eScan Web Console
User Guide

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

Document Number: 5BUG/20.05.2011/11.x
Current Software Version: 11.x.x

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:	May, 2011

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 11 AV SMB Edition for Windows®. For convenience, we have referred to eScan 11 AV SMB Edition as eScan throughout this document. The names of other eScan products are spelt out in full, 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 with 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 & Notifications
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: Unmanaged Computers
This chapter provides you 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 12: Configuring the Settings
This chapter provides you with information on how to configure the settings for EMC, the eScan Web Console, and Updater.

Chapter 13: Managing User Accounts

This chapter provides you information on how to manage local and Active Directory user accounts.

Typographic Conventions Used in this Guide

The following table lists the typographic conventions used in this guide.

Typeface	Meaning	Example
Bold	UI element, input text	In the **Report** dialog box, click **OK**. In the **Value** box, type **1**
Bold, Red	Warning	**Warning!** Do not install A before installing B.
Bold, Green	Important	**Important:** Remember to always perform step A before performing step B.

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 11 User Guide** contains information on the features of eScan 11. In addition, it contains detailed steps on how to install and configure eScan 11.
  - **eScan 11 Web Management Console Administrator's 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 11 Quick Reference Guide** provides an overview of eScan features and includes detailed instructions and steps for installing it.

  Note: 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.

Note: 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

Contents

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.

Note: 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.)

Note: 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.

- **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 cross 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.

- The **Policies for Specific Computers** page enables you to create and deploy policy on specific client computers, 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.

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** 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
- **Microsoft .Net Framework it is already included in the eScan setup file**

Note: All these components are installed when you install a version of eScan 11 that contains the eScan Web Console. eScan Web Console runs on Apache Server

Hardware and Software Requirements

The software and hardware requirements for installing eScan are as follows:

- Software Requirements
- Minimum Hardware Requirements

Software Requirements

eScan products run on the 32-bit or 64-bit editions of the Windows® operating system. Your computer should have any one of the following operating systems installed on it.

- Windows® 2000 SP4 with KB891861
- Windows® XP Professional with SP2 and above (For 32-bit edition only)
- Windows® XP with SP1 and above (For 64-bit edition only)
- Windows® Vista Ultimate
- Windows® Vista Business
- Windows® Vista Enterprise
- Windows® 7 Ultimate
- Windows® 7 Business
- Windows® 7 Enterprise
- Windows Server® 2003
- 32-bit edition of Windows Server® 2008
- 64-bit edition of Windows Server® 2008
- Microsoft SBS 2011
- Microsoft SBS 2011 Essential

In addition, a PDF reader and Internet Explorer® version 5.0 or higher should be installed on the computer.

Minimum Hardware Requirements

Your computer must meet the following minimum requirements.

- Processor: 1GHz
- RAM: 1024 Megabytes (MB) of RAM (recommended 2048 MB)
- Monitor Resolution: 800 x 600
- Hard Disk Space: 1 GB of free hard disk space
- Additional Drives: CD-ROM drive

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.

- Schemes for Deploying eScan
- Considerations for Selecting a Deployment Scheme
- Installing SSL Certificate

Schemes for Deploying eScan

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

- Installing eScan Manually
- 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.

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 for when the actual deployment take place. For these kind of scenarios Adminsitrators scan either install MWAgent on those systems or manually install the eScan client setup. To access the MWAent setup file follow the below steps

Access MWAgent setup file and install eScan client

1. On the taskbar, right-click the eScan Protection Center icon, and then click **Pause Protection**.
2. From the eScan installation folder, double-click the **eserv.ini** file.
   The **eserv.ini** file opens.
3. Search for "ShowAgentSetup" entry, default value is "0", change the value from "0" to "1"
4. Save the file. And then on the taskbar, right-click the eScan Protection Center icon, and then click **Resume Protection**
5. When you access the eScan Management Console , you view a https://<IP/hostnameofserver>:10443/Agent_Setup.exe link for MWAgent on login screen.
6. Click the https://<IP/hostnameofserver>:10443/Agent_Setup.exe link.
   A **File Download** window appears.
7. 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.

Installing SSL Certificate

The SSL certificate can be installed as well as upgraded, and while upgrading the certificate has to be installed again.

Perform the following steps to install SSL certificate for eScan Web console login page.

To install SSL certificate

- **Fresh Installation**

1. Open Internet Explorer and then type **https://<IP/hostname>:10443** in the **Address** bar.
   Where,
   IP/hostname = eScan server IP or hostname

An error message appears displaying three options before installing the SSL certificate.

