This document provides information to install and use eScan Management Console.

eScan Management Console
User Guide

eScan User Guide

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

Document Number : 10ESERV/29.05.09

Copyright Notice

Copyright (C) 2004. 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 change without prior notice.

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

Trademarks.

MicroWorld, MicroWorld Logo, eScan, eScan logo, MWL, MailScan are trademarks of MicroWorld.

All product names referenced herein are trademarks or registered trademarks of their respective companies. MicroWorld Software Services Pvt. Ltd. (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 Software Services Pvt. Ltd. reserves the right to modify specifications cited in this document without prior notice.

List of Figures

The following figures are included in this guide

Table of Contents

Welcome

eScan Management Console, functions as a centralized server that allows you to remote install, distribute updates and upgrades to multiple clients in your eScan network. In a large corporate network environment, you can significantly reduce the costs and the Internet traffic by setting up a centralized updating structure. You don't have to download updates, deploy license keys or assign security policies for individual machines but can create a central server and then effect deployment to individual machines.

MicroWorld Content Security and Anti-Virus products, provide a blanket, round-the-clock security screen against viruses delivered into your PC or network. After the software is installed it is always active. You carry out your normal work, surf the net, exchange mails, download your favorite programs, run them and so on, secure in the knowledge that you are protected from virus attacks.

MicroWorld is one of the leading solution providers in the areas of content security and Anti-Virus products. With its corporate head quarters in New Jersey and development center in Mumbai, India, we offer round-the-clock support, through our regional offices and over 10,000 channel partners spread across the globe. This section provides information about eScan. Details about its features, how to use it; what to do when you have a virus etc is given.

eScan is a comprehensive Content Security and Traffic Scanning software package that checks the content in e-mails and its attachments for viruses. Checks are done for viruses, restricted words and phrases, embedded objects such as Java applets etc, before the e-mails reach you. It thus offers unprecedented "real-time" security at various levels in any organization, from the Internet Gateway to your desktop. It is also synchronized with the Internet to provide real-time security for your organization. It offers a Centralized Security Management System. This feature allows your network administrator to configure Global Security Policies for the organization from a single console.

eScan is also designed to understand different file types, data streams and compression formats. It can look inside data streams and identify complex file architecture. It has a user-friendly interface and you can automatically download Updates from our download site. This gives you the "ultimate convenience and confidence in computing".

eScan Content Security and Anti-Virus application is delivered in four modules:

eScan for Windows: Provides and Anti-Virus engine to scan and protect your system against virus and other threats. You can set a schedule for auto scan.

eScan AV Monitor: Provides a monitor to quickly scan your system for virus and other threats.

eScan Updater: Allows you to download updates to detect and remove new viruses.

Content Administrator: Allows you to set security policies to permit or prohibit specific type of content from bring accessed.

eScan Management Console. Allows you to remotely configure and administer the eScan network, installed on multiple clients.

Access to these modules depends on the version of eScan you are using. For more details, please refer to the section eScan Products.

About this Guide

This chapter provides details about the following topics:

- **Audience**
- **How this guide is organized**
- **Typographical Conventions**
- **Contact Us**

Audience

This Guide is for system administrators and users involved in installing and using the application.

How this guide is organized

This guide is organized into separate books and chapters.

Getting Started: gives information about a typical screen, its components, types of fields, dialog boxes, tab pages and how to validate them.

eScan Management Console:This feature provides a centralized server that allows remote installation of software, deploys upgrades, updates, security policy etc, across all clients running eScan. The chapter also provides details to configure e-mail of reports. The book name under which this chapter is covered is "**eScan Management Console**".

Appendix: Provides a brief write-up on various aspects involved in running and maintaining eScan.

Typographical Conventions

The following typographical conventions are used in this guide.

This	Represents
Bold	A Menu or a menu option. When enclosed in " ", the name is as displayed in the screen.
' '	A long name is denoted by the first few words and ……. It is enclosed in ' '.
SMALL CAPS	Buttons on dialog boxes/child windows.
Italics	Entry Fields in dialog boxes/child windows.
Type	Information you need to enter.
Hyperlink	Is a hyperlink. Click to access related topics.
Tasks	Represents a key task of feature.

- When you have to navigate between menus the following convention is used: **menu** > **menu** >…

For e.g..... **eScan** > **Monitor** > **Settings**. Means: in eScan, **select** (click) the Monitor menu and **choose** (click) Settings..

Contact Us

We offer 24x7 support to our customers through e-mail, telephone and Chat.

Chat Support
- Chat with our support team at '**escanchat**' using: MSN or Yahoo messenger service.

E-Mail Support

- If you have any queries about our products or have suggestions and comments about this guide, please send them to support@mwti.net

Head Office:	Asia Pacific:
MicroWorld Technologies Inc. 33045 Hamilton Court East, Suite 105 Farmington Hills, MI 48334-3385, USA. Tel: (248) 848 9081/ 848 9084 Fax: (248) 848 9085	**MicroWorld Software Services Pvt Ltd..** Plot No 80, Road 15, MIDC, Marol, Andheri (E), Mumbai, INDIA. Tel (91) - 22- 28265701 - 05 Fax (91) - 22-28304750

For Technical Support, please write to: support@mwti.net
For getting solutions to eScan related problems, please visit: http://forums.mwti.net
For online-help, please visit: http://www.mwti.net/wiki
For sales related queries, please write to: sales@mwti.net

Getting Started

This chapter gives details of standard conventions used in this guide. Also included are components of a typical user interface, how to navigate the screens, meanings of various symbols and buttons, types of fields and how to enter values in them.

User Interface

User interface is the front end of the software. The software is made of different screens. You carry out tasks, enter values, set preferences, etc., using screens. This section explains the components of a typical user interface.
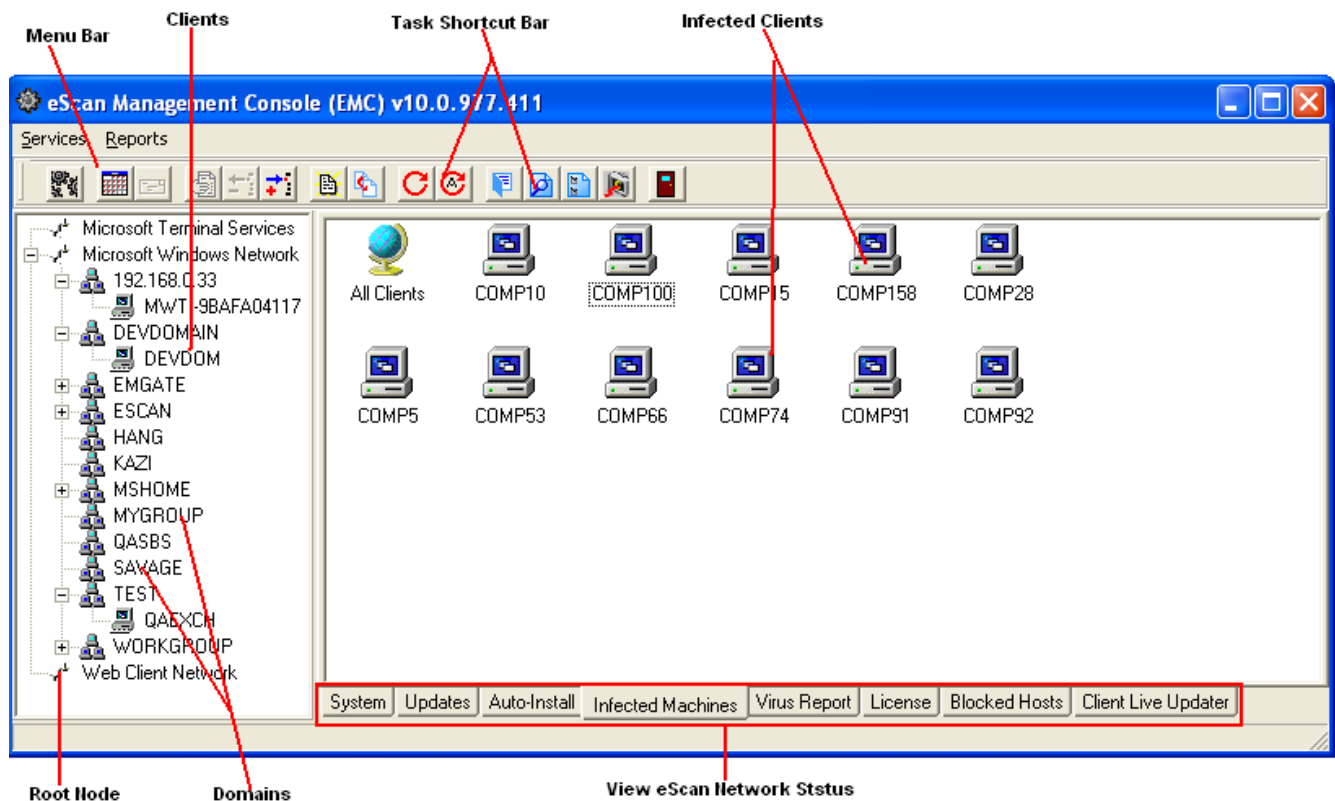

Figure 10.1: Typical User Interface

Screen Components

Typical screen components are explained below:

Screen Component	Function
eScan Management Console	Launches the eScan Management Console (Available for eScan PRO and Corporate only)
Configure Report Mailing	Configure settings to auto e-mail log reports of eServ
Mail Reports Now	Immediately mail selected report in eServ
Delete	Delete user log reports
Delete All User Logs	Delete all user logs
Deploy License	Deploy License keys to all clients using eServ
Refresh User	View updated settings for a user
Refresh All	View updated settings for all users
Shutdown Management Console	Shuts down eServ.

