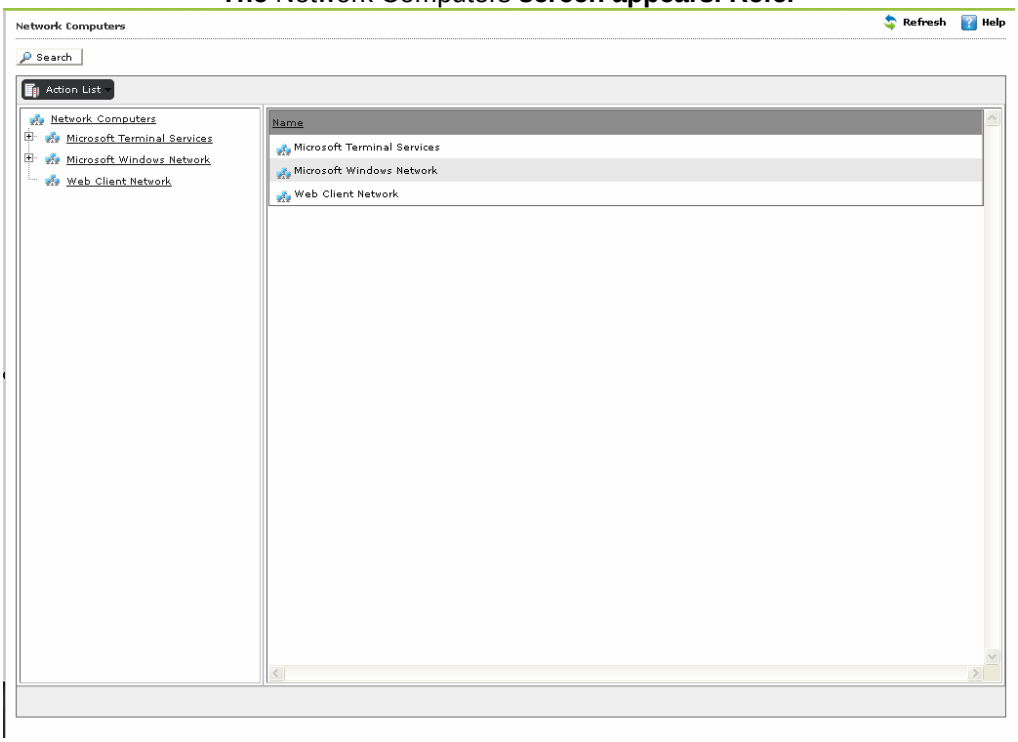
5. Under **Move Computer(s) to Group** section, click the group in which you want to move, and then click **Ok** button.
6. If you want to create new group, click **New Group** button, and then specify name to a group. You can either create a New Group under Managed computers or any of its sub-groups.

Viewing the Properties

It enables you to view properties of the selected computer. The properties are divided in to three sections – **General**, **AV-Status**, and **Protection**.

To view the properties

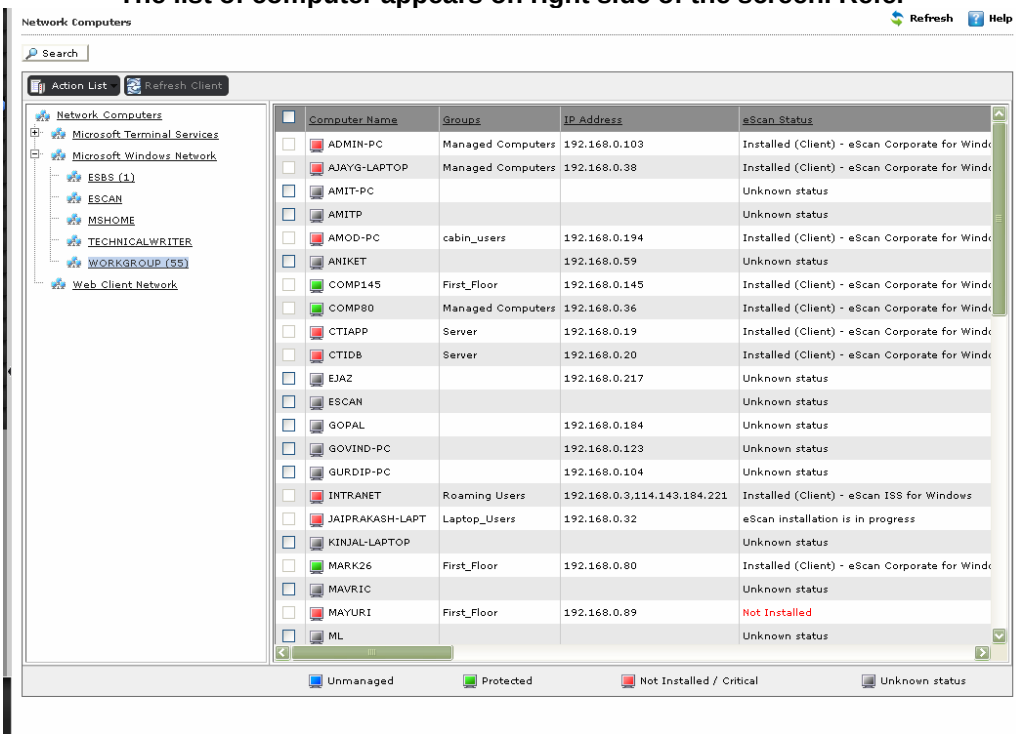
On the navigation pane, click Unmanaged Computers**, and then click** Network Computers**.**
The Network Computers **screen appears. Refer**



1. Figure 10533.

Click the (+) sign to expand the folder and view the options and click the (-) sign to collapse the required folder.

On the left pane, under Network Computers**, click an appropriate computer. The list of computer appears on right side of the screen. Refer**



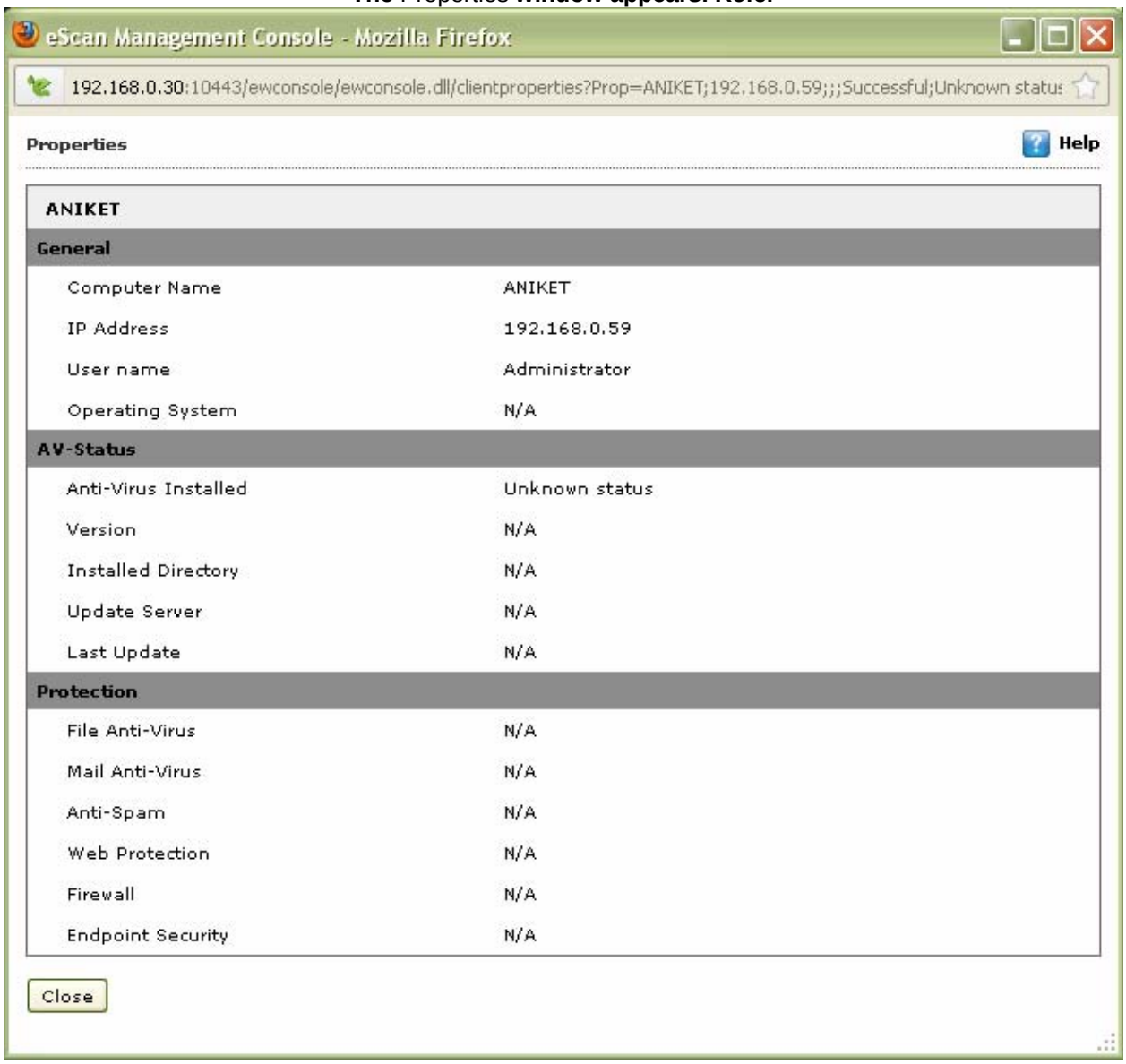
2. Figure 10634.

The 🖥 symbol indicates status as unmanaged, 🖥 symbol indicates status as protected, 🖥 symbol indicates status as not installed/critical, and 🖥 symbol indicates status as unknown.

3. Select an appropriate computer name check box for which you want to view properties.

The **Properties** menu and **Refresh Client** button is available, only when you select an appropriate computer name check box from the list.

Click the Action List **drop-down menu, and then click** Properties**.**
The Properties **window appears. Refer**



4. Figure 10937.

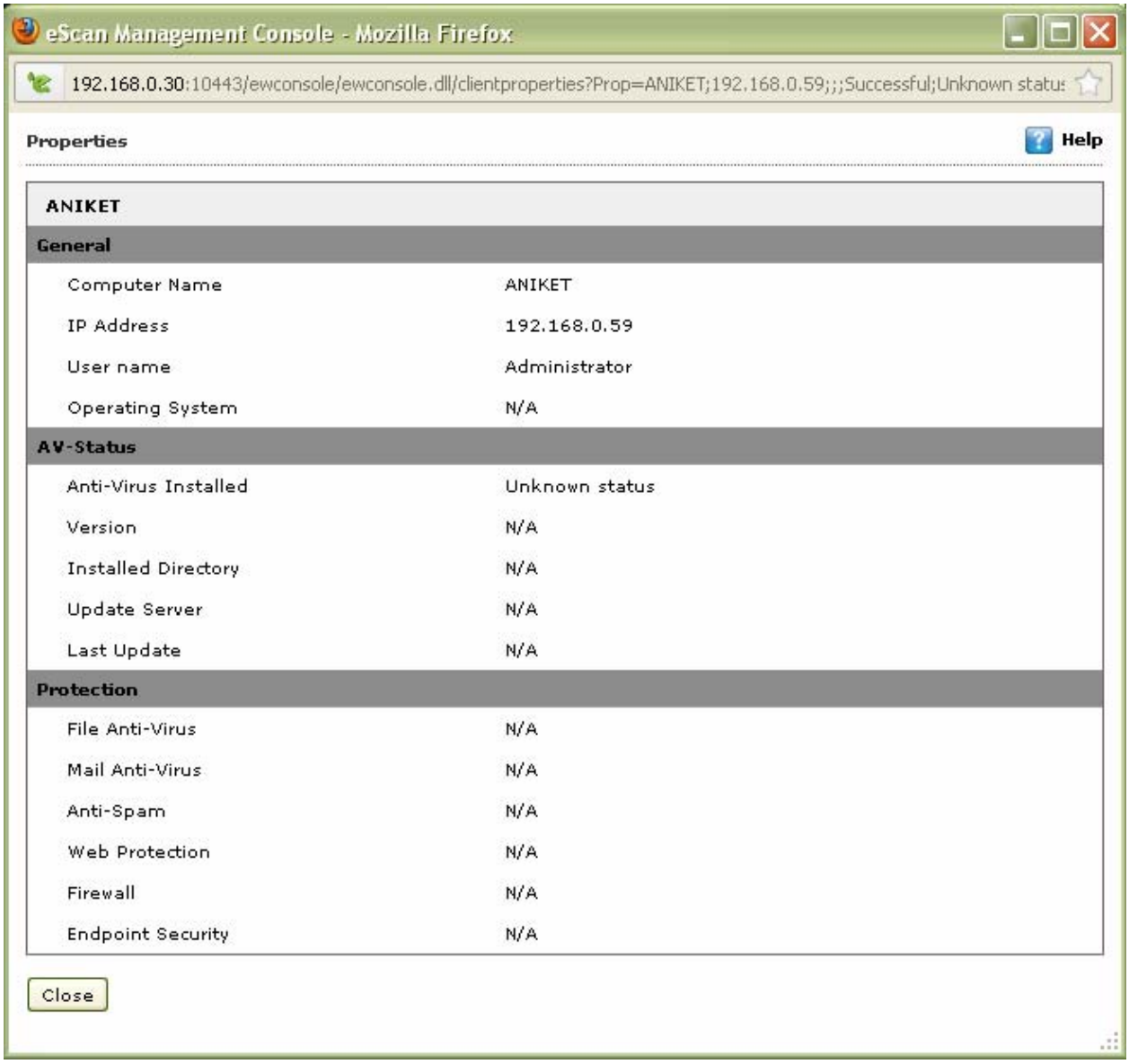


Figure 10937

5. View the following field details as required:

The status N/A appears incase if eScan is not installed on selected computer and when the selected host details are not available on eScan server.

Field	Description
General	
This section provides you the following basic details: • Computer Name • IP Address • User name • Operating System	
AV – Status	
Anti-Virus Installed	It indicates status whether Anti-Virus is installed or not, and also version name of eScan installed on the selected computer.
Version	It indicates version of eScan installed.
Installed Directory	It indicates installation path of eScan.
Update Server	It indicates IP address of the update server or internet address. In case, if the selected computer downloads the virus signature updates directly from the internet.
Last Update	It indicates the date when selected computer was last updated.
Protection	
This section provides you the status details of following eScan modules whether they are enabled or disabled on the client machine: • File Anti-Virus • Mail Anti-Virus • Anti-Spam • Web Protection • Firewall • Endpoint Security • Privacy Control	

IP Range

The **IP Range** page allows you to specify a certain number of IP range. You can view the list of computers within the specified IP range in the console tree. If you want, you can click a node from the console tree to view the list of computers within that IP range. You can click the IP range to view its details in the task pane in the form of a table. The table displays information such as the computer name, groups, IP address, eScan status, eScan version, last connection, path of the installed directory, status of the monitor, status of the Anti-Spam, Mail Anti-Virus, Web Protection, Endpoint Security, and Firewall modules, status of the server, date and time when the client computer was last updated, IP address of the update server, operating system on the client computer, and the status of client computer (if eScan installed).

You can also add a new IP range by clicking **New IP Range** and remove existing IP ranges by clicking **Delete IP Range**.

You can do the following activities:

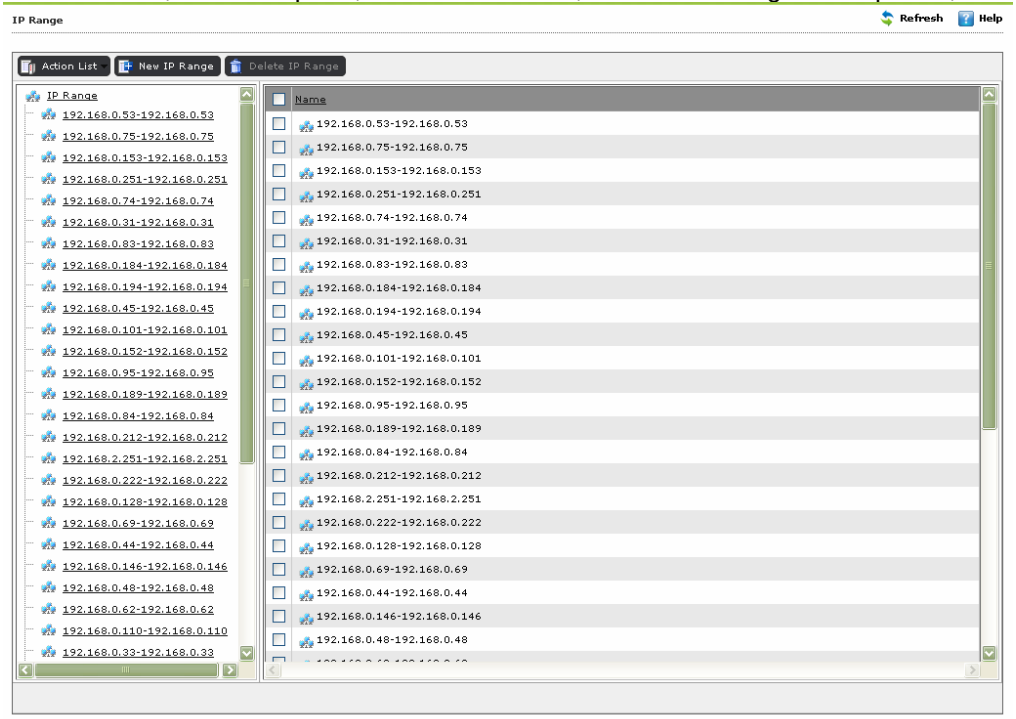
- Create a New IP Range
- Delete an Existing IP Range

Create a New IP Range

For ease of management of computers and for the deployment of policies, specific IP ranges are defined. The eScan Web Console also allows you to create IP ranges based on your requirements.