2. Click **Continue to this website (not recommended).** option.

As the certificate is not added to the browser, you get a certificate error.

3. Click the **Certificate Error** message, and then click **View Certificates** link.
   The **Certificate** dialog box appears.
4. Click the **Certification Path** tab.
   The **Certification Path** tab appears.
5. Under **Certification path** section, click **MicroWorld Software Services Pvt. Ltd. Internal_CA** option, and then click **View Certificate** button.
   The **Certificate** dialog box appears.
6. Click the **General** tab.
   The **General** tab appears.
7. Click **Install Certificate…** button.
   The **Certificate Import Wizard** dialog box appears.
8. Click the **Next >** button.
   The next dialog box appears.
9. Click **Place all certificates in the following store** option.
10. Click the **Browse…** button, to browse and select the **Trusted Root Certification Authorities** from the **Select Certificate Store** dialog box.
11. Click the **Next >** button.
    The next dialog box appears.
12. Click the **Finish** button.
    This initiates the process of adding certificate to local certificate repository.
    The **Security Warning** dialog box appears.
13. Click the **Yes** button.
14. Once the installation is complete, click the **OK** button, and then restart the browser.
    This installs the necessary SSL certificates for eScan Web console login page on your system.

- **Upgrade**

In case, if product is upgraded, a fresh certificate is issued, due to which the existing certificate becomes null and void. Hence, browser requests you to add the certificate wherein you have to install certificate again.

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:

1. Open a browser window and in the Address bar, type the following URL:
   https://<*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.

2. 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

Dashboard is a special page that contains tabs, which display the eScan deployment status, protection status, and protection statistics 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 three sub-items: **Network Computers**, **IP range**, and **Active Directory** 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 IP ranges in the network.
- The **Active Directory** page displays the computers in the Active Directory.

Reports and Notifications

The **Reports and Notifications** 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 additional systems whenever required.

Outbreak Notification

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

Settings

The **Settings** menu item has three sub-items: **EMC settings**, **Web Console Settings**, and **Update Settings**.

- 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.
- The **Web Console Settings** page allows you to configure the eScan Web Console timeout, Dashboard setting and SQL server connection setting.
- The **Update Settings** page allows you to configure the general, update notification, and update scheduling settings.

User Accounts

The **User Accounts** page allows you to add custom accounts or Active Directory users or groups.

The following sections describe UI of each of the links in 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** tabs, and **Configure Dashboard Display** link.

- Deployment Status
- Protection Status
- Protection Statistics
- 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.

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 **eScan Version** pie chart displays the versions of eScan available in the network and the number of computers running that version. You can click the value in the legend to view the names of the computers and the versions installed on them.

- 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.

In Manage License, you can move the licensed computers to non-licensed computers and non-licensed computers to licensed computers. You can manage licenses in the following ways:

- To move licensed computers to non-licensed computers
- To move non-licensed computers to licensed computers

- **To move licensed computers to non-licensed computers**

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

1. Click the **Manage License** link.
   The **Manage License** window appears.

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

Note: 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.

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

- **To move non-licensed computers to licensed computers**

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

1. Click the **Manage License** link.
   The **Manage License** window appears.

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

Note: 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.

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

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 and its status in a popup window.

- File Anti-Virus
- Proactive
- Mail Anti-Virus
- Anti-Spam
- Mail Anti-Phishing
- Firewall

  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 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/YYY)**, **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, Firewall 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.

- 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 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.
      - **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 executables.

  - 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 executables. 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.

Configuring Dashboard

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

To configure dashboard

1. Click the **Configure Dashboard Display** link, at upper-right corner of the screen.
   The **Configure Dashboard Display** window appears.
2. Select an appropriate check box from all sections that you want to configure on the dashboard.
3. 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.

Note: 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.
2. Click the **Next >**button.
   The **Create Group to Manage Computers** screen appears.
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**.

Note: 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.
6. By default, the **Add IP/Host** and **Add Host from the unassigned Computer** button appears dimmed.
7. 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.
8. Click the **Add** button.
   A window appears.
9. In the **Select Computer** field, type the host name that you want to add.
10. Click the **Ok** button.
    The added computer appears in **Add Computers** list.
11. Click the **Add IP Address Range** button.
    A window appears where you can add IP addresses of computers that you want to add.
12. In the **Starting IP Address** field, type IP address of the computer from which range you want to add. It is a mandatory field.
13. In the **Ending IP Address** field, type IP address of the computer till which range you want to add. It is a mandatory field.

