eScan™

Enterprise Security

#1 Choice of DIGITAL WORLD

INTERNET SECURITY SUITE for BUSINESS

User Guide

www.escanav.com

sales@escanav.com

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/05.02.2017/14.1
Current Software Version: 14.1
Copyright Notice: Copyright © 2017. All rights reserved.
Any technical documentation that is made available by MicroWorld is the copyrighted work of MicroWorld and is owned by MicroWorld.

NO WARRANTY: The technical documentation is being delivered to you AS-IS and MicroWorld makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user.
Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make changes without prior notice.
No part of this publication may be copied without the express written permission of MicroWorld.
Trademarks: The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, MailScan are trademarks of MicroWorld.

Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All product names referenced herein are trademarks or registered trademarks of their respective companies. MicroWorld disclaims proprietary interest in the marks and names of others. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. MicroWorld reserves the right to modify specifications cited in this document without prior notice.
No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical Support:	**support@escanav.com**
Sales:	**sales@escanav.com**
Forums:	http://forums.escanav.com
eScan Wiki:	http://www.escanav.com/wiki
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld
Date:	February, 2017

Table of Contents

Introduction - eScan Management Console

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

Using this console you can perform following activities –

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

Pre-requisites for eScan Server

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

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

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

System Requirements

Platforms supported for Server and clients
Microsoft® Windows® 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-Bit & 64-Bit Editions)
Hardware for Clients and Server (Server)
CPU - 2GHz Intel™ Core™ Duo processor or equivalent. Memory - 4 GB & above Disk Space – 8 GB & above
Hardware for Endpoints
1.4 Ghz minimum (2.0 Ghz recommended) Intel Pentium or equivalent 1.0 GB minimum (1.5GB recommended) Disk Space – 800 MB and more
eScan Console can be accessed by using below browsers
Internet Explorer 7 / 8 / 9 / 10 Firefox 14 & above Google Chrome latest version

Installing eScan ISS for Business Server

- **Installing eScan from CD/DVD**

  Installing eScan ISS for Business from the CD/DVD is very simple, just insert the CD/DVD in the ROM and wait for few seconds for auto run to start the installation process and follow the instructions on screen. In case if installation does not start on its own then locate and double click on the WMCiwn4ksmk.exe on CD Rom, this will open the wizard based setup of eScan ISS for Business Edition on your computer. To complete the installation follow the instructions on screen.

- **Downloading and installing eScan ISS Business Edition from internet**

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

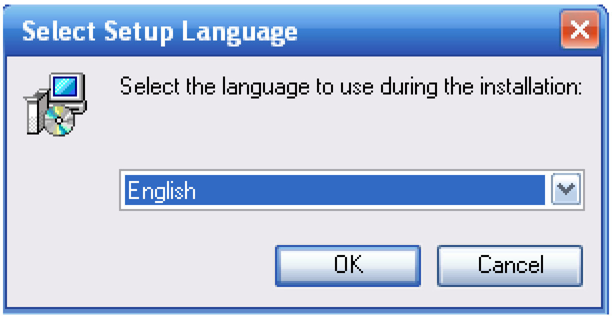
  For installing eScan ISS Business Edition from the setup file downloaded from Internet, just double click on the iwn4ksmk.exe and follow the instructions on screen to complete the installation process.

- **Installation Process**

The installation process comprises of following steps –

- **Step 1 - Selecting Language**

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



Select Setup Language

Select the language to use during the installation:

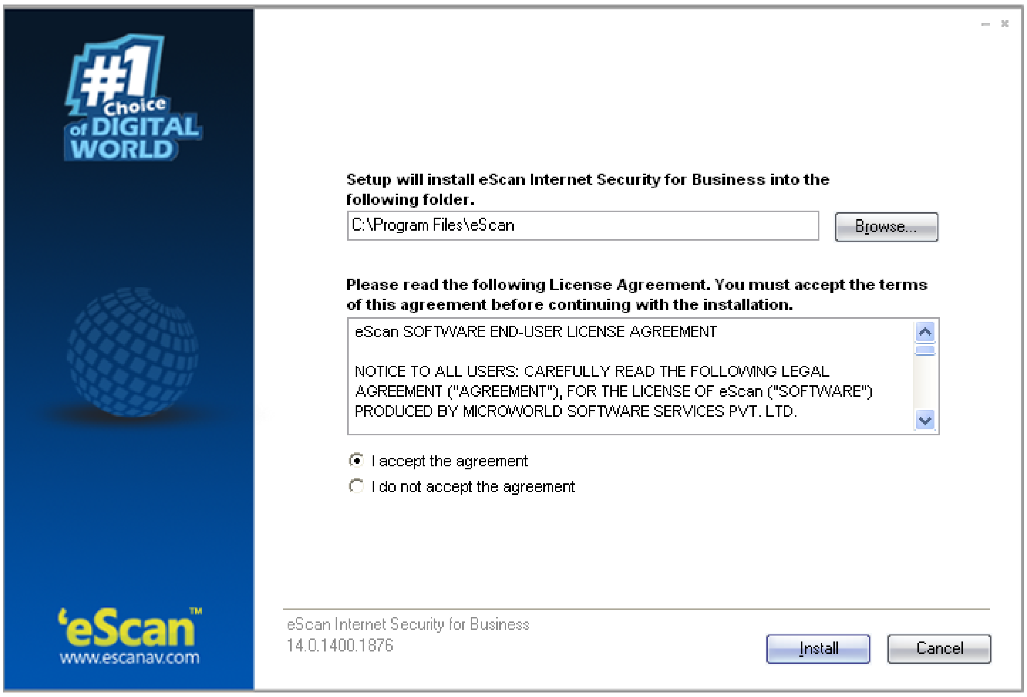
English

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

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

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

To proceed with the installation click **Next**, this will forward you to the License Agreement Screen; Select "I accept the agreement" option and click **Install**.



Setup will install eScan Internet Security for Business into the following folder.

C:\Program Files\eScan

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

eScan SOFTWARE END-USER LICENSE AGREEMENT

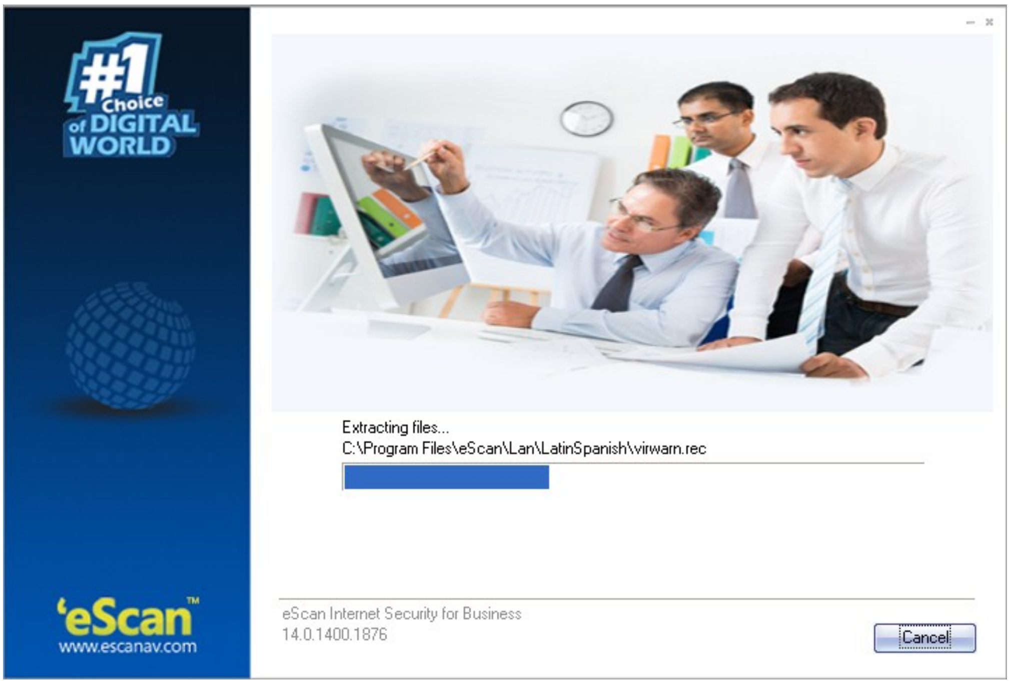
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF eScan ("SOFTWARE") PRODUCED BY MICROWORLD SOFTWARE SERVICES PVT. LTD.

● I accept the agreement
○ I do not accept the agreement

eScan Internet Security for Business
14.0.1400.1876

- **Step 5 – Installation Progress**

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

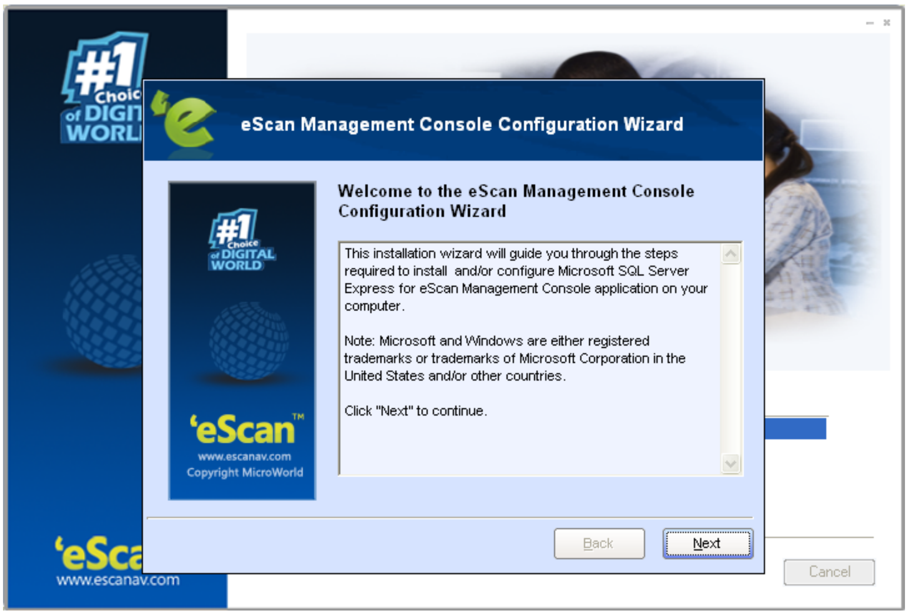


Extracting files...
C:\Program Files\eScan\Lan\LatinSpanish\virwarn.rec

eScan Internet Security for Business
14.0.1400.1876

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

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



Welcome to the eScan Management Console Configuration Wizard

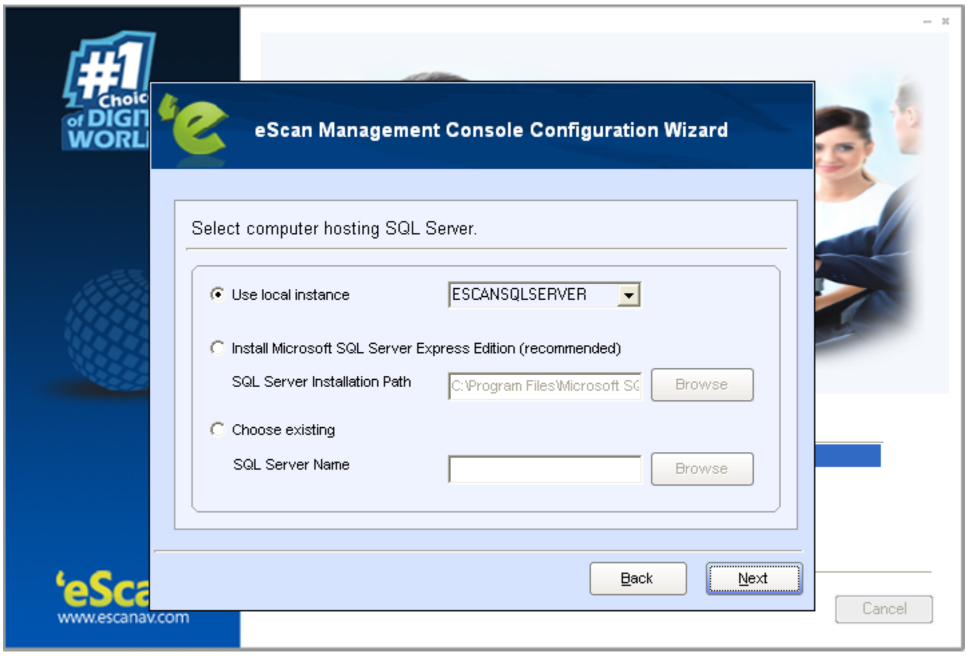
This installation wizard will guide you through the steps required to install and/or configure Microsoft SQL Server Express for eScan Management Console application on your computer.

Note: Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Click "Next" to continue.

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

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



Select computer hosting SQL Server.

● Use local instance ESCANSQLSERVER

○ Install Microsoft SQL Server Express Edition (recommended)

SQL Server Installation Path C:\Program Files\Microsoft SC

○ Choose existing

SQL Server Name

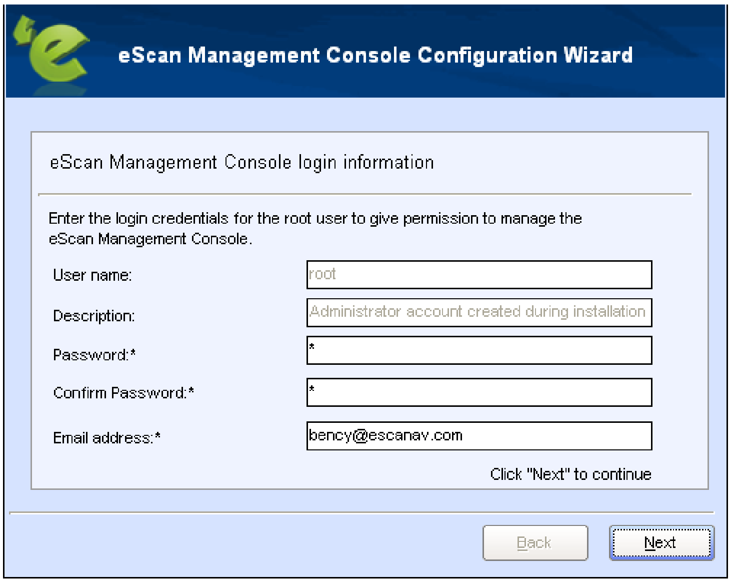
Options	Description
Use Local Instance	**[Radio button]** Use the drop down to select the desired instance for Hosting the SQL Server. It displays a list of instances present on the system. This option is being used if you already have SQL Instance running locally.
Install Microsoft SQL Server Express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

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

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

Step 9 - Filling Login Credentials for eScan Management Console

Fill up the required Login credentials that will be required to Login to the eScan Management Console, click **Next** when done.



eScan Management Console Configuration Wizard

eScan Management Console login information

Enter the login credentials for the root user to give permission to manage the eScan Management Console.

User name: root

Description: Administrator account created during installation

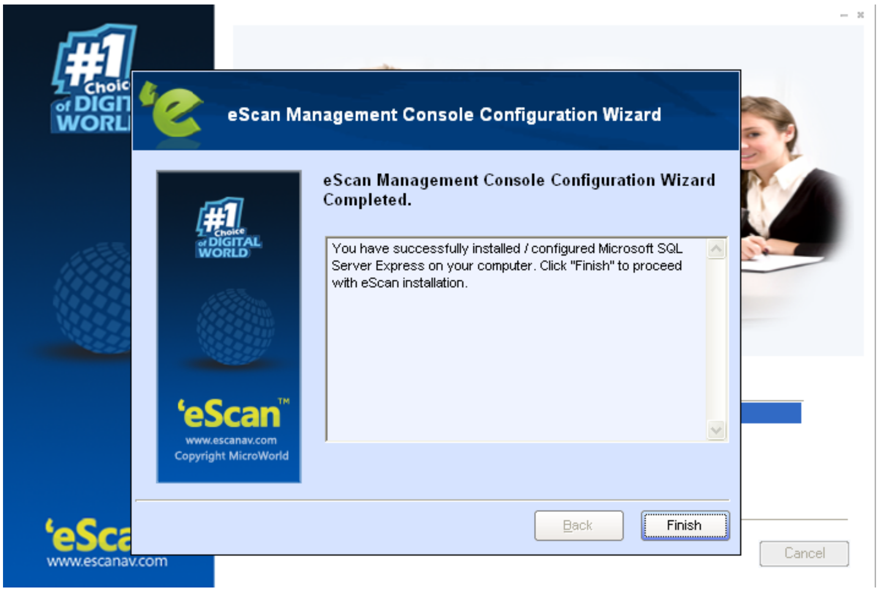
Password:* *

Confirm Password:* *

Email address:* bency@escanav.com

Click "Next" to continue

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

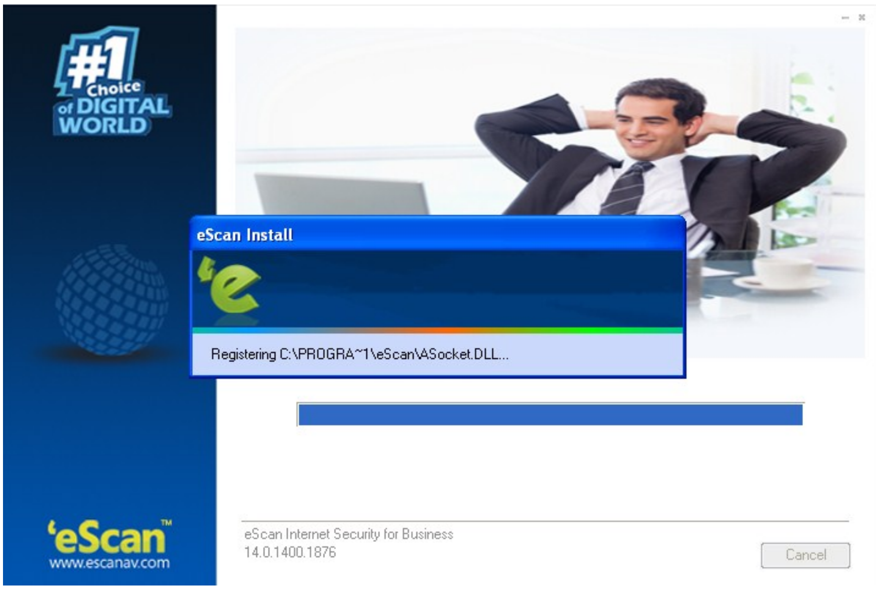


eScan Management Console Configuration Wizard Completed.

You have successfully installed / configured Microsoft SQL Server Express on your computer. Click "Finish" to proceed with eScan installation.

For completing the configuration of eScan Management Console, click **Finish**.

- **Step 11 – Installation process**

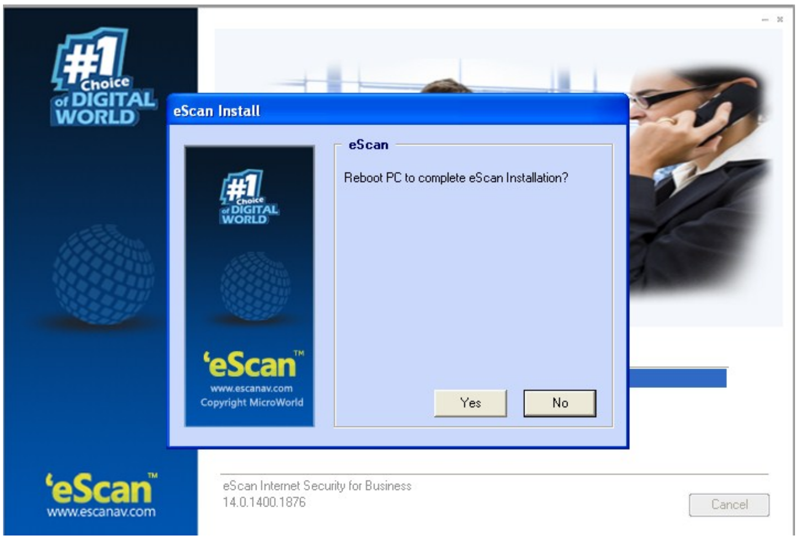


Registering C:\PROGRA~1\eScan\ASocket.DLL...

eScan Internet Security for Business
14.0.1400.1876

It will take a few minutes to complete the installation process.

- **Step 12 – Reboot**



eScan Install

eScan

Reboot PC to complete eScan Installation?

To complete the installation you will have to restart the computer. Click **Yes** to restart the computer.

Components of eScan Server

The eScan Server comprises the following components.

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

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

- **eScan Management Console** - It is a web-based application hosted on the eScan server. It allows administrators to manage eScan on endpoints in the network.

- **Microsoft SQL Server Express Edition**- Database for storing events and logs already included in the eScan Setup file.

Note:
On Windows 8 / 8.1 / 2008 /2012 operating systems, SQL 2008 Express edition should be installed else SQL 2005 Express edition will be installed.)

- **Apache -** For running eScan Management Console. (Already included in the eScan Setup file)

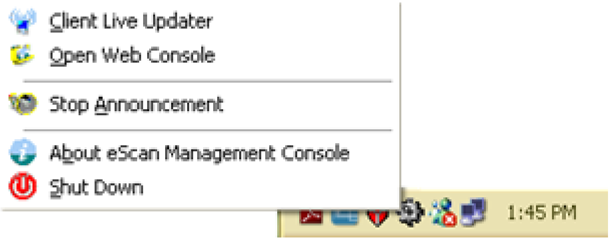
Note:
Uninstallation of eScan server will not remove SQL and APACHE software from the system

User Interface of eScan Management Console

- **Taskbar Menu –**

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

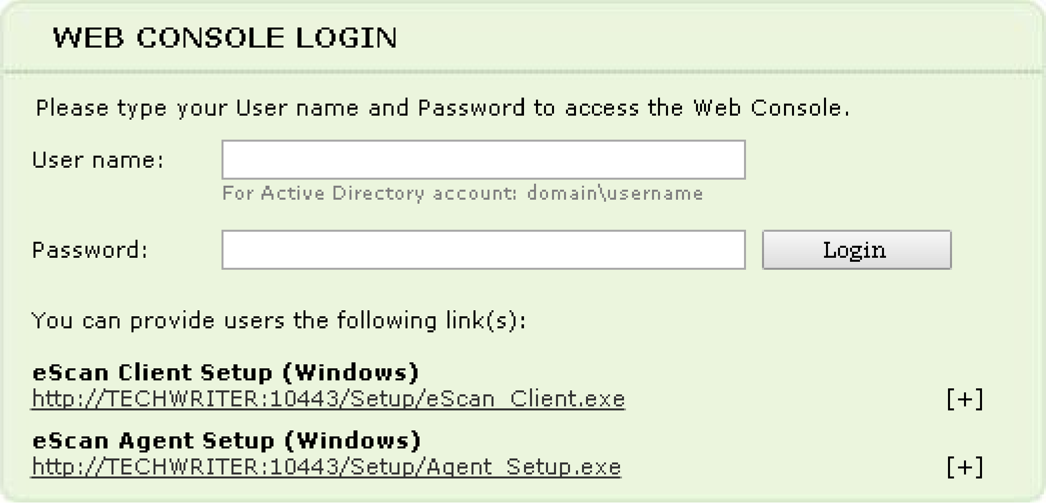
- **Options on Right Click (eScan Management Console Icon in taskbar)**



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

- **The Login Page**

Enter the Username and Password defined by you during installation of eScan ISS for Business to login to the **eScan Management Console**.


WEB CONSOLE LOGIN

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

User name:

For Active Directory account: domain\username

Password:

You can provide users the following link(s):

eScan Client Setup (Windows)
http://TECHWRITER:10443/Setup/eScan_Client.exe [+]

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

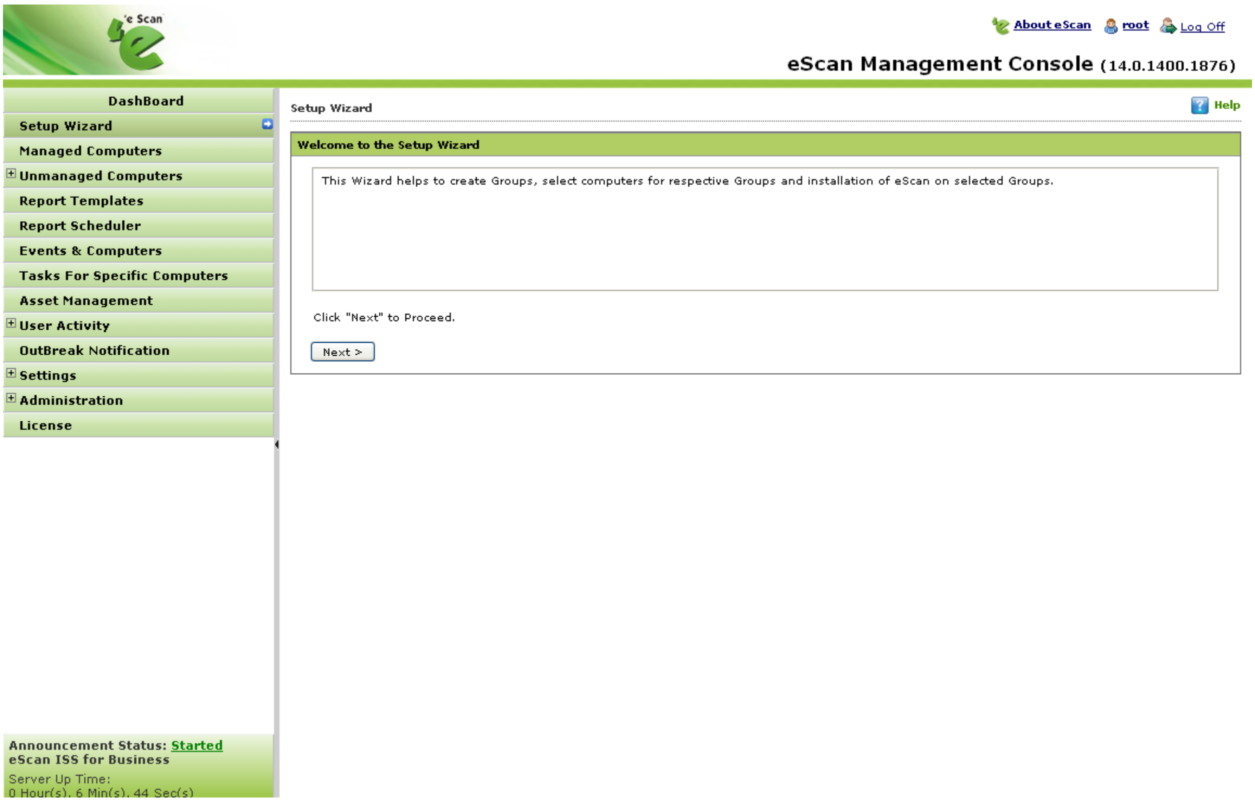
Copyright © 2015 MicroWorld Technologies Inc. All rights reserved.

Note:

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

Options	Description
Username	**[Field]** Enter the username to login to eScan Management Console.
Password	**[Field]** Enter the Password to login to eScan Management Console.
Login	**[Button]** Enter the Username and Password and click **Login** to enter the eScan Management Console.
eScan Client Setup Links	**[Download Links]** Client setup links is present on the Web Console Login page; you can send these links on mail to the users where remote installation is not possible. Using this link they can download the client setup and install it manually on their computers or they can directly access eScan Management console from their desktop.
eScan Agent Setup Link	**[Download Links]** You can give this link on mail to the user where you are not able to get system information or communication is breaking frequently. Once the Agent is downloaded and installed on the Managed Computer. It will establish the connection between Server and Client computer.

- **Main Interface - eScan Management Console**



About eScan root Log Off

eScan Management Console (14.0.1400.1876)

Setup Wizard

Help

Welcome to the Setup Wizard

This Wizard helps to create Groups, select computers for respective Groups and installation of eScan on selected Groups.

Click "Next" to Proceed.

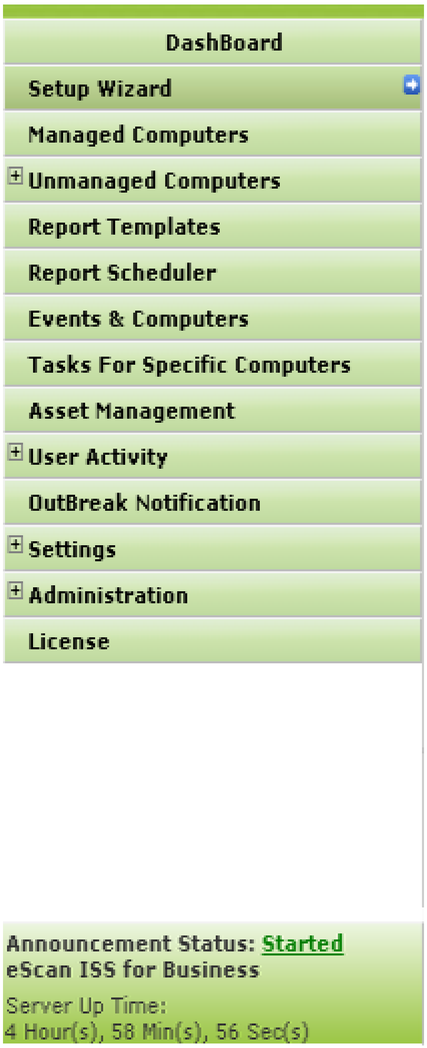
Next >

Announcement Status: Started
eScan ISS for Business
Server Up Time:
0 Hour(s), 6 Min(s), 44 Sec(s)

Links	Description
About eScan About eScan	**[Link]** Click this link to visit our Home page – **www.escanav.com**
root (Username) root	**[Link]** Click this link to edit User Login details like Full name, Password and email address that you use to Login to the eScan Management Console.
Log off Log Off	**[Link]** Click this link to Log out of the eScan Management Console.
Navigation Panel	It displays all modules of eScan Management Console providing access to numerous functionalities present under them.
Announcement Status	It displays the status of broadcasts done by ISS for Business as **Started** or **Stopped**

- **eScan Management Console - Navigation Panel**

Navigation Panel is present on the left side after you login to eScan Management console and gives you direct access to various modules present in the console for managing security on endpoints connected to the network. It will allow you to install, update and configure eScan client on all the endpoints on the network. Using this panel you can also configure settings for the Web console and manage user roles and permissions for Management Console. Using this console you can easily ensure complete security of endpoints from malware infections and viruses. It also helps you in configuring notification mails to warn or alert in case of occurrence of a virus outbreak.

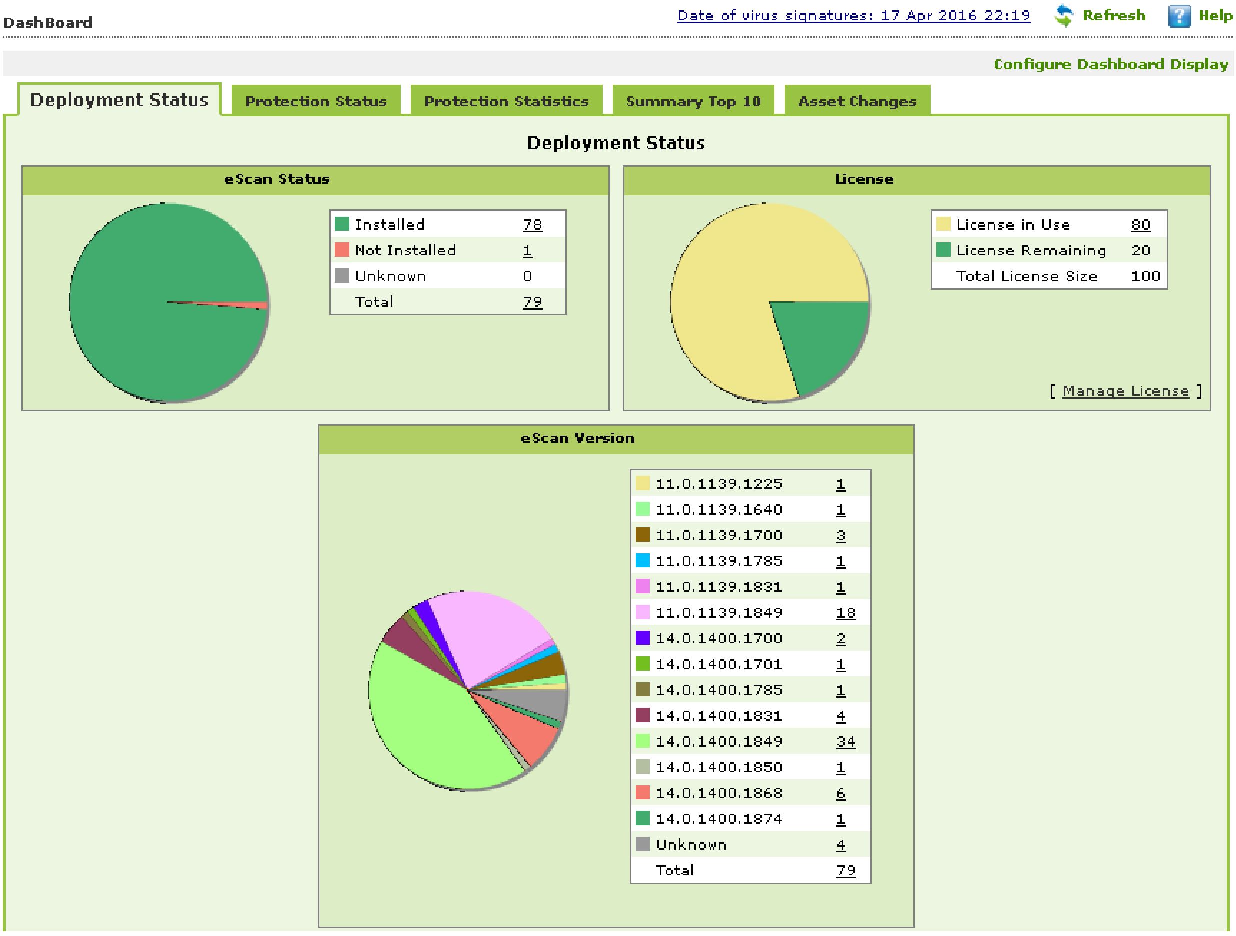


Announcement Status: Started
eScan ISS for Business
Server Up Time:
4 Hour(s), 58 Min(s), 56 Sec(s)

Overview of the Navigation Panel

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

- **Dashboard** - The dashboard of eScan Management Console displays charts showing deployment status, Protection status, Protection Statistics, Top 10 Summary and Asset Changes on managed endpoints. For **more details click here**.



DashBoard

Date of virus signatures: 17 Apr 2016 22:19 Refresh Help

Configure Dashboard Display

Deployment Status

eScan Status

■ Installed	78
■ Not Installed	1
■ Unknown	0
Total	79

License

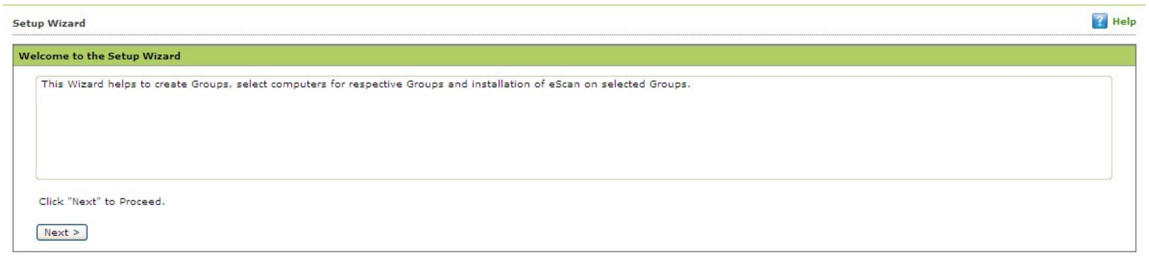
■ License in Use	80
■ License Remaining	20
Total License Size	100

[Manage License]

eScan Version

■ 11.0.1139.1225	1
■ 11.0.1139.1640	1
■ 11.0.1139.1700	3
■ 11.0.1139.1785	1
■ 11.0.1139.1831	1
■ 11.0.1139.1849	18
■ 14.0.1400.1700	2
■ 14.0.1400.1701	1
■ 14.0.1400.1785	1
■ 14.0.1400.1831	4
■ 14.0.1400.1849	34
■ 14.0.1400.1850	1
■ 14.0.1400.1868	6
■ 14.0.1400.1874	1
■ Unknown	4
Total	79

- **Setup Wizard –** It guides you in step by step creation of groups, adding computers to respective groups, adding hosts from the network and installing client on the connected computer at a desired path/ location on that computer.



Setup Wizard

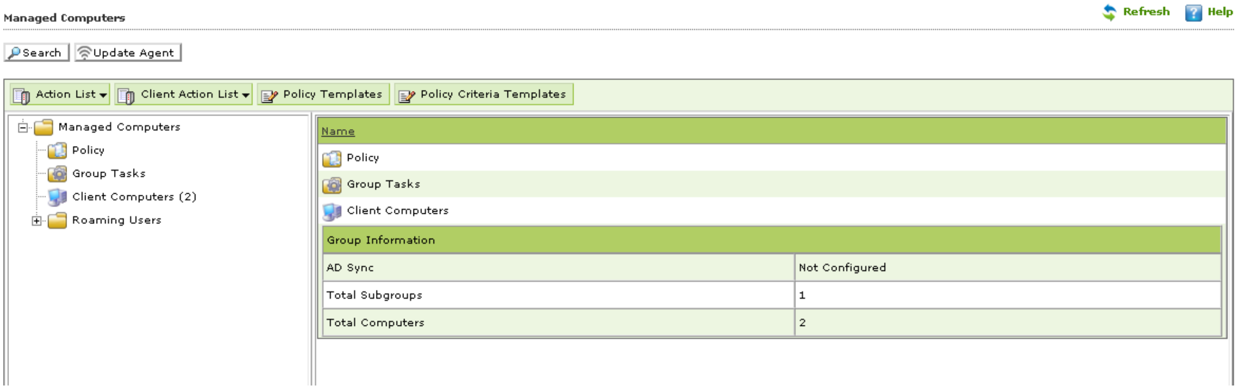
Help

Welcome to the Setup Wizard

This Wizard helps to create Groups, select computers for respective Groups and installation of eScan on selected Groups.

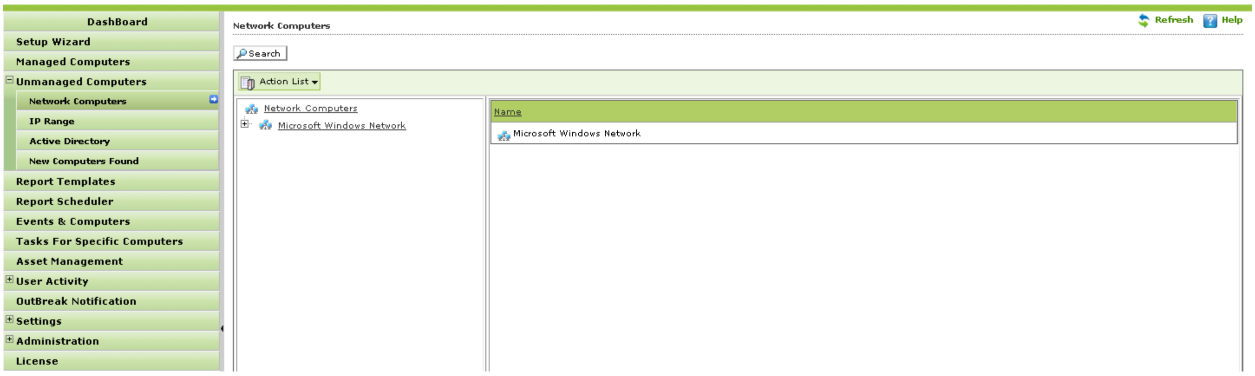
Click "Next" to Proceed.

- **Managed Computers –** It consists of a managed group tree structure on the left and a task pane on right. Using this section you can deploy eScan, Create Policy template and Criteria for endpoints. Additionally, it provides various options for creating groups, adding tasks, deploying or uninstalling client application, moving computers from one group to the other and redefining properties of the endpoints from normal to roaming users and vice versa. For **more details click here**.



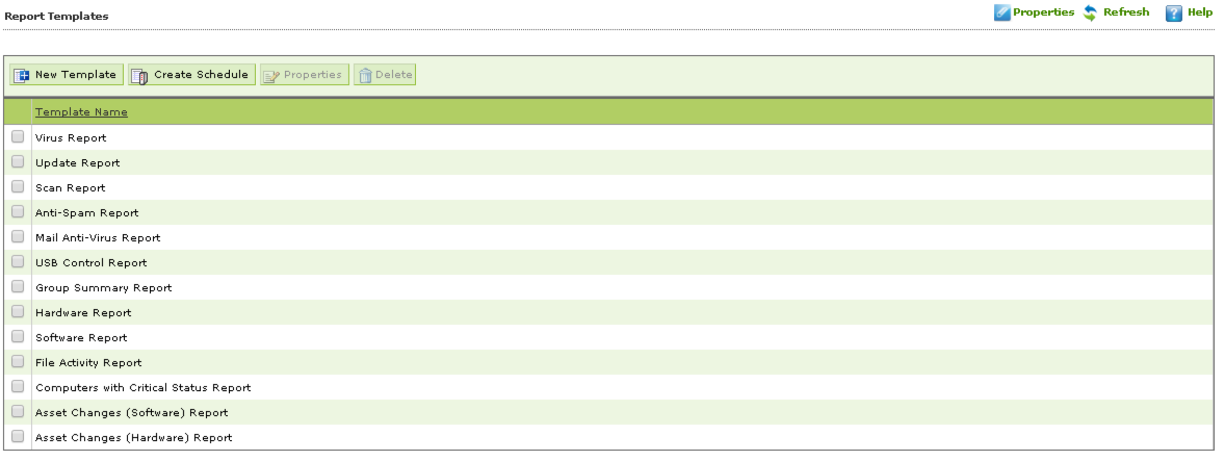
Group Information	
AD Sync	Not Configured
Total Subgroups	1
Total Computers	2

- **Unmanaged Computers –** This module displays information about the computers that have not yet been assigned to any group. It allows you to set the host configuration, move computers to a desired group for eScan deployment and management, view the properties of a computer, or refresh the information about a client computer by using the **Action List** menu. This module is subdivided into **Network Computers, IP Range, Active Directory** and **New Computers Found.**



Sub Module	Description
Network Computers	It displays the eScan Internet for Business endpoints and workgroups in the network in a console tree. You can click on the name of a computer or group to view its details
IP Range	It displays the IP range for the network as nodes in a console tree and also allows you to add or delete an IP range by clicking New IP Range and Delete IP range respectively.
Active Directory	The Active Directory page shows a console tree list of all the domain controllers in the network. It allows you to add computers from Active Directory.
New Computers Found	It displays the list of endpoints where eScan is not installed. You can select and move computers to desired groups for eScan Deployment and security management or set host configuration of selected endpoint.

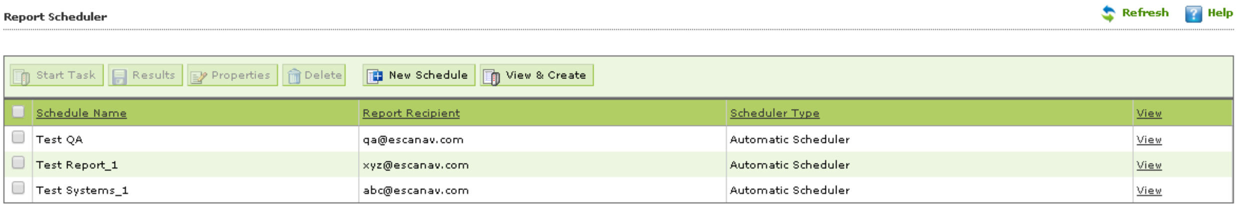
- **Report Templates –** This module allows you to create new report templates and create a schedule for the templates. It also provides options for configuring or scheduling reports, viewing report properties, and refreshing or deleting Admin created reports. For **more details click here**.



Report Templates

	Template Name
□	Virus Report
□	Update Report
□	Scan Report
□	Anti-Spam Report
□	Mail Anti-Virus Report
□	USB Control Report
□	Group Summary Report
□	Hardware Report
□	Software Report
□	File Activity Report
□	Computers with Critical Status Report
□	Asset Changes (Software) Report
□	Asset Changes (Hardware) Report

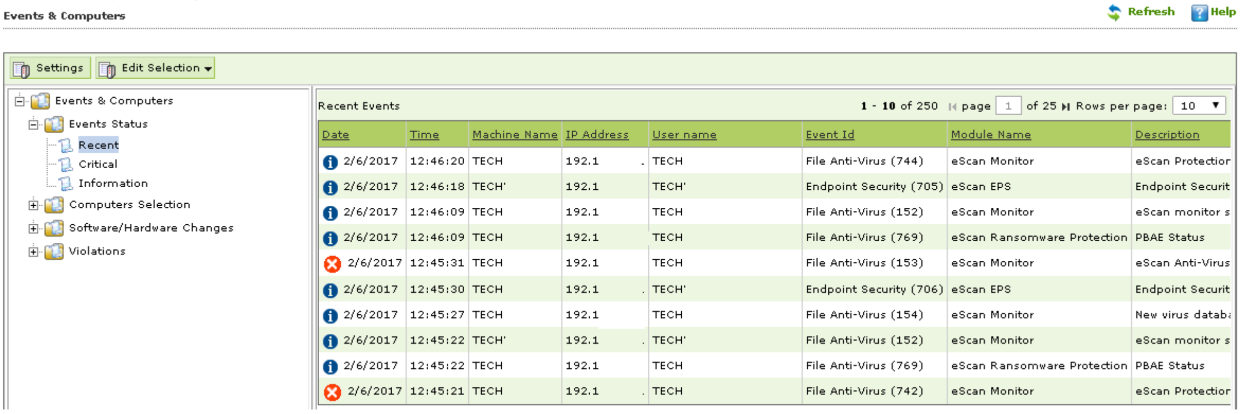
- **Report Scheduler -** The **Report Scheduler** page allows you to schedule a new reporting task, run an already created reporting schedule or view its properties. It also allows you to view results of an already executed report schedule. For **more details click here**.



Report Scheduler

□	Schedule Name	Report Recipient	Scheduler Type	View
□	Test QA	qa@escanav.com	Automatic Scheduler	View
□	Test Report_1	xyz@escanav.com	Automatic Scheduler	View
□	Test Systems_1	abc@escanav.com	Automatic Scheduler	View

- **Events and Computers -** The Events & Computers page enables you to monitor various activities performed on managed endpoints. For convenience all events are categorized on the basis of Event Status, Computer Selection or Software/Hardware changes on all managed endpoints. Using the Settings option in this module, you can define settings for event capturing as desired. **For more details click here.**

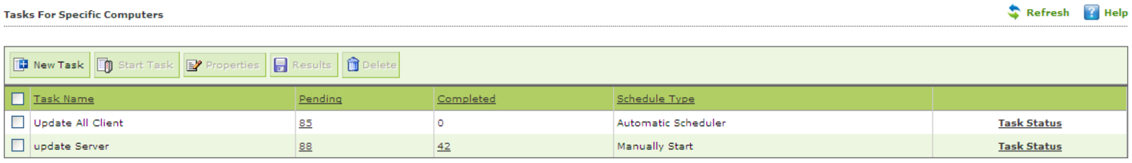


Events & Computers

Recent Events   1 - 10 of 250 page 1 of 25 Rows per page: 10

	Date	Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
ⓘ	2/6/2017	12:46:20	TECH	192.1 .	TECH	File Anti-Virus (744)	eScan Monitor	eScan Protectior
ⓘ	2/6/2017	12:46:18	TECH'	192.1	TECH'	Endpoint Security (705)	eScan EPS	Endpoint Securit
ⓘ	2/6/2017	12:46:09	TECH	192.1	TECH	File Anti-Virus (152)	eScan Monitor	eScan monitor s
ⓘ	2/6/2017	12:46:09	TECH	192.1	TECH	File Anti-Virus (769)	eScan Ransomware Protection	PBAE Status
✖	2/6/2017	12:45:31	TECH	192.1	TECH	File Anti-Virus (153)	eScan Monitor	eScan Anti-Virus
ⓘ	2/6/2017	12:45:30	TECH	192.1 .	TECH'	Endpoint Security (706)	eScan EPS	Endpoint Securit
ⓘ	2/6/2017	12:45:27	TECH	192.1	TECH	File Anti-Virus (154)	eScan Monitor	New virus datab:
ⓘ	2/6/2017	12:45:22	TECH'	192.1 .	TECH'	File Anti-Virus (152)	eScan Monitor	eScan monitor s
ⓘ	2/6/2017	12:45:22	TECH	192.1	TECH	File Anti-Virus (769)	eScan Ransomware Protection	PBAE Status
✖	2/6/2017	12:45:21	TECH	192.1 .	TECH	File Anti-Virus (742)	eScan Monitor	eScan Protectior

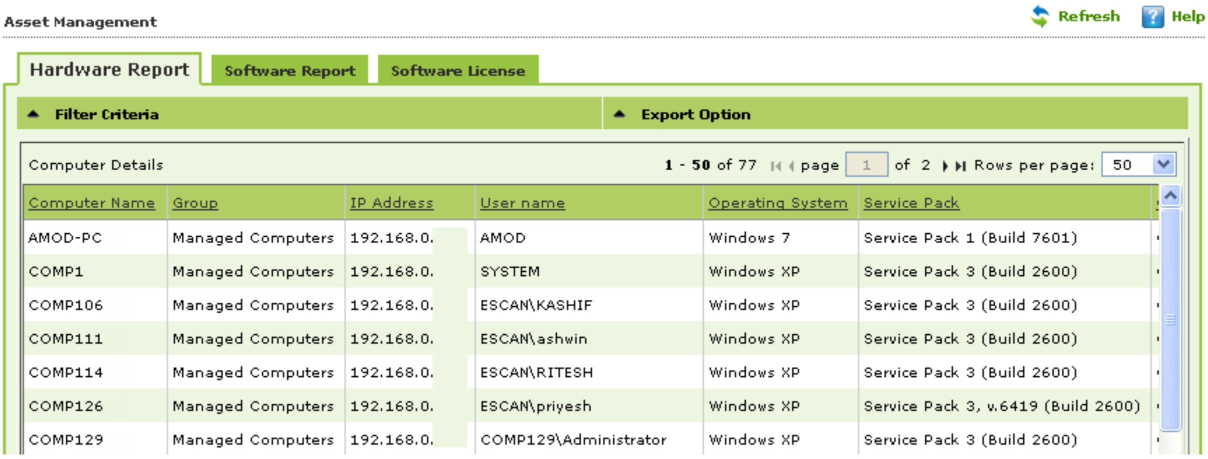
- **Tasks for Specific Computers** – This section will allow you to create and run tasks on specific endpoints, it also allows you to schedule or modify created tasks for selected endpoints or groups. You can easily re-define settings of already created tasks for desired endpoints. It also allows you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



Tasks For Specific Computers

□	Task Name	Pending	Completed	Schedule Type	
□	Update All Client	85	0	Automatic Scheduler	Task Status
□	update Server	88	42	Manually Start	Task Status

- **Asset Management -** This module provides you the entire Hardware configuration and list of software installed on endpoints in a tabular format. Using this module, you can easily filter the information as per you requirement search based on different criteria you can easily, it also displays licensing details of Microsoft product installed on managed endpoints. You can export the entire system information available through this module in PDF, Microsoft Excel or HTML formats.

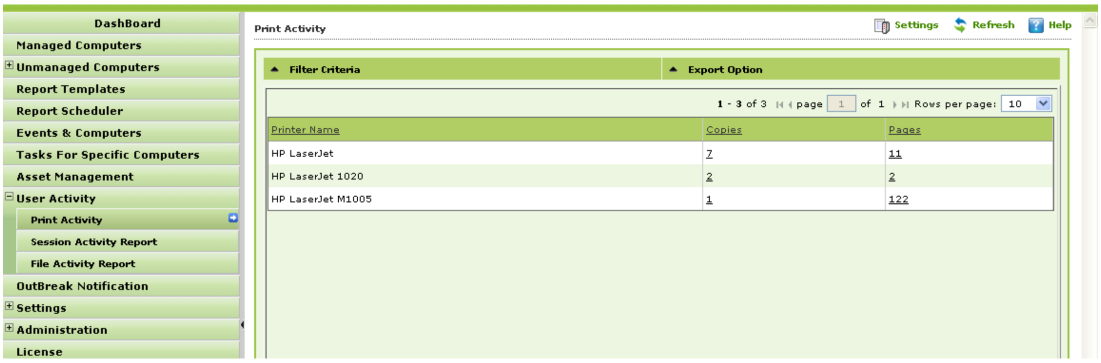


Asset Management

Computer Details 1 - 50 of 77 page 1 of 2 Rows per page: 50

Computer Name	Group	IP Address	User name	Operating System	Service Pack
AMOD-PC	Managed Computers	192.168.0.	AMOD	Windows 7	Service Pack 1 (Build 7601)
COMP1	Managed Computers	192.168.0.	SYSTEM	Windows XP	Service Pack 3 (Build 2600)
COMP106	Managed Computers	192.168.0.	ESCAN\KASHIF	Windows XP	Service Pack 3 (Build 2600)
COMP111	Managed Computers	192.168.0.	ESCAN\ashwin	Windows XP	Service Pack 3 (Build 2600)
COMP114	Managed Computers	192.168.0.	ESCAN\RITESH	Windows XP	Service Pack 3 (Build 2600)
COMP126	Managed Computers	192.168.0.	ESCAN\priyesh	Windows XP	Service Pack 3, v.6419 (Build 2600)
COMP129	Managed Computers	192.168.0.	COMP129\Administrator	Windows XP	Service Pack 3 (Build 2600)

- **User Activity –** This will monitor the user activity such as the print activity, remote session activity and file action reports of managed endpoints. It monitors and logs printing tasks done by all the endpoints, you can create report of all logged data in PDF, EXCEL or HTML formats.