Options for the task	Displays tasks related to selected tasks
Action Buttons	Help you perform and execute functions related to tasks. Refer to the Section "Action Buttons" for detailed explanation about different action buttons.

eScan Management Console

eScan Management Console, functions as a centralized server that allows you to remote install, distribute updates and upgrades to all machines in your network, using eScan products. In a large corporate network environment, you can significantly reduce the costs and the Internet traffic by setting up a centralized updating structure. You don't have to download updates, deploy license keys or assign security policies for individual machines but can assign a central server and then effect deployment to individual machines.

This module provides an answer to many problems faced in administering security solutions to multi machines in networks: installation; admin control; deployment of updates, upgrades, license keys, security policies, covering rogue machines, etc. The common feature of MicroWorld products - salability, is extended to eServ and it can be used effectively for small networks with a few machines as well as large networks with a few thousand machines

The eScan FTP server automatically downloads the updates at regular pre-defined intervals from the Internet and includes them in a dedicated directory on the hard disk of the system such as the file server that is accessible to all the network users. Security policies and license keys can be deployed globally to all machines. This ensures uniformity, consistency and removes human errors.

You can create multiple eScan servers on a LAN. If one eScan server is down, the updates can be pulled from another eScan server. The machine designated as the eScan server must have Internet connectivity. It need not be a dedicated machine. The eServ tasks run in the background while you carry out your normal work.

In a network, it takes a single 'rogue' machine that has missed installation or not pulled and run an update, to spread infection across the network.

This chapter provides information to navigate to the relevant screens, validate fields and run the tasks. eScan Management Console feature is **only available in eScan for SMB / SME and eScan Corporate / Enterprise** products.

The chapter is for **system administrators** and other **qualified** personnel who manage the eScan network.

Important Terms of eServ

Announcement Mechanism eScan server has an announcement mechanism that broadcasts to its clients that it is the eScan server on the network. This is done through User Datagram Protocol (UDP). The client has a **listening mechanism** that listens to the UDP broadcasts and updates its' information pertaining to the server's IP address.

If one machine is designated as an eScan announcement server and it does not have an Internet connection, you can have access through a proxy or a dial-up modem on another machine. The eScan announcement server will pull updates and distribute them to its clients.

Centralized Reporting & Updating Updates are pushed to eScan clients by the eScan Server. eScan Clients can also pull updates at scheduled time intervals.. eScan Server uses industry standard TCP/IP based HTTP and FTP for file transfer and general communication. eScan clients can automatically detect the eScan update servers.

Comprehensive Activity Log eScan Server maintains a comprehensive activity log of all the events on an eScan client. Logs include security violation events, the name of the machine, the date & time of the event, the action taken, etc. Activity log can be automatically pulled by the eScan Server at pre-defined intervals. eScan Server allows the Administrators to track down offending sources of violations.

Deploy Refers to distribution of resources like license keys, upgrades, rule-sets, etc., to many clients from a single server. Deployments are not 'pushed' to clients but are 'pulled' by them. eScan clients pull the updates and upgrades from the eScan Server.

Remote Installation For a client, you can remotely install and uninstall eScan and other software using this feature.

To launch eServ

In the application tool bar, select the icon.

- Screen in Figure 10.1 is displayed. There are two panels in the screen.
- Right panel displays activity carried by the management console. Left panel displays client computers that are connected to the server as clients and pull updates from the server.

Note: Some of the icons in the tool bar are enabled only after settings in Reports or Services are activated. Click F5 to refresh the screen.

Navigating the screen

Left Pane: A directory tree showing clients in the eScan network is shown in Figure 10.1. All machines in the network are listed. They are grouped as per their domains. When you right click different objects in the left pane, you can perform additional tasks.

Right Pane: This is the area where eServ activity is displayed. When you run a task from the menu, the activity or the results are displayed in this area. At the bottom of the right pane, tabs are provided. These tabs allow you to run specific tasks and the results are displayed in the screen.

Left Pane

The left pane shows a virtual map of your eScan network. In a typical network, there

will be multiple machines grouped in domains. Many domains make up the network. eServ allows you to remotely administer all these machines from a single server.

When you right click on nodes, domains or individual machines, you can perform tasks like host configuration, IP configure, remote install or deploy, etc.
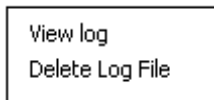
When you right click on an object a popup is displayed. The popup provides links that allow you to run tasks. Following table provides a brief description of the tasks. Depending on the object you have right clicked on, only some of the links may be available.

Dropdown Menu Name	**Description**
Refresh User Log	Refreshed user log for the selected client is displayed
Find Computer	Allows you to find a computer in the network
Get Status of eScan Installation	Status of eScan installation for the selected client is displayed
Set Host Configuration	Host Configuration Settings for the selected client
Set Domain Settings	Set Domain Settings for the selected domain
Move Host/IP to another Domain	Allows you to move a host or IP from one domain to another
Show System Information of this Host	The Client System Information for the selected host screen is displayed. There are multiple tabs that provide information about different features of the system.
Add Domain	Allows you to Add Domains
Get Client Status by IP	Get Status by IP of clients in the selected domain

Based on the settings for Log Settings in EMC Settings menu you can select the number of days for which the log files are to be kept. For a client, a folder with a date is dis-

played. The folder label shows the date since when the Log files are retained.

After choosing **one of the files**, when you right click, the following drop-down menu is displayed. Click on the links to view related information as explained below:
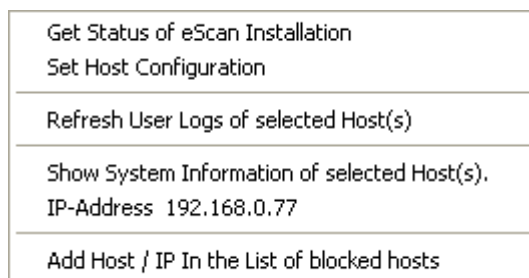
```
View log
Delete Log File
```

View log file: Displays details of selected log file.

**Delete Log File**: Deletes selected log file.

The pop is displayed only if log files have been generated.

- When you right click on a Client the following popup is displayed.

```
Get Status of eScan Installation
Set Host Configuration

Refresh User Logs of selected Host(s)

Show System Information of selected Host(s).
IP-Address  192.168.0.77

Add Host / IP In the List of blocked hosts
```


Get Status of eScan Installation Allows you to get the status of eScan Installation for the selected Client.

Set Host Configuration Allows you to set the **User Name** and **Password** to configure the Host**.** If you wish Remote Installation to be enabled for the host, select the check box for "**Enable Auto-Install".** You enter the preliminary information required for re-mote installation. Data entered here is used by eServ to obtain status of clients.
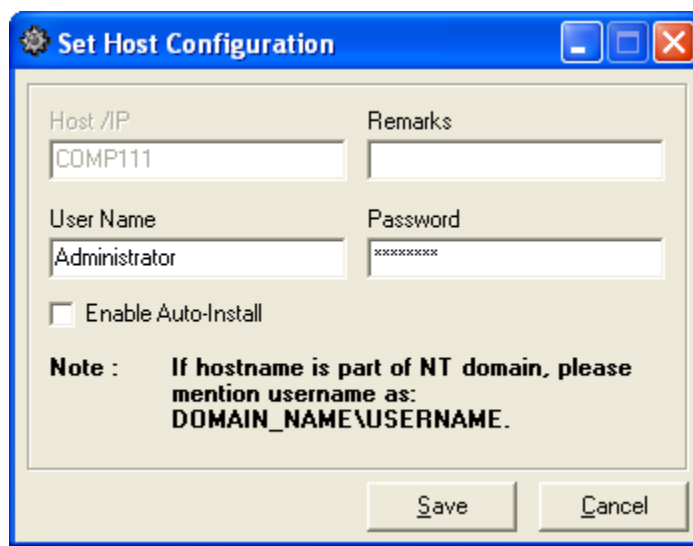
**Refresh User Logs of selected Host(s)** Displays updated and fresh information for the selected Client.

Show System Information of Selected Host(s) Displays the Client's System Information from the eServ. There are multiple tabs that provides information like Machine details, Operating System installed etc.

IP-Address Displays the IP Address of the selected hosts.

Add Host / IP in the List of blocked hosts Allows you to block the selected Host / IP from connecting the eScan Server and downloading the updates.

Right Pane

- **Right Pane** Displays the task or activity that you have selected.

- Tabs at the bottom of the screen add more functionality and allow you to run tasks like: getting system information, getting Updates, auto install, finding out infected machines, generating detailed virus reports and deploying license.

- **Announcements of eServ.** Typically messages show date and time when a listed log event was performed. There are two columns: **Logged Event** gives a brief description of the logged event and **Date-Time**, gives the date and time when the logged event took place. Right click to view following box.

```
  Select All   Ctrl+A
  Clear All

  Delete
  Print
```
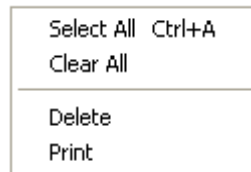
Select All: Selects all Clients

Clear All: Clears the display for all Clients.

Delete: Deletes logged events from the log file.

Print: Prints the logged event. Select the Client or all Clients and click Print. The events are displayed in a .text file. that can be printed.

Services

eScan Management Console, functions as a centralized server that distributes updates and upgrades to all machines in your organization, using eScan products..

Services carries a group of tasks that help you configure and run eScan Management Console. The tasks include: Start/Stop announcements; deploy license and upgrades and deploy rule-sets. eScan Management console allows these tasks to be performed from a single server.

Start Stop Announcement

Network / Normal View

EMC Settings

Set Host Configuration

Deploy License

Deploy RuleSets

Update All Clients

Shutdown Management Console

Get status of eScan Installation

Get Client status by IP

[Connection Errors](#)

Start/Stop Announcement

eScan server has an announcement mechanism that broadcasts to its clients that it is the eScan server on the network. This is done through User Datagram Protocol (UDP). The client has a **listening mechanism** that listens to the UDP broadcasts and updates its' information pertaining to the server's IP address.

If one machine is designated as an eScan announcement server and it does not have an Internet connection, you can have access through a proxy or a dial-up modem on another machine. The eScan announcement server will pull updates and distribute them to its clients.

