This document provides information to install and use eServ.

User Guide for

eServ for eScan Version 2.6

Copyright Notice:

For Technical support, contact: support@mwti.net

For Sales enquiry, contact: sales@mwti.net

Document Number 2ESV2.6/01.01.03

List of Figures

The following figures are included in this guide

Table of Contents

Tell me about

eServ has many features that help you run your tasks easily and quickly. An extremely user-friendly interface makes most of the tasks a simple point and click affair. This chapter provides a quick way to access the important features. It is recommended that you read the whole guide before using the links in this chapter.

Welcome

eServ allows remote administration of eScan Anti-Virus and Content Security software in your network. It allows you to create a central server and simultaneously install and deploy eScan on multiple clients in the network.

This guide provides information about what eServ does and how to get the most out of it. eServ is available only with eScan CORPORATE Edition.

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 chapters the first three chapters provide information related to what eServ does, how to install it and how to navigate through the interface. Chapter 4, provides all details and features of eServ. Each screen and field in the user interface is explained in detail along with the relevant screen shots.

Overview: Provides details of What eServ does, Featuresof eServ and How to use eServ.

Tell me about… Provides a quick reference to key features and tasks in the application.

Installation: Gives the Software and Hardware requirements to run the application along with Prerequisites you have to complete before the installation. Details of Installation Process are given along with screen shots.

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: Chapter gives details of how to create 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.

Appendix Provides answers to Frequently Asked Questions. Also given are details on availing our Support, and a Glossary of terms occurring in the guide. Included is an Index of words occurring in this guide.

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. It is enclosed in ' '.
`Type`	Information you need to enter.
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..

Note:
Provides additional information about a certain topic.

- Bulleted lists provide information or indicate procedures with steps that you carry out sequentially.

Contact Us

If you have any queries about our products or have suggestions and comments about this guide, please send them to:

Our Head Office:
MicroWorld Technologies Inc.
109 White Oak Lane, Suite # 200-P, Old Bridge,
NJ 08857, US.
Tel (732) 607-7501/02 Fax (732) 607-7503

Our Asia Pacific office:
MicroWorld Software Services.
Plot No 80, Road 15, MIDC, Marol,
Andheri (E), Mumbai,
India.
Tel (91) - 22- 28265701 - 05 Fax (91) - 22- 28304750

For sales enquiry, e-mail: sales@mwti.net

For support enquiry, e-mail: support@mwti.net

For more information about our products please visit
www.mwti.net

Overview

About MicroWorld

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 the need for eServ, what eServ does and how to use it.

Need for eServ

In an organization with many machines in the network, uniform installation and deployment of Anti-Virus and Content Security software across all machines is a formidable task. One obvious solution is to form a team of higly paid system administrators who go to individual machines, wait for the elusive users to turn up, force them to give out the passwords, stop the current process and begin the installation.

The same process needs to be followed for installing updates, upgrades, license keys, etc. Every month more than 500 nre viruses 'appear'. These can be only cleaned if you regularly download and run Updates. It needs only one machine to spread a virus in a network.

Next comes the issue of enforcing global security policies across your network. It would be very daunting to form a task force that monitors the surfing activity on all machines around the clock.

Every machine needs a CDROM drive. We have to assume that the team is very diligent and will not 'forget' a machine. If you have given up trying to calculate the costs, then read on.

What eServ does

eServ allows you to create a Central Server on any machine in your network. It functions as a server for other machines in the network. These are designated as clients. The server allows you to run the following tasks:

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 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.
- 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.
- 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.

Admin Control: eServ allows you to administer the uniform security policy that governs Internet access activity on all clients. You first define the uniform 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 to block net access for any or all machines.

- **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 deployables. 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' machines.

Components of eServ

eServ has the following components. They are interlinked and work in tandem.

Server: You create a central server on a machine. Initial installation of eScan in a network needs to be done on only this machine.

How to Use eServ

You must forst install eScan as a server on one machine in the network. Subsequent installations for clients are done through this server.

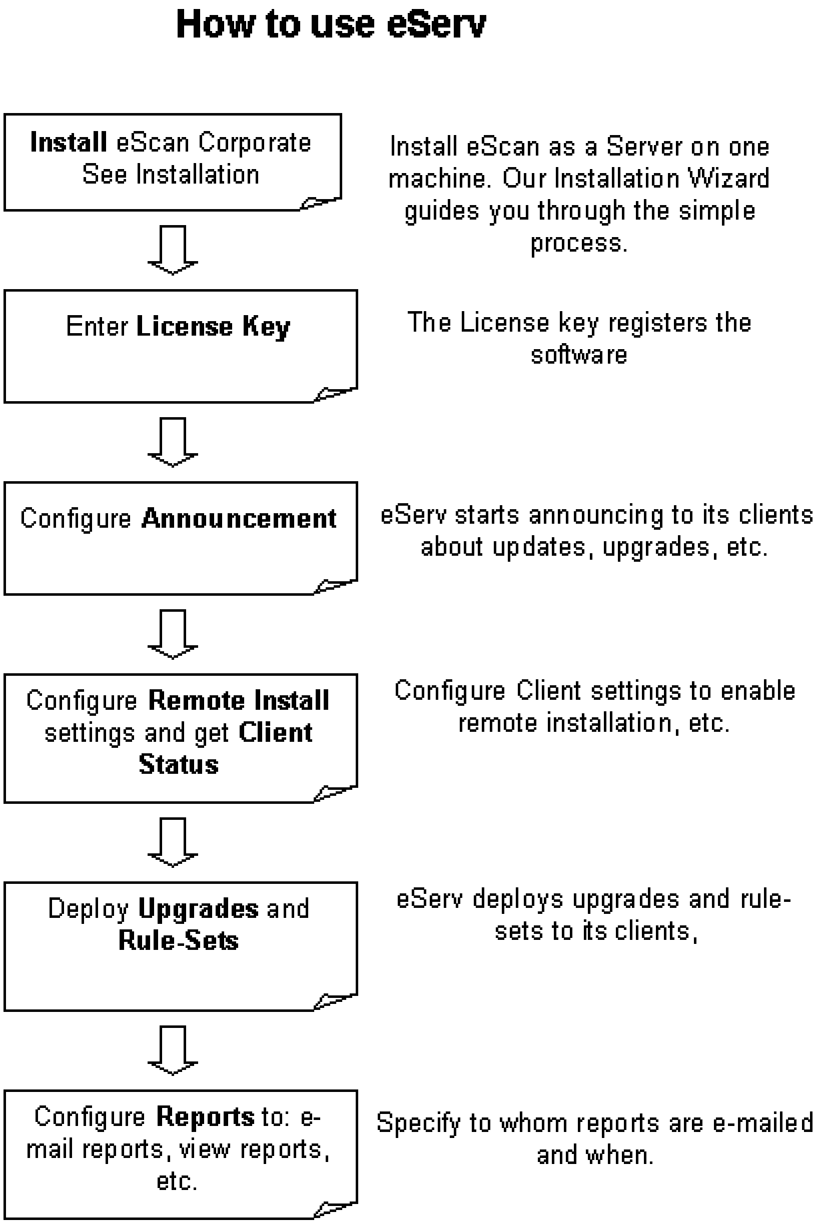

How to use eServ
Install eScan Corporate See Installation
Install eScan as a Server on one machine. Our Installation Wizard guides you through the simple process.
Enter License Key
The License key registers the software
Configure Announcement
eServ starts announcing to its clients about updates, upgrades, etc.
Configure Remote Install settings and get Client Status
Configure Client settings to enable remote installation, etc.
Deploy Upgrades and Rule-Sets
eServ deploys upgrades and rule-sets to its clients,
Configure Reports to: e-mail reports, view reports, etc.
Specify to whom reports are e-mailed and when.

Figure A. How to use eServ

Installation

This chapter provides information about the software and hardware requirements of your machine for using our products and gives step-by-step instructions on installation. eServ is bundled with eScan CORPORATE Edition and is self installed when you install eScan.

Note

- eScan must first be installed as a **server** on one machine. In **step 5** of the installtion process, select **Yes** in the dialog box showing the message 'Do you want to make this system as the eScan server?' The section Installation Process provides all details.
- Remote install on multiple **clients** using this server. In Step 5, select **NO** in the dialog box showing the message 'Do you want to make this system as the eScan server?'
- Installation process is the same for both Server and Clients. You need to gather additional imformation when installing on multiple clients.

Software and Hardware Requirements

Your system should have **Windows 95/NT (II nd Edition)** or above installed.

Your system should have minimum of **64 MB RAM, 50 MB** of free hard disk space and a CD ROM player.