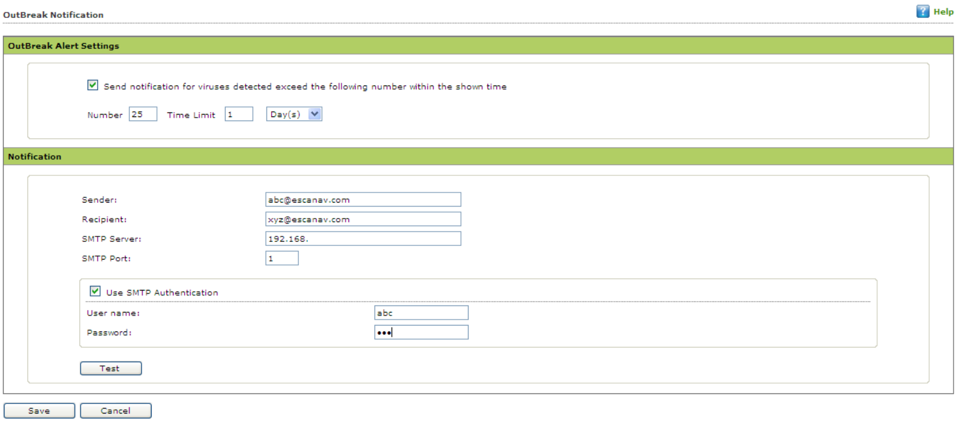


Print Activity

1 - 3 of 3 page 1 of 1 Rows per page: 10

Printer Name	Copies	Pages
HP LaserJet	7	11
HP LaserJet 1020	2	2
HP LaserJet M1005	1	122

- **Outbreak Notification:** In this module, you can configure settings for sending notification when virus count exceeds the limit defined by you.



OutBreak Notification

OutBreak Alert Settings

☑ Send notification for viruses detected exceed the following number within the shown time

Number 25 Time Limit 1 Day(s)

Notification

Sender: abc@escanav.com

Recipient: xyz@escanav.com

SMTP Server: 192.168.

SMTP Port: 1

☑ Use SMTP Authentication

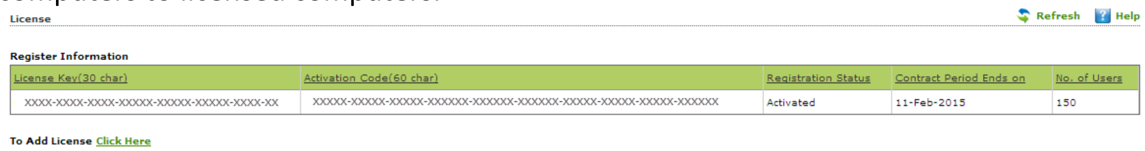
User name: abc

Password: •••

- **Settings –** In this module you can define important settings for FTP downloads, maintaining logs, eScan Management Console timeout settings, update download settings along with important settings for eScan as well as settings for autogrouping the endpoints connected to the network. For more information **Click Here**

- **Administration -** Using this module you can create User Accounts and allocate Admin rights for accessing and configuring security settings for managed endpoints through eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. For more information **Click Here**

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

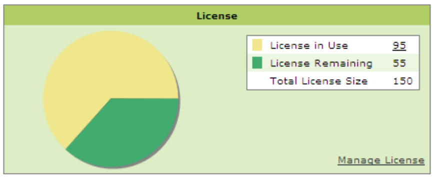


License

Register Information

License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users
XXXX-XXXX-XXXX-XXXXX-XXXXX-XXXXX-XXXX-XX	XXXXX-XXXXX-XXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXX-XXXXX-XXXXX-XXXXXX	Activated	11-Feb-2015	150

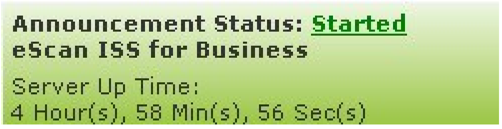
To Add License Click Here



License

🟨	License in Use	95
🟩	License Remaining	55
	Total License Size	150

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



Announcement Status: Started
eScan ISS for Business

Server Up Time:
4 Hour(s), 58 Min(s), 56 Sec(s)

eScan Management Console

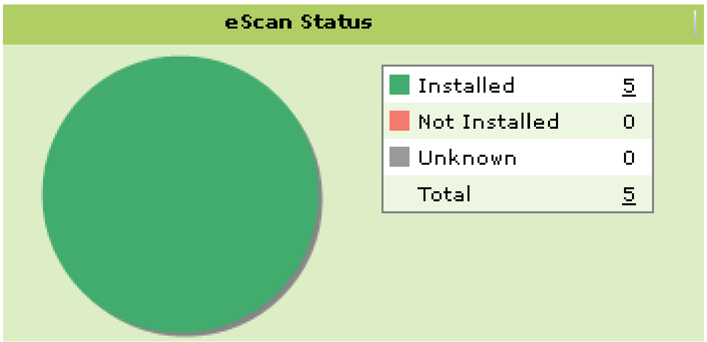
Dashboard and its Configuration

It displays the Installation, licensing as well as activity status of eScan client under it sub modules **Deployment Status**, **Protection Status**, **Protection Statistics, Summary Top 10 and Asset changes** on managed endpoints graphically in the form of pie charts.

- **Deployment Status**

  It displays the deployment status of eScan client on the managed endpoints. Displays charts showing status of eScan client installation, licenses and eScan versions installed on managed endpoints.

  - **eScan Status**

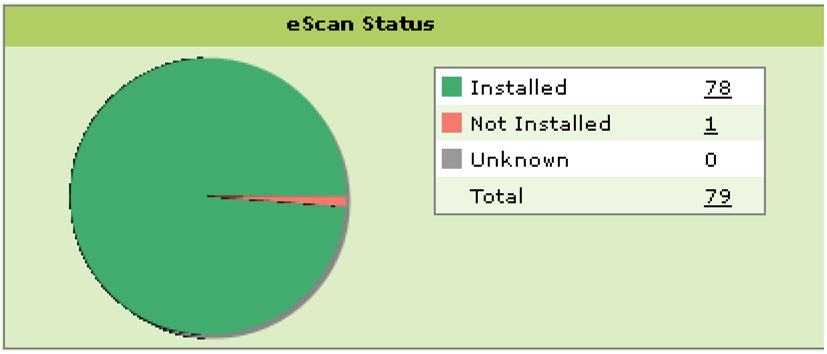


eScan Status

🟩	Installed	5
🟥	Not Installed	0
■	Unknown	0
	Total	5

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

- **License –**



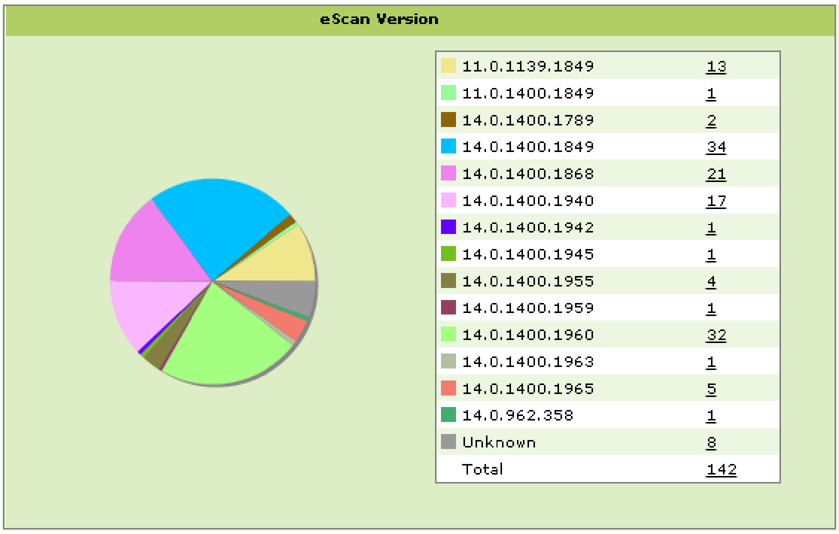
eScan Status

🟩	Installed	78
🟥	Not Installed	1
⬜	Unknown	0
	Total	79

  - **License in Use** - Total number of licenses that have been activated.
  - Total number of **Licenses remaining**.
  - **Total license size** i.e. – The total number of licenses purchased, it includes the number of licenses that are activated and not activated.

- **eScan Version -**

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



eScan Version

🟨	11.0.1139.1849	13
🟩	11.0.1400.1849	1
🟫	14.0.1400.1789	2
🟦	14.0.1400.1849	34
🟪	14.0.1400.1868	21
🟪	14.0.1400.1940	17
🟪	14.0.1400.1942	1
🟩	14.0.1400.1945	1
🟫	14.0.1400.1955	4
🟥	14.0.1400.1959	1
🟩	14.0.1400.1960	32
⬜	14.0.1400.1963	1
🟥	14.0.1400.1965	5
🟩	14.0.962.358	1
⬜	Unknown	8
	Total	142

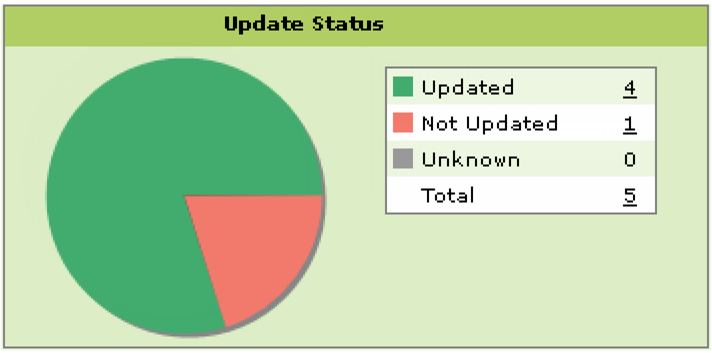
  - Also displays number of computers on which specific versions are installed.

Note:

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

- **Protection Status -** It displays the activity status of all the modules of eScan client along with update status of eScan on endpoints.

  - **Update Status** –

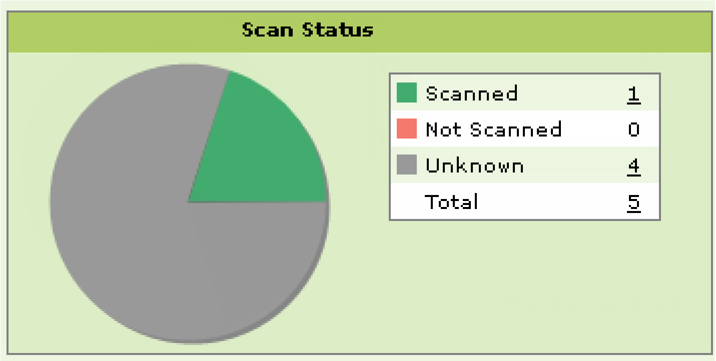


Update Status

🟩	Updated	4
🟥	Not Updated	1
▨	Unknown	0
	Total	5

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

- **Scan Status** –



Scan Status

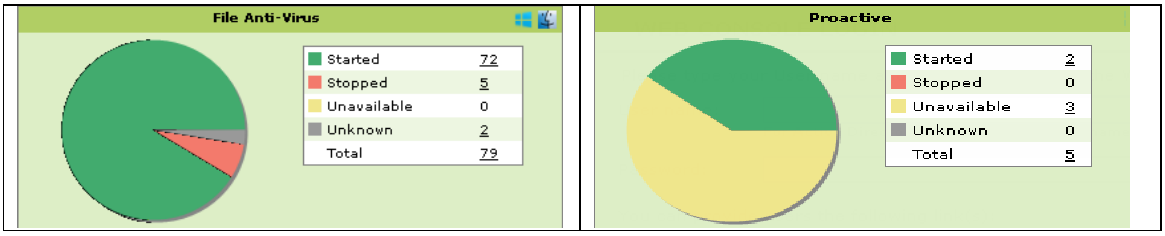
🟩	Scanned	1
🟥	Not Scanned	0
▨	Unknown	4
	Total	5

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

Pie chart of Module Activity Status includes / displays following details

- **Started** - Number of computers on which the module is in started state or turned on.
- **Stopped** - Number of computers on which the module is in stopped state or turned off.
- **Unavailable** – Number of computers where the module is not present.
- **Unknown** - Number of computers where the status is unknown.
- **Total** - Total number of managed computer where module is started, stopped, unavailable or the status is unknown.

For example



File Anti-Virus

🟩	Started	72
🟥	Stopped	5
🟨	Unavailable	0
⬛	Unknown	2
	Total	79

Proactive

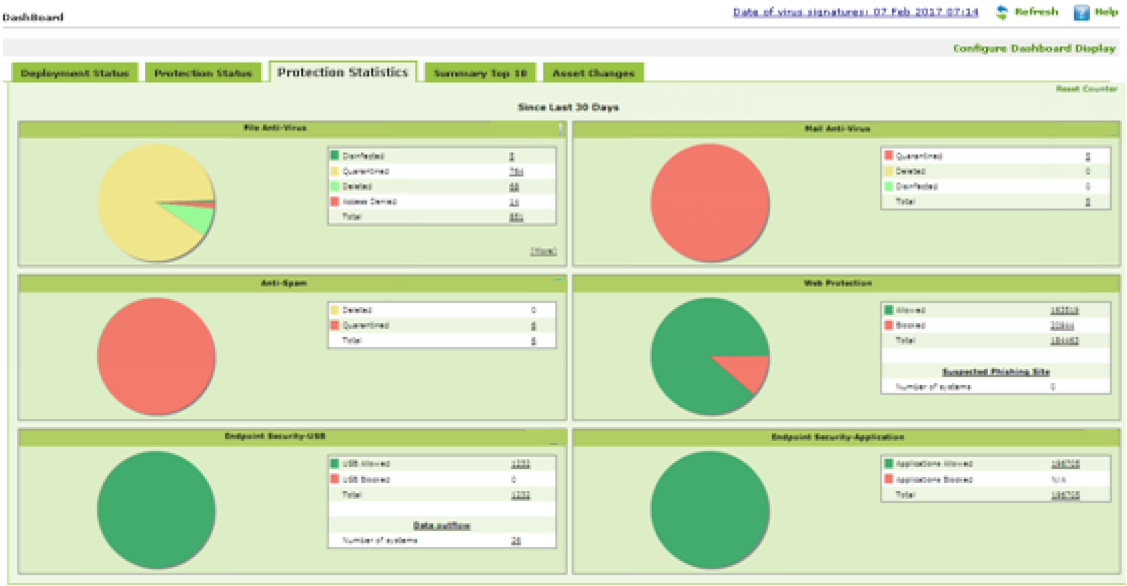
🟩	Started	2
🟥	Stopped	0
🟨	Unavailable	3
⬛	Unknown	0
	Total	5

You can configure the dashboard display and select the modules to view activity status under protection status in dashboard using configure dashboard display option present at the top right corner on the interface.

Configure Dashboard Display

- **Protection Statistics**

  This tab displays activity statistics of all modules of eScan client on all the endpoints in pie charts. It displays the actions taken by eScan modules on the endpoints as count. You can reset the protection statistics using the **Reset Counter** option present in the window.



Since Last 30 Days

File Anti-Virus

🟩	Disinfected	3
🟨	Quarantined	[illegible]
🟩	Deleted	48
🟥	Access Denied	11
	Total	[illegible]

Mail Anti-Virus

🟥	Quarantined	2
🟨	Deleted	0
🟩	Disinfected	0
	Total	2

Anti-Spam

🟨	Deleted	0
🟥	Quarantined	6
	Total	6

Web Protection

🟩	Allowed	[illegible]
🟥	Blocked	[illegible]
	Total	[illegible]
	Suspected Phishing Site	
	Number of systems	0

Endpoint Security-USB

🟩	USB Allowed	[illegible]
🟥	USB Blocked	0
	Total	[illegible]
	Data outflow	
	Number of systems	28

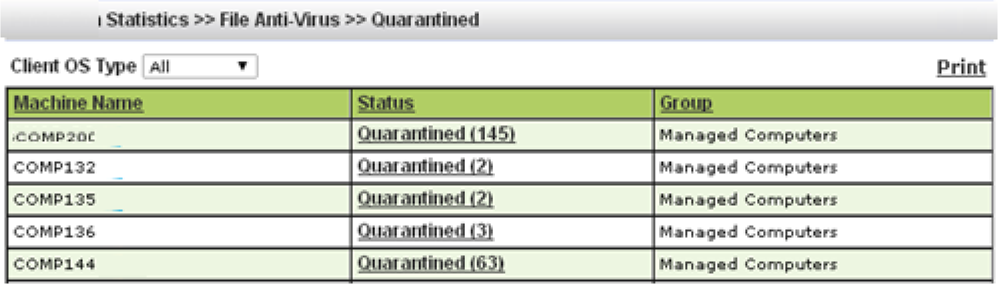
Endpoint Security-Application

🟩	Applications Allowed	[illegible]
🟥	Applications Blocked	N/A
	Total	[illegible]

Note:

- Reset counter option resets the protection statistics to 0, this option is useful when a group of endpoints is infected with a virus and **you have scanned and secured the computers. To monitor the group for** infection you can reset the counter to 0.

- Click on the count to view the details of the affected computer, action taken and group to which it belongs to.

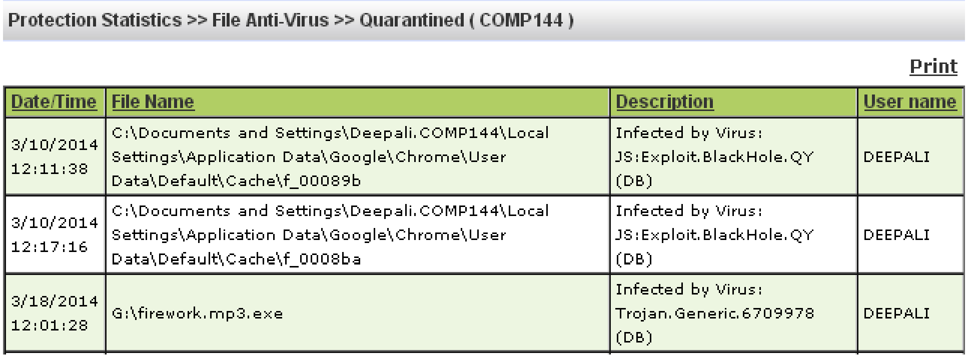


Statistics >> File Anti-Virus >> Quarantined

Client OS Type All ▾ **Print**

Machine Name	Status	Group
COMP20C	Quarantined (145)	Managed Computers
COMP132	Quarantined (2)	Managed Computers
COMP135	Quarantined (2)	Managed Computers
COMP136	Quarantined (3)	Managed Computers
COMP144	Quarantined (63)	Managed Computers

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

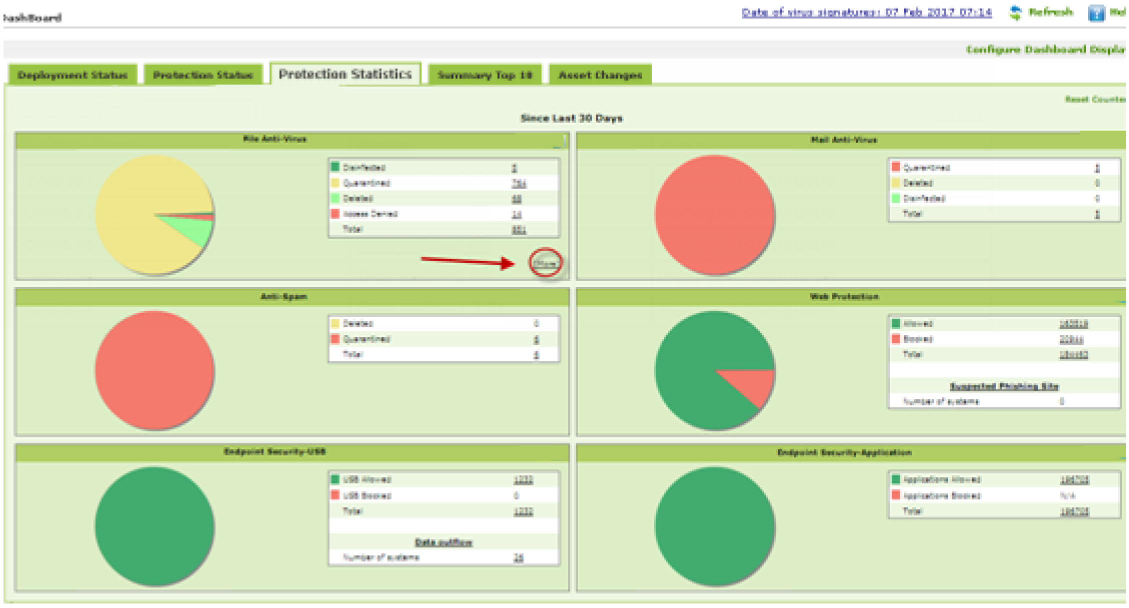


Protection Statistics >> File Anti-Virus >> Quarantined (COMP144)

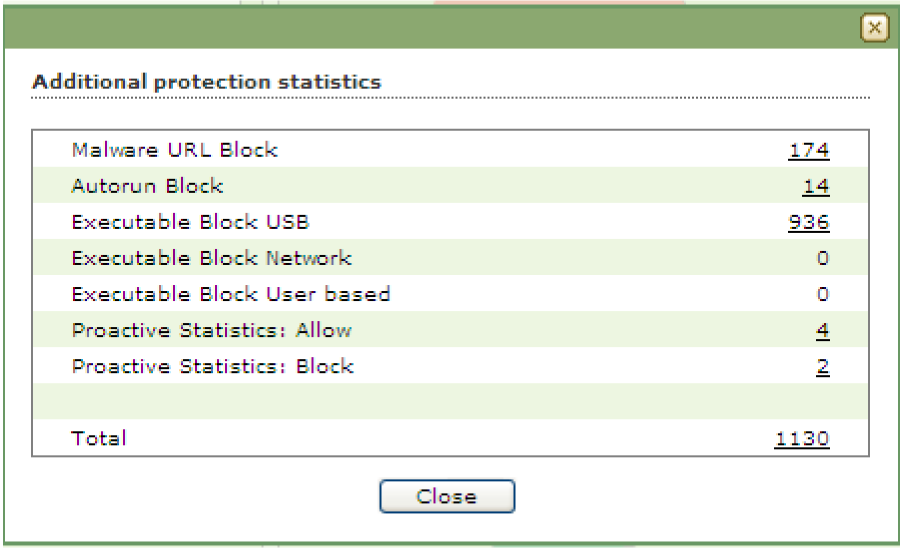
Print

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

- Additional protection statistics can be viewed using the [More] option present on the interface.



- It displays the statistics counter for the following –

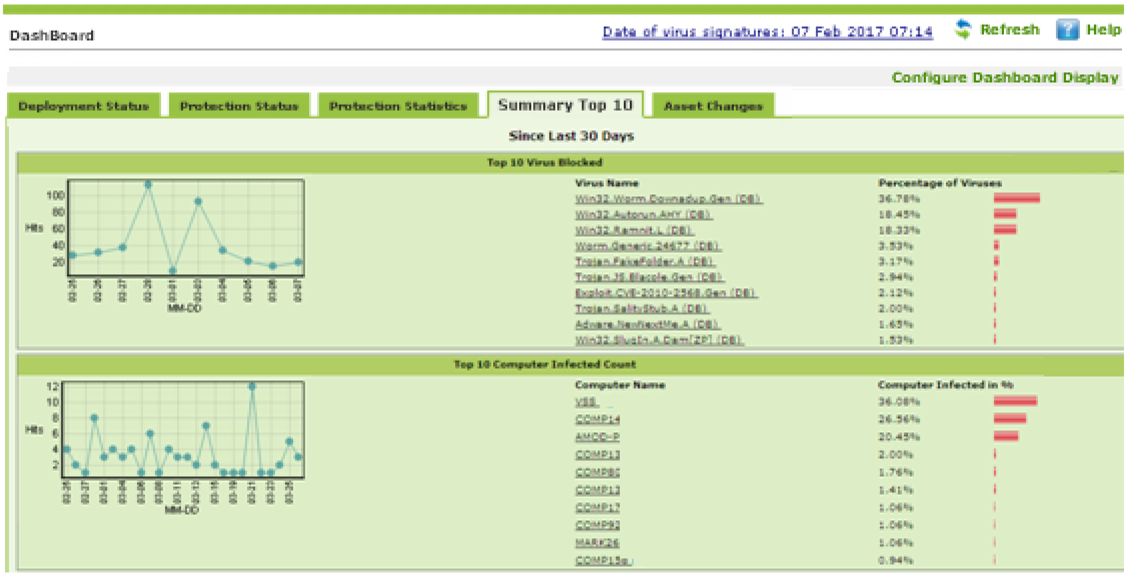


Additional protection statistics

Malware URL Block	174
Autorun Block	14
Executable Block USB	936
Executable Block Network	0
Executable Block User based	0
Proactive Statistics: Allow	4
Proactive Statistics: Block	2
Total	1130

- **Summary top 10**

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



DashBoard

Date of virus signatures: 07 Feb 2017 07:14

Since Last 30 Days

Top 10 Virus Blocked

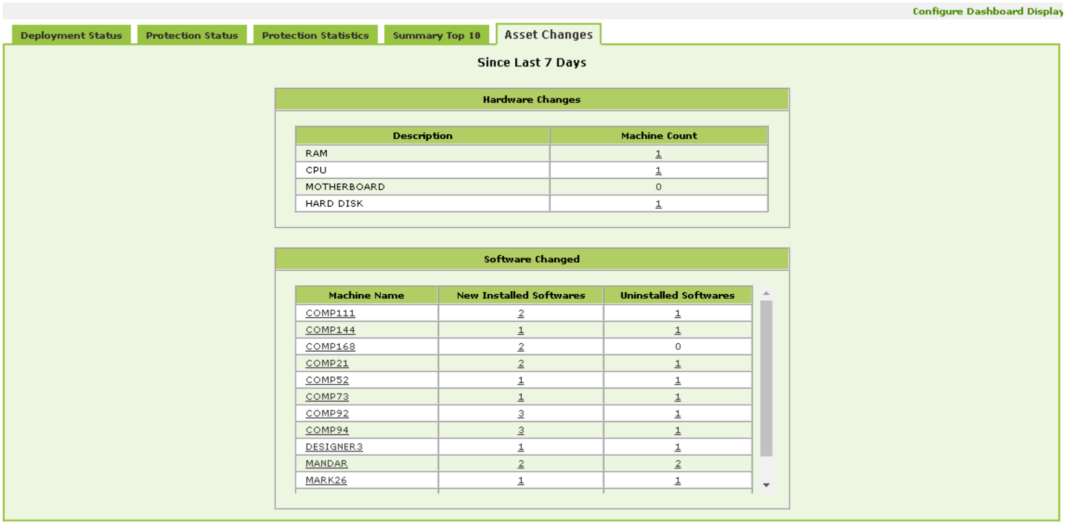
Virus Name	Percentage of Viruses
Win32.Worm.Downadup.Gen (DB)	36.78%
Win32.Autorun.AHY (DB)	18.45%
Win32.Ramnit.L (DB)	18.33%
Worm.Generic.24677 (DB)	3.53%
Trojan.FakeFolder.A (DB)	3.17%
Trojan.JS.Blacole.Gen (DB)	2.94%
Exploit.CVE-2010-2568.Gen (DB)	2.12%
Trojan.SalityStub.A (DB)	2.00%
Adware.NewNextMe.A (DB)	1.65%
Win32.Slugin.A.Gam[ZP] (DB)	1.53%

Top 10 Computer Infected Count

Computer Name	Computer Infected in %
VSS	36.08%
COMP14	26.56%
AMOD-P	20.45%
COMP13	2.00%
COMP80	1.76%
COMP13	1.41%
COMP17	1.06%
COMP92	1.06%
MARK26	1.06%
COMP15a	0.94%

- **Asset Changes**

This tab displays summary of all the hardware and software changes on the managed endpoints. It displays the list of the hardware changes and the list of software installed and uninstalled.



Since Last 7 Days

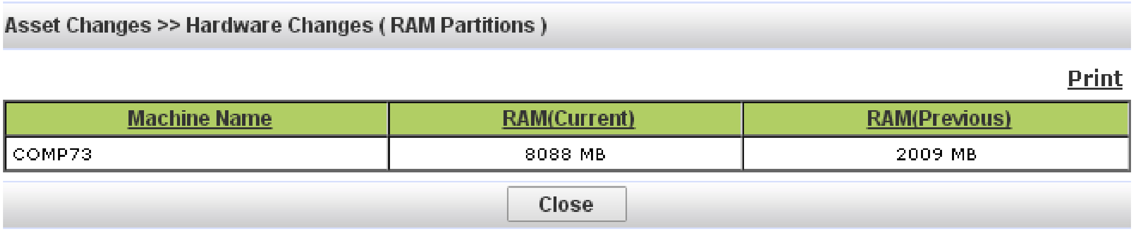
Hardware Changes

Description	Machine Count
RAM	1
CPU	1
MOTHERBOARD	0
HARD DISK	1

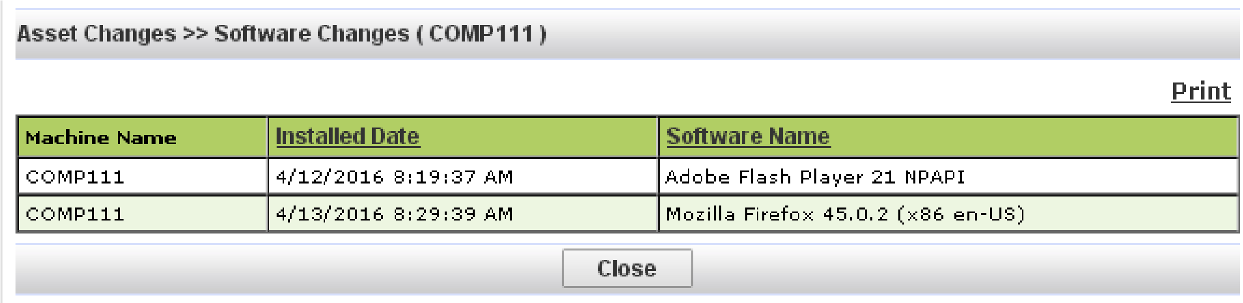
Software Changed

Machine Name	New Installed Softwares	Uninstalled Softwares
COMP111	2	1
COMP144	1	1
COMP168	2	0
COMP21	2	1
COMP52	1	1
COMP73	1	1
COMP92	3	1
COMP94	3	1
DESIGNER3	1	1
MANDAR	2	2
MARK26	1	1

- Click on the count to view the details of the managed endpoints to which the changes were made.


Asset Changes >> Hardware Changes (RAM Partitions)

Machine Name	RAM(Current)	RAM(Previous)
COMP73	8088 MB	2009 MB

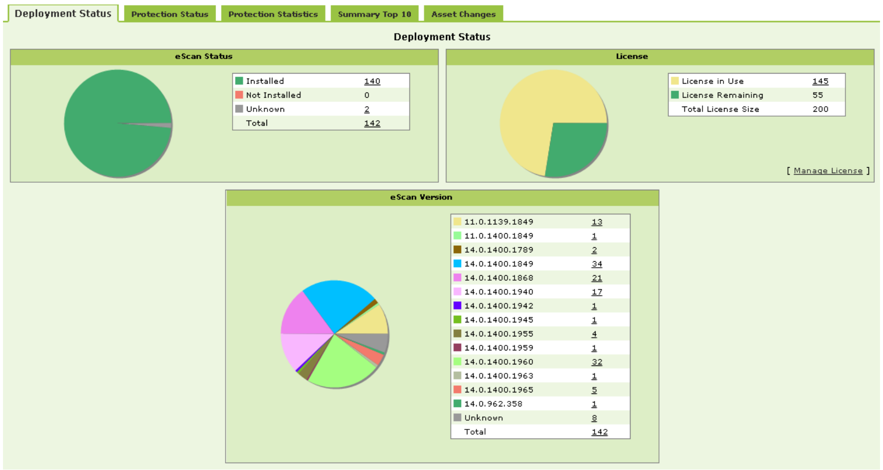

Asset Changes >> Software Changes (COMP111)

Machine Name	Installed Date	Software Name
COMP111	4/12/2016 8:19:37 AM	Adobe Flash Player 21 NPAPI
COMP111	4/13/2016 8:29:39 AM	Mozilla Firefox 45.0.2 (x86 en-US)

- **Configuring Dashboard Display**

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

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



Deployment Status

eScan Status

🟩 Installed	140
🟥 Not Installed	0
▨ Unknown	2
Total	142

License

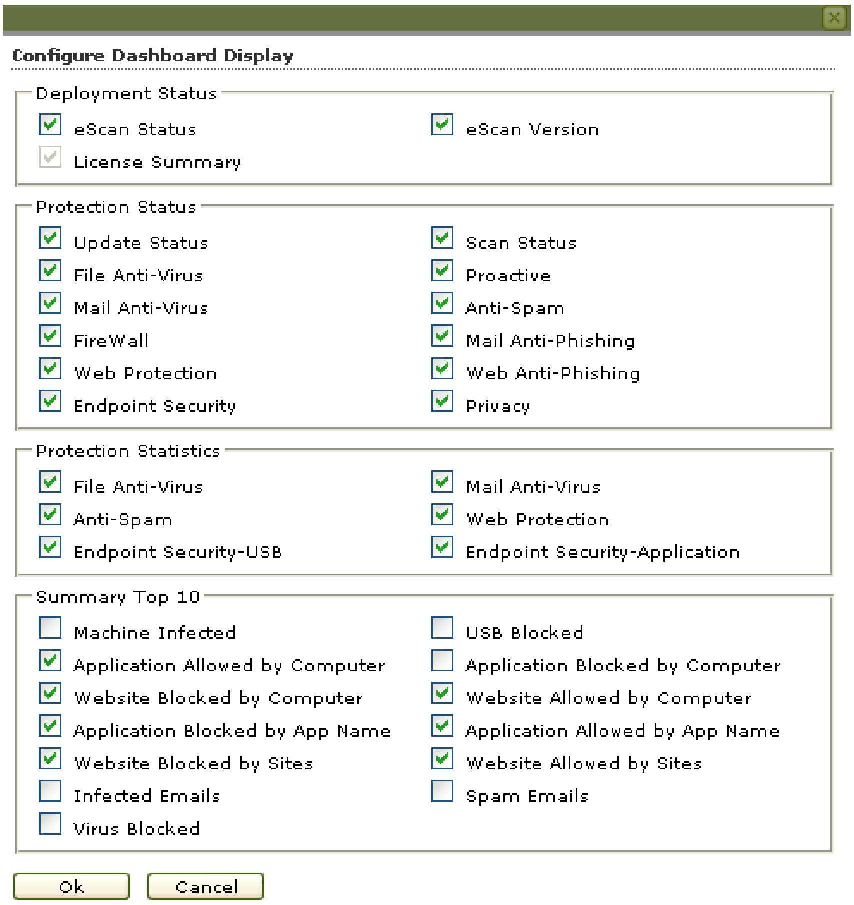
🟨 License in Use	145
🟩 License Remaining	55
Total License Size	200

[Manage License]

eScan Version

11.0.1139.1849	13
11.0.1400.1849	1
14.0.1400.1789	2
14.0.1400.1849	34
14.0.1400.1868	21
14.0.1400.1940	17
14.0.1400.1942	1
14.0.1400.1945	1
14.0.1400.1955	4
14.0.1400.1959	1
14.0.1400.1960	32
14.0.1400.1963	1
14.0.1400.1965	5
14.0.962.358	1
Unknown	8
Total	142

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



Configure Dashboard Display

Deployment Status

☑ eScan Status ☑ eScan Version
☑ License Summary

Protection Status

☑ Update Status ☑ Scan Status
☑ File Anti-Virus ☑ Proactive
☑ Mail Anti-Virus ☑ Anti-Spam
☑ FireWall ☑ Mail Anti-Phishing
☑ Web Protection ☑ Web Anti-Phishing
☑ Endpoint Security ☑ Privacy

Protection Statistics

☑ File Anti-Virus ☑ Mail Anti-Virus
☑ Anti-Spam ☑ Web Protection
☑ Endpoint Security-USB ☑ Endpoint Security-Application

Summary Top 10

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

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

Managing Computers

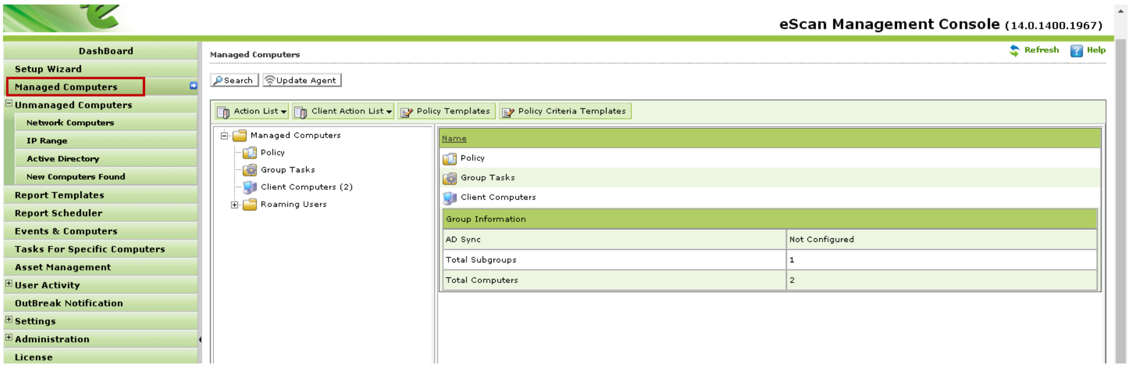
This section helps you in creating logical computer groups, defining policies for the created groups, and creating tasks for the desired group of computers. It is recommended that you group all the computers on the network in Logical group; it will help you in defining tasks and policies and monitoring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

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

Creating Logical Computer Groups

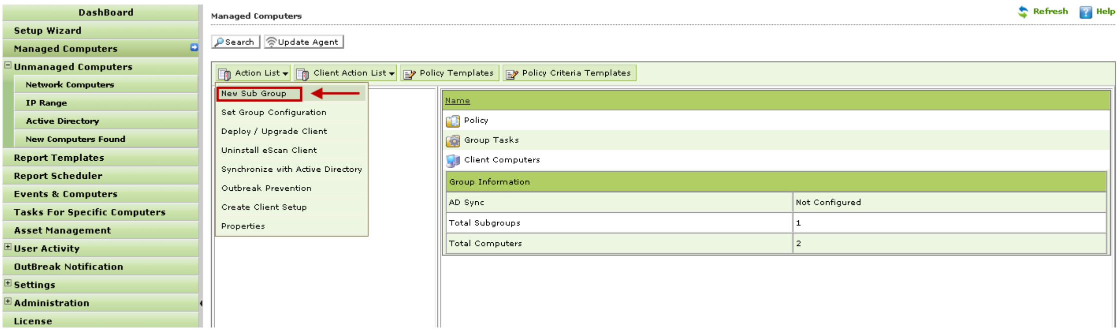
For securing and managing computers present on the network, create groups and then add all computers in the groups created by you. It will help in better management, monitoring and security of the endpoints. You can create the groups using following steps.

1. Click **Managed Computers** option present in the Navigation Panel, as shown below –



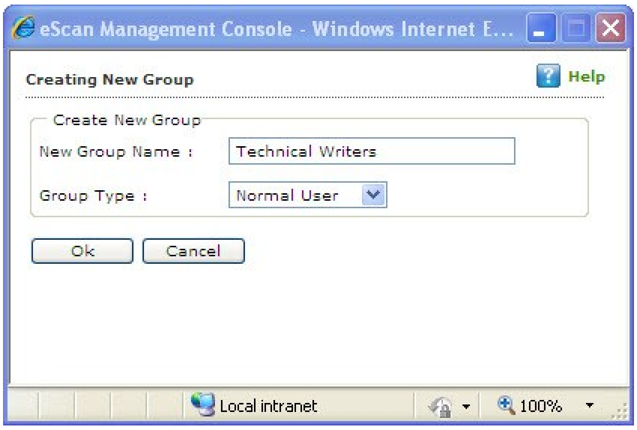
Group Information	
AD Sync	Not Configured
Total Subgroups	1
Total Computers	2

2. This will open the **Managed Computers** section on the right; now click **New Sub Group** option present in **Action List** drop down menu on the interface, as shown below –



Group Information	
AD Sync	Not Configured
Total Subgroups	1
Total Computers	2

- **Creating New Sub Group** window will pop up, Fill in the New Group Name and Select the Group type as Normal user or Roaming user using the drop down present on the interface, as shown below –



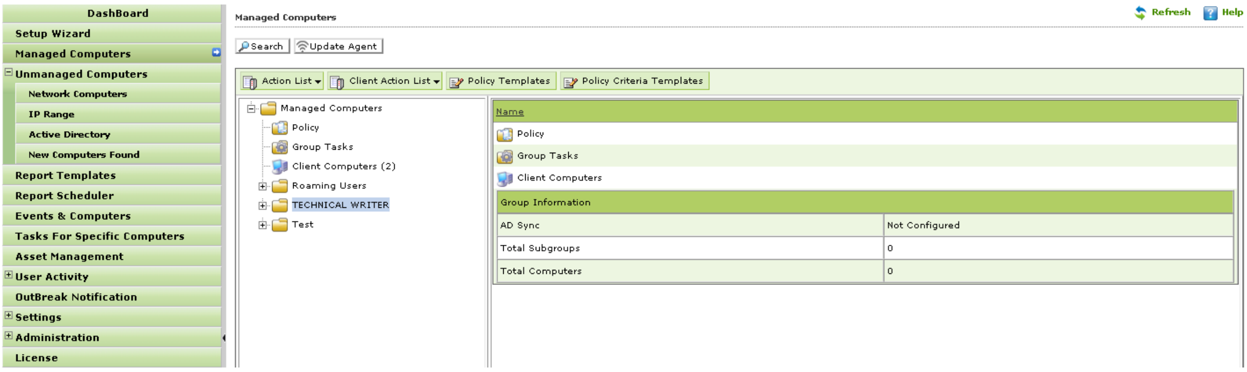
Creating New Group

Create New Group

New Group Name : Technical Writers

Group Type : Normal User

3. Click **OK**, the group will be created under **Managed Computers** in eScan Management Console.



Group Information	
AD Sync	Not Configured
Total Subgroups	0
Total Computers	0

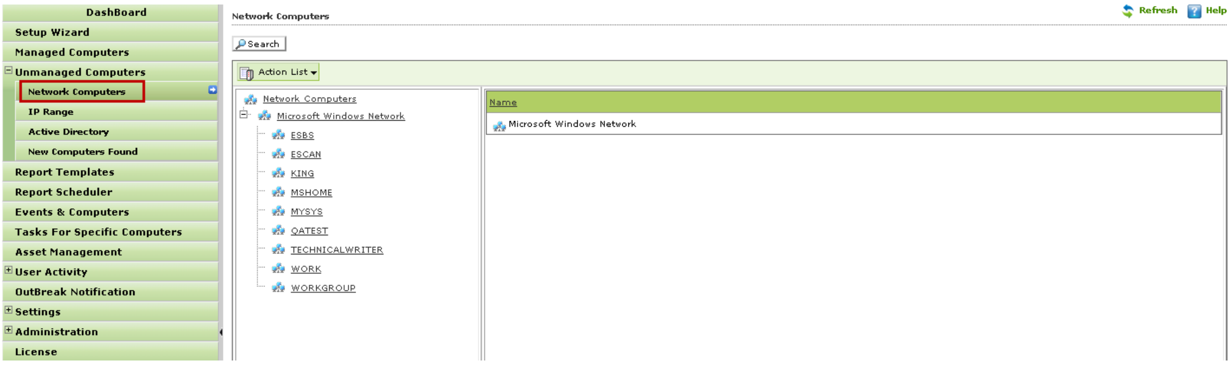
Moving Computers to the created Groups

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

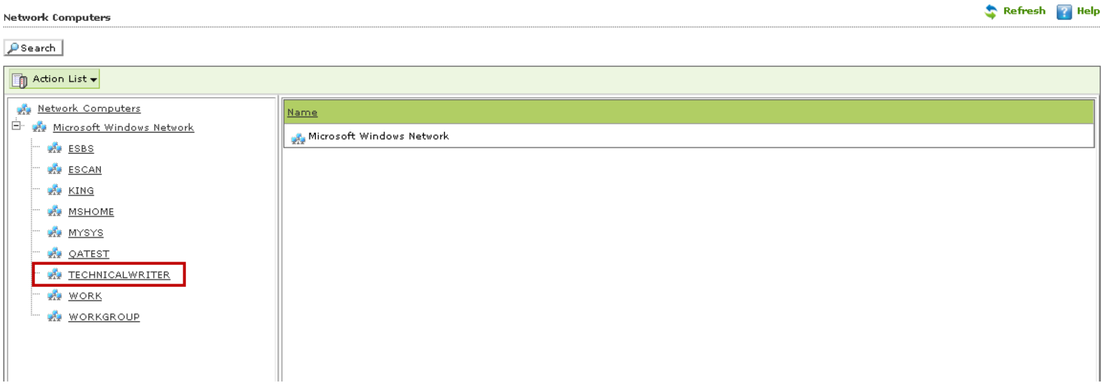
- Moving Computers from **Network Computers.**
- Moving all Computers within selected **IP Range.**
- Moving Computers from **Active Directory.**
- Moving Computers from the **New Computers Found** List.

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

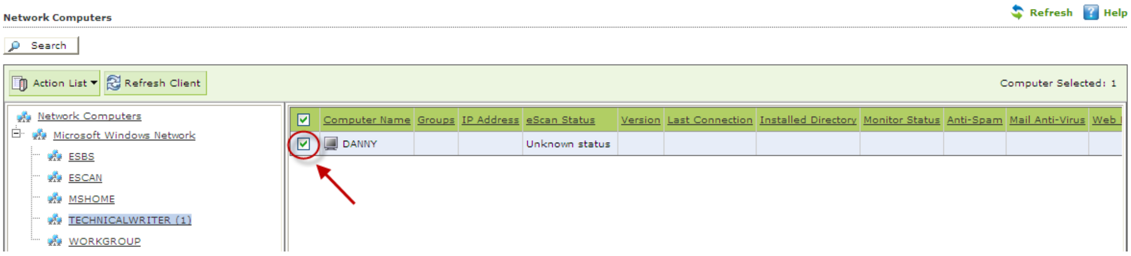
1. Click **Network Computers** option present in the **Navigation Panel** under Unmanaged Computers, as shown below



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



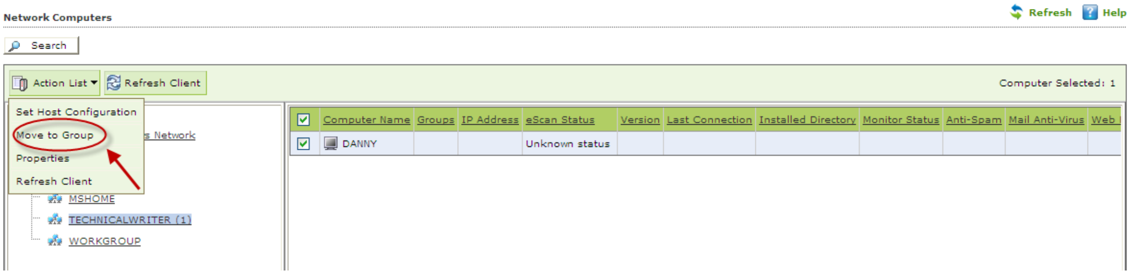
3. Now select the Computer(s) that you wish to move to the desired groups that you created under Managed computers. You can do so by selecting the check box beside the **Computer Names**, as shown below -



☑	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web
☑	DANNY			Unknown status							

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

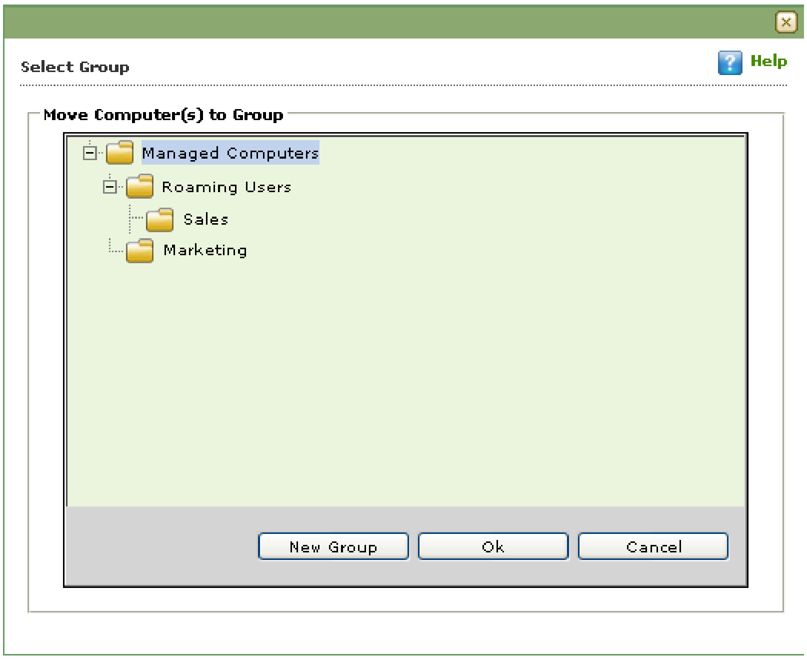
4. Click **Move to Group** option present in the **Action List** drop down menu present on the interface, as shown below -



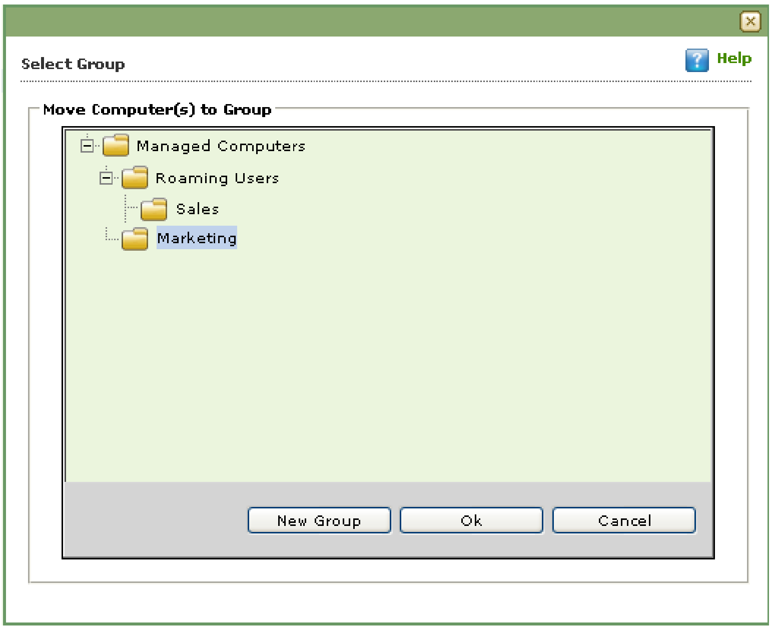
Computer Selected: 1

☑	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web
☑	DANNY			Unknown status							

5. **Select Group** window will open on the screen. Expand the Managed Computers tree to view the groups that you created earlier, as shown below -



6. Now select the group where you wish to move the selected computer(s), as shown below -



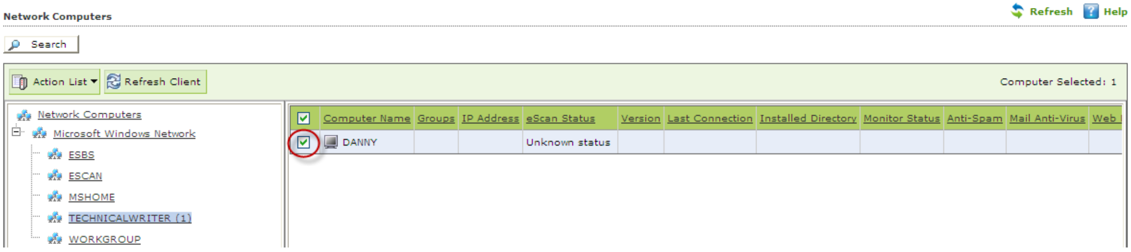
7. Now Click **OK**, selected Computer(s) will be moved to the group. Click **Cancel** if you do not wish to move the selected computers to this group.

   <u>Also see Creating New Group from the Select Group window</u>.

Viewing Properties of Selected Computer

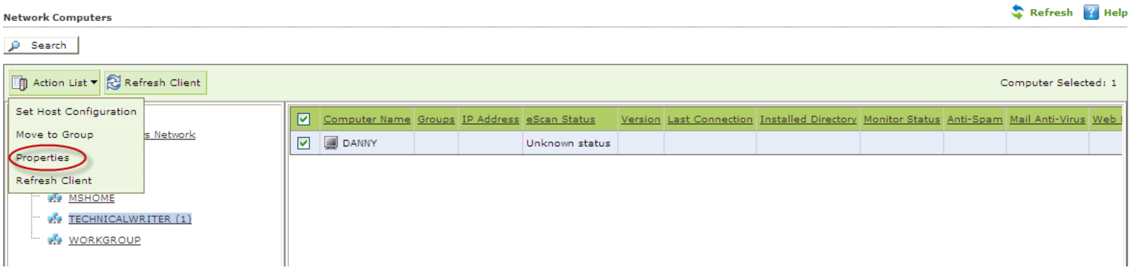
You can view the properties of the selected computer using following steps –

1. Select the desired computer in the network computers list to view its properties



☑	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web
☑	DANNY			Unknown status							

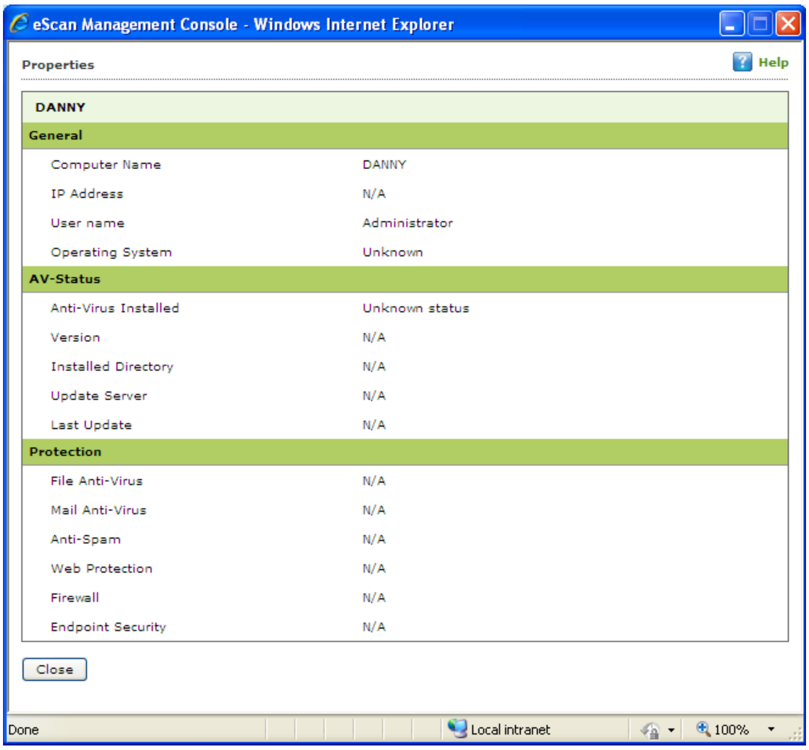
2. Now click **Properties** option in the **Action List** drop down menu present on the interface.