- In [Figure 10.1](#), select **Services** or in the Tool bar select . The drop-down list shows a list of tasks. The first task displayed is **Stop Announcement**.

- This signifies that the announcement mechanism **is active and running**. If you click on the menu, it stops the announcement mechanism and the menu changes to **Start Announcement**. When announcements are stopped, clients are not able to download updates.

Network / Normal View

eScan Management Console has two views: Network and Normal.

Network: In Network view, you will see all the domains on the left & can enumerate all the clients inside a domain.

Normal View: In Normal view, you can add your own domains & also clients. You can group clients using IP and drag-drop any IP or client to any domain.

EMC Settings

This screen allows you to set the settings for the local eServ server. If the server has multiple IPs, then you can select the IP to use for announcements. You can also set the maximum number of FTP clients that are allowed to upload files.
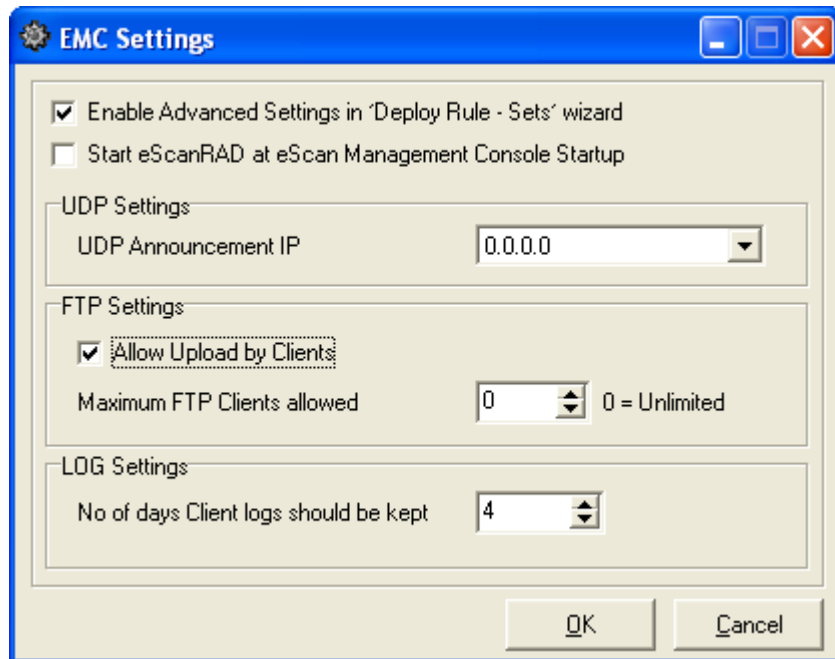
Field Name	Description
Enable Advanced Settings in 'Deploy Rule – Sets' wizard	Allows you to enable settings to Deploy Rulesets.
Start eScanRAD at eScan Management Console Startup	Allows eScanRAD to be loaded on startup of the system.
UDP Announcement IP	Select the IP to be used for announcements, from the drop-down list. If the value 0,0,0,0 is selected then eServ finds the available IP.
Allow Upload from Clients	Select the check box to allow FTP clients to upload files.
Maximum FTP Clients allowed	Select the number of FTP clients that should be allowed to upload files, at the same time. If you select 0, then there is no limit.
No of Days Keep Logs	Select the number of days to keep logs

Set Host Configuration

Hosts are machines or clients in a network for whom you wish install eScan. The menu allows you to add the IP address of a host and configure eScan remote install options for a host.

To launch Host Configuration

- In <u>Figure 10.1</u>, select Remote Install Settings or select 📭 from the tool bar.
- Screen in Figure 10.3 is displayed.
- Existing host name, user name, flag denoting if Auto-Install is enabled and remarks are displayed in the non-editable display fields.
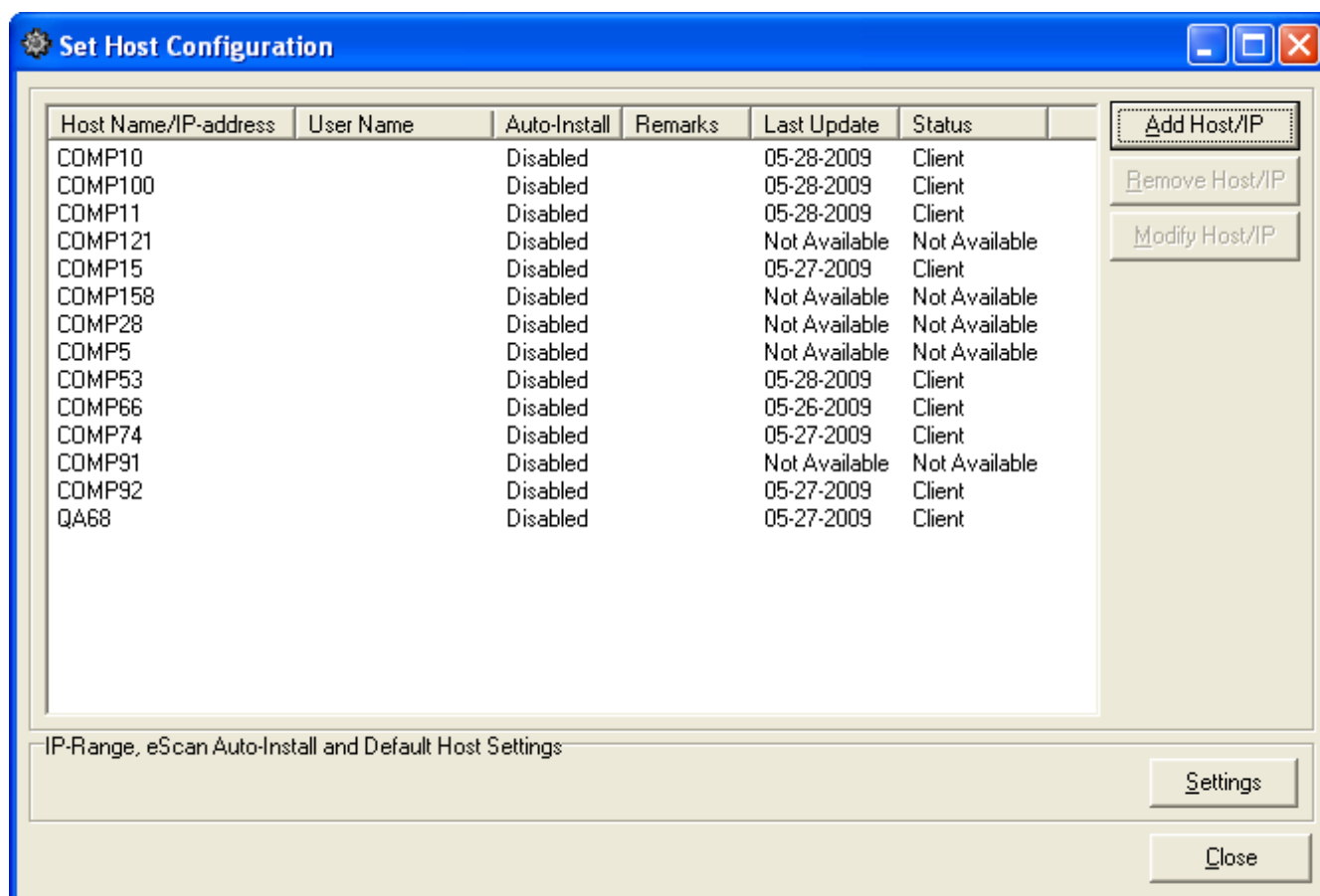

Figure 10.3: Set Host Configuration

Add IP Range

Refer <u>Get Client Status by IP</u>

Tab Page Name	Description
To Add Host/IP	**To Add Host/IP** Select the button to view **Host Configuration** dialog box. You can add a new host to the eServ network. Enter the computer name, user name, the password and your remarks and select **Save**.

|	
Remove Host/IP	The button allows you to remove a Host or IP from the list for hosts that have remote install enabled. Select the host and click the button. An alert appears warning you that user setting and log files for the host will be deleted. Select Yes or No.
Host Settings	Allows you to Configure Host. You enter the preliminary information required for remote installation. Data entered here is used by eServ to obtain status of clients. Host can be the client or server in the eScan environment. The following dialog box is displayed:

The selected host/client name and IP address is displayed in the Host/Name/IP non-editable display field. Enter the User Name and Password. If you wish Remote Installation to be enabled for the host, select the check box for "Enable

Auto-Install." Select **Save**.

Settings

To configure eScan install

Select the button to view **Settings** dialog box shown below. You can: add host names to include them in the list for Auto Install; set the time interval after which auto install begins and set other eScan remote install options.
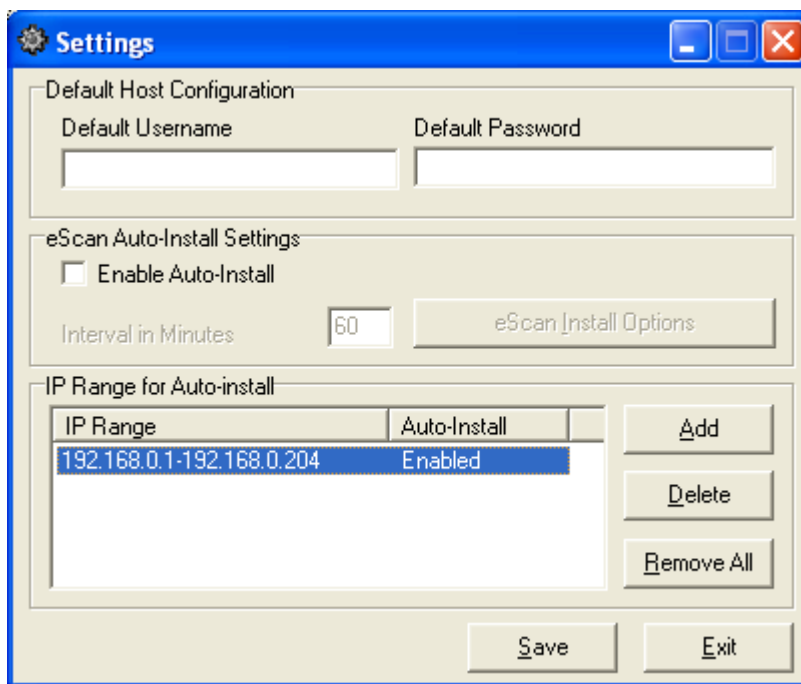
Default Username: Enter the default user name.