The steps to create a new IP range are as follows:

1. In the eScan Web Console, in the left pane, under Dashboard, under Unmanaged Computers, click IP range. Refer **Figure** 110**.**



2.

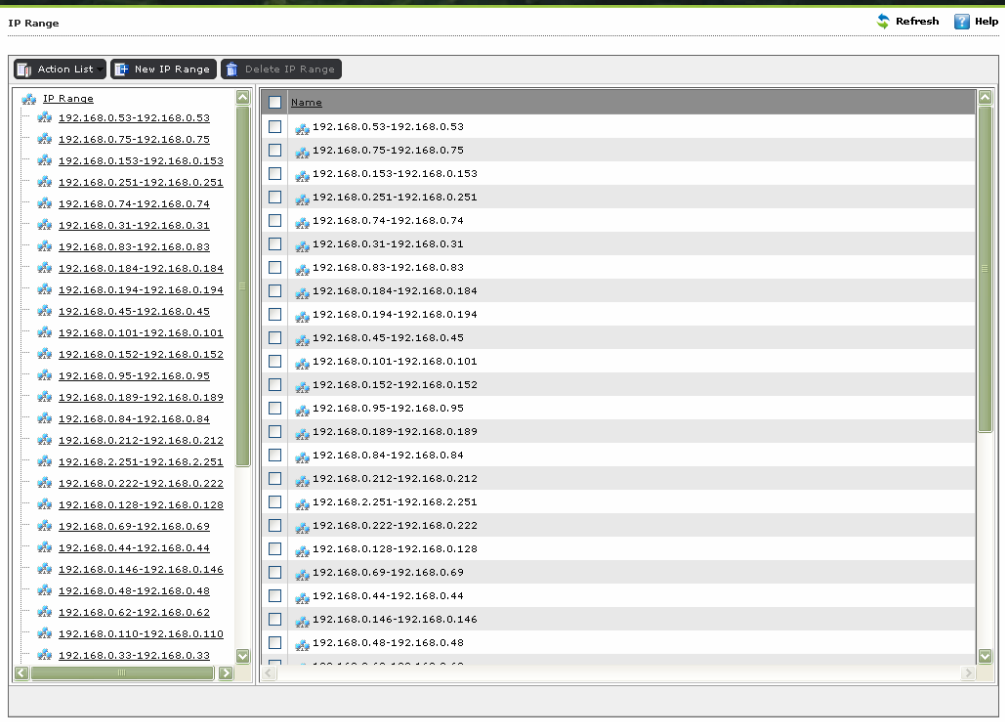


Figure 110

3. On the **IP range** screen, click **New IP range**.

The Specify IP Range **window appears. Refer**

4. Figure 1119.

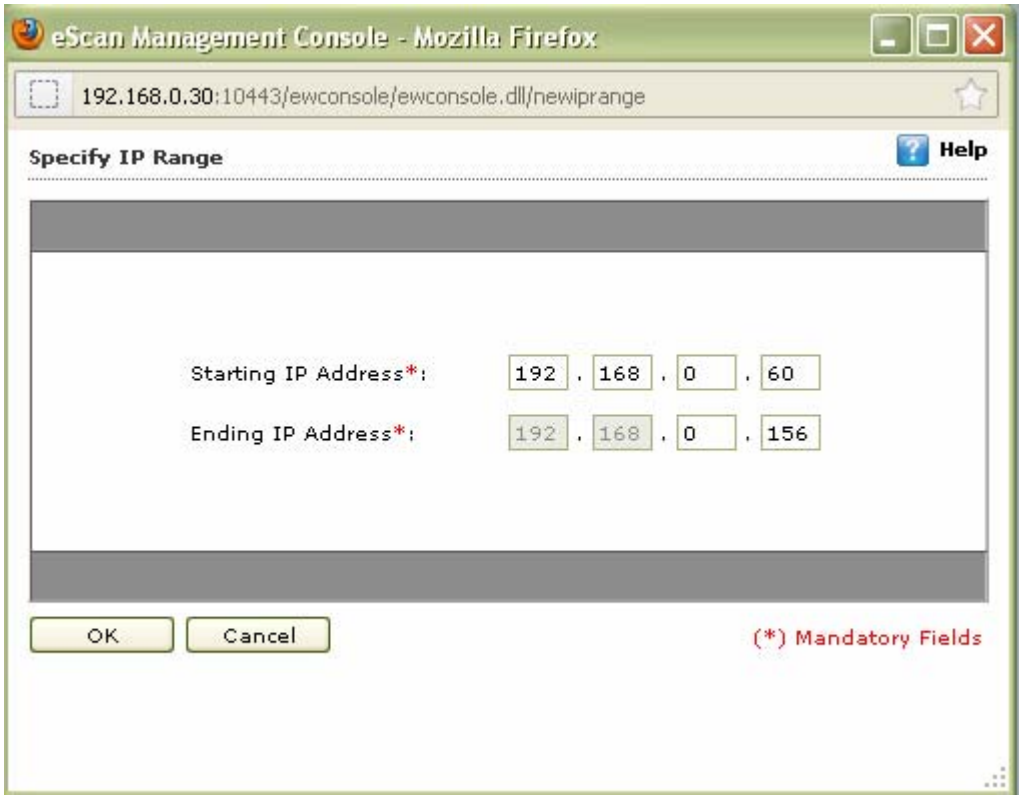


Figure 111

5. In the **Starting IP Address** field, type the IP address from where you want to start the IP range.
6. In the **Ending IP Address** field, type the IP address till where you want to create the IP range.
7. Click the **OK** button.

Delete an Existing IP Range

In a large network, you may often have to add or remove computers based on business requirements. The eScan Web Console also allows you to delete an existing IP range if it is no longer required.

The steps to delete an existing IP range are as follows:

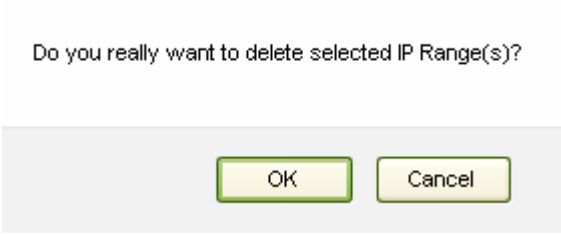
In the eScan Web Console, in the left pane, under Dashboard**, under** Unmanaged Computers**, click** IP range**. The** IP range **screen appears. Refer**

1. Figure 11240.

Figure 11240

Select the IP range check box that you want to delete, and then click the Delete IP range **button.**

The following window appears. Refer



2. Figure 11341.

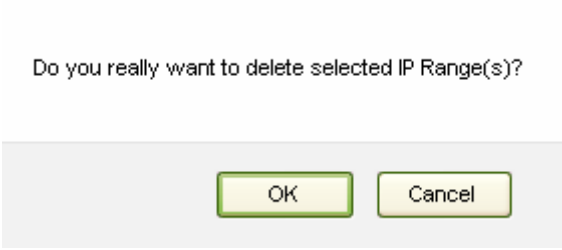
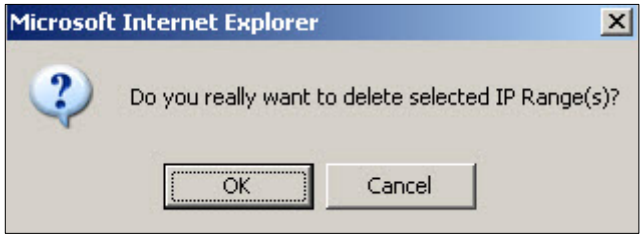


Figure 11341

3. Click the **OK** button.
   The selected IP range gets deleted.



Active Directory

The **Active Directory** page helps you to connect to active directory that are present in the network. It helps you to fetch computers that are already present in the active directory structure. You can connect them by providing the logon settings for the respective active directory.

These computers may or may not have eScan installed on them.

You can do the following activities:

- Adding Logon Settings of an Active Directory Domain Controller

- Modifying Logon Settings of an Active Directory Domain Controller
- Deleting an Active Directory Domain Controller Address
- Viewing Active Directory Domain Controller Details

Adding Logon Settings of an Active Directory Domain Controller

The **Active Directory** menu enables you to add the basic logon setting details of an active directory domain controller.

To add logon settings of an active directory domain controller

On the navigation pane, click Unmanaged Computers**, and then click** Active Directory**.**
The Active Directory **screen appears. Refer**

1. Figure 11442.

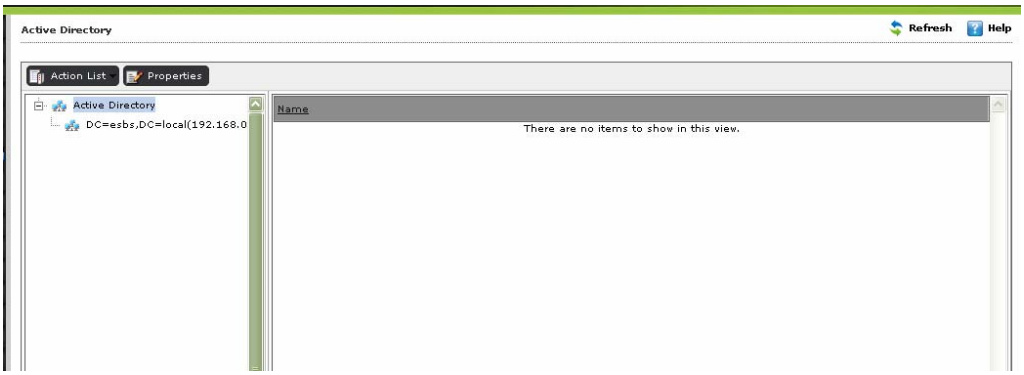
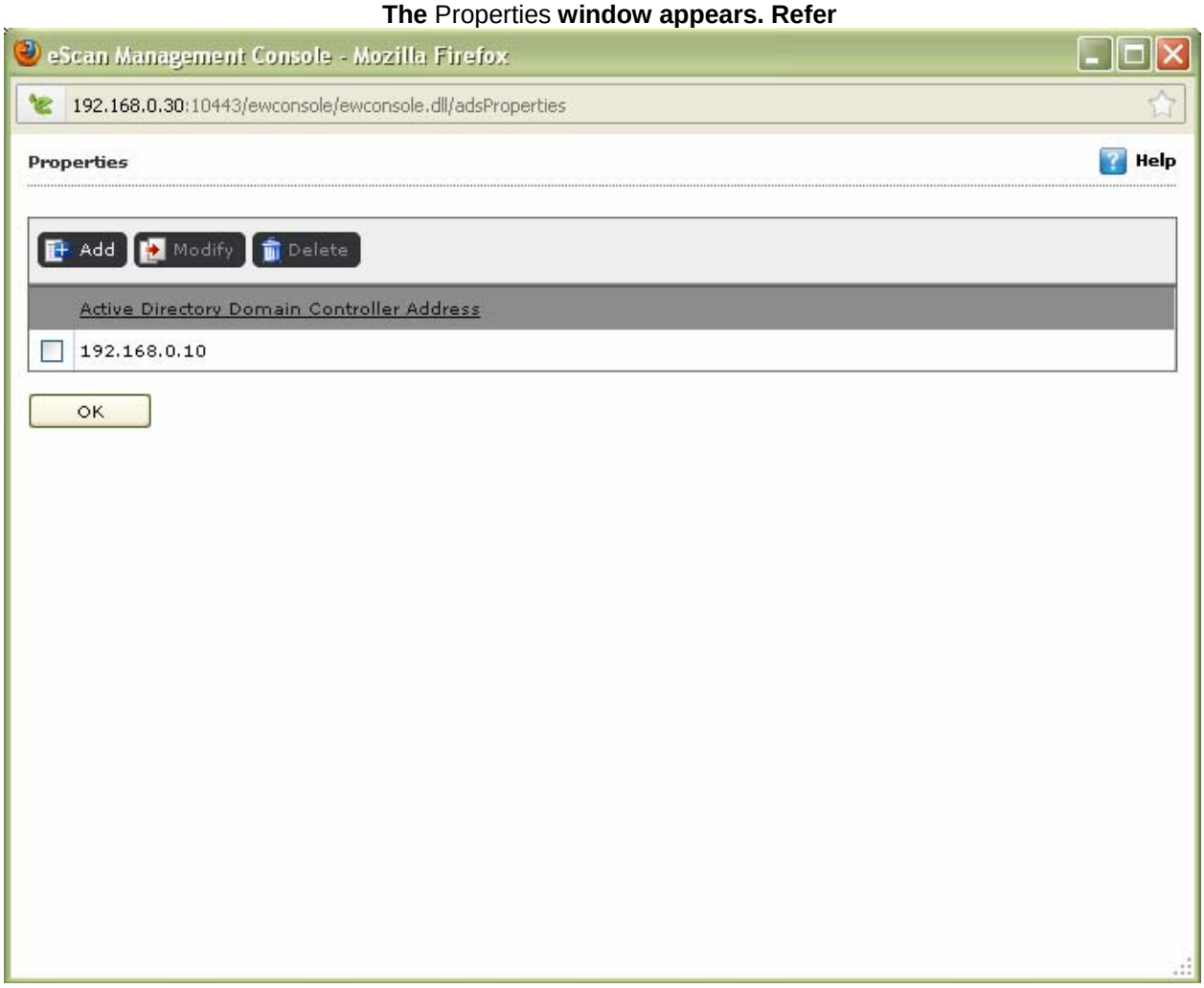