☑	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web
☑	DANNY			Unknown status							

3. This will open the **Properties** window on a pop up. It displays general information of the computer like Computer Name, IP Address, User name and Operating System, along

with details of the Antivirus installed, its version and update summary. It also displays protection status of all the Modules of eScan client, as shown below -



DANNY	
General	
Computer Name	DANNY
IP Address	N/A
User name	Administrator
Operating System	Unknown
AV-Status	
Anti-Virus Installed	Unknown status
Version	N/A
Installed Directory	N/A
Update Server	N/A
Last Update	N/A
Protection	
File Anti-Virus	N/A
Mail Anti-Virus	N/A
Anti-Spam	N/A
Web Protection	N/A
Firewall	N/A
Endpoint Security	N/A

Note:

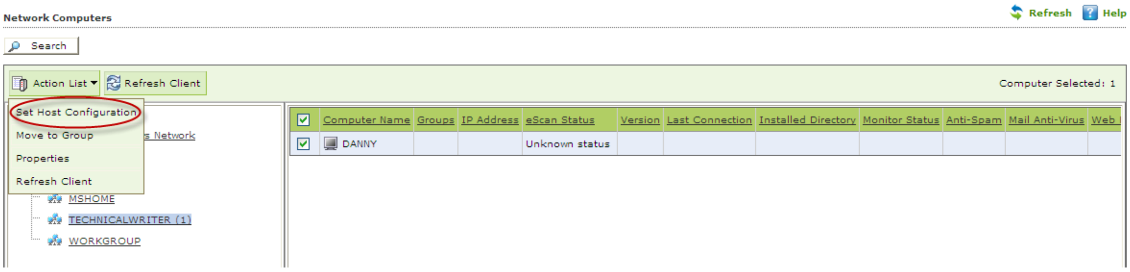
- In case of Multiple Selection of Computers, the properties option will be disabled.

- **Setting Host Configuration**

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

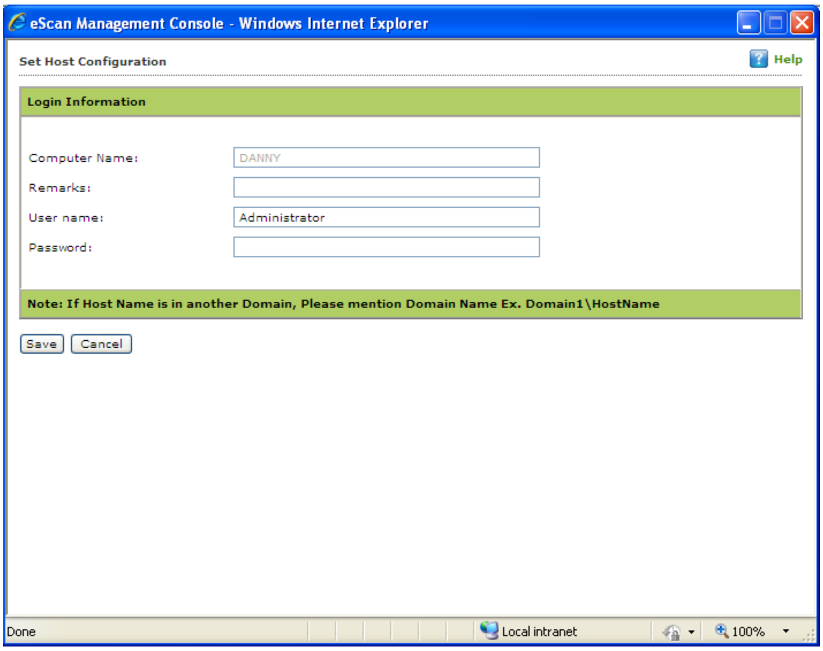
You can set Host Configuration using following Steps –

1. Select the desired computer, the Properties of which you want to view.
2. Now click **Set Host Configuration** option present in the **Action List** drop down menu.



☑	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web
☑	DANNY			Unknown status							

3. Now write remarks and define the Administrator Username and Password and then click **Save**.



eScan Management Console - Windows Internet Explorer

Set Host Configuration

Login Information

Computer Name: DANNY

Remarks:

User name: Administrator

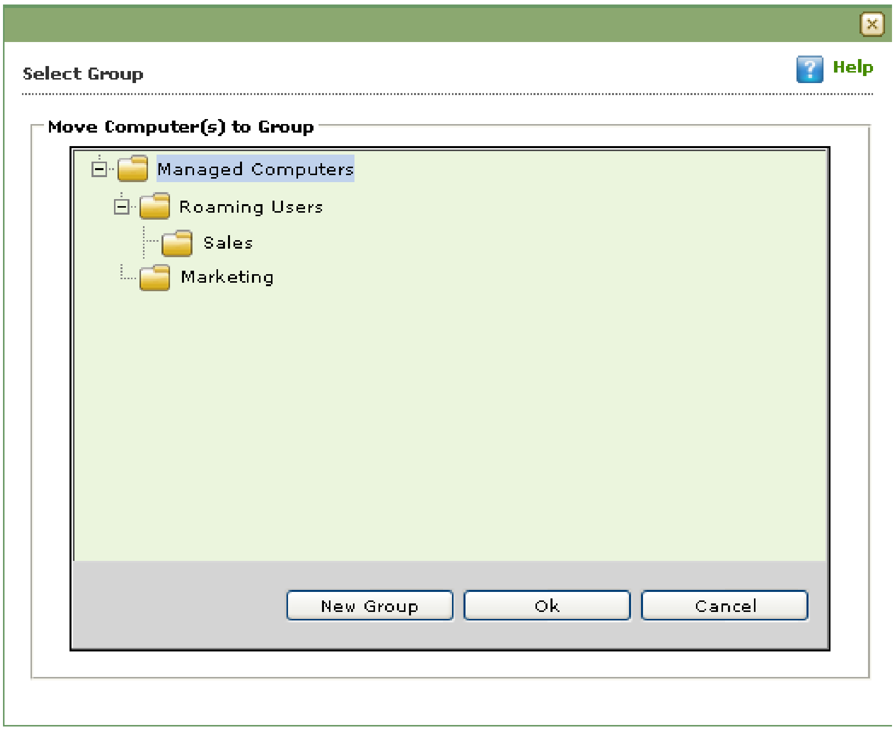
Password:

Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName

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

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

(The Select Group Window opens when you click Move to Group)

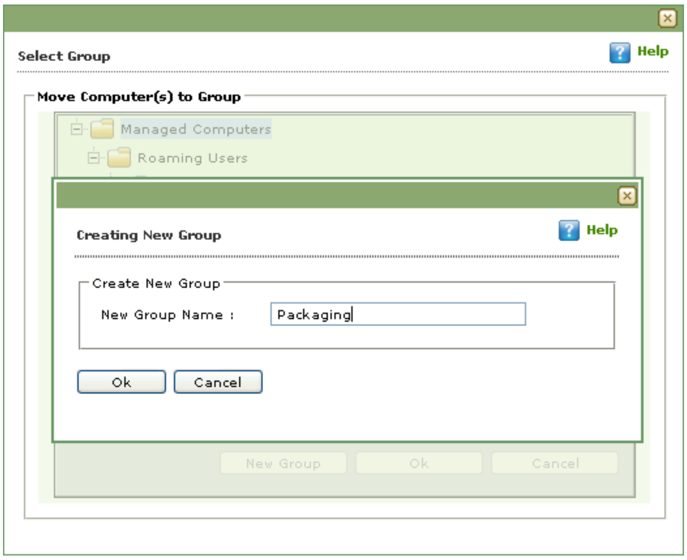


Select Group

Move Computer(s) to Group

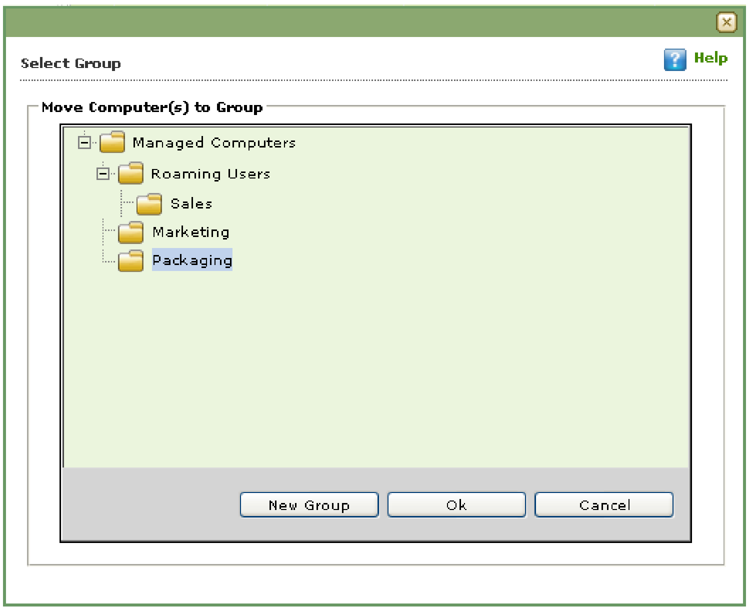
You can create a **New Group** from this window using the following steps –

1. Click **New Group**, write the name of the Group and click **Ok**, as shown below -



New Group Name : Packaging

2. The group will be created instantly, as shown below -

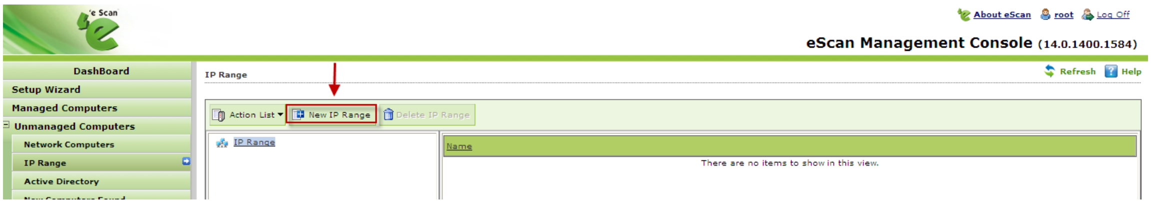


- **Moving all Computers within selected IP Range to a Group –**

It includes following steps --

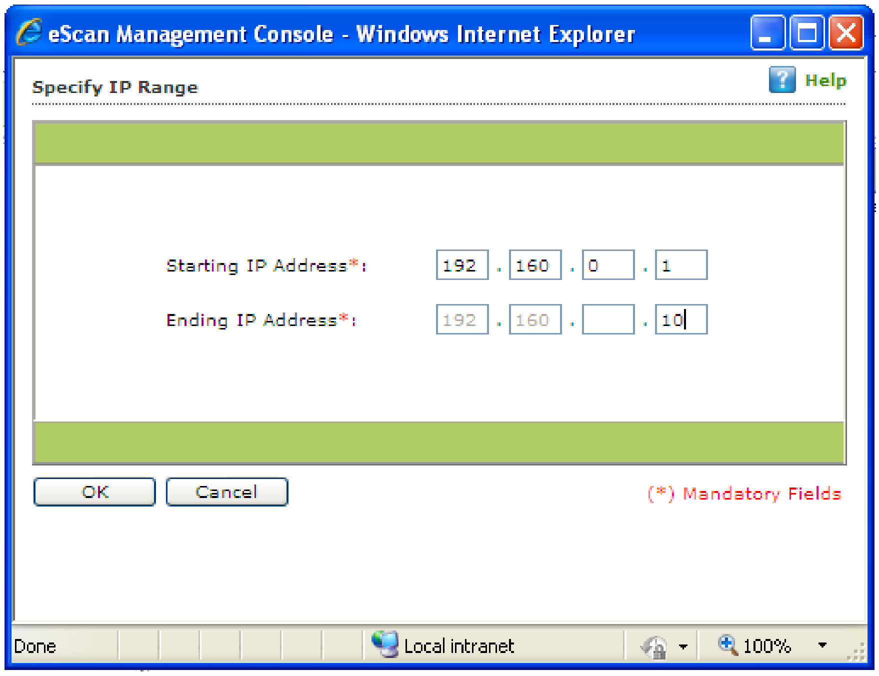
- **Adding New IP Range -** You can **Add** the Computers within certain IP range using the **IP Range** option present under **Unmanaged Computers**. It can be done using the following simple steps –

1. Click **IP range** option under Unmanaged Computers, and then click **New IP Range** option in the Window, as shown below -



There are no items to show in this view.

2. You will be forwarded to **Specify IP Range** window. Specify the desired IP Range and click **Ok**, as shown below -

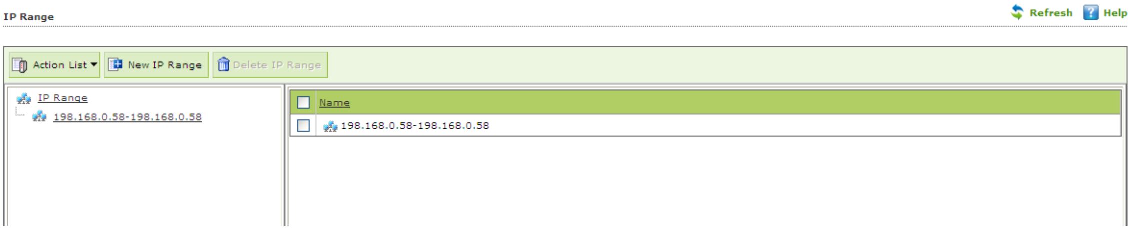


Starting IP Address*: 192 . 160 . 0 . 1

Ending IP Address*: 192 . 160 . . 10

(*) Mandatory Fields

3. The selected IP Range will be added to the IP Range tree. All computers present in that IP range will be displayed when you select the IP Range on the interface, as shown below -



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

- **Action List (Menu)**

  - **Setting Host Configuration -** Select the computer and define the Host Configuration settings using Set Host Configuration option present in Action List.

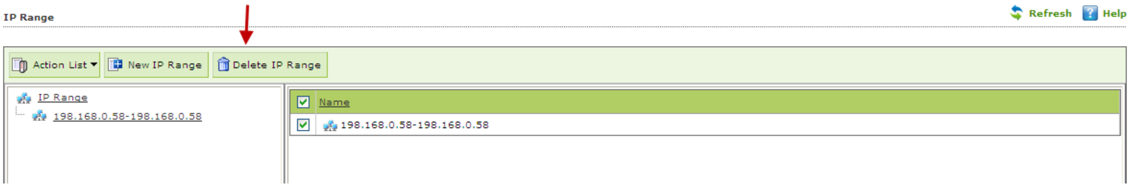
This will help you in fetching Computer Properties before adding them to a group under Managed Computers. (For Endpoints with Windows operating system).

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

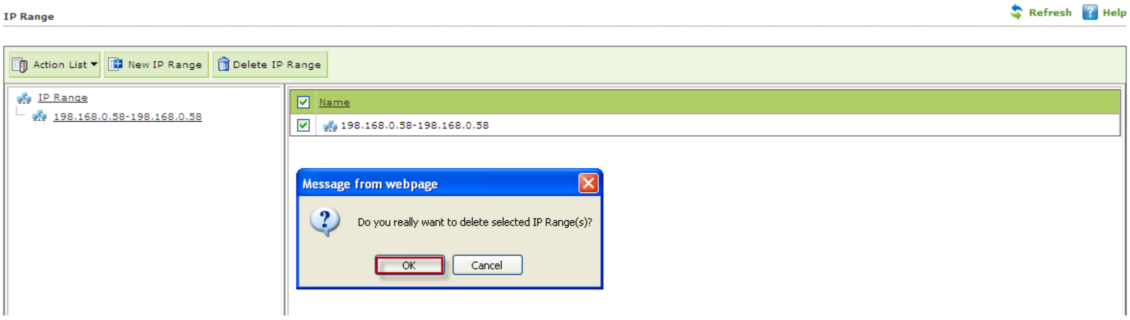
- **Refreshing Client –** Click this option to fetch latest information / details of the selected computer. This option is present on IP Range window as well as under Action List Menu.

- **Delete IP Range**

1. Select the desired IP Range and click Delete IP Range option present on the screen, as shown below -



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



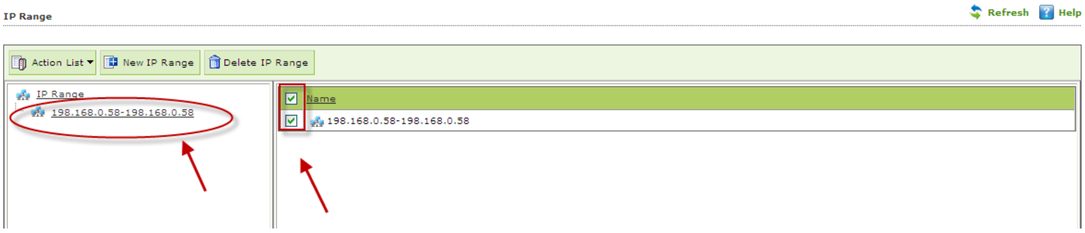
Do you really want to delete selected IP Range(s)?

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

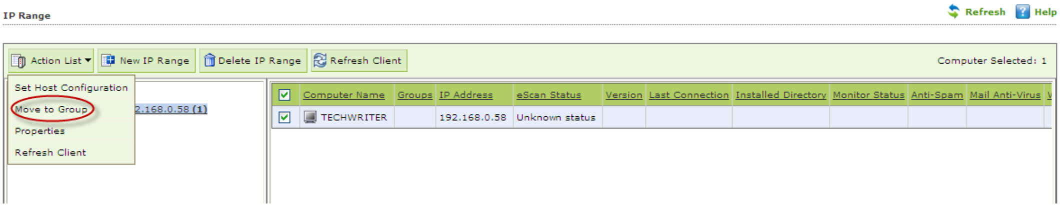
- **Moving to a Group**

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

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

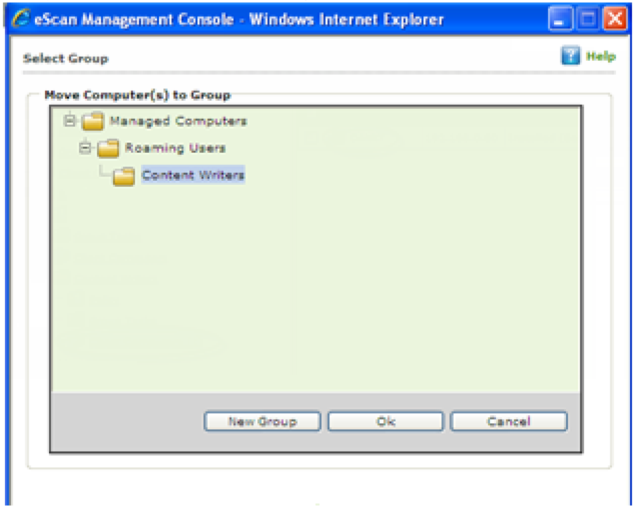


2. Now Click **Move to Group** under **Action List** drop down menu.

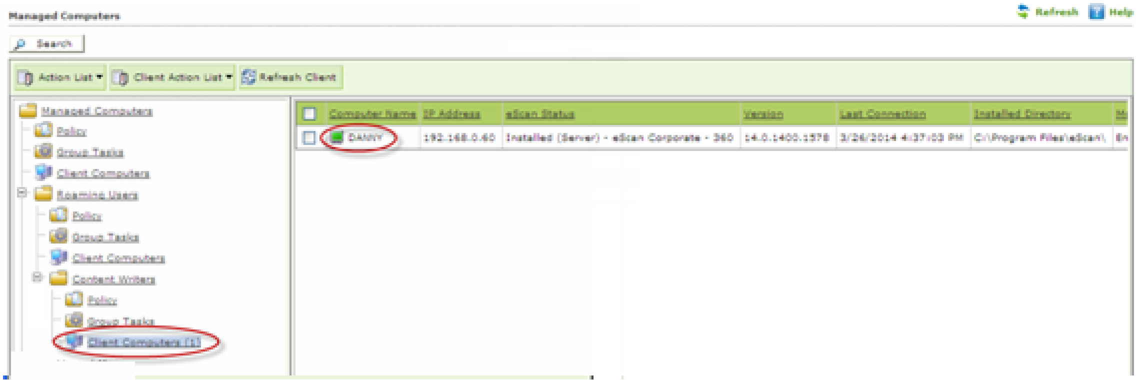


☑	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus
☑	TECHWRITER		192.168.0.58	Unknown status						

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



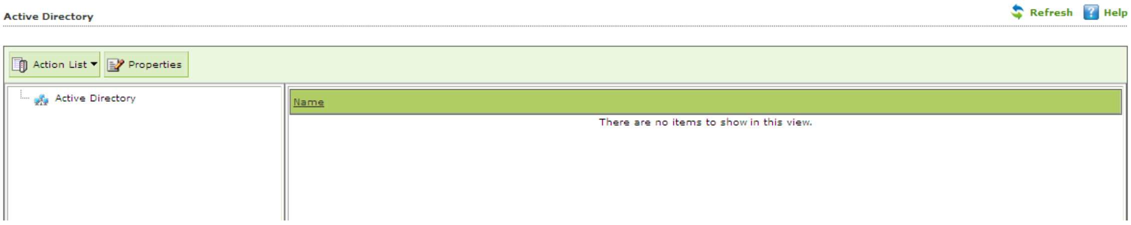
4. The selected computer(s) will be moved to the selected group under **Managed Computers** section.



□	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory
□	DANNY	192.168.0.60	Installed (Server) - eScan Corporate - 360	14.0.1400.1578	3/26/2014 4:37:03 PM	C:\Program Files\eScan\

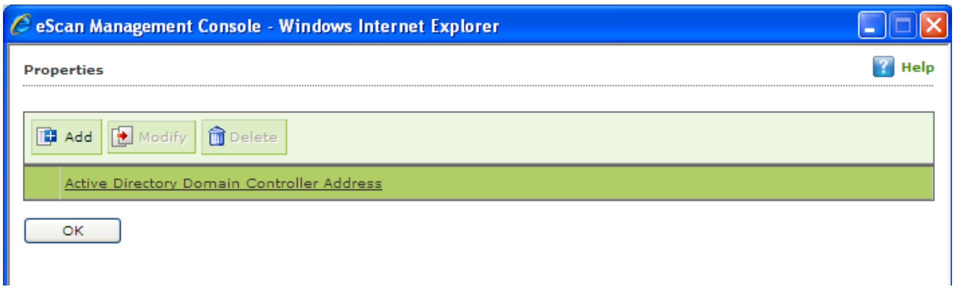
i. **Moving Computer from Active Directory –** You can use the following simple steps to add computers from the Active Directory.

1. Click **Active directory** under Unmanaged Computers in the Navigation Panel of eScan management Console and Select **Active Directory** present in the tree. Now click **Properties**, as shown below -

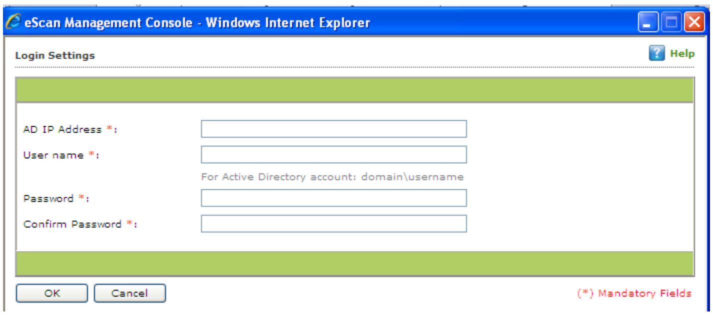


There are no items to show in this view.

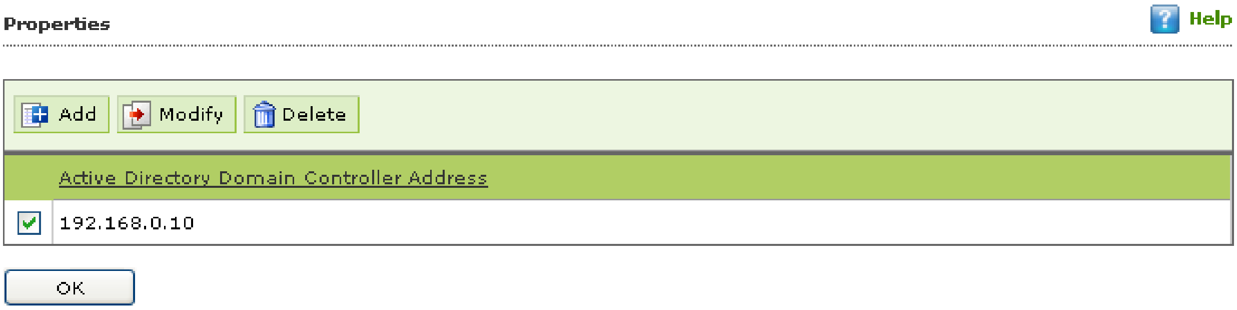
2. You will be forwarded to the Properties window. Click **Add**.


eScan Management Console - Windows Internet Explorer
Properties
Help
Add
Modify
Delete
Active Directory Domain Controller Address
OK

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

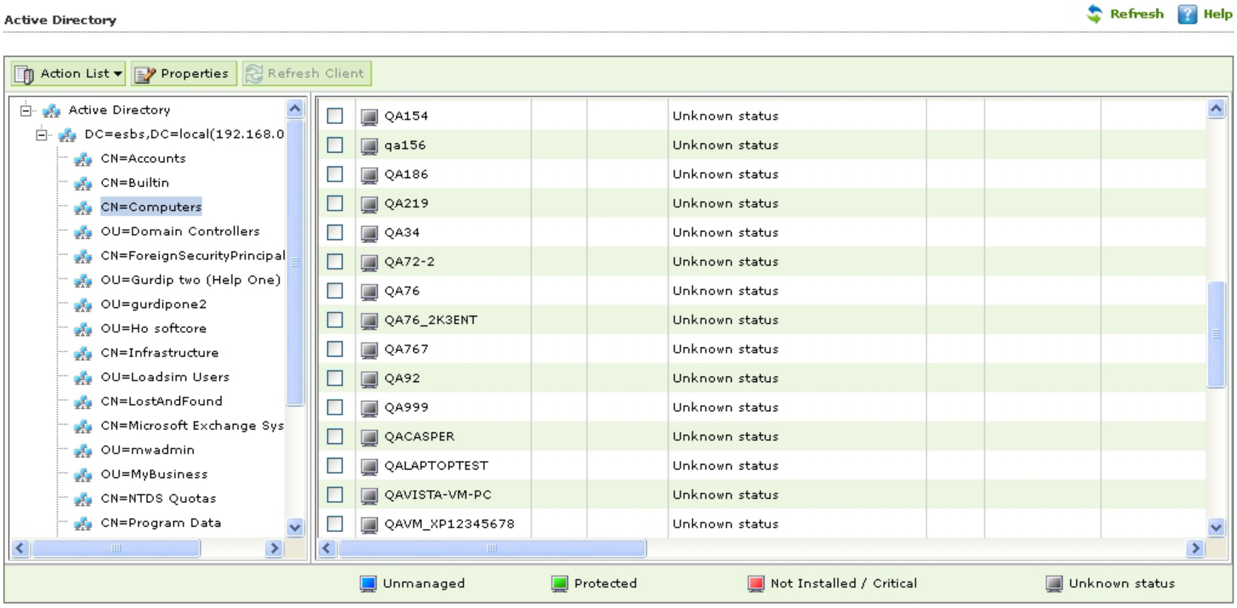


4. The details including IP Addresses from active directory will be added instantly.



	Active Directory Domain Controller Address
☑	192.168.0.10

5. Select the Active Directory and click **OK**. The selected Active Directory will be added to the Active directory tree, to view the details click on the directory present under Active directory tree, as shown below -



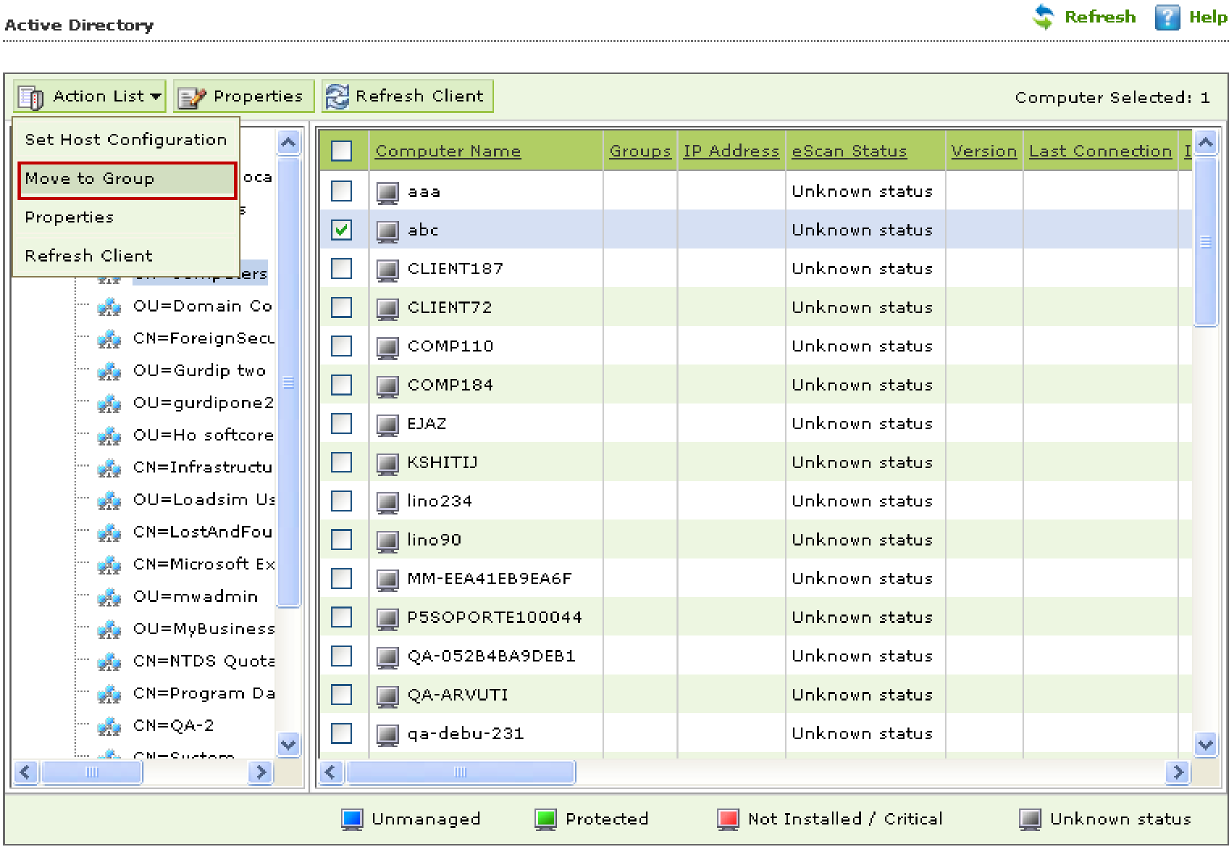
Active Directory

- Active Directory
  - DC=esbs,DC=local(192.168.0
    - CN=Accounts
    - CN=Builtin
    - CN=Computers
    - OU=Domain Controllers
    - CN=ForeignSecurityPrincipal
    - OU=Gurdip two (Help One)
    - OU=gurdipone2
    - OU=Ho softcore
    - CN=Infrastructure
    - OU=Loadsim Users
    - CN=LostAndFound
    - CN=Microsoft Exchange Sys
    - OU=mwadmin
    - OU=MyBusiness
    - CN=NTDS Quotas
    - CN=Program Data

□	QA154			Unknown status			
□	qa156			Unknown status			
□	QA186			Unknown status			
□	QA219			Unknown status			
□	QA34			Unknown status			
□	QA72-2			Unknown status			
□	QA76			Unknown status			
□	QA76_2K3ENT			Unknown status			
□	QA767			Unknown status			
□	QA92			Unknown status			
□	QA999			Unknown status			
□	QACASPER			Unknown status			
□	QALAPTOPTEST			Unknown status			
□	QAVISTA-VM-PC			Unknown status			
□	QAVM_XP12345678			Unknown status			

🟦 Unmanaged 🟩 Protected 🟥 Not Installed / Critical ▨ Unknown status

6. To move computers present in the Active Directory, select the computers in the list and click **Move to Group** option under Action List menu, as shown below -



Active Directory

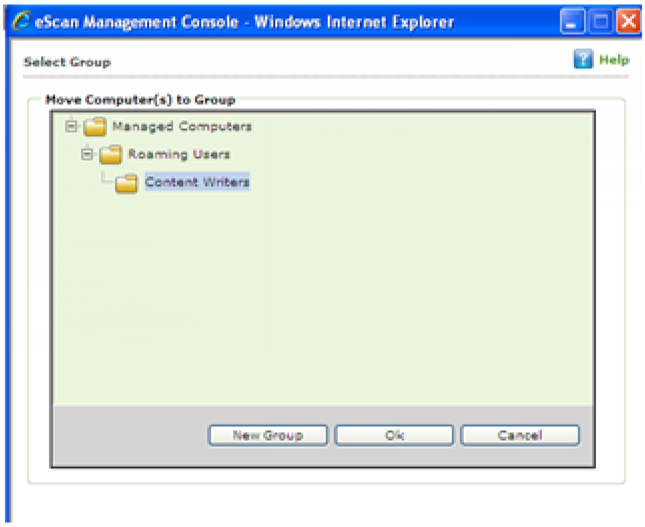
Computer Selected: 1

- OU=Domain Co
- CN=ForeignSecu
- OU=Gurdip two
- OU=gurdipone2
- OU=Ho softcore
- CN=Infrastructu
- OU=Loadsim Us
- CN=LostAndFou
- CN=Microsoft Ex
- OU=mwadmin
- OU=MyBusiness
- CN=NTDS Quota
- CN=Program Da
- CN=QA-2

□	Computer Name	Groups	IP Address	eScan Status	Version	Last Connection	I
□	aaa			Unknown status			
☑	abc			Unknown status			
□	CLIENT187			Unknown status			
□	CLIENT72			Unknown status			
□	COMP110			Unknown status			
□	COMP184			Unknown status			
□	EJAZ			Unknown status			
□	KSHITIJ			Unknown status			
□	lino234			Unknown status			
□	lino90			Unknown status			
□	MM-EEA41EB9EA6F			Unknown status			
□	P5SOPORTE100044			Unknown status			
□	QA-052B4BA9DEB1			Unknown status			
□	QA-ARVUTI			Unknown status			
□	qa-debu-231			Unknown status			

🟦 Unmanaged 🟩 Protected 🟥 Not Installed / Critical ▨ Unknown status

7. Select the Group and Click **OK**.



eScan Management Console - Windows Internet Explorer

Select Group

Move Computer(s) to Group

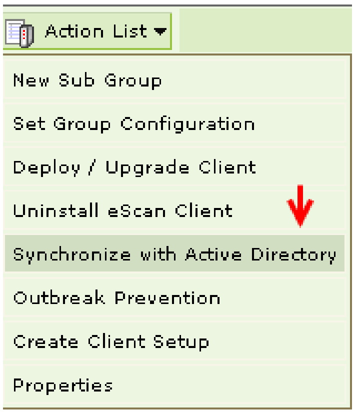
8. The selected computers will be moved to the selected group.

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

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

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

- **Active Directory Synchronization**



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

Note:

- Ensure that your protect Windows Critical Server Manually if they are a part of Active Directory, before start of the Synchronization.
- If any computer or container is removed, it will also be removed from eScan Console when it synchronizes with Active Directory.
- By Default, the synchronization interval is of 60 minutes. You can set it to a minimum of 5 minutes.

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

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

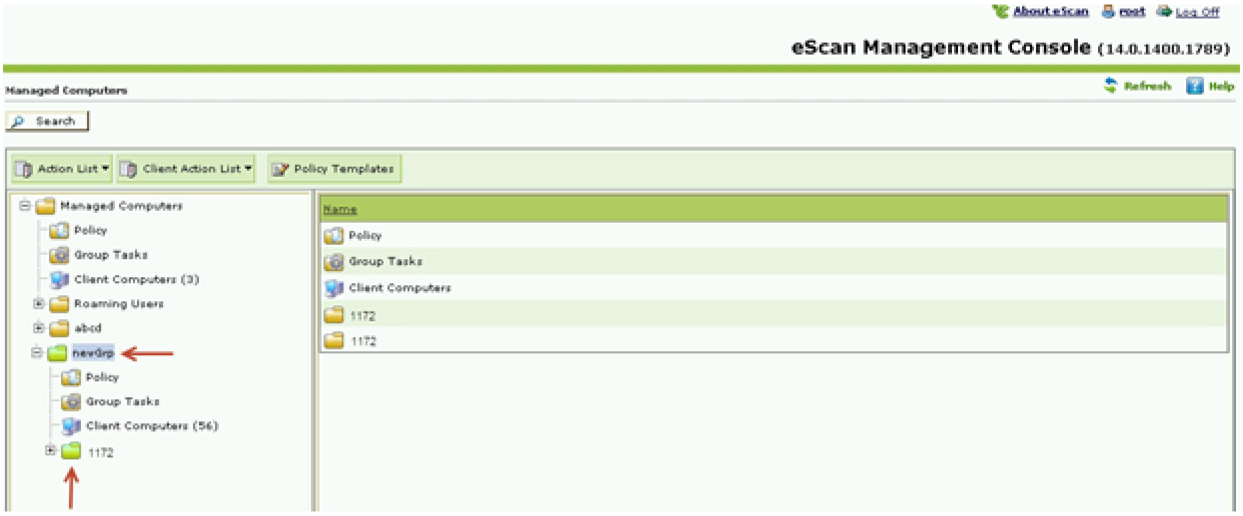
  Once the Active Directory is synced with the eScan Server, it will automatically install eScan on all the client machines in the Active Directory.

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

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

Note:

- Active Directory groups will be denoted by Dark Green Color.



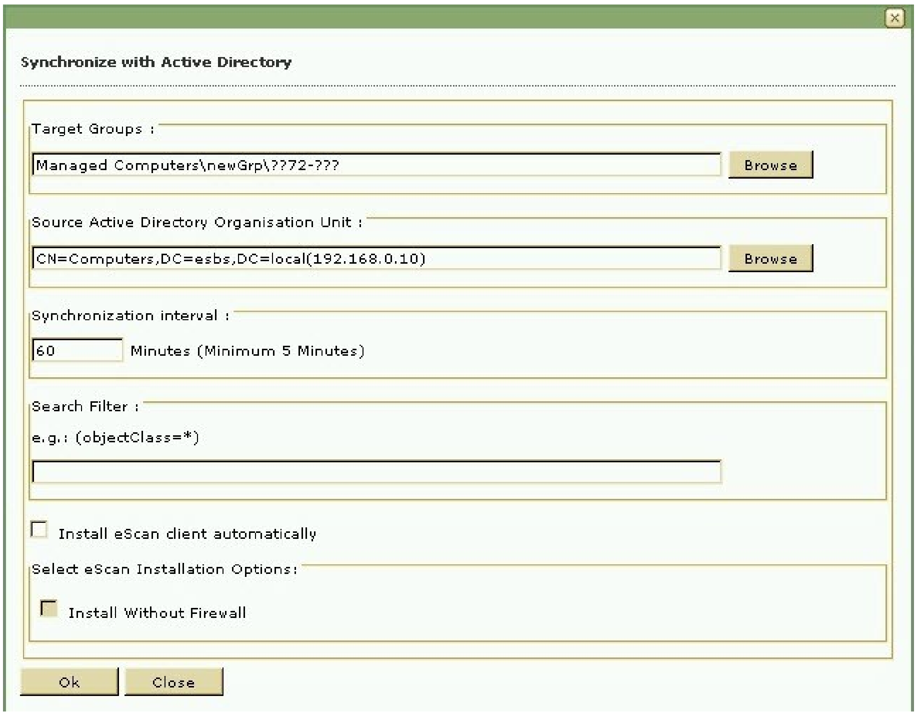
Name
Policy
Group Tasks
Client Computers
1172
1172

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

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

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

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


Synchronize with Active Directory

Target Groups : Managed Computers\newGrp\??72-???

Source Active Directory Organisation Unit : CN=Computers,DC=esbs,DC=local(192.168.0.10)

Synchronization interval : 60 Minutes (Minimum 5 Minutes)

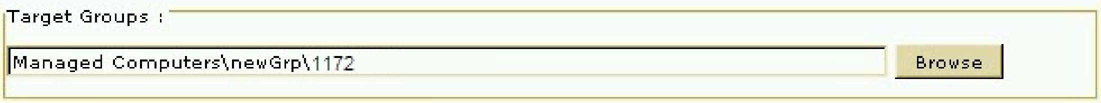
Search Filter : e.g.: (objectClass=*)

□ Install eScan client automatically

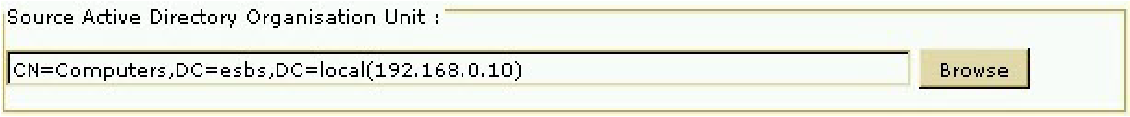
Select eScan Installation Options:

□ Install Without Firewall

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


Target Groups : Managed Computers\newGrp\1172

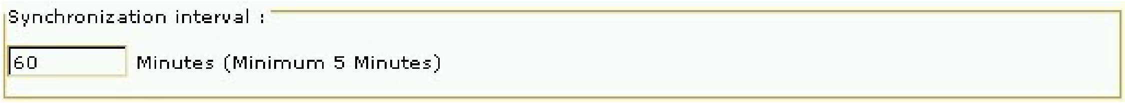
- **Source Active Directory Organization Unit:** Click **browse** and select the path of the source Active Directory. The target groups in the above column will be synced with the group in this path.



Source Active Directory Organisation Unit :

CN=Computers,DC=esbs,DC=local(192.168.0.10)

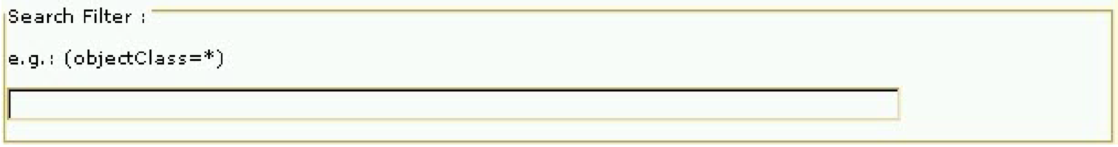
- **Synchronization Interval:** This option will allow you to set the synchronization intervals, the active directory will be automatically synced after the defined time period. The minimum interval that can be defined is of five minutes.



Synchronization interval :

60 Minutes (Minimum 5 Minutes)

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

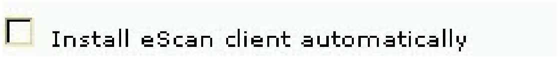


Search Filter :

e.g.: (objectClass=*)

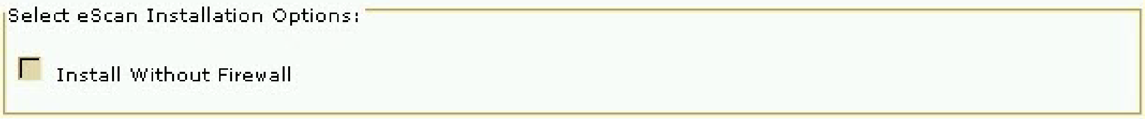
- **Install eScan client automatically:** Select this check box to install eScan automatically on to the client computers in the group. eScan will be automatically installed on the computers that are newly added in the group whenever next AD synchronization takes place.

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



□ Install eScan client automatically

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



Select eScan Installation Options:

□ Install Without Firewall

- Click **OK** to Apply settings

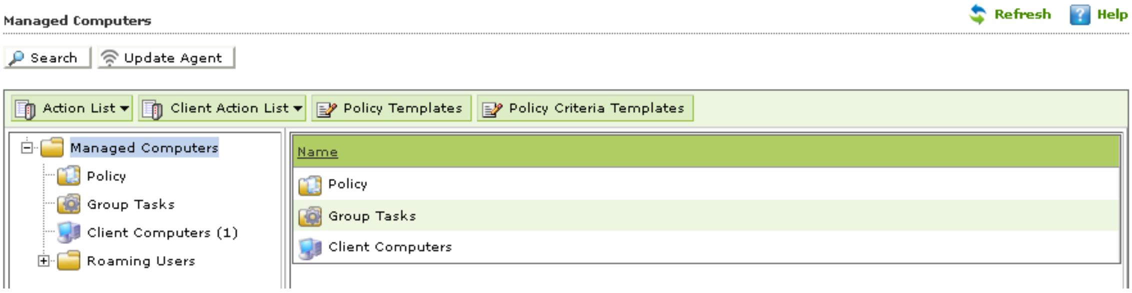
- **Properties**

It will display the properties of the selected managed group.

General: This tab will display the following details about the selected group

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

- **Update Agent**



This option will allow you to add or remove computers as Update Agents. This will reduce the traffic between the eScan ISS for Business Server and the client.

Features of Update Agents:

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

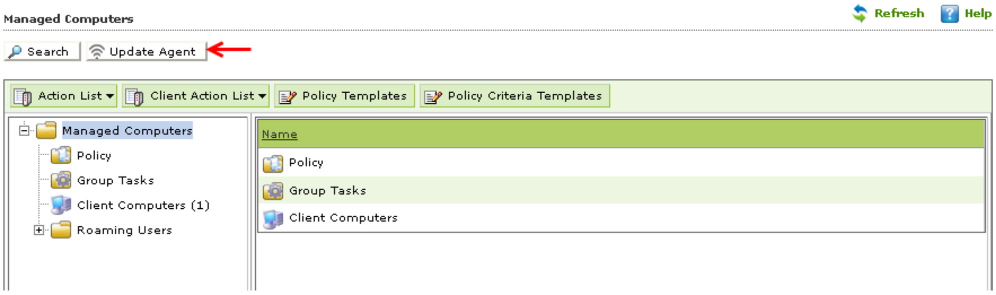
Advantages of Update Agents

1. Update Agent can be installed on any client computer connected to the network (where eScan is already installed).
2. Update Agent will take the signature updates from eScan Server and distribute the same to other managed computers in the group. (Bandwidth is saved).

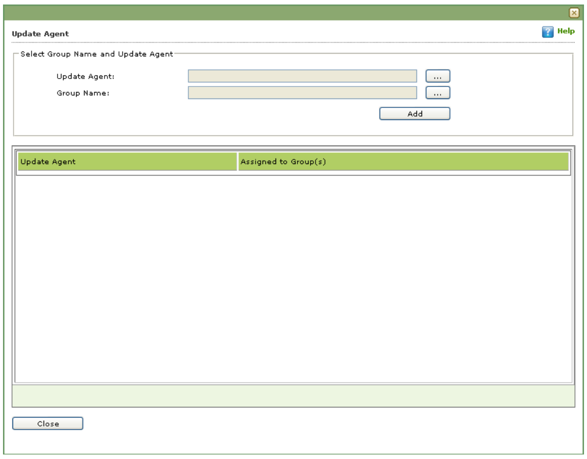
3. Update Agent will alternatively query eScan Update servers on internet for getting updates whenever there is a connectivity problem between the update agent and eScan Server.

Steps for Creating Update Agent

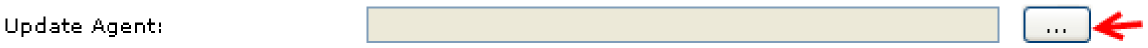
1. Go to Managed Computers and click on Update Agent button, as shown below –



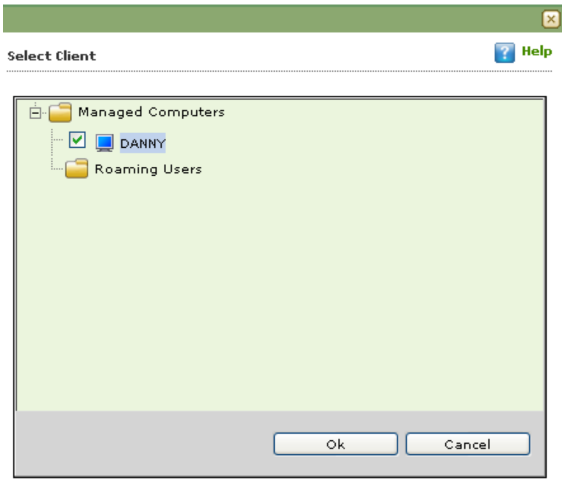
2. You will be forwarded to Update Agent window, as shown below –



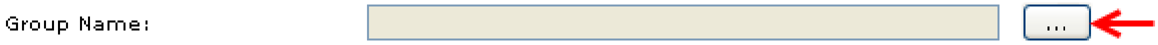
3. Browse the Endpoint that you want to make update agent for desired group using ... button present beside “**Update Agent**” field, as shown below -



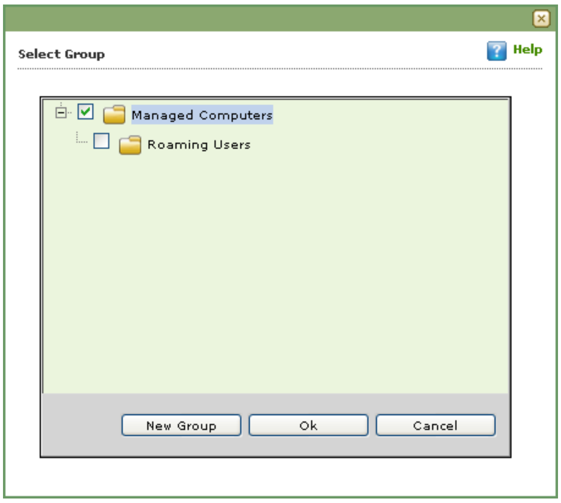
4. Select the Endpoint to make it as an update agent for the group and click OK, as shown below –



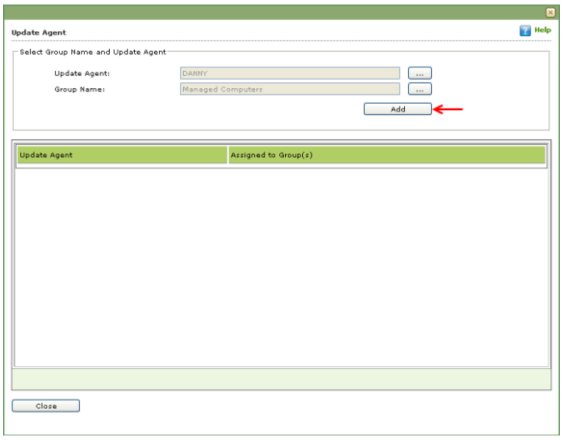
5. Click on browse button present beside “**Group Name**” to select the group for which update agent is being created.



6. You will be forwarded to **Select Group** Window, as shown below –



7. Click OK, and then Click on **ADD** button present on the interface, as shown below-

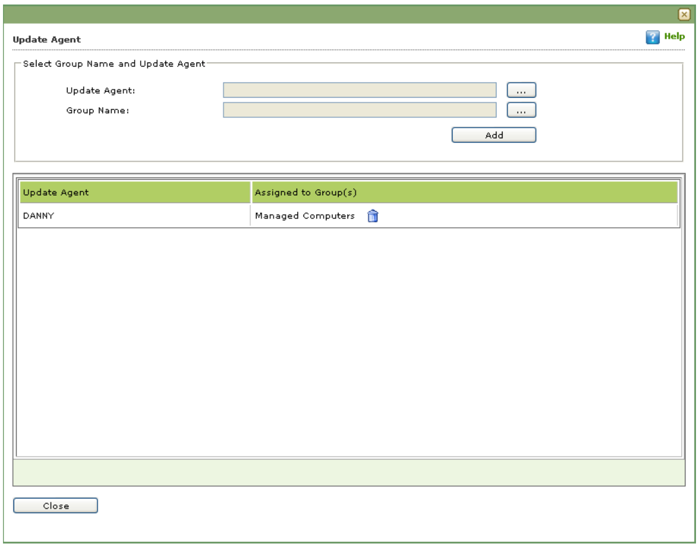


Update Agent: DANNY

Group Name: Managed Computers

Update Agent	Assigned to Group(s)

8. Update Agent will be created for the selected group and detail will be displayed on the interface, as shown below –



Update Agent	Assigned to Group(s)
DANNY	Managed Computers 🗑

9. Click on 🗑 in case if you wish to remove the selected endpoint as update agent.
10. Update Agent will be removed instantly.