Default Password: Enter the default password.

Enable Auto-Install: Select the check box to allow remote install.

Interval in Minutes: Remote install begins after the time interval you enter in this field.

IP Range Settings: Frame allows you to include a range of IP address for remote installation. The existing range is displayed in the list box. To add a new range, select **Add**. A dialog box "Add IP Range" is displayed. Enter the range of IP addresses in the fields. Select the check box for "Add this IP Range to Auto-Install" and select Add. The range is displayed in the list box.

Add IP Range   Enter the range of IP addresses in the fields. Select the check box for "Add this IP Range to Auto-Install" and select **Add**.
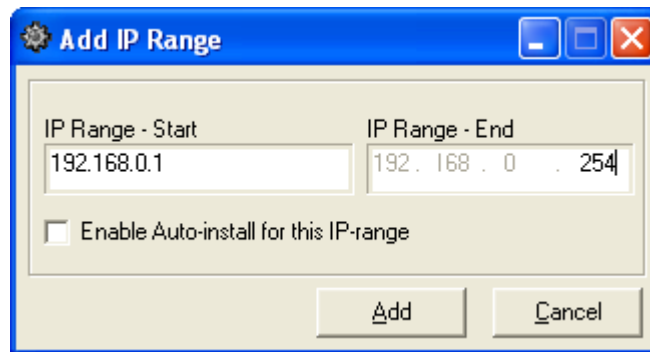
eScan Install Options   Select the button to view **Install Options** dialog box shown below. The box allows you to configure other settings for remote installation. Button is enabled only when "Enable Auto-Install" check box is selected.
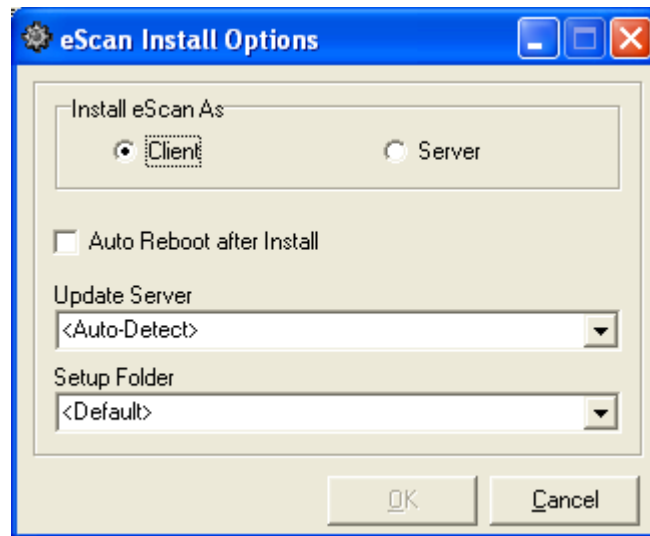
Client/Server: You can choose to install eScan as a Client or Server for the range of IPs, selected earlier. If you have a large number of clients in the network, this feature allows you to install eScan as multiple servers. If the number of machines is smaller, then install as Client.

Update Server: If you have selected "Client" as the mode, then this drop-down is enabled. It allows you to select the server from whom updates, upgrades, etc. are pulled.

Get Status of eScan Installation

Provides information about eScan installation details for a client.

To Launch Get Status of eScan Installation

- In Figure 10.1, select the client from the left pane and choose [icon] from the tool bar.
- The dialog box shown below is displayed. For the selected hosts, it provides details of eScan software, version details , status of connections, etc. Use the scroll bar to view all the details.

- If you double click on a client, a dialog box that allows you to configure the host, is displayed.

- In the above figure, when you right click on a client, the following popup is displayed. It allows you to run the following tasks:

```
Edit Host Configuration
Refresh Details of selected host(s)

Remote Install / Uninstall / Upgrade software
Remote Uninstall eScan

Change eScan Monitor Status of Selected Host(s)
Change Alternate Download Status of Selected Host(s)
Force Selected Host(s) to Download Updates
Scan Local Drives of Selected Host(s)
Scan System Drive of Selected Host(s)
Set Update Server of Selected Host(s)
Scan Memory of Selected Host(s)
Change Firewall Status
```

Field Name	Description
Edit Host Configuration	Opens the dialog box for Host Configuration. Edit the values and select Save.
Refresh Details of selected host(s)	Displays updated information about the selected host.
Remote Install/Uninstall/Upgrade Software	The button displays the following Remote Install/Uninstall/Upgrade Software dialog box. It allows you to configure settings for remote installation of software.
	Install eScan: Select the button if you are installing eScan. All fields except the buttons in the bottommost frame are now disabled.
	eScan Install Options: Opens the dialog box explained in eScan Install Options. Make the selections and select **Start.**
	Install other Software: Select the button if you wish to install other software. The following fields are en-

abled that allow you to: **Browse** your system for **Required files for installation,** select the **Files to Execute** and enter the **Command-line** parameters.
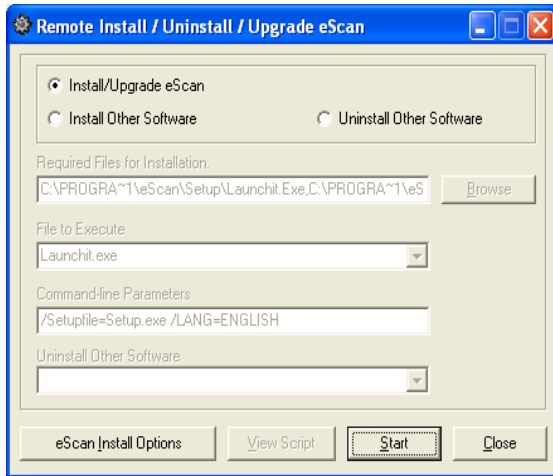
Edit Script: Allows you to edit a script file used for the installation.

Start: After the above selections are completed, select the **Start** button. The following status box is displayed that gives the status. Select **Close** to close the box.
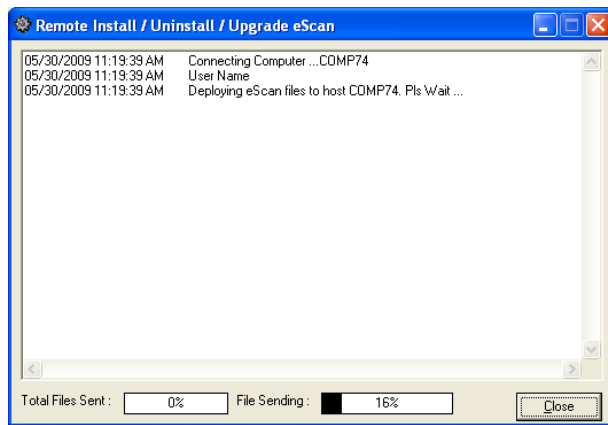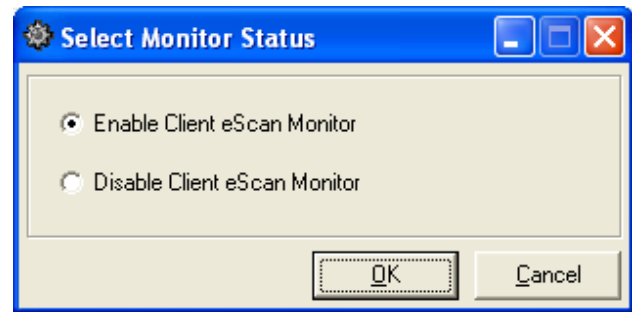
Remote Uninstall eScan Software

Select the button to uninstall eScan software on the selected client.

Change eScan Monitor Status of Selected Host(s)

Select the link to view the following dialog box. You can enable or disable Monitor on the selected client.

Change Alternate Download Status of Selected Hosts

Allows you to change the alternate sites or machine IPs from which hosts can download eScan.

Force Selected Host(s) to Download Updates

Select this menu to force the selected client to download updates and upgrades. Downloading of updates and upgrades by a client is always a pull operation – it is the client who downloads as per the schedule. But in emergencies, this option is used to force the client to download upgrades and updates.

Scan Local Drives of Selected Host(s)

Allows you to scan the local drives of selected hosts for virus. Scanning is done in the background and additional dialog boxes are not displayed.

Scan System Drive of Selected Host(s)

Allows you to scan the System drive of the selected Hosts.

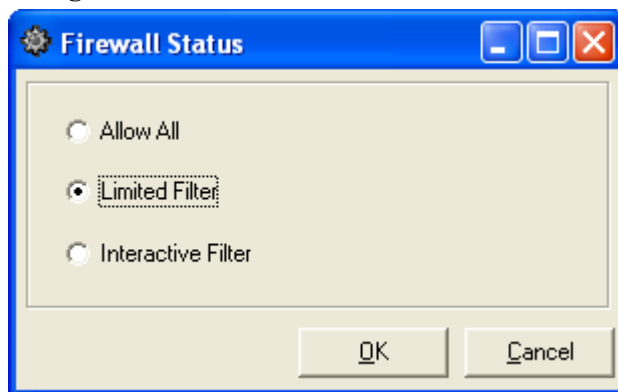**Set Update Server of Selected Host(s)**   Select the link to view the following dialog box. The box allows you to specify IP address of server from which the host can download updates.
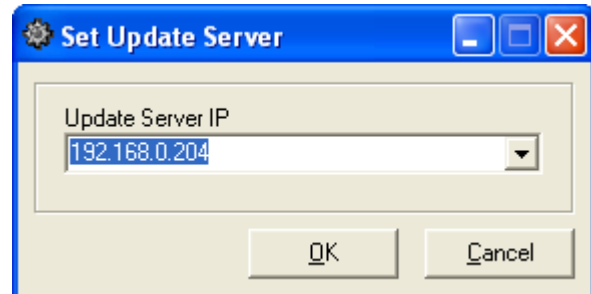
Scan Memory of Selected Host(s)   Allows you to scan the Memory of the selected Hosts.