14. Click the **Ok** button.
    The added computer appears in **Add Computers** list.
15. If you want to cancel the action, click the **Cancel** button.
16. 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.
17. Click the **Ok** button.
    The computers get added in their respective group.
18. Click the **Next >**button.
    The **Select Groups for Installation/Deployment** screen appears.
19. 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.
20. Select the **Auto Reboot after install** check box, if you want to auto restart the client system after installation.
21. Select the **Show Progress On Client (Only for XP/2000)** check box, if you want to view installation progress on client system.

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

22. Select the **Install Without Firewall** check box, if you want to view install eScan without Firewall module.
23. In the **Installation Path** drop-down list, default path appears.
24. To change path, click the **Add** button.
    A window appears.
25. 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.
26. If you want to cancel the action, click the **Cancel** button.
27. Click the **Next >**button, to install/deploy.

Note: The computers having same or newer verison of eScan are not affected.

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

Adding Host from the unassigned Computer

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.

2. To add computer from domain, click the group name for which you want to add host, and then click the **Add Host from the unassigned Computer** button.
   A window appears with an unmanaged computer list from where you can add computers.
3. Select the appropriate check boxes, 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 27 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
- Task Pane
- Accessing the Search Feature
- Menus

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
- Group Tasks Pane
- Client Computers Pane

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.

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

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

Note: 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 has the following options:
  - **Create 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:** 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 & 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.

- **Client Action List** menu has the following options:
  - **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.

Note: 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.
- **Connect to client:** It enables you to take a remote desktop connection to client system.

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 three sub-nodes: **Network Computers**, **IP range**, and **Active Directory**. 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 & Notifications

The **Reports & Notifications** 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 & Notifications** in the navigation bar. The page displays a table containing report names and a **View** link next to each name. 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 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 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.

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. (EMC – eScan Management Console)

Managing User Accounts

Typically this is being used to Manage EMC and Web Console. The **User Accounts** page is displayed when you click **User Accounts** in the navigation bar. This page allows you to add users from custom accounts or Active Directory user lists or groups. It also displays a table that lists the user name, description, domain name, role, and enabled/disabled status of user accounts. In addition, you can add local users or Active Directory users or delete users as per your requirements.

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.

Note: 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.

Note: 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.

Note: 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.

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

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

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

Note: 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.

Note: 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.

Note: The **Properties** 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 **Properties**.
   The **Properties** window appears.

5. View the following details as required:

Note: 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	

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td colspan="2">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
• Firewall</td></tr>
</table>

Deploying Hotfix

It enables you to deploy hotfix on the client machine.

Note: 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

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

Note: 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.

Note: 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.

Note: 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

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

Note: 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.

Note: 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.

Note: The **Move to Group** 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 **Move to Group**.
   The **Select Group** window appears.
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.

Note: 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.

Note: 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.

Note: 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.

Note: 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.
3. In the **New Group Name** field, type name.
4. Click the **Ok** button.
   The group gets created.
5. If you want to create sub group under any group, perform the following steps:

   i. On the left pane, click an appropriate managed group folder.
   ii. Click the **Action List** drop-down menu, and then click **New Sub Group**.
   The **Creating New Group** window appears.
   iii. In the **New Group Name** field, type name.
   iv. 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. To remove a computer from the group, in the eScan Web Console, in the left pane, under **Dashboard**, click **Managed Computers**.
2. On the **Managed Computers** page, on the right pane, in the console tree, click the name of the group from which you want to remove the computer.
3. In the console tree, under the selected group, click **Client Computers**.
4. In the right pane, select the name of the computer that you want to remove, and then on the **Client Action List**, click **Remove from group**.

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. To delete a computer group, in the eScan Web Console, in the left pane, under **Dashboard**, click **Managed Computers**.
2. On the **Managed Computers** page, on the right pane, in the console tree, select the computer group that you want to delete, and then on the **Action List** menu, click **Delete**.

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. In previous versions of eScan if you have a branch office you had to create a eScan Child server to distribute the updates to eScan clients located in that branch. In Version 11, you do not have to install eScan as a child server in branch, 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
- Creating Update Agent
- Removing Update Agent

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.

Note: 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.
3. 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.
4. Click the **General** tab.
   The **General** tab appears.
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.
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.

Note: 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.
3. Click the **Action List** drop-down menu, and then click **Properties**.
   The **Properties (a)** window appears.
6. Click the **Update Agents** tab.
   The **Update Agents** tab appears.
4. Click the **Add/Remove** button.
   A window appears displaying selected sub-group with its client machine.
5. 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.