Prerequisites for Installation as Server

Before installing the software ensure that the following are done:

- Uninstall any Anti Virus software including previous versions of our products.
- Check for the largest drive/partition and install eScan / Mail Scan on that drive/partition.
- Hard Disk Space and type SCSI/IDE.
- Mail Server and the Service Pack if applied.
- Operating System [version and build and the Service Pack if applied).
- Valid Username and Password for Logon to the PC and the Internet access.
- Administrator or Postmaster ID or e-mail Address.

- IP/PORTS Address of the Mail Server Machine.
- DNS IP Address if applicable.
- Gateway IP Address if applicable.
- Relay IP Address in setup of MS-Exchange/Lotus Notes.
- Other software like Proxy; Firewall, DHCP installed on your system and third party software used for downloading.
- Domain Names and the IP Address from where the mails are downloaded from and to where they are forwarded.
- SWAP Partition Size.

Prerequisites for Installation on Clients/Hosts

You need to have the following additional information before installing on Clients.

- IP address. It is possible to enter a range of IP addresses.
- Client machine User name and password.
- You need to configure each host and **enable Auto Install** option on them.
- Global security policies for the network must be configured in the Server. These are set in **Content Administrator** Module of eScan. The policies can then be assigned to Clients.

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**

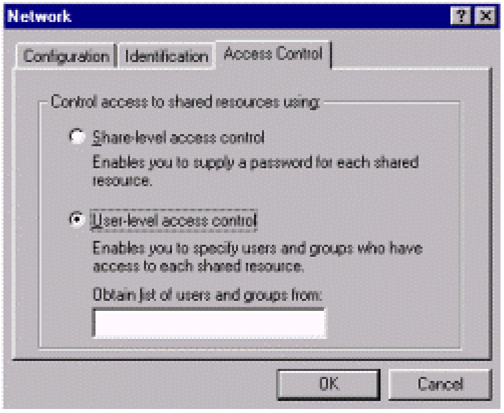
```
    [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanma
nServer\Parameters]

            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.



Control access to shared resources using:

○ Share-level access control

Enables you to supply a password for each shared resource.

● User-level access control

Enables you to specify users and groups who have access to each shared resource.

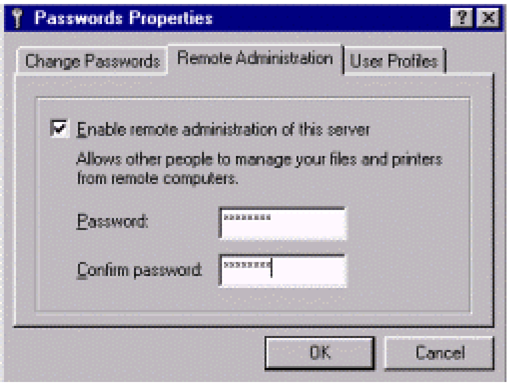
Obtain list of users and groups from:

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 Start > Settings > Control Panel. > select Passwords. 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**.



Passwords Properties

Change Passwords | Remote Administration | User Profiles

☑ Enable remote administration of this server

Allows other people to manage your files and printers from remote computers.

Password: ********

Confirm password: ********

- Click Start > Settings > Control Panel > Network.

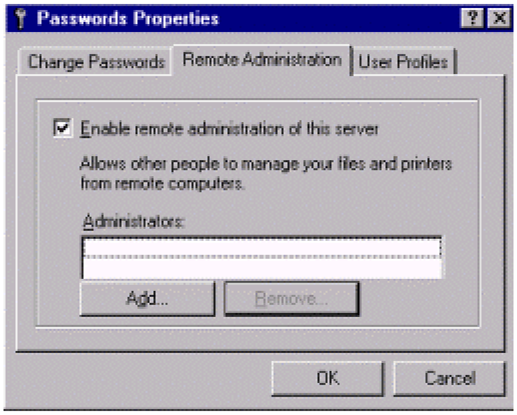
- In **Configuration** tab page, select "**File and Print Sharing…**" button. The dialog box "**File and Print Sharing**" is displayed.

- 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 Start > Settings > Control Panel. select Passwords. 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**.**



Passwords Properties

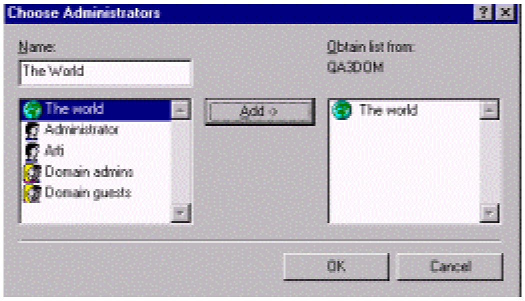
Change Passwords | Remote Administration | User Profiles

☑ Enable remote administration of this server

Allows other people to manage your files and printers from remote computers.

Administrators:

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



Name: The World

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 Start > Settings > Control Panel > Network.

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

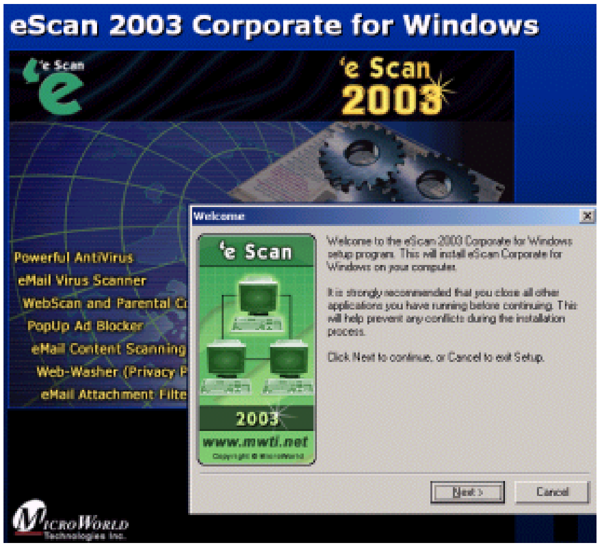
- Select the check boxes "**I want to be able to give others access to my files.**" and "**I want to be able to allow others to print to my printer(s).**" and select **OK**. Select **OK** in the main dialog box.

Installation Process

Installation is very simple, a point and click operation and done using the built-in install wizard. A user-friendly interface prompts you and presents a range of choices. Instructions are displayed in the screens that give you specific information. To abort installation, select "Cancel" in any of the screen. This section gives the step-by-step installation process.

- The software is sent to you in a CD. Load the CD in the player and open the CD ROM directory. A small movie that gives a preview of key features in eScan is run. You can click the "**Skip Intro**" link to directly go to installation.

- Installation is started automatically. Screen in Figure 1.1 is displayed. This is the start up screen for installing the application.



Welcome to the eScan 2003 Corporate for Windows setup program. This will install eScan Corporate for Windows on your computer.

It is strongly recommended that you close all other applications you have running before continuing. This will help prevent any conflicts during the installation process.

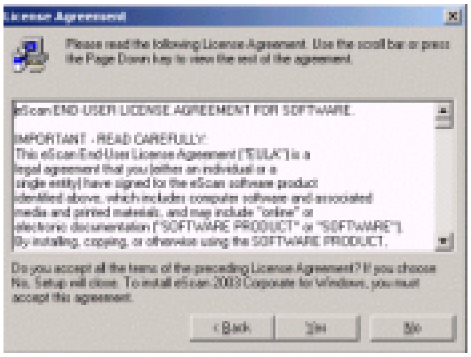
Click Next to continue, or Cancel to exit Setup.

Figure 1.1 Install – Opening Screen

Step 1

- In Figure 1.1, select **Next** to begin installation. Screen in Figure 1.2 is displayed.

- This screen shows the license agreement between you and MicroWorld. Read the instructions and select **Yes** if you accept the terms. Select **No** if you do not accept the terms in which case the installation process is aborted.



Please read the following License Agreement. Use the scroll bar or press the Page Down key to view the rest of the agreement.

eScan END-USER LICENSE AGREEMENT FOR SOFTWARE.

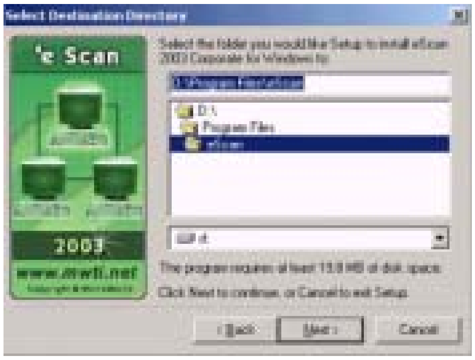