**Change Firewall Status**   Allows you to change the status of Firewall either to Allow All / Limited Filter / Interactive Filter of the selected Hosts.

Get Client Status by IP

The feature allows you to select a client for a range of IP addresses and obtain their eScan software installation and other details

- In Figure 10.1 , select the client from the left pane and choose from the tool bar.

- Get Client Status by IP : The "**Client Status by IP**" dialog box is displayed. The box allows you to find clients for a range of IP address. Enter the first and the last IP address in the two fields and select **Next >>**.
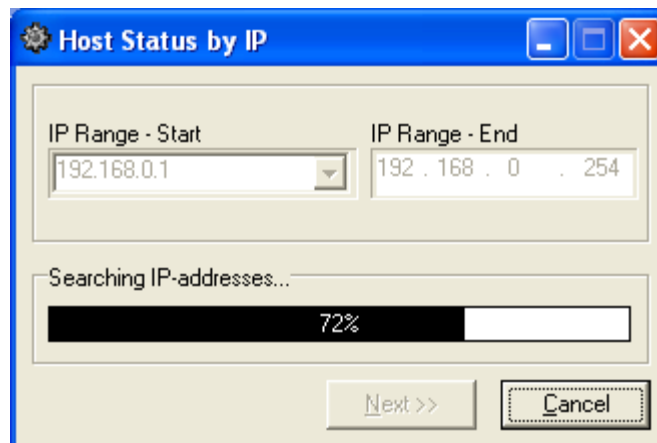
- eServ searches for clients whose IP is in the entered range. Progress bar displays the status. The next screen allows you to view details on eScan Installation. Refer Get Status of eScan Installation.

Set Domain Settings

Screen allows you to select a domain and specify the user name and assign a password. This feature is useful when the administrator needs to connect to a domain."When you click the menu, Add Domain Settings" screen is displayed.

Domain name is displayed in the non-editable field. Enter the user name and password and click Save.

Deploy License

License keys are required to register the software. If you are currently running a trial version, you can use it for 30 days, after which it stops running. You have to then purchase the License keys. This feature allows you to deploy keys to all clients from a single server. License keys can be deployed simultaneously on all clients.

To Launch Deploy License
- In Figure 10.1 select **Deploy License** or click 📄 from the tool bar..
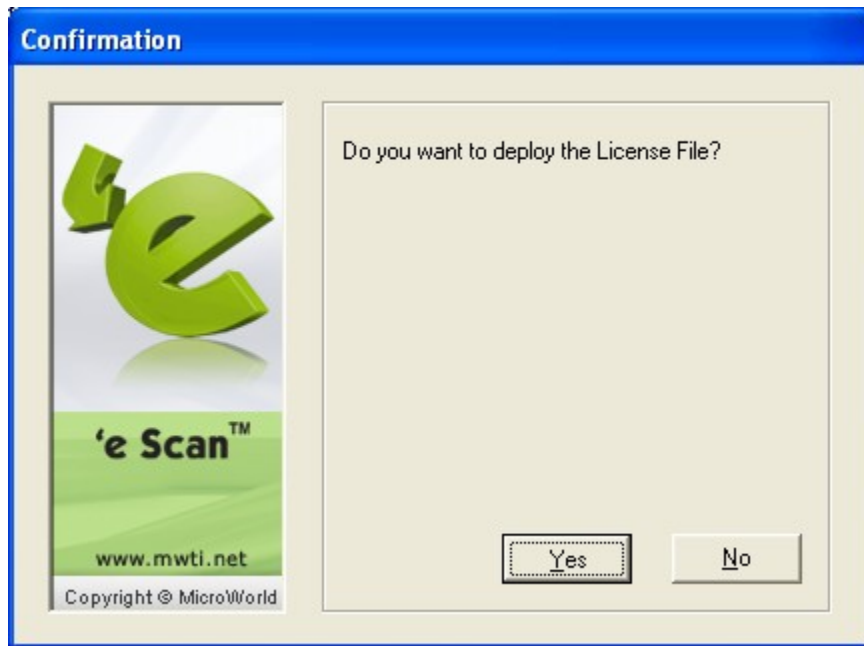- Screen in Figure 10.11 is displayed.

Figure 10.11: To Deploy License Key

- Click on Yes to confirm the license to be deployed on eScan Client.
- The license file will be queued for deployment and eScan clients will download the license as and when they are connected to the eScan server. The below figure shows the confirmation of the license being deployed. Click on OK

Deploy Rule-Sets

Rule-Sets are security policies assigned to govern Internet use in your organization. They are created using the Content Administrator module. eScan Management Console allows you to deploy these uniform global rule-sets to all clients from the server. Rule - Sets can be deployed simultaneously on all clients.

To Launch Deploy Rule Sets

- [Figure 10.1](#) , select Deploy Rule sets or select   from the tool bar.
- Screen in Figure 10.14 is displayed. This window will display the list of policy previously deployed.

Figure 10.14 : Deploy Rule-Sets

- To deploy a new policy click on **Create New Policy** link (screen in Figure 10.15 is displayed)
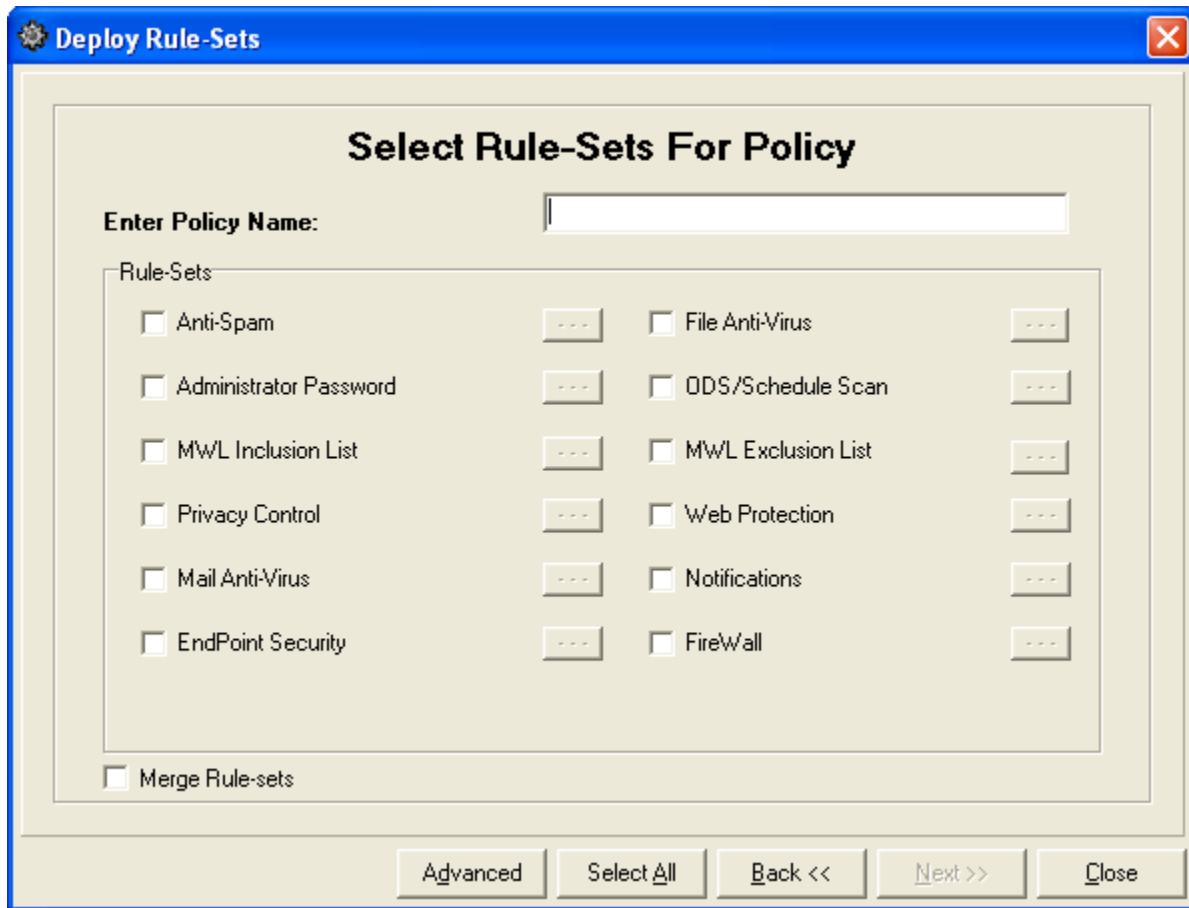

Figure 10.15 : Deploy Rule-Sets (New Policy)

- Field meanings are given in the following table. List of features available in Content Administrator are displayed. To deploy the rule set for the associated feature, select the check box and click . The related screen from content administrator is displayed. Make the required changes and select **Deploy**.

| Field Name	Description
Anti-Spam	Select the check box to deploy Anti-Spam Rule-Sets. These include banned words and phrases in e-mails and actions run for them when such e-mails are detected.
Administrator Password	Select the check box to deploy eScan Protection Center password to the eScan clients. After an eScan client downloads this rule-set, and open eScan Protection Center, a password is requested. The check box is enabled if new password is entered in eScan Content Administrator refer To Change Password.
MWL Inclusion List	If you want to include only some files from MWL-Binding (and exclude all others), you can edit the INCLUDEX.DAT file in the eScan folder & add the necessary files to INCLUDEX.DAT. Click on the button to see the include.dat file.
MWL Exclusion List	Due to compatibility problems if any, it is possible that the MWL layer may not scan some files. Such files are grouped in the MWL exclusion list. Select the check box to associate the list with eServ. Button opens the exclude.dat file.
File Anti-Virus	Select the check box to deploy eScan Monitor settings on its clients.
ODS/Schedule Scan Settings	Select the check box to deploy eScan ODS (On-Demand Scanner) settings and the Scan Scheduler settings.
Privacy Control	Select the check box to deploy Privacy control rule set like Browser Cleanup for the clients.
Web Protection	Select the check box to deploy Web Protection rule set for Web-Page Scanning for the clients.
Mail Anti-Virus	Select the check box to deploy policies like eMail Attachment Control for the clients.
Notifications	Select the check box to deploy eScan Notification on the eScan client systems.
EndPoint Security	Select the check box to deploy Endpoint Security on eScan client systems..