Figure 114

2. Click the **Properties** button.

The Properties **window appears. Refer**

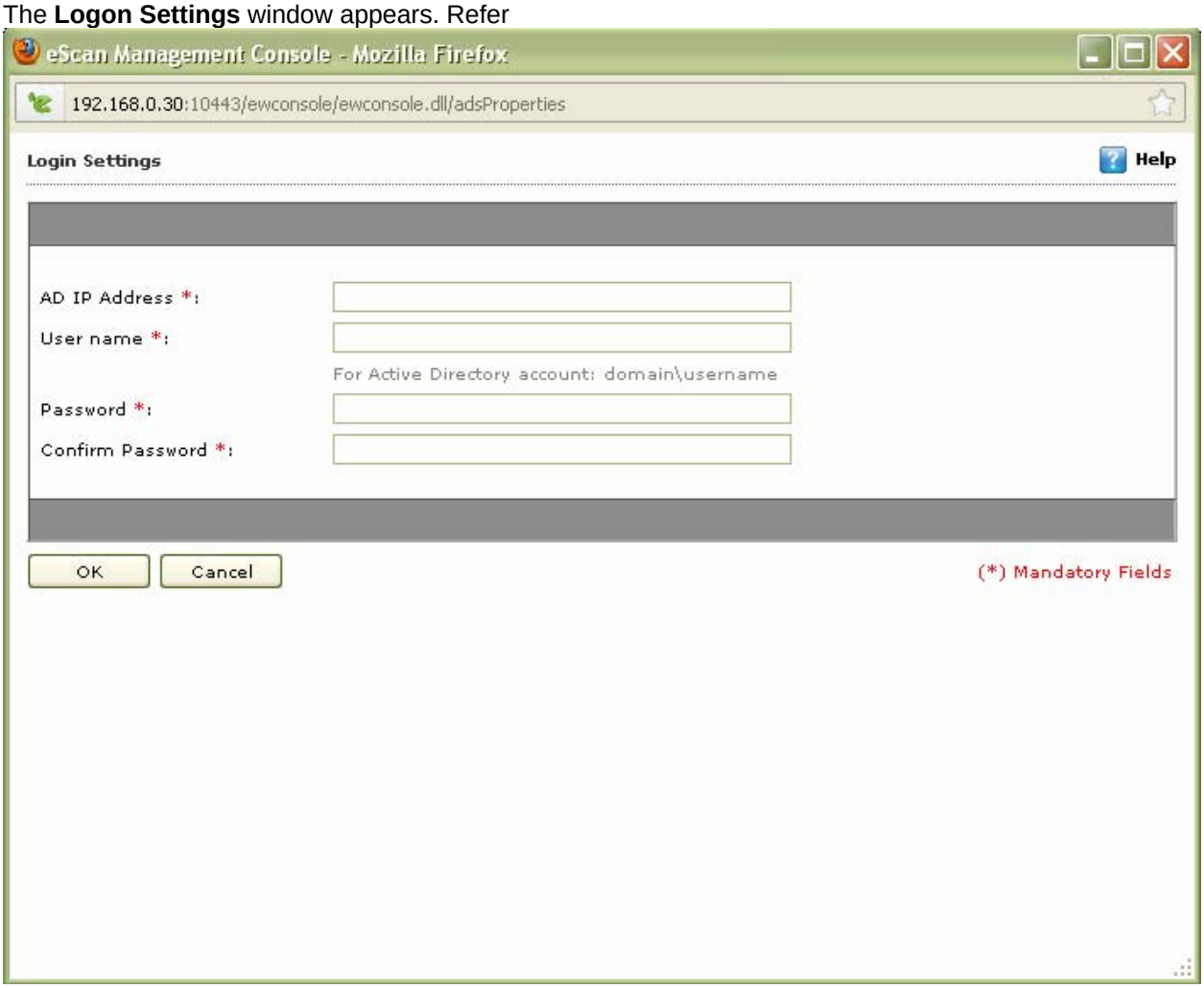


3. Figure 11543.

Figure 115

4. Click the **Add** button.

The **Logon Settings** window appears. Refer



5. Figure 116.

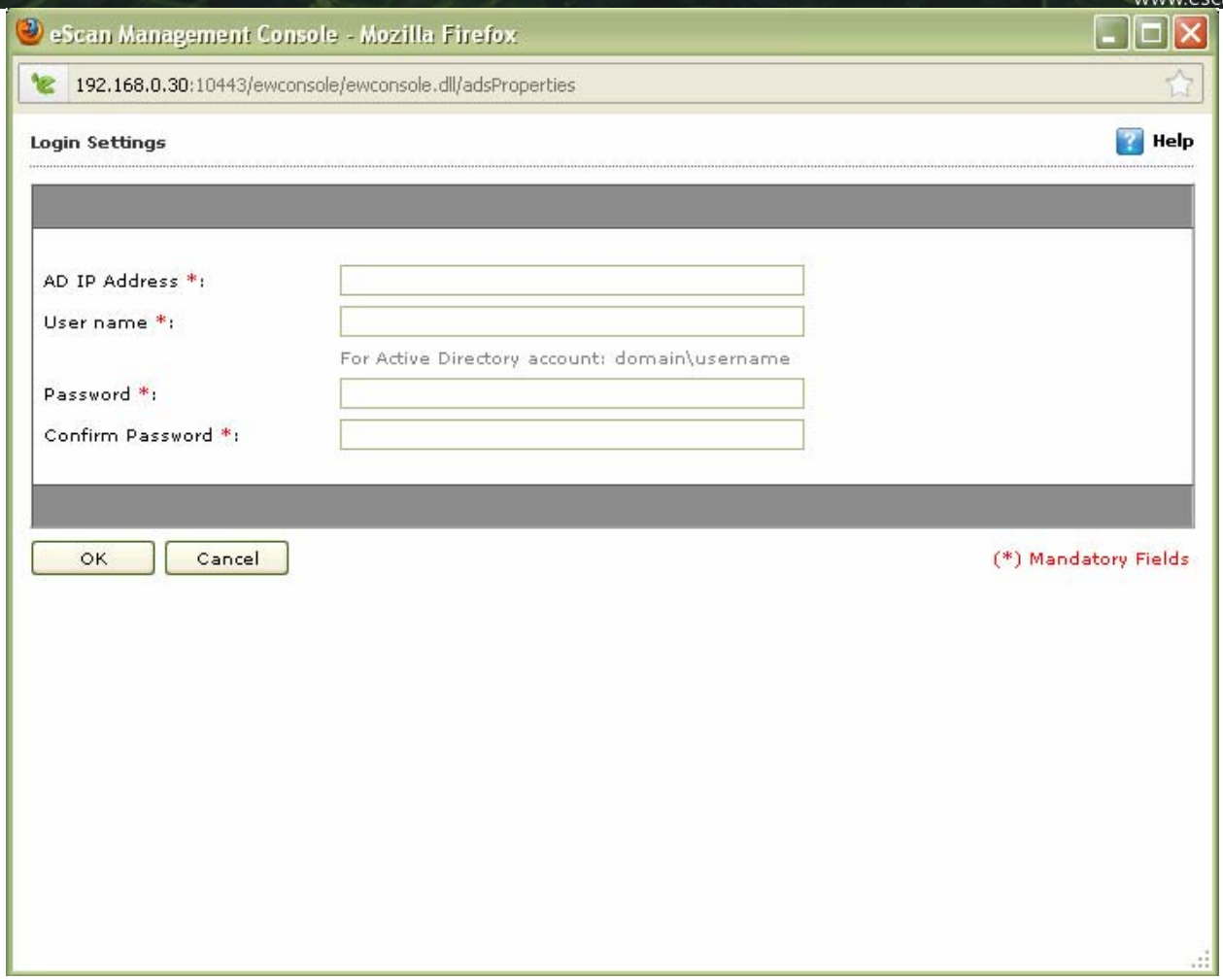

eScan Management Console - Mozilla Firefox
192.168.0.30:10443/ewconsole/ewconsole.dll/adsProperties
Login Settings
Help
AD IP Address *:
User name *:
For Active Directory account: domain\username
Password *:
Confirm Password *:
OK
Cancel
(*) Mandatory Fields

Figure 116

6. Specify the following field details.

Field	Description
AD IP Address*:	Type the IP address of the active directory domain controller.
User name*:	Type the user name.
Password*:	Type the password.
Confirm Password*:	Re-type the password for confirmation.

7. Click the **OK** button.
   The active directory IP address gets added to the active directory domain controller list.

Modifying Logon Settings of an Active Directory Domain Controller

The **Active Directory** menu enables you to modify the basic logon setting details of an active directory domain controller details.

To modify logon settings of an active directory domain controller

On the navigation pane, click Unmanaged Computers**, and then click** Active Directory**.**
The Active Directory **screen appears. Refer**

1. Figure 11442.

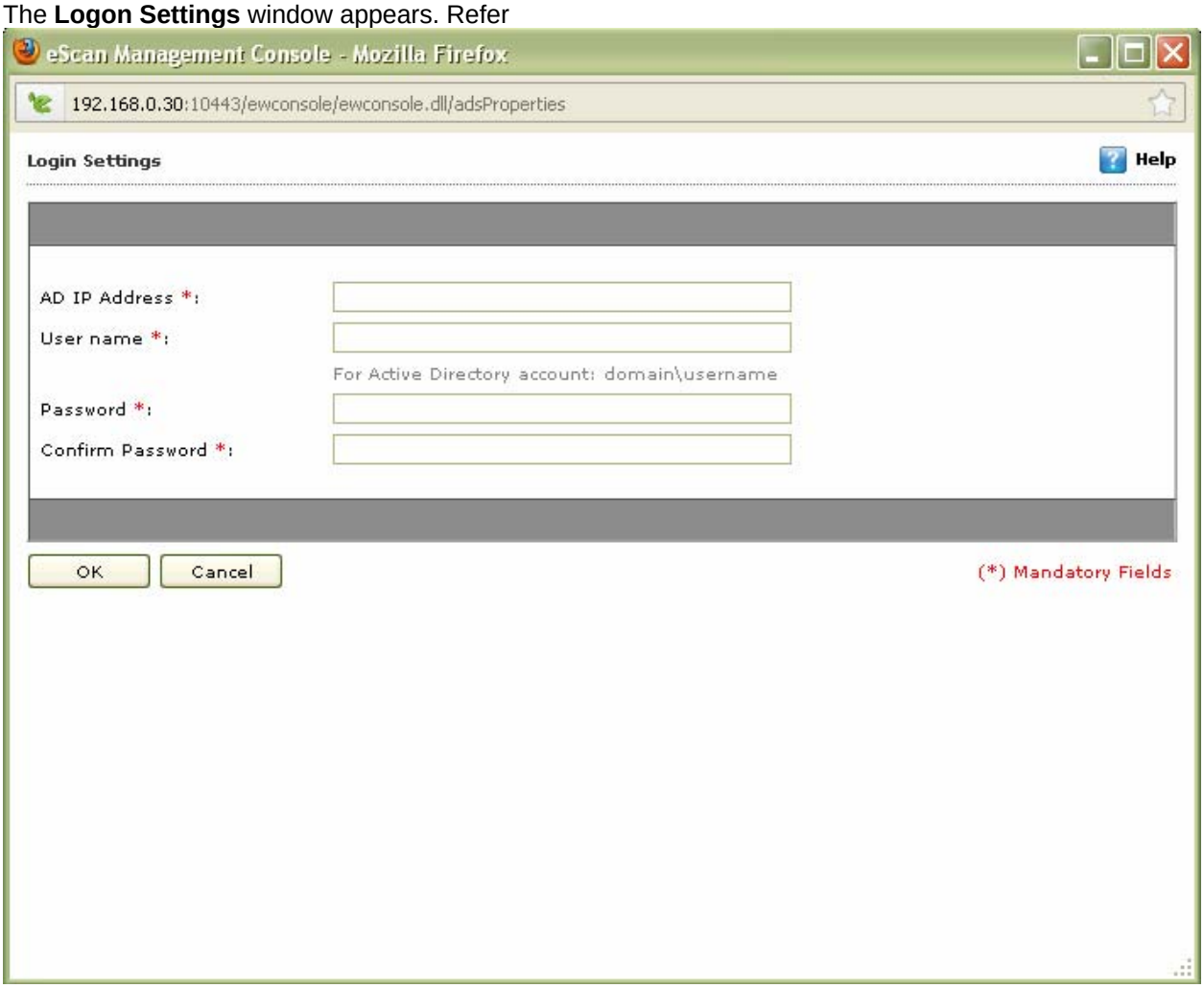
Click the Properties **button.**
The Properties **window appears. Refer**

2. Figure 11745.

Figure 11745

Select an appropriate active directory domain controller address check box, which you want to modify, and then click the **Modify** button.

The **Logon Settings** window appears. Refer



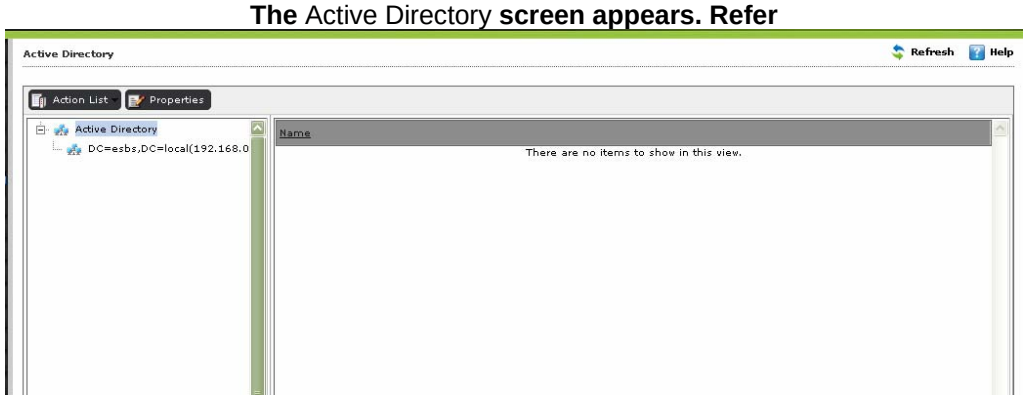
3. Figure 116.
4. Modify the required field details as required.

Deleting an Active Directory Domain Controller Address

The **Active Directory** menu also enables you to delete an active directory domain controller address.

To delete an active directory domain controller address

On the navigation pane, click Unmanaged Computers**, and then click** Active Directory**.**
The Active Directory **screen appears. Refer**



1. Figure 114.

Click the Properties **button.**
The Properties **window appears. Refer**

2. Figure 11745.
3. Select an appropriate active directory domain controller address check box, which you want to delete, and then click the **Delete** button.
   The following window appears. Refer Figure 11846.

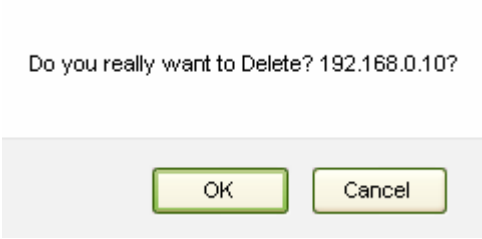


Figure 11846

4. Click the **OK** button.
   The active directory IP address gets deleted from the active directory domain controller list.

Viewing Active Directory Domain Controller Details

The **Active Directory** menu enables you to view the active directory domain controller details.

To view active directory domain controller details

1. On the navigation pane, click **Unmanaged Computers**, and then click **Active Directory**.
   The **Active Directory** screen appears.
2. Click the **Properties** button.
   The **Properties** window appears.
3. View the details as required.

Chapter 14: Configuring the Settings

The eScan Web Console provides several options for configuring the behavior of eScan modules such as EMC, Web Console, and Update.

- Configuring the EMC Settings
- Configuring the Web Console Setting
- Configuring the Update Settings

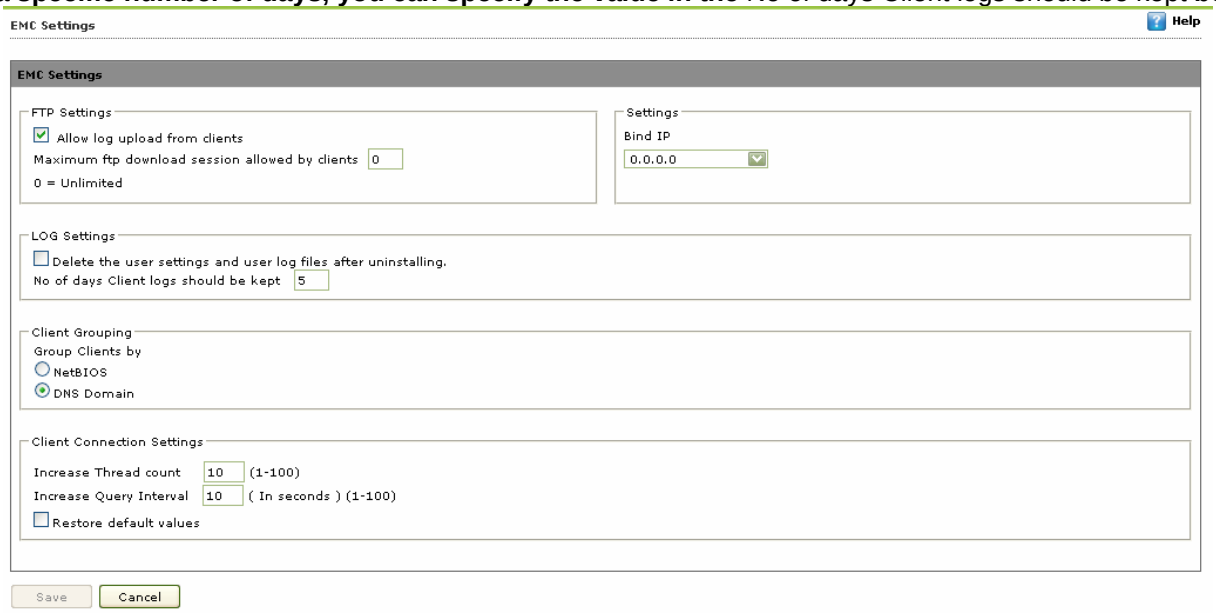
Configuring the EMC Settings

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 the Console 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 listen on all available interface/IP.

You can also enable FTP settings such as allowing upload by client computers by selecting the **Allow Upload by Clients** check box. If you are doing that, you can set a maximum limit for the number of FTP clients that you want to allow. If you specify this number as 0, it means that any number of client computers can upload files.

You can also choose to delete the user settings and user log files stored by eScan after uninstalling eScan by selecting the Delete the user settings and user log files after uninstalling **check box. If you want to keep the files for a specific number of days, you can specify the value in the** No of days Client logs should be kept **box.**



Refer

Figure 11947.

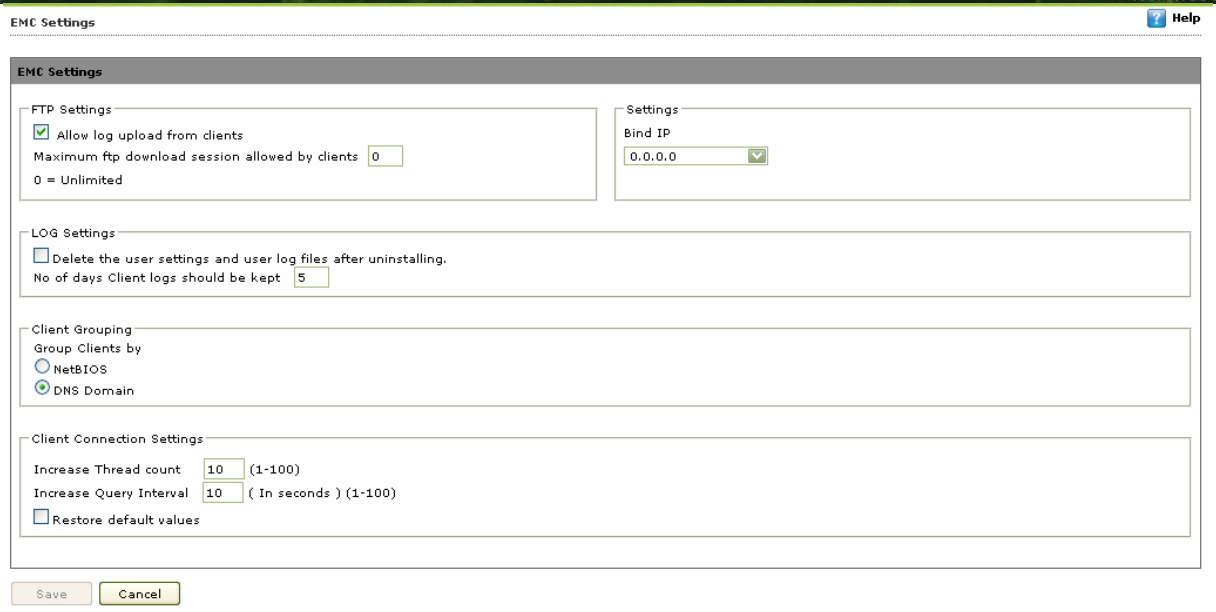


Figure 11947

The steps to configure the EMC settings are as follows:

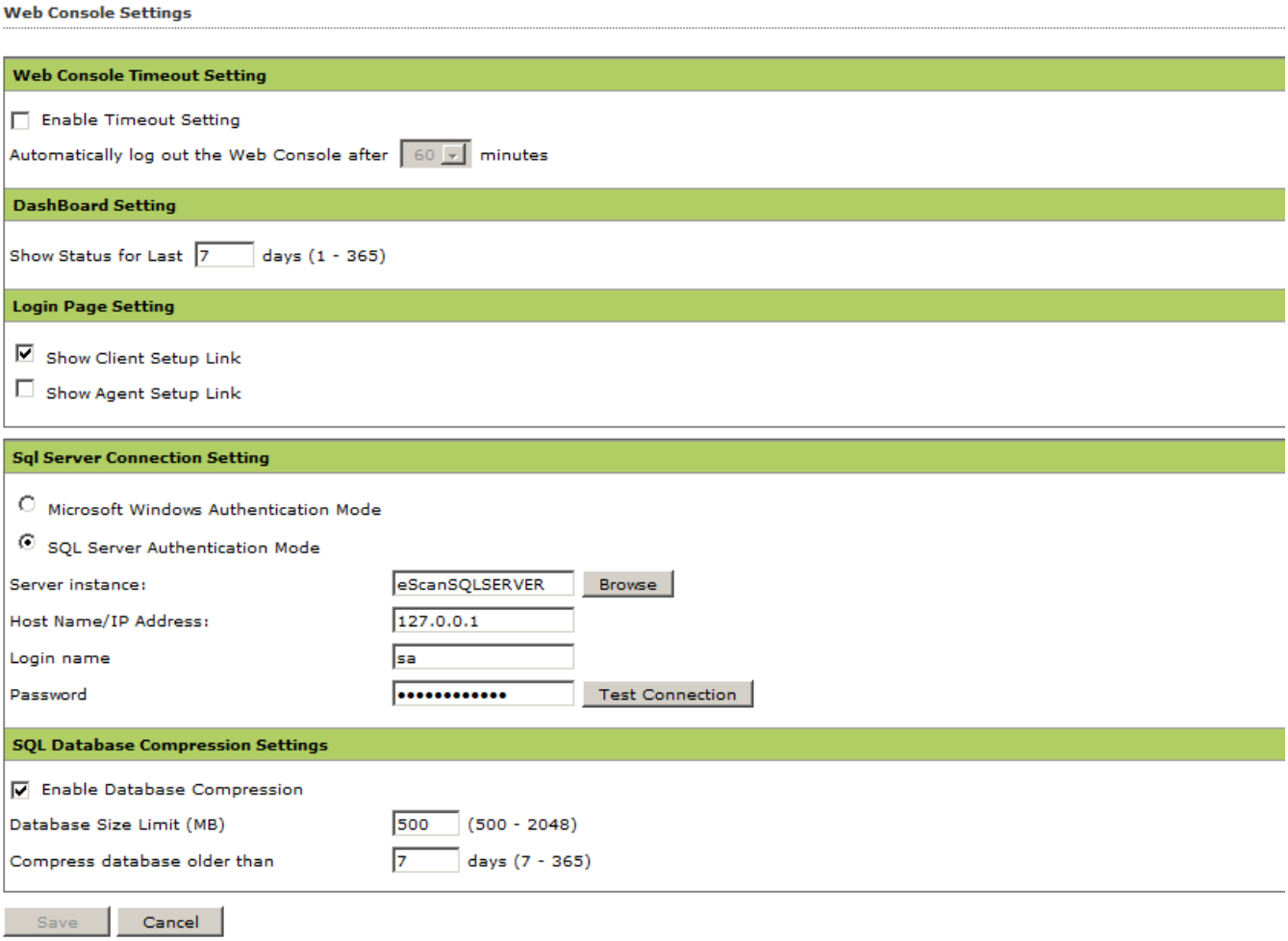
- To configure the Bind IP address, under BIND IP, in the box, click the required IP address. The default IP address is 0.0.0.0.
- To allow uploads by client computers, under FTP Settings, select the Allow Upload by Clients check box.
- To restrict the maximum number of FTP client computers, in the Maximum FTP Clients allowed box, type or select the maximum number of FTP client computers to be allowed. The default value is 0; this allows an unlimited number of FTP client 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** option, if you want to sort clients only by hostname.
  - Click **DNS** Domain option, if you want to sort clients by hostname containing the domain name.

Configuring the Web Console Settings

The **Web console settings** page allows you to configure the Web console time-out settings, Dashboard settings, and Sql Server connection settings.

To configure Web Console settings

On the navigation pane, under Settings**, click** Web Console Settings**.**
The Web Console Settings **screen appears. Refer**



1. Figure 12048.

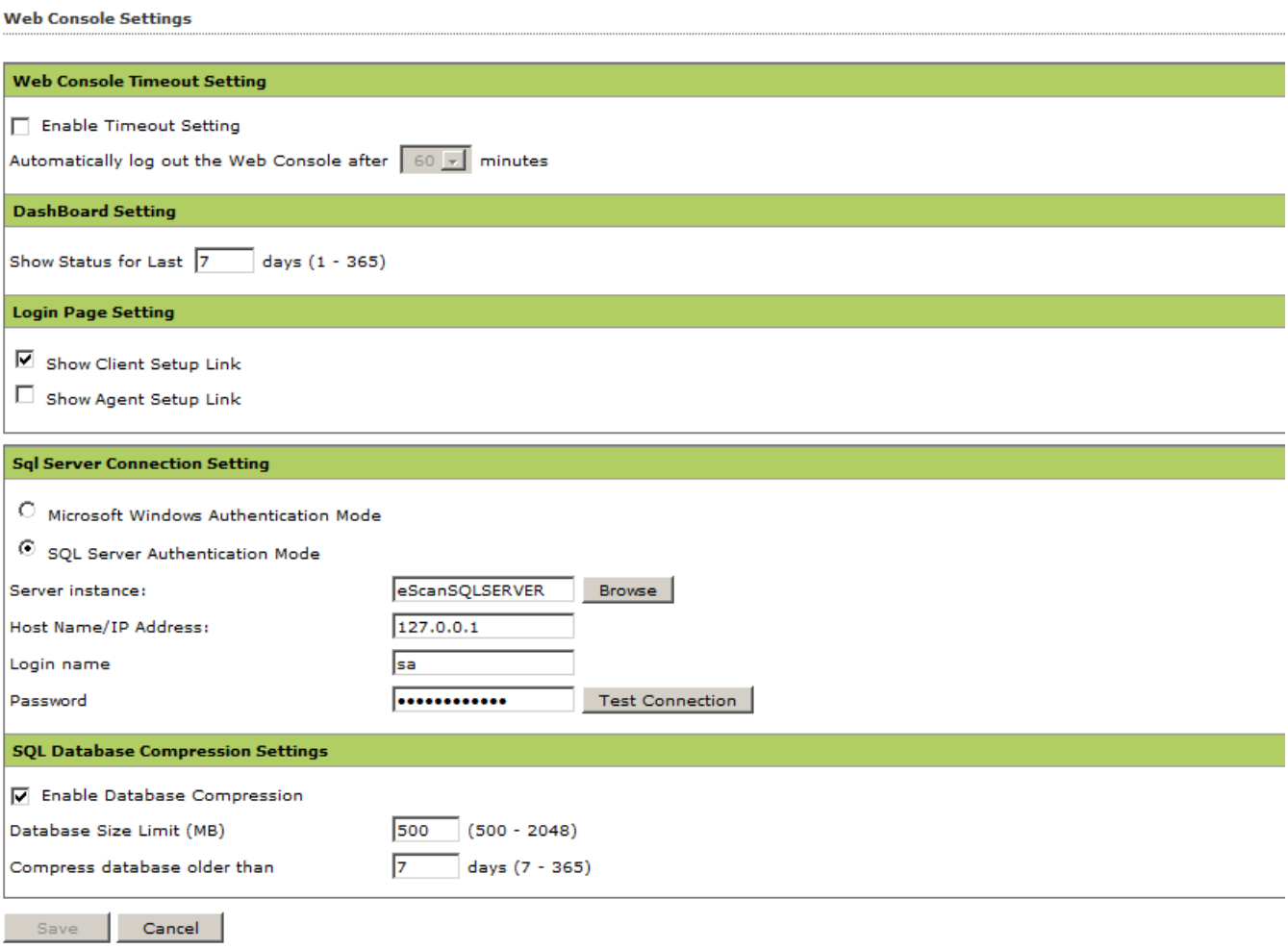


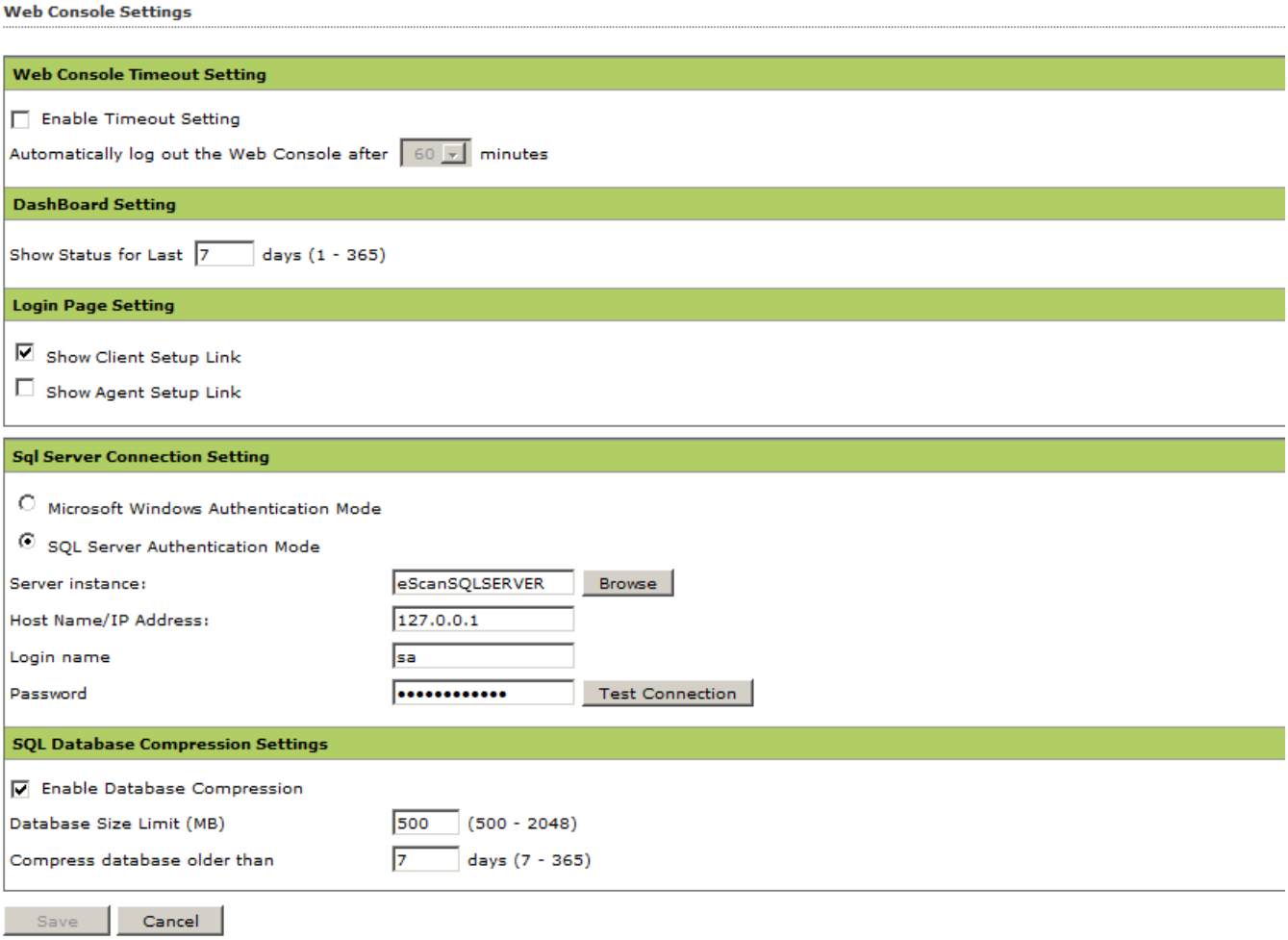
Figure 12048

2. In the Web Console Timeout Setting area, select the **Enable timeout setting** check box.
3. The **Automatically log out the web console after minutes** field appears dimmed, it is available only when you select the **Enable timeout setting** check box.
4. Select number of minutes from the **Automatically log out the web console after X minutes** box, that is, X means total number of minutes.
5. In the **DashBoard Setting** section, type number of days in the **Show Status for Last X days (1-365)** field, that is, X means total number of days.
6. Under **Login Page Settings** section, select an appropriate check box:
   - **Show Client Setup Link:** Select this check box, if you want to show the client setup link on the login page.
   - **Show Agent Setup Link:** Select this check box, if you want to show the agent setup link on the login page.
7. Under **SQL server Connection Settings** section, there are two modes of authentication, do any one of the following:

- Microsoft Windows Authentication Mode:

8. Click this option, if you want to authenticate through Microsoft Windows.

The Login name **and** Password **field becomes unavailable. Refer**



- Figure 1219.

Web Console Settings

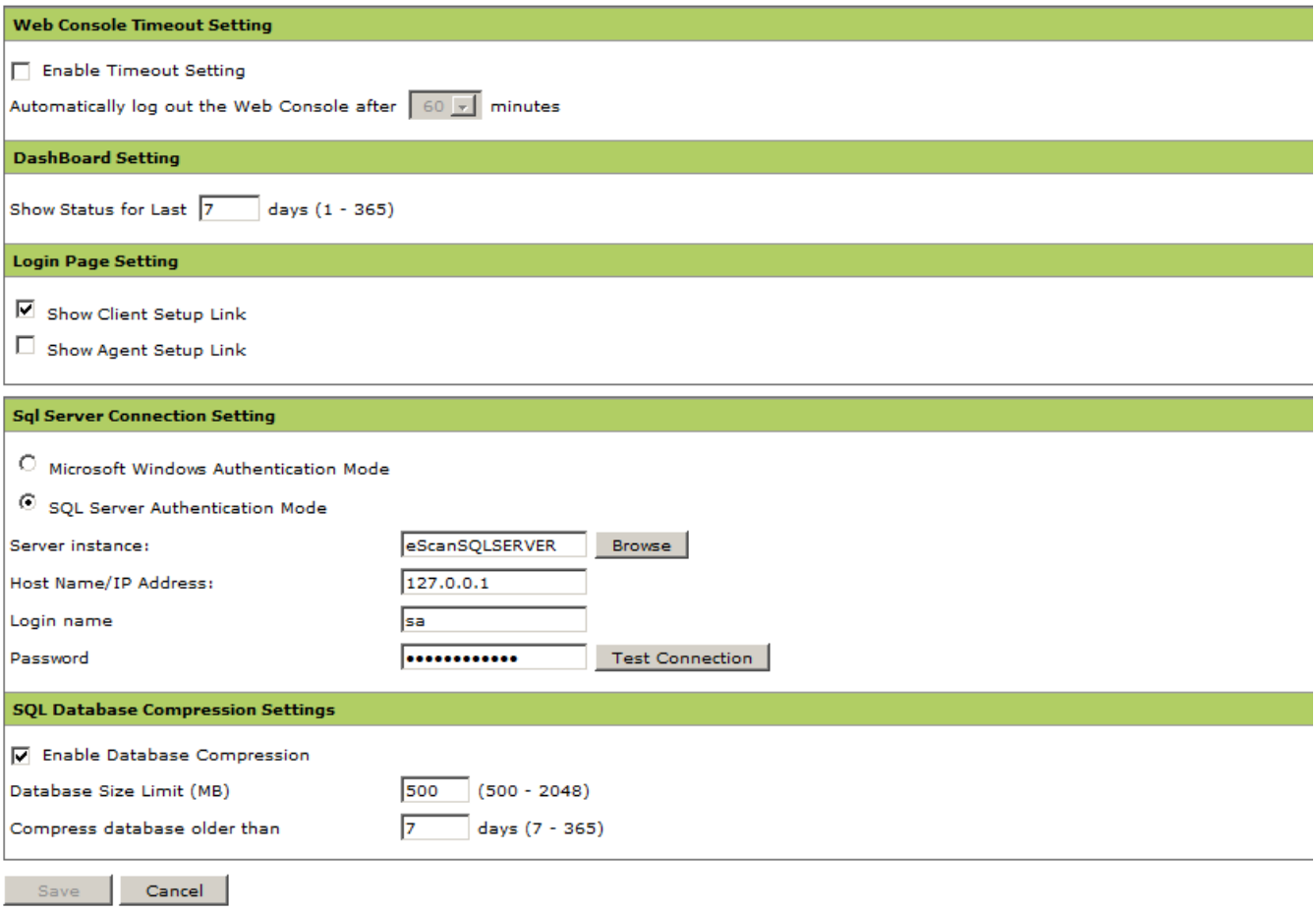
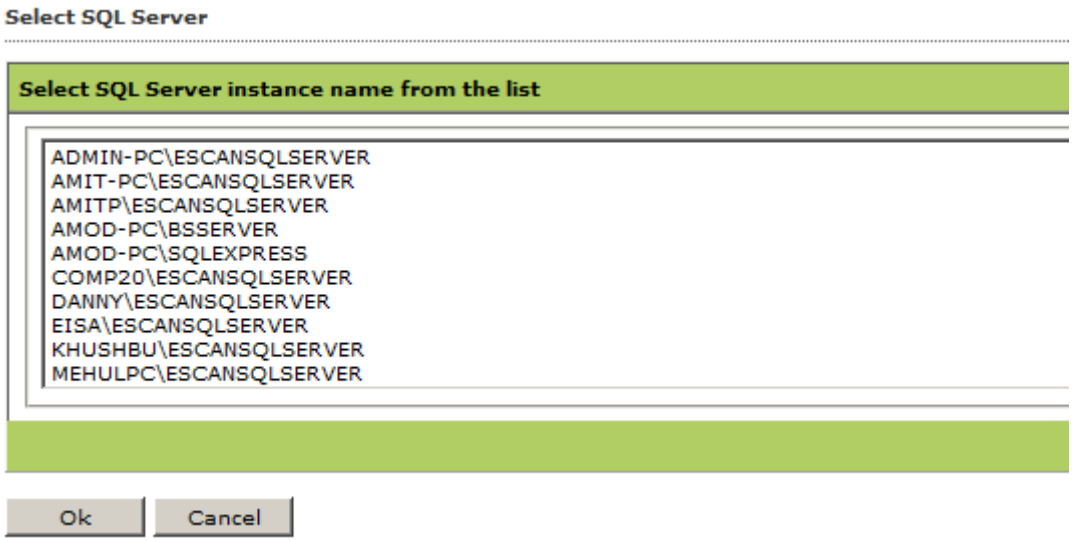