IMPORTANT - READ CAREFULLY:
This eScan End-User License Agreement ("EULA") is a legal agreement that you (either an individual or a single entity) have signed for the eScan software product identified above, which includes computer software and associated media and printed materials, and may include "online" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT,

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install eScan 2003 Corporate for Windows, you must accept this agreement.

Figure 1.2 License Agreement

Step 2

- If you select **Yes**, screen in Figure 1.3 is displayed.
- You select the directory to install the application. The default path is displayed. To change the location, browse your PC and select the directory.


Select Destination Directory

Select the folder you would like Setup to install eScan 2003 Corporate for Windows to:

D:\Program Files\eScan

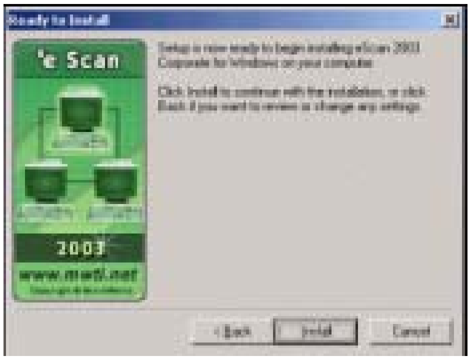
The program requires at least 15.9 MB of disk space.

Click Next to continue, or Cancel to exit Setup.

Figure 1.3 Select Destination Directory

Step 3

- Select "**Next**". Screen in Figure 1.4 is displayed.
- The application is ready to be installed. Select **Install**.


Ready to Install

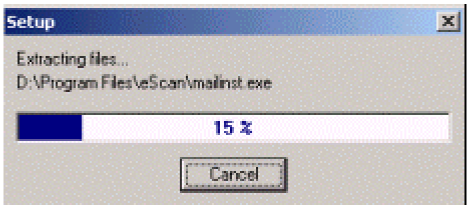
Setup is now ready to begin installing eScan 2003 Corporate for Windows on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Figure 1.4 Begin Installation

Step 4

- The software is copied and uploaded into the directory you have selected. A folder with the applications name is created.
- A progress bar showing status of installation is displayed.


Setup

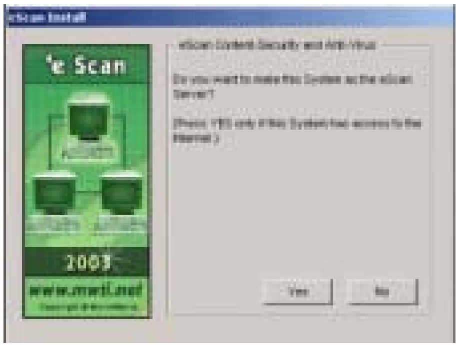
Extracting files...
D:\Program Files\eScan\mailinst.exe

15 %

Figure 1.5 Installation progress bar

Step 5

- Screen in Figure 1.6 is displayed.
- If you are installing eScan Corporate, system asks you if eScan should be installed as a Client or a Server on the system. Select "**Yes**" to install eScan as Server or "**No**" to install eScan as Client.
- Install eScan as a **server** on one machine, when you want to deploy across a network. This server can be used to install across multiple clients in a network.
- If you install it as the eScan Server, access to the Internet should be


eScan Install

eScan Content Security and Anti-Virus

Do you want to make this System as the eScan Server?

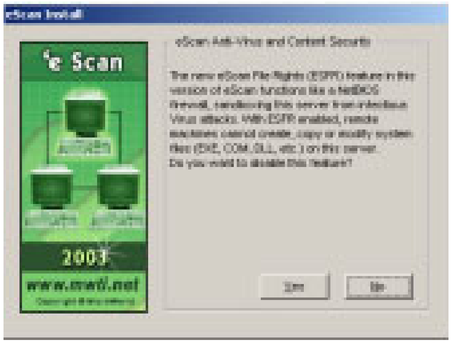
(Press YES only if this System has access to the Internet.)

Figure 1.6 Install as Server or Client.

available on the system.

Step 6

- The new feature in eScan allows you to restrict users from remotely modifying files on the eScan Server.
- Select **No** to prevent others from modifying server files (recommended). Select **Yes** to permit them.



eScan Install

eScan Anti-Virus and Content Security

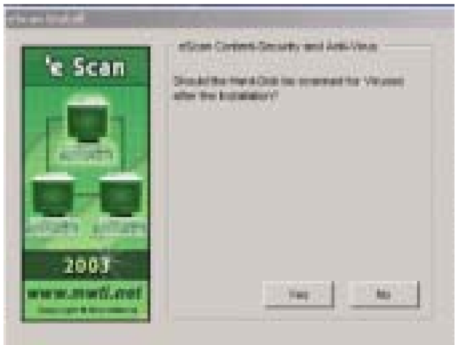
The new eScan File Rights (ESFR) feature in this version of eScan functions like a NetBIOS firewall, sandboxing this server from infectious Virus attacks. With ESFR enabled, remote machines cannot create, copy or modify system files (EXE, COM, DLL, etc.) on this server.
Do you want to disable this feature?

Yes No

Figure 1.7 Assign Remote File Modify Rights

Step 7

- Screen in Figure 1.8 is displayed. You can begin scanning of your hard disk after the installation is over by selecting "**Yes**".
- If you have other Anti Virus systems running or have never used Anti-Virus software before then MicroWorld strongly recommends that you select **Yes**. Select "No" to scan later.



eScan Install

eScan Content Security and Anti-Virus

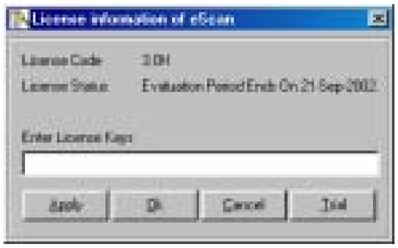
Should the Hard Disk be scanned for Viruses after the Installation?

Yes No

Figure 1.8 Assign Rights

Step 8

- Screen in Figure 1.9 is displayed. You need to enter the license key code to register the software. Select **Apply** and **OK**. If you are using a trial version or are unable to find the key, select the **Trial** button. You can purchase the License keys from MicroWorld.



License information of eScan

License Code 3 DH

License Status Evaluation Period Ends On 21 Sep 2002

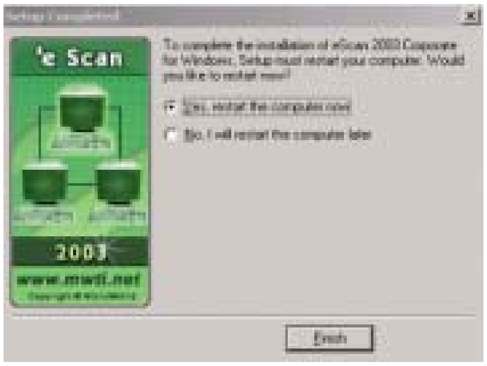
Enter License Keys

Apply Ok Cancel Trial

Figure 1.9 Enter License Key

Step 9

- You need to restart your system to initialize the software. Select **Yes**.



Setup Completed

To complete the installation of eScan 2003 Corporate for Windows, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now

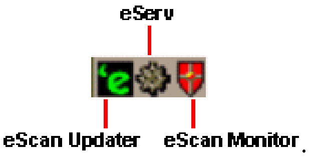
○ No, I will restart the computer later

Finish

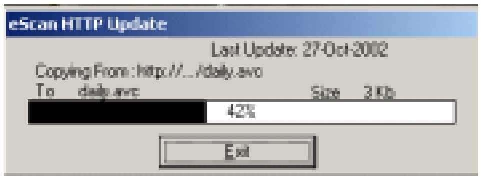
Figure 1.10 Opening Credits of eScan

Step 10

- eScan is installed on your machine. The following icons are added to the task bar at the bottom of your screen.



- The component eServ appears only if eScan is installed as a Server in step 5.


eScan HTTP Update

Last Update: 27-Oct-2002

Copying From : http://.../daily.avc

To daily.avc Size 3 Kb

42%

Figure 1.11 eScan Auto Update

- If your Internet access is on, the latest vaccine updates are automatically downloaded and run. Progress bar shows the download progress.

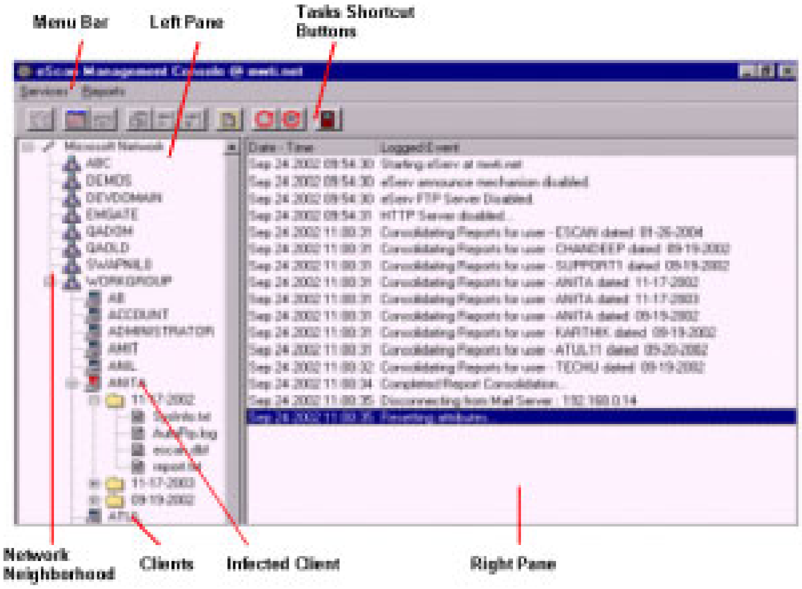
After the application is installed you can access the on-line help from **Help** in the menu bar. The online help provides detailed information to use

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.