FireWall   Select the check box to deploy Firewall policy on eScan client systems.

Merge Rule-sets   While assigning rule sets, you can merge the new list with old list on the client machine. The list has names related to eScan configuration like blocked/allow sites, restricted words, registry settings, etc. If the button is not selected, then the old list on the client machine is overwritten.

Advanced   Allows you to deploy eScan or MailScan Lite rule sets. Select the button to view the Advanced Settings box.
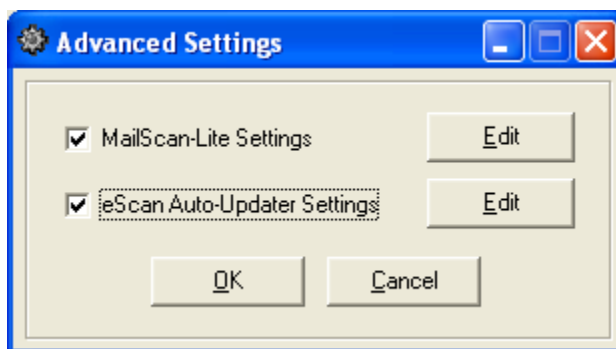

Click **Edit** to edit the settings for eScan and MailScan. The dialog box that is displayed allows you to configure settings for eScan or MailScan. If you select edit for MailScan Lite Settings, then the mailscan.ini box is displayed. If you select eScan, then eupdate.ini box is displayed.
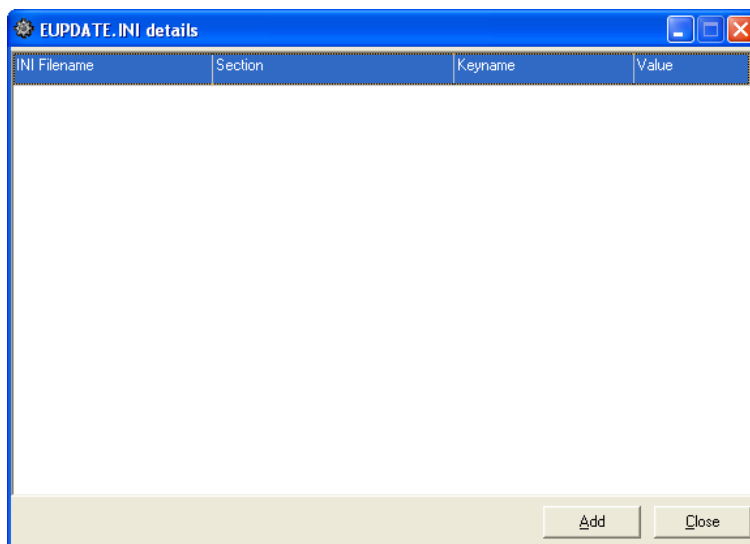
If you have configured settings earlier, they are displayed in the

box under the appropriate columns. Select Add. The Add dialog box that is displayed, allows you to assign values for key names.

eScan has different sections like HTTP, FTP, Config, etc. These are displayed in the drop-down for Section. You need to select a section. Each section has key fields or names displayed in the drop-down for Keyname. For a Keyname, you can either accept the default values that are displayed in the field, Value or enter new values.
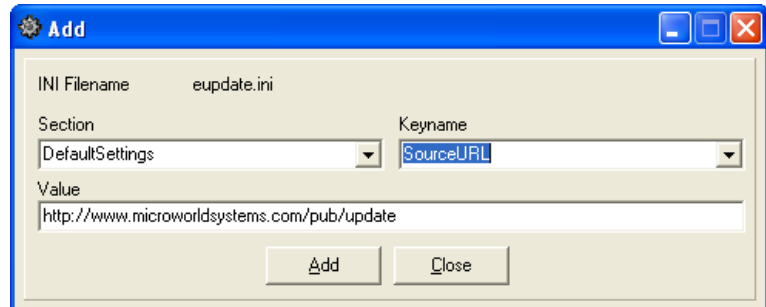
Back / Next Butto	This buttons will take to previous or the next window.
Select All/Unselect All	Select All button allows you to select all the check boxes. After this option is used, the button label changes to Unselect All and in this mode you can unselect all the check boxes.
Deploy	Select the button to deploy with the above settings.
Select All/Unselect All	Select All button allows you to select all the check boxes. After this option is used, the button label changes to Unselect All and in this mode you can unselect all the check boxes.

NOTE: **For more detailed information of eScan features, click on** **Online Help on eScan Features.**
        Click here for Online Help on eScan Features in other Langauages.

Selecting User for Deployment
- After configuring the Rule-sets to be deployed, click the Next Button
- Screen in Figure 10.16 is displayed. This frame allows you to deploy rule-sets for either selected users or all users. This feature allows you to selectively allow users to access and set content the control options.
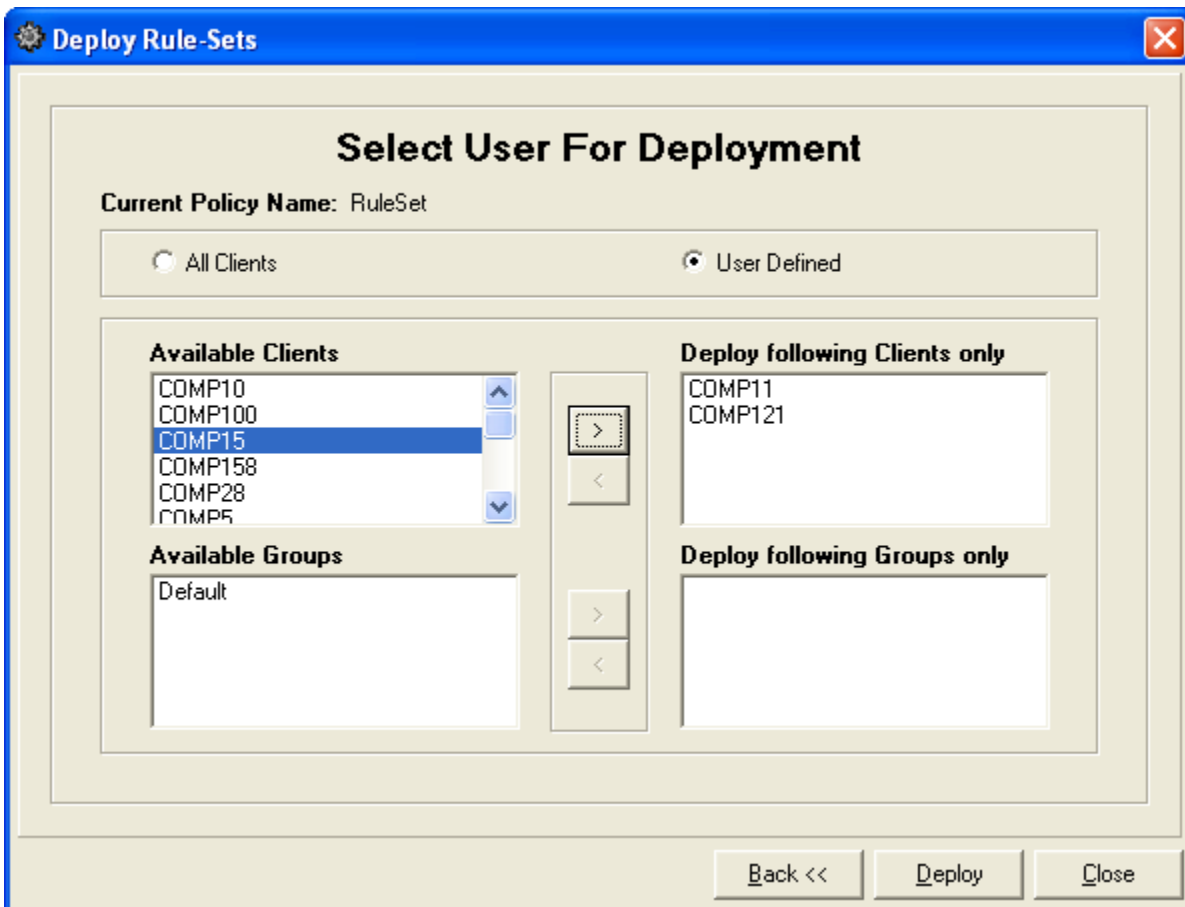
Figure 10.16: Select User for Deployment

All Clients: Deploy rule sets for all clients on the network.
User Defined: Select individual users for whom rule sets can be deployed.

Update All Clients

You can update all clients in the eScan network with the latest Anti-virus signatures that are auto downloaded. This ensures that no client is left uncovered.

When you click on this link, process of updating all clients begins. A progress bar displays the the percentage of clients that are updated.

Shutdown Management Console

This feature allows you to shutdown eServ.

- In [Figure 10.1,](#) select .
- eServ asks you if you wish to shutdown eScan Management Console. Select **Yes**.

Connection Errors

This section provides a list of solutions to errors you might face while using eServ.