Managing Installations

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

This section will give you an overview on following activities –

- **Installing eScan Client** - eScan client can be installed on computers connected to the network in the following ways

    - **Remote Installation** – It allows you to install eScan Client on all the computers in a selected group at once. You can initiate and monitor eScan Client installation using eScan Management Console. **For more click here**

    - **Manual Installation** – In case remote installation fails, you can allow computer users to install eScan client manually on their computers. It does not require any remote assistance. **For more Click here**

    - **Installing eScan using agent** - Installation of agent ensures that you have Administrator rights on the computer and you can now remotely install eScan Client on that computer. **For more click here**

- **Installing other Software (3rd Party software)** – eScan Management Console allows you to install third party software on networked computers remotely. **For more click here**.

- **Deploying hotfixes** - Using this option you can deploy hotfixes that eScan Server has downloaded from eScan website. This option is highlighted only when downloaded hotfix is saved in program files\escan\wgwin folder.

- **Uninstall eScan Client** – Using this option you can uninstall eScan Client from selected endpoint.

- **Connecting to the Client** – Using this option you can take the remote access of the selected Client Computer.

- **Move from Group** - Using this option you can move selected endpoint from one group to other.

- **Remove from Group** - Using this option you can remove selected endpoint from the group.

- **Viewing Installed Software List** – Using this option you can view list of software installed on Endpoints connected to your network.

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

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

- **Send Message**

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

- **Sending a message to client:**

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

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

- **Outbreak Prevention**

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

- **Deploy Outbreak Prevention**

Administrator can define following policies:

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

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

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

    - **Block All Ports (Other than trusted client-server ports):** Select this option and it will block all the ports except the trusted client-server ports in case of a virus outbreak.

    - **Automatically restore outbreak prevention:** The administrator can set the hours (using the dropdown) after which the system will automatically restore the outbreak prevention settings.

  - **Restore Outbreak Prevention**

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

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

  - **Delete All Quarantine Files** - Using this option you can Delete all Quarantined Files from Selected Endpoint.

  - **Change Client System File -** Using this option you can sync clock of managed endpoint with that of eScan Server.

- **Remote Installation of eScan Client –**

  - **Preparing Client Computer for Remote Deployment**

    To install eScan ISS for Business on the client system, check if the basic system requirements are in place.

  - **Configuring the settings on -**

    - **Windows XP Professional systems (Windows XP, 2000, 2003, all editions)**

      1. Click **Start**, and then click **Control Panel**.
      2. Double-click the **Administrative Tools** icon.
      3. Double-click the **Local Security Policy** icon.
      4. On the navigation pane, click **Local Policies** folder, and then click **Security Options** folder.

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

- **For Windows XP Home:**

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

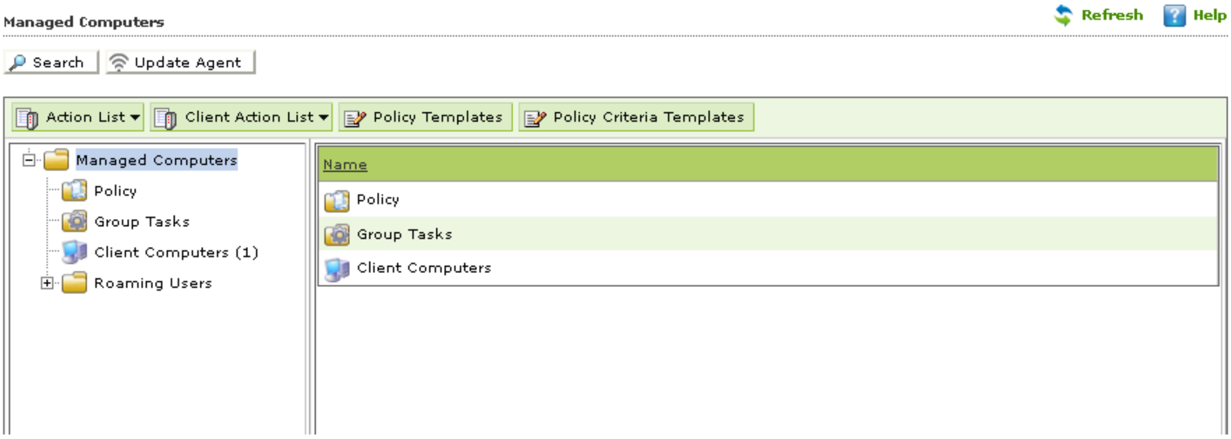
- **For Windows Vista /Windows 7 / Windows 8 / Windows 8.1**

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

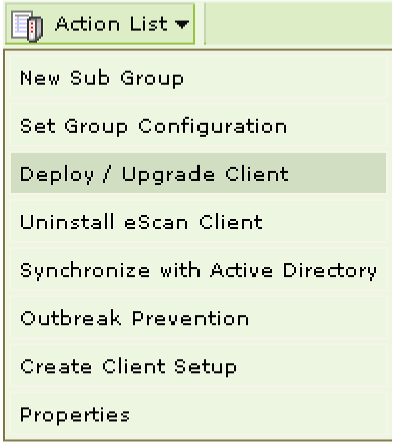
You can install eScan remotely on any computer or group present in Managed Computer using the following simple steps –

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

1. Click Managed Computer and select the **Group** where you wish to install eScan Client.

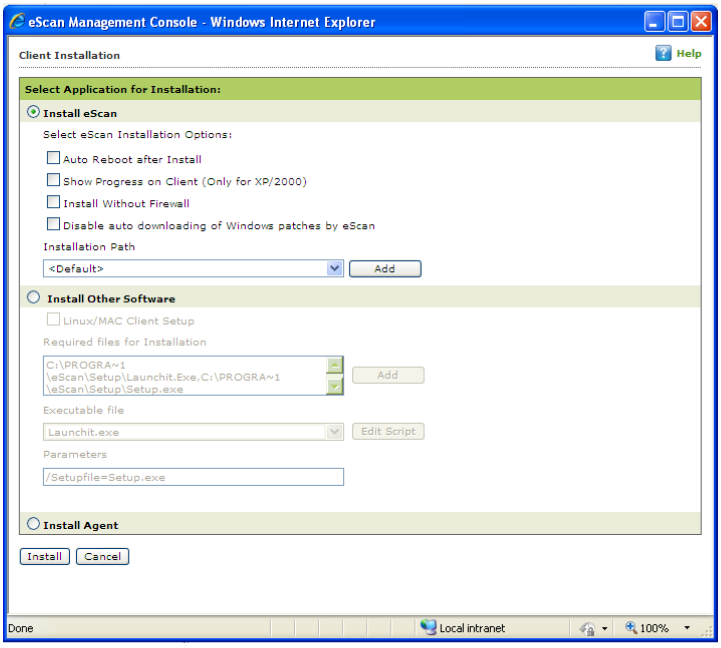


2. Now click **Deploy/ Upgrade Client** option present in the Action List drop down menu.



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

3. You will be forwarded to Client Installation Window, select the desired options and Click **install**.



Client Installation

Select Application for Installation:

● Install eScan

Select eScan Installation Options:

□ Auto Reboot after Install

□ Show Progress on Client (Only for XP/2000)

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default>

○ Install Other Software

□ Linux/MAC Client Setup

Required files for Installation: C:\PROGRA~1\eScan\Setup\Launchit.Exe,C:\PROGRA~1\eScan\Setup\Setup.exe

Executable file: Launchit.exe

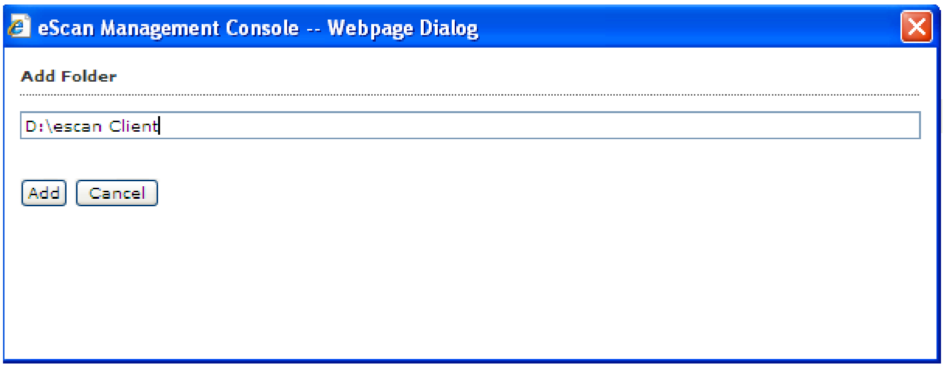
Parameters: /Setupfile=Setup.exe

○ Install Agent

4. By Default eScan is installed at the following Path on managed endpoint.

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

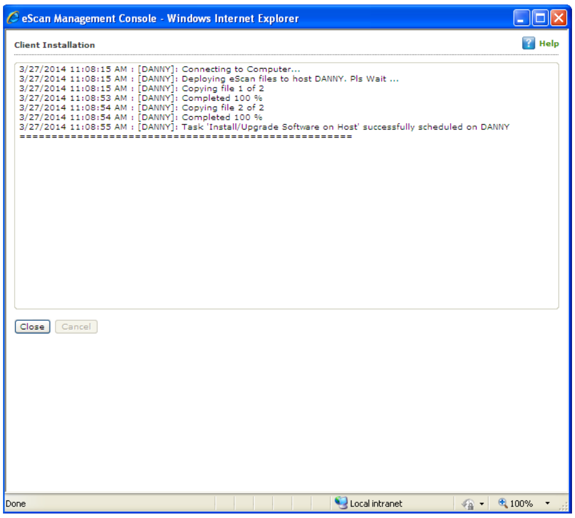
5. You can also define the installation path where you wish to install eScan using the **Add** option.



Add Folder

D:\escan Client

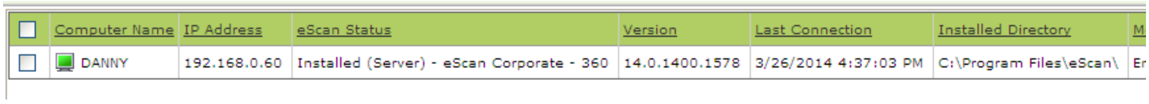
6. Click **Install**.
7. The progress of File transfer will be displayed.
8. The progress of File transfer will be displayed.



Client Installation

```
3/27/2014 11:08:15 AM : [DANNY]: Connecting to Computer...
3/27/2014 11:08:15 AM : [DANNY]: Deploying eScan files to host DANNY. Pls Wait ...
3/27/2014 11:08:15 AM : [DANNY]: Copying file 1 of 2
3/27/2014 11:08:53 AM : [DANNY]: Completed 100 %
3/27/2014 11:08:54 AM : [DANNY]: Copying file 2 of 2
3/27/2014 11:08:54 AM : [DANNY]: Completed 100 %
3/27/2014 11:08:55 AM : [DANNY]: Task 'Install/Upgrade Software on Host' successfully scheduled on DANNY
====================================================
```

9. After Installation the eScan status will be updated in Managed Computers list “**Installed (Client) – eScan ISS for Business**”.



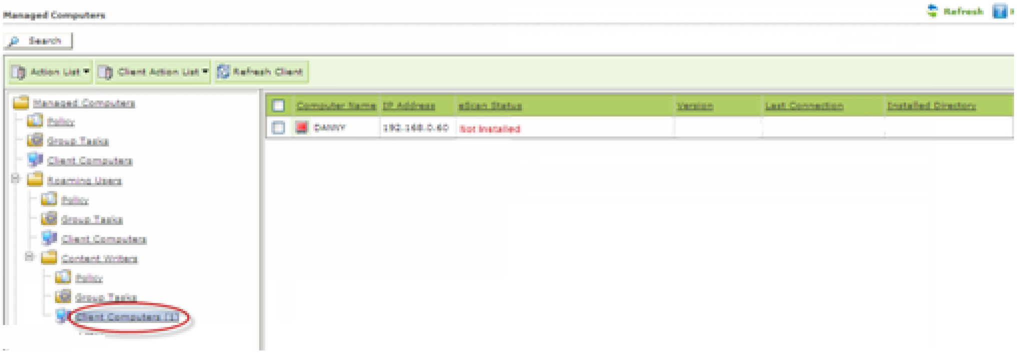
□	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory	M
□	DANNY	192.168.0.60	Installed (Server) - eScan Corporate - 360	14.0.1400.1578	3/26/2014 4:37:03 PM	C:\Program Files\eScan\	Er

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

1. Click Managed Computer.

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

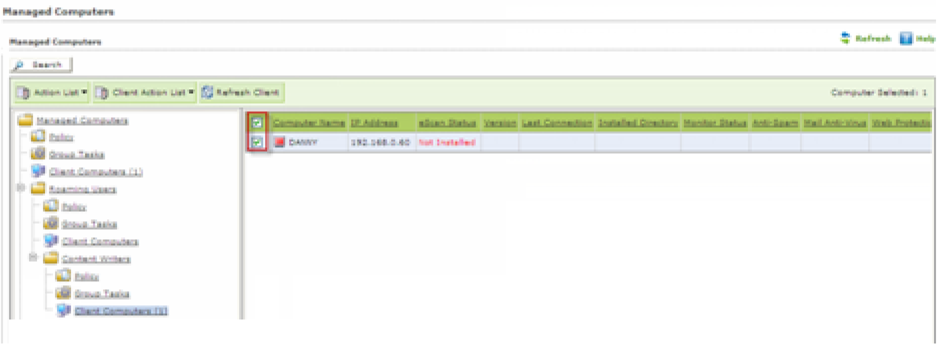
3. Click **Client Computers** option present under the Group tree.



Managed Computers

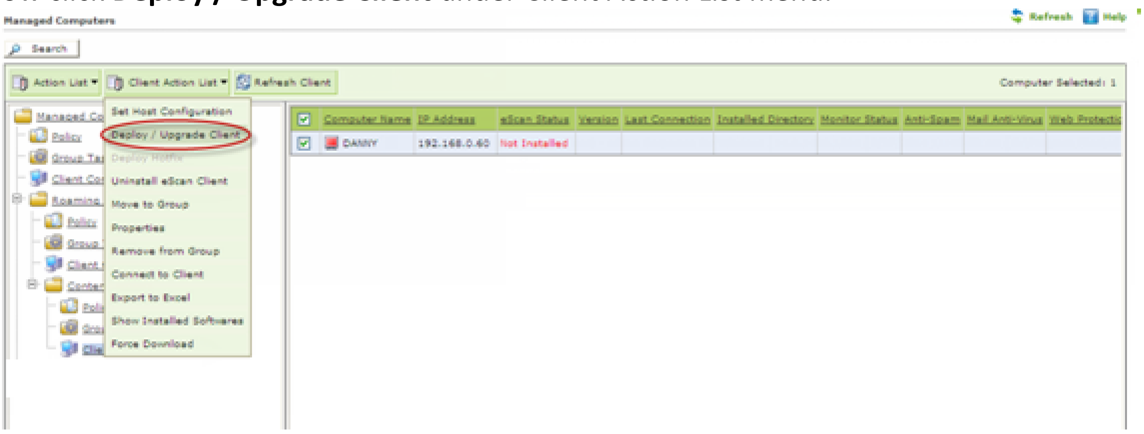
□	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory
□	DANNY	192.168.0.60	Not Installed			

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



☑	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web Protectio
☑	DANNY	192.168.0.60	Not Installed							

5. Now click **Deploy / Upgrade Client** under Client Action List menu.



☑	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web Protectio
☑	DANNY	192.168.0.60	Not Installed							

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

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

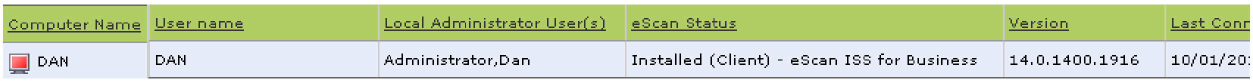
8. By Default eScan is installed at the following Path on Client computer.

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

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

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

    After installation eScan status will be "**Installed (Client) –eScan ISS for Business**".



Computer Name	User name	Local Administrator User(s)	eScan Status	Version	Last Conn
DAN	DAN	Administrator,Dan	Installed (Client) - eScan ISS for Business	14.0.1400.1916	10/01/20

- **eScan Client Protection Status**

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

- **Viewing Properties of a Group**

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

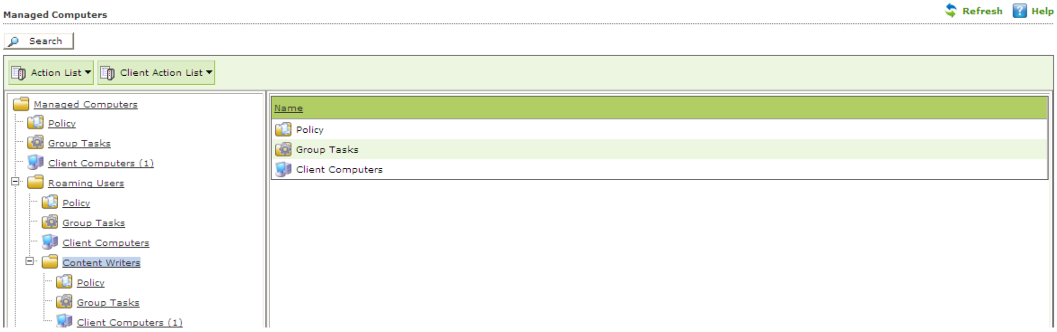
- **General Tab**

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

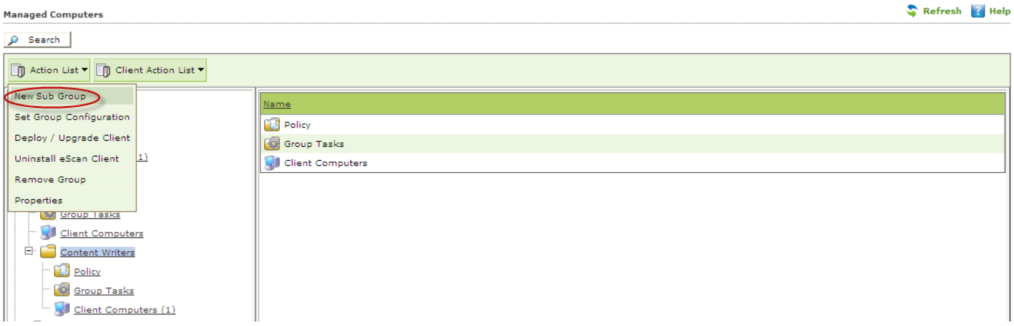
- **Creating Sub Groups**

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

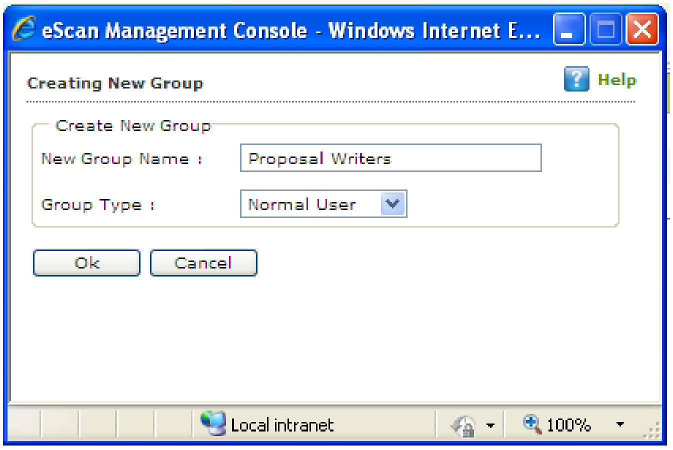
1. Click **Managed Computers.**
2. Select the Group under which you wish to create a **Sub Group**.



3. Now click **New Sub Group** under **Action List** menu.



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



Creating New Group

Create New Group

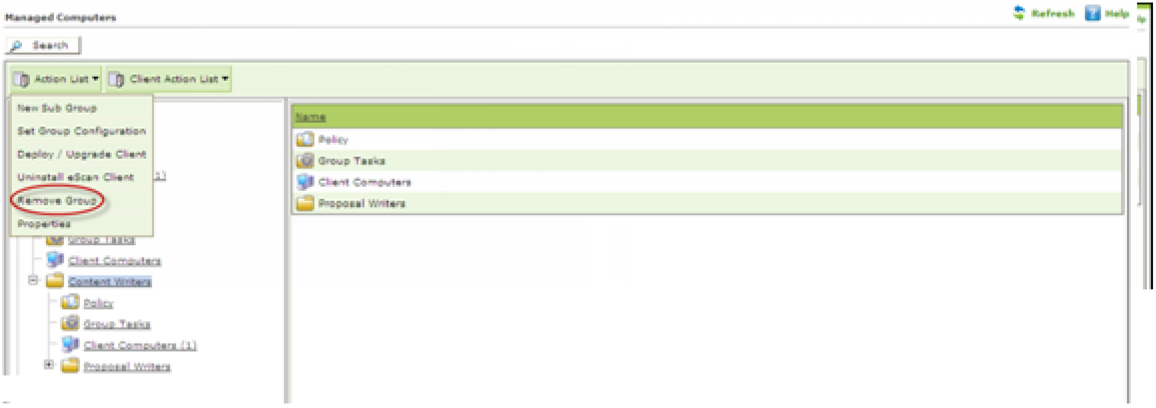
New Group Name : Proposal Writers

Group Type : Normal User

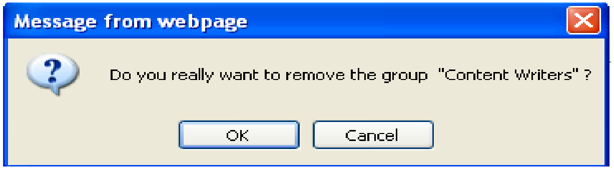
5. The created group will be added under the Parent Group.

- **Removing a Group**

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



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


Message from webpage

Do you really want to remove the group "Content Writers" ?

- **Setting Group Configuration**

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

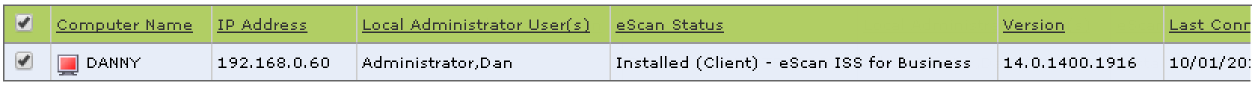
1. Click **Managed Computers**.
2. Now Select the Group for setting the Configuration.
3. Now click **Set Group Configuration** under **Action List** dropdown menu.
4. Now define the Username and Password for the group and click **Save**.
5. The settings will be configured instantly.

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

- **Refreshing Client**

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

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



☑	Computer Name	IP Address	Local Administrator User(s)	eScan Status	Version	Last Conr
☑	🟥 DANNY	192.168.0.60	Administrator,Dan	Installed (Client) - eScan ISS for Business	14.0.1400.1916	10/01/20

3. Now click **Refresh Client**.

4. The Status will be refreshed once the process is over.

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

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

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

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

Use the following Steps to view installed software on client computers --

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

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

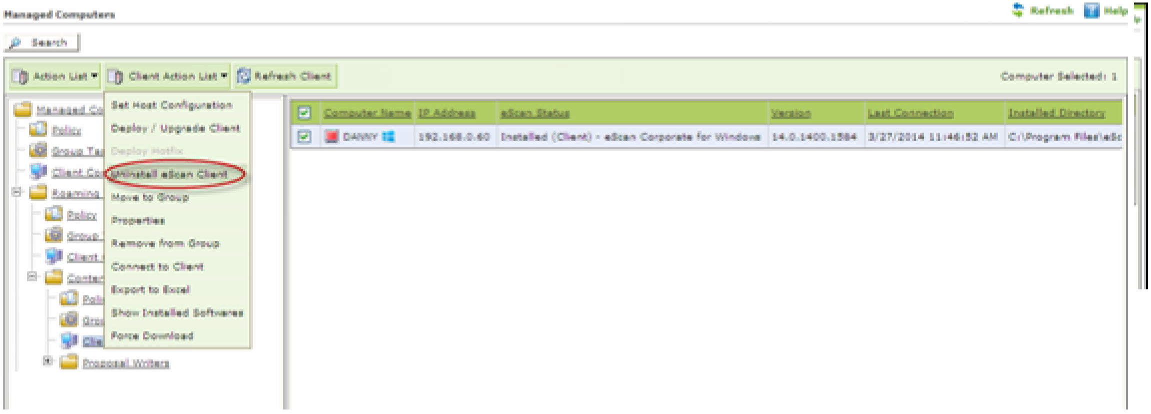
Use the following Steps to remove selected computers from a group --

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

- **Uninstalling eScan Client**

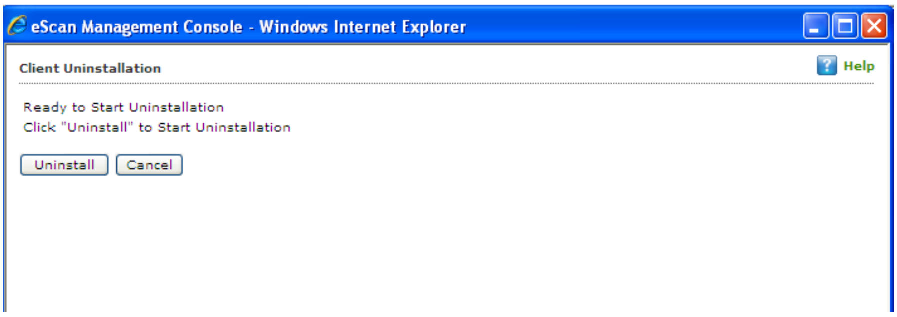
Use the following simple steps for uninstalling eScan Client on any networked computer.

1. Select the Computer and click **Uninstall eScan Client** under Client Action List menu.



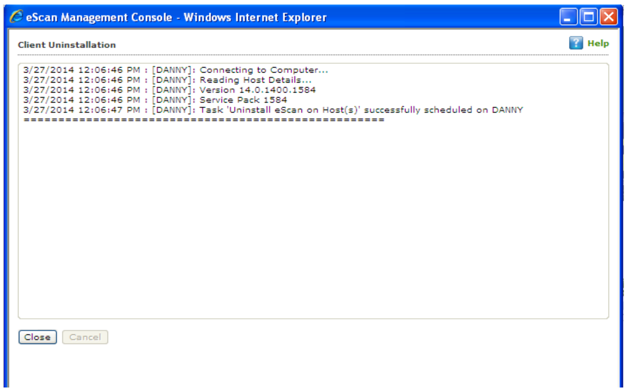
☑	Computer Name	IP Address	eScan Status	Version	Last Connection	Installed Directory
☑	DANNY	192.168.0.60	Installed (Client) - eScan Corporate for Windows	14.0.1400.1584	3/27/2014 11:46:52 AM	C:\Program Files\eSc

2. You will be forwarded to the **Client Uninstallation** window



Ready to Start Uninstallation
Click "Uninstall" to Start Uninstallation

3. The task will start instantly. **eScan Management Console** will display the progress details.



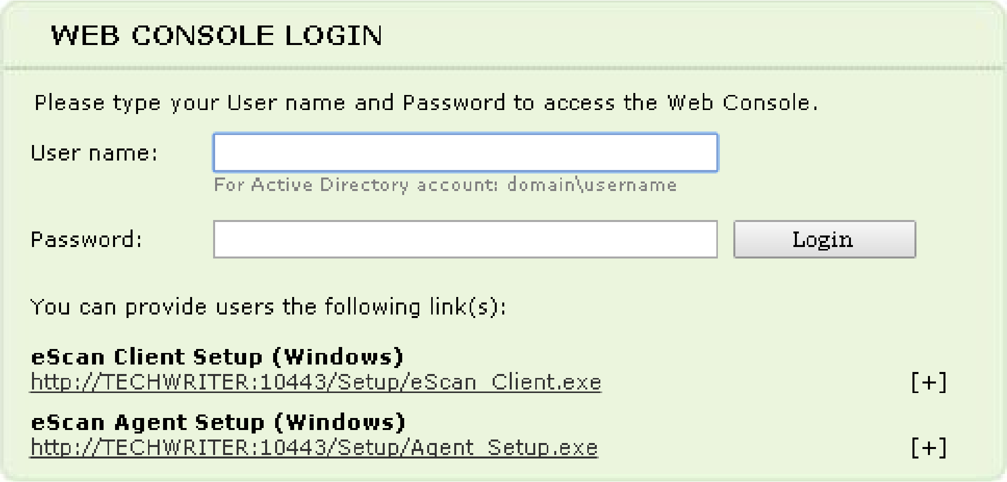
```
3/27/2014 12:06:46 PM : [DANNY]: Connecting to Computer...
3/27/2014 12:06:46 PM : [DANNY]: Reading Host Details...
3/27/2014 12:06:46 PM : [DANNY]: Version 14.0.1400.1584
3/27/2014 12:06:46 PM : [DANNY]: Service Pack 1584
3/27/2014 12:06:47 PM : [DANNY]: Task 'Uninstall eScan on Host(s)' successfully scheduled on DANNY
====================================================
```

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

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

- **Manually Installing eScan Client on Network Computers**

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



WEB CONSOLE LOGIN

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

User name:

For Active Directory account: domain\username

Password:

You can provide users the following link(s):

eScan Client Setup (Windows)
http://TECHWRITER:10443/Setup/eScan_Client.exe [+]

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

Copyright ©2015 MicroWorld Technologies Inc. All rights reserved.

Forward this link to the user of the Client computer on mail and guide him through the installation process.

Also check - Show Client Setup Link

- **Installing eScan client using agent**

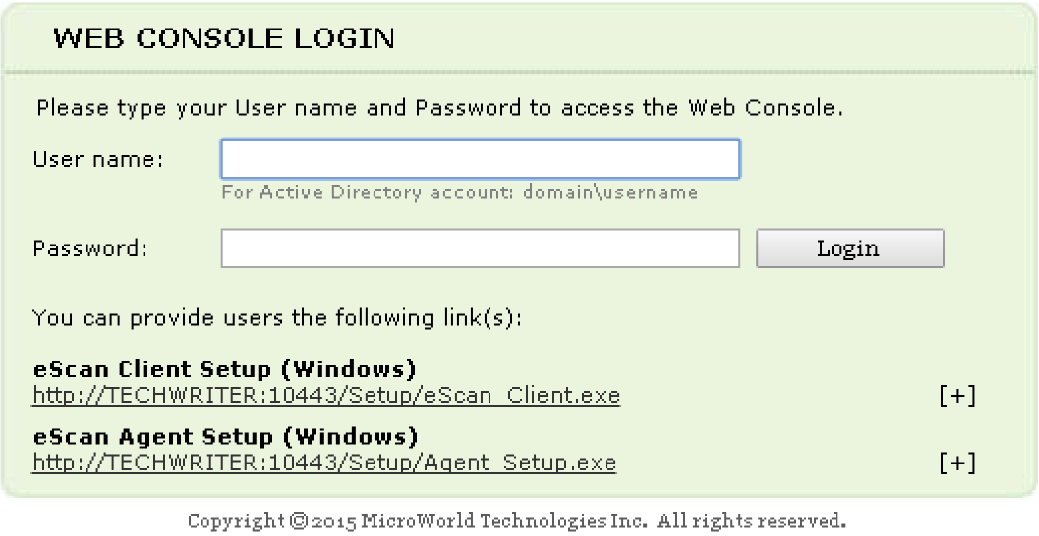
Use the following simple steps to install eScan using agent --

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

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

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

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



WEB CONSOLE LOGIN

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

User name:

For Active Directory account: domain\username

Password:

Login

You can provide users the following link(s):

eScan Client Setup (Windows)
http://TECHWRITER:10443/Setup/eScan_Client.exe [+]

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

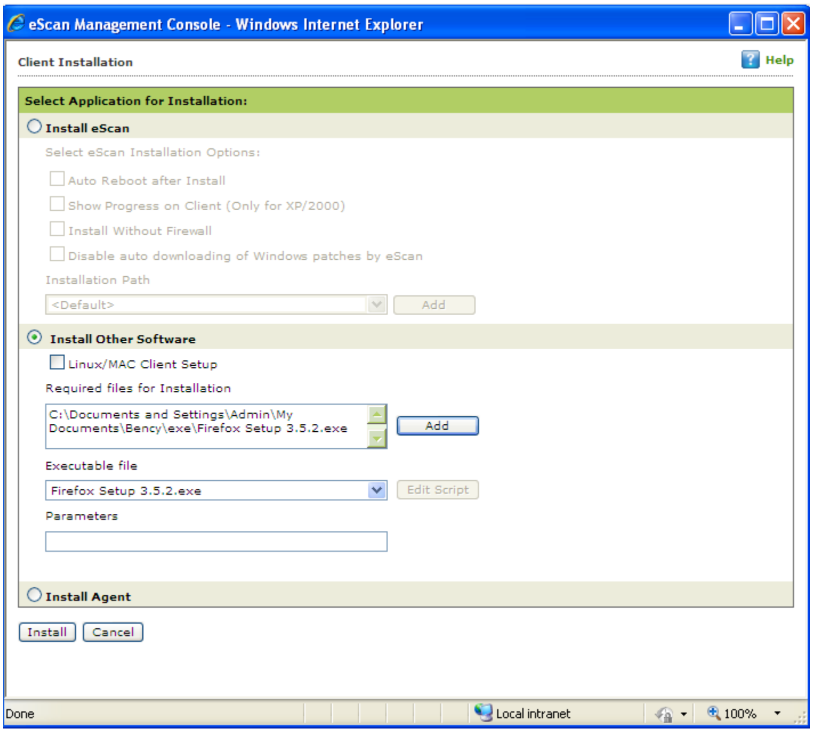
Copyright © 2015 MicroWorld Technologies Inc. All rights reserved.

Also check - Show Agent Setup Link

- **Installing other Software (3rd Party Software)**

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

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

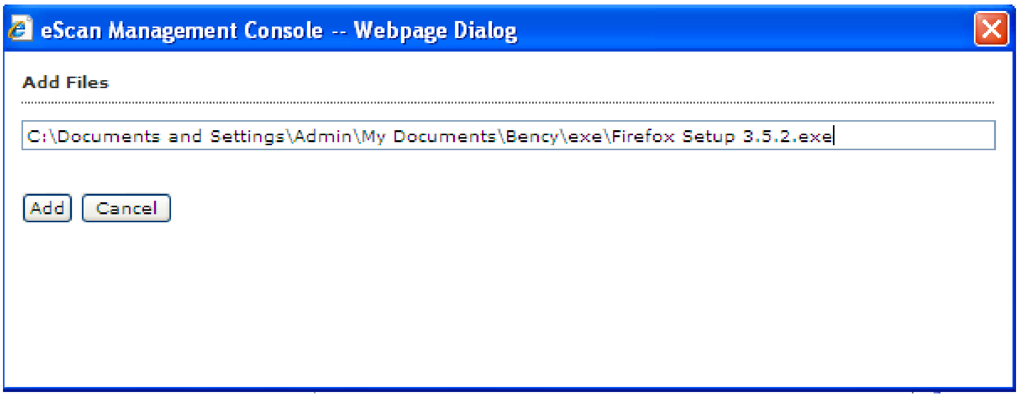


eScan Management Console - Windows Internet Explorer
Client Installation
Help
Select Application for Installation:
○ Install eScan
Select eScan Installation Options:
□ Auto Reboot after Install
□ Show Progress on Client (Only for XP/2000)
□ Install Without Firewall
□ Disable auto downloading of Windows patches by eScan
Installation Path
<Default>
Add
● Install Other Software
□ Linux/MAC Client Setup
Required files for Installation
Add
Executable file
Edit Script
Parameters
○ Install Agent
Install
Cancel
Done
Local intranet
100%

Required files for Installation: C:\Documents and Settings\Admin\My Documents\Bency\exe\Firefox Setup 3.5.2.exe

Executable file: Firefox Setup 3.5.2.exe

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

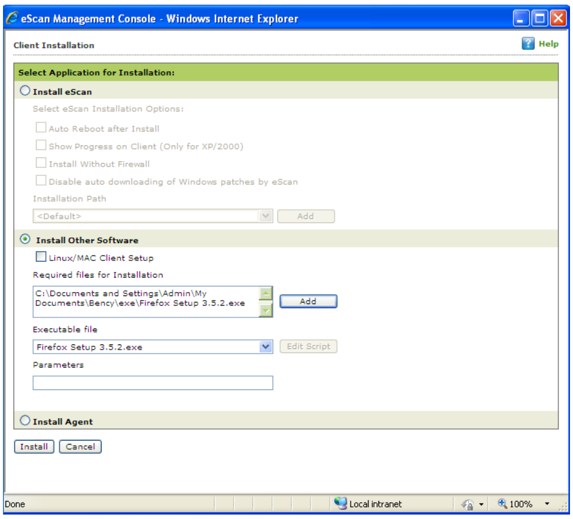


eScan Management Console -- Webpage Dialog

Add Files

C:\Documents and Settings\Admin\My Documents\Bency\exe\Firefox Setup 3.5.2.exe

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



eScan Management Console - Windows Internet Explorer

Client Installation

Select Application for Installation:

○ Install eScan

Select eScan Installation Options:

□ Auto Reboot after Install

□ Show Progress on Client (Only for XP/2000)

□ Install Without Firewall

□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default>

● Install Other Software

□ Linux/MAC Client Setup

Required files for Installation

C:\Documents and Settings\Admin\My Documents\Bency\exe\Firefox Setup 3.5.2.exe

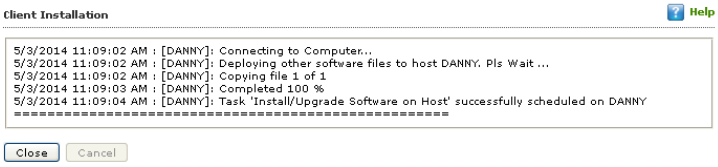
Executable file

Firefox Setup 3.5.2.exe

Parameters

○ Install Agent

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



Client Installation

```
5/3/2014 11:09:02 AM : [DANNY]: Connecting to Computer...
5/3/2014 11:09:02 AM : [DANNY]: Deploying other software files to host DANNY. Pls Wait ...
5/3/2014 11:09:02 AM : [DANNY]: Copying file 1 of 1
5/3/2014 11:09:03 AM : [DANNY]: Completed 100 %
5/3/2014 11:09:04 AM : [DANNY]: Task 'Install/Upgrade Software on Host' successfully scheduled on DANNY
====================================================
```

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

Managing Policies and Tasks for the Group

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

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

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

Modules	Description
File Anti-virus	This would scan all the existing files and folders for any infection. It will allow you to report / disinfect/ quarantine/delete objects. This will also save a copy of report file for future reference, and will display alert messages.
Anti-Spam	This will prevent you from receiving spam mails by checking the content of outgoing and incoming mails, quarantines or deletes the mails based on the phrases added and allows mails based on the whitelist settings.
Firewall	This will help you in putting up a restriction to incoming and outgoing traffic and hacking. You can define the firewall settings here. You can define the IP range, permitted applications, trusted MAC addresses and local IP addresses.
Privacy Control	This will allow you to schedule an auto erase of your cache, ActiveX, cookies, plugins, and history. You can also secure delete your files and folders where the files will be deleted directly and no traces of that could be found.
Mail Anti-Virus	This will allow you to analyze all the incoming mails. This analyses the mails by breaking it into three sections the header, subject and the body.
Endpoint Security	This will control the devices from the point of end users by allowing/ restricting USB, white listing.

Steps for Defining Policy templates for the group

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

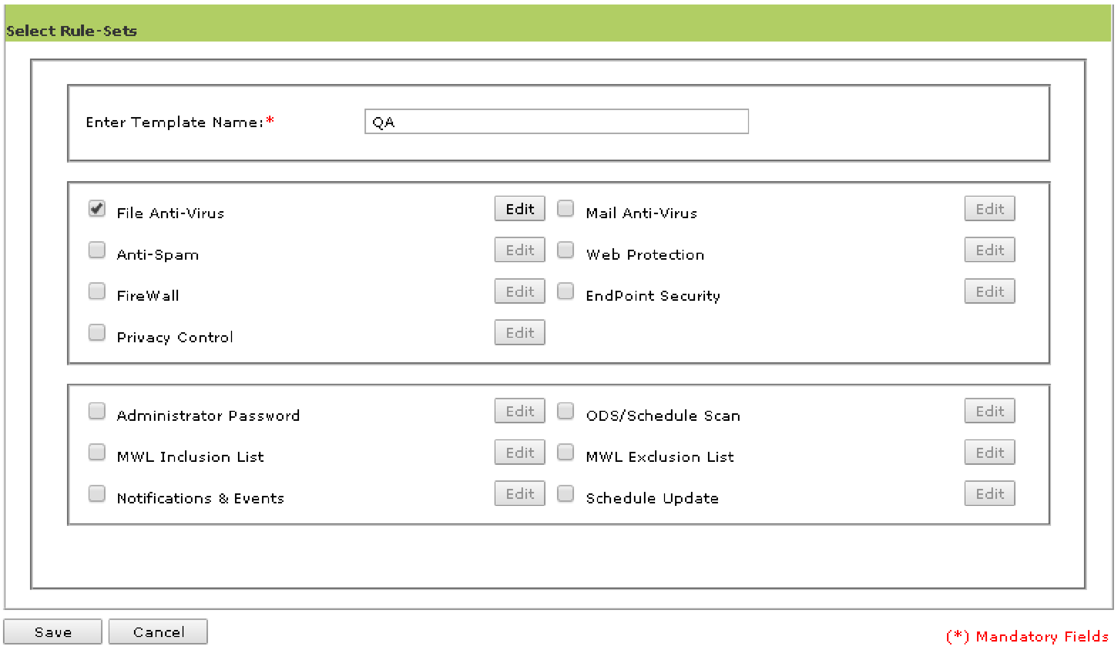
- **Assign to Group(s):** This option will allow you to assign the policy template to group(s). All the policies that are defined in the particular template will be applied to the group(s).
- **Assign to Computer(s):** This option will allow you to assign the policy template to specific computer(s).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

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

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

Rule – Sets for Policy templates

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



Select Rule-Sets

Enter Template Name:* QA

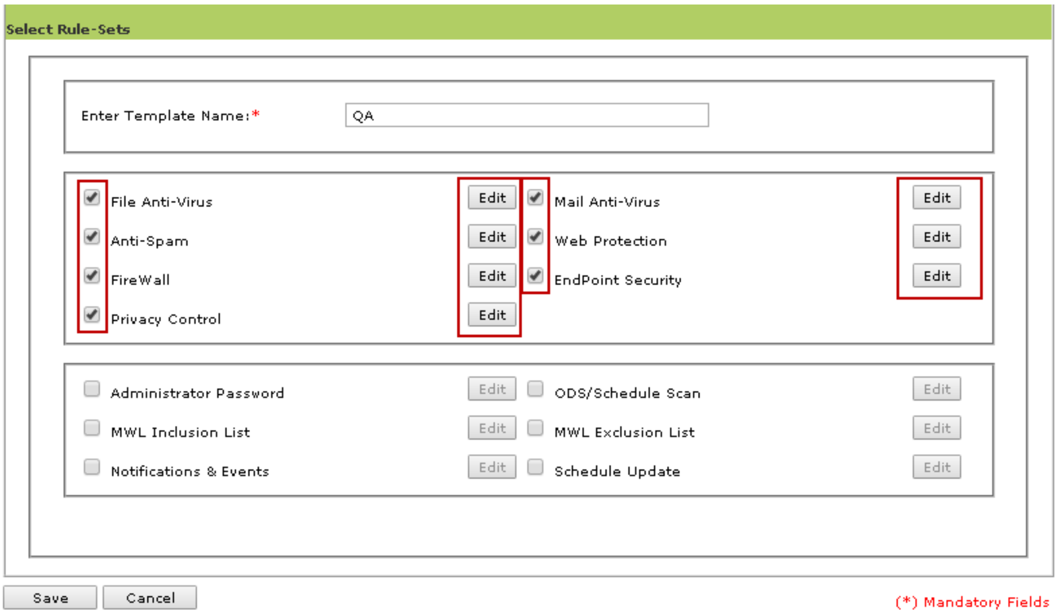
☑ File Anti-Virus Edit
□ Mail Anti-Virus Edit
□ Anti-Spam Edit
□ Web Protection Edit
□ FireWall Edit
□ EndPoint Security Edit
□ Privacy Control Edit

□ Administrator Password Edit
□ ODS/Schedule Scan Edit
□ MWL Inclusion List Edit
□ MWL Exclusion List Edit
□ Notifications & Events Edit
□ Schedule Update Edit

Save Cancel

(*) Mandatory Fields

- Select the Module in the group and click **Edit** to define the policies for the Module.



Select Rule-Sets

Enter Template Name:* QA

☑ File Anti-Virus [Edit] ☑ Mail Anti-Virus [Edit]
☑ Anti-Spam [Edit] ☑ Web Protection [Edit]
☑ FireWall [Edit] ☑ EndPoint Security [Edit]
☑ Privacy Control [Edit]

□ Administrator Password [Edit] □ ODS/Schedule Scan [Edit]
□ MWL Inclusion List [Edit] □ MWL Exclusion List [Edit]
□ Notifications & Events [Edit] □ Schedule Update [Edit]

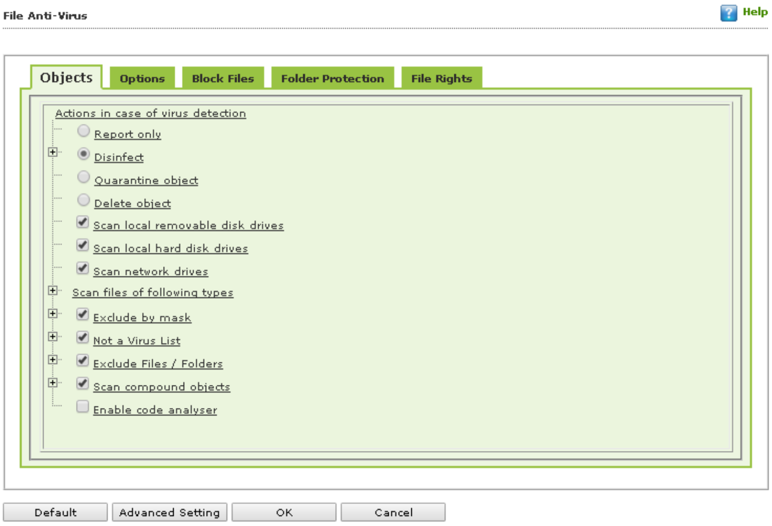
[Save] [Cancel] (*) Mandatory Fields

- You will be forwarded to a page where you can define actions and policies specifically for that module which you wish to be implemented on all Endpoints in that group. **eScan Management Console** allows you to define policy template for every option present in all the Modules of eScan Client . All Policies are automatically implemented after next update on the endpoints.

  Configurable Policies for the endpoints

1. File Anti-Virus

Objects



File Anti-Virus Help

Objects | Options | Block Files | Folder Protection | File Rights

Actions in case of virus detection
- ○ Report only
- ● Disinfect
- ○ Quarantine object
- ○ Delete object
- ☑ Scan local removable disk drives
- ☑ Scan local hard disk drives
- ☑ Scan network drives
- Scan files of following types
- ☑ Exclude by mask
- ☑ Not a Virus List
- ☑ Exclude Files / Folders
- ☑ Scan compound objects
- □ Enable code analyser

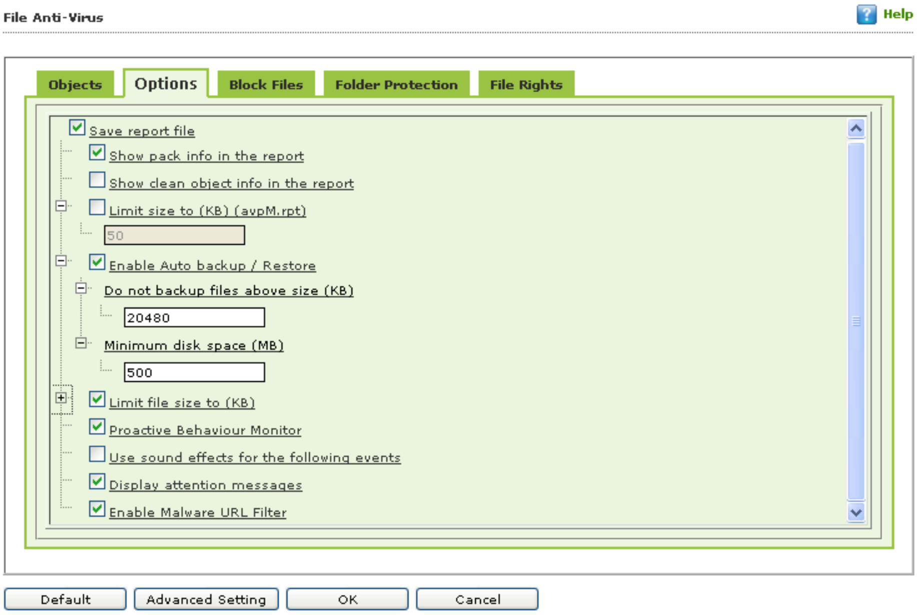
[Default] [Advanced Setting] [OK] [Cancel]

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

- **Actions in case of virus detection:** This section lists the different actions that File Anti- Virus can perform when it detects a virus infection. These actions are Report only, Disinfect, Quarantine, and Delete object. Out of these, the **Disinfect** option is selected by default. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected folder**

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

> Options



File Anti-Virus

- ☑ Save report file
  - ☑ Show pack info in the report
  - ☐ Show clean object info in the report
  - ☐ Limit size to (KB) (avpM.rpt)
    - 50
  - ☑ Enable Auto backup / Restore
    - Do not backup files above size (KB)
      - 20480
    - Minimum disk space (MB)
      - 500
  - ☑ Limit file size to (KB)
  - ☑ Proactive Behaviour Monitor
  - ☐ Use sound effects for the following events
  - ☑ Display attention messages
  - ☑ Enable Malware URL Filter

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

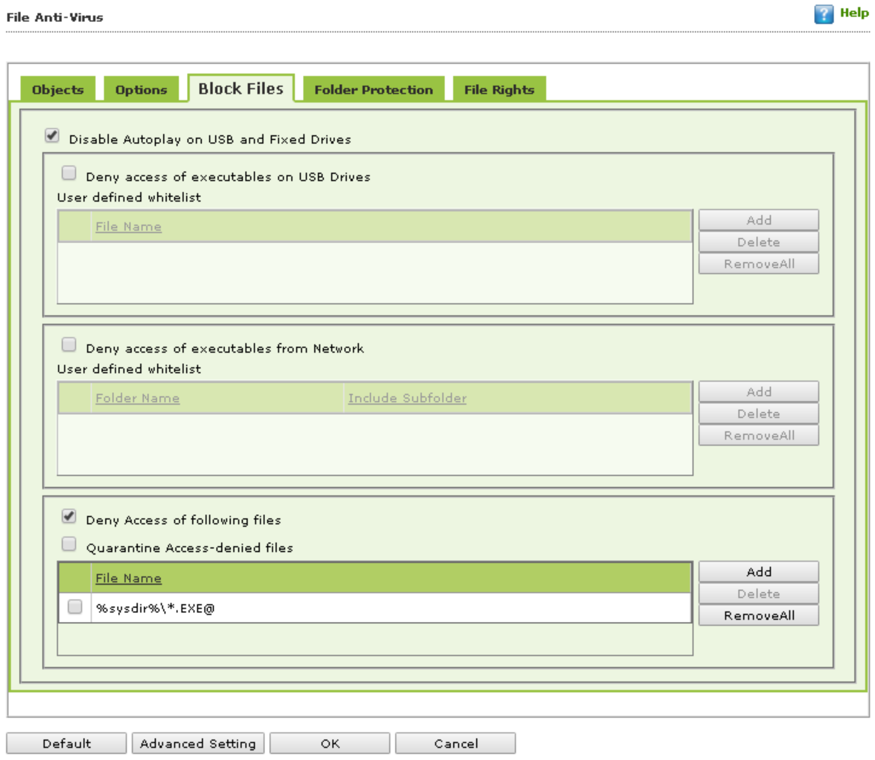
You can configure the following settings:

- **Save report file: *[Default]*-** Select this check box if you need eScan to save the reports generated by the File Anti-Virus module. The report file logs information about the scanned files and the action taken by File Anti-Virus when an infected file was found during the scan.
- **Show pack info in the report: *[Default]* -** Select this check box if you need File Anti-Virus to add information regarding scanned compressed files, such as .ZIP and .RAR files to the Monvir.log file.
- **Show clean object info in the report:** Select this check box if you need File Anti-Virus to add information regarding uninfected files found during a scan operation to the Monvir.log file. You can select this option to find out which files are not infected.
- **Limit size to (Kb) (avpM.rpt):** Select this check box if you need File Anti-Virus to limit the size of the Monvir.log file and avpM.rpt file. You can double-click the size box and specify the size of the log file.
- **Enable Auto backup / Restore: *[Default]* :** Select this check box to back up the critical files of the Windows® operating system installed on your computer and then automatically restores the clean files when eScan finds an infection in any of the system files that cannot be disinfected. You can do the following settings:
- **Do not backup files above size (KB): *[Default]* –** Select this check box to prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified.
- **Minimum disk space (MB)**: *[Default]* eScan Auto-backup will first check for the minimum available space limit defined for a hard disk drive. If the minimum defined space is available then only the Auto-backup will function, if not it will

stop without notifying. You can allot the minimum disk space to be checked from this option.

- **Limit file size to (KB):** ***[Default]*** Select this checkbox to set a size limit for the objects or files to be scanned. The default value is set to **20480 Kb**.
- **Proactive Behaviour monitor:** Select this check box for File Anti-Virus to monitor your computer for suspicious applications and prompts you to block such applications when they try to execute.
- **Use sound effects for the following events:** Select this checkbox to configure eScan to play a sound file and show you the details regarding the infection within a message box when any malicious software is detected by File Anti-Virus. However, you need to ensure that the computer's speakers are switched on.
- **Display attention messages:** ***[Default]*** Select this checkbox to display an alert; it will display the path and name of the infected object and the action taken by the File Anti-Virus module.
- **Enable Malware URL Filter:** Select this checkbox to display an alert in case a malicious URL has been detected.