```
Date - Time           Logged Event
Sep 24 2002 09:54:30  Starting eServ at mwti.net
Sep 24 2002 09:54:30  eServ announce mechanism disabled
Sep 24 2002 09:54:30  eServ FTP Server Disabled
Sep 24 2002 09:54:31  HTTP Server disabled.
Sep 24 2002 11:00:31  Consolidating Reports for user - ESCAN dated 01-26-2004
Sep 24 2002 11:00:31  Consolidating Reports for user - CHANDEEP dated 09-19-2002
Sep 24 2002 11:00:31  Consolidating Reports for user - SUPPORT1 dated 09-19-2002
Sep 24 2002 11:00:31  Consolidating Reports for user - ANITA dated 11-17-2002
Sep 24 2002 11:00:31  Consolidating Reports for user - ANITA dated 11-17-2003
Sep 24 2002 11:00:31  Consolidating Reports for user - ANITA dated 09-19-2002
Sep 24 2002 11:00:31  Consolidating Reports for user - KARTHIK dated 09-19-2002
Sep 24 2002 11:00:31  Consolidating Reports for user - ATUL11 dated 09-20-2002
Sep 24 2002 11:00:32  Consolidating Reports for user - TECHU dated 09-19-2002
Sep 24 2002 11:00:34  Completed Report Consolidation...
Sep 24 2002 11:00:35  Disconnecting from Mail Server : 192.168.0.14
Sep 24 2002 11:00:35  Resetting attributes...
```

Figure 2.1 Typical User Interface

Screen Components

Typical screen components are explained below:

Screen Component **Function**

Menu Bar: These are the main menus that contain similar group of sub-menus: **Services** and **Reports**. You perform specific tasks with them. The menus and their sub-menus are explained below.

Services

Carries a group of tasks that allow you to configure and run eServ. The following tasks are provided:

Start Stop Announcement: Toggle to start and stop announcement mechanism of eServ.

Host Configuration: Allows you to configure hosts or clients in the eScan networkl.

Deploy Upgrade: Deploy upgrades on a multiple clients, identified by a range of IP address.

Get Client Status by IP: View and configure clients by the IP address.

Deploy License: Deploy license keys to multiple clients.

Deploy Rule-Sets: Deploy Rule-Sets to multiple clients.

Shutdown Management Console: Shuts down the management console on the server.

Get status of eScan Installation: Allows you to view eScan installed components status on each client. You can see when a client has pulled updates, upgrades, version details of eScan, etc.

Reports

Allows you to configure, view and mail Reports related to eScan activity in the eScan network:

Configure Reports Mailing: Specify e-mails Ids of persons sending and receiving reports, their IP address and time at which reports are mailed.

View Reports: Allows you to view reports generated by eServ.

Mail Reports: Select the link to immediately e-mail reports.

Delete: Delete selected report.

Delete All: Delete all reports.

Refresh User: Displays fresh activity details for the selected user.

Refresh All: Displays fresh activity details for all users in the eScan network.

Task Shortcut Buttons: These menus allow you to perform specific tasks. The main tasks are listed below.

eScan Management Console Launches the eScan Management Console (Available for eScan PRO and Corporate only).

Start/Stop Announcement Starts and stops announcement mechanism of eServ. (Available for eScan PRO and Corporate only).

Configure Report Mailing Configure settings to auto e-mail log reports of eServ (Available for eScan PRO and Corporate only).

Mail Reports Now Immediately mail selected report in eServ (Available for eScan PRO and Corporate only).

View Report	View selected report (Available for eScan PRO and Corporate only).
Delete	Delete user log reports (Available for eScan PRO and Corporate only).
Delete All User Logs	Delete all user logs (Available for eScan PRO and Corporate only).
Deploy License	Deploy license keys to all clients using eServ (Available for eScan PRO and Corporate only).
Refresh User	View updated settings for a user (Available for eScan PRO and Corporate only).
Refresh All	View updated settings for all users (Available for eScan PRO and Corporate only).
Shutdown Management Console	Shuts down eServ (Available for eScan PRO and Corporate only).
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.

Other components are explained below:

Screen Component	**Function**
Selected Task	Selected task name is displayed here. You will be performing functions related to this task. The screen and its related features are displayed in the application window.
Tip Bar	When you rest the cursor over an icon or task the software shows you a related tip.

Your PC directory tree

Displays the directory tree of your PC

Application Window

Displays screen of selected task. This is the work area and you perform related tasks in this area.

Application Status Bar

After the software is installed it is always active and working in the background. Various icons of the related running tasks, are displayed here. Select the icon to open the task.

In this example, the Monitor icon has a yellow spot. The **yellow spot** means that a **virus is detected** on your system.

Action Buttons

These enable you to perform tasks and carry out work related to a feature. You select preset values or ask the software to accept a value, which is used to run the application. Some of the action buttons appear on a few screens and dialog boxes. This section provides information about these buttons and explains their significance and use. Detailed explanation is provided in the section where they occur.

Action Button **Function**

Check Box

Allows you to select a function of the screen. There are two parts: on the left is the check box and on the right is the function it performs. To begin with the box is blank. To enable the function, click in the check box. A ✓ symbol appears in the check box meaning that you have selected the function shown on the right side. To deselect, click again in the box and the symbol disappears. MicroWorld assigns certain default selections and some of the check boxes are enabled when you start the application.

Some check boxes are enabled after other check boxes, radio buttons etc are selected.

Radio Button

Allow you to select a function of feature. There are two parts: on the left is the radio button and on the right is the function it performs. To begin with the button is blank. To enable the function, click on the radio button. A • symbol appears in the radio button meaning that you have selected the function shown on the right side. To deselect, click again on the box and the symbol disappears.

Some radio buttons are enabled after other check boxes, radio buttons etc are selected.

Dropdown list box

The field has two parts. Label on left/right side tells you what the function does. Box on the right has preset values hard coded by Micro World. You can assign only one of them. To assign a value, select the arrow to view the list and choose on of them.

Selection Button

✓

In some screens, when you move the mouse over the menu tree, the cursor changes to ✓. You can drop the symbol over a file or folder and set it up for additional actions. To deselect, move the cursor over the object and click.

Browse

Allows you to browse your PC for a file or folder. It also opens a new dialog box.

Provides statistics of checked, infected files etc. Select the button to open the “Monitor Statistics” box where information is listed in the non-editable display fields.

Exclude any file or folder from being scanned. Select the button to open the “Monitor Excludes” dialog box. Make suitable selections and select OK.

Performs configure related tasks. Select the button to open a dialog box. Make selections and close the box.

After you make changes or new selections in a screen, this button is enabled. Select it to apply the changes.

After you make changes or new selections in a screen, this button is enabled. Select it to discard the changes.

Allows you to make advanced settings. Select the button to open a new dialog box.

Allows you to select files or folders and set them up for further action. A new dialog box is displayed and you make your selection in it.

Add selections to the screen or dialog box.

Change selections made in the screen or dialog boxes.

Delete selections made in the screen or dialog box.

Select to accept all changes done in a dialog box or screen

Select to cancel changes made to a dialog box or screen

Select to load sample files created by Micro World.

Entering Values

The user interface is typically point and click. You select preset values in the form of radio buttons; check boxes etc in almost all areas and screens. Values need to be entered in a few screens or dialog boxes. You enter values in fields. This section provides details about different fields and how to enter values for them. .

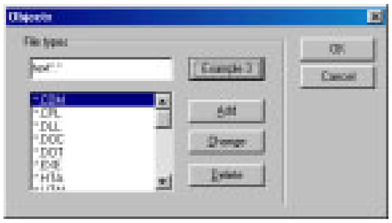
Field Type	Function
Editable Fields 	Fields where you enter valid values. To enter the value, click in the field and type. These fields can be mandatory, where in a value must be entered or they can be optional, wherein entry may be skipped. MicroWorld recommends that all fields be validated. The software does not accept invalid entries and gives an error message.
Non-editable display fields 	Values for these fields are extracted from the records and displayed here. They are read-only and cannot be edited. In this guide, such fields may be identified by the sentence "This is a non-editable display field".

Dialog Boxes

These are provided in a screen and offer a range of selections or choices. They are further linked to other features of different screens. Dialog boxes are displayed when specific buttons or selections are made. They may have radio buttons, check boxes, drop down list boxes, fields, etc. You upload information using these features. Following table shows a typical dialog box. The dialog boxes are explained in greater detail in screens where they occur.

Value Entry Dialog box

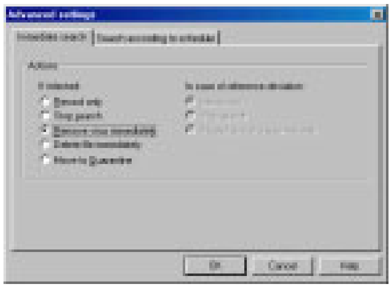
This type of dialog box has a field where values are entered; a drop-down list box where preset values are selected and action buttons to enable or disable selections



Tab Pages

Tab pages are nested in a dialog box or screen. They are displayed when an action button or fields are selected. These perform tasks related to the main task. They may have various components like action buttons, radio buttons, fields, etc., and may have further links. The tab page is identified by a name that appears on the header area of a dialog box. To open a tab page, select the relevant tab page. Following table shows a typical dialog box with tab pages. The tab pages are explained in greater detail in screens where they occur.

Tab Page


Advanced settings
Immediate search
Search according to schedule
Actions
If infected
○ Record only
○ Stop search
● Remove virus immediately
○ Delete file immediately
○ Move to Quarantine
In case of reference deviation
OK
Cancel
Help

This type of dialog box has tab pages. Each tab page may have a screen with radio buttons; check boxes etc., where values are uploaded. Make the appropriate selections and select the relevant action button.

eScan Management Console

This chapter gives details of different features of eServ and gives information of all tasks provided in Services and Report menu.

Note:
eScan Management Console feature is **only available** for **eScan Corporate**.

The chapter is for **system administrators** and other **qualified** personnel.

Topics in eScan Management Console

The chapter provides information about the following topics:

- Important Terms of eServ
- How to use eServ
- To launch eServ
- Services
- Start Stop Announcement
- Host Configuration
- Get status of eScan Installation
- Get Client status by IP
- Deploy Upgrade
- Deploy License
- Deploy Rule-Sets
- Shutdown Management Console
- Connection Errors
- Reports
- Configure Reports Mailing
- View Reports
- Mail Reports Now
- Other Report Menus

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 and 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 10.2 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.

Important Tasks

The following tasks are described in this section:

- To detect Infected Client
- Get Client Status by IP
- Host Configuration

- Announcements of eServ
- Connection Errors
    - Unsupported OS - Error 4000
    - Logon Failure - Error 1326

Left Pane

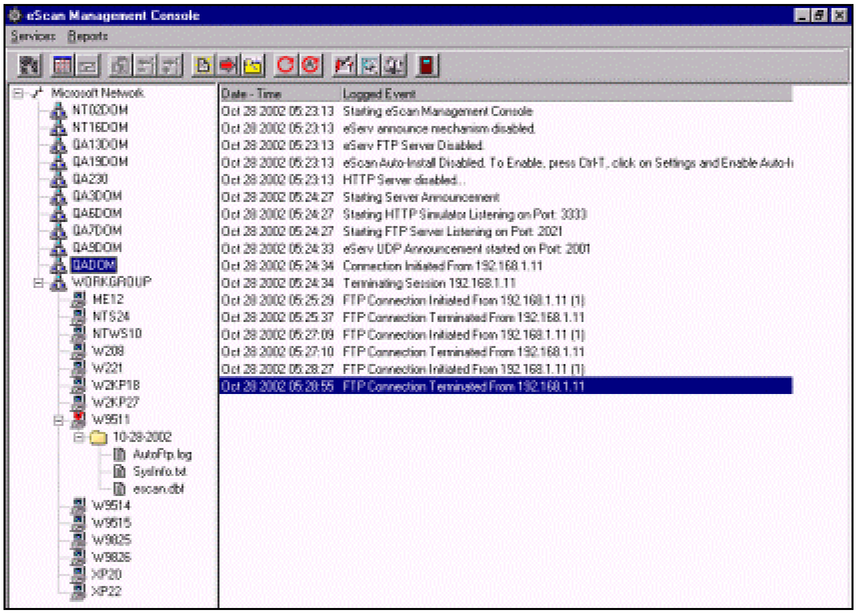
To detect which client is infected

A tree showing the computers and information for a date are displayed. The list of computers shown on the left-hand side will either be in blue or red color. **Red** indicates that some virus was reported on this computer. Blue indicates that the machine is virus free. There are typically four types of files displayed. Double click on the item to view its details. A brief description is listed below:

SysInfo.txt: Displays client system related information.

AutoFtp.log: Displays log file of auto ftp activity of the client.

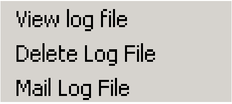
escan.dbf: Displays escan.dbf file of eScan client.