Note: 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.
3. Click the **Action List** drop-down menu, and then click **Properties**.
   The **Properties (a)** window appears.
7. Click the **Update Agents** tab.
   The **Update Agents** tab appears.
4. Click the **Add/Remove** button.
   A window appears displaying selected sub-group with its client machine.
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

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

2. Click the **Action List** drop-down menu, and then click **Set Group Configuration**.
   The **Set Group Configuration** window appears.
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.
2. Click the **Action List** drop-down menu, and then click **Create Groups and Tasks**.
   The **Group Structure Wizard** window appears.
3. Under **Create Group Structure based on** section, click the **Microsoft Windows Domains and Workgroups** option.
4. Click the **Next >** button.
5. Under **Target Groups** section, click the **Browse** button.
   The **Select Group** window appears.

Note: 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.

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.

Note: 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 the computers to the selected group.
9. Click the **Next >** button.
   A message of creating the group wizard appears.
10. Click the **Finish** button.
    The window gets close.

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.
2. Click the **Action List** drop-down menu, and then click **Create Groups and Tasks**.
   The **Group Structure Wizard** window appears.
3. Under **Create Group Structure based on** section, click the **Active Directory** option.
4. Click the **Next >** button.
5. Under **Target Groups** section, click the **Browse** button.
   The **Select Group** window appears.

Note: 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.
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.

Note: 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.

Note: 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 Organisation Unit** section, click the **Browse** button.
   The **Select Source Active Directory** window appears.

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

10. Click an appropriate active directory source that you want to add, and then click **Ok** button.
11. Click the **Next >** button.
    A message of creating the group wizard appears.
12. 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.
2. Click the **Action List** drop-down menu, and then click **Deploy/Upgrade Client**.
   The **Client Installation** window appears.
3. Click **Install eScan** option, if you want to install eScan application.

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

4. Specify the following field details:

Field	Description

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. **Note:** 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.

5. In the **Installation Path** drop-down list, by default <Default> appears, which installs eScan in "%systemroot%/programfiles/eScan" folder.
6. Click the **Add** button, to add path for installation.
   The **Add Folder** dialog box appears.

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

7. 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.

Note: 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.

Note: 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.

Note: The **Deploy/Upgrade Client** 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/Upgrade Client**. The **Client Installation** window appears.
5. Click **Install Other Software** option, if you want to install other software.

Note: 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.
7. Type the file path that you want to add.
8. In **Executable file** drop-down list, click the file that you want to execute on client machine.
9. In **Parameters** field, type the parameters using which you want to execute the executable file.
10. Click the **Install** button.
    A message of successful installation of eScan appears.

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**.

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

Note: 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.
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.

Note: 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.

Note: 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.
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
- Start an Existing Task
- View the Status of Tasks
- View the Properties of an Existing Task
- Delete an Existing Task

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 Mail nti-virus 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.

Note: 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.
2. Click the **New Task** button.
   The **New Task Template** screen appears.
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.

Field	Description
	• Click **Disabled**, if you want to stop **Anti-Spam** 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, and click an appropriate option. • Click **Server IP**, then select an appropriate option from the drop-down list to set update server. • Click **Others**, if you want to set update server through other IP address, and then type an appropriate IP address.
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.

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

Note: 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.
9. Under **Task Scheduling Settings** section, specify the following field details.

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: 1. Click the Time icon. The Timer appears. 2. 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, under **Dashboard**, click **Tasks for Specific Computers**.
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**.
   A window appears displaying status of the running task.
3. To close the status window, click **Close**.

View the Status of Tasks

You can view the status of scheduled tasks or the tasks that you have run manually by clicking the **Results** button. 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, timestamp, and the description. You can select a computer name in the table to view its status, timestamp of execution of the task, and description 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:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Tasks for Specific Computers**.
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**.
3. This will open the **Task Results** page, which will display the client computer or group on which the task was executed, the name of the group, the status of completion of the task, time at which the task was completed, and the description of the task.

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**.
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.
    - The **Schedule** tab displays the date options.
    - The **Machines** tab displays all the groups as well as managed computers in the network.
    - The **Settings** tab displays the template used for creating the task. You can make changes to the settings, if required.

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, under **Dashboard**, click **Tasks for Specific Computers**.
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 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:

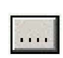
Policies are also available in **Managed Computers**, which is divided in to two tabs - **General** and **Policy Details**. In **General** tab, you can view the general policy details and in **Policy Details** tab**,** you can configure the policy details.

- Creating and Deploying New Policy
- Viewing Policy Properties
- Deleting Policy
- Viewing General Policy Settings
- Configuring 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.
2. Click the **New Policy** button.
   The **New Policy** screen appears.
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  icon, if you want to view and configure settings.
5. Under **Select Computers/ Groups** section.