Figure 121

By default, the details appear. If you want you can change by typing server instance name in the Server instance field or click Browse **button to select server instance name from the list.**

The Select SQL Server **screen appears. Refer**



9. Figure 12250.

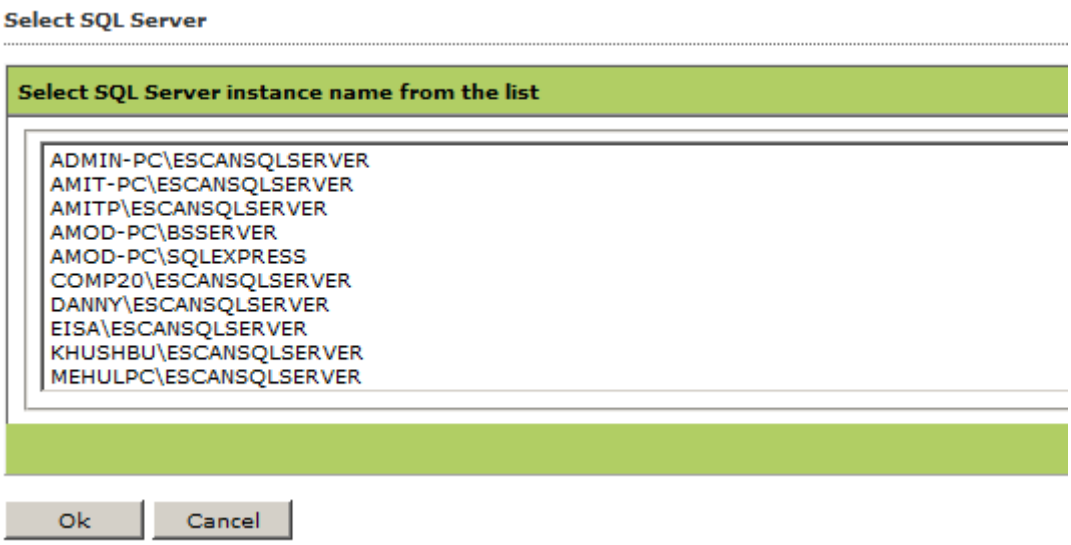


Figure 12250

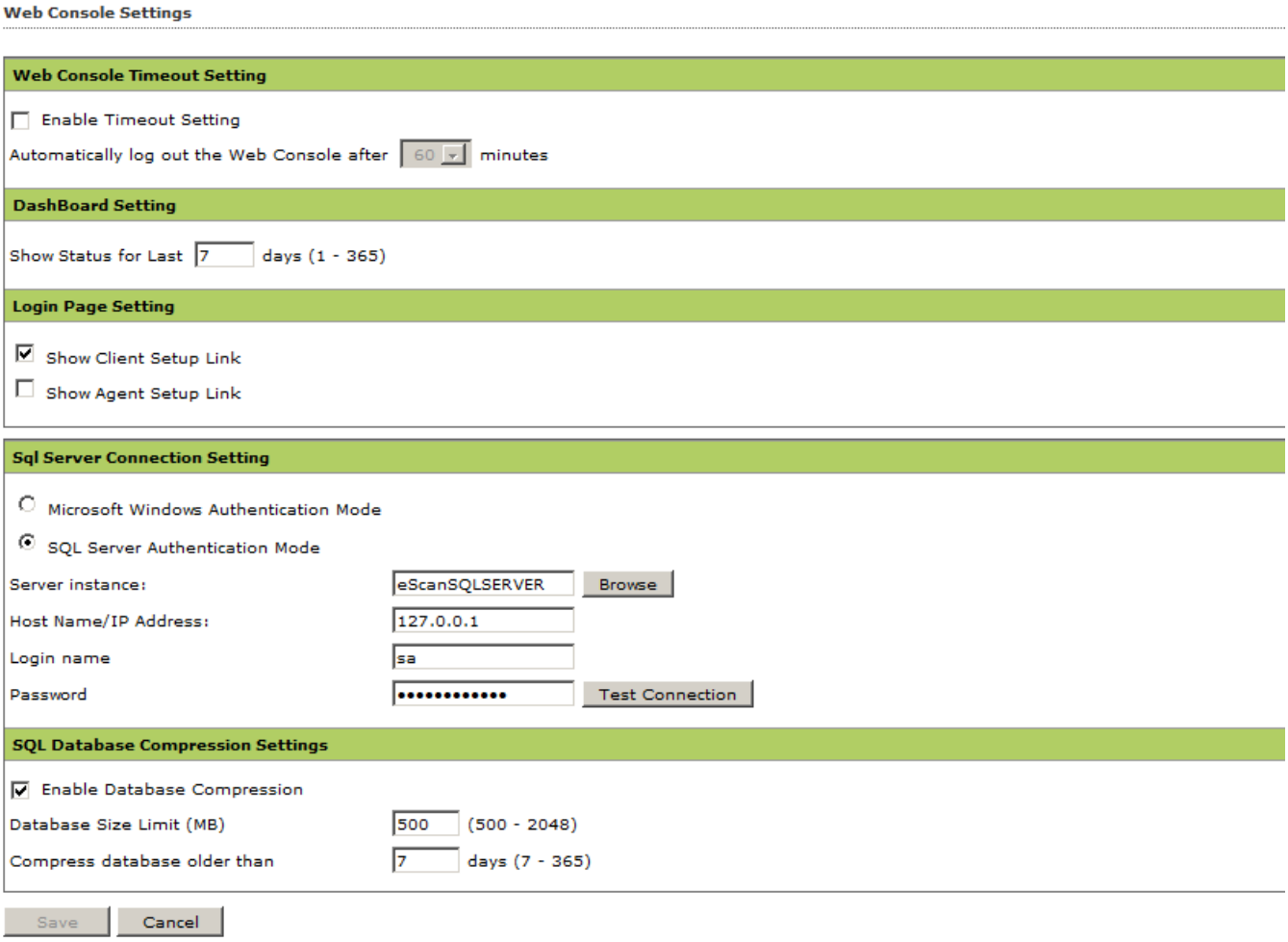
10. Click an appropriate server instance name from the **Select SQL Server instance name from the list**, and then click the **Ok** button.
    The selected server instance name appears.
11. By default, the details appear. If you want you can change by typing host name or IP address of the server in the **Host Name/IP Address** field.
12. Click the **Test Connection** button.
    The message of server successfully connected appears on the screen.

Please make sure that you specify correct field details for the successful server connection. In case, of incorrect details, the **"Connection failed!"** error message appears.

13. Click the **Save** button.
    The settings get saved.

- SQL Server Authentication Mode:

Click this option, if you want to authenticate through SQL server. Refer



14. Figure 120.
15. Specify the following field details.

Field	Description
Server instance	By default, the details appear. If you want you can change by typing server instance name in the **Server instance** field or click **Browse** button to select server instance name from the list.
Host Name/ IP Address	By default, the details appear. If you want you can change by typing host name or IP address of the server.
Login name	Type the login name.

Password	Type the password.

16. Click the **Test Connection** button.
    A message of server successfully connected appears.

    Please make sure that you specify correct field details for the successful server connection. In case, of incorrect details, the **"Connection failed!"** error message appears.

17. Click the **Save** button.
    The settings get saved.

Configuring the Update Settings

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

You can access the Update settings page from the navigation bar. This page provides you with information regarding the mode of updation. It also provides you with options for configuring the module. It also helps you the Update module to download updates automatically. This page has the following tabs.

The **Update Settings** page has three tabs: **General Config**, **Update Notifications**, and **Scheduling**.

- General Config
- Update Notification
- Scheduling

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.

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. 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.

After making the necessary changes, you must save the changes. To save the changes, click Save. You can also update the server manually by clicking Update **Button. Refer**

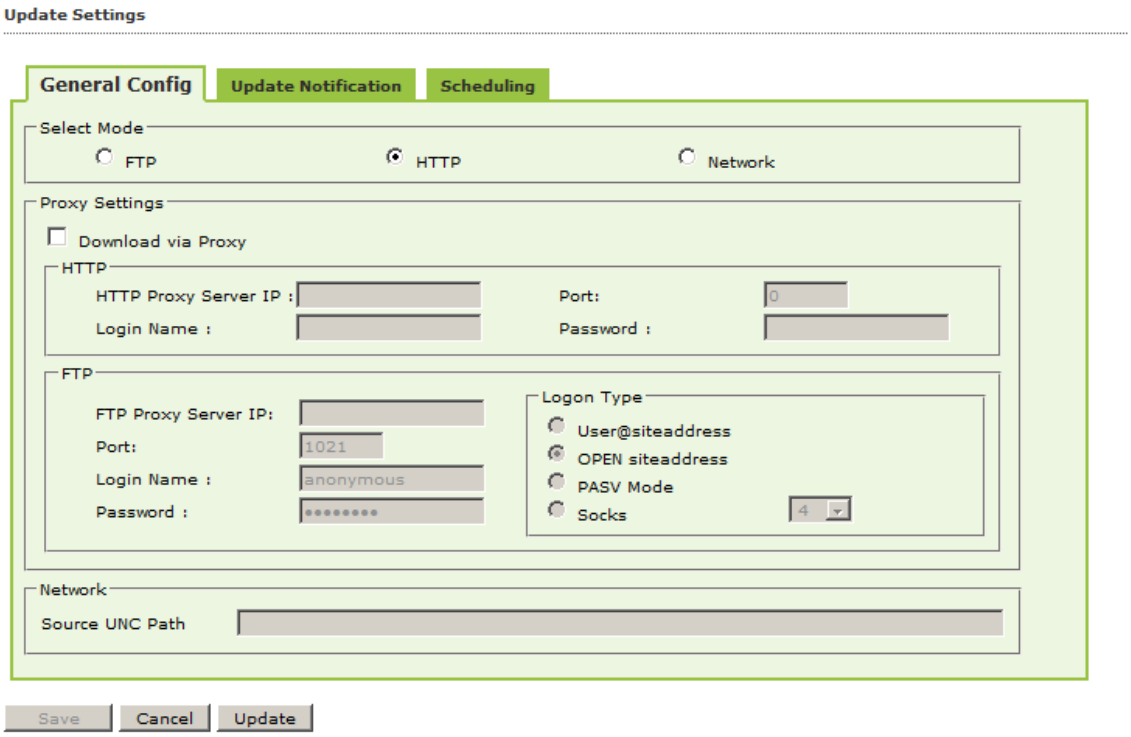


Figure 12351.

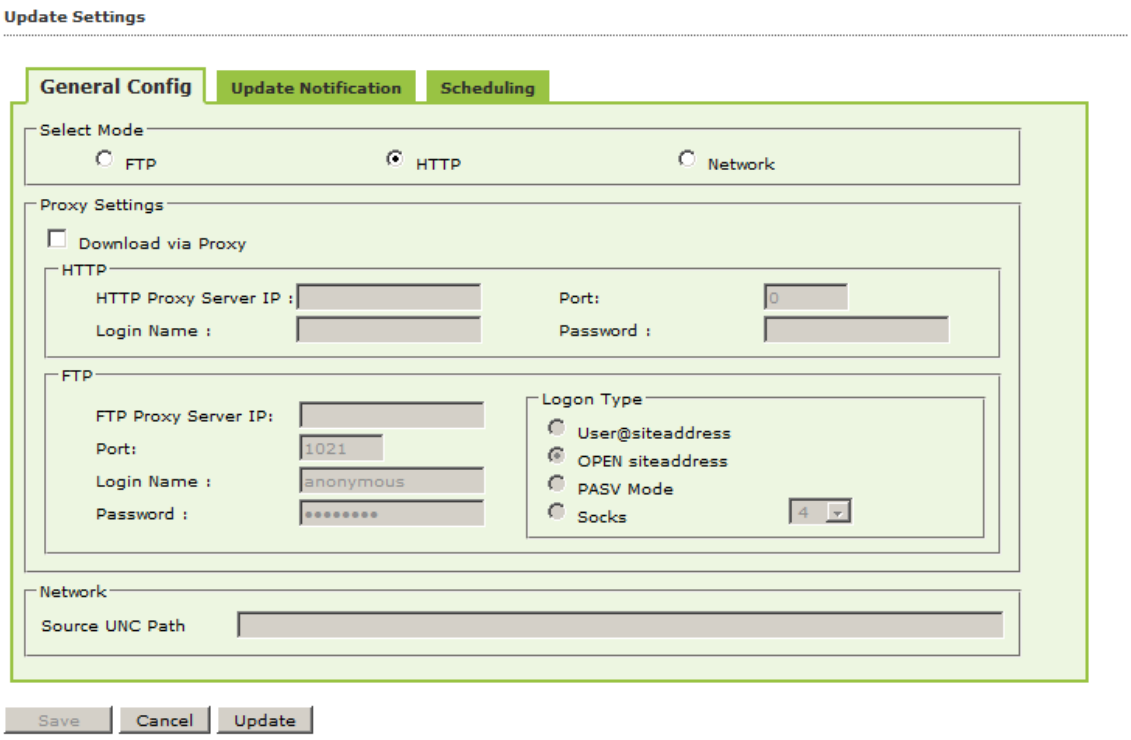


Figure 12351

The steps to configure the EMC settings are as follows:

- To select the mode for downloading updates, under Select Mode, depending on the type of mode that you want to select for downloading updates, click FTP, HTTP, or Network.
- To configure the proxy settings for downloading updates via a proxy, ensure that you have selected either FTP or HTTP, and then select the Download via Proxy check box.
- HTTP proxy server

1. If you are using an HTTP proxy server, under **HTTP**, in the **HTTP Proxy Server IP** box, type the IP address of the HTTP proxy server, and then in the **Port** box, type its port number.
2. In the **Login Name** box, type the login name of the user, and then in the **Password** box, type the password.

- FTP proxy server

1. If you are using an FTP proxy server, under **FTP**, in the **FTP Proxy Server IP** box, type the IP address of the FTP proxy server, and then in the **Port** box, type its port number.
2. In the **Login Name** box, type the login name of the user, and then in the **Password** box, type the password.
3. To select a logon type, under **Logon Type**, click any one of the following:
   - User@siteaddress
   - OPEN siteaddress

- PASV Mode
- Socks

- To configure the network settings, ensure that you have selected the Network mode, and then under Network section, in the Source UNC Path box, specify the UNC path.

Update Notification

The **Update Notification** tab helps you configure the actions that eScan should perform after Updater downloads the eScan updates.

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

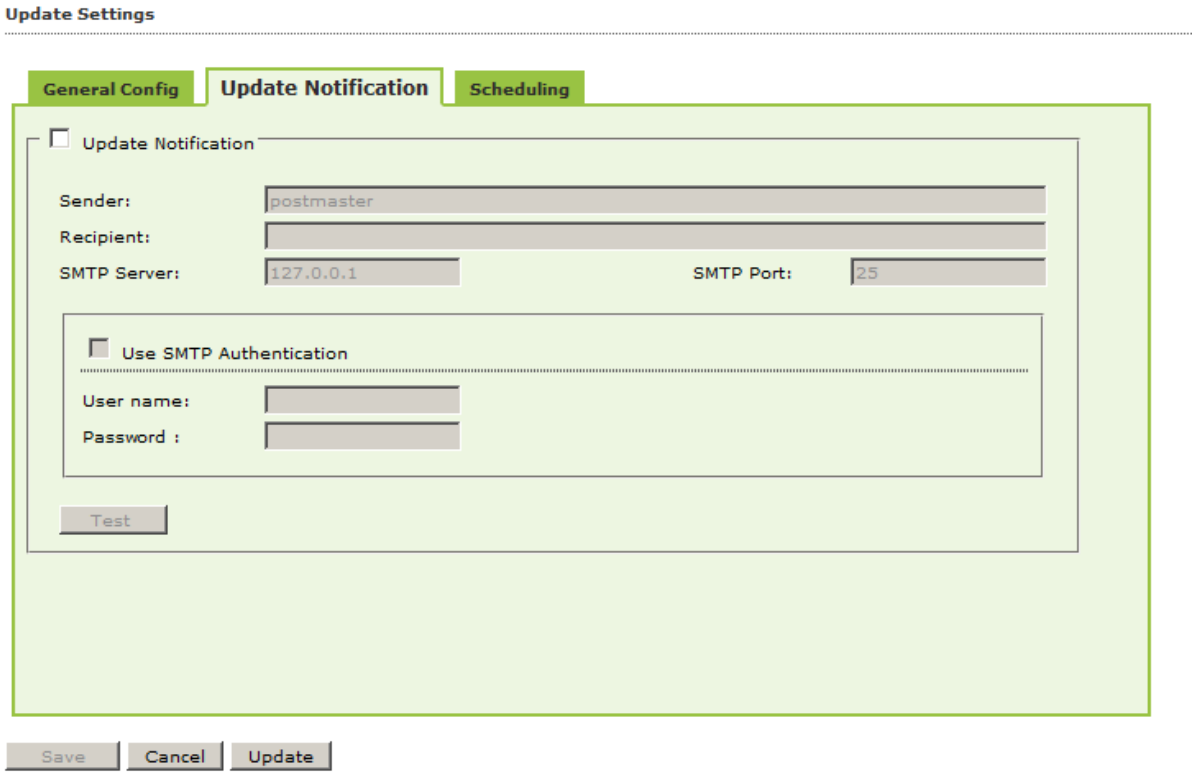


Figure 12452.