```
Date - Time           Logged Event
Oct 28 2002 05:23:13  Starting eScan Management Console
Oct 28 2002 05:23:13  eServ announce mechanism disabled.
Oct 28 2002 05:23:13  eServ FTP Server Disabled.
Oct 28 2002 05:23:13  eScan Auto-Install Disabled. To Enable, press Ctrl-T, click on Settings and Enable Auto-I
Oct 28 2002 05:23:13  HTTP Server disabled...
Oct 28 2002 05:24:27  Starting Server Announcement
Oct 28 2002 05:24:27  Starting HTTP Simulator Listening on Port: 3333
Oct 28 2002 05:24:27  Starting FTP Server Listening on Port: 2021
Oct 28 2002 05:24:33  eServ UDP Announcement started on Port: 2001
Oct 28 2002 05:24:34  Connection Initiated From 192.168.1.11
Oct 28 2002 05:24:34  Terminating Session 192.168.1.11
Oct 28 2002 05:25:29  FTP Connection Initiated From 192.168.1.11 (1)
Oct 28 2002 05:25:37  FTP Connection Terminated From 192.168.1.11
Oct 28 2002 05:27:09  FTP Connection Initiated From 192.168.1.11 (1)
Oct 28 2002 05:27:10  FTP Connection Terminated From 192.168.1.11
Oct 28 2002 05:28:27  FTP Connection Initiated From 192.168.1.11 (1)
Oct 28 2002 05:28:55  FTP Connection Terminated From 192.168.1.11
```

Figure 3.1 eScan Management Console

- 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:

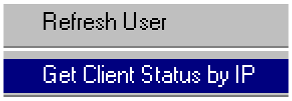


View log file: Displays details of selected log file.

Delete Log File: Deletes selected log file

Mail Log File: eScan connects to your default mail service. You can mail the log file to recipients.

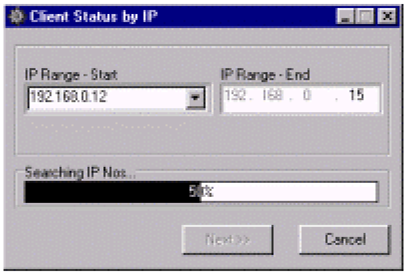
- When you right click on a Client the following popup is displayed.



Refresh User: Displays latest information for the selected user.

Get Client Status by IP

- Displays the "**Client Status by IP**" dialog box. 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 >>**.



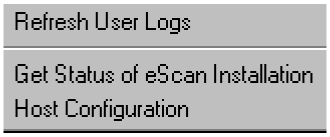
IP Range - Start: 192.168.0.12

IP Range - End: 192 . 168 . 0 . 15

Searching IP Nos..: 50%

- Further details are explained in Get Client Status by IP and Get Status of eScan Installation.

- In the left pane, when you right click on a client, the following dropdown is displayed. Click on the link to perform its task. Meanings of each link is given below:

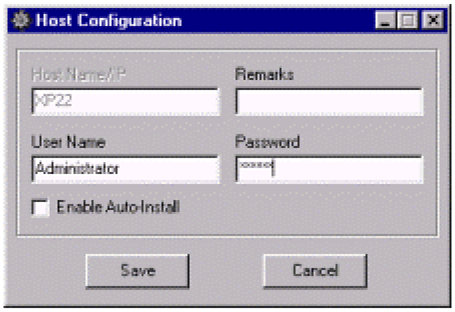


Refresh user Displays updated and fresh information for the selected Client.

Get Status of eScan Installation Allows you to get Status of eScan Installation for a client as explained in Get Client Status by IP.

Host Configuration

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:



Host Configuration

Host Name/IP: XP22

Remarks:

User Name: Administrator

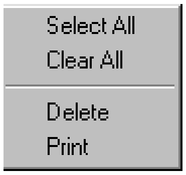
Password: *****

□ Enable Auto-Install

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**. Details are explained in Host Configuration.

Announcements of eServ.

- **Right Pane** Displays announcements made by the server. 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: 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

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. This chapter provides information to navigate to the relevant screens, validate fields and run the tasks.

- Start Stop Announcement
- Host Configuration

- Get status of eScan Installation
- Get Client status by IP
- Deploy Upgrade
- Deploy License
- Deploy Rule-Sets
- Shutdown Management Console
- 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 3.1, 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.

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.

Related Topics

What eServ does.

To enable hidden shared folders on Win NT/2000/XP Clients

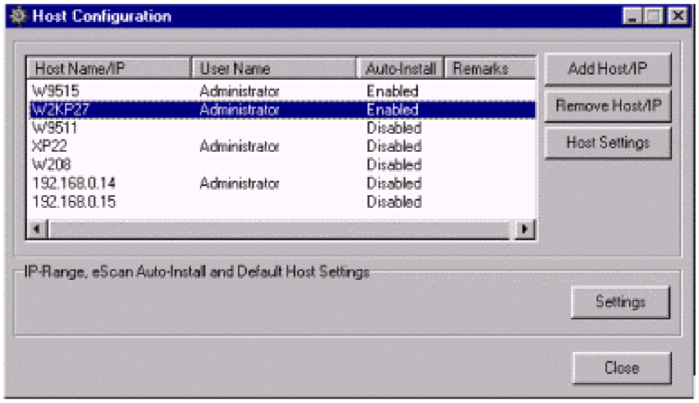
To enable Remote Install Settings on win 95/98/ME Clients

Important Topics

- To Add Host/IP
- To configure eScan install
- eScan Install Options

To launch Host Configuration

- In Figure 3.1, select Remote Install Settings or select . from the tool bar.
- Screen in Figure 3.2 is displayed.
- Existing host name, user name, flag denoting if Auto-Install is enabled and remarks are displayed in the non-editable display fields.



Host Name/IP	User Name	Auto-Install	Remarks
W9515	Administrator	Enabled	
W2KP27	Administrator	Enabled	
W9511		Disabled	
XP22	Administrator	Disabled	
W208		Disabled	
192.168.0.14	Administrator	Disabled	
192.168.0.15		Disabled	

Figure 3.2 Host Configuration

Add IP Range

- Refer Get Client Status by IP

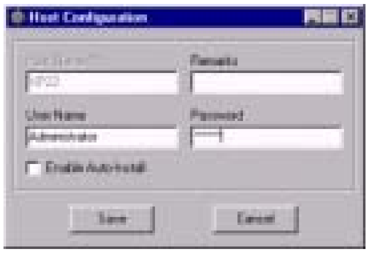
Tab Page Name **Description**

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 eScan 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 enable remote install for a selected host. Displays the dialog box explained in Host Configuration.

Settings

To configure eScan install

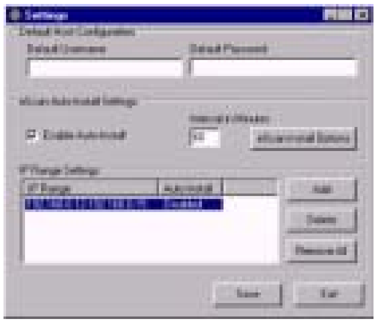
Select the button to view **Settings** dialog box shown below. You can: add host names to include them in the list for Auto Install; set the time interval after which auto install begins and set other eScan remote install options.

Default Username: Enter the default user name.

Default Password: Enter the default password.

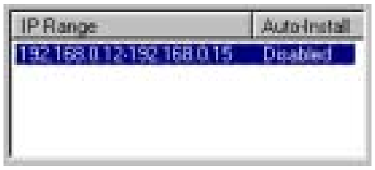
Enable Auto-Install: Select the check box to allow remote install.

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.



IP Range	Auto-Install
192.168.0.12-192.168.0.15	Disabled

The range is displayed in the list box.

eScan Install Options

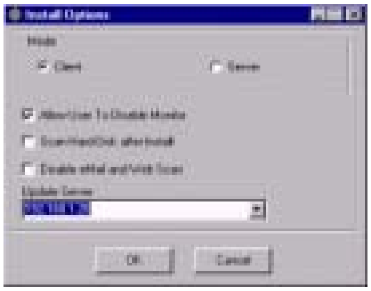
Select the button to view **Install Options** dialog box shown below. The box allows you to configure other settings for remote installation. Button is enabled only when "Enable Auto-Install" check box is selected.

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.

Allow User to Disable Monitor: Select the check box to allow clients to disable their eScan Monitor settings.

Scan Hard-Disk after Install: Select the check box to scan hard disk automatically after installation.

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.



Install Options

Mode

● Client ○ Server

☑ Allow User To Disable Monitor

□ Scan HardDisk after Install

□ Disable eMail and Web Scan

Update Server: [illegible]

Disable eMail and Web Scan: Select the check box to disable Webpage Scanning, Popup Filter and Browser Cleanup on the client's machine. Clients listed in the IP range cannot use the features on their machines. These features are available in Content Administrator.

Get Status of eScan Installation

Provides information about eScan installation details for a client.

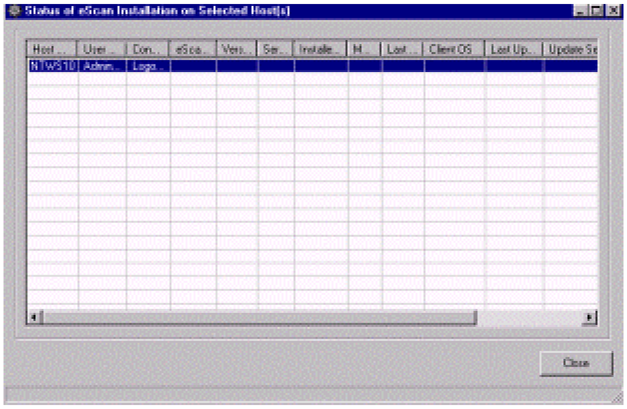
Important Topics:

- Edit Host Configuration
- Remote Install/Uninstall Software
  - To enable hidden shared folders on Win NT/2000/XP Clients
  - To enable Remote Install Settings on win 95/98/ME Clients
- Remote Uninstall eScan Software
- Change eScan Monitor Status of Selected Host
- Force Client to Download Update/Upgrade

To Launch Get Status of eScan Installation

- In Figure3.1, select the client from the left pane and choose 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.

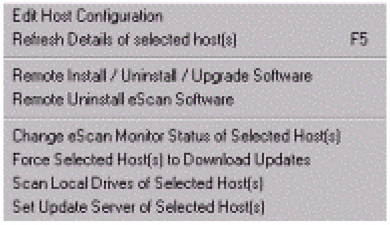


Status of eScan Installation on Selected Host(s)

Host ...	User ...	Con...	eSca...	Vers...	Ser...	Installe...	M...	Last ...	Client OS	Last Up...	Update Se
NTWS10	Admin...	Logo...									

If you double click on a client, a dialog box that allows you to configure the host, is displayed. Refer To Add Host/IP

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



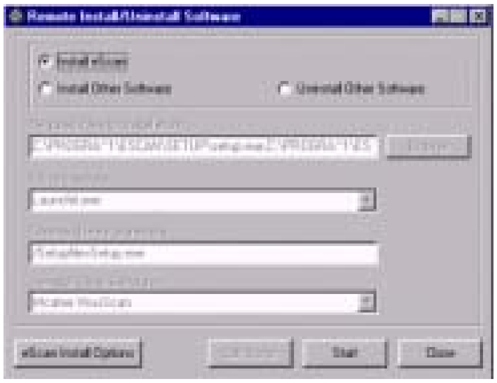
Edit Host Configuration
Refresh Details of selected host(s) F5
Remote Install / Uninstall / Upgrade Software
Remote Uninstall eScan Software
Change eScan Monitor Status of Selected Host(s)
Force Selected Host(s) to Download Updates
Scan Local Drives of Selected Host(s)
Set Update Server of Selected Host(s)

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) F5	Displays updated information about the selected host. You can also use the short cut key F5.
Remote Install/Uninstall/Upgrade Software	The button displays the **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.

Field Name **Description**

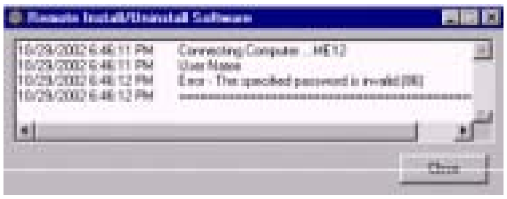
eScan Install Options: Opens the dialog box explained in eScan Install Options. Make the selections and select **Start.**

Install Other Software: Select the button if you wish to remote install other software. The following fields are enabled that allow you to: **Browse** your system for **Required files for installation**, select the **Files to Execute** and enter the **Command-line parameters**.



Uninstall Other Software: MicroWorld recommends that other Anti-Virus software be uninstalled before installing eScan. Select the radio button to **Uninstall Other Software**. Drop-down list displays the common Anti-Virus applications. Select the ones installed on your system and select **Start**.

Edit Script: Allows you to edit a script file used for the installation.