Note: 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

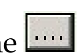
It enables you to view the list of created policy and its properties.

To view policy property

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

Note: 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.
3. Click the **General** tab.
   The **General** tab appears.
4. View the field details as required.
5. Click the **Policy Details** tab.
   The **Policy Details** tab appears.
6. Select an appropriate check box, and then click the  icon, if you want to view settings.
7. View the field details as required.
8. Click the **Machines** tab.
   The **Machines** tab appears.
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.

Note: 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.
3. Click the **Properties** button.
   The **Properties** window appears.
4. Click the **General** tab.
   The **General** tab appears.
5. By default, Group Default Policy appears in the **Name of Deployed Policy** field, it indicates name of the policy.
6. In the **Last Modified** section, you can view the details of when and at what time the last policy is deployed. For example, Apr11 2011 04:11:38 PM
7. In the **Deploy To Whom** section you can view the name of the group on which the policy is deployed.
8. View the details as required.

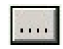
Configuring Policy Details

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.

Note: 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.
3. Click the **Properties** button.
   The **Properties** window appears.
4. Click the **Policy Details** tab.
   The **Policy Details** tab appears.
5. Select an appropriate check box, and then click the  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.
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.

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

1. On the navigation pane, click **Reports & Notifications**.
   The **Reports & Notifications** screen appears.
2. Click the **New Template** button.
   The **New Template** screen appears.
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**,

Field	Description
	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**.
Report Period & Sort By	
Date Options	Click an appropriate option. For example, Today, This Week, This Month, and so on. **Note:** The options changes depending upon the report type.
Sort By	Click an appropriate option. For example, Date, computer, and so on. **Note:** The options changes depending upon the report type.

Field	Description
Select Computers/Groups	
Select Condition	
Generate a Report for Groups	Click this option, if you want to generate report for groups, and then select an appropriate Managed Computer group check box from the **Select Target Groups** section, for which you want to generate report.
Generate a Report for a List of Computers	Click this option, if you want to generate report for computer, and then select an appropriate Managed Computers check box from the **Select Client Computers** section, for which you want to generate report.

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

Viewing the Properties of a Report

You can view the properties of existing reports by clicking the report names 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 an existing report are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Reports & Notifications**.
2. On the **Reports & Notifications** 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 report name, and details regarding the report such as the template type, date of creation, and date of modification. The **Report Period & Sort By** tab displays the date options and the sort criteria. The **Groups** tab displays the available groups in the left list and the selected groups in the right list. You can make changes, if required.
4. To save the report, click **Save**.

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:

1. On the navigation pane, click **Reports & Notifications**.

The **Reports & Notifications** screen appears.

2. Click the **Properties** button, on upper-right side of the screen.
   The **Properties** screen appears.

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.

3. Click the **Test** button, to test the connection.
   A message of successful connection and sending of notification appears.
4. 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
- Start an Existing Report Generation Task
- View the Status of Report Creation Schedules
- Configure the Properties of an Existing Report Creation Task

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, Anti-Spam Report, Mail Anti-Virus 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 Mail Anti-Virus 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:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Report Scheduler**.
2. On the **Report Scheduler** page, on the right pane, click **New Schedule**.
3. 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.

4. 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.)
5. To enable the scheduler, under **Task scheduling settings**, click **Enable Scheduler**. Alternately, you can start the scheduler manually by clicking **Manual Start**.
6. 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.
7. To generate reports on a monthly basis, click **Monthly**, and then select the number of months from the drop-down list.
8. Click the Time icon.
   The Timer appears.
9. 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.

10. 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:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Report Scheduler**.
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**.
3. This will open the Task window. The Task window will display the status of the running task.
4. To close the status window, click **Close**.

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:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Report Scheduler**.
2. 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**.
3. This will open the **Task Results** page, which will display the client computer or group on which the task was executed, the name of the group, the status of completion of the task, time at which the task was completed, and the description of the task.

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:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **Report Scheduler**.
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.
    - The **Schedule** tab displays the date options and the sorting criteria. If you want you can change schedule of the report.
    - 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.

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:

1. Click the **Settings** button.
   The **Events & Computers Settings** window appears.
2. Select type of event from the **Event Name** drop-down list.
3. Type the number of events that you want to view in a list, in the **Number of Records** field.
4. 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. Specify the following field details.

Field	Description
Check for eScan Not Installed	Select this check box if you want to view the list of client systems under managed computers on which eScan has not been installed.
Check for Monitor Status	Select this check box if you want to view the client systems on which eScan monitor is not enabled.