> Block Files



☑ Disable Autoplay on USB and Fixed Drives

□ Deny access of executables on USB Drives

User defined whitelist

File Name

□ Deny access of executables from Network

User defined whitelist

Folder Name	Include Subfolder

☑ Deny Access of following files

□ Quarantine Access-denied files

	File Name
□	%sysdir%*.EXE@

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

You can configure the following settings:

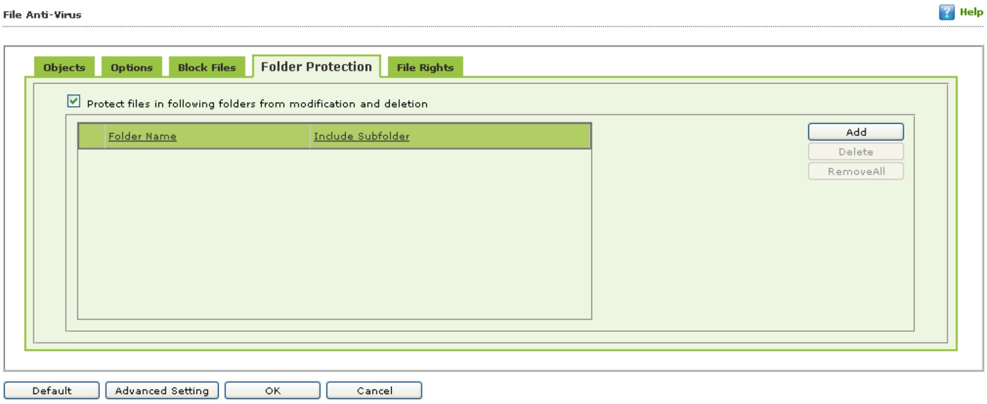
- **Disable Autoplay on USB and Fixed Drives:** Select this check box to prevent the automatic execution of the files on USB and Fixed Drives.
- **Deny access of executables on USB Drives:** Select this check box if you need to prevent executables stored on USB drives from being accessed.
- **Deny access of executable from Network:** Select this check box if you need to prevent executables on the client computer from being accessed from the network.

- **User defined whitelist:** This option is effective when the **Deny access of executable from Network** tab is enabled. You can use this option to enter the folders that need to be whitelisted so that executables can be accessed in the network from the folders mentioned under this list. You need to click the **Add** button.
- **Deny Access of following files:** [Default] - Select this check box if you need to prevent the files in the list from running on the Endpoints.
- **Quarantine Access-denied files**: You should select this check box if you need to quarantine files that have been denied access.

Add

- Enter the complete path of the folder to be whitelisted on the client systems. You can either whitelist the parent folder only or select the Include subfolder option for whitelisting the sub folders as well.
- You can prevent specific files from running on the eScan client computer by adding them to the Block Files list. By default, this list contains the value %sysdir%\\*.EXE@. You need to click the Add Button.
- Enter the full name of the file to be blocked from execution on the client systems.

Folder Protection



☑ Protect files in following folders from modification and deletion

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

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

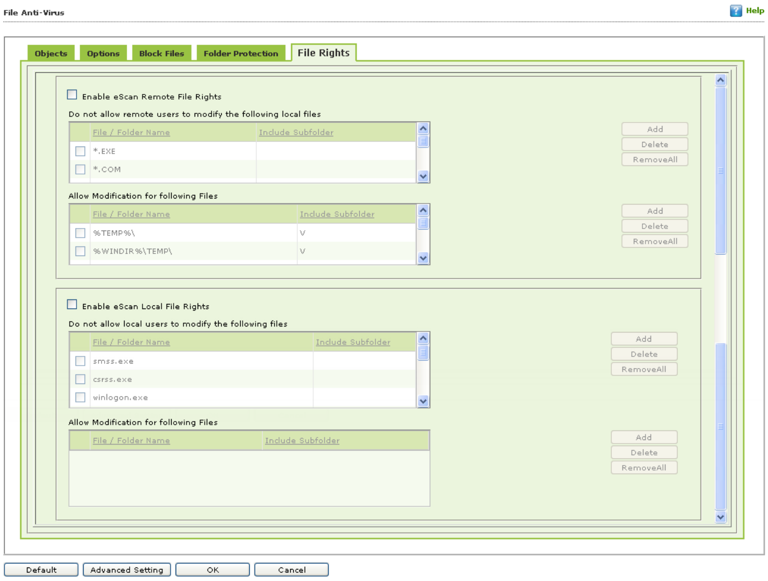
Add

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

Default

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

- **File Rights**



File Anti-Virus

Help

Objects | Options | Block Files | Folder Protection | File Rights

□ Enable eScan Remote File Rights

Do not allow remote users to modify the following local files

	File / Folder Name	Include Subfolder
□	*.EXE	
□	*.COM	

Add · Delete · RemoveAll

Allow Modification for following Files

	File / Folder Name	Include Subfolder
□	%TEMP%\	V
□	%WINDIR%\TEMP\	V

Add · Delete · RemoveAll

□ Enable eScan Local File Rights

Do not allow local users to modify the following files

	File / Folder Name	Include Subfolder
□	smss.exe	
□	csrss.exe	
□	winlogon.exe	

Add · Delete · RemoveAll

Allow Modification for following Files

	File / Folder Name	Include Subfolder

Add · Delete · RemoveAll

Default · Advanced Setting · OK · Cancel

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

Enable eScan Remote File Rights: Select this check box to allow/ restrict the remote users to make any modifications to the file.

Do not allow remote users to modify the following local files: The Files added to this list cannot be changes by the remote users.

Allow modification for following files: The files added to this list can be modified by the remote user.

Enable eScan local file rights: Select this checkbox to allow / restrict the local users to make any modifications to the file.

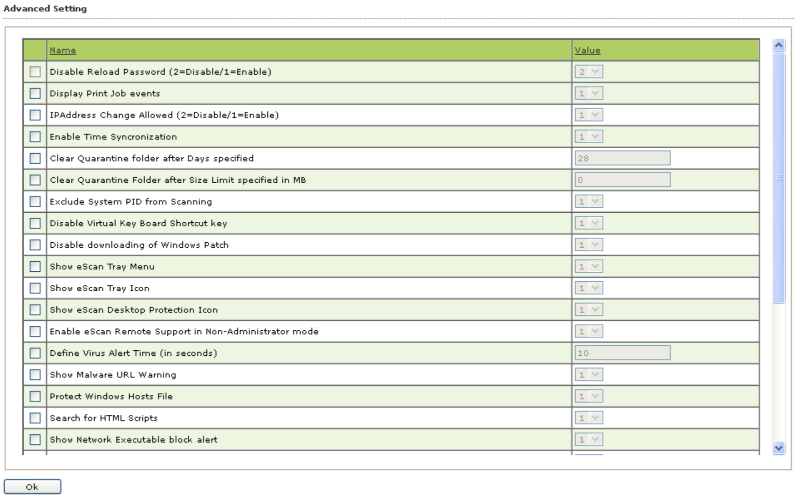
Do not allow local users to modify the following files: the files added to this list cannot be modified by the local users.

Allow modification for files: The files added to this list can be modified by the local users.

- **Add:** This will allow you to add the files or the folder path to the list
- **Delete:** This will remove the selected file or folder and subfolder from the list.
- **Remove all:** This will remove all the files and folders from the list.

- **Advanced Settings**

Using **Advanced Settings** option you can define Policies for more advanced options in eScan Client. These policies are defined in the .ini file or registry of the endpoints.

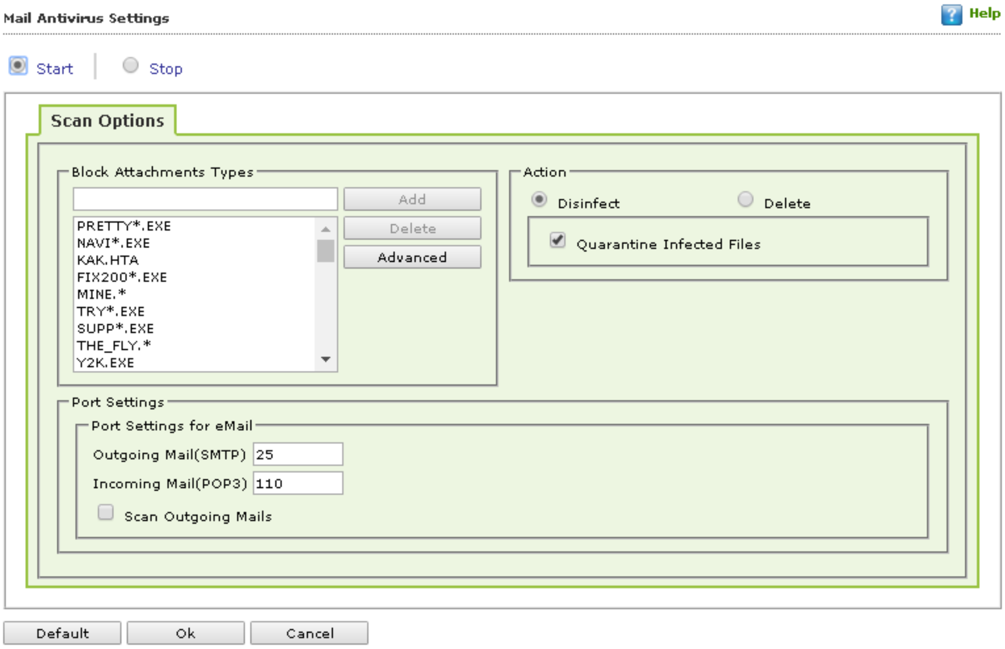


Advanced Setting

	Name	Value
□	Disable Reload Password (2=Disable/1=Enable)	2
□	Display Print Job events	1
□	IPAddress Change Allowed (2=Disable/1=Enable)	1
□	Enable Time Syncronization	1
□	Clear Quarantine folder after Days specified	28
□	Clear Quarantine Folder after Size Limit specified in MB	0
□	Exclude System PID from Scanning	1
□	Disable Virtual Key Board Shortcut key	1
□	Disable downloading of Windows Patch	1
□	Show eScan Tray Menu	1
□	Show eScan Tray Icon	1
□	Show eScan Desktop Protection Icon	1
□	Enable eScan Remote Support in Non-Administrator mode	1
□	Define Virus Alert Time (in seconds)	10
□	Show Malware URL Warning	1
□	Protect Windows Hosts File	1
□	Search for HTML Scripts	1
□	Show Network Executable block alert	1

It allows you to configure advanced settings for eScan.

Mail Anti-Virus



Mail Antivirus Settings

● Start | ○ Stop

Scan Options

Block Attachments Types

PRETTY*.EXE
NAVI*.EXE
KAK.HTA
FIX200*.EXE
MINE.*
TRY*.EXE
SUPP*.EXE
THE_FLY.*
Y2K.EXE

Action

● Disinfect ○ Delete

☑ Quarantine Infected Files

Port Settings

Port Settings for eMail

Outgoing Mail(SMTP) 25

Incoming Mail(POP3) 110

□ Scan Outgoing Mails

This module scans all incoming and outgoing emails for viruses, spyware, adware, and other malicious objects. It helps you send virus warnings to client computers on the Mail Anti- Virus activities. By default, Mail Anti -Virus scans only the incoming e mails and attachments, but you can configure it to scan outgoing e-mails and attachments as well. Moreover, it helps you notify the sender or system administrator whenever you receive an infected e-mail or attachment. This page provides you with options for configuring the module.

Scan Options

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

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

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

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

- **Port Settings for email:** Specify the ports for incoming and outgoing emails so that eScan can scan the emails sent or received through those ports.

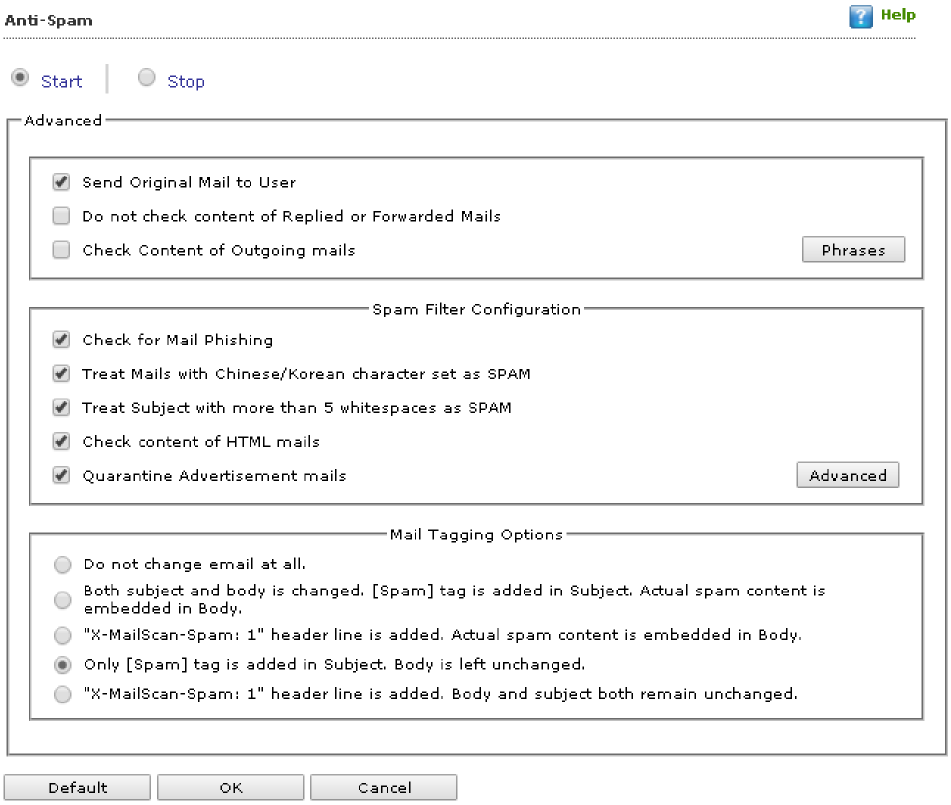
    1. **Outgoing Mail (SMTP):** ***[Default: 25]*** Specify a port number for SMTP.
    2. **Incoming Mail (POP3):** ***[Default: 110]*** Specify a port number for POP3.
    3. **Scan Outgoing Mails:** Select this check box if you need to Mail Anti-Virus to scan outgoing emails as well.

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

    - **Delete all Attachment in email if disinfection is not possible:** Select this check box if you need to delete all the email attachments that cannot be cleaned.
    - **Delete entire email if disinfection is not possible:** ***[Default]*** Select this check box if you need to delete the entire email if any attachment cannot be cleaned.
    - **Delete entire email if any virus is found:** Select this check box if you need to delete the entire email if any virus is found in the email or the attachment is infected.
    - **Quarantine blocked Attachments:** ***[Default]*** Select this check box if you need to quarantine the attachment if it has an extension that is blocked by eScan.
    - **Delete entire email if any blocked attachment is found:** ***[Default]*** **-** Select this check box if you need to delete an email if it contains an attachment with an extension type that is blocked by eScan.
    - **Quarantine email if attachments are not scanned:** Select this check box if you need to quarantine an entire email if it contains an attachment that is not scanned by Mail Anti-virus.
    - **Quarantine Attachments if they are scanned:** Select this check box if you need to quarantine attachments that are scanned by Mail Anti-virus.

- **Exclude Attachments (White List):** This list is empty by default. You can add file names and file extensions that should not be blocked by eScan. You can also configure eScan to allow specific files even though if the file type is blocked. For example, if you have listed *.PIF in the list of blocked attachments and you need to allow an attachment with the name ABC, you can add abcd.pif to the Exclude Attachments list. Add D.PIFing *.PIF files in this section will allow all *.PIF to be delivered. MicroWorld recommends you to add the entire file name like ABCD.PIF.

3. Anti – Spam


Anti-Spam

● Start | ○ Stop

Advanced

☑ Send Original Mail to User

☐ Do not check content of Replied or Forwarded Mails

☐ Check Content of Outgoing mails

Spam Filter Configuration

☑ Check for Mail Phishing

☑ Treat Mails with Chinese/Korean character set as SPAM

☑ Treat Subject with more than 5 whitespaces as SPAM

☑ Check content of HTML mails

☑ Quarantine Advertisement mails

Mail Tagging Options

○ Do not change email at all.

○ Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.

○ "X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.

● Only [Spam] tag is added in Subject. Body is left unchanged.

○ "X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.

This module filters all your junk and spam emails by using the NILP technology and sends content warnings to specified recipients. This page provides you with options for configuring the module. You can configure the following settings.

1. **Advanced**

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

- **Send Original Mail to User:** ***[Default]*** This check box is selected by default. eScan creates Spam folder within the email client. When an email is tagged as SPAM, it is moved to this folder. You should select this check box, if you need to send original email that is tagged as spam to the recipient as well.

- **Do not check content of Replied or Forwarded Mails:** You can select this check box, if you need to ensure that eScan does not check the contents of emails that you have either replied or forwarded to other recipients.
- **Check Content of Outgoing mails:** You can select this check box, if you need Anti-Spam to check outgoing emails for restricted content.
- **Phrases:** You can click the **Phrases** button to open the **Phrases** dialog box. This dialog box helps you configure additional email related options. In addition, it allows you to specify a list of words that the user can either allow or block. This list is called the **user specified whitelist**. You can specify certain words or phrases so that mails containing those words or phrases in the subject, header, or body are recognized as spam and are quarantined or deleted.
- **User specified whitelist of words/phrases:** (Color Code: **GREEN**) Click this option to list the words or phrases that are present in the whitelist. A phrase that is added to the whitelist cannot be edited, enabled, or disabled.
- **User specified List of Blocked words/phrases:** (Color Code: **RED**) Click this option to list the words or phrases that are defined in block list.
- **User specified words/phrases disabled:** (Color Code: **GRAY**) Click this option to list the words or phrases that are defined excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

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

- **Check for Mail Phishing:** ***[Default]*** Select this check box, if you need Anti-Spam to check for fraudulent emails and quarantine them.
- **Treat Mails with Chinese /Korean character set as SPAM:** ***[Default]*** Select this checkbox to scan emails with Chinese or Korean characters. This is based on the research data conducted by MicroWorld’s various spam email samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their emails.
- **Treat Subject with more than 5 whitespaces as SPAM:** ***[Default]-*** Select this check box to check the spacing between characters or words in the subject line of emails and treat emails with more than five whitespaces in their subject lines as spam emails. MicroWorld had found in its research that spam emails usually contain more than five consecutive white spaces.
- **Check content of HTML mails:** ***[Default]*** Select this check box when you need Anti-Spam to scan emails in HTML format along with textual content.
- **Quarantine Advertisement mails:** ***[Default]-*** Select this check box when you need Anti-Spam to check for advertisement types of emails and quarantine them.
- **Advanced:** Click this button to open the **Advanced Spam Filtering Options** dialog box. This dialog box helps you configure the following advanced options for controlling spam.
- **Enable Non- Intrusive Learning Pattern (NILP) check: [Default]** NILP is MicroWorld’s revolutionary technology that uses Bayesian Filtering and works on the principles of

Artificial Intelligence (AI) to analyze each email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user. You should select this check box if you need to enable NILP check.

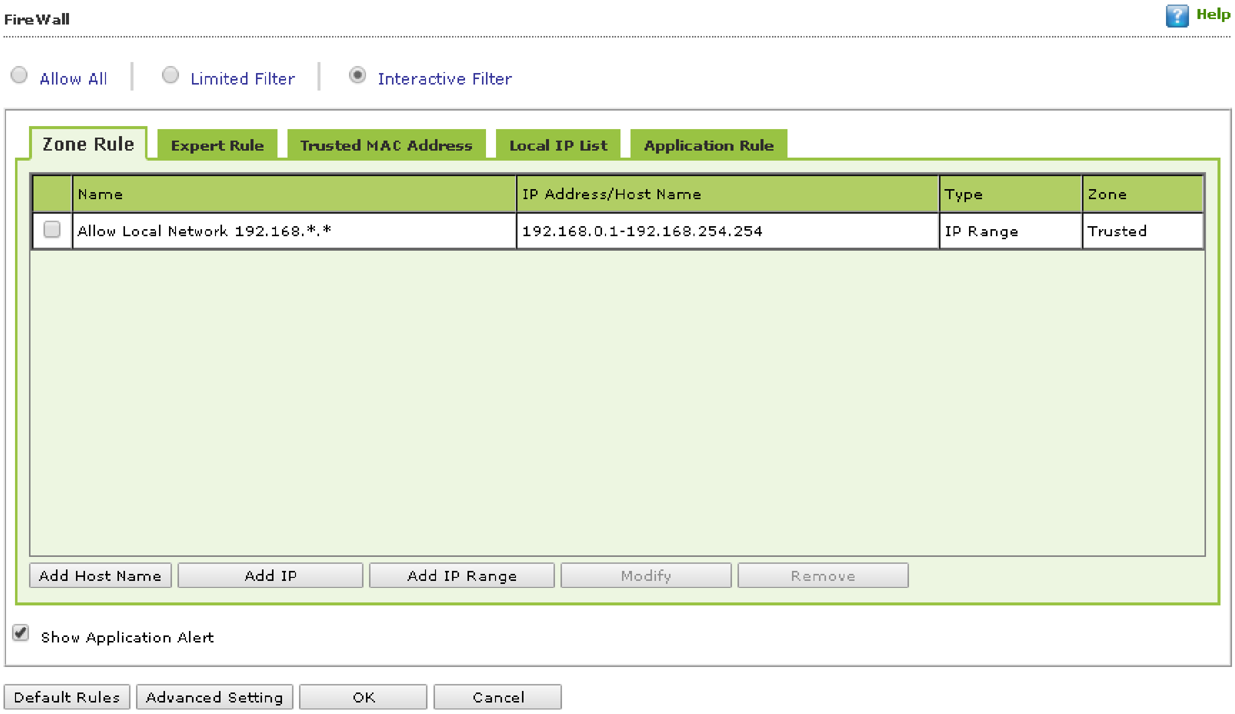
- **Enable email Header check:** ***[Default]*** Select this check box if you need to check the validity of certain generic fields like From, To, and CC in an email and marks it as spam if any of the headers are invalid.
- **Enable X Spam Rules check:** ***[Default]*** X Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The X Spam Rules Check technology matches X Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.
- **Enable Sender Policy Framework (SPF) check:** SPF is a world standard framework that is adopted by eScan to prevent hackers from forging sender addresses. It acts as a powerful mechanism for controlling phishing mails. You should select this check box if you need Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.
- **Enable Spam URI Real-time Blacklist (SURBL) check:** Select this option if you need Anti-Spam to check the URLs in the message body of an email. If the URL is listed in the SURBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **Enable Real-time Blackhole List (RBL) check:** Select this option if you need Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **RBL Servers:** RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.
- **Auto Spam Whitelist:** Unlike normal RBLs, SURBL scans emails for names or URLs of spam Web sites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid email addresses that can bypass the above Spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

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

    - **Do not change email at all:** Select this option when you need to prevent Anti-Spam from adding the *[Spam]* tag to emails that have been identified as spam.

- **Both subject and body is changed: *[Spam]* tag is added in Subject: Actual spam content is embedded in Body:** Select this option to add a *[Spam]* tag in the subject line and the body of the email that has been identified as spam. This option helps you to identify spam emails.
- **"X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body:** Select this option to add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.
- **Only *[Spam]* tag is added in Subject: Body is left unchanged: *[Default]*** *Select* this option to add the *[Spam]* tag only in the subject of the email, which has been identified as spam.
- **"X MailScan Spam: 1" header line is added: Body and subject both remain unchanged:** Select this option to add a header line to the email. However, it does not add any tag to the subject line or body of the email.

3. Firewall



FireWall

○ Allow All | ○ Limited Filter | ● Interactive Filter

	Name	IP Address/Host Name	Type	Zone
☐	Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted

☑ Show Application Alert

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

- Connect to Internet Relay Chat (IRC) servers and join other people on the numerous channels on the IRC network.

- Use Telnet to connect to a server on the Internet and then execute the commands on the server.
- Use FTP to transfer files from a remote server to your computer.
- Use Network basic input/output system (NetBIOS) to communicate with other users on the LAN that is connected to the Internet.
- Use a computer that is a part of a Virtual Private Network (VPN).
- Use a computer to browse the Internet.
- Use a computer to send or receive email.

By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and **Interactive Filter** to turn off and block all. The eScan Firewall also allows you to specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. You can configure the following settings to be deployed to the eScan client systems.

Allow All – Clicking on this button will disable the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored / filtered.

Limited Filter – Clicking on this button will enable eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed / blocked as per the conditions or rules defined in the Firewall.

***Interactive* -** Clicking on this button will enable eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed / blocked as per the conditions or rules defined in the Firewall.

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

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

1. **Add Host Name –** This will allow you to add a new name to the Zone rule. Click this and Add Host Name (New Zone) window will be opened, Enter a new name in the Host Name field, select the Zone as trusted or blocked to add a host in the Zone rule; also enter a name for this particular Zone. Click OK to Save all the details; a new host name will be added.
2. **Add IP –** This will allow you to add a new IP address to this particular Zone. Click this and Add IP (New Zone) window will be opened, enter an IP address in this field here and select the Zone (Trusted / Blocked) and enter a name for the Zone Rule. Click OK to Save all the details; a new IP address will be added.
3. **Add IP Range –** This will allow you to add an IP range to be added to this particular Zone rule. Click this and Add IP range (New Zone), add the IP Range

(i.e. a range of IP that the Zone rule should be applied), select the Zone (Trusted / Blocked) and enter a name for the Zone Rule. Click OK to Save all the details.

4. **Modify –** This will allow you to modify / change an already existing Zone Rule(s), select the zone rule to be modified and click Modify.
5. **Remove –** This will allow you to delete any listed Zone Rule(s), select the zone rule to be deleted and click Remove.

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

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

Buttons (to configure an Expert Rule)

1. **Add** – Click Add to create a new Expert Rule. In the Add Firewall Rule Window:

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

- **Rule Name –** Provide a name to the Rule, for easier understanding on a future date give a name that would depict what the rule is about.
- **Rule Action –** Action to be taken, whether to Permit Packet or Deny Packet.
- **Protocol –** Select the network protocol (eg. TCP, UDP, ARP etc…) on which the Rule will be applied.
- **Apply rule on Interface –** Select the Network Interface on which the Rule will be applied.

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

iii. **Source IP Address –**

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

- **Any IP Address –** Select this option to apply the rule for traffic originating from ANY IP Addresses.
- **My Network -** Select this option to apply the rule for the outgoing traffic originating from all the computers in my network.

iv. **Source Port –**

- **Any –** Select this option to apply the rule for the outgoing traffic originating from ANY port(s).
- **Single Port –** Select this option to apply the rule for the outgoing traffic originating from the specified / defined port.
- **Port Range –** Select this option to enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.
- **Port List –** Select this option to apply the rule for an outgoing traffic originating from the ports as specified in the list. You can add or specify a list of ports.

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

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

v. **Destination IP Address –**

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

vi. **Destination Port –**

- **Any –** When this option is selected, the rule will be applied for the incoming traffic to ANY port.

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

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

- **Advanced tab –** This tab contains advance setting for Expert Rule.
  - **Enable Advanced ICMP Processing -** This is activated when the ICMP protocol is selected in the General tab.
  - **The packet must be from/to a trusted MAC address –** Select this option to apply the rule to the MAC address defined / listed in the Trusted MAC Address tab.
  - **Log information when this rule applies –** This will enable to log information of the Rule when it is implied.

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

C. Trusted MAC Address – This section contains the information of the MAC address of the system.

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

Options (to configure the Trusted MAC Address)

1. **Add –** To add a MAC address click on this button. Enter the MAC address to be added in the list for eg. AO-B3-8F-YZ-O0-BC
2. **Edit –** To modify / change the MAC Address click on this button.
3. **Remove –** To delete the MAC Address click on this button.
4. **Clear All –** To delete all listed MAC Address click on this button.

D. Local IP List – This section contains a list of Local IP addresses.

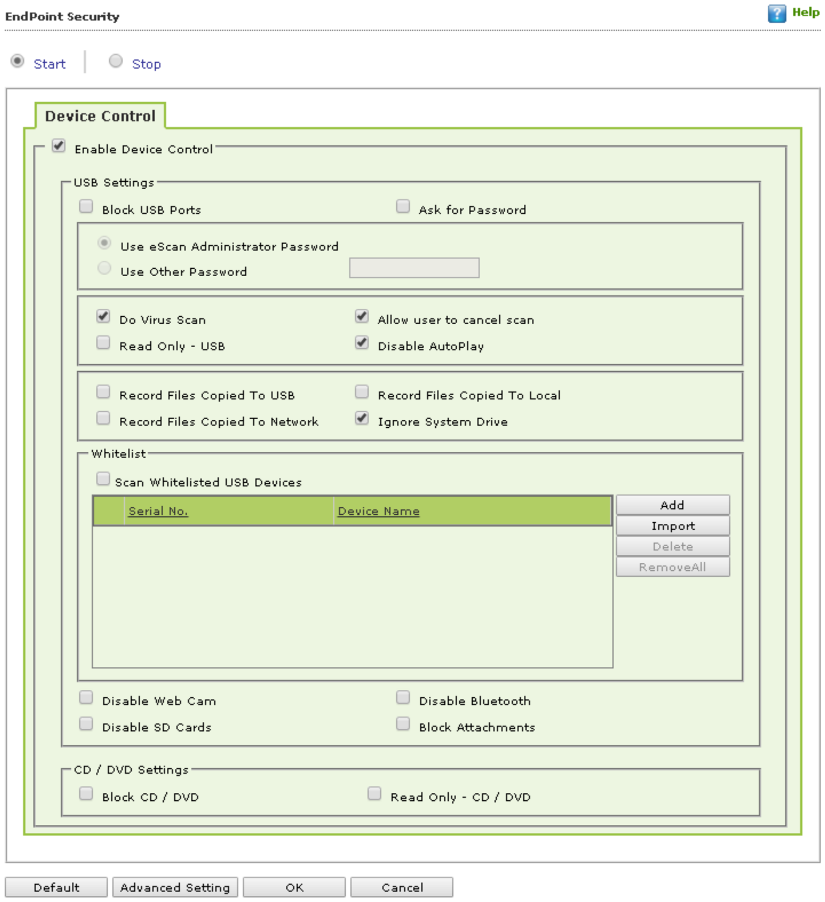
Buttons (to configure the Local IP List)

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

Other Options

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

6. Endpoint Security



EndPoint Security

● Start | ○ Stop

Device Control

☑ Enable Device Control

USB Settings

☐ Block USB Ports ☐ Ask for Password

● Use eScan Administrator Password

○ Use Other Password

☑ Do Virus Scan ☑ Allow user to cancel scan

☐ Read Only - USB ☑ Disable AutoPlay

☐ Record Files Copied To USB ☐ Record Files Copied To Local

☐ Record Files Copied To Network ☑ Ignore System Drive

Whitelist

☐ Scan Whitelisted USB Devices

Serial No.	Device Name

☐ Disable Web Cam ☐ Disable Bluetooth

☐ Disable SD Cards ☐ Block Attachments

CD / DVD Settings

☐ Block CD / DVD ☐ Read Only - CD / DVD

This module protects your computer or endpoints from data thefts and security threats through USB or FireWire® based portable devices. It comes with a Device control feature, which helps you block USB ports, scan the portables, record accessed files via the USB device on your computer. In addition, this feature provides you with a comprehensive reporting feature that helps you determine which portable devices are allowed or blocked by eScan.

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

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

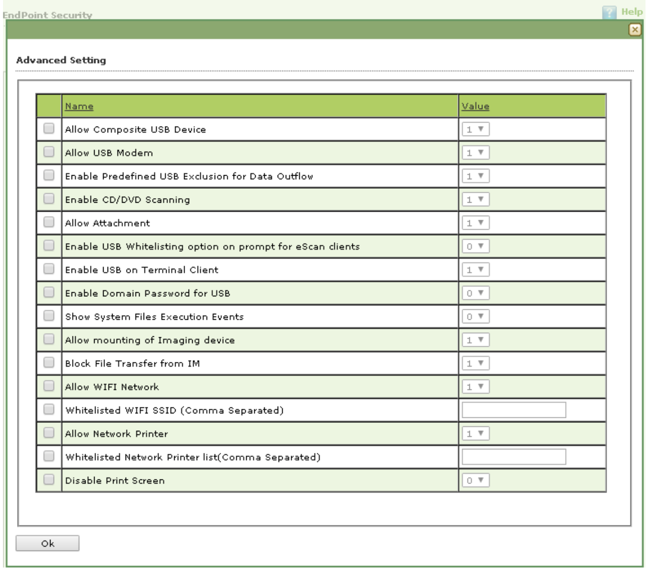
- **Device Control -** The Endpoint Security feature of eScan protects your computer from unauthorized portable storage devices by prompting you for the password whenever you plug in such devices. The devices are also scanned immediately when connected to prevent any infected files running and infecting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

You can configure the following settings:

- **Enable Device Control:** ***[Default]* -** Select this check box if you need to monitor all the USB storages devices connected to your computer.
  - **USB Settings:** This section will allow you to customize the settings for controlling access to USB storage devices.
  - **Block USB Ports:** Select this check box to block all the USB ports.
  - **Ask for Password:** Select this check box to prompt for a password whenever a USB storage device is connected to the computer. You have to type the correct password to access USB storage device. It is recommended that you always keep this check box selected.
  - **Use eScan Administrator:** Select this checkbox to assign the eScan Administrator password for accessing USB Storage device; this option is enabled only when the **Ask for Password** check box is selected.
  - **Use Other Password:** Select this option to assign a unique password for accessing USB Storage device; this option is enabled only when the **Ask for Password** check box is selected.
  - **Do Virus Scan:** ***[Default]*** Select this check box to run a virus scan if the USB storage device is activated. It is recommended to keep this check box selected.
  - **Disable AutoPlay:** ***[Default]*** Select this check box to disable the automatic execution of any program stored on a USB storage device when you connect the device.
  - **Read Only USB:** Select this check box to allow access of the USB device in read-only mode.
  - **Allow user to cancel scan:** Select this check box, to allow the user to the automatic scan of the USB device.
  - **Disable AutoPlay:** Select this checkbox to disable the auto play of the USB devices.
  - **Record Files Copied To USB:** Select this check box to create a record of the files copied from the system to USB drive.
  - **Record Files Copied To Local:** Select this check box to create a record of the files copied to the Local network.

- **Record Files Copies to the Network:** Select this check box to create a record of the files copied to the Network.
- **Ignore System Drive:** Select this check box in case of you do not want eScan to record files that are copied from System drive of managed endpoint to either network drive or any local drive.
- **Whitelist:** eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password but will directly display the files or folders stored on the device. This section displays the serial number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking on the **Add** button.
- **Scan Whitelisted USB Devices:** Select this option to scan USB devices that have been added to the whitelist.
- Click **Add** to enter the **Serial number** (unique for each USB device) and **Device Name** of the USB device to be whitelisted. The Serial Number and the Device Name details are shown in Endpoint security module in eScan Protection Center under the same sub-section. You need to insert the USB device on the eScan server and copy the details onto the eScan web console settings.
- Disable Web Cam: Select this option to Disable Webcams connected
- Disable SD Cards: Select this option to disable the SD cards
- Disable Bluetooth: Select this option to disable Bluetooth
- Block Attachments: Select this option to block all attachments.

Advanced Settings



Advanced Setting

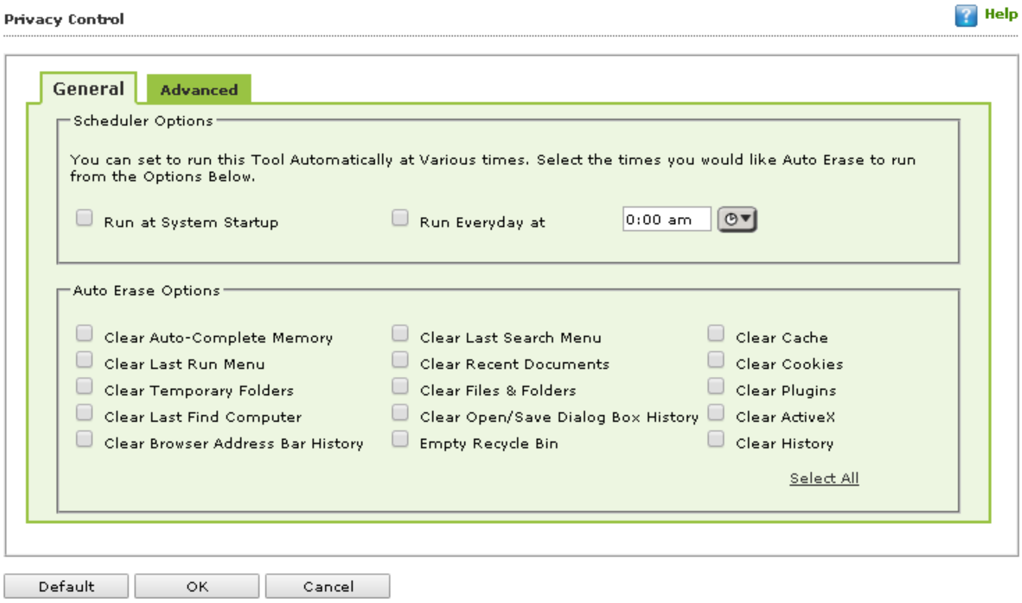
	Name	Value
□	Allow Composite USB Device	1 ▼
□	Allow USB Modem	1 ▼
□	Enable Predefined USB Exclusion for Data Outflow	1 ▼
□	Enable CD/DVD Scanning	1 ▼
□	Allow Attachment	1 ▼
□	Enable USB Whitelisting option on prompt for eScan clients	0 ▼
□	Enable USB on Terminal Client	1 ▼
□	Enable Domain Password for USB	0 ▼
□	Show System Files Execution Events	0 ▼
□	Allow mounting of Imaging device	1 ▼
□	Block File Transfer from IM	1 ▼
□	Allow WIFI Network	1 ▼
□	Whitelisted WIFI SSID (Comma Separated)	
□	Allow Network Printer	1 ▼
□	Whitelisted Network Printer list(Comma Separated)	
□	Disable Print Screen	0 ▼

Default

Note:

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

7. Privacy Control



Privacy Control

Scheduler Options

You can set to run this Tool Automatically at Various times. Select the times you would like Auto Erase to run from the Options Below.

□ Run at System Startup □ Run Everyday at 0:00 am

Auto Erase Options

□ Clear Auto-Complete Memory
□ Clear Last Run Menu
□ Clear Temporary Folders
□ Clear Last Find Computer
□ Clear Browser Address Bar History
□ Clear Last Search Menu
□ Clear Recent Documents
□ Clear Files & Folders
□ Clear Open/Save Dialog Box History
□ Empty Recycle Bin
□ Clear Cache
□ Clear Cookies
□ Clear Plugins
□ Clear ActiveX
□ Clear History

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

1. *General*

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

You can configure the following settings.

- **Scheduler Options:** You can set the scheduler to run at specific times and erase private information, such as your browsing history from your computer. The following settings are available in the **Scheduler Options** section.
    - **Run at System Startup:** It auto executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.
    - **Run Everyday at:** It auto-executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.

- **Auto Erase Options:** The browser stores traceable information of the Web sites that you have visited in certain folders. This information can be viewed by others. eScan allows you to remove all traces of Web sites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. You can select the following options based on your requirements.
    - **Clear Auto Complete Memory:** Auto Complete Memory refers to the suggested matches that appear when you type text in the Address bar, the Run dialog box, or forms in Web pages. Hackers can use this information to monitor your surfing habits. Select this check box to clear all this information from the computer.
    - **Clear Last Run Menu:** Select this check box, to clear this information in the Run dialog box.
    - **Clear Temporary Folders:** Select this check box to clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive of the computer and boosts the performance of the computer.
    - **Clear Last Find Computer:** Select this check box to clear the name of the computer for which you searched last.
    - **Clear Browser Address Bar History:** Select this check box to clears the Web sites from the browser's address bar history.
    - **Clear Last Search Menu:** Select this check box to clear the name of the objects that you last searched for by using the Search Menu.
    - **Clear Recent Documents:** Select this check box to clear the names of the objects found in Recent Documents.
    - **Clear Files & Folders:** Select this check box to delete selected Files and Folders. You should use this option with caution because it permanently deletes unwanted files and folders from the computer to free space on the computer.
    - **Clear Open / Save Dialog box History:** Select this check box to clear the links of all the opened and saved files.
    - **Empty Recycle Bin:** Select this check box to clear the Recycle Bin. You should use this option with caution because it permanently clears the recycle bin.
    - **Clear Cache:** Select this check box to clear the Temporary Internet Files.
    - **Clear Cookies:** Select this check box to clear the Cookies stored by Web sites in the browser's cache.
    - **Clear Plugins:** Select this check box to remove the browser plug-in.
    - **Clear ActiveX:** Select this check box to clear the ActiveX controls.
    - **Clear History:** Select this check box to clear the history of all the Web sites that you have visited.

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

- **Select All/ Unselect All:** Click this option to select / unselect all the auto erase options.

2. *Advanced*

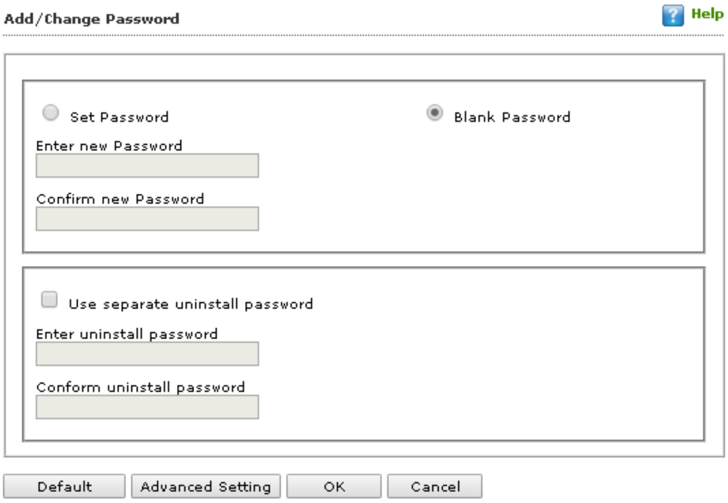
This tab helps you to select unwanted or sensitive information stored in the browser's cache that you need to clear.

Default

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

It also allows you to do the following

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



Add/Change Password

○ Set Password ● Blank Password

Enter new Password

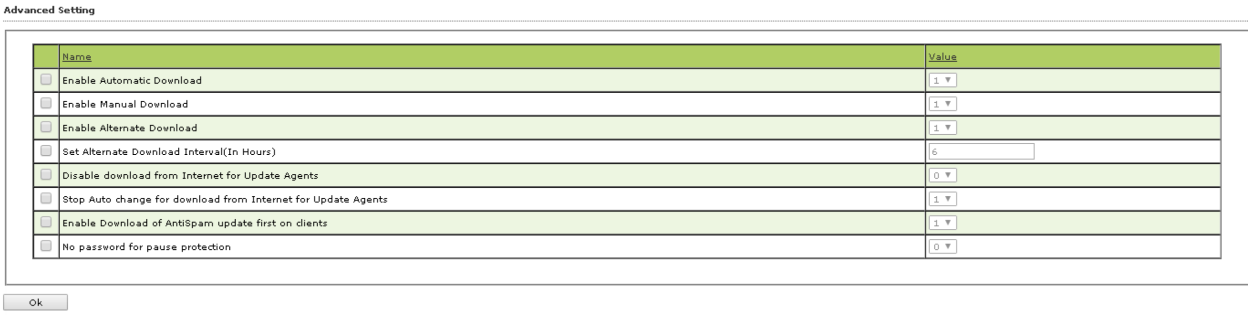
Confirm new Password

□ Use separate uninstall password

Enter uninstall password

Conform uninstall password

Advanced Setting

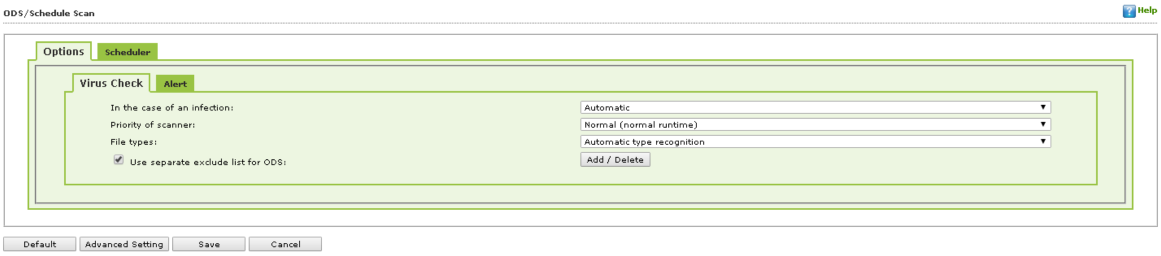


Advanced Setting

	Name	Value
□	Enable Automatic Download	1 ▼
□	Enable Manual Download	1 ▼
□	Enable Alternate Download	1 ▼
□	Set Alternate Download Interval(In Hours)	6
□	Disable download from Internet for Update Agents	0 ▼
□	Stop Auto change for download from Internet for Update Agents	1 ▼
□	Enable Download of AntiSpam update first on clients	1 ▼
□	No password for pause protection	0 ▼

ODS/ Schedule Scan:

Using ODS/ Schedule Scan you can check for viruses, and make settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.
There are two tabs – Options and Scheduler.



In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

☑ Use separate exclude list for ODS: Add / Delete

Options

Options tab enables you to make the settings for checking viruses and receiving alerts. There are two tabs – Virus Check and Alerts. You can do the following activities.

Virus Check: Define the settings for checking viruses.

Note:
Click Default to apply default settings that were set during installation of eScan. It will load and reset the rules to default settings.

Field	Description
In the case of an infection	Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
Priority of scanner	Select an appropriate option from the drop-down list. For example, High (short runtime), [Default] Normal (normal runtime), and Low (long runtime).
File types	Select an appropriate option from the drop-down list. For example, [Default] Automatic type recognition and Only program files.

Alert
It enables you to define the settings for virus alert. You can also create a log of the infected viruses.

Note:
Click Default to apply default settings that were set during installation of eScan. It will load and reset the rules to default settings.

To set alerts

Warn, if virus signature is more than _days old: Select this check box and then type the number of days in the _days old field to receive alerts when virus signature exceeds the specified days. By default, you get warning after 3 days.
Warn, if the last computer analysis was more than _days old: Select this check box and then type the number of days in the _days ago field to receive alerts when last computer

analysis exceeds the specified days. By default you get warning if the analysis was more than 3 days old.

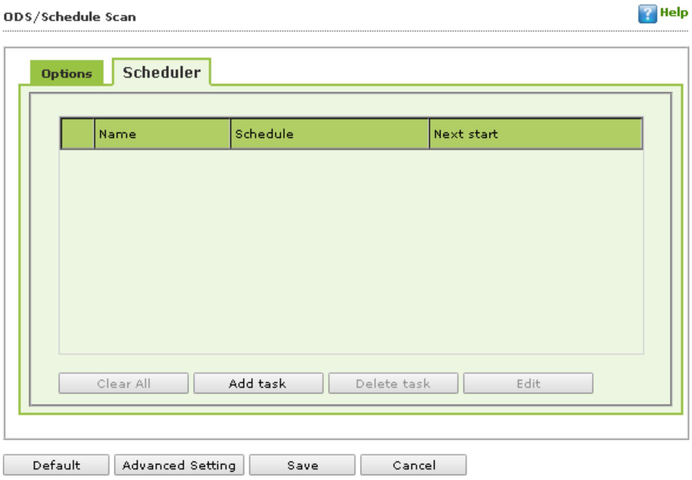
Log Settings

Prepare Log: Select this check box to prepare log of the infected files, and then click an appropriate option.

Only infection to be logged: Select this check box to prepare a log of all the infected files.
Full log: Select this check box to prepare a complete log of all the infected and clean files.

Click **Save**.

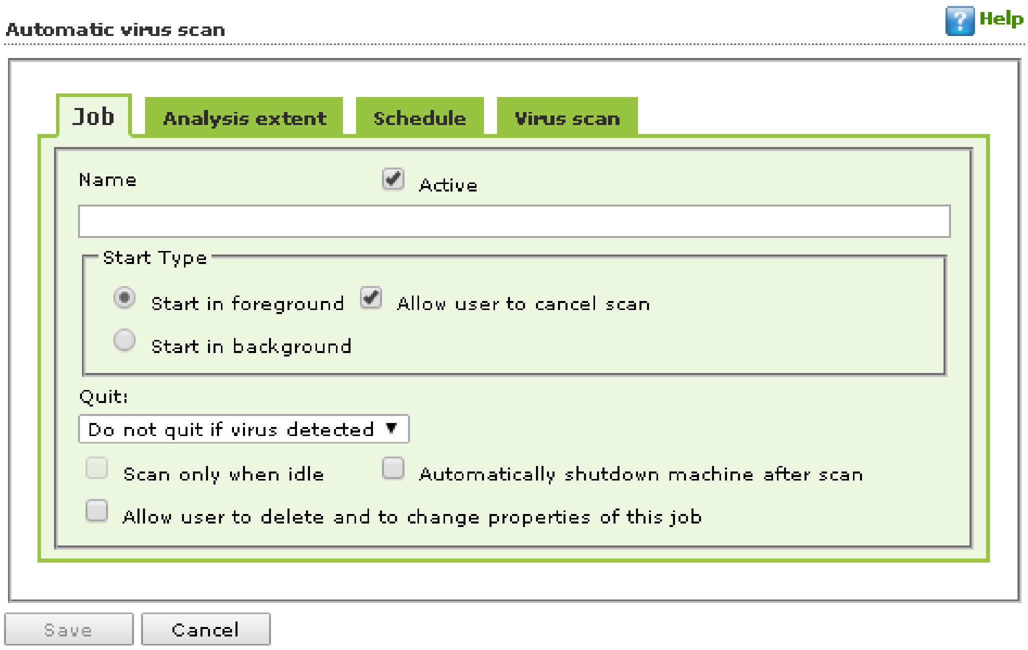
Scheduler



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

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

  - **Job**



Name

☑ Active

Start Type

● Start in foreground ☑ Allow user to cancel scan

○ Start in background

Quit:

Do not quit if virus detected ▼

□ Scan only when idle □ Automatically shutdown machine after scan

□ Allow user to delete and to change properties of this job

It will allow you to create the Job details for Virus Scanning

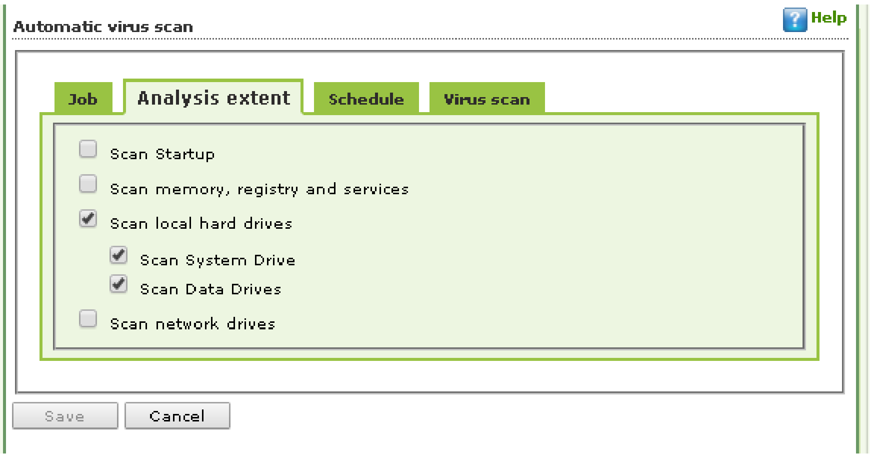
- **Name:** Give any name to this particular schedule
- **Active:** Select this check box to schedule the task.
- **Start in foreground [Default]**: Click this option to view scanning process in the foreground.
- **Start in background**: Click this option to view scanning process in the background.
- **Allow user to cancel scan**: Click this option to allow the user to cancel scan.

Quit

Select an appropriate option from the drop-down list **Do not quit if virus detected/Select**
Never quit automatically/Always quit

- **Scan only when idle:** Select this option to scan only when the system is idle
- **Automatically shutdown machine after scan:** Select this option to automatically shut down the machine after scan.
- **Allow user to delete and to change properties of this job:** Select this check box if you want to allow user to edit or delete the scheduler settings.

Analysis Extent:
It enables you to make the analysis extent settings for virus scanning.



Automatic virus scan

□ Scan Startup

□ Scan memory, registry and services

☑ Scan local hard drives

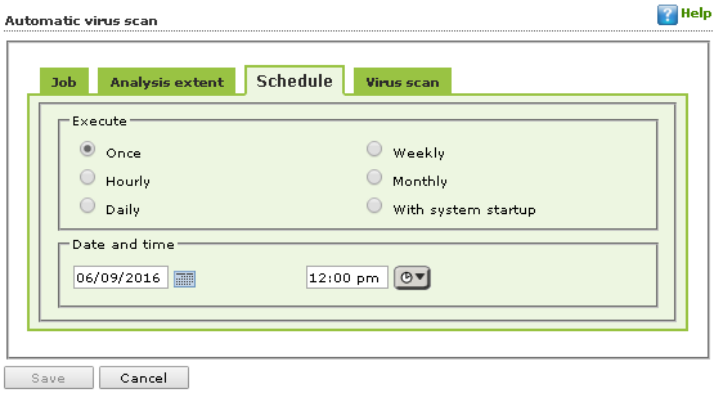
  ☑ Scan System Drive

  ☑ Scan Data Drives

□ Scan network drives

1. **Scan Start up:** – Select this option to scan your system on startup
2. **Scan memory, registry and Services:** Select this option to scan all memory registry and services.
3. **Scan local hard drives:** Select this option is scan all local hard drives.
4. **Scan system drive:** Select this option to scan all system drives
5. **Scan Data drives:** select this option to scan all data drives.
6. **Scan network drives:** select this option to scan all network drives.