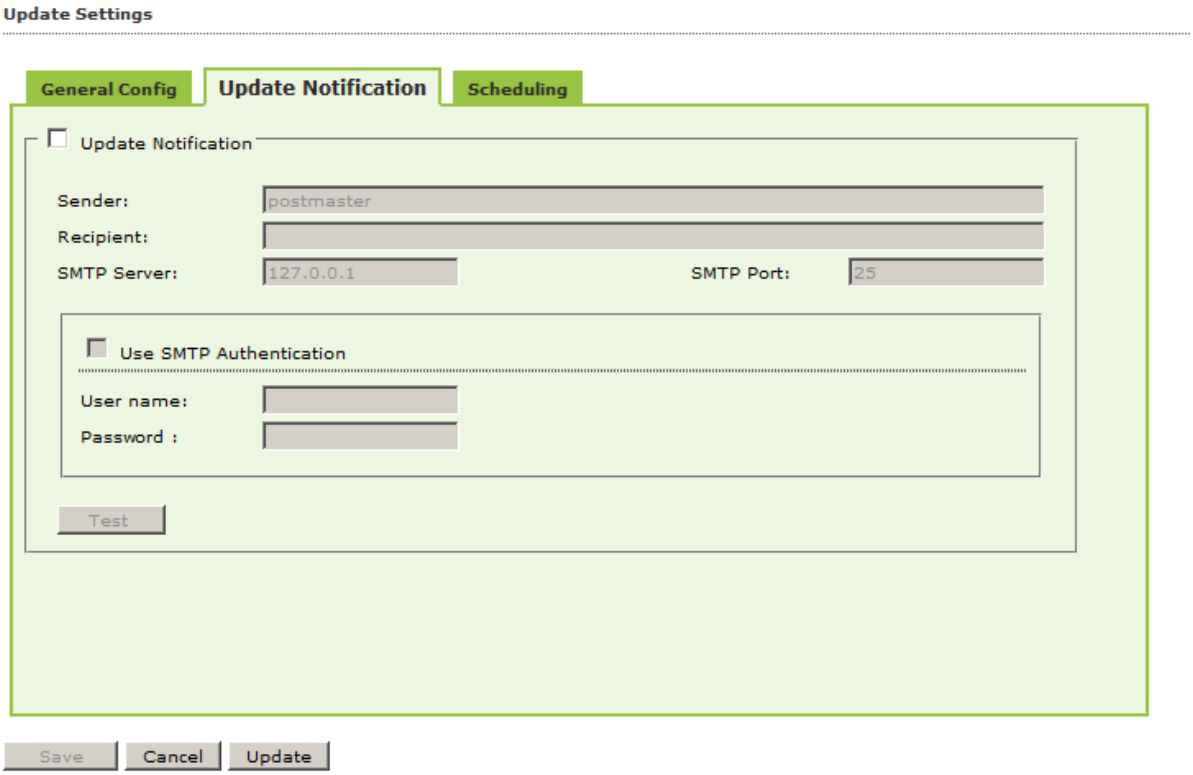


Figure 12452

The steps to configure the **Update Notification** settings are as follows:

1. To configure the update notification settings, on the **Update Notification** tab, select the **Update Notification** check box.
2. In the **Sender** box, type the e-mail address of the sender, and in the **Recipient** box, type the e-mail address of the receiver. You can add multiple email ID's by separating with a comma.
3. In the **SMTP Server** box, type the IP address of the SMTP server, and in the **SMTP Port** box, type the port number of the SMTP server.
4. Select the **Use SMTP Authentication** check box, if you use SMTP authentication.
5. The **User name** and **Password** field appears only when you select **Use SMTP Authentication** check box.
6. Type the user name in the **User name** field.
7. Type the password in the **Password** field.
8. Click the **Test** button. It will show you as connection successful if the credentials entered are correct.

Scheduling

The eScan Scheduler automatically polls the update server for latest 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.

You can configure the Update module to query and download the latest updates automatically from the MicroWorld update server 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 MicroWorld Web site for latest updates on the specified day at the specified time and downloads them if they are available. Refer

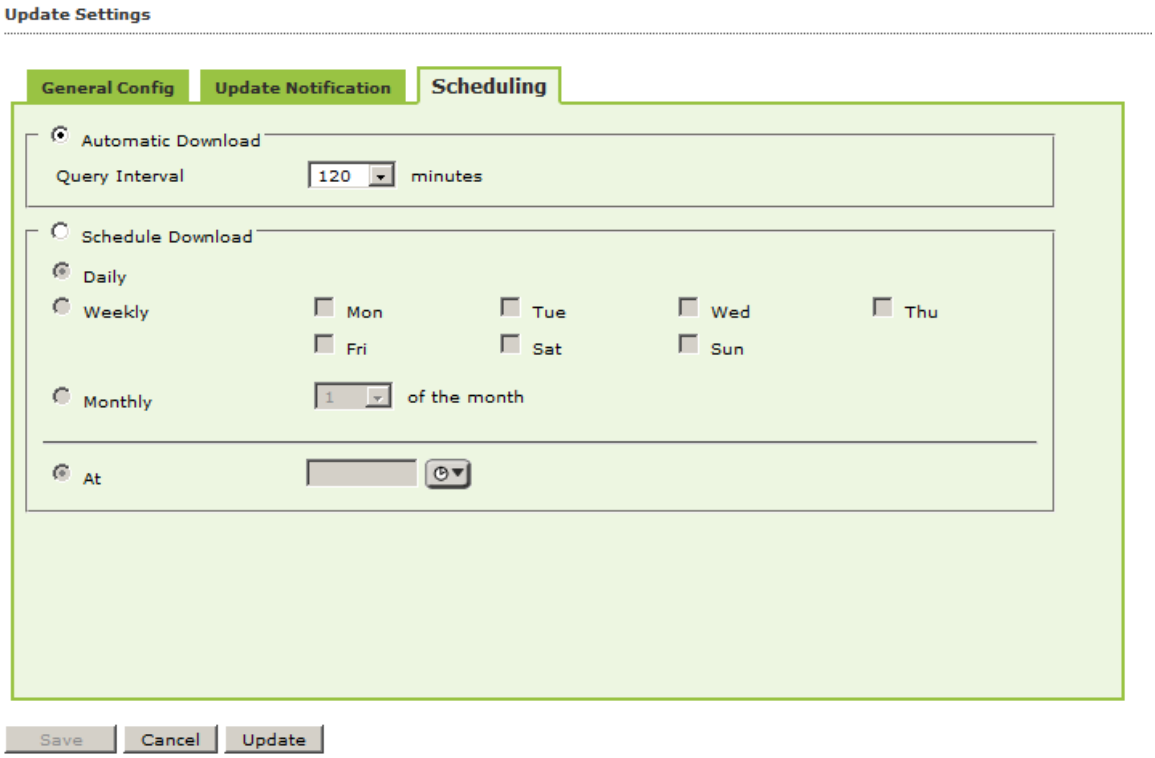


Figure 125.

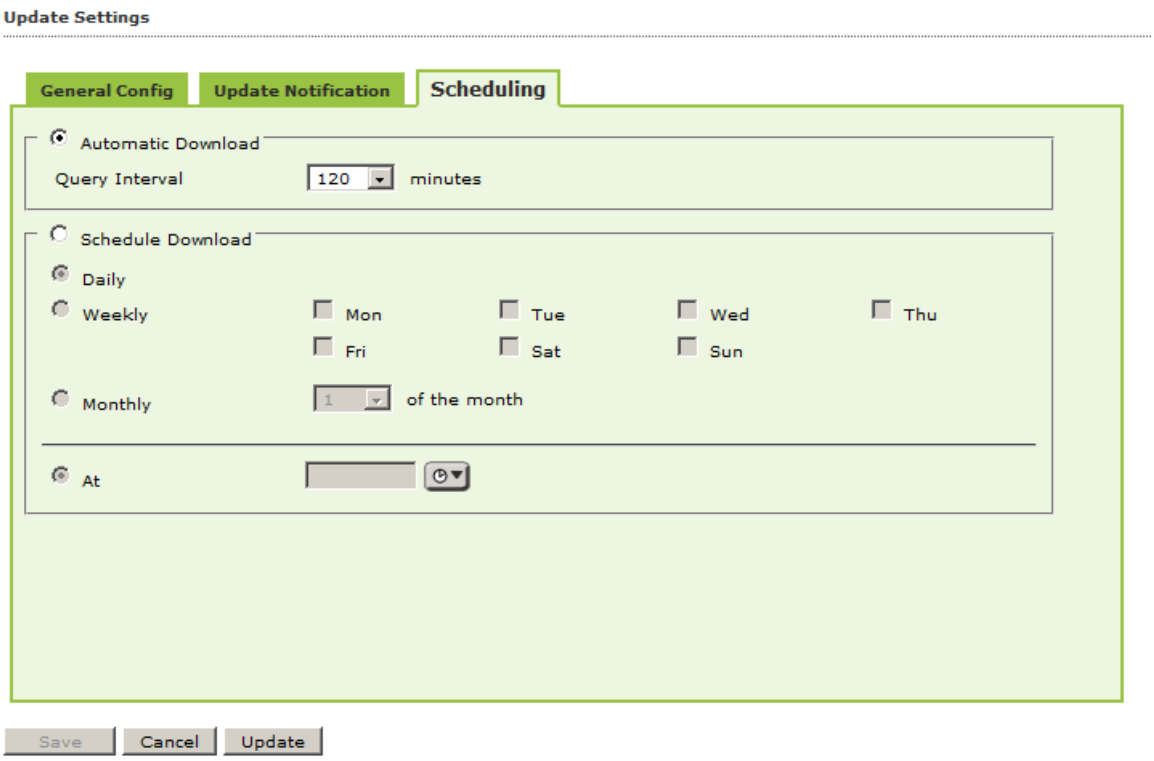


Figure 125

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

- Automatic Download of Updates
- To configure the automatic download of updates, click Automatic Download, and then in the Query Interval list, select the appropriate value in minutes.

- Scheduled Download of Updates

1. To configure the download schedule, click **Schedule Download**, and then depending on whether you want to download updates on a daily, weekly, or monthly basis, select the appropriate options.
2. Under **At**, specify when you want the scheduler to download the update.

Chapter 15: Managing User Accounts

The **User Accounts** menu enables you to create user account for both local and active directory users/groups. It also helps you assign a role for the users/groups.

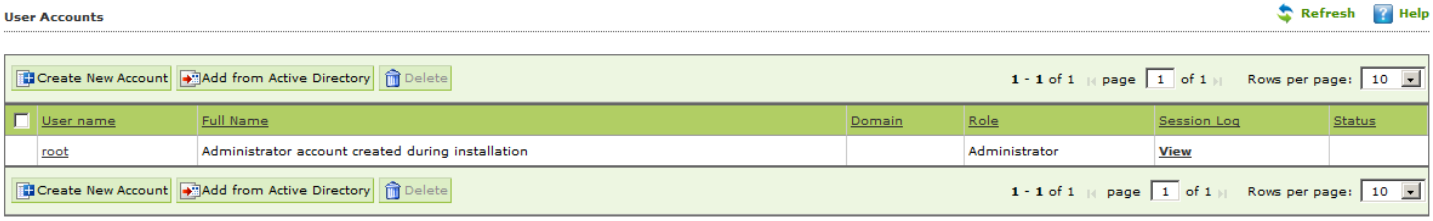
You can do the following activities:

- Adding an User Account
- Adding an Active Directory User or Group
- Deleting an User Account
- Modifying the User Account Details

Adding a User Account

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

On the navigation pane, under Administration**, click** User Accounts**.**
The User Accounts **screen appears. Refer**



1. Figure 12654.

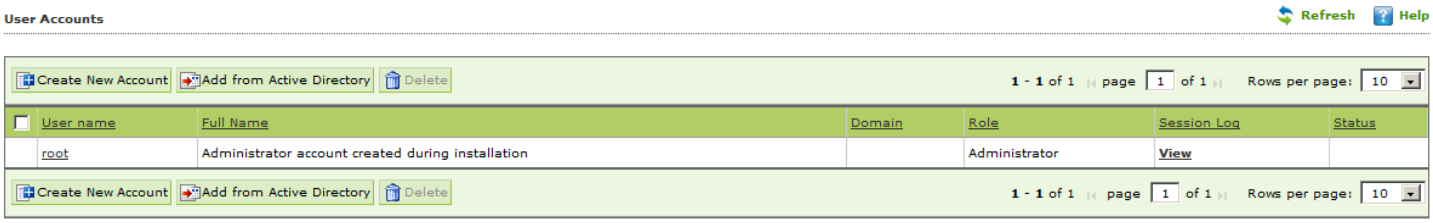
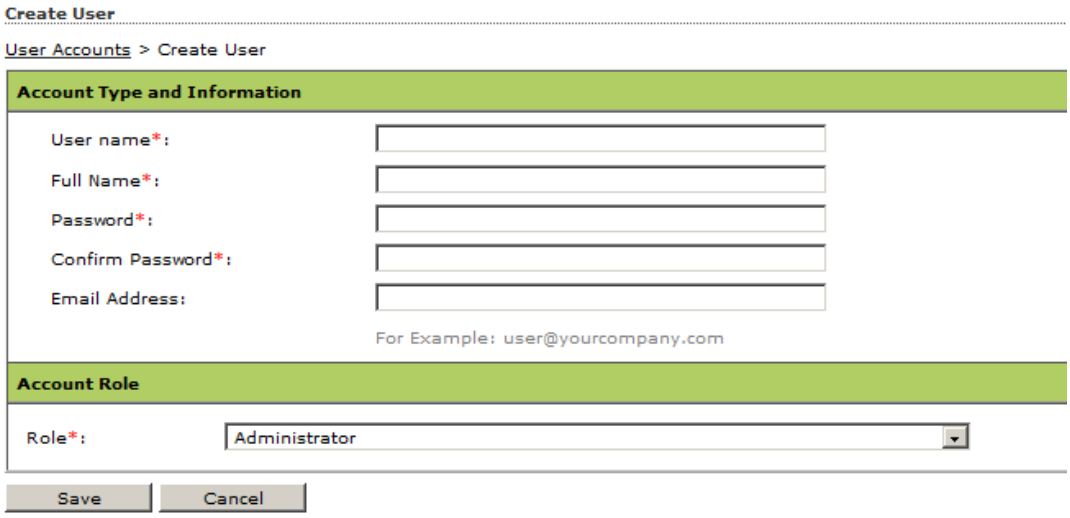


Figure 12654

Click the Create New Account **button.**
The Create User **screen appears. Refer**



2. Figure 12755.

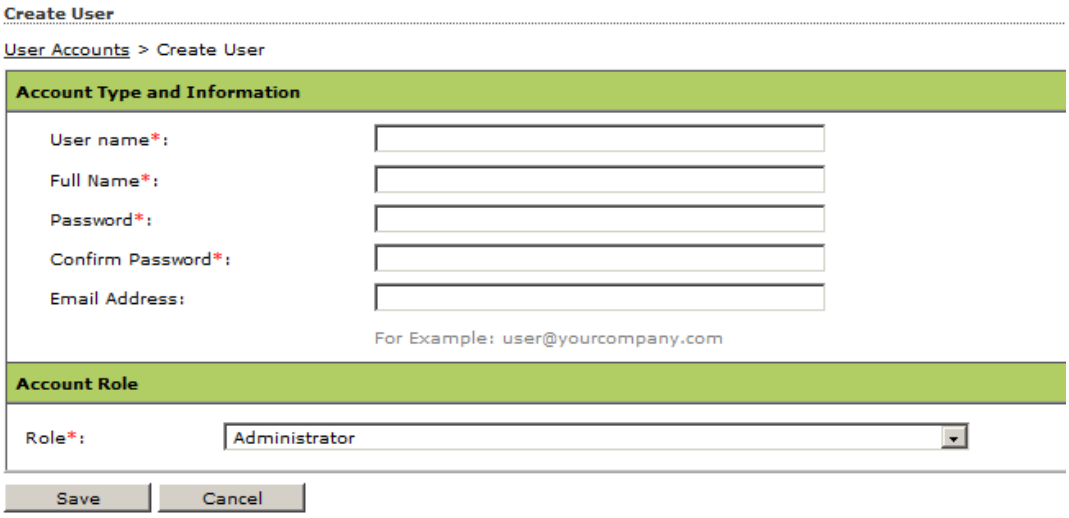


Figure 12755

3. Specify the following field details.

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

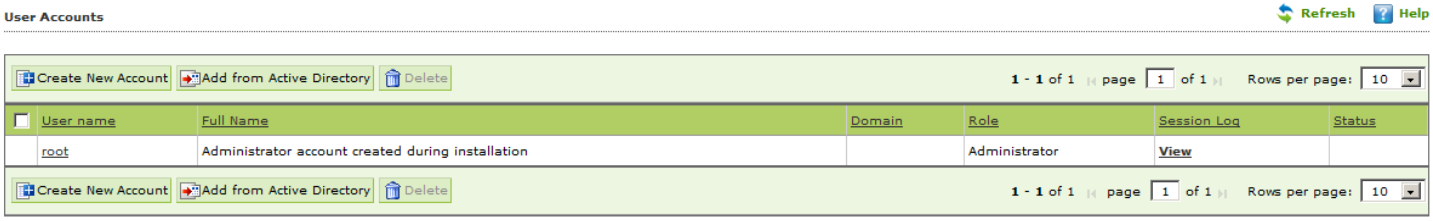
4. Click the **Save** button.

Adding an Active Directory User or Group

The **User Accounts** menu also enables you to add users from the active directory for creating user account.