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.
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. Specify the following field details.

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

Saving Computer Settings

Perform the following steps to save the computer settings:

1. Click the **Settings** button.
   The **Events & Computers Settings** window appears.
2. By default, the **Events Status** window appears.
3. Click the **Computers Selection** tab.
   The **Computers Selection** window appears.
4. Select type of status for which you want to set criteria, from the **Computer status** drop-down list.
5. 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.
6. 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. Click the **Settings** button.
   The **Events & Computers Settings** window appears.
2. By default, the **Events Status** window appears.
3. Click the **Software/Hardware Changes** tab.
   The **Software/Hardware Changes** window appears.
4. 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.

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

Edit selection

Note: 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:

1. On the navigation pane, click the **Computer Selection** folder, and then click the computer status for which you want to edit.
2. The list of selected computer status records appear on right side of the screen.
3. Select the appropriate check box, the client system for which you to edit the properties, and then click the **Edit Selection** drop-down menu.
4. 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.

Note: 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

1. 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.
2. 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.

Column heading	Description
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.

3. 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.

Note: 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

1. 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.
2. 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.

Column heading	Description
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.
Firewall	It indicates the firewall 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.

3. 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.

Note: 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 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.
2. 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

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.

- Hardware 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.
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

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.

Column heading	Description
Motherboard	It indicates name of the motherboard.
HDD	It indicates the capacity that is, size of HDD (Hard Disk).

3. View the details as required.

Chapter 11: 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 three nodes under **Unmanaged Computers**: **Network Computers**, **IP range**, and **Active Directory**.

- 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.

Note: 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 eScan 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, path of the installed directory, status of the monitor, status of the Anti-Spam, Mail Anti-Virus, 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.

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

1. On the navigation pane, click **Unmanaged Computers**, and then click **Network Computers**.
   The **Network Computers** screen appears.
2. At the upper left side, click the **Search** button.
   The **Search for Computers** window appears.
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, 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

Note: 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.

Note: 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

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

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

Note: 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. Click an appropriate computer name check box for which you want to set configuration.

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

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

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

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

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

Note: 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. Click an appropriate computer name check box that you want to move to group.

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

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

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

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

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

> **Note:** 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. Click an appropriate computer name check box for which you want to view properties.

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

4. Click the **Action List** drop-down menu, and then click **Properties**.
   The **Properties** window appears.
5. View the following details as required:

> **Note:** 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.

Field	Description
	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 • Firewall	

IP Range

The **IP Range** page displays the IP range for the network as nodes in a console tree. You can select a node in the console tree to view the computers in that IP range. You can click the name of 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, path of the installed directory, status of the monitor, status of the Anti-Spam, Mail Anti-Virus, 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.

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**.
2. On the **IP range page**, click **New IP range**.
   The **Specify IP Range** window appears.
3. In the **Starting IP Address** field, type the IP address from where you want to start the IP range.
4. In the **Ending IP Address** field, type the IP address till where you want to create the IP range.
5. 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:

1. In the eScan Web Console, in the left pane, under **Dashboard**, under **Unmanaged Computers**, click **IP range**.
2. On the **IP range** page, in the console tree, select the IP range that you want to delete, and then click **Delete IP range**.

Active Directory

The **Active Directory** page shows a console tree, which lists all the domain controllers in the network. You can click a domain controller to view its details in the task pane. You can also add, modify, or delete the Active Directory domain controller details from the Properties window, which opens when you click **Properties**. You can also specify a user name and password for the domain controller, if required.

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

You can do the following activities:

- View the Properties of a Domain Controller
- Add the Logon Settings for a Domain Controller
- Modify the Logon Settings of a Domain Controller
- Delete the Logon Settings of a Domain Controller

View the Properties of a Domain Controller

The eScan Web Console allows you to view the properties of a domain controller.

The steps to view the properties of a domain controller are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, under **Unmanaged Computers**, click **Active Directory**.
2. On the **Active Directory** page, click **Properties**. This will show you the IP address of all available the domain controllers.

Add the Logon Settings for a Domain Controller

You can specify the log on settings for a domain controller by specifying a user name and password along with its IP address in the Logon Settings window.

The steps to add the logon settings for a domain controller are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, under **Unmanaged Computers**, click **Active Directory**.
2. On the **Active Directory** page, click **Properties**.
3. On the Properties window, click **Add**.
4. In the Logon Settings window. in the **AD IP Address** box, type the IP address of the domain controller, and then in the **User Name** box, specify the user name. (Note that in some case you need to specify the domainname\username while entering the username field)
5. In the **Password** box, specify a password, in the **Confirm password** box, type the password again to confirm it, and then click **OK**.