Schedule



Automatic virus scan

Execute

● Once ○ Weekly

○ Hourly ○ Monthly

○ Daily ○ With system startup

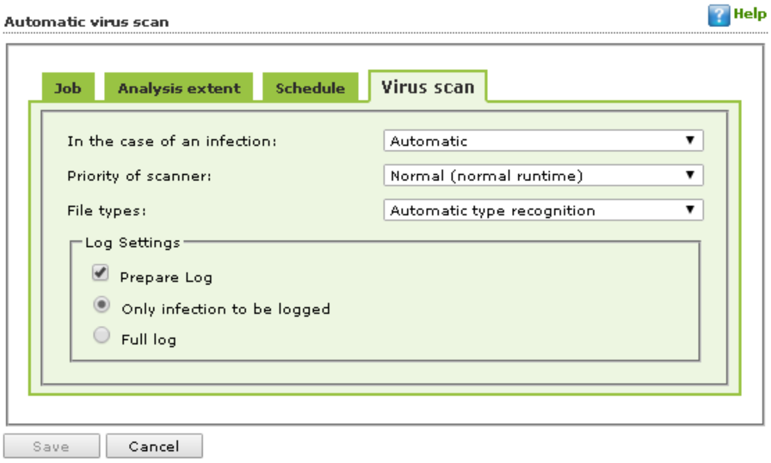
Date and time

06/09/2016 12:00 pm

Execute
Choose the frequency at which the automatic virus scan should be executed. You can choose from once/hourly/daily/weekly/monthly/with system startup.

Date and time: Select and set the appropriate date and time at which you want the scan to be executed.

- **Virus Scan**


Automatic virus scan

In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

Log Settings

☑ Prepare Log

● Only infection to be logged

○ Full log

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

  It indicates a type of action which you want eScan real-time protection to take, in case of virus detection.
  By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

  - **In the case of an infection:** Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
  - **Priority of scanner:** Select an appropriate option from the drop-down list. For example: High (short runtime), [Default] Normal (normal runtime), and Low (long runtime).
  - **File types:** Select an appropriate option from the drop-down list. For example, [Default] Automatic type recognition and only program files.

- **Log Settings**

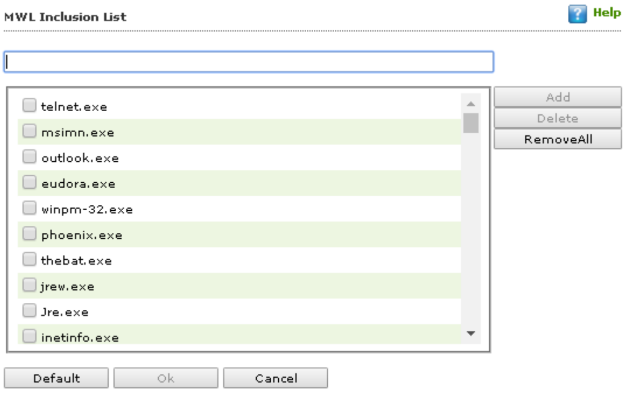
  - **Prepare Log:** Select this check box to prepare log of the infected files, and then click an appropriate option.
  - **Only infection to be logged:** Select this check box to prepare a log of all the infected files.
  - **Full log:** Select this check box to prepare a complete log of all the infected and clean files.
  - **Click Save.**

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

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

You can do the following activities.

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



MWL Inclusion List

□ telnet.exe
□ msimn.exe
□ outlook.exe
□ eudora.exe
□ winpm-32.exe
□ phoenix.exe
□ thebat.exe
□ jrew.exe
□ Jre.exe
□ inetinfo.exe

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

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

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

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

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

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

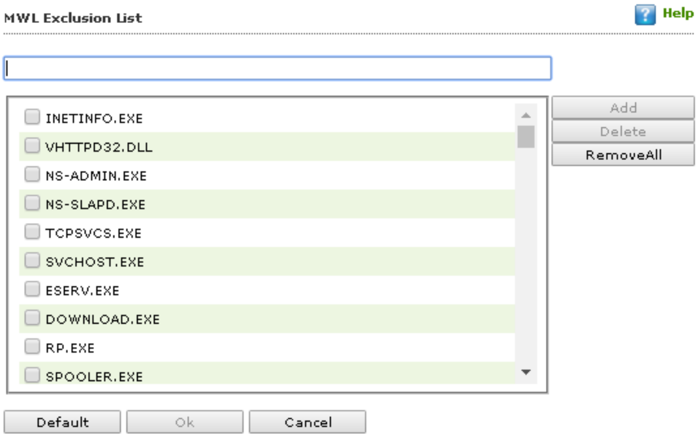
2. MWL Exclusion List

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

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

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

- **Removing all files** from exclusion list


MWL Exclusion List

INETINFO.EXE
VHTTPD32.DLL
NS-ADMIN.EXE
NS-SLAPD.EXE
TCPSVCS.EXE
SVCHOST.EXE
ESERV.EXE
DOWNLOAD.EXE
RP.EXE
SPOOLER.EXE

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

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

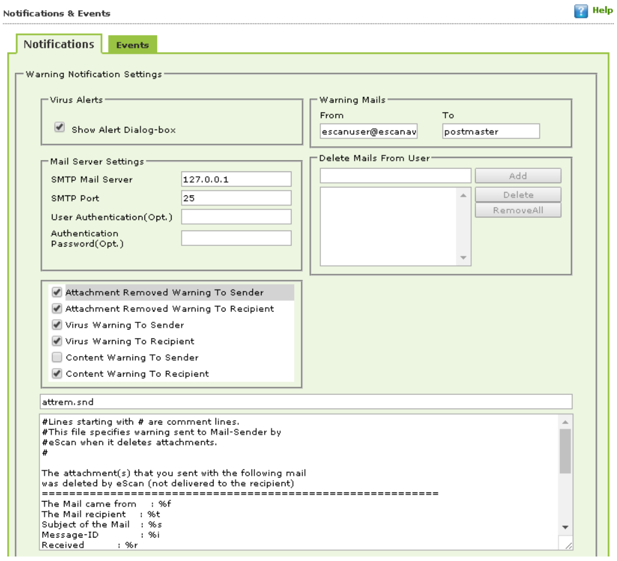
- **Deleting files from exclusion list.** It enables you to delete executable files from the list.

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

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

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

5. **Notifications and Events**



Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

Warning Mails

From: escanuser@escanav

To: postmaster

Mail Server Settings

SMTP Mail Server: 127.0.0.1

SMTP Port: 25

User Authentication(Opt.)

Authentication Password(Opt.)

Delete Mails From User

☑ Attachment Removed Warning To Sender

☑ Attachment Removed Warning To Recipient

☑ Virus Warning To Sender

☑ Virus Warning To Recipient

□ Content Warning To Sender

☑ Content Warning To Recipient

attrem.snd

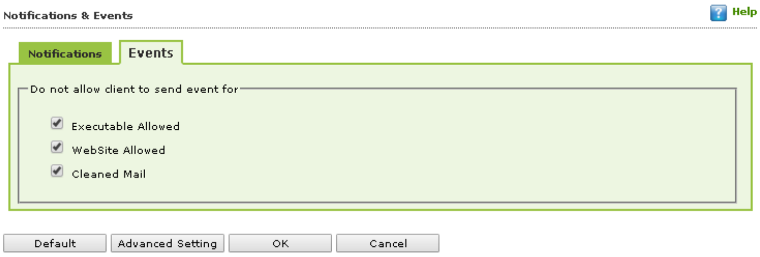
```
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#eScan when it deletes attachments.
#

The attachment(s) that you sent with the following mail
was deleted by eScan (not delivered to the recipient)
==============================================================
The Mail came from    : %f
The Mail recipient    : %t
Subject of the Mail   : %s
Message-ID            : %i
Received        : %r
```

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

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

- **Delete Mails From User:** You can configure eScan to automatically delete e mails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons are disabled. Once you type text in the **Delete Mails From User** field, the buttons appear.

Events

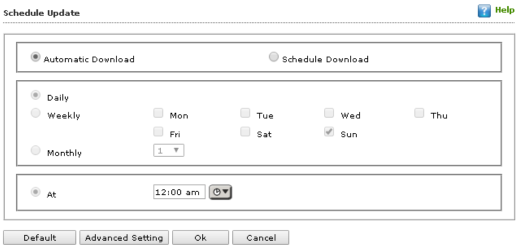


Do not allow client to send event for

☑ Executable Allowed
☑ WebSite Allowed
☑ Cleaned Mail

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

Schedule Update



● Automatic Download ○ Schedule Download

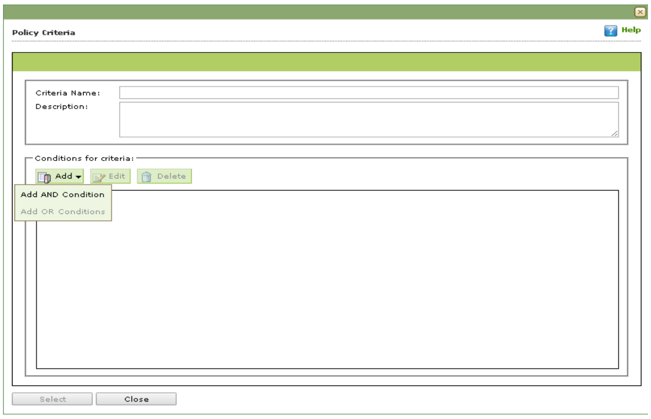
● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ Sun
○ Monthly 1

● At 12:00 am

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

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

Policy Criteria



Criteria Name:
Description:

Conditions for criteria:

This option will allow the administrator to specify policy criteria and deploy it to endpoints automatically if it complies with the pre – defined criteria in the management console. The Administrator will select Policy Criteria based on which the policies will be deployed.

It allow you to define the following –

- **Criteria Name**: Define the criteria Name.

- **Description:** Give a brief description about the policy here, so that it is easier to understand the policy criteria details on a future date.

Conditions of criteria

This option will allow the administrator to select the conditions for the policy criteria; the policy template will be applied only when the selected criteria is/are met.

- **Add**: This option will allow the administrator to add conditions for the policy criteria; the policy templates will be applied to the selected group or managed endpoint only if the criteria are matched. For more details **click here**

- **Edit**: This will allow the administrator to make changes to the existing policy criteria. The administrator can make changes like adding or removing of an IP address or can even make changes to the criteria itself.

- **Delete:** This will allow the administrator to delete an already defined policy criterion.

Creating Policy Criteria

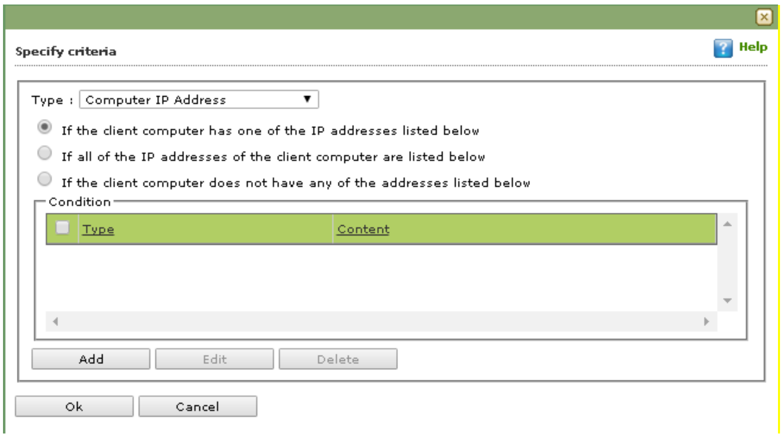
1. Go to managed computers on the navigation panel and click **Policy Criteria Templates** tab on the right side; this will open the Policy criteria window.
2. Click **New Criteria** and a new window will be displayed, enter a criteria name and a brief description of the criteria.
3. Click **Add** option under conditions for criteria section; and select a condition. You can select from the following

    - **Add 'AND' Condition** – In case if you have selected multiple criteria, then the policy will be applied only if all the defined criteria are met.
    - **Add 'OR' Condition** - In case if you have selected multiple criteria, then the policy will be applied only if any of the defined criteria is met.

4. Specify criteria window will open; this Window allows you to Select Criteria Type and Conditions for the defined Criteria.
5. It also allows you to Add, Edit or Delete IP Address, IP Range or Subnet Address to which the Criteria will be applicable.

Selecting Criteria Type

It allows you to define the following -



Specify criteria

Help

Type : Computer IP Address ▼

● If the client computer has one of the IP addresses listed below

○ If all of the IP addresses of the client computer are listed below

○ If the client computer does not have any of the addresses listed below

Condition

□ Type	Content

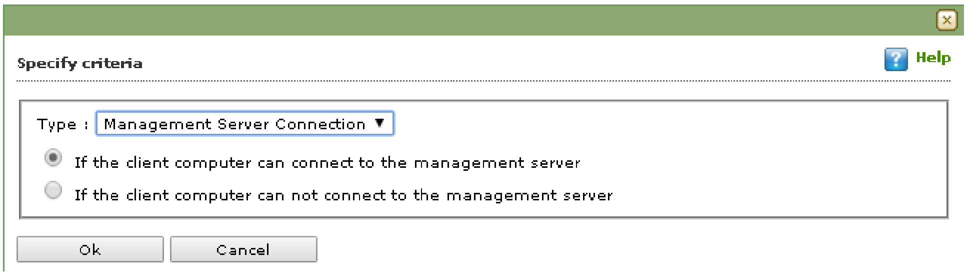
Add | Edit | Delete

Ok | Cancel

Computer IP Address: If you select this type of criteria, then the policy criteria will be around the IP addresses of the client. The conditions would be as follows

a. If the client computer has one of the IP listed below.
b. If all the IP address of the client computers are listed below.
c. If the client computer does not have any of the addresses listed below.

Management Server connections: This particular type of criteria will have conditions around the management server connection.



Specify criteria

Help

Type : Management Server Connection ▼

● If the client computer can connect to the management server

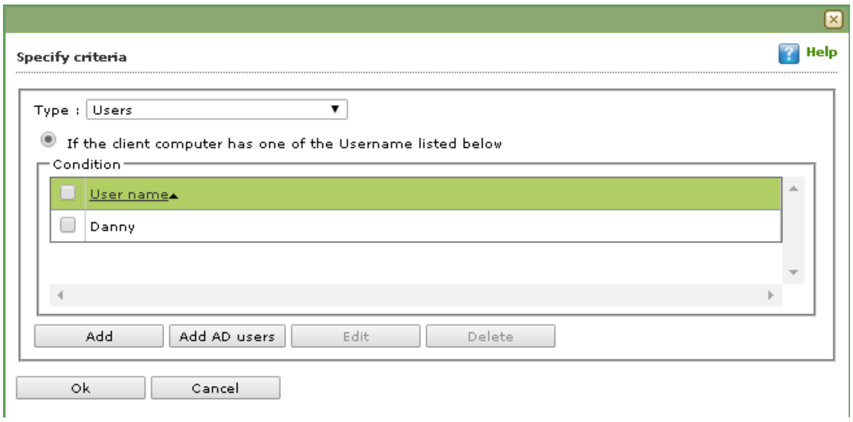
○ If the client computer can not connect to the management server

Ok | Cancel

a. If the client computer can connect to the management server
b. If the client computer cannot connect to the management server

Users: This particular type of criteria will have conditions around the username of the client.

- If the client computer has one of the user names listed below.



Specify criteria

Help

Type : Users ▼

● If the client computer has one of the Username listed below

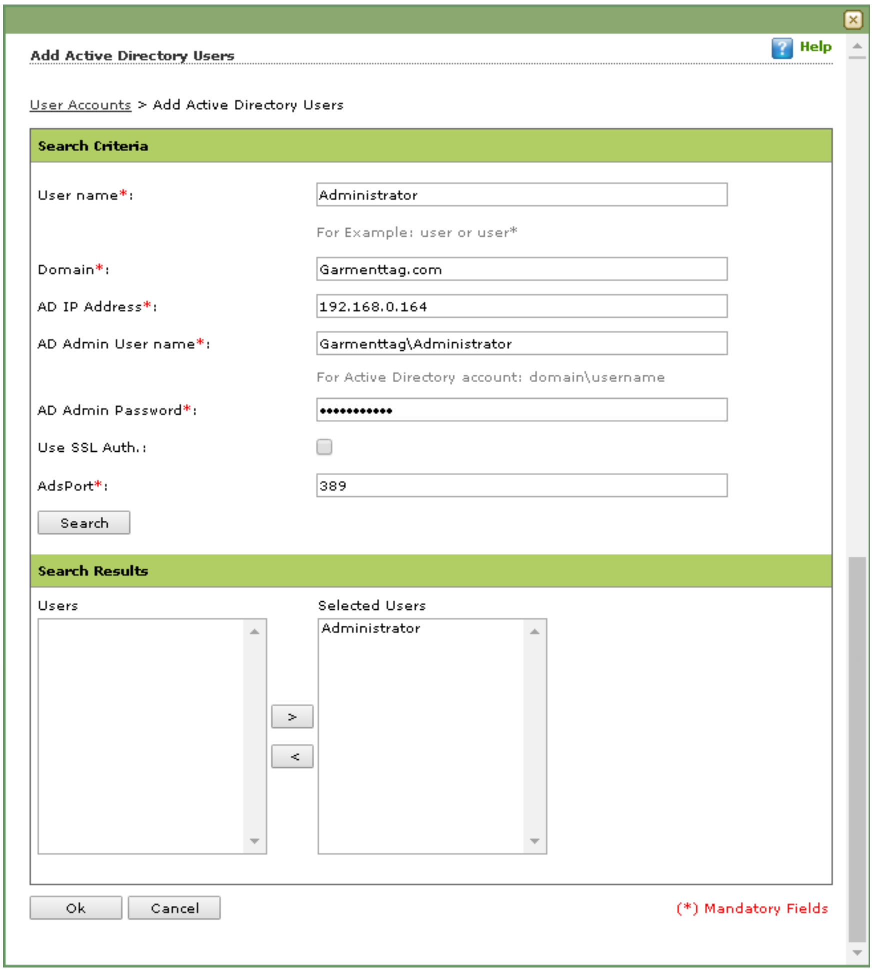
Condition

□ User name▲
□ Danny

Add | Add AD users | Edit | Delete

Ok | Cancel

- It will allow you to add usernames directly or you can also add users from the Active Directory.
- To Add AD users you can search the users listed on the AD server and select from the users' list as shown below.



Add Active Directory Users

User Accounts > Add Active Directory Users

Search Criteria

User name*: Administrator

For Example: user or user*

Domain*: Garmenttag.com

AD IP Address*: 192.168.0.164

AD Admin User name*: Garmenttag\Administrator

For Active Directory account: domain\username

AD Admin Password*: •••••••••••

Use SSL Auth.: □

AdsPort*: 389

Search Results

Users

Selected Users: Administrator

(*) Mandatory Fields

6. If you select the Computer IP Address type condition, choose criteria from the listed criteria and then click **Add**.
7. A new window will be displayed; select IP address / IP address range or subnet address and enter the IP address details or the Subnet details and click **OK**.
8. The defined IP address / IP address range or subnet address will be displayed on the specify criteria window, Click **Ok**.
9. On clicking OK you will be taken back to the Policy criteria window and here it will display the details of the policy criteria, the name, description and the policy criteria that you have selected.
10. You can edit the criteria by selecting the policy criteria and also make any other changes, once all changes are completed, click **Save**.
11. You have successfully defined policy criteria.

How to deploy a Policy Criteria to Managed group?

1. Go to managed computers, click on policy criteria, it will display the list of already created policy criteria. The list will display the name of the policy criteria, the date when the policy criteria was created and modified etc. For more details on creating a policy criteria **click here**
2. Select desired criteria, Properties, Delete criteria and Assign to will be enabled.
3. Click on Assign tab and from the drop down select Groups.
4. On selecting groups a window "Assign Criteria to Group" will be opened and a list of policy templates will be displayed.
5. Select a template as per your requirement and click OK; you will be forwarded to a list of managed groups.
6. Select a managed group from the listed groups or you can also create a new group and Click OK to assign the policy criteria to that particular group.

How to deploy a Policy Criteria to Managed Computer?

1. Go to managed computers, click policy criteria, it will display the list of already created policy criteria. The list will display the name of the policy criteria, the date when the policy criteria was created and modified etc. For more details on creating a policy criteria **click here**.
2. Select policy criteria and the tabs Properties, delete criteria and Assign to will be enabled.
3. Click on Assign tab and from the drop down select computers.
4. On selecting computers a window "Assign Criteria to computers" will be opened and a list of policy templates will be displayed.
5. Select a particular template as per your requirement and click OK; you will be forwarded to a list of managed computers.
6. Select a managed computer from the list and Click OK to assign the policy criteria to this managed computer.

How to delete Policy Criteria?

1. Go to managed computers, click on policy criteria, it will display the list of already created policy criteria. The list will display the name of the policy criteria, the date when the policy criteria was created and modified etc. For more details on creating a policy criteria **click here**.
2. Select policy criteria and the tabs Properties, delete criteria and Assign to will be enabled.
3. Click on delete and the policy criteria will be deleted.

Example

Mr. X from the sales department uses office laptop on sales calls that are generally out of the office. While he is in office, he will be connected to the office network and an IP address will be assigned to the laptop. Administrator can define Policy Criteria for such employees; the policy will be deployed / implemented automatically whenever the defined IP Address or the computers in the defined IP Range connects to the eScan network.

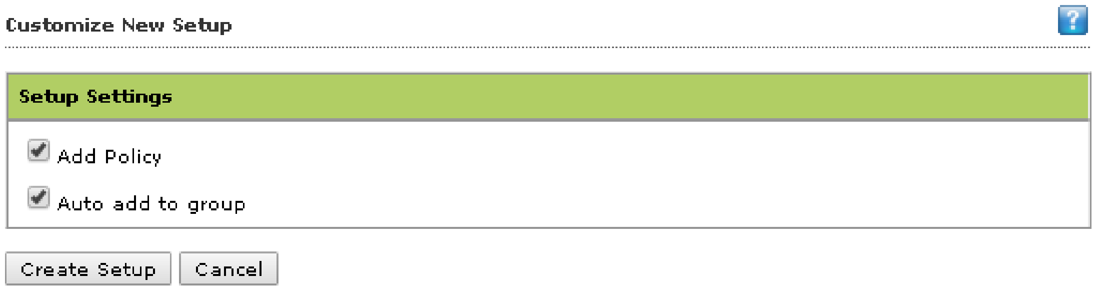
Customized Client Setup

eScan allows you to create customized client setup with pre-defined Policy Template. This allows you to implement group policies to the endpoints automatically when eScan Client is installed on the endpoint manually. The major benefit of this feature is that even if the endpoint is not connected to the eScan server, the Policy template will be deployed on to the endpoint while customized eScan Client is installed on the endpoint. On installing this customized setup, the endpoint will be automatically moved to the selected group.

Note:
The policy should be already defined for the group.

How to create customized policy setup?

1. Go to Managed Computers and select the group for which you wish to create customized build with pre-defined Policy.
2. Go to Action List and click Create Client Setup option.
3. Define Setup Settings



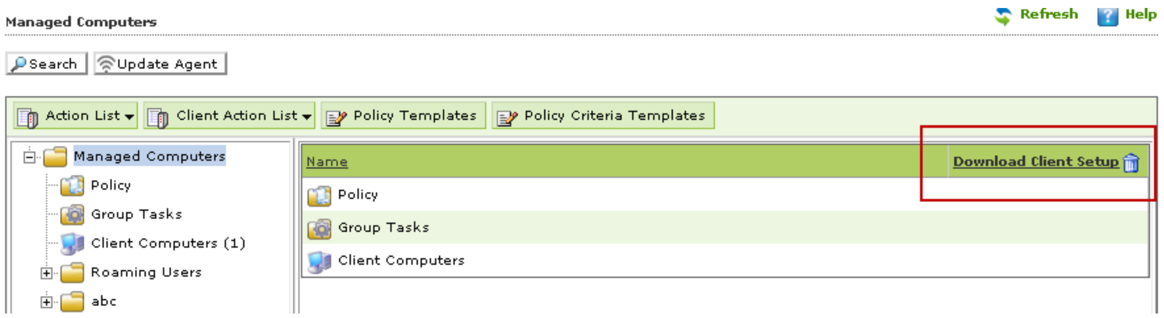
Customize New Setup

Setup Settings

☑ Add Policy

☑ Auto add to group

4. Click **Create Setup**.
5. Setup download link will be created; you can either send the created setup from the path or deploy it through eScan remotely. By default the setup will saved in C:\ProgramFiles\CommonFiles\MicroWorld\apache2\EMCWEBADMIN\CustomizedSetup



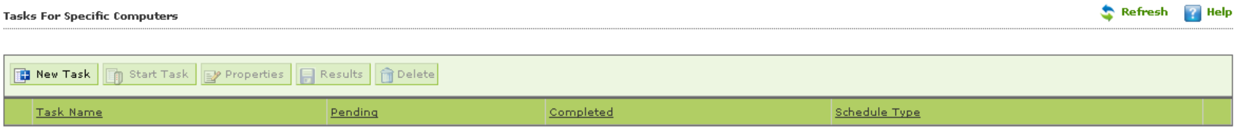
Managing Tasks and Policies for Specific Computers

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

- **Managing Tasks for Specific Computers**

1. Click **Tasks for Specific Computers** in **Navigation Panel** of eScan Management Console.

2. Now Click **New Task**.

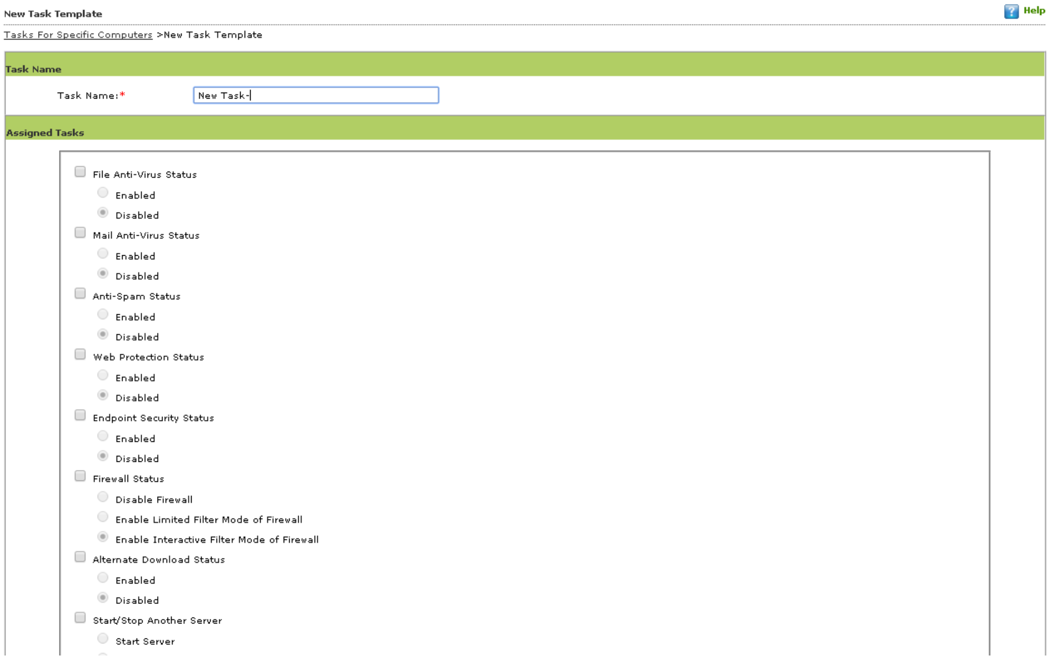


Tasks For Specific Computers

Task Name	Pending	Completed	Schedule Type

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

4. Define the **Task Name** in the text field.



New Task Template

Tasks For Specific Computers >New Task Template

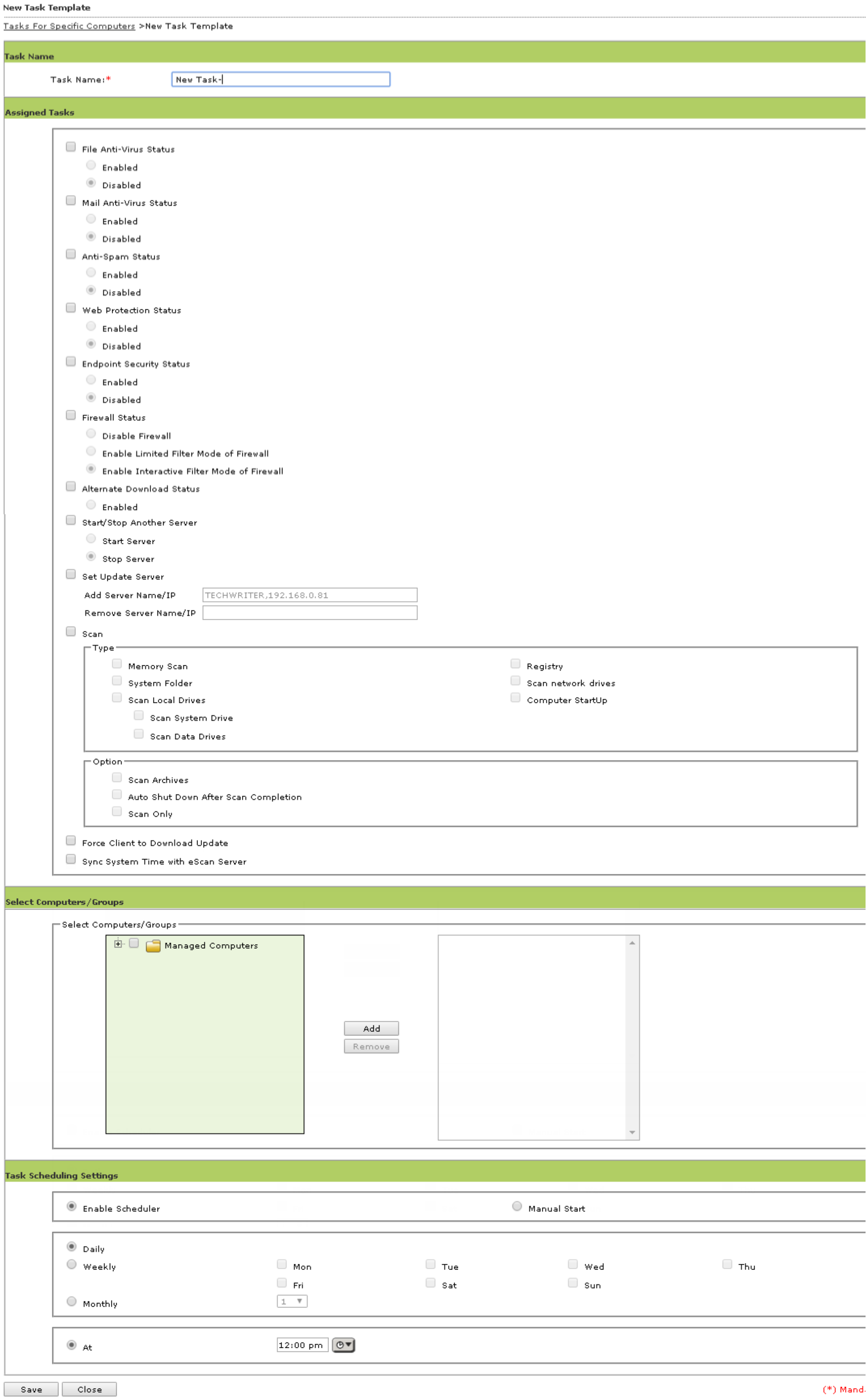
Task Name

Task Name:* New Task-

Assigned Tasks

□ File Anti-Virus Status
○ Enabled
● Disabled
□ Mail Anti-Virus Status
○ Enabled
● Disabled
□ Anti-Spam Status
○ Enabled
● Disabled
□ Web Protection Status
○ Enabled
● Disabled
□ Endpoint Security Status
○ Enabled
● Disabled
□ Firewall Status
○ Disable Firewall
○ Enable Limited Filter Mode of Firewall
● Enable Interactive Filter Mode of Firewall
□ Alternate Download Status
○ Enabled
● Disabled
□ Start/Stop Another Server
○ Start Server

2. Select the desired options for assigning tasks.



New Task Template

Tasks For Specific Computers >New Task Template

Task Name

Task Name:* New Task-

Assigned Tasks

□ File Anti-Virus Status
○ Enabled
● Disabled

□ Mail Anti-Virus Status
○ Enabled
● Disabled

□ Anti-Spam Status
○ Enabled
● Disabled

□ Web Protection Status
○ Enabled
● Disabled

□ Endpoint Security Status
○ Enabled
● Disabled

□ Firewall Status
○ Disable Firewall
○ Enable Limited Filter Mode of Firewall
● Enable Interactive Filter Mode of Firewall

□ Alternate Download Status
○ Enabled

□ Start/Stop Another Server
○ Start Server
● Stop Server

□ Set Update Server
Add Server Name/IP TECHWRITER,192.168.0.81
Remove Server Name/IP

□ Scan

Type
□ Memory Scan
□ System Folder
□ Scan Local Drives
□ Scan System Drive
□ Scan Data Drives
□ Registry
□ Scan network drives
□ Computer StartUp

Option
□ Scan Archives
□ Auto Shut Down After Scan Completion
□ Scan Only

□ Force Client to Download Update
□ Sync System Time with eScan Server

Select Computers/Groups

Select Computers/Groups
□ Managed Computers

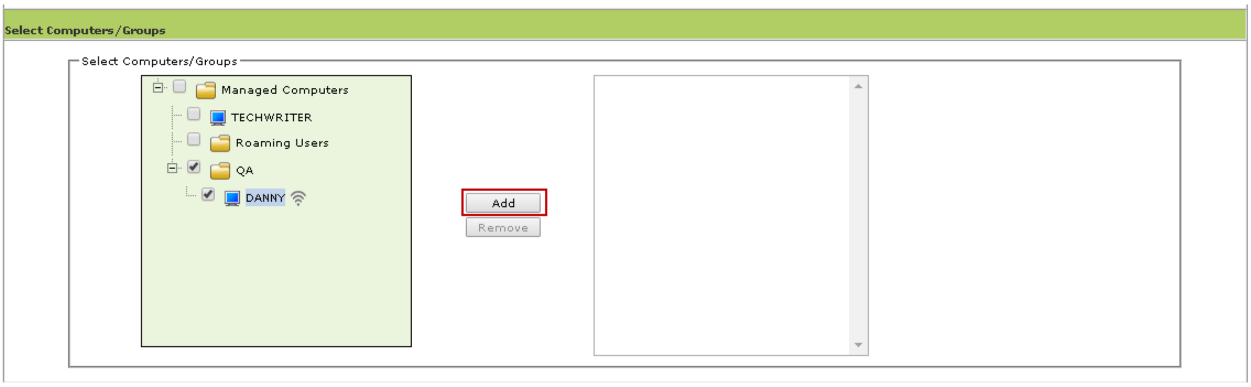
Task Scheduling Settings

● Enable Scheduler ○ Manual Start

● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
○ Monthly 1

● At 12:00 pm

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

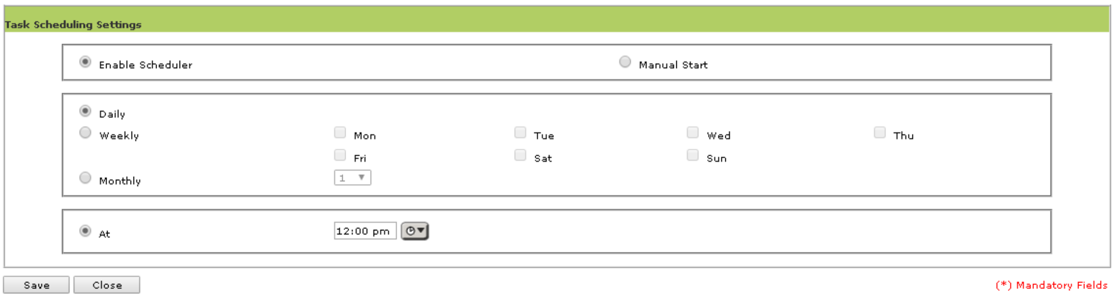


Select Computers/Groups

Select Computers/Groups

- □ Managed Computers
  - □ TECHWRITER
  - □ Roaming Users
  - ☑ QA
    - ☑ DANNY

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



Task Scheduling Settings

● Enable Scheduler ○ Manual Start

● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu
□ Fri □ Sat □ Sun
○ Monthly 1

● At 12:00 pm

(*) Mandatory Fields

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

One Time Password

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

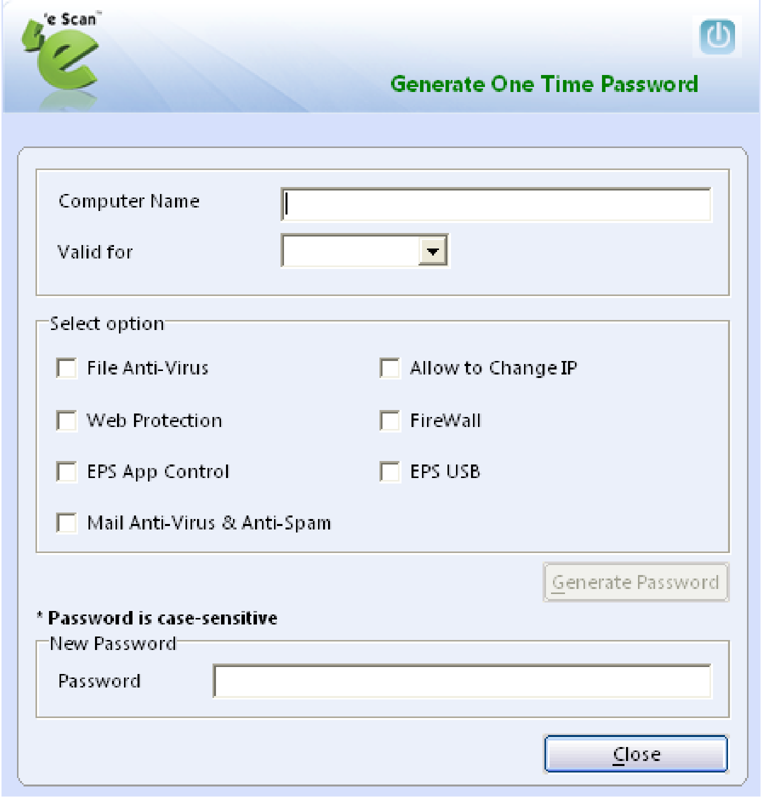
Working:

1. eScan Server Administrator defines a policy for a particular group blocking access to the USB ports through the web console. The USB access is blocked through the endpoint security module through Policies for Specific Computers.
2. For some specific reason, access to a USB port is required in one of the systems within a group where the security policy has been defined. The administrator is notified of this request manually.
3. The administrator generates a one-time password on the server and manually notifies the user who requires access to the USB port for a specific time period.

4. The user utilizes the one-time password within the group for accessing the USB port for the specified time period defined by the administrator. Other systems within the group cannot access the USB ports as the security policy is set for them thus ensuring that the group policy is not infringed.

How to Access

Use the following simple steps to access OTPass.EXE.



Generate One Time Password

Computer Name

Valid for

Select option

□ File Anti-Virus

□ Allow to Change IP

□ Web Protection

□ FireWall

□ EPS App Control

□ EPS USB

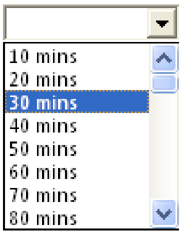
□ Mail Anti-Virus & Anti-Spam

* Password is case-sensitive

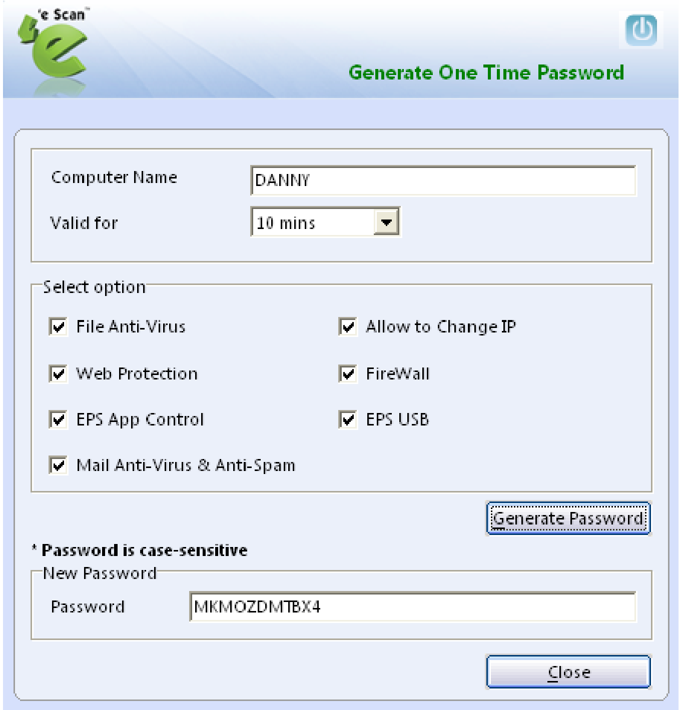
New Password

Password

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



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



Computer Name: DANNY

Valid for: 10 mins

Select option

☑ File Anti-Virus ☑ Allow to Change IP

☑ Web Protection ☑ FireWall

☑ EPS App Control ☑ EPS USB

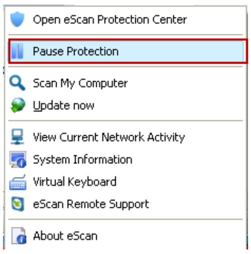
☑ Mail Anti-Virus & Anti-Spam

* Password is case-sensitive

New Password

Password: MKMOZDMTBX4

8. Send this password to the user.
9. To Pause the selected module on his computer, the user should open eScan ISS for Business Client using right click on eScan ISS for Business icon and click on Pause Protection from the task bar.



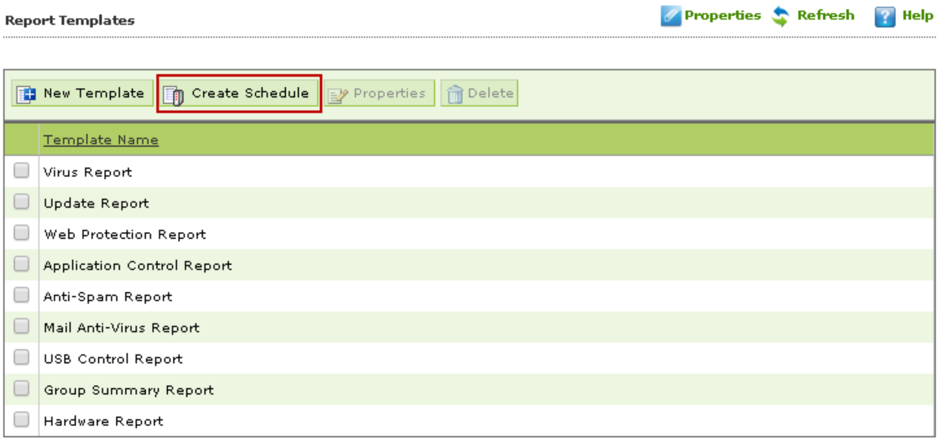
Managing and Scheduling Reports

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

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

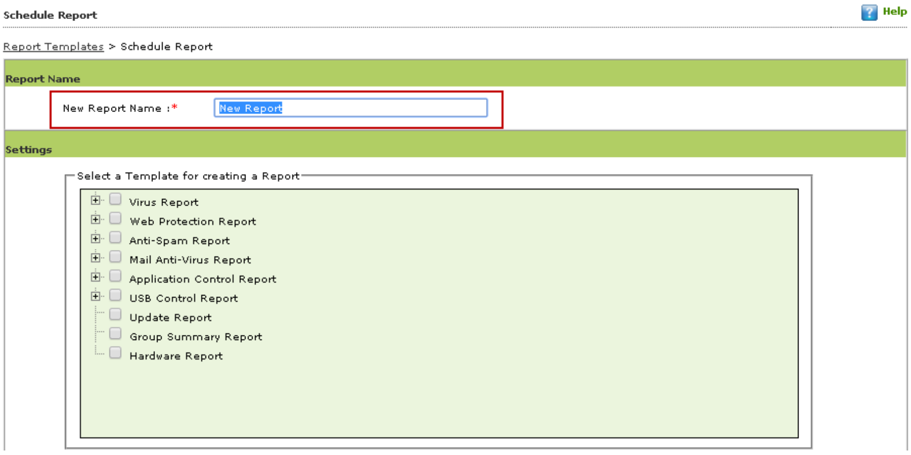
- **Scheduling an existing Report Template**

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



	Template Name
□	Virus Report
□	Update Report
□	Web Protection Report
□	Application Control Report
□	Anti-Spam Report
□	Mail Anti-Virus Report
□	USB Control Report
□	Group Summary Report
□	Hardware Report

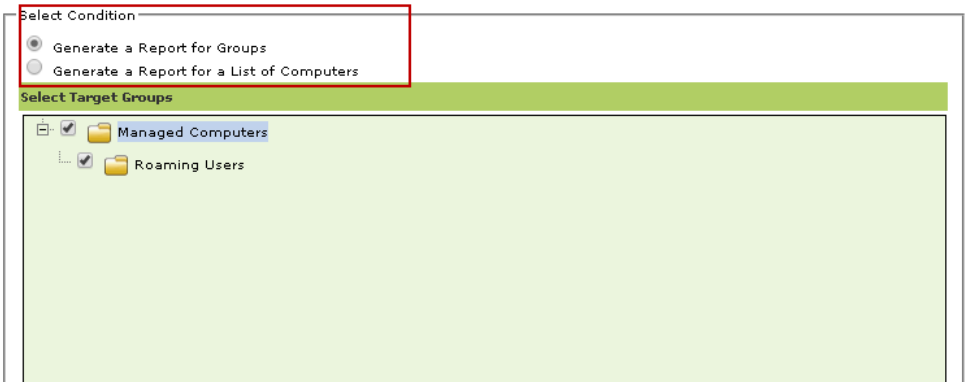
3. Now define the **Report Name** and filter the criteria for generating report by expanding the tree.



New Report Name :* New Report

Select a Template for creating a Report
- □ Virus Report
- □ Web Protection Report
- □ Anti-Spam Report
- □ Mail Anti-Virus Report
- □ Application Control Report
- □ USB Control Report
- □ Update Report
- □ Group Summary Report
- □ Hardware Report

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



Select Condition

● Generate a Report for Groups

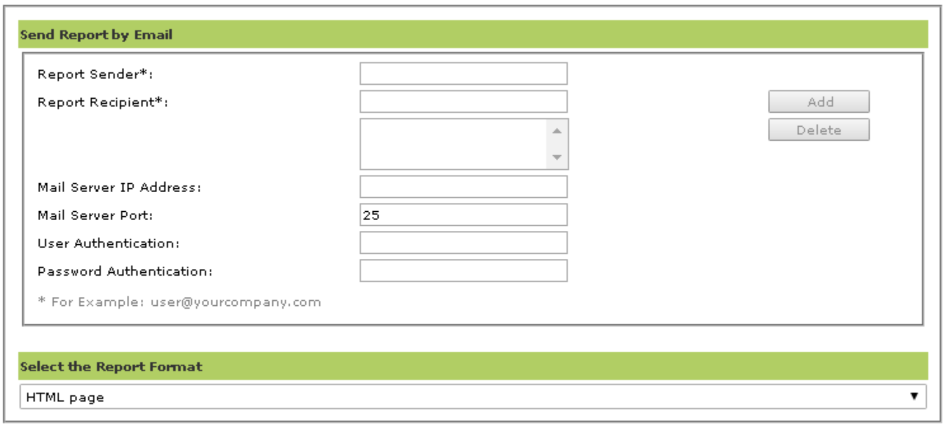
○ Generate a Report for a List of Computers

Select Target Groups

☑ Managed Computers

☑ Roaming Users

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



Send Report by Email

Report Sender*:

Report Recipient*:

Mail Server IP Address:

Mail Server Port: 25

User Authentication:

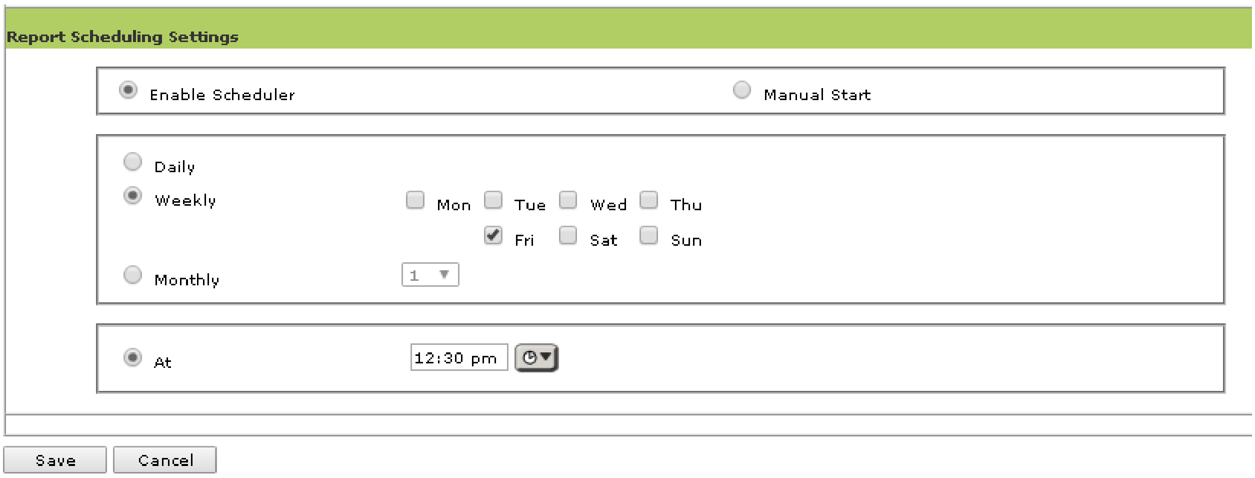
Password Authentication:

* For Example: user@yourcompany.com

Select the Report Format

HTML page

6. Schedule the report as desired and click **OK.**



Report Scheduling Settings

● Enable Scheduler ○ Manual Start

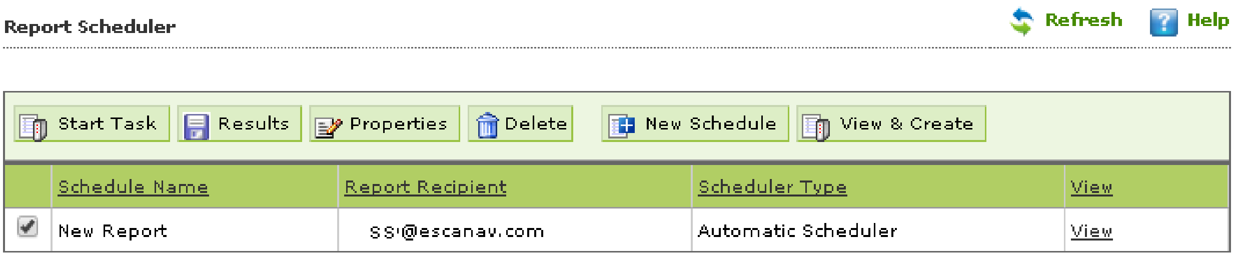
○ Daily

● Weekly □ Mon □ Tue □ Wed □ Thu ☑ Fri □ Sat □ Sun

○ Monthly 1

● At 12:30 pm

7. Once the report has been successfully scheduled it will be displayed as below.



Report Scheduler

	Schedule Name	Report Recipient	Scheduler Type	View
☑	New Report	ss'@escanav.com	Automatic Scheduler	View

Note:

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

Report Templates

Report Templates allows you to create and view customized reports based on a selected template, for a given period; sorted by date, computer, or action taken; and for a selected condition or target group. It also provides options for configuring or scheduling reports, viewing report properties, and refreshing or deleting existing reports.

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

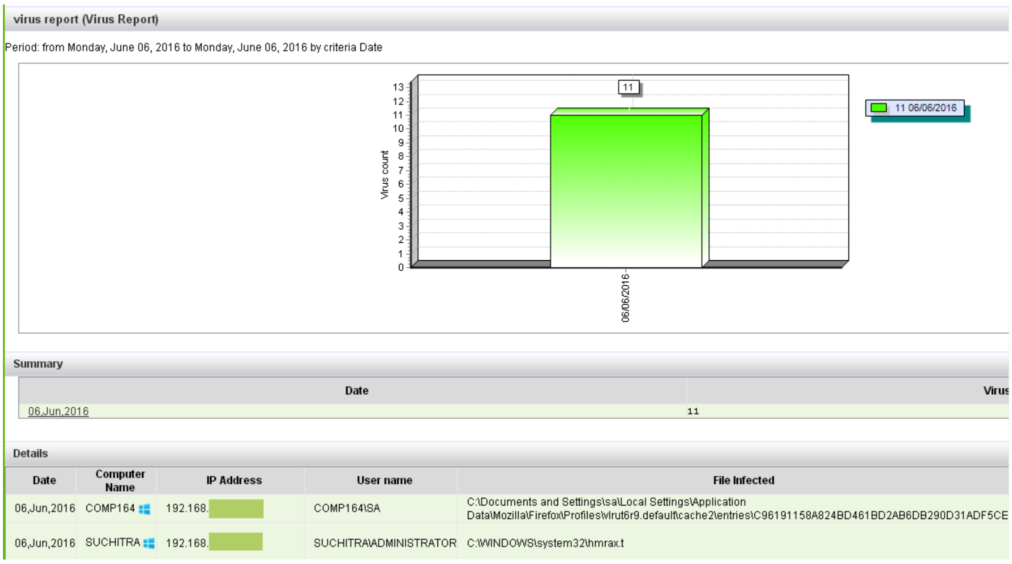
Steps for Scheduling an existing Report Template

1. Click Reports Template in the navigation bar and select the desired template.
2. Click create schedule.
3. Now define the Report Name and filter the criteria for generating report by expanding the tree.
4. Select the conditions and target groups for generating reports.
5. Define email and server settings for sending reports by mail, also select the format for the report, you can generate report in html, CSV,PDF and Excel formats, as required by you.
6. Schedule the report as desired and click oK.
7. Report will be created and scheduled instantly.
8. To save the settings and to create a report, click Save.