```
10/29/2002 6:46:11 PM    Connecting Computer ...ME12
10/29/2002 6:46:11 PM    User Name
10/29/2002 6:46:12 PM    Error - The specified password is invalid [86]
10/29/2002 6:46:12 PM    ************************************
```

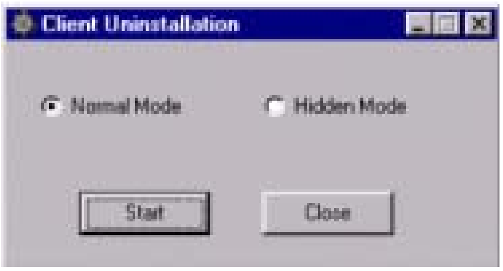
Start: After the above selections are completed, select the **Start** button. The following status box is displayed that gives the status. Select **Close** to close the box.

Remote Uninstall eScan Software

Select the button to view **Client Uninstallation** dialog box. The box allows you to Unistall eScan software on the selected client.

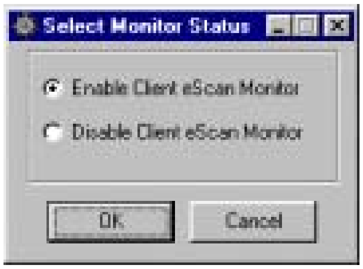
Select **Normal mode** if personnel are present to complete the uninstallation and interact with the dialog boxes. Select **Hidden Mode** if the uninstallation is unattended.

Select **Start** to begin the process.



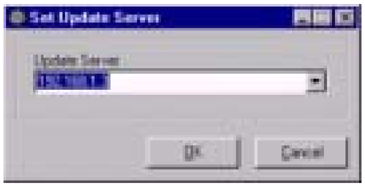
Change eScan Monitor Status of Selected Host(s)

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



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.

Field Name	Description
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.
Set Update Server of Selected Host(s)	Select the link to view **Set Update Server** dialog box. The box allows you to specify IP address of server from which the host can download updates. 

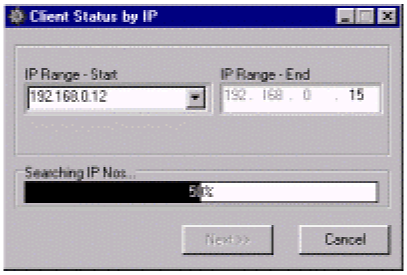
Get Client Status by IP

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 3.1, 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 >>**.



IP Range - Start: 192.168.0.12

IP Range - End: 192 . 168 . 0 . 15

Searching IP Nos...

50%

- 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

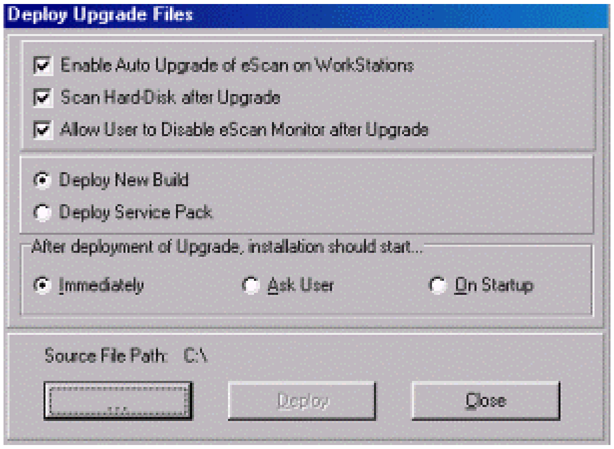
Deploy Upgrade

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:

Upgrades are new version or patches of the software or new builds, released by MicroWorld. Upgrade may carry new features or functions, all you to perform new tasks. This feature allows you to deploy Upgrades and Updates to all machines in the network from a single server. Upgrades and Updates can be deployed simultaneously on all clients.

To Launch Deploy Upgrade

- In Figure 3.1, select Deploy Upgrade or select ➡ from the tool bar.
- Screen in Figure 3.3 is displayed



Deploy Upgrade Files

☑ Enable Auto Upgrade of eScan on WorkStations
☑ Scan Hard-Disk after Upgrade
☑ Allow User to Disable eScan Monitor after Upgrade

● Deploy New Build
○ Deploy Service Pack

After deployment of Upgrade, installation should start...

● Immediately ○ Ask User ○ On Startup

Source File Path: C:\

Figure 3.3 Deploy Upgrade

Field Name	Description
Enable Auto Upgrade of eScan on WorkStations	Select the check box to allow clients to automatically download upgrades from the server as and when the server uploads upgrades.
Scan Hard- Disk after Upgrade	Select the check box to start hard disks and drives of the client's machine, after the upgrades are downloaded.
Allow User to Disable eScan Monitor after Upgrade	Select the check box to allow users to disable the eScan Monitor on their own machine. This action is not recommended.
Deploy New Build	Build are new versions of software released by MicroWorld. Select the radio button when a new build is deployed. Above three check boxes are enabled only when this radio button is selected.
Deploy Service Pack	Service packs are small patches released by MicroWorld that may cover bugs etc. Select the radio button when a new service patch is deployed.

After deployment of Upgrade, installation should start ...

Immediately When eScan client downloads the upgrade, the eServ checks if the client is already upgraded. If not, it will run the upgrade file immediately.

Ask User After clients download upgrade from the server, if this radio button is selected, the server asks them when the upgrade should be installed.

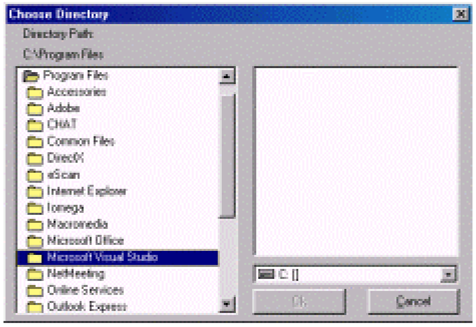
On Startup After clients download upgrade from the server, if this radio button is selected, the server installs the upgrade when the client is rebooted.

... ***To Specify location of upgrade source file***

Select the button to view **Change Directory** dialog box. The server in a specific location stores upgrades. Clients must be told, where the files are located. This allows them to download the files automatically. The box allows you to specify the path and directory where the upgrade is stored.

eScan files, searched by the Deploy Upgrade option are in the form three file: c95bxxx.exe (xxx is build number, example c95b181.exe), cntbxxx.exe and launchit.exe. The **Ok** button is only enabled when all the above three files are present in the same directory.

Browse to the required directory and select the relevant file. Select **Ok**



Directory Path:
C:\Program Files

Deploy After the fields are validated, select the button to deploy as per the selections.

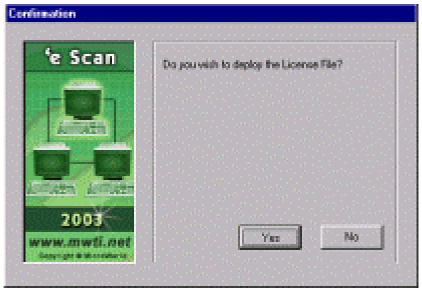
Close Closes the screen.