Modify the Logon Settings of a Domain Controller

If you have already configured the logon settings, you can modify them by accessing the Properties window, selecting the name of the domain controller, and then by clicking **Modify**.

The steps to modify the logon settings for a domain controller are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, under **Unmanaged Computers**, click **Active Directory**.
2. On the **Active Directory** page, click **Properties**.
3. On the Properties window, select the check box next to the IP address of the domain controller whose settings you want to modify, and then click **Modify**.
4. In the Logon Settings window, in the **AD IP Address** box, select the existing IP address and then type the IP address of the domain controller, and then in the **User Name** box, select the existing name and then specify the user name.

5. In the **Password** box, remove the existing password, if any, and then specify the new password, in the **Confirm password** box, remove the existing password, if any, and then type the password again to confirm it. Then click **OK**.

Delete the Logon Settings of a Domain Controller

After you have configured the logon settings, you can delete it at any point of time.

The steps to delete the logon settings for a domain controller are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, under **Unmanaged Computers**, click **Active Directory**.
2. On the **Active Directory** page, click **Properties**.
3. On the Properties window, select the check box next to the IP address of the domain controller whose settings you want to delete, and then click **Delete**. Then click **OK**.

Chapter 12: 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.

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 computers.

- 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.

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

1. In the **Web Console Timeout Setting** area, select the **Enable timeout setting** check box.
2. 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.
3. Select number of minutes from the **Automatically log out the web console after** X **minutes** box, that is, X means total number of minutes.
4. In the **DashBoard Setting** area, type number of days in the **Show Status for Last** X **days (1-365)** field, that is, X means total number of days.
5. In the **Sql Server Connection Setting** area, specify the following field details.

Field	Description
Server instance	Type server path or click the **Browse** button to select path from the list, and then click the **Ok** button
Host Name/ IP Address	Type host name or IP address of the server
Login name	Type the login name
Password	Type the password

Note: The test is successfully connected only if you specify all field details correctly, else you get message of error in connection. If you forgot the Root password or SQL server password gets changed you can change that password using **chanpass.exe** located in eScan folder. VERY IMP: Do not change SQL Password unless it is changed by the administrator of SQL. Else you will not be able to login to the eScan Web Console.

6. Click the **Test Connection** button.
   A message of server successfully connected appears.
7. 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 either from eScan update servers or from the local network by using FTP or HTTP.

You can access the **Update settings** page from the navigation 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 Server**.

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 administrator, 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 administrator, 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**, 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 e-mail address from a specified e-mail address. To use this feature, you must also specify the IP address of SMTP server and its port number.

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 **From** box, type the e-mail address of the sender, and in the **To** box, type the e-mail address of the receiver. You can add multiple email ids with comma separater.

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.

Scheduling

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

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

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

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

- **Automatic Download of Updates**

    1. 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 13: Managing User Accounts

You can use the eScan Web Console to add local users, Active Directory users, or groups.

Adding a Custom Account

Many a times, you need to add users belonging to the local network to the user list. While adding a user name, you need to specify the full name of the user, password, and e-mail address of the user.

The steps to add a custom account are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **User Accounts**.
2. On the **User Accounts** page, in the right pane, click **Add**.
3. To create a custom account, on the **Add User** page, select **Custom Account.**
4. In the **User Name** box, type the user name, and then in the **Full Name** box, type the full name.
5. In the **Password** box, type the password, and then in the **Confirm password** box, type the password again.
6. In the **Email address** box, type the e-mail address.
7. To save and add the account to the user list, click **Save**.

Adding an Active Directory User or Group

Apart from adding local users, you can also add Active Directory Users or groups to the user list.

The steps to add an Active Directory user or group are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **User Accounts**.
2. On the **User Accounts** page, in the right pane, click **Add**.
3. To create a custom account, on the **Add User** page, select **Active Directory User or group.**
4. In the **User name** box, type the user name, and then in the **Domain** box, type the name of the domain.

5. In the **AD IP Address** box, type the AD IP address of the domain.
6. In the **AD Admin User name** box, type the name of the AD Admin, and in the **AD Admin Password** box, type the password of the AD Admin.
7. To save and add the account to the user list, click **Save**.

Searching and Adding Active Directory Users

Sometimes, you may not know all the details about the user that you want to add to the user list. So, you may need to search for the user in the Active Directory by specifying certain search criteria.