Report Templates

- **Virus Report** - This report displays the detailed report of Malware infection on managed computers. The report can be generated / filtered on the basis of – Date, Computer, Virus, Action taken.

  Following information is captured in the Summary Report -



virus report (Virus Report)

Period: from Monday, June 06, 2016 to Monday, June 06, 2016 by criteria Date

Summary

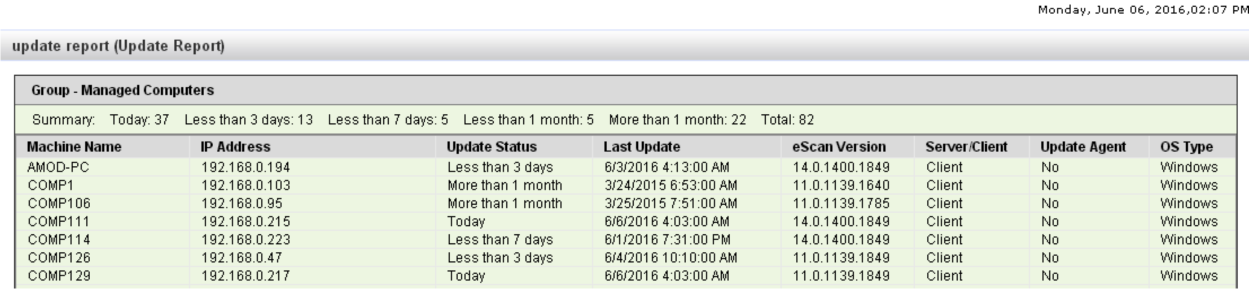
Date	Virus
06,Jun,2016	11

Details

Date	Computer Name	IP Address	User name	File Infected
06,Jun,2016	COMP164	192.168.[redacted]	COMP164\SA	C:\Documents and Settings\sa\Local Settings\Application Data\Mozilla\Firefox\Profiles\wlrut6r9.default\cache2\entries\C96191158A824BD461BD2AB6DB290D31ADF5CE
06,Jun,2016	SUCHITRA	192.168.[redacted]	SUCHITRA\ADMINISTRATOR	C:\WINDOWS\system32\hmrax.t

  - Virus Count – Displays the total number of virus count in managed computers
  - Date - Displays the date on which the malware was detected
  - Computer Name - Displays the computer name on which the malware was detected
  - IP Address – Displays the IP address of the computer where malware was detected
  - Username – Displays the username of the computer where malware was detected
  - File Infected – Displays the details of the file that is infected on the managed endpoint

- **Update Report** – This report displays the update status of all managed endpoints. Following information is captured in the report –



Monday, June 06, 2016,02:07 PM

update report (Update Report)

Group - Managed Computers

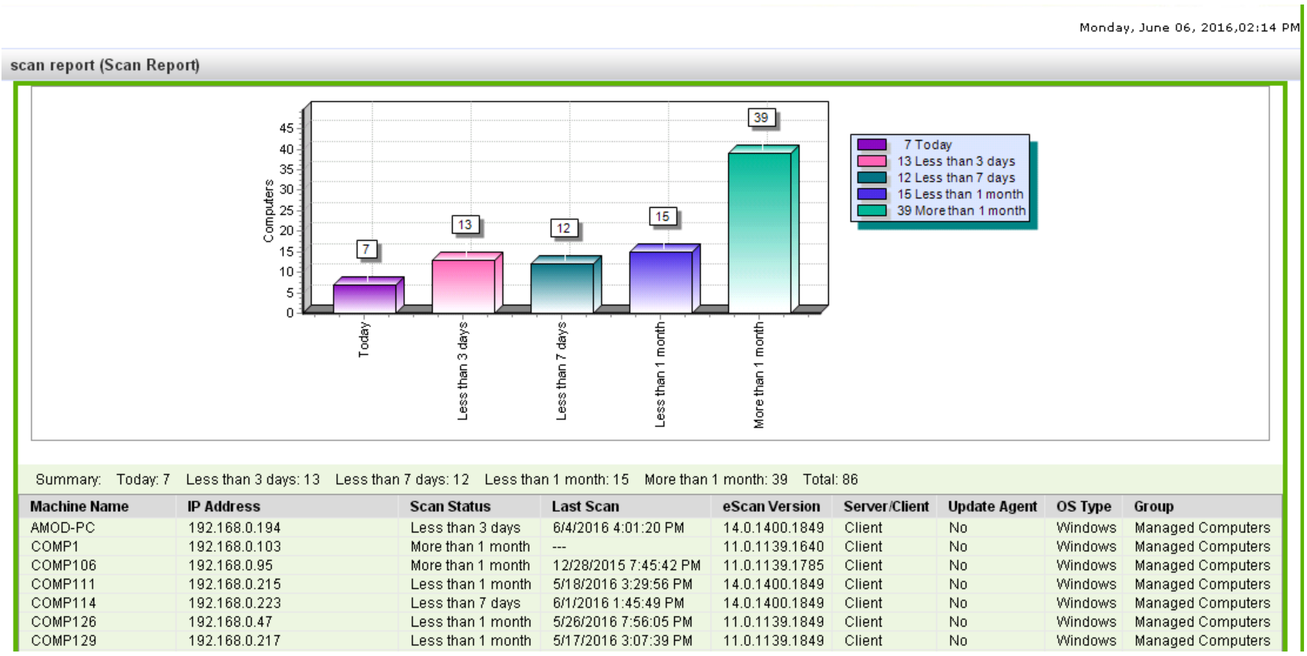
Summary: Today: 37 Less than 3 days: 13 Less than 7 days: 5 Less than 1 month: 5 More than 1 month: 22 Total: 82

Machine Name	IP Address	Update Status	Last Update	eScan Version	Server/Client	Update Agent	OS Type
AMOD-PC	192.168.0.194	Less than 3 days	6/3/2016 4:13:00 AM	14.0.1400.1849	Client	No	Windows
COMP1	192.168.0.103	More than 1 month	3/24/2015 6:53:00 AM	11.0.1139.1640	Client	No	Windows
COMP106	192.168.0.95	More than 1 month	3/25/2015 7:51:00 AM	11.0.1139.1785	Client	No	Windows
COMP111	192.168.0.215	Today	6/6/2016 4:03:00 AM	14.0.1400.1849	Client	No	Windows
COMP114	192.168.0.223	Less than 7 days	6/1/2016 7:31:00 PM	14.0.1400.1849	Client	No	Windows
COMP126	192.168.0.47	Less than 3 days	6/4/2016 10:10:00 AM	11.0.1139.1849	Client	No	Windows
COMP129	192.168.0.217	Today	6/6/2016 4:03:00 AM	11.0.1139.1849	Client	No	Windows

  - Machine Name - Displays the name of machine.
  - IP Address – Displays the IP Address
  - Update Status – Update status of the machine

- Last Update – Displays the date on when eScan was last updated
- eScan Version – Displays the version of eScan installed on the endpoint
- Server / Client – Displays whether the eScan Server is installed or eScan client is installed on the computer
- Update Agent – Displays whether the system is an update agent for the group or not
- OS Type - Displays the OS (Operating system) type of the endpoint

- **Scan Report –** It displays the scan report of all connected endpoints, following information is captured in the report.



Monday, June 06, 2016,02:14 PM

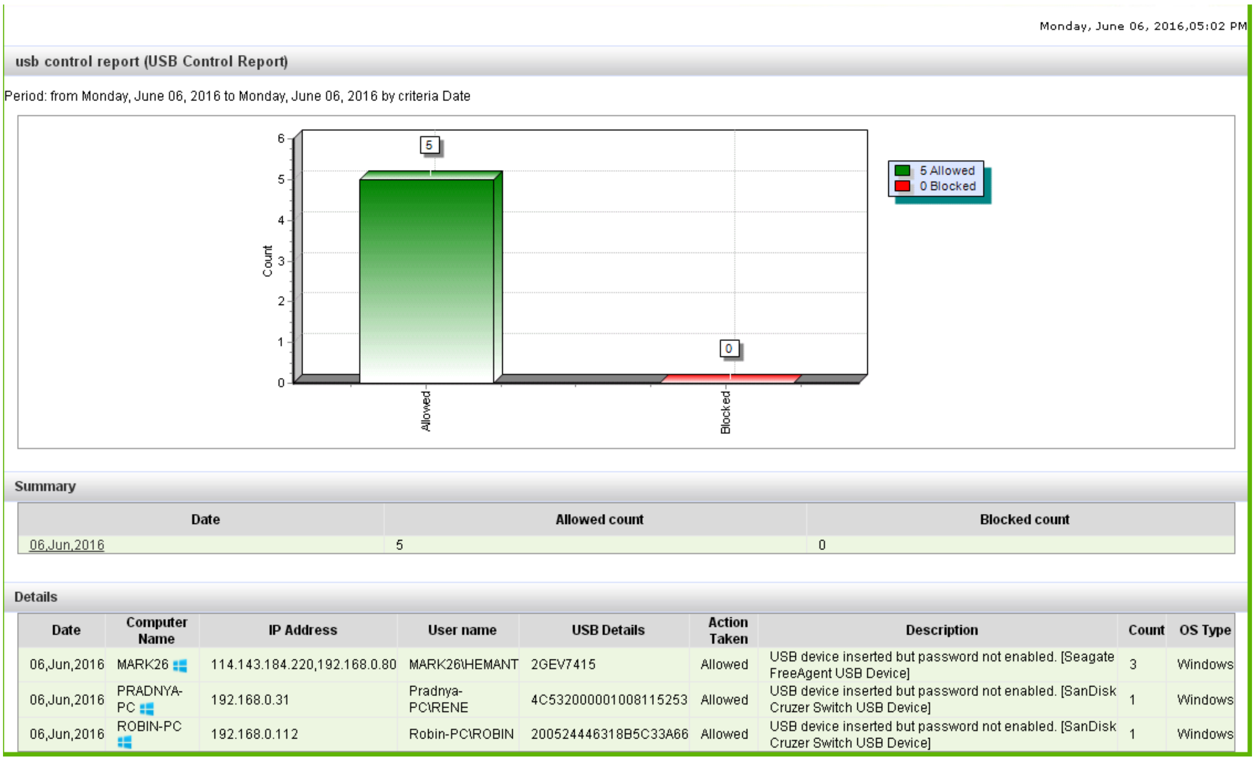
scan report (Scan Report)

Summary: Today: 7 Less than 3 days: 13 Less than 7 days: 12 Less than 1 month: 15 More than 1 month: 39 Total: 86

Machine Name	IP Address	Scan Status	Last Scan	eScan Version	Server/Client	Update Agent	OS Type	Group
AMOD-PC	192.168.0.194	Less than 3 days	6/4/2016 4:01:20 PM	14.0.1400.1849	Client	No	Windows	Managed Computers
COMP1	192.168.0.103	More than 1 month	---	11.0.1139.1640	Client	No	Windows	Managed Computers
COMP106	192.168.0.95	More than 1 month	12/28/2015 7:45:42 PM	11.0.1139.1785	Client	No	Windows	Managed Computers
COMP111	192.168.0.215	Less than 1 month	5/18/2016 3:29:56 PM	14.0.1400.1849	Client	No	Windows	Managed Computers
COMP114	192.168.0.223	Less than 7 days	6/1/2016 1:45:49 PM	14.0.1400.1849	Client	No	Windows	Managed Computers
COMP126	192.168.0.47	Less than 1 month	5/26/2016 7:56:05 PM	11.0.1139.1849	Client	No	Windows	Managed Computers
COMP129	192.168.0.217	Less than 1 month	5/17/2016 3:07:39 PM	11.0.1139.1849	Client	No	Windows	Managed Computers

  - Machine Name - Displays the name of machine.
  - IP Address – Displays the IP Address
  - Scan Status – Scan status of the machine i.e. – Last scan date and time of the endpoint
  - eScan Version – Displays the version of eScan installed on the endpoint
  - Server / Client – Displays whether the eScan Server is installed or eScan client is installed on the computer
  - Update Agent – Displays whether the system is an update agent for the group or not
  - OS Type - Displays the OS type of the endpoint
  - Group - Displays the group name to which the managed endpoint belongs

- **Anti-Spam Report -** Displays the Anti -Spam report for the managed endpoints based on Date, Computer and Action taken.
- **Mail AV report -** Displays Mail AV report for the managed endpoints based on Date, Computer and Action taken.
- **USB Control Report -** Displays the USB Control report for managed endpoints based on Date, Computer, and Action Taken. Following details are captured in the report –



Monday, June 06, 2016,05:02 PM

usb control report (USB Control Report)

Period: from Monday, June 06, 2016 to Monday, June 06, 2016 by criteria Date

Summary

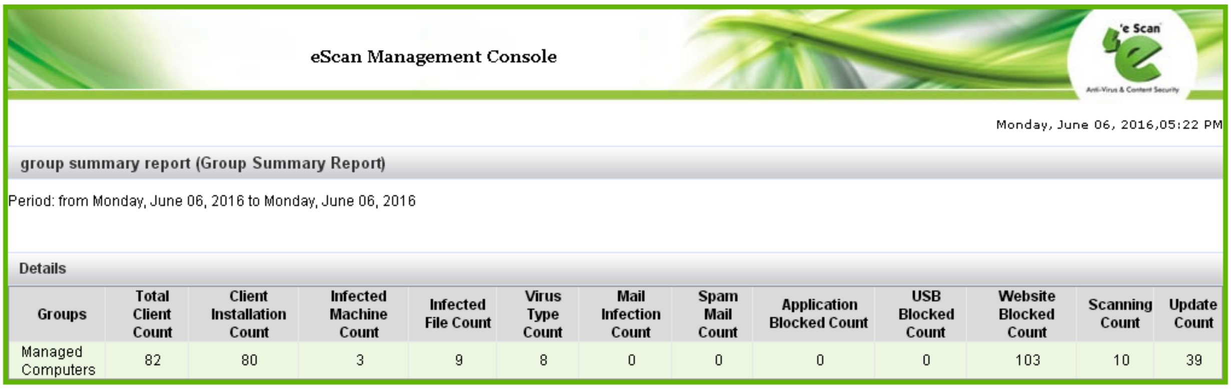
Date	Allowed count	Blocked count
06,Jun,2016	5	0

Details

Date	Computer Name	IP Address	User name	USB Details	Action Taken	Description	Count	OS Type
06,Jun,2016	MARK26	114.143.184.220,192.168.0.80	MARK26\HEMANT	2GEV7415	Allowed	USB device inserted but password not enabled. [Seagate FreeAgent USB Device]	3	Windows
06,Jun,2016	PRADNYA-PC	192.168.0.31	Pradnya-PC\RENE	4C532000001008115253	Allowed	USB device inserted but password not enabled. [SanDisk Cruzer Switch USB Device]	1	Windows
06,Jun,2016	ROBIN-PC	192.168.0.112	Robin-PC\ROBIN	200524446318B5C33A66	Allowed	USB device inserted but password not enabled. [SanDisk Cruzer Switch USB Device]	1	Windows

- Date - Displays the date for which the information was captured.
- Computer Name - Displays the name of machine.
- IP Address – Displays the IP Address.
- Username – Displays the username of the computer for which Protection report was captured.
- USB Details – Displays the Serial number of the Pen drive.
- Action taken – Displays the Action taken by eScan such as Allowed or blocked.
- Description – Displays the details of the action taken.
- Count – Displays the number of times the infection was detected.
- OS type – Displays the OS type of the managed endpoint.

- **Group Summary Report –** It captures security status of all managed endpoints in the group. Following details are captured in the group.



eScan Management Console

Monday, June 06, 2016,05:22 PM

group summary report (Group Summary Report)

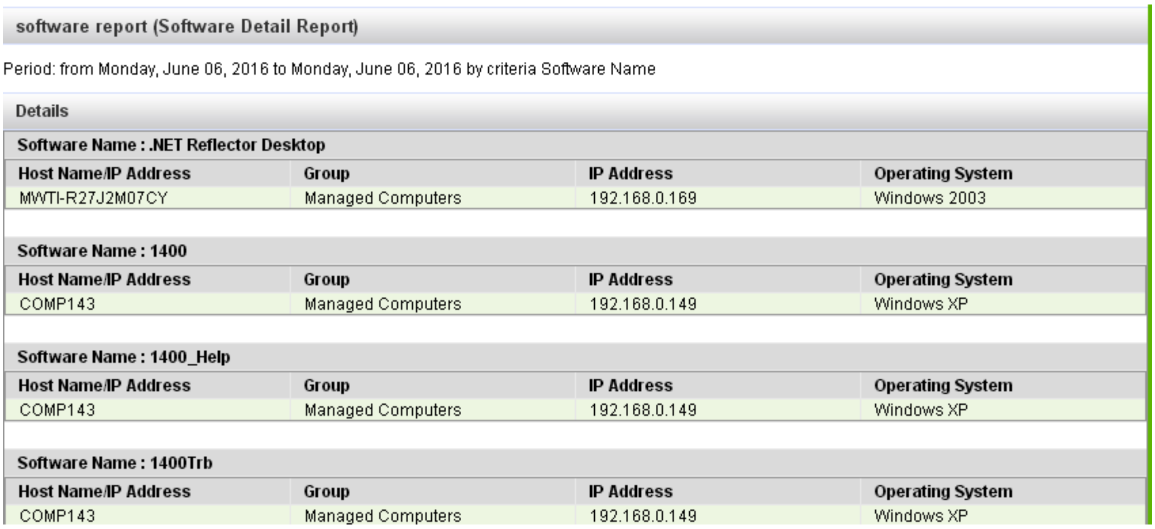
Period: from Monday, June 06, 2016 to Monday, June 06, 2016

Details

Groups	Total Client Count	Client Installation Count	Infected Machine Count	Infected File Count	Virus Type Count	Mail Infection Count	Spam Mail Count	Application Blocked Count	USB Blocked Count	Website Blocked Count	Scanning Count	Update Count
Managed Computers	82	80	3	9	8	0	0	0	0	103	10	39

- **Hardware Report Summary –** It captures change in hardware on all managed endpoints in the group. Following details are captured in the group.
    - Computer Name
    - Group
    - IP Address
    - Username
    - OS name
    - Service Pack
    - OS version
    - OS installed Date
    - Internet Explorer
    - Processor
    - Motherboard Details
    - RAM details
    - Hard disk details
    - Mac Address
    - Local Adapter
    - Wi-Fi Adapter
    - Motherboard serial number
    - Client OS type

- **Software Report Summary –** It displays the report for number of software installed on managed endpoints. Report can be generated on the basis of Computer or Software installed. It captures following Data –



software report (Software Detail Report)

Period: from Monday, June 06, 2016 to Monday, June 06, 2016 by criteria Software Name

Details

Software Name : .NET Reflector Desktop

Host Name/IP Address	Group	IP Address	Operating System
MWTI-R27J2M07CY	Managed Computers	192.168.0.169	Windows 2003

Software Name : 1400

Host Name/IP Address	Group	IP Address	Operating System
COMP143	Managed Computers	192.168.0.149	Windows XP

Software Name : 1400_Help

Host Name/IP Address	Group	IP Address	Operating System
COMP143	Managed Computers	192.168.0.149	Windows XP

Software Name : 1400Trb

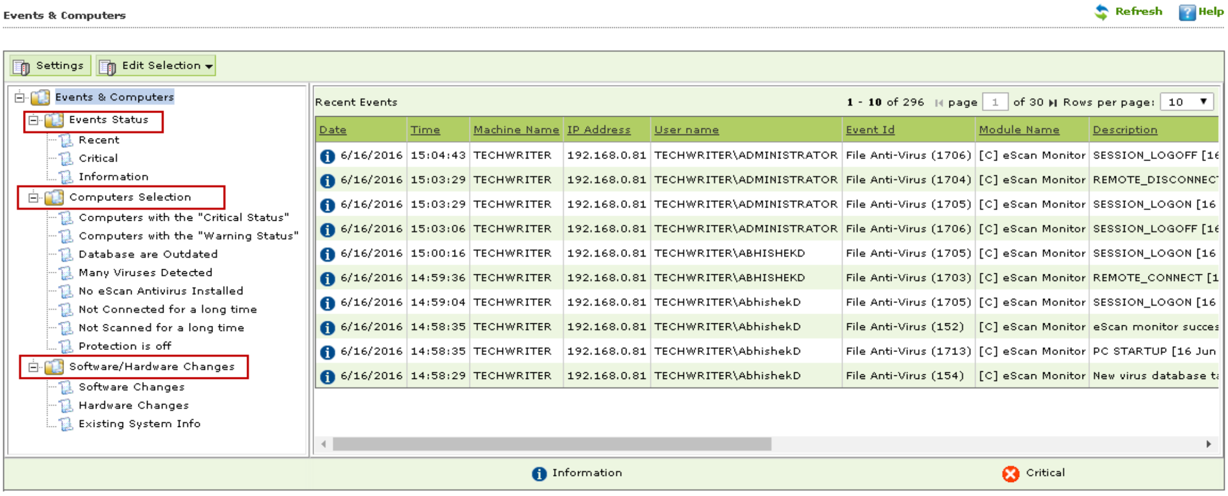
Host Name/IP Address	Group	IP Address	Operating System
COMP143	Managed Computers	192.168.0.149	Windows XP

- Period for which the report is generated
- Software name
- Host name / IP address on which the software was installed
- Group to which the endpoint belongs to
- IP Address of the endpoint where software was installed
- Operating System of the endpoint

Note:
Apart from the default templates available in eScan Management Console, administrator can create customized report template as required by him.

Viewing Events

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



Recent Events 1 - 10 of 296 page 1 of 30 Rows per page: 10

Date	Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
6/16/2016	15:04:43	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (1706)	[C] eScan Monitor	SESSION_LOGOFF [16
6/16/2016	15:03:29	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (1704)	[C] eScan Monitor	REMOTE_DISCONNEC
6/16/2016	15:03:29	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (1705)	[C] eScan Monitor	SESSION_LOGON [16
6/16/2016	15:03:06	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (1706)	[C] eScan Monitor	SESSION_LOGOFF [16
6/16/2016	15:00:16	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (1705)	[C] eScan Monitor	SESSION_LOGON [16
6/16/2016	14:59:36	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (1703)	[C] eScan Monitor	REMOTE_CONNECT [1
6/16/2016	14:59:04	TECHWRITER	192.168.0.81	TECHWRITER\AbhishekD	File Anti-Virus (1705)	[C] eScan Monitor	SESSION_LOGON [16
6/16/2016	14:58:35	TECHWRITER	192.168.0.81	TECHWRITER\AbhishekD	File Anti-Virus (152)	[C] eScan Monitor	eScan monitor succes
6/16/2016	14:58:35	TECHWRITER	192.168.0.81	TECHWRITER\AbhishekD	File Anti-Virus (1713)	[C] eScan Monitor	PC STARTUP [16 Jun
6/16/2016	14:58:29	TECHWRITER	192.168.0.81	TECHWRITER\AbhishekD	File Anti-Virus (154)	[C] eScan Monitor	New virus database ta

- **Event Status**

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

- **Computer Selection**

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

Node Name	Description
Computer with critical status	This node records all the system that has critical status.
Computer with warning status	This node will display all the system with warning status.
Database is outdated	This node will display all the systems with older/outdated virus database.
Many Viruses Detected	When the virus count exceeds the specified limit that system will fall in this node.
No eScan Installed	Computers where eScan client is not installed will be shown in this node
Not connected for a long	This node will have the systems that are not connected to the

time	server (status can’t be taken by the server) for a long time.
Not scanned for a long time	This node will show all the systems which are not scanned for a long time (specified time).
Protection is off	The system whose File Protection is disabled will fall under this node. We can specify the option by which Protection status will be checked.

- **Software/Hardware Changes**

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

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

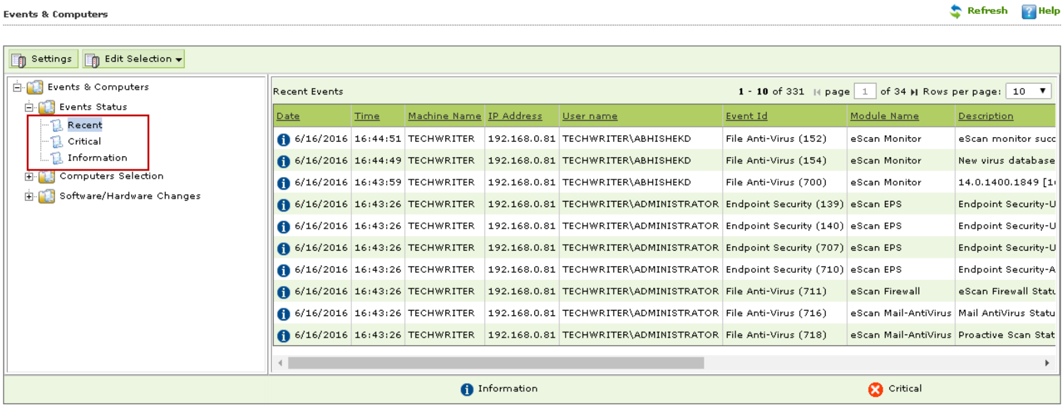
- **Defining Settings**

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

A. Event Status

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

- **Event Name**



Recent Events 1 - 10 of 331 page 1 of 34 Rows per page: 10

Date	Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
6/16/2016	16:44:51	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (152)	eScan Monitor	eScan monitor succ
6/16/2016	16:44:49	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (154)	eScan Monitor	New virus database
6/16/2016	16:43:59	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (700)	eScan Monitor	14.0.1400.1849 [1
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (139)	eScan EPS	Endpoint Security-U
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (140)	eScan EPS	Endpoint Security-U
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (707)	eScan EPS	Endpoint Security-U
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (710)	eScan EPS	Endpoint Security-A
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (711)	eScan Firewall	eScan Firewall Statu
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (716)	eScan Mail-AntiVirus	Mail AntiVirus Statu
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (718)	eScan Mail-AntiVirus	Proactive Scan Stat

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

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.

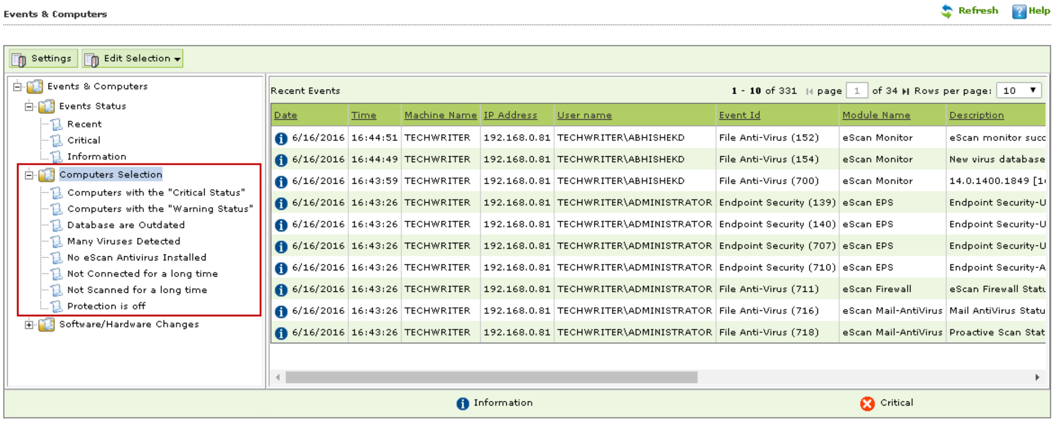
- **Critical:** It displays all critical events occurred on managed client computers, such as virus detection, monitor disabled status, and so on.
- **Information:** It displays all informative type of events, such as virus database update, status, and so on.

Saving event status settings

Perform the following steps to save the event status settings:

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

B. Computer Selection



Events & Computers

Events & Computers
- Events Status
  - Recent
  - Critical
  - Information
- Computers Selection
  - 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
- Software/Hardware Changes

Recent Events 1 - 10 of 331 page 1 of 34 Rows per page: 10

Date	Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
6/16/2016	16:44:51	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (152)	eScan Monitor	eScan monitor succ
6/16/2016	16:44:49	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (154)	eScan Monitor	New virus database
6/16/2016	16:43:59	TECHWRITER	192.168.0.81	TECHWRITER\ABHISHEKD	File Anti-Virus (700)	eScan Monitor	14.0.1400.1849 [1
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (139)	eScan EPS	Endpoint Security-U
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (140)	eScan EPS	Endpoint Security-U
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (707)	eScan EPS	Endpoint Security-U
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	Endpoint Security (710)	eScan EPS	Endpoint Security-A
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (711)	eScan Firewall	eScan Firewall Statu
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (716)	eScan Mail-AntiVirus	Mail AntiVirus Statu
6/16/2016	16:43:26	TECHWRITER	192.168.0.81	TECHWRITER\ADMINISTRATOR	File Anti-Virus (718)	eScan Mail-AntiVirus	Proactive Scan Stat

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

- **Computers**

  - Types and criteria of **Computer Status**

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

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

Field	Description
Check for eScan Not Installed	Select this check box 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 to view the client systems on which eScan monitor is not enabled.
Check for Not Scanned	Select this check box to view the list of client systems which has not been scanned.
Check for Database Not Updated	Select this check box to view the list of client systems on which database has not been updated.
Check for Not Connected	Select this check box 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; eScan database not updated for the mentioned days will be listed.
System Not Scanned for more than	Type the number; system not scanned for the mentioned days will be listed.
System Not Connected for more than	Type the number; client systems not connected to eScan server for the mentioned days will be listed here.
Number Of Records	Type the number of client systems that you want to view in the list.

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

Field	**Description**
Check for Not Scanned	Select this check box to view the list of client systems that are not scanned.
Check for Database Not Updated	Select this check box to view the list of client systems on which database has not been updated.
Check for Not Connected	Select this check box to view the list of eScan client systems that are not communicating with eScan server.
Check for Protection off	Select this check box 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 to view the list of client systems on which maximum viruses are detected.
Database Not Updated from more than	Type the number of days from when the database has not been updated.
System Not Scanned for more than	Type the number of days from when the system has not been scanned.
System Not Connected for more than	Type the number of days from when the client system has not been connected to eScan server.
Number Of Virus	Type the number of viruses detected on client system.

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

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

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

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

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

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

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

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

Field	**Description**
System Not Connected from more than	Type the number. A system not connected to the server for the mentioned days will be listed.
Number Of Records	Type the number of client systems that you want to view in the list.

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

Field	**Description**
System Not Scanned for more than	Type the number. A system not scanned for the mentioned days will be listed.
Number Of Records	Type the number of client system that you want to view in the list.

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

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

Saving computer settings

Perform the following steps to save the computer settings:

1. Click the **Computers Selection** tab.
2. Select type of status for which you want to set criteria, from the **Computer status** drop-down list.
3. Select the appropriate check boxes, and then type field details in the available fields. For more information, refer [Types and criteria's of computer status-] section.
4. Click the '***Save'*** button to save the settings.

C. Software/ Hardware Changes

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

- **Updates**

  - Type of **Updates**

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

Changing software/hardware settings

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

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

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

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

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

Asset Management

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

- **Viewing Hardware Reports**

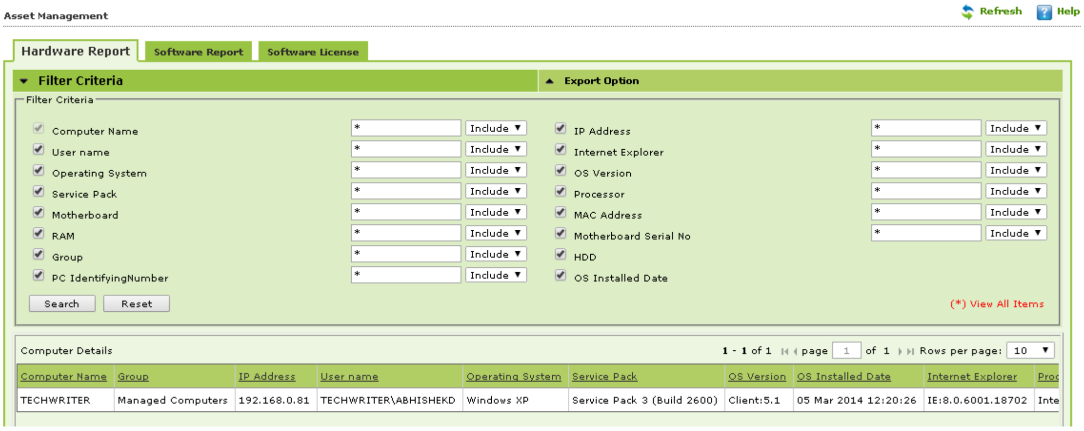
For Viewing the Hardware Configuration of all the Managed Computers connected to the Network, click on Asset Management section present in the Navigation Panel on the left in the eScan Management Console. Following Information will populate in the table on the right.

Sr.No.	Column Name	Description
1.	**Computer Name**	It displays the Host Name of the Computers as defined by the Administrator.
2.	**Group**	It displays the Name of the Group to which that Computer belongs to, as defined in Managed Computer section of eScan Management Console.
3.	**IP Address**	It displays the IP address of the Endpoints.
4.	**User Name**	It displays the current Username of the Endpoints (who is logged on the system).
5.	**Operating System**	It displays the Operating system installed on the Endpoints.
6.	**Service Pack**	It displays the Service Pack version and build installed on the Endpoints.
7.	**OS Version**	It displays the version of the Operating system installed in the Endpoints.
8.	**OS Installed Date**	It displays the Date and Time of Installation of the Operating system on the Endpoints.
9.	**Internet Explorer**	It displays the version of internet explorer installed on the Endpoints.
10.	**Processor**	It displays the Processor details like Processor Name, Type and Processing Speed of the Endpoints.
11.	**Motherboard**	It displays the details of the motherboard of the Endpoints.
12.	**RAM**	It displays the details of the RAM installed on the Endpoints.
13.	**HDD**	It displays the details of the Hard Disk like number of Partitions and their respective sizes.

14.	**MAC Address**	It displays the MAC Address of the Endpoints.
15.	**Software**	By clicking on the view link present in this Column, you can view the list of softwares along with the installation dates on the Managed Computer.

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

For Filtering the Hardware Report as per your requirements, click on the drop Menu Link of Filter Criteria ▲ Filter Criteria in **Asset Management** section. The Hardware report can be filtered on the basis of following Criteria.



☑	Computer Name	*	Include ▼	☑	IP Address	*	Include ▼
☑	User name	*	Include ▼	☑	Internet Explorer	*	Include ▼
☑	Operating System	*	Include ▼	☑	OS Version	*	Include ▼
☑	Service Pack	*	Include ▼	☑	Processor	*	Include ▼
☑	Motherboard	*	Include ▼	☑	MAC Address	*	Include ▼
☑	RAM	*	Include ▼	☑	Motherboard Serial No	*	Include ▼
☑	Group	*	Include ▼	☑	HDD		
☑	PC IdentifyingNumber	*	Include ▼	☑	OS Installed Date		

1 - 1 of 1 page 1 of 1 Rows per page: 10

Computer Name	Group	IP Address	User name	Operating System	Service Pack	OS Version	OS Installed Date	Internet Explorer	Proc
TECHWRITER	Managed Computers	192.168.0.81	TECHWRITER\ABHISHEKD	Windows XP	Service Pack 3 (Build 2600)	Client:5.1	05 Mar 2014 12:20:26	IE:8.0.6001.18702	Inte

Note:

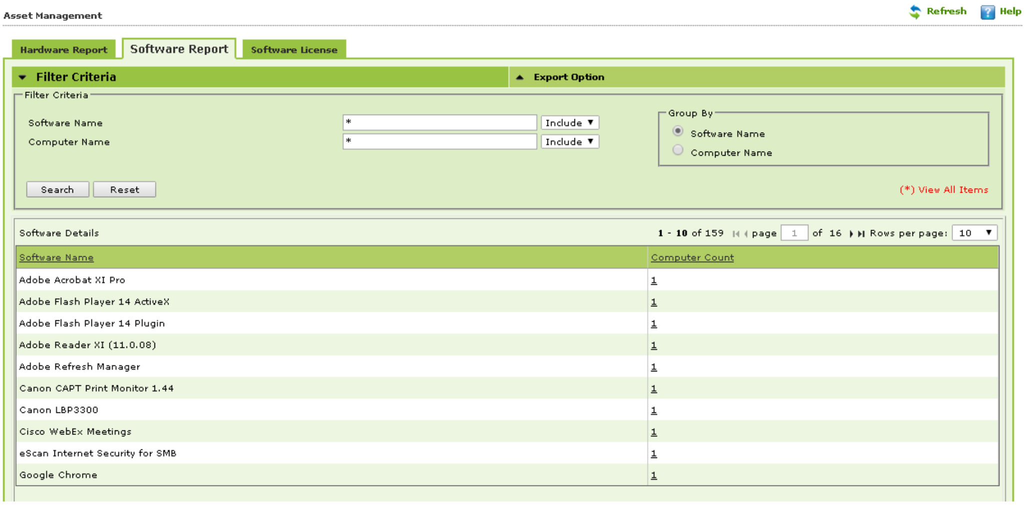
- You can define criteria for the text / Column Content to be included or excluded in your Search result using the drop downs present on the interface.

- **Viewing the Software Report**

This section displays list of Software along with the number of Endpoints on which it is installed. To view the Software Report, click Asset Management and then click Software Report Tab present on the right. This will populate the Software Name with computer count in a tabular format.

For knowing the computer details where specific Software is installed, click on the computer count present in the computer count column. A window with the respective computer details will pop up.

For filtering the software report, click on the Filter Criteria drop down ▲ Filter Criteria in Asset Management section. The software report can be filtered on the basis of following criteria.



Filter Criteria

Software Name: * Include ▼

Computer Name: * Include ▼

Group By
● Software Name
○ Computer Name

(*) View All Items

Software Details — 1 - 10 of 159, page 1 of 16, Rows per page: 10

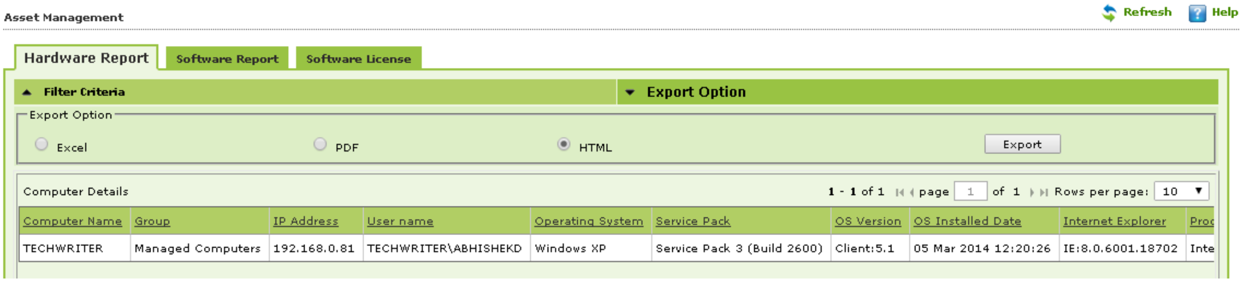
Software Name	Computer Count
Adobe Acrobat XI Pro	1
Adobe Flash Player 14 ActiveX	1
Adobe Flash Player 14 Plugin	1
Adobe Reader XI (11.0.08)	1
Adobe Refresh Manager	1
Canon CAPT Print Monitor 1.44	1
Canon LBP3300	1
Cisco WebEx Meetings	1
eScan Internet Security for SMB	1
Google Chrome	1

You can filter your search on the basis of the options provided; using the drop down, you can either include or exclude or by checking or unchecking the check box a particular criteria can be added or excluded.

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

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

It can easily be done by clicking on Export Option drop down ▲ Export Option in **Asset Management** Section. It will display the following options.

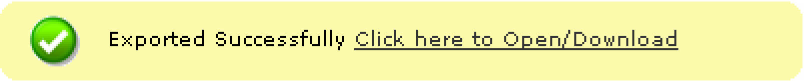


Export Option
○ Excel ○ PDF ● HTML

Computer Details — 1 - 1 of 1, page 1 of 1, Rows per page: 10

Computer Name	Group	IP Address	User name	Operating System	Service Pack	OS Version	OS Installed Date	Internet Explorer	Proc
TECHWRITER	Managed Computers	192.168.0.81	TECHWRITER\ABHISHEKD	Windows XP	Service Pack 3 (Build 2600)	Client:5.1	05 Mar 2014 12:20:26	IE:8.0.6001.18702	Inte

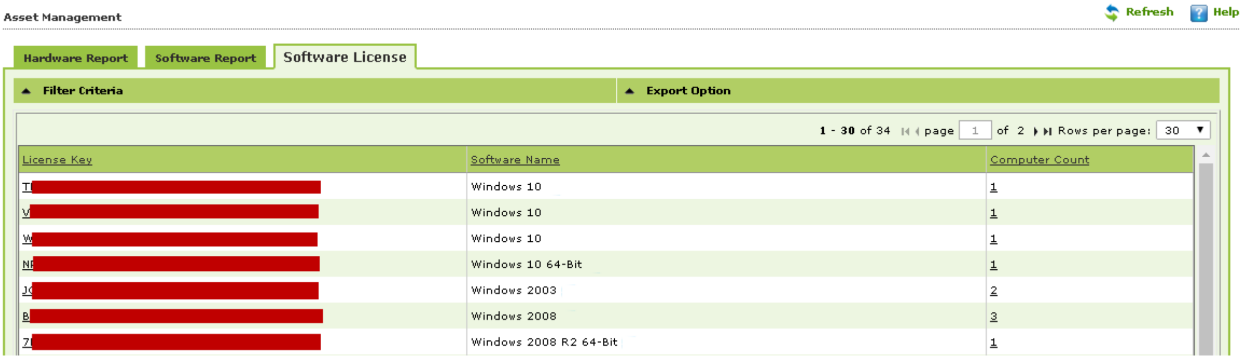
Click on the desired Radio button for exporting the report in available formats. When the Export is over, you will be informed with the following message –


Exported Successfully Click here to Open/Download

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

- **Software Licensing**

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



1 - 30 of 34 page 1 of 2 Rows per page: 30

License Key	Software Name	Computer Count
[redacted]	Windows 10	1
[redacted]	Windows 10	1
[redacted]	Windows 10	1
[redacted]	Windows 10 64-Bit	1
[redacted]	Windows 2003	2
[redacted]	Windows 2008	3
[redacted]	Windows 2008 R2 64-Bit	1

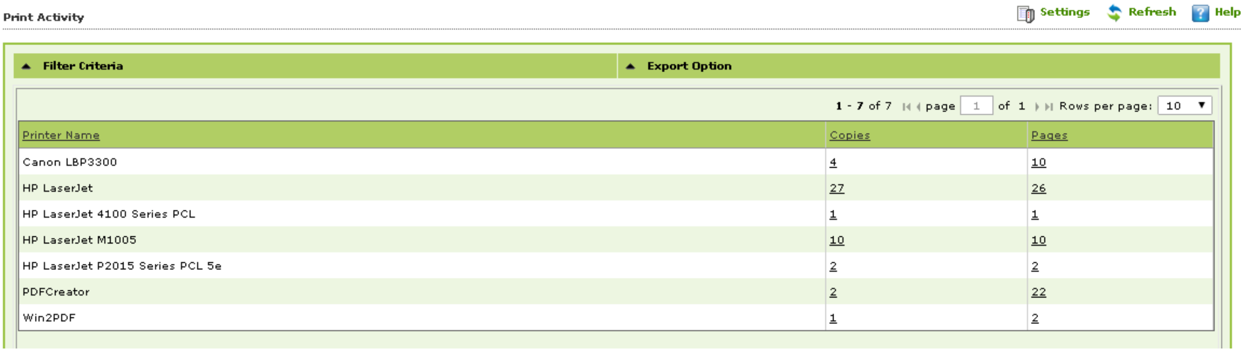
User Activity

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

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

- **Viewing the Print Activity Log**

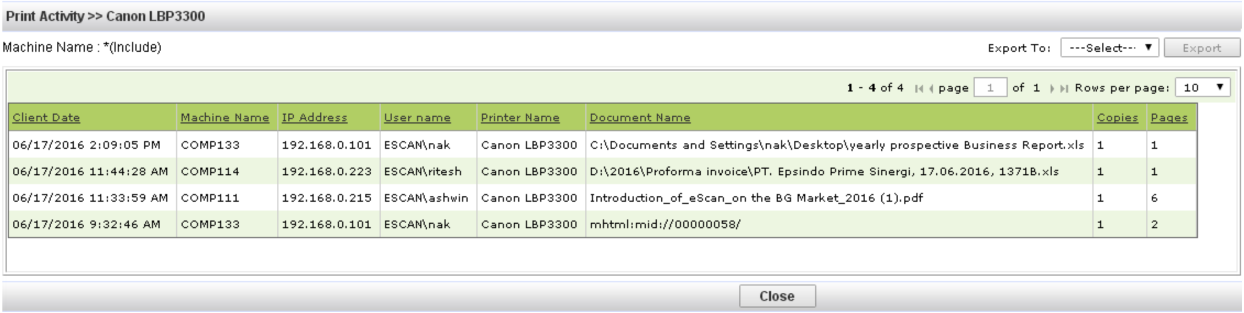
  Click **Print Activity** under dashboard on the left in eScan Management Console. A table with the list of printers and number of copies printed by them will populate on right. Options for filtering or exporting the log in desired formats are also present on the same interface.



Printer Name	Copies	Pages
Canon LBP3300	4	10
HP LaserJet	27	26
HP LaserJet 4100 Series PCL	1	1
HP LaserJet M1005	10	10
HP LaserJet P2015 Series PCL 5e	2	2
PDFCreator	2	22
Win2PDF	1	2

- **Viewing the Print Logs**

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

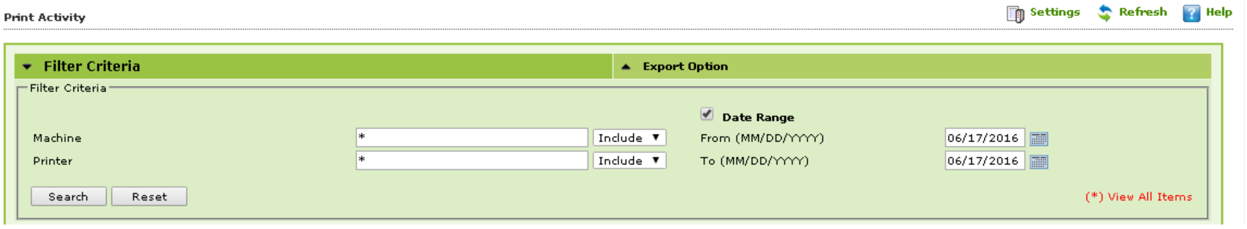

Print Activity >> Canon LBP3300
Machine Name : *(Include)
Export To: ---Select--- ▼
Export
1 - 4 of 4 page 1 of 1 Rows per page: 10 ▼
Close

Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies	Pages
06/17/2016 2:09:05 PM	COMP133	192.168.0.101	ESCAN\nak	Canon LBP3300	C:\Documents and Settings\nak\Desktop\yearly prospective Business Report.xls	1	1
06/17/2016 11:44:28 AM	COMP114	192.168.0.223	ESCAN\ritesh	Canon LBP3300	D:\2016\Proforma invoice\PT. Epsindo Prime Sinergi, 17.06.2016, 1371B.xls	1	1
06/17/2016 11:33:59 AM	COMP111	192.168.0.215	ESCAN\ashwin	Canon LBP3300	Introduction_of_eScan_on the BG Market_2016 (1).pdf	1	6
06/17/2016 9:32:46 AM	COMP133	192.168.0.101	ESCAN\nak	Canon LBP3300	mhtml:mid://00000058/	1	2

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

Filter Criteria

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



Machine: * Include

Printer: * Include

☑ Date Range

From (MM/DD/YYYY): 06/17/2016

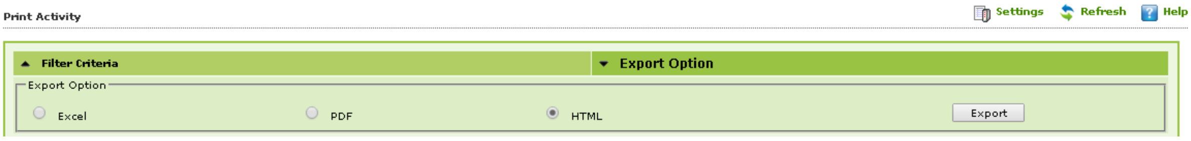
To (MM/DD/YYYY): 06/17/2016

Sr. No.	Option	Description
1.	Machine	Type the desired machine name that you wish to exclude or include in your Log.
2.	Not	Tick on this checkbox, if you wish to exclude a machine in the log report.
3.	Printer	Type the desired printer name that you wish to exclude or include in your log.
4.	Not	Tick on this checkbox, if you wish to exclude a printer to in the log report.
5.	Date Range	Tick on this checkbox, if you wish to generate report between certain dates.
6.	From((MM/DD/YYYY)	Select the starting date for report generation.
7.	To(MM/DD/YYYY)	Select the Ending date for report generation.
8.	Search	Click this option to Filter the Log on the defined criteria.
9.	Reset	Click this option to reset the defined criteria for filtering.

- **Exporting the Print Activity Log**

eScan Management Console offers exporting of Print Activity logs in PDF, Excel or HTML formats.

It can easily be done by Clicking on Drop Menu Link of Export Option ▲ Export Option in Print Activity Section. It will display the following options.

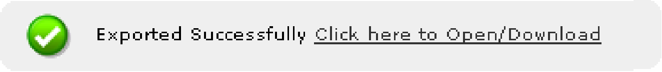


Print Activity

Export Option

○ Excel ○ PDF ● HTML

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

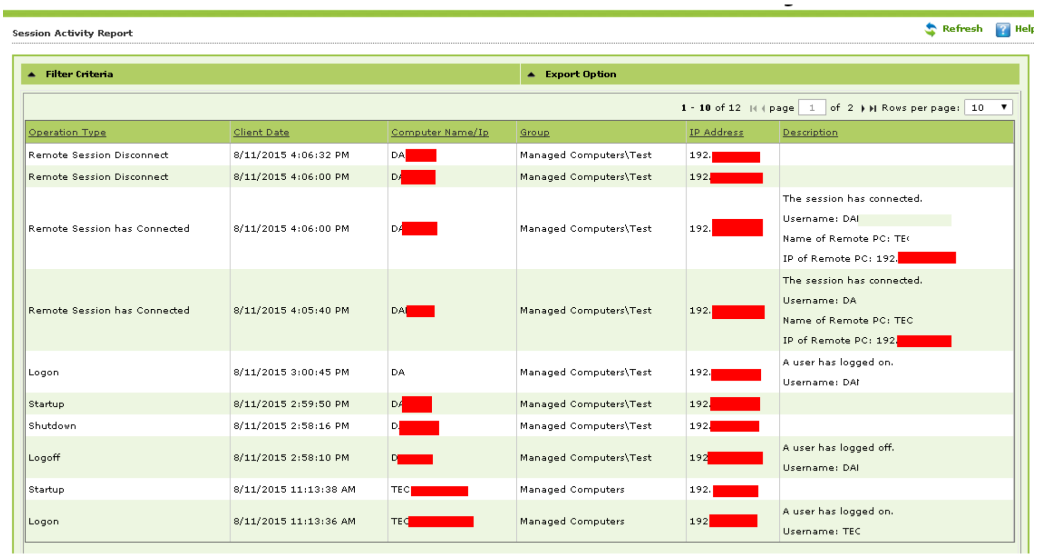


Exported Successfully Click here to Open/Download

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

- **Session Activity Report**

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



Session Activity Report

1 - 10 of 12 page 1 of 2 Rows per page: 10

Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Remote Session Disconnect	8/11/2015 4:06:32 PM	DA[redacted]	Managed Computers\Test	192.[redacted]	
Remote Session Disconnect	8/11/2015 4:06:00 PM	D[redacted]	Managed Computers\Test	192[redacted]	
Remote Session has Connected	8/11/2015 4:06:00 PM	D[redacted]	Managed Computers\Test	192.[redacted]	The session has connected. Username: DAI Name of Remote PC: TE IP of Remote PC: 192.[redacted]
Remote Session has Connected	8/11/2015 4:05:40 PM	DA[redacted]	Managed Computers\Test	192.[redacted]	The session has connected. Username: DA Name of Remote PC: TEC IP of Remote PC: 192[redacted]
Logon	8/11/2015 3:00:45 PM	DA	Managed Computers\Test	192.[redacted]	A user has logged on. Username: DAI
Startup	8/11/2015 2:59:50 PM	D[redacted]	Managed Computers\Test	192[redacted]	
Shutdown	8/11/2015 2:58:16 PM	D[redacted]	Managed Computers\Test	192[redacted]	
Logoff	8/11/2015 2:58:10 PM	D[redacted]	Managed Computers\Test	192[redacted]	A user has logged off. Username: DAI
Startup	8/11/2015 11:13:38 AM	TEC[redacted]	Managed Computers	192.[redacted]	
Logon	8/11/2015 11:13:36 AM	TE[redacted]	Managed Computers	192[redacted]	A user has logged on. Username: TEC

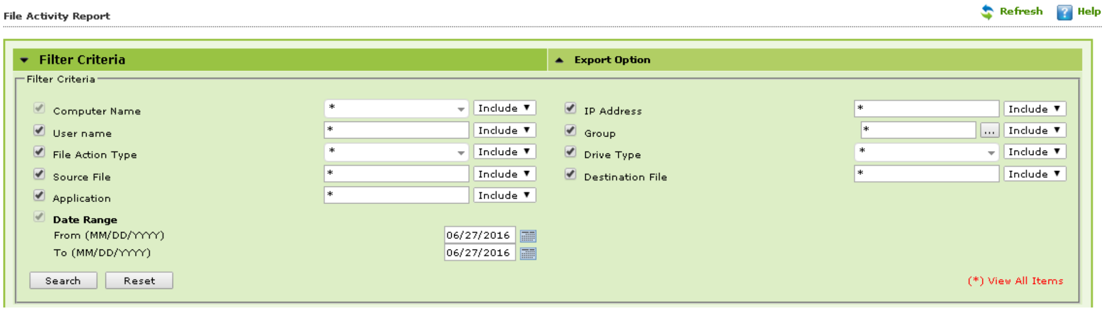
The log report generated in this section keeps the log of the operation type, computer name, group name, IP address and the description of the activity. It also gives you options for filtering the report on the basis of excluding or including the computer name, operation type, IP Address, Group, description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

- **File Activity Report**

eScan Management Console monitors and logs the file activity of the managed computers. It will display a report of the files created, copied, modified, and deleted. With this report the administrator can trace the file activities on all the managed computers. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report.