Error Name/Number	Error Message	Solution
Error 4000	Unsupported OS	You can deploy Softwares from a machine having NT or above Operating System to Clients running on Win 95/98/Me/NT/2000/XP/ME. But, if you try to install from a Win 95/98/Me machine to a Client running Win NT/2000/XP/ME, then you get an error 4000. To solve the problem, install/deploy from a Win NT or higher OS machine.
Logon Failure/1326	Unknown username or bad password	If you get the error while deploying to machines running NT & above OS, verify the Administrator password of the machines. In case you get this error while deploying to 9x machines, verify that the remote-administration password is correct.
Error 67	Network name cannot be found	If you are remote deploying to machines running Win NT/2000/XP, then you need [To enable hidden shared folders on Win NT/2000/XP Clients](#)
Error 86	Specified Password is invalid	If you are remote installing on Clients running on Win 95/98/ME, then you need to [To enable Remote Install Settings on Win 95/98/ME Clients](#)

System

Displays the default screen of eServ. Refer Figure 10.1 for details.

Updates

Displays a list date and time when an event was logged. You can right click and choose to clear/delete all or print the list.

Auto Install

Displays logged events of auto install. Press CTRL+T to set up Host Configuration.

Infected Machines

You can see a list of infected machines in the network. Right Click on the screen and select Refresh. Network machine names are displayed. Right click on the screen and select View. Double click on a machines to see the virus report for the machine.

The machine name/IP, name of the detected virus and the location in the machine where it was found and the action taken are given.

You can generate graphs that show number of infections, number of viruses, etc. Click Graph and select one of the options that allow you to generate graphs by number of infected computers, number of viruses, by date and by action.

The default graph is displayed as a pop-up. You can choose the type of graph like Bar, Stacked, Pie, etc. Scroll buttons on the tool bar allow you to scroll left, right, up and down the screen. Select an area of the graph and zoom in or out.

The graph can be saved as an image or printed.

Virus Report

The screen allows you to generate a variety of virus activity reports. You can select to generate reports for All Computers or a range of IPs. The report can be generated daily, weekly, monthly, annually or since eServ was installed. You can also create Custom report by specifying the Starting and Ending dates.

You can generate graphs that show number of infections, number of viruses, etc. Click Graph and select one of the options that allow you to generate graphs by number of infected computers, number of viruses, by date and by action.

The default graph is displayed as a pop-up. You can choose the type of graph like Bar, Stacked, Pie, etc. Scroll buttons on the tool bar allow you to scroll left, right, up and down the screen. Select an area of the graph and zoom in or out.

The graph can be saved as an image or printed.

License

The screen displays the License version and information like License size and number of days remaining for Renewal.

Blocked Hosts

The screen displays the ip address or range of ip address which is blocked from connecting to the eScan server and downloading the updates. Right click on the screen and select **Add IP Range in the List of blocked hosts** to add clients from connecting to the eScan server.

To remove the IP range from the Blocked list, select the IP address and right click and then select **Remove From the List of blocked Hosts.**

Client Live Updater

The screen displays the online status of all the eScan clients connected to the eScan server. It will display the online processes running on the eScan clients systems.

Reports

eScan Management Console, functions as a centralized server that distributes updates and upgrades to all machines in your organization, using eScan products.. In a large corporate network environment, you can significantly reduce the costs and the Internet traffic by setting up a centralized updating structure. You don't have to download updates, deploy license keys or assign security policies for individual machines.

The eScan FTP server automatically downloads the updates at regular pre-defined intervals from the Internet and includes them in a dedicated directory on the hard disk of the system such as the file server that is accessible to all the network users. Security policies and license keys can be deployed globally to all machines. This ensures uniformity, consistency and removes human errors.

You can create multiple eScan servers on a LAN. If one eScan server is down, the updates can be pulled from another eScan server. The machine designated as the eScan server must have Internet connectivity. It need not be a dedicated machine. The eServ tasks run in the background while you carry out your normal work.

Reports feature allows automatic mailing of reports from clients to system administrator. The report typically displays activity details like files downloaded, virus detected, etc.

Process of mailing reports: In the eScan Management Console, select **Reports** > **Configure Report Mailing** (Set Configure Mailing and Schedule) > **View Reports** > **Mail Reports Now**

- Configure Reports Mailing
- View Log
- Mail Reports Now
- Other Reports Menu

<u>Configure Reports Mailing</u>

The first step is to configure the settings. You specify e-mail IDs of sender, receiver, IP address and at what time the reports are mailed. Reports are generated by the system and user intervention is not required for this. Once all the valid values are entered, the system automatically generates and sends reports at the specified time.

- In Figure 10.1, select **Reports** and choose **Configure Reports Mailing** or select from the tool bar.

- Screen in Figure 10.17 is displayed.

- There are two tab pages: Mail Configuration and Schedule.

- **Mail Configuration** Allows you to specify e-mail IDs of sender, receiver, Mail Server IP address and port number.

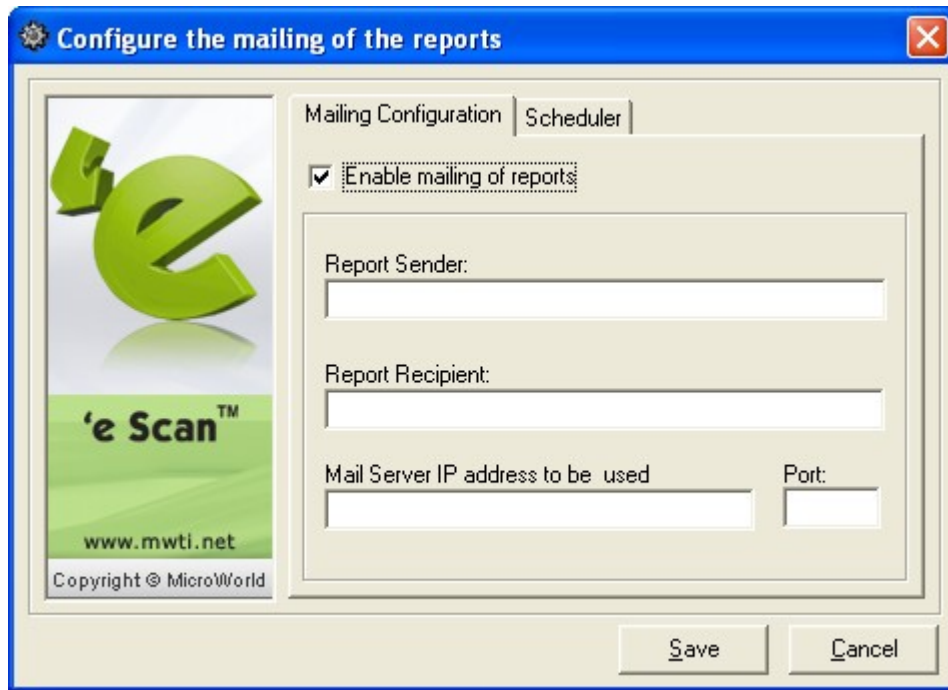- **Schedule** Allows you to specify when the reports are mailed.

Figure 10.17: Reports Mail Configuration

Field Name	Description
Enable email Reports	Select the check box to enable reports to be e-mailed. Fields in this screen are enabled only if the check box is selected.
Report Sender	Enter email ID of person sending the report.
Report Recipient	Enter email ID of person receiving the report.
Mail Server IP address to be used	Enter MailServer IP address from which e-mail reports are sent.
Port	Enter port number of above mail server.

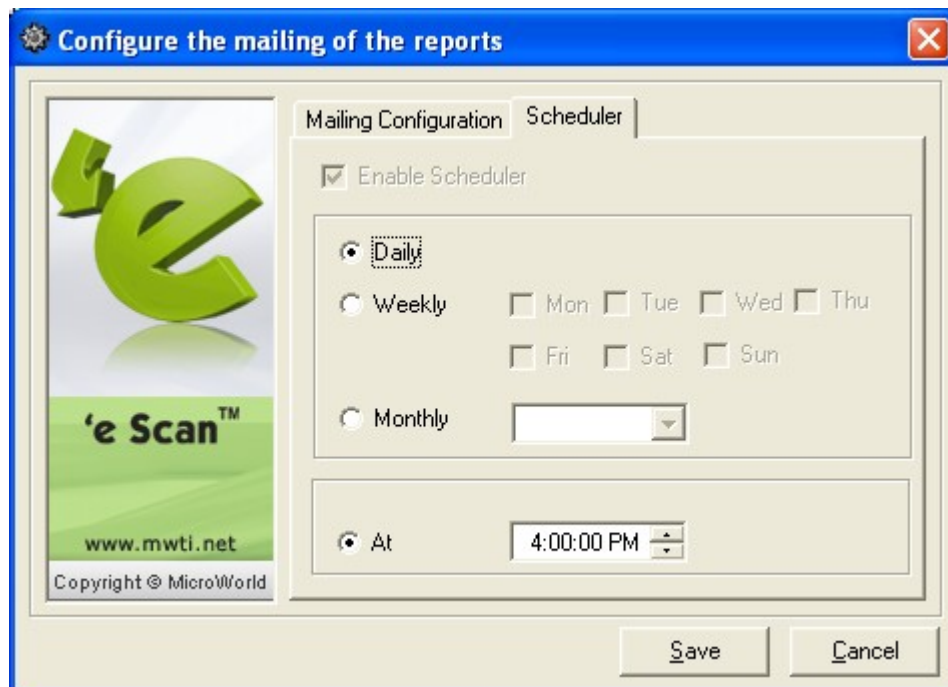- Select the Schedule tab to view screen shown in Figure 10.18

Figure 10.18 : Set Report Scheduler

View Log

You can view detailed report of any log activity, displayed in the screen under 'Logged Event'. This feature is enabled only when Reports Mail Configure is set.

- Select the logged event whose report you want to view.

- Reports menu, select **View Report** or select [icon] from the toolbar.

Mail Reports Now

The feature allows you to e-mail a report to the receiver specified in the Configure Report Mailing.

- In <u>Figure 10.1</u> , select the activity from the screen under 'Logged Events'.

- In **Reports** menu, select **Mail Reports Now** or select ⊡ from the tool bar. The report is e-mailed to the specified receiver.

Other Reports Menus

Other features available in Reports menu are explained below: Select the logged event or client and click on the menu to run it.