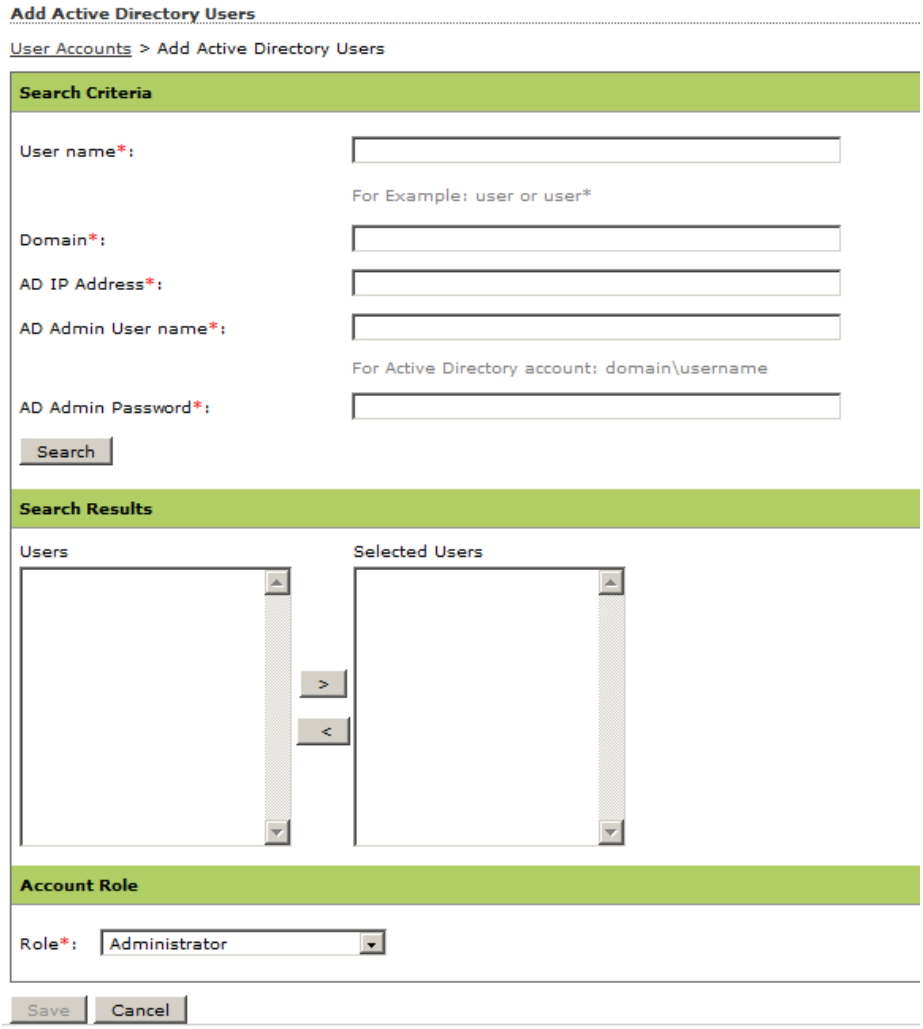
To add an active directory or group

On the navigation pane, under Administration**, click** User Accounts**.**
The User Accounts **screen appears. Refer**



1. Figure 126.

Click the Add from Active Directory **button.**
The Add from Active Directory Users **screen appears. Refer**



2. Figure 12856.

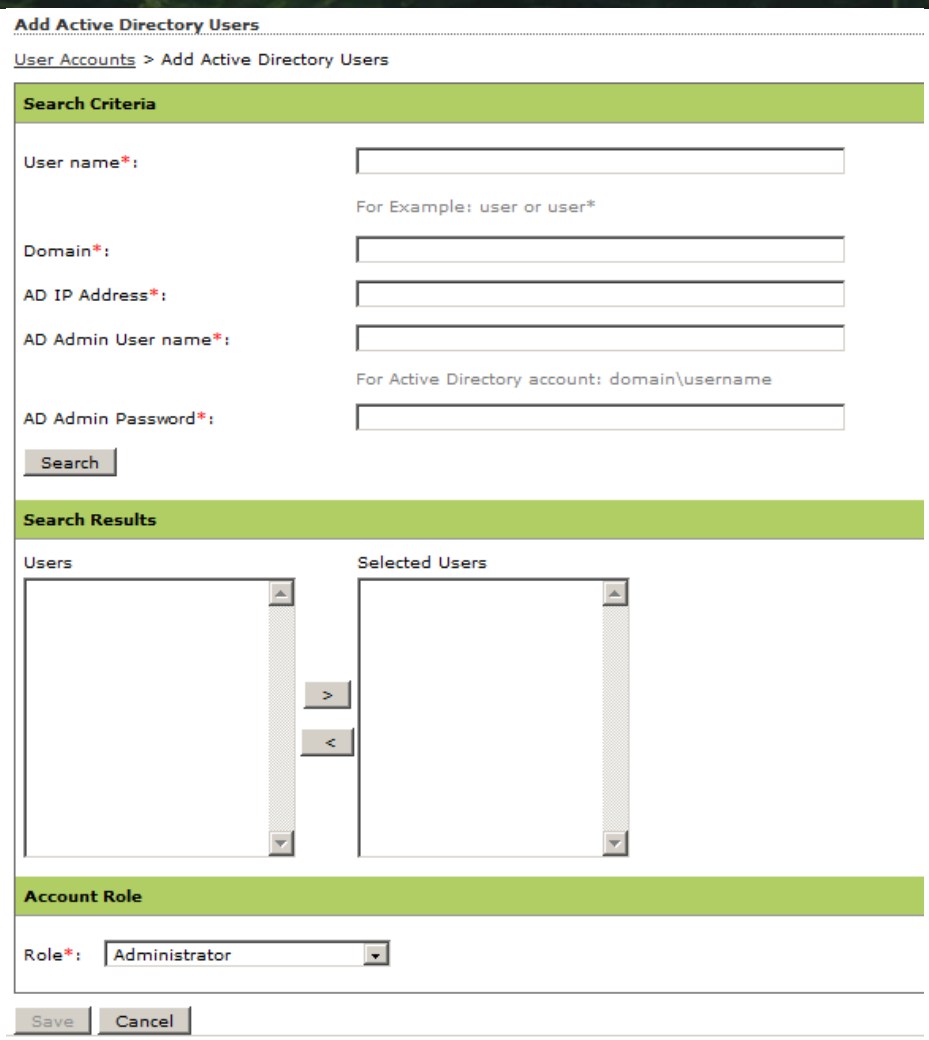

Add Active Directory Users
User Accounts > Add Active Directory Users
Search Criteria
User name*:
For Example: user or user*
Domain*:
AD IP Address*:
AD Admin User name*:
For Active Directory account: domain\username
AD Admin Password*:
Search
Search Results
Users
Selected Users
>
<
Account Role
Role*:
Administrator
Save
Cancel

Figure 128

3. Specify the following field details.

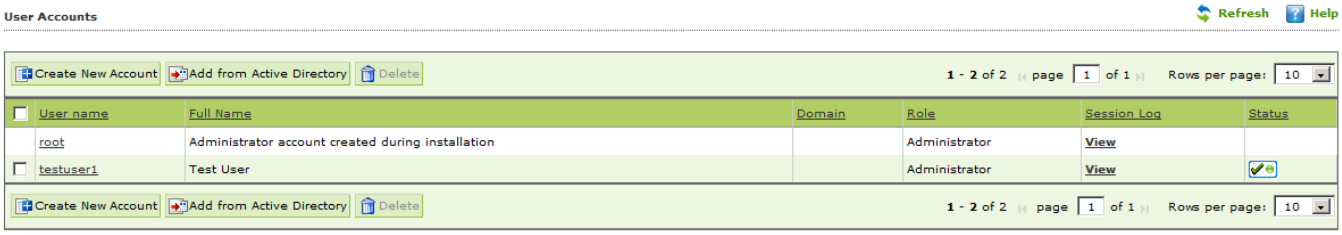
Field	Description
Search criteria	
User name*:	Type the user name. For example, if you want to search for a single user name, type **Admin** and if you want search for all the users under **Admin**, then type **Admin***.
Domain *:	Type the domain name.
AD IP Address*:	Type the active directory IP address.
AD Admin User name*:	Type the active directory administrator user name.
AD Admin password *:	Type the active directory administrator password.
Search	Click this button to search the user. The searched user appears in the **Users** column, under **Search Results** section.
Search Results	
Users	The users appear only when you specify all the field details in the **Search criteria** section.
Selected Users	The selected users appear only when you select users from the **Users** column. Select the user from the **Users** column, and then click the > icon, to add it to the **Selected Users** column, and click the < icon to remove the added user from the **Selected Users** column.
Account Role	
Role*:	Select an appropriate role that you want to assign to the user from the drop-down list.

4. Click the **Save** button.

Deleting an User Account

Perform the following steps to delete an user account.

On the navigation pane, under Administration**, click** User Accounts**.**
The User Accounts **screen appears. Refer**



1. Figure 12958.

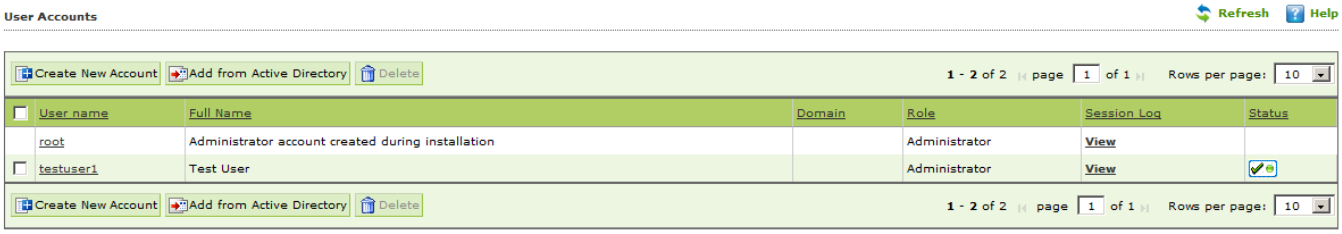
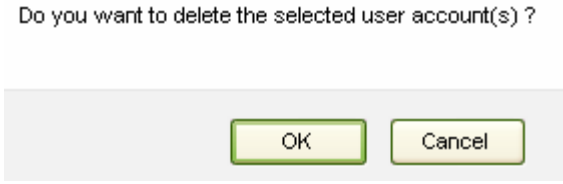


Figure 129

Select an appropriate role check box, and then click the Delete **button.**

The following window appears. Refer



2. Figure 13059.

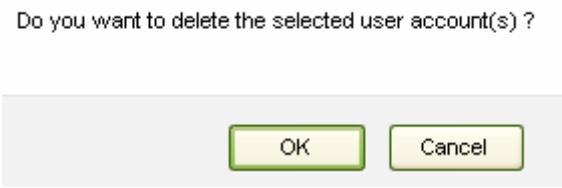


Figure 13059

3. Click the **OK** button.
   The user account gets deleted.

Modifying the User Account Details

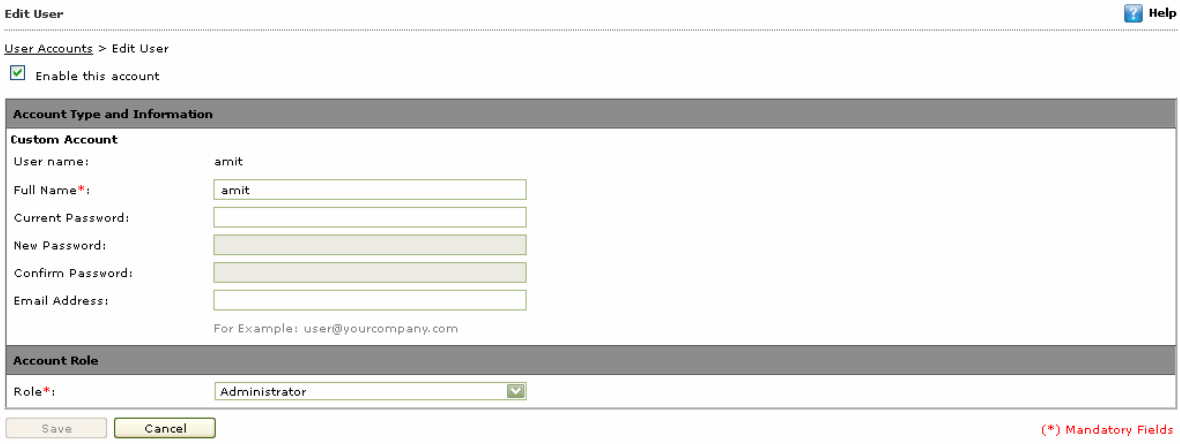
Perform the following steps to modify the user account details.

> You can modify only the root and local user account details.

To modify user account details

1. On the navigation pane, under **Administration**, click **User Accounts**.
   The **User Accounts** screen appears.
2. Click the user link from the **User name** column.

The Edit User **screen appears. Refer**



3. Figure 13160.

Figure 13160

4. Modify the field details as required.
5. Click the **Save** button.

Chapter 16: Export and Import Settings

The eScan Web Console enables you to take backup, which helps ensure that you do not lose your settings and also helps you to restore the settings and policies of WMC and database, whenever required. You can export the settings or you can download the file at a specific location that you want to import. Similarly, you can import the settings or you can browse and select the file that you want to import.

You can do the following settings:

- Export Settings
- Import Settings

Export Settings

Perform the following steps to export the settings.

On the navigation pane, under Administration**, click** Export & Import**.**
The Export Import Settings **screen appears. Refer**

1. Figure 13261.

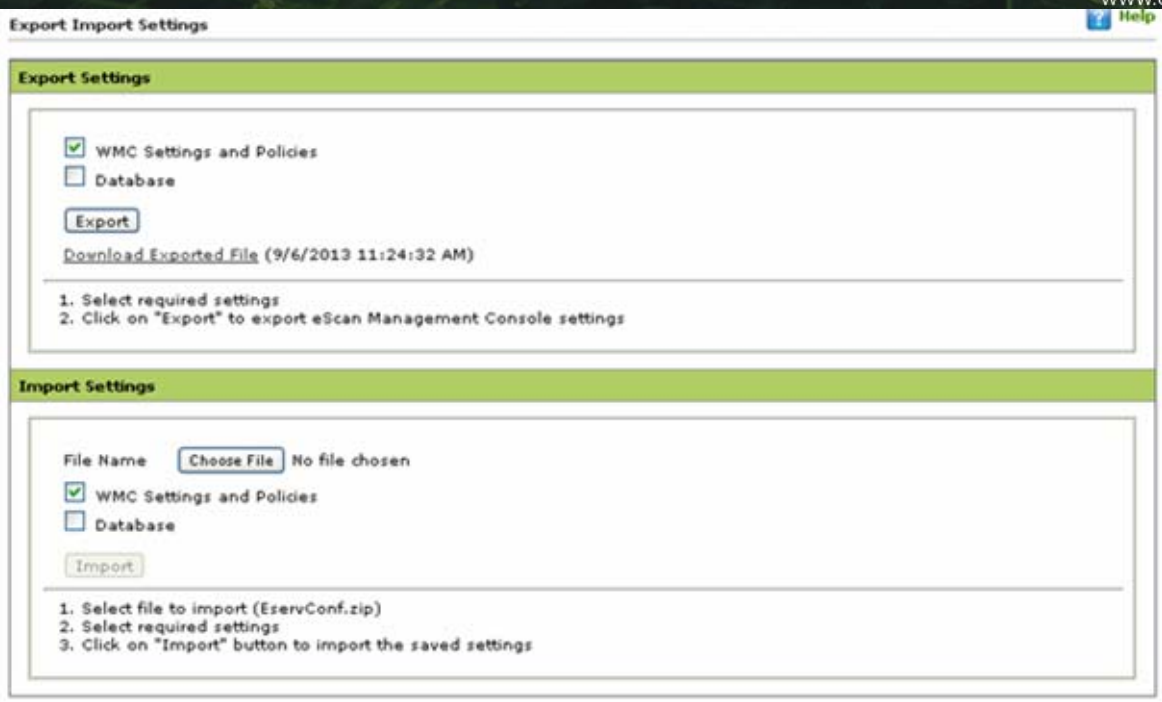
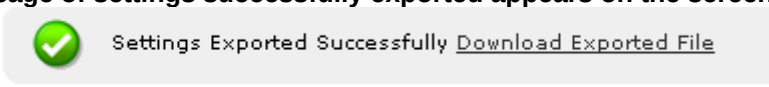


Figure 13261

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 database.

Click the Export **button.**
A message of settings successfully exported appears on the screen. Refer



3. **Figure** 13362.

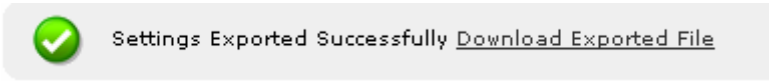


Figure **13362**

4. Click the **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 is downloaded.

Import Settings

Perform 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 the **Browse…** button 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 the **Import** button.
   A message of settings successfully imported appears on the screen.

.

Chapter 17: License

The eScan Web Console enables you to manage license keys. 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.

You can do the following activities:

- Adding License
- Activating License
- Managing License

Adding License

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

To add license

1. On the navigation pane, click **License**.
   The **License** screen appears. Refer Figure 163

Figure 13463

2. Click **To Add License Click Here** link.

3. A window appears. Type the 30 character license key. Refer Figure 164

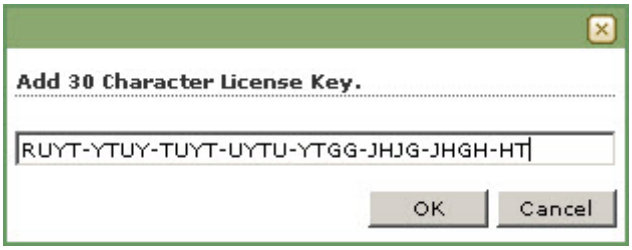


Figure 164

4. Click the **Ok** button.
   The added license appears on the license screen under **Register Information** table.

Activating License

It enables you to activate license after you have added the license.