The steps for searching and adding active directory users are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **User Accounts**.
2. On the **User Accounts** page, in the right pane, click **Add from Active Directory**.
3. To search for an active directory user, in the **User name** box, type the user name, and then in the **Domain** box, type the name of the domain.
4. In the **AD IP Address** box, type the AD IP address of the domain.
5. In the **AD Admin User name** box, type the name of the AD Admin, and in the **AD Admin Password** box, type the password of the AD Admin.
6. To search for the user, click **Search**.
7. To add a user to the user list of selected users, under **Search Results**, in the **Users** list, click the name of the user and then click **>**.
8. To remove a user from the **Selected Users** list, in the list, click the name of the user that you want to remove then click **<**.
9. To save the results and to add the user to the user list, click **Save**.

Deleting a User Account

Many a times, you need to delete users from the user list.

The steps to delete a user account are as follows:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **User Accounts**.
2. On the **User Accounts** page, in the right pane, select the user that you want to remove from the user list, and then click **Delete**.

Modifying User Details

You can also modify the details that you have added about a given user.

The steps to modify a user account are as follows:

For Local Users:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **User Accounts**.
2. On the **User Accounts** page, in the right pane, click the name of the user in the **User Name** column of the table.
3. In the **Full Name** box, type the full name.
4. In the **Password** box, type the password, and then in the **Confirm password** box, type the password again.
5. In the **Email address** box, type the e-mail address.
6. To enable the account, select the **Enable this account** check box. To disable the account, unselect the **Enable this account** check box.
7. To save and add the account to the user list, click **Save**.

For the root user:

1. In the eScan Web Console, in the left pane, under **Dashboard**, click **User Accounts**.
2. On the **User Accounts** page, in the right pane, click the name of the user in the **User Name** column of the table.
3. In the **Full Name** box, type the full name.
4. In the **Password** box, type the password, and then in the **Confirm password** box, type the password again.
5. In the **Email address** box, type the e-mail address.
6. To enable the account, select the **Enable this account** check box. To disable the account, unselect the **Enable this account** check box.
7. To save and add the account to the user list, click **Save**.

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.
		Connect to Client	To connect the client system remotely using RDP protocol.
- Policy	Properties		To view 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 Unmanaged 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 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.
- 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
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.

Glossary

A

Activation Code
A string of alphanumeric digits required to activate the license key.

AUTORUN.exe
An executable file intended to run with the AutoRun feature of the Windows® operating system.

B

Backup
A copy of objects created by eScan before it disinfects or removes them during scanning.

C

Command-line Parameters
A switch or an argument specified after the name of the executable file while running an executable file from the command prompt.

Computer Group
A group of computers are grouped together for ease of management. The group can have subgroups within it and can have policies applied to it.

D

Dynamic Host Configuration Protocol (DHCP)
A protocol used to assign IP addresses to the computers in a network.

E

End-user License Agreement (EULA)
A license agreement that specifies the legal ways in which a user can use the software.

eScan Client
A client computer that has only the eScan client components installed on it.

eScan Server
A server that has eScan Server components installed on it. Administrators can use the eScan Web Console to access the eScan server and perform management tasks.

eScan Web Console
A Web-based management console that allows administrators to perform the management of eScan servers and client computers on a network.

F

FaxRegister.TXT
A text file that contains the contact details, machine code, standard key, date, and version of eScan installed on the computer.

Firewall
A software that controls access to computers by monitoring incoming and outgoing network traffic.

File Transfer Protocol (FTP)
A protocol that is used to transfer files over the Internet.

G

Group Task
A task that is defined and applied to a computer group.

I

Internet Protocol (IP)
A networking protocol that is used to provide connectionless services to the transport protocol.

L

IP Address
A 32-bit address unique address that is assigned to computers that use the TCP/IP protocol suite.

License Key
An alphanumeric string required to run a software program.

P

Policy
Same as Rule-set

Protocol
A set of formal for exchanging information between two communication devices.

Protection Status
A status that defines the level upto which the computer is protected.

R

Remote Installation
A method of installing a software on a remote computer.

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

S

Spam
A junk or unsolicited e-mail.

Spyware
A malicious program that extracts information a computer without informing the user.

T

Task
A set of actions defined by the administrator to be performed on either a computer or a computer group.

U

Update

A mechanism for ensuring that the eScan is up-to-date with the latest files and virus definitions.

User Access Control (UAC)
A security feature of Windows® Vista and later operating systems.

V

Virus
A malicious program or piece of code that infects and performs malicious operations on a computer.

Virus Signature
A hash string that uniquely identifies a given virus.

W

Worm
A program that performs malicious action and propagates over a computer network by replication.

Index

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 2020/2021 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