Delete log ⊡**:** Allows you to delete a logged event of selected eScan client system

Delete All user Logs ⊡**:** Allows you to delete all logged events displayed in the screen.

Refresh User Logs ⟳**:** Displays updated logs for a client.

Refresh All user Logs ⟳ **:** Displays updated values for all.

Appendix

What eServ does

Remote Installation: You can **simultaneously** install eScan on multiple clients or workstations in your network, from a single machine. Remote installation runs in the background and the normal activity on a workstation can continue without interruption. This saves time, labor and ensures that no machine is 'missed'. To install the software on one machine, takes about three to four minutes. If you had to install on 100 machines, it would take about 400 minutes. Add to this work stoppage for the workstations, need for CD ROM drive on individual workstations, etc. eServ avoids all these costs.

You must first install eScan as a Server on one machine. This is called as the central server. The central server does not require any special 'server hardware configurations' but can be any convenient machine. Further remote installations on clients are done using this machine. The reverse process, remote uninstall is also supported.

- Only machine designated as the central server needs to auto download updates. These are deployed to individual clients. This ensures reduced Internet access costs and uniformity in deployment of upgrades to all machines.

- The Server has an **announcement** mechanism that announces to clients when new deployables are received. Client has a **listening** mechanism and listens to announcements from the server.

- Upgrades need to be manually installed only on the central server. These are deployed to individual clients. This ensures reduced downtime costs for installation and ensures that all machines are covered.

- Security policy for eScan Protection administration, attachment blocking, restricting website and web page access, script/Spam/e-mail blocking, etc. can be first set up on the central server and tested. This can be then deployed on all machines. It ensures a uniform security policy across the network.

- As an added benefit, eServ also allows other software to be remotely installed and uninstalled.

Remote Deployment: Simultaneous deployment of updates, upgrades, license keys and security policies to all clients in the network, is one of the critical assignments that eServ handles easily. Updates are vaccines for new viruses stored in MicroWorld's, dedicated download sites. Deployment is normally a 'pull' operation meaning that clients have to pull updates on their own from the server. The following points illustrate tasks eServ does for you:

- Only machine designated as the central server needs to auto download updates. These are deployed to individual clients. This ensures reduced Internet access costs and uniformity in deployment of upgrades to all machines.

- The client has an **announcement** mechanism that announces to clients when new deployables are received. Client has a **listening** mechanism and listens to announcements from the server.

- Upgrades need to be manually installed only on the central server. These are deployed to individual clients. This ensures reduced downtime costs for installation and ensures that all machines are covered.

- Security policy for content administration, attachment blocking, restricting website and web page access, script/Spam/e-mail blocking, etc. can be first set up on the central server and tested. This can be then deployed on all machines. It ensures a uniform security policy across the network.

- License keys can be deployed simultaneously on all clients.

Admin Control: eServ allows you to administer the Internet access activity on all clients. You first define the security policy for your organization, on the central server. These are then deployed to all clients. The following tasks can be performed:

- Selective net access – You can specify any time interval, when net access is blocked.

  Monitor activity – You can view in real-time, sites and web pages, accessed

from any or all client and create a log file.

- Archive e-mails – You can archive e-mails sent and received by any user, logging in through your network, create an archive of attachments, etc.

Rogue machines These are machines that for some reason fail to pull updates, etc. from the server. In such cases, the server can force the truculent machine to pull the deployable. It takes one out of sync machine with no updates, to spread infections.

Client Status: eServ allows the administrator to view status of all clients. Details displayed include logged events, last update pulled, if any client is infected, actions taken etc. The reports can be e-mailed to specified IDs. This allows immediate and focused actions for 'rogue'

Enable Hidden Shared Folders on Win NT/2000/XP machines

- For clients running on Win NT/2000/XP, the hidden shared folder "`admin$`" should be enabled. When networking is installed on a Windows machine, it will automatically create hidden shares to the local disk drives. It is possible to disable the sharing at run-time, but this tweak will stop the automatic sharing altogether. If the default share is disabled then enable it through the windows Registry.

- **Registry Path**

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters]

  Name: AutoShareServer (For Windows NT/2000 Server), AutoShareWks (Windows NT/2000 Workstaions)
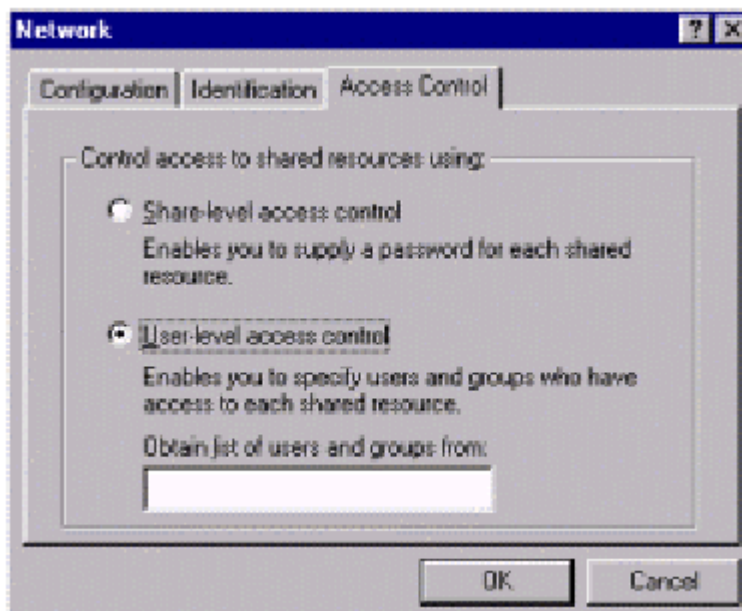
  Type: REG_DWORD (DWORD Value)

  Value: (0 = disable shares, 1 = enable)

To enable Remote Install Settings on Win 95/98/ME Clients

- **Click**   [Start] > [Settings] > [Control Panel] > [Network]

- Select "**Access Control**" tab page shown below.

- Check which radio button is enabled. Normally, by default, radio button for "**Share-level access control**" is selected. The other radio button is "**User-level access control**". Process for enabling Remote Install is explained for both selections.

  When **"Share-level access control"** radio button is selected, follow the following procedure to enable Remote Administration.

- Click

There are three tab pages in the dialog box.

- Choose the **Remote Administration** tab page and select "**Enable remote administration of this server"** check box**.** Enter a password for Remote Administration and select **OK**.
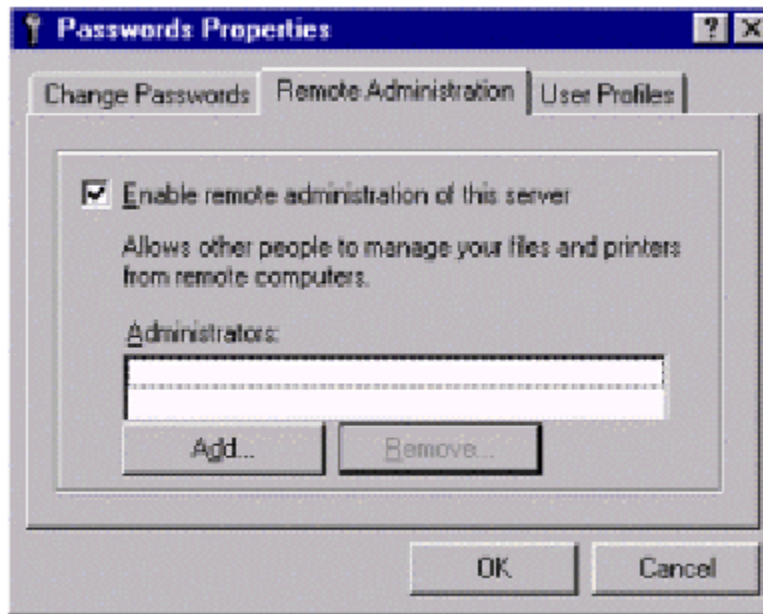

- Click

- In **Configuration** tab page, select "**File and Print Sharing…**" button. The dialog box "**File and Print Sharing**" is displayed.

- Select the check boxes "**I want to be able to give others access to my files.**" and "**I want to be able to allow others to print to my printer(s).**" and select **OK**. Select **OK** in the main dialog box.

  When **"User-level access control"** radio button is selected, follow the following procedure to enable Remote Administration.
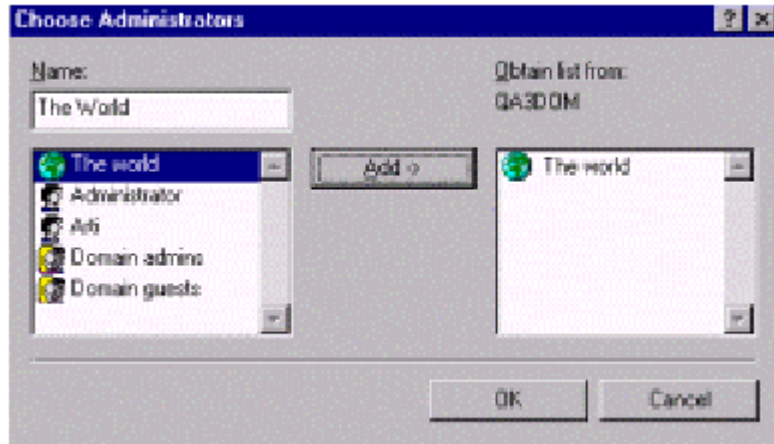
- Click

- Choose the **Remote Administration** tab page and select "**Enable remote administration of this server"** check box**.**

- Select **Add**. Following dialog box is displayed.

Select **"The World"** from the left panel and choose **Add >>** and click **OK**. Previous screen is displayed and **"The World"** you have added is displayed in the list box.

- Click

- In **Configuration** tab page, select "**File and Print Sharing…**" button. The dialog box "**File and Print Sharing**" is displayed.

- Select the check boxes "**I want to be able to give others access to my files.**" and "**I want to be able to allow others to print to my printer(s).**" and select **OK**. Select **OK** in the main dialog box.