To activate license

1. On the navigation pane, click **License**.
   The **License** screen appears. Refer Figure 165.

Figure 13565

2. Under **Registration Information** table, click **Activate Now** link.
   The **Online Register Information** screen appears. Refer Figure 166

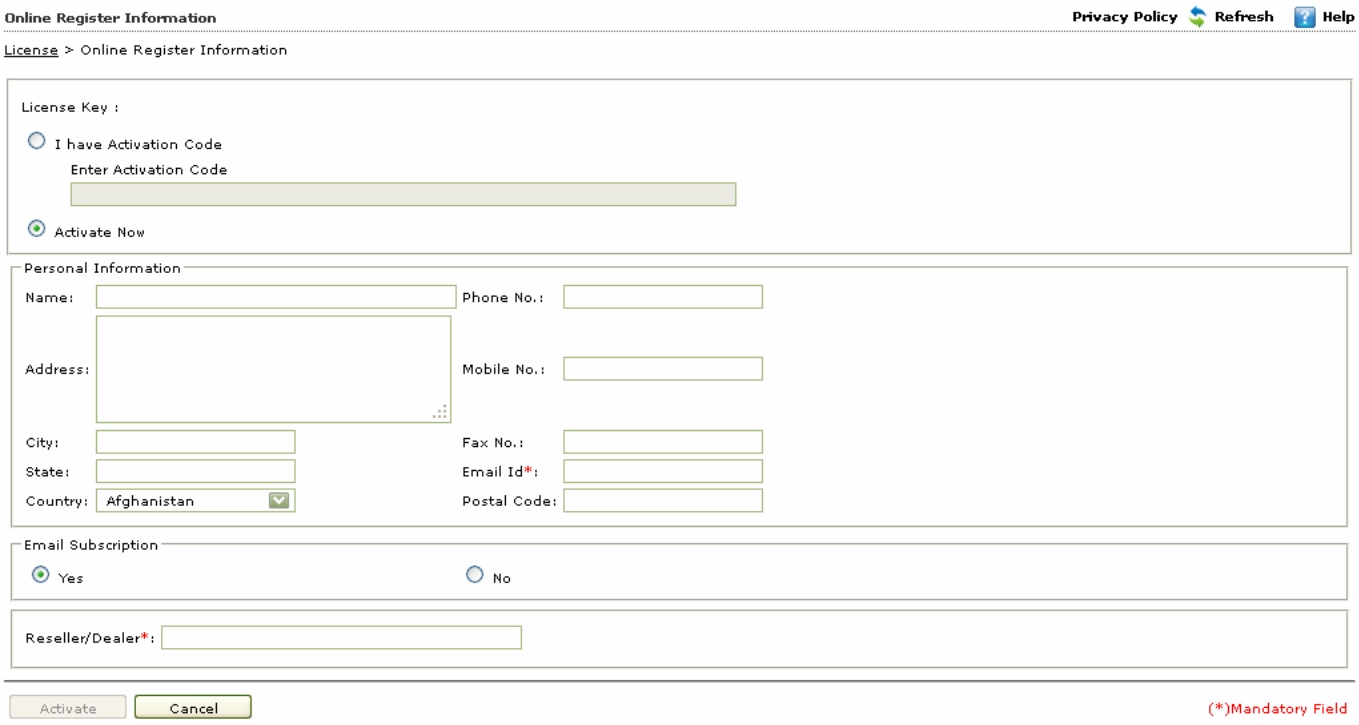


Figure 166

3. Under **License Key:** section, do any one of the following:
   - Click the **I have Activation Code** option, if you have an activation code, and when you click this option, the **Personal Information** section becomes unavailable.
   - Click the **Activate Now** option, if you want to activate the license.

4. Under **Personal Information** section, specify the following details:

Field	Description
Name	Type the customer 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*:	Type an email ID. This is a mandatory field.
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 the **Activate** button.
   The license gets activated.

   (To activate the license key online the computer should have an active internet connection)

Managing Licenses

It enables you move the licensed computers to non-licensed computers and non-licensed computers to licensed computers.

You can do the following activities:

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

Moving licensed computers to non-licensed computers

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

1. On the navigation pane, click **License**.
   The **License** screen appears.
2. Under **License** section, click the **Manage License** link.
   The **Manage License** window appears. Refer Figure 167

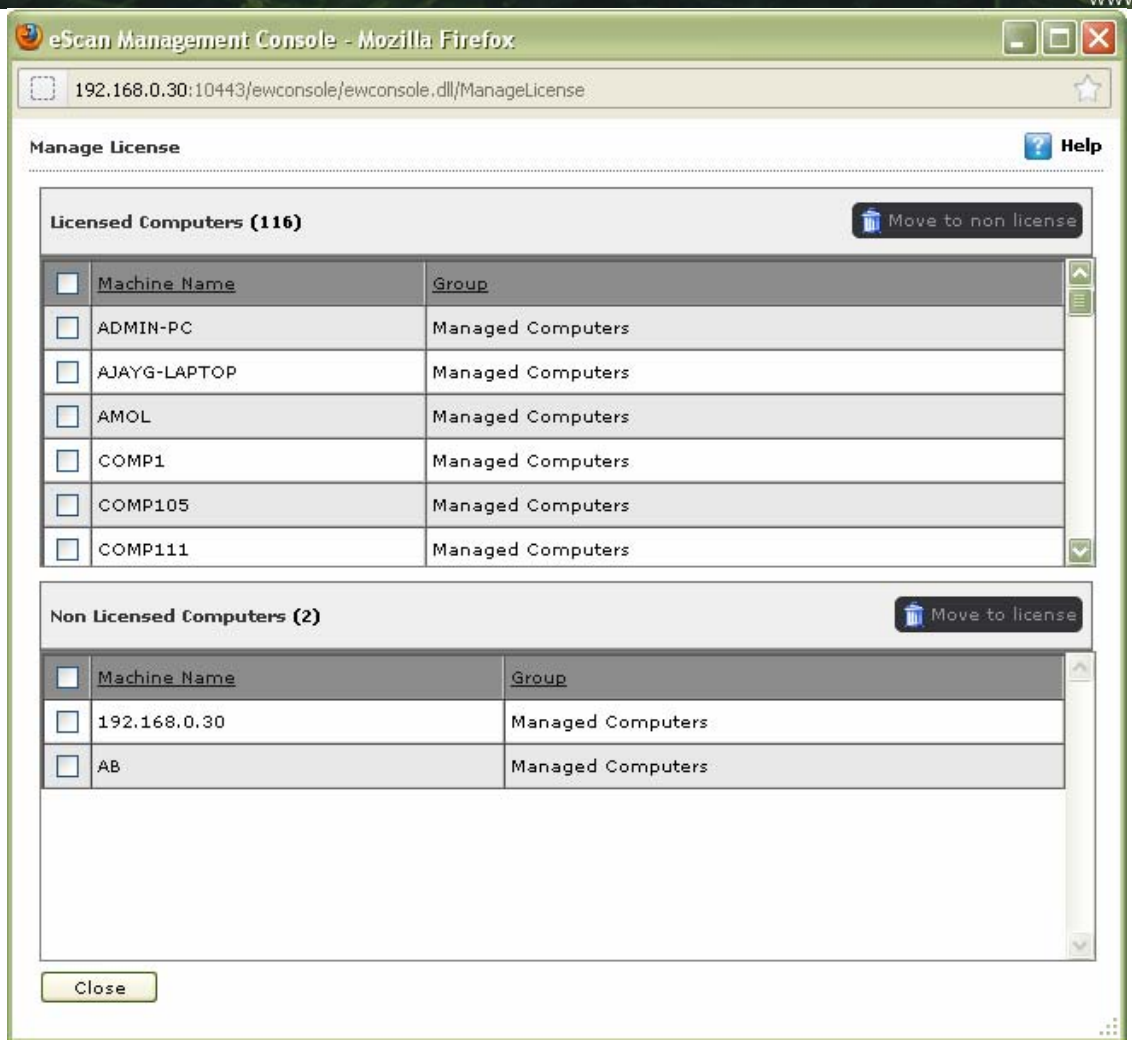


Figure 13667

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. Once the computer is moved to non Licensed computers that client computer will not be allowed to download policies and virus signatures from eScan Server.

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

Moving non-licensed computers to licensed computers

Perform 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 the **Manage License** link.
   The **Manage License** window appears. Refer Figure 168

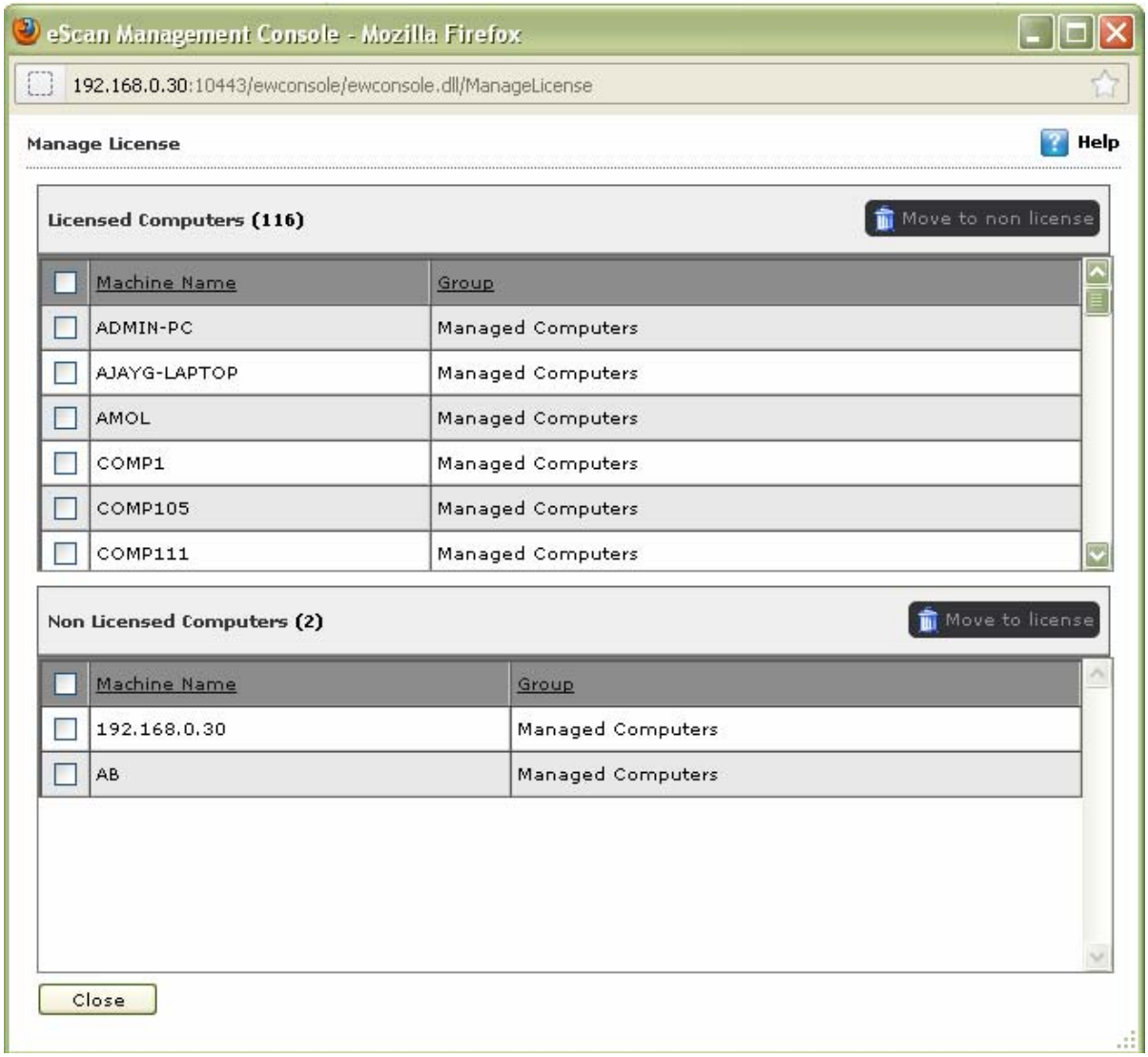


Figure 168

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

Reference

Context Menu

Module/Screen name	Menu/Button	Sub-menu	Description
Managed Computers	Search		To search for the required computer in a network.
	Action List	New Group	To create a new user group.
		Set Group Configuration	To configure the logon settings for the group.
		Install Applications	To install eScan and other applications on the computers in the group.
		Uninstall Applications	To uninstall eScan applications from the computers in the group.
		Create Groups And Tasks	To Create Groups and Tasks.
		Properties	To view general properties of the group, and create and remove update agent.
	Client Action List	Set Host Configuration	To configure the logon settings for the client computer.
		Install Applications	To install eScan and other applications on the client computers.
		Deploy Hotfix	
		Uninstall Applications	To uninstall eScan applications from client computer.
		Move to group	To move the computer to a group.
		Properties	To view the properties of the client computer.
		Remove from group	To remove the client computer from the computer group.
		Refresh Client	To refresh the information about the client computer.
- Policy	Properties		To view and deploy the properties of the selected policy.

- Group Tasks	New Task		To create a new task.
	Start Task		To start the selected task.
	Properties		To view the properties of a task.
	Results		To view the results of the selected task.
	Delete		To delete a task.
- Client Computers			To view the managed client computers on the network
Unmanaged Computers			
- Network Computers	Search		To search for the required computer in a network.
	Action List	Set Host Configuration	To set the host configuration like username and password for a computer.
		Move to group	To move the computer to a group.
		Properties	To view the properties of the computer.
		Refresh Client	To refresh the client computer.
- IP ranges	Action List	Set Host Configuration	To set the host configuration of a group.
		Move to group	To move the computer to a group.
		Properties	To view the properties of the group.
		Refresh Client	To refresh the client group.
	New IP Range		To add a new IP range.
	Delete IP Range		To delete an IP range.
- Active Directory	Action List	Set Host Configuration	To set the host configuration of a computer.
		Move to group	To move the computer to a group.
		Properties	To view the properties of the computer.
		Refresh Client	To refresh the client computer.
	Properties		To view the properties for the Active Directory.

Reports & Notifications	New Template		To create a new template.
	Properties		To view the properties of a report.
	Refresh		To refresh a report.
	Delete		To delete the selected report.
	Properties		To create and save notification properties.
Report scheduler	New Schedule		To create a new schedule.
	Start Task		To start a task.
	Results		To view the results of a new report generation task.
	Properties		To view properties of the report generation task.
Events & Computers	Settings	Event Status	To select the types of event status.
		Computer Selection	To select the types of computer status and its criteria's.
		Software/Hardware Changes	To select the types of update.
	Edit Selection	Protection	To view the computer protection status.
		Events	To view both critical and information events that occurred recently on managed client computers.
		Deploy/Upgrade Client	To deploy/upgrade eScan on client system.
		Check Connection	To view the connection status between server and client.
		Connect to Client	To take a remote desktop connection to client system.
		Properties	To view the properties of a specific client system.
Tasks For Specific Computers	New Task		To create a new task.
	Start Task		To start an existing task.
	Properties		To view the properties of an existing task.
	Results		To view the results of executing a task.

	Delete		To delete a task.
Policies For Specific Computers	New Policy		To create a new policy.
	Properties		To view the properties of the selected policy.
	Delete		To delete a policy.
Outbreak Notifications			To configure the outbreak notification settings.
Settings	EMC settings		To configure the EMC settings.
	Web Console Settings		To configure the Web Console settings.
	Update Settings		To configure the Update settings.
Administration	User Accounts	Create New Account	To create a new user account.
		Add from Active Directory	To add a computer from the Active Directory.
		Delete	To delete a computer from the Active Directory.
	Export & Import		To export and import settings.
License			To enter eScan license key

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.

Registered Offices

Asia Pacific

MicroWorld Software Services Pvt. Ltd.

Plot No 80, Road 15, MIDC, Marol

Andheri (E), Mumbai

India

Tel : (91) (22) 2826-5701

Fax: (91) (22) 2830-4750

E-mail : sales@escanav.com

Web site: http://www.escanav.com

Malaysia

MicroWorld Technologies Sdn.Bhd.

(Co.No. 722338-A)

E-8-6, Megan Avenue 1, 189, Jalan Tun Razak, 50400 Kuala Lumpur

Malaysia

Tel : (603) 2333-8909 or (603) 2333-8910

Fax: (603) 2333-8911

E-mail : sales@escanav.com

Web site: http://www.escanav.com

South Africa

MicroWorld Technologies South Africa (PTY) Ltd.

376 Oak Avenue

Block C (Entrance from 372 Oak Avenue) Ferndale, Randburg, Gauteng, South Africa

Tel : Local 08610 eScan (37226)

Fax: (086) 502 0482

International : (27) (11) 781-4235

E-mail : sales@microworld.co.za

Web site: http://www.microworld.co.za

USA

MicroWorld Technologies Inc.

31700 W 13 Mile Rd, Ste 98

Farmington Hills, MI 48334

USA

Tel : (1) (248) 855 2020

Fax: (1) (248) 855 2024

E-mail : sales@escanav.com

Web site: http://www.escanav.com

Germany

MicroWorld Technologies GmbH

Drosselweg 1,

76327 Pfinztal,

Germany

Tel : (49) 7240 944909 20

Fax: (49) 7240 944909 92

E-mail : sales@escanav.de

Web site: http://www.escanav.de