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

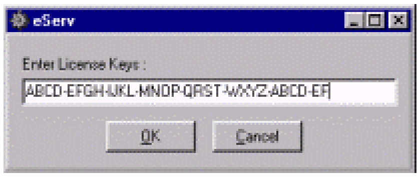
- In Figure 3.1, select **Deploy License** or click from the tool bar.
- Screen in Figure 3.4 is displayed.



Do you wish to deploy the License File?

Figure 3.4 To Deploy License Key

- Select **OK.** Screen in Figure 3.5 is displayed.



Enter License Keys : ABCD-EFGH-IJKL-MNOP-QRST-WXYZ-ABCD-EF

Figure 3.5 Enter License Key

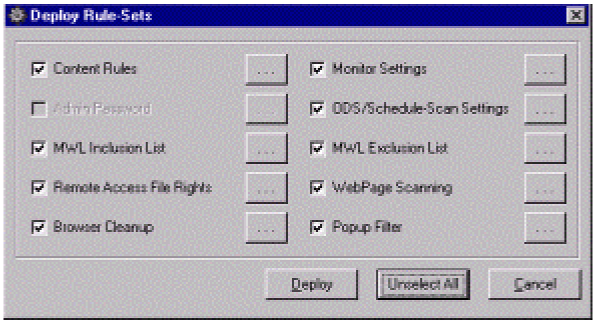
- Enter the license keys in the field and select **Ok.**

Deploy Rule-Sets

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

To Launch Deploy Rule Sets

- In Figure 3.1, select Deploy Rule sets or select from the tool bar.
- Screen in Figure 3.6 is displayed. 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** module in eScan is displayed. Make the required changes and select **Deploy**.
- You can select the button **Select All** to select all the rule sets. When selected, the button label changes to **Unselect All**



Deploy Rule-Sets

☑ Content Rules

□ Admin Password

☑ MWL Inclusion List

☑ Remote Access File Rights

☑ Browser Cleanup

☑ Monitor Settings

☑ ODS/Schedule-Scan Settings

☑ MWL Exclusion List

☑ WebPage Scanning

☑ Popup Filter

Figure 3.6 Deploy Rule-Sets

Field Name	Description
Content Rules	Select the check box to deploy content Rule-Sets. These include banned words and phrases in e-mails and actions run for them when such e-mails are detected. Please see eMail Content Scanning.
Admin Password	Select the check box to deploy eScan Content Administrator password to the eScan clients. After an eScan client downloads this rule-set, and open eScan Content Administrator, a password is asked. This password is the same as the one used to star eScan Content Administrator on eScan Server. 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.
Monitor Settings	Select the check box to deploy eServ Monitor settings on its clients. Refer Monitor System for Virus.
ODS Settings	Select the check box to deploy eScan ODS (On-Demand Scanner) settings and the Scan Scheduler settings. Refer Analyze System for Virus.
Remote Access File Rights	Select the check box to deploy Remote Access File Rights for the clients. Refer Assign Remote Access File Rights.
Browser Cleanup	Select the check box to deploy Browser Cleanup for the clients. Refer Browser Cleanup.
WebPage Scanning	Select the check box to deploy Webpage Scanning for the clients. Refer Webpage Scanning.

Popup Select the check box to deploy Popup for clients. Refer Popup Filter.

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.

Shutdown Management Console

This feature allows you to shutdown eServ.

- In Figure 3.1, 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

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**

- Process of Mailing Reports
- Configure Reports
  - To enable Report Scheduler
  - To enable mail config for e-mail of reports
  - To enable Report Scheduler
- View Reports
- Mail Reports Now
- Other Reports Menu

Configure Reports Mailing

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 3.1, select **Reports** and choose **Configure Reports Mailing** or select from the tool bar.

- Screen in Figure 3.7 is displayed.

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

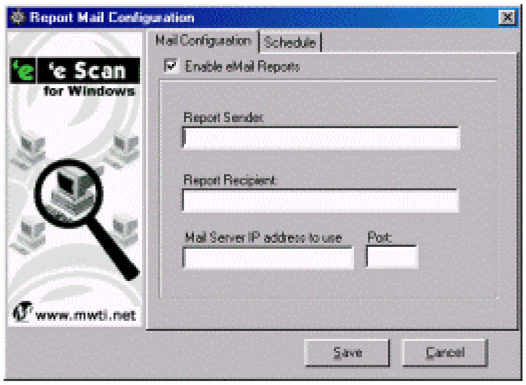
- **Mail Configuration** Allows you to specify e-mail IDs of sender, receiver, Mail Server IP address and port number.

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

Next section gives details of fields descriptions and validations.

Mail Configuration

To enable mail config for e-mail reports



☑ Enable eMail Reports

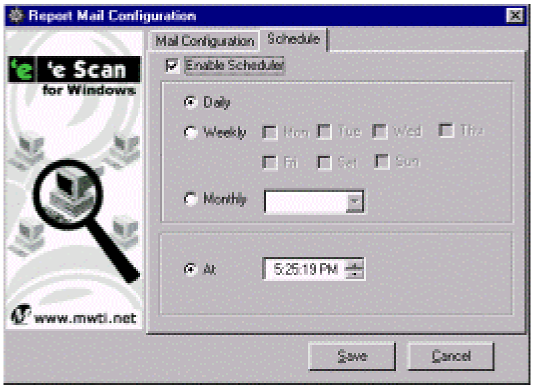
Figure 3.7 Reports Mail Configuration

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 use	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 3.8

Schedule

To enable Report Scheduler



☑ Enable Scheduler

● Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

○ Monthly

● At 5:25:19 PM

Figure 3.8 Set Report Scheduler

Field Name	Description
Enable Scheduler	Select the check box to enable the scheduler. Rest of the fields in this screen as enabled only if the check box is selected.
Daily	Select the radio button to generate reports on a daily basis.
Weekly	Select the radio button to generate reports on a weekly basis. You can select the day on which reports are generated by selecting the appropriate check box for the day.
Monthly	Select the radio button to generate reports once a month. Select the appropriate day of the month from the drop-down list. Reports are generated on this date, every month.
At	You can specify the exact time on which report is generated. Enter the time and select the suffix from the drop-down list.

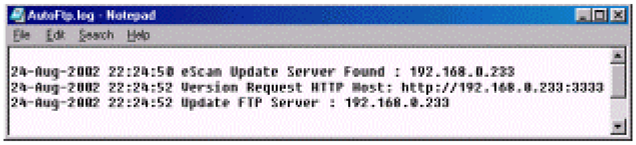
View Reports

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.

- In Reports menu, select **View Report** or select from the tool bar.

Figure in screen Figure 3.9, shows a typical report