Filter Criteria

For filtering the File Activity Report as desired, click **Filter** Criteria on the main interface of File Activity Report, following options will be populated on screen.



File Activity Report

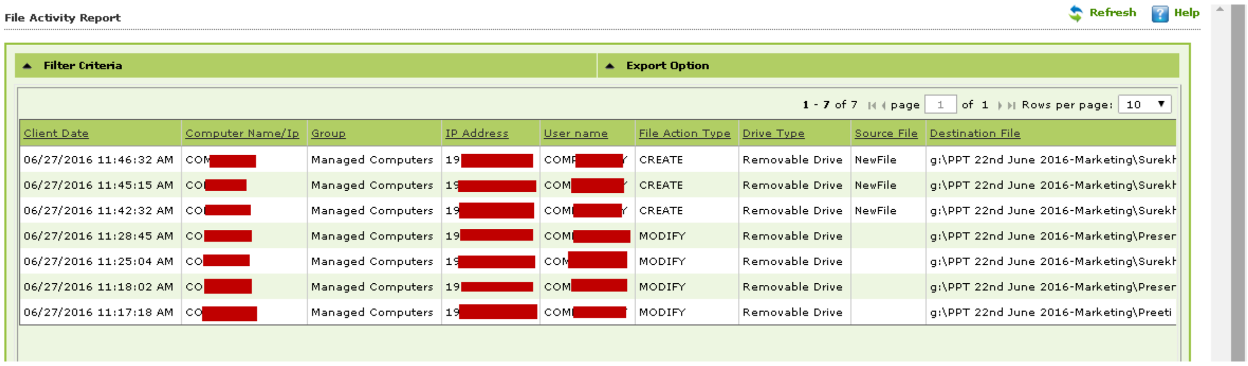
Filter Criteria

☑ Computer Name: * — Include
☑ User name: * — Include
☑ File Action Type: * — Include
☑ Source File: * — Include
☑ Application: * — Include
☑ IP Address: * — Include
☑ Group: * — Include
☑ Drive Type: * — Include
☑ Destination File: * — Include
☑ **Date Range**
From (MM/DD/YYYY): 06/27/2016
To (MM/DD/YYYY): 06/27/2016

(*) View All Items

Sr. No.	Option	Description
1.	Computer Name	This checkbox is selected by default; type the desired computer name that you wish to exclude or include in the report
2.	IP Address	Select this checkbox and type the desired IP Address that you wish to exclude or include in the report.
3.	User name	Select this checkbox and type the desired username that you wish to exclude or include in the report.
4.	Group	Select this checkbox and select the desired managed group that you would like to include or exclude in the report.
5.	File Action type	Select this check box and also select the File action type that you want to include or exclude in the report.
6.	Drive type	Select this check box and select the drive type that you want to include or exclude in the report
7.	Source File	Select this option to include or exclude the source file details in the report
8.	Destination File	Select this option to include or exclude the details of the destination file in the report
9.	Application	Select this option to include or exclude the details of the application in the report.
10.	Date Range	Tick on this checkbox, if you wish to generate report between certain dates.
11.	From((MM/DD/YYYY)	Select the starting date for report generation.
12.	To(MM/DD/YYYY)	Select the Ending date for report generation.

13.	Search	Click this option to Filter the Log on the defined criteria.
14.	Reset	Click this option to reset the defined criteria for filtering.



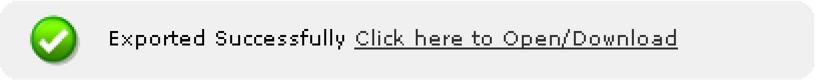
File Activity Report

1 - 7 of 7 page 1 of 1 Rows per page: 10

Client Date	Computer Name/Ip	Group	IP Address	User name	File Action Type	Drive Type	Source File	Destination File
06/27/2016 11:46:32 AM	COM[redacted]	Managed Computers	19[redacted]	COM[redacted]	CREATE	Removable Drive	NewFile	g:\PPT 22nd June 2016-Marketing\Surekh
06/27/2016 11:45:15 AM	CO[redacted]	Managed Computers	1[redacted]	COM[redacted]	CREATE	Removable Drive	NewFile	g:\PPT 22nd June 2016-Marketing\Surekh
06/27/2016 11:42:32 AM	CO[redacted]	Managed Computers	1[redacted]	COM[redacted]	CREATE	Removable Drive	NewFile	g:\PPT 22nd June 2016-Marketing\Surekh
06/27/2016 11:28:45 AM	CO[redacted]	Managed Computers	19[redacted]	COM[redacted]	MODIFY	Removable Drive		g:\PPT 22nd June 2016-Marketing\Preser
06/27/2016 11:25:04 AM	CO[redacted]	Managed Computers	1[redacted]	CO[redacted]	MODIFY	Removable Drive		g:\PPT 22nd June 2016-Marketing\Surekh
06/27/2016 11:18:02 AM	CO[redacted]	Managed Computers	19[redacted]	COM[redacted]	MODIFY	Removable Drive		g:\PPT 22nd June 2016-Marketing\Preser
06/27/2016 11:17:18 AM	CO[redacted]	Managed Computers	19[redacted]	COM[redacted]	MODIFY	Removable Drive		g:\PPT 22nd June 2016-Marketing\Preeti

Export

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



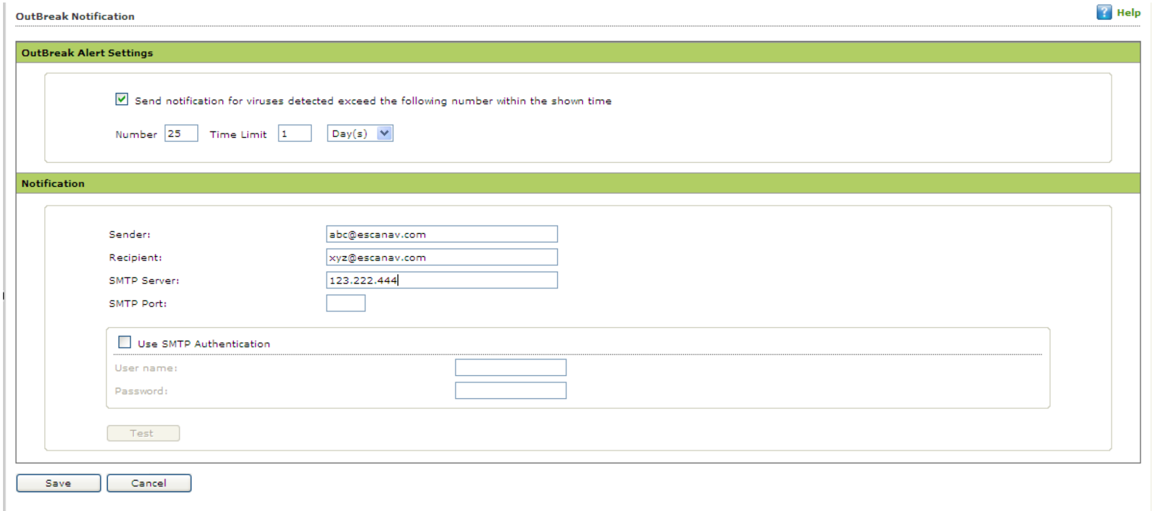
Exported Successfully Click here to Open/Download

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

Outbreak Notifications

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

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



OutBreak Notification

OutBreak Alert Settings

☑ Send notification for viruses detected exceed the following number within the shown time

Number 25 Time Limit 1 Day(s)

Notification

Sender: abc@escanav.com

Recipient: xyz@escanav.com

SMTP Server: 123.222.444

SMTP Port:

□ Use SMTP Authentication

User name:

Password:

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

Defining Settings

Using this section you can define important settings for the following

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

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

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

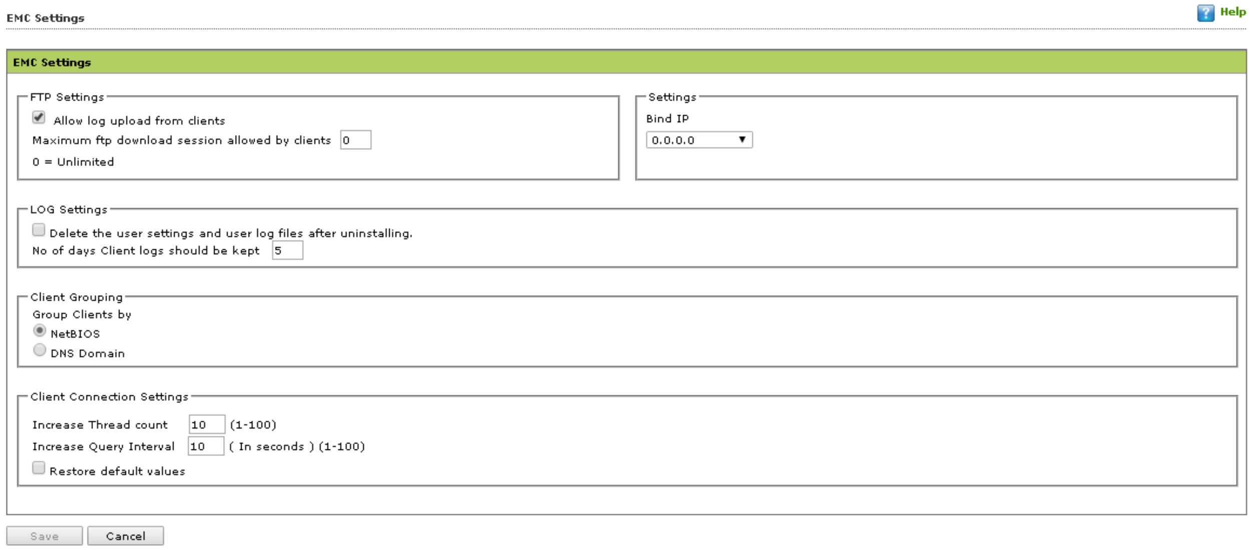
eScan Management Console Settings

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

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

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

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



EMC Settings

EMC Settings

FTP Settings

☑ Allow log upload from clients

Maximum ftp download session allowed by clients 0

0 = Unlimited

Settings

Bind IP 0.0.0.0 ▼

LOG Settings

□ Delete the user settings and user log files after uninstalling.

No of days Client logs should be kept 5

Client Grouping

Group Clients by

● NetBIOS

○ DNS Domain

Client Connection Settings

Increase Thread count 10 (1-100)

Increase Query Interval 10 (In seconds) (1-100)

□ Restore default values

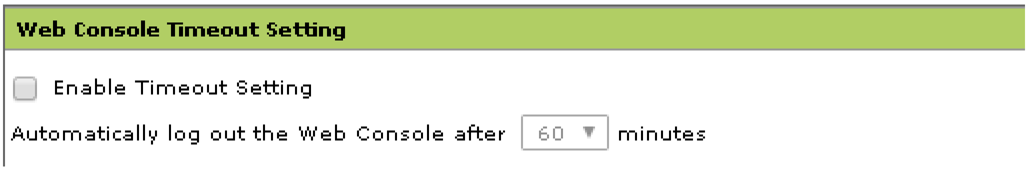
The **steps** to configure the EMC settings are as follows:

1. 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.
2. To allow uploads by Endpoints, under FTP Settings, select the Allow Upload by Clients check box.
3. To restrict the maximum number of FTP connections, in the Maximum FTP Clients allowed box, type or select the maximum number of FTP Connections to be allowed. The default value is 0; this allows an unlimited number of FTP connections.
4. 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.
5. Under Client Grouping section, you can sort group clients either by NetBIOS or DNS domain. This setting is especially useful only during fresh client installations. After installation, it enables you to manually manage domains and the clients grouped under them.
6. Click NetBIOS, if you want to sort clients only by hostname.
7. Click DNS Domain, if you want to sort clients by hostname containing the domain name.
8. Click Save button to implement the defined settings.

Web Console settings

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

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

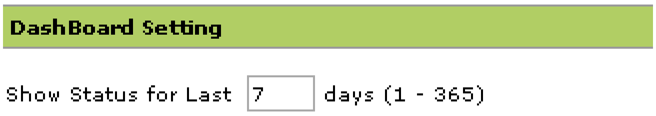


Web Console Timeout Setting

□ Enable Timeout Setting

Automatically log out the Web Console after 60 minutes

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



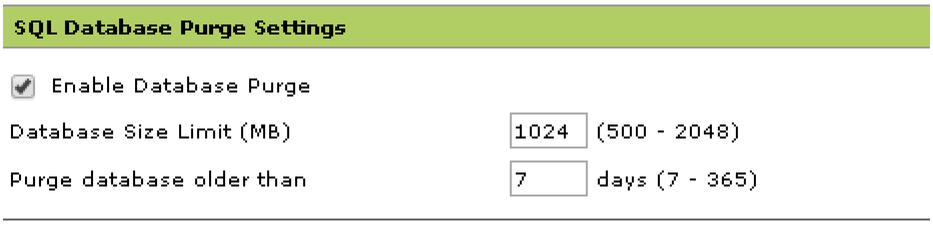
DashBoard Setting

Show Status for Last 7 days (1 - 365)

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

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

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



SQL Database Purge Settings

☑ Enable Database Purge

Database Size Limit (MB) 1024 (500 - 2048)

Purge database older than 7 days (7 - 365)

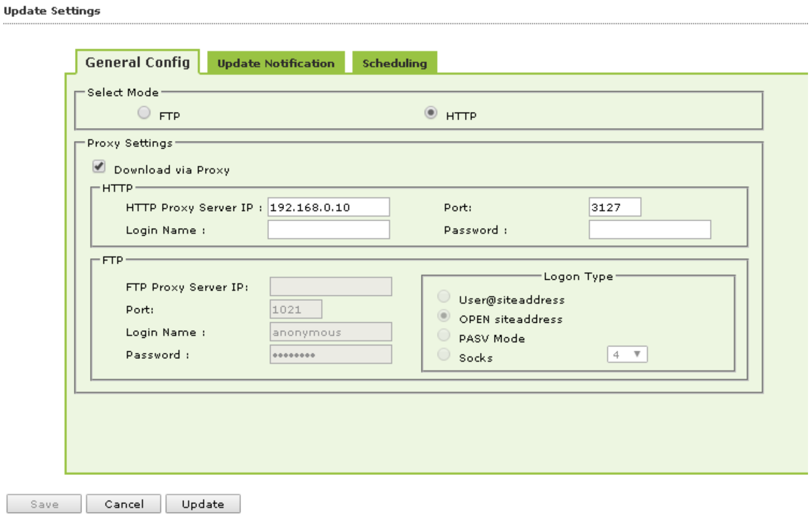
Click **Save** to save the defined settings

Update Settings

The Update module automatically keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP.

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

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



Select Mode: ○ FTP ● HTTP

Proxy Settings

☑ Download via Proxy

HTTP

HTTP Proxy Server IP : 192.168.0.10 Port: 3127

Login Name : Password :

FTP

FTP Proxy Server IP:

Port: 1021

Login Name : anonymous

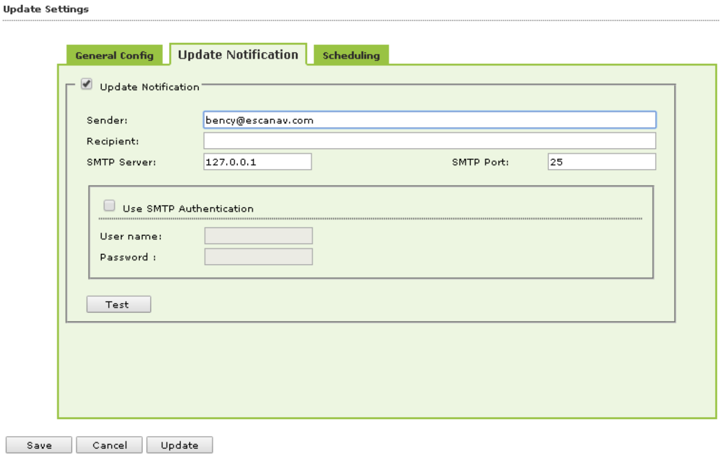
Password : ********

Logon Type: ○ User@siteaddress ● OPEN siteaddress ○ PASV Mode ○ Socks 4

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

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

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



☑ Update Notification

Sender: bency@escanav.com

Recipient:

SMTP Server: 127.0.0.1 SMTP Port: 25

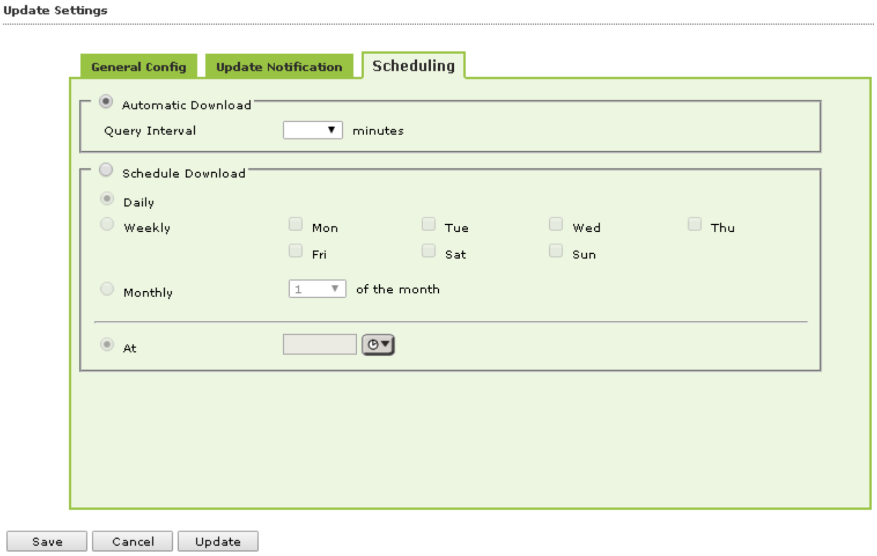
□ Use SMTP Authentication

User name:

Password :

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

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


Update Settings

General Config | Update Notification | Scheduling

● Automatic Download

Query Interval ▾ minutes

○ Schedule Download

● Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

○ Monthly 1 ▾ of the month

● At

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

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

Auto Grouping

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

Advantages of Auto Grouping

1. On Auto Grouping, the clients will be automatically added to the specified managed groups.
2. The clients can be added or removed from Auto Grouping with ease.

It contains the following section:

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

How to configure Auto Grouping?

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

For example:

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

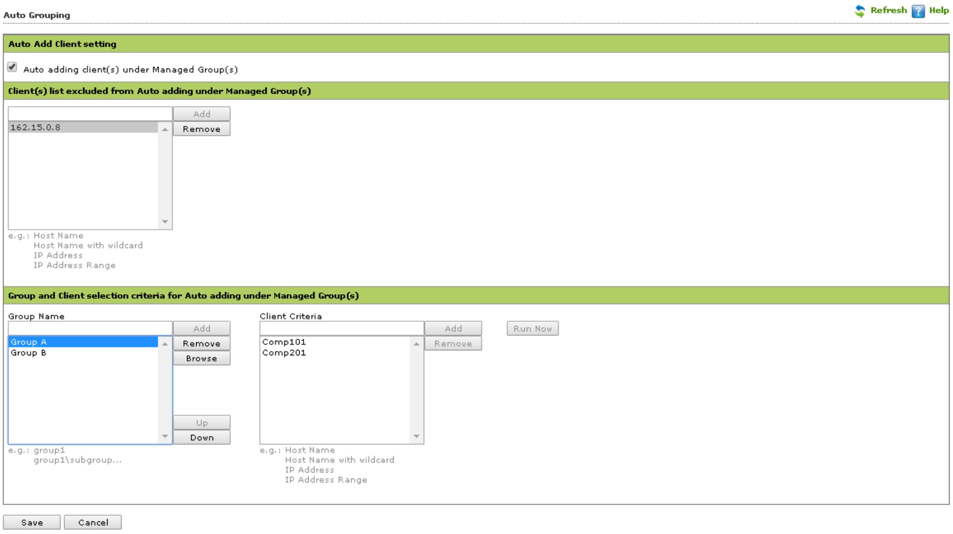
The above example displays the Groups and the client criteria for Auto Grouping into the desired group.

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

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

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

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



Auto Grouping

Auto Add Client setting

☑ Auto adding client(s) under Managed Group(s)

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

162.15.0.8

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

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

Group Name

Group A
Group B

e.g.: group1
group1\subgroup...

Client Criteria

Comp101
Comp201

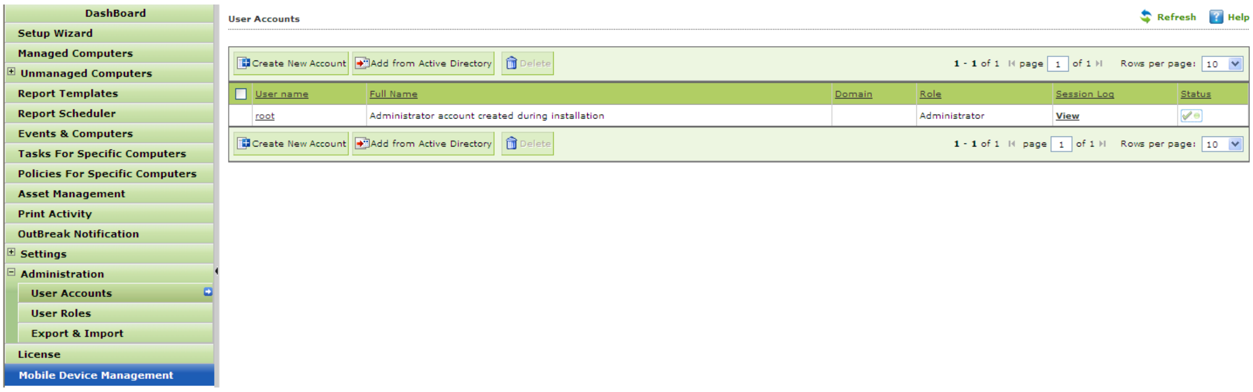
e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

Managing User Accounts

Using this section you can create User Accounts and allow those admin rights for using eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. Using this option responsibility can be shared between multiple administrators.

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

1. On the navigation pane, under **Administration**, click **User Accounts**.



□	User name	Full Name	Domain	Role	Session Log	Status
	root	Administrator account created during installation		Administrator	View	✓

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

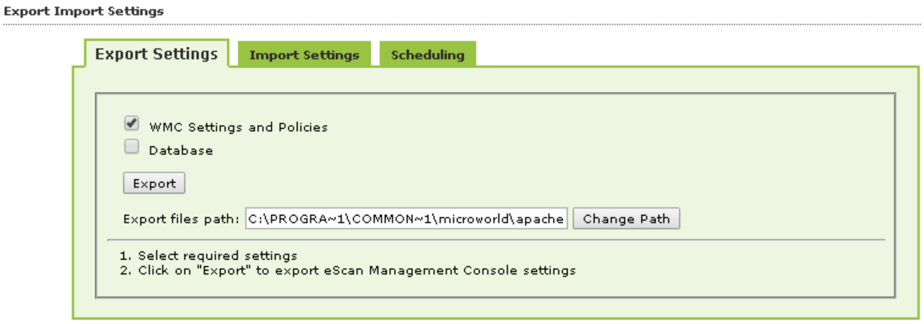
Field	Description
Account type and information	
User name*:	Type the user name.
Full Name*:	Type the full name.
Password*:	Type the password.
Confirm Password*:	Re-type the password for confirmation.
Email Address:	Type the email address.

3. Now click **Save**.

Export and Import Settings

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

- **Export Settings –**



☑ WMC Settings and Policies
□ Database

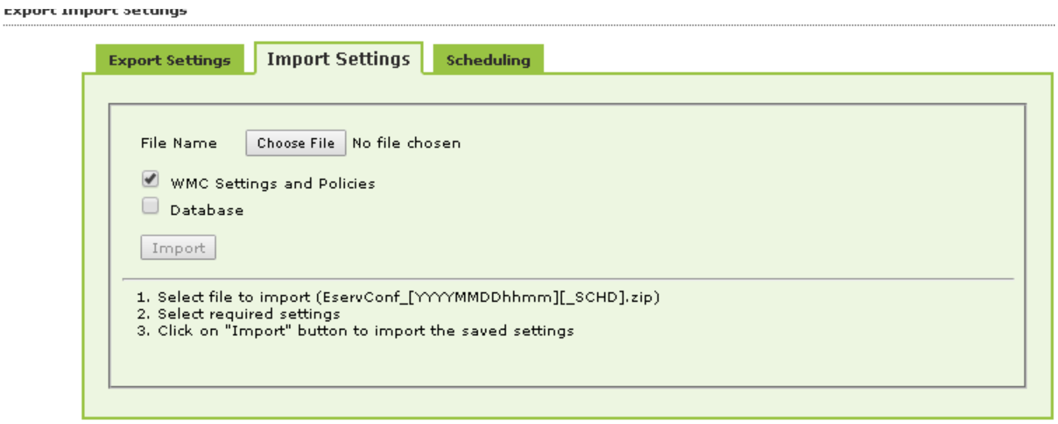
Export files path: C:\PROGRA~1\COMMON~1\microworld\apache

1. Select required settings
2. Click on "Export" to export eScan Management Console settings

Use the following steps to export the settings.

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

Import Settings



File Name: No file chosen

☑ WMC Settings and Policies
□ Database

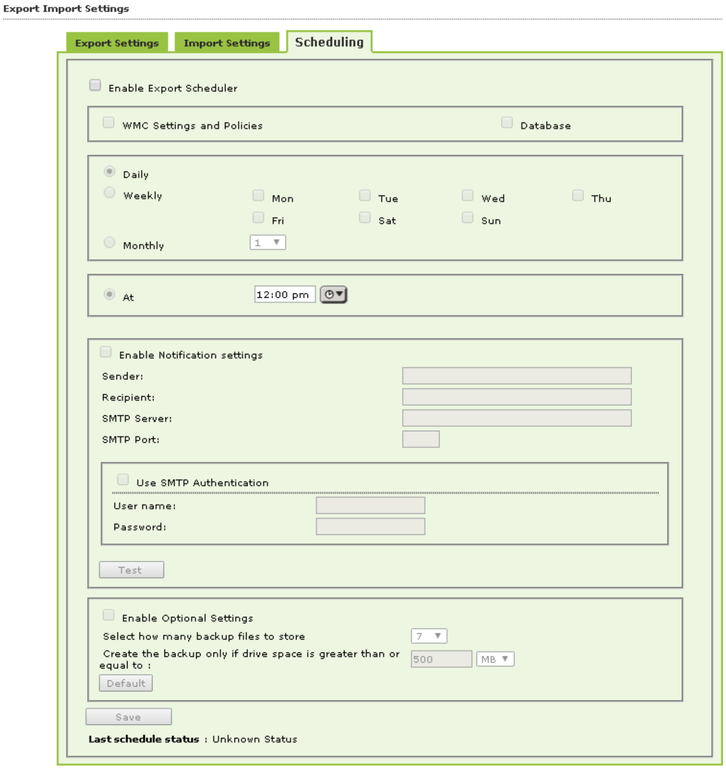
1. Select file to import (EservConf_[YYYYMMDDhhmm][_SCHD].zip)
2. Select required settings
3. Click on "Import" button to import the saved settings

Use the following steps to import the settings.

1. On the navigation pane, under **Administration**, click **Export & Import**.
   The **Export Import Settings** screen appears.
2. Under **Import Settings** section, type the file name or click **Browse** to select the file that you want to import

3. Under **Import Settings** section, select an appropriate check box:
   - **WMC Settings and Policies:** Select this check box, if you want to import WMC settings and policies.
   - **Database:** Select this check box, if you want to import database.
4. Click **Import**.
   A message of settings successfully imported appears on the screen.

Schedule



Export Import Settings

Export Settings | Import Settings | Scheduling

□ Enable Export Scheduler

□ WMC Settings and Policies □ Database

● Daily
○ Weekly □ Mon □ Tue □ Wed □ Thu
□ Fri □ Sat □ Sun
○ Monthly 1 ▼

● At 12:00 pm

□ Enable Notification settings
Sender:
Recipient:
SMTP Server:
SMTP Port:

□ Use SMTP Authentication
User name:
Password:

Test

□ Enable Optional Settings
Select how many backup files to store 7 ▼
Create the backup only if drive space is greater than or equal to : 500 MB ▼
Default

Save

Last schedule status : Unknown Status

Using this option you can do the following –

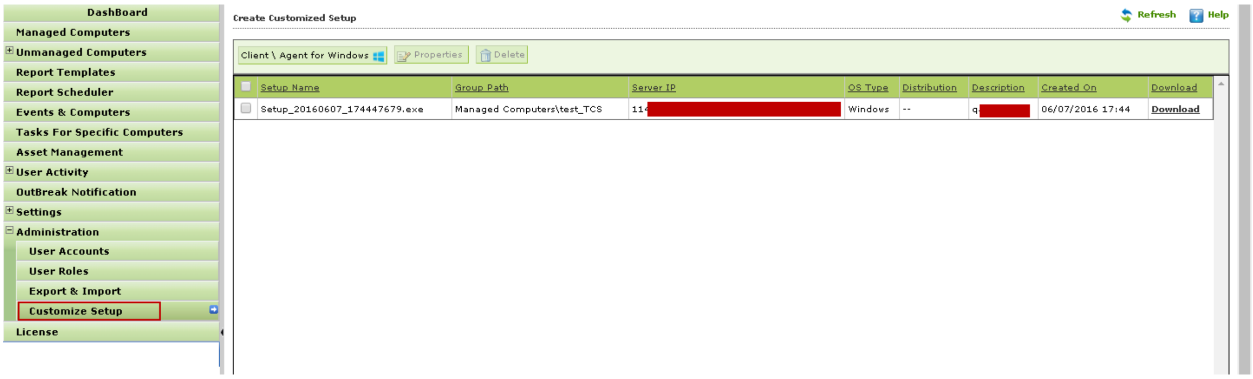
1. Enable scheduling of WMC settings and Policies or Database.
2. Schedule the Export/Import at a specific tie that can be daily, weekly or desired day(s) of a week or a desired date in a Month.
3. Send Notifications to specific recipient.
4. Allows you to define Username and Password for SMTP authentication.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

Customize Setup

Customized Setup will allow you to create a customized setup for a particular Windows client machine. You can define the settings for a customized setup; It will allow you to define the customized settings for File antivirus, mail antivirus, Anti-Spam, Firewall, endpoint security, Privacy control, Client Installation Settings, Update Intervals, exclude/ remove download files.

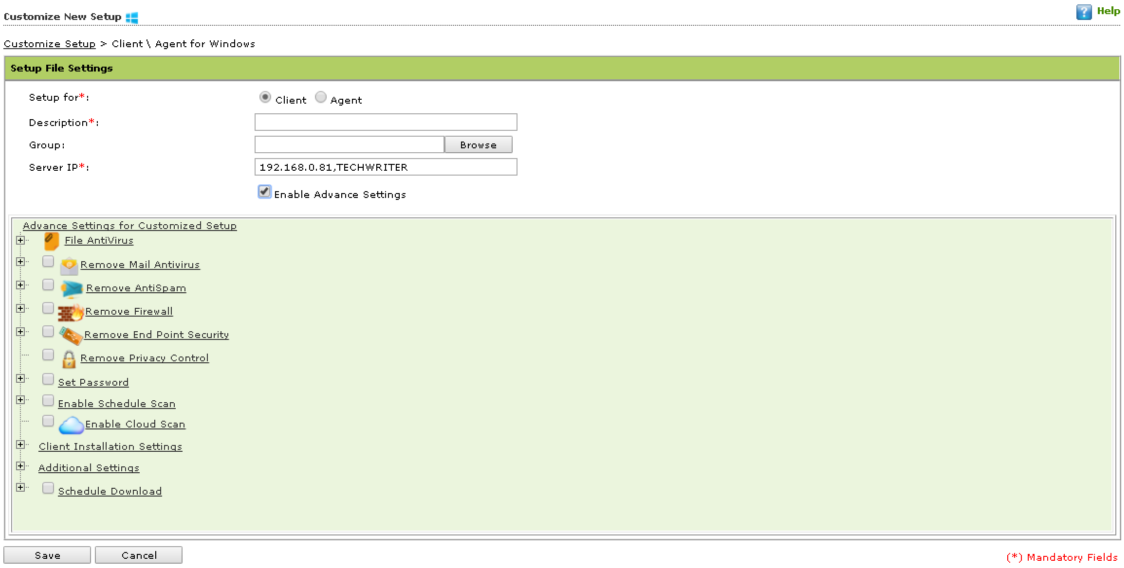
Ho w to create a Customized client Setup for Windows?

1. Go to Administration > click customize setup, a new window create customized setup window will be displayed.



□	Setup Name	Group Path	Server IP	OS Type	Distribution	Description	Created On	Download
□	Setup_20160607_174447679.exe	Managed Computers\test_TCS	114[redacted]	Windows	--	q[redacted]	06/07/2016 17:44	Download

2. Click client for Windows and a new window customize new setup will be displayed.



Setup for*: ● Client ○ Agent

Description*:

Group: Browse

Server IP*: 192.168.0.81,TECHWRITER

☑ Enable Advance Settings

Advance Settings for Customized Setup
- File AntiVirus
- □ Remove Mail Antivirus
- □ Remove AntiSpam
- □ Remove Firewall
- □ Remove End Point Security
- □ Remove Privacy Control
- □ Set Password
- □ Enable Schedule Scan
- □ Enable Cloud Scan
- Client Installation Settings
- Additional Settings
- □ Schedule Download

3. Define the following settings
   - **Setup for:** Select the option Client to create a client endpoint setup.
   - **Description:** Provide a brief description about the Setup for better understanding on a future date.
   - **Group:** select the managed group to which this client should be added to.
   - **Server IP:** This will automatically display the IP address of the server.
   - **Enable Advance Settings:** Select this check box to define customized action settings for this client setup that you are about to create.
4. Click **Save**.
5. eScan Management console will collect the data and create a setup package; once the package has been successfully created it will be listed on the create customized setup window. By default the setup will be saved at the following path on the eScan Server:

C:\Program Files\Common Files\MicroWorld\apache2\EMCWEBADMIN\CustomizedSetup

How to edit a Client Customized setup?

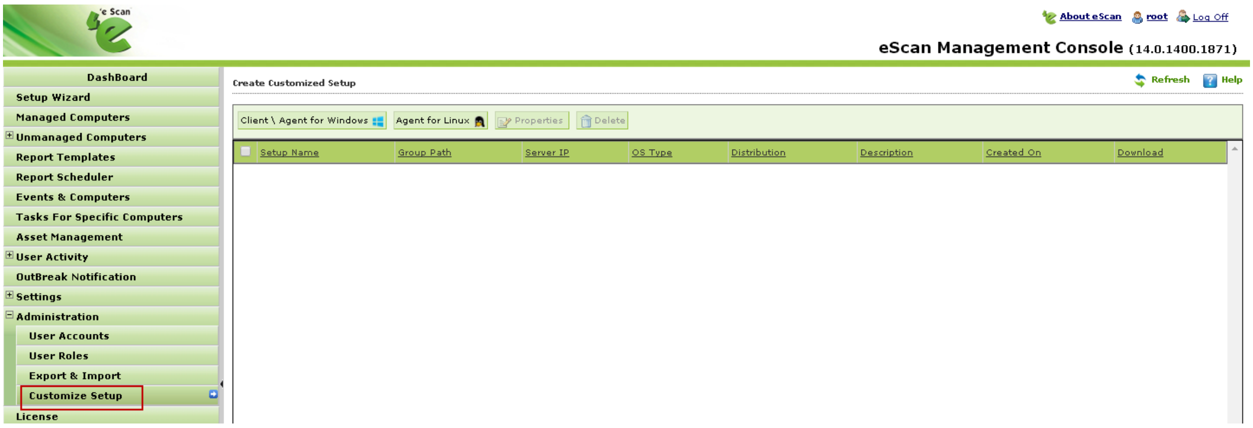
1. Go to Administration > click customize setup, a new window create customized setup window will be displayed.
2. It will display the list of all the customized setups.
3. Select the checkbox next to the setup name and click **Properties**; it will display the existing properties of this particular setup.
4. You can now edit the advance settings for this setup.
5. Click Save

How to delete a Client \Agent customized setup?

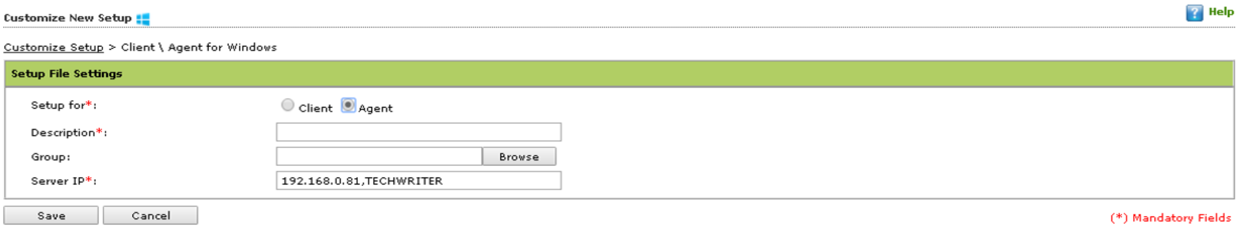
1. Go to Administration > click customize setup, a new window create customized setup window will be displayed.
2. It will display the list of all the Customized setups.
3. Select the checkbox next to the setup name and click delete.

Ho w to Create a Customized Agent Setup for Windows?

1. Go to Administration > click customize setup, a new window create customized setup window will be displayed.



2. Click Client\Agent for Windows and a new window Setup File Settings will be displayed.



Customize New Setup

Customize Setup > Client \ Agent for Windows

Setup File Settings

Setup for*: ○ Client ● Agent

Description*:

Group: Browse

Server IP*: 192.168.0.81,TECHWRITER

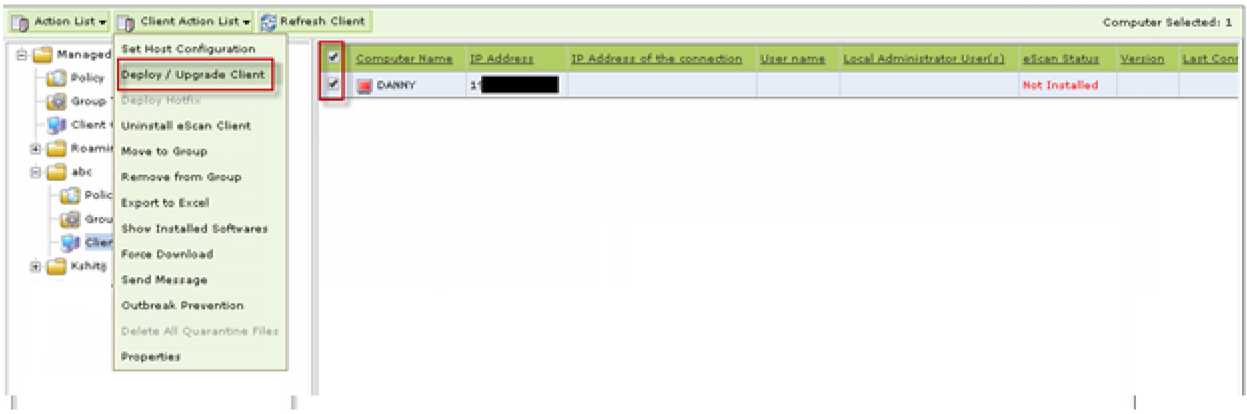
Save Cancel

(*) Mandatory Fields

3. Define the following settings
   - **Setup for:** Select the option Agent to create an Agent setup.
   - **Description:** Provide a brief description about the Setup for better understanding on a future date.
   - **Group:** select the managed group to which this will act as an Agent.
   - **Server IP:** This will automatically display the IP address of the server from where the agent will take updates.
4. Click **Save**.
5. eScan Management console will collect the data and the create a setup package; once the package has been successfully created it will be listed on the create customized setup window. By default the setup will be saved at the following path on the eScan Server: ***C:\Program Files\Common Files\MicroWorld\apache2\EMCWEBADMIN\CustomizedSetup***

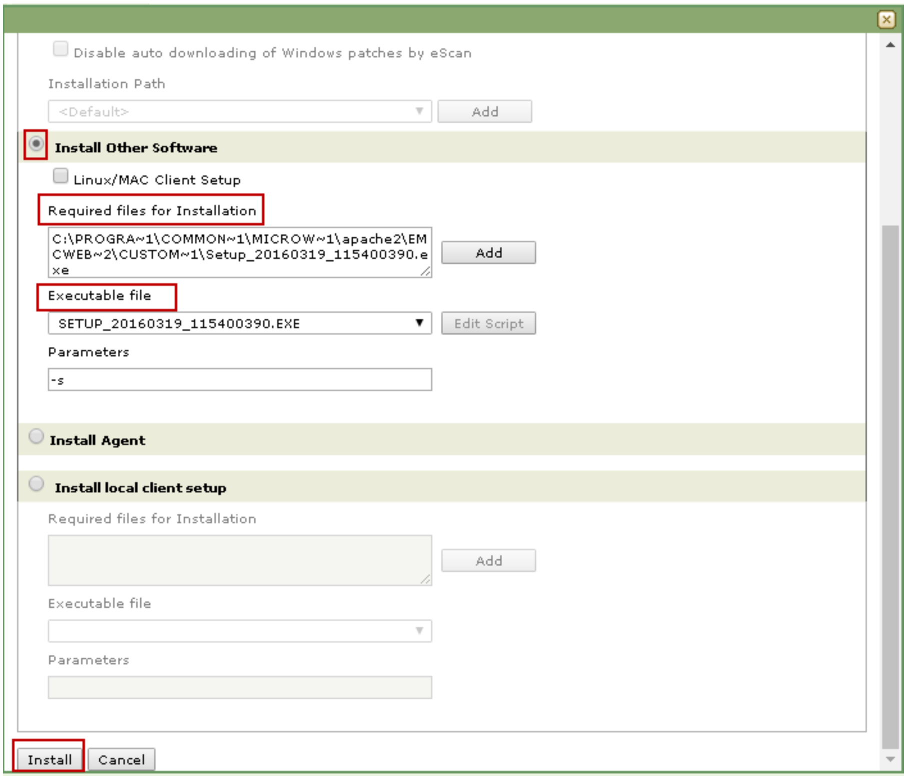
How to deploy a customized client setup for Windows?

1. Go to Managed Computers > select the desired client computer under the desired managed group.



☑	Computer Name	IP Address	IP Address of the connection	User name	Local Administrator User(s)	eScan Status	Version	Last Con
☑	DANNY	1[redacted]				Not Installed		

2. Click Deploy/ upgrade client under Client Action List.
3. On the Client Installation window, select install other Software.
4. On the “Required files for installation” field copy paste the path of the setup file including the file name.
5. The executable file field will automatically pull the file name of the setup file.
6. Click Install.



□ Disable auto downloading of Windows patches by eScan

Installation Path

<Default> ▼ Add

● **Install Other Software**

□ Linux/MAC Client Setup

Required files for Installation

C:\PROGRA~1\COMMON~1\MICROW~1\apache2\EMCWEB~2\CUSTOM~1\Setup_20160319_115400390.exe

Add

Executable file

SETUP_20160319_115400390.EXE ▼ Edit Script

Parameters

-s

○ **Install Agent**

○ **Install local client setup**

Required files for Installation

Add

Executable file

Parameters

Install Cancel

7. The user interactive installation wizard will be start on the client machine.

Managing Licenses

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

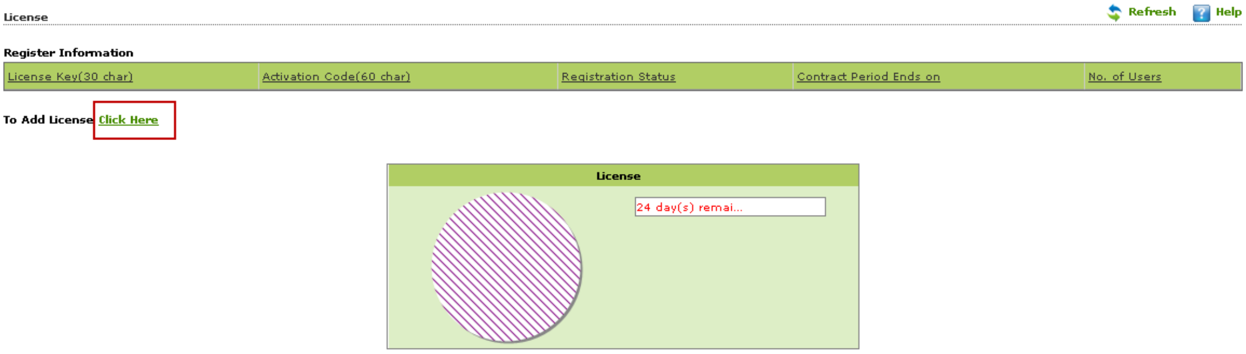
- **Adding License and Activating License Key**

It enables you to add licenses of users.

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

Steps -

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



License

Register Information

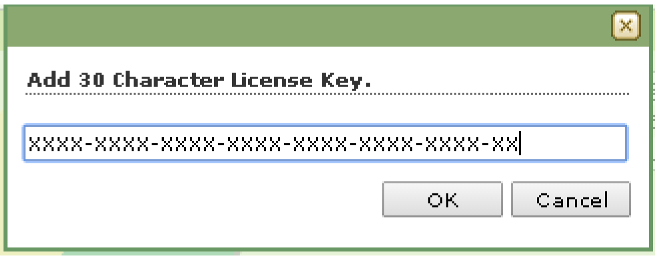
License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users

To Add License Click Here

License

24 day(s) remai...

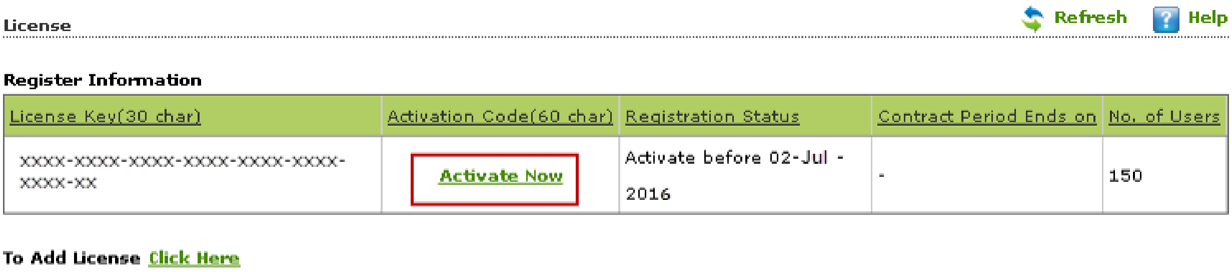
2. Add the 30 Digit License key and Click **Ok**. The added license key will be visible displayed in the **Register Information** table.



Add 30 Character License Key.

XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX

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



License

Refresh Help

Register Information

License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX	Activate Now	Activate before 02-Jul - 2016	-	150

To Add License Click Here

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

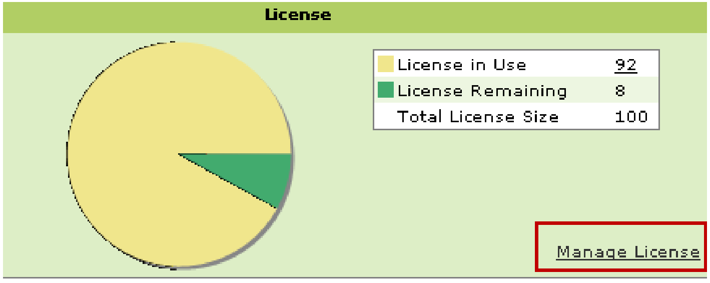
Field	Description
Name	Enter the machine name
Phone No.:	Enter the phone number
Address:	Type the address
Mobile No.:	Type the mobile number
City	Type the city name
Fax No.:	Type the fax number
State:	Type name of the state
Email Id*:	**[Mandatory]** Type an email ID
Country:	Select the country from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

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

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

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

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

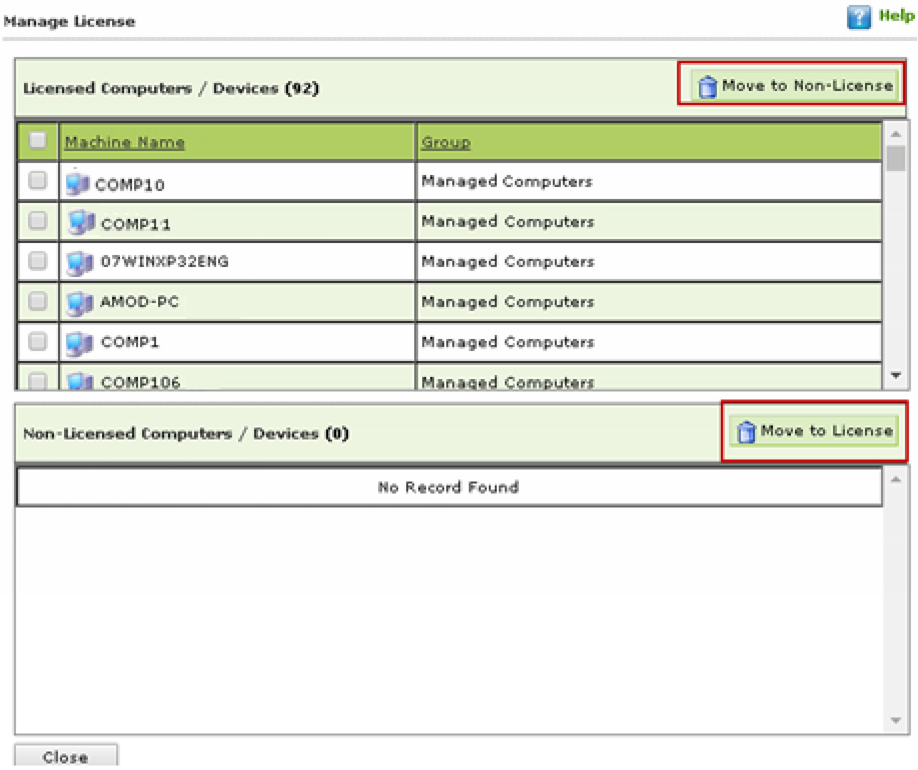


License

🟨	License in Use	92
🟩	License Remaining	8
	Total License Size	100

Manage License

3. Under **Licensed Computers** section, select an appropriate check box, the computer that you want to move to non-licensed computers.
   The **Move to non-license** button is available only when you select an appropriate check box under **Licensed Computers** section, and you can move multiple computers at a time.
4. Click **Move to non-license**.
   The licensed computer moves to non-licensed computers section.



Manage License

Licensed Computers / Devices (92)

□	Machine Name	Group
□	COMP10	Managed Computers
□	COMP11	Managed Computers
□	07WINXP32ENG	Managed Computers
□	AMOD-PC	Managed Computers
□	COMP1	Managed Computers
□	COMP106	Managed Computers

Non-Licensed Computers / Devices (0)

No Record Found

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

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

1. On the navigation pane, click **License**; the **License** screen will be displayed.
2. Under **License** section, click **Manage License** link.
3. Under **Non Licensed Computers** section, select an appropriate check box, the computer that you want to move to licensed computers.
4. Click **Move to license** to move the non-licensed computer to licensed computers section.

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.

- **Email Support**

  Please send your queries, suggestions, and comments about our products about our products or this guide to **support@escanav.com**.

Registered Offices

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

Malaysia
MicroWorld Technologies Sdn.Bhd.
(Co.No. 722338-A)
E-8-6, Megan Avenue 1, 189, Jalan Tun Razak, 50400 Kuala Lumpur, Malaysia
Tel : (603) 2333-8909 or (603) 2333-8910
Fax: (603) 2333-8911
E-mail : **sales@escanav.com**
Web site: **http://www.escanav.com**

South Africa
MicroWorld Technologies South Africa (PTY) Ltd.
376 Oak Avenue
Block C (Entrance from 372 Oak Avenue) Ferndale, Randburg, Gauteng, South Africa
Tel : Local 08610 eScan (37226)
Fax: (086) 502 0482
International : (27) (11) 781-4235
E-mail : **sales@microworld.co.za**
Web site: **http://www.microworld.co.za**

USA
MicroWorld Technologies Inc.
31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334, USA
Tel : (1) (248) 855 2020
Fax: (1) (248) 855 2024
E-mail : **sales@escanav.com**
Web site: **http://www.escanav.com**

Germany
MicroWorld Technologies GmbH
Drosselweg 1, 76327 Pfinztal,
Germany
Tel : (49) 7240 944909 20
Fax: (49) 7240 944909 92
E-mail : **sales@escanav.de**
Web site: **http://www.escanav.de**