```
24-Aug-2002 22:24:50 eScan Update Server Found : 192.168.0.233
24-Aug-2002 22:24:52 Version Request HTTP Host: http://192.168.0.233:3333
24-Aug-2002 22:24:52 Update FTP Server : 192.168.0.233
```

Figure 3.9 View Report

Mail Reports Now

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

- In Figure 3.1, 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 : Allows you to delete a logged event.

Delete All : Allows you to delete all logged events displayed in the screen.

Refresh User : Displays updated values for a client.

Refresh All : Displays updated values for all.

Frequently Asked Questions

This section gives answers to frequently asked questions.

What should I check before installing eScan Anti-Virus on Windows 95/98/ME?
You should check for the memory, i.e..., there should be a minimum of 32MB of RAM and a minimum of 100MB of hard disk space. If there is any other Anti-Virus software already installed on the machine, then uninstall it before installing eScan Anti-Virus software, as you cannot have two Anti-Virus software's, installed on the same machine.

What should I check before installing eScan on Windows NT Server & Workstation?
The service pack should be SP4 and above. If there is any other Anti-Virus software already installed on the machine, then uninstall it before installing eScan Anti-Virus software, as you cannot have two Anti-Virus software installed on the same machine.

NOTE - After installing or uninstalling any software you should restart the machine once]

After the installation of eScan, it gives an error "Unable to bind to port 2001: HTTP simulator failed".
In such a case, you should uninstall the software and then install it again. If the problem still persists, then contact the System Administrator or your Hardware Engineer. TCP/IP will have to be installed/reinstalled on the system. After TCP/IP is installed, you can proceed with the eScan installation process again.

After the installation of eScan on Windows 95/98, it gives an error "WS2_32.dll file is missing".
Let the installation process complete and then reboot the machine. If the problem still persists, then copy the two files - WS2_32.dll & WS2HELP.dll - from another Windows 95/98 computer and paste them in "c:\windows\system" of your computer. Alternatively, these two files are also available in the Windows installation CD.

After the installation is complete and the computer is restarted, the Monitor icon doesn't appear in the System Tray.
This might happen due to incomplete entries in the registry during installation. This means your installation was not done properly. Uninstall eScan and reinstall it.

After the installation is complete and the machine is restarted, the e icon doesn't appear in the System Tray.
This might happen due to incomplete entries in the registry during installation. This means your installation was not done properly. Uninstall eScan and reinstall it.

During installation, a screen pops up saying, "Your machine is infected with Boot Sector virus".

If there is any Boot Sector virus, you will have to boot your computer with a clean Windows 95/98 bootable disk and then run the DOS scanner of eScan. Please follow the steps below:

1. a:\>c:
2. c:\>cd avpdos
3. c:\avpdos>avpdos32 c: /-

eScan provides a special utility called cleanwyx.exe for WYX.b or . Boot Sector virus. You will have to boot your computer with a clean Windows 95/98 bootable disk (having cleanwyx.exe) and then run the following command from the floppy:

```
a:>cleanwyx.exe
```

If the message "Writing to hard disk successfully" appears, it means the Boot Sector virus has been removed from your hard disk.

Note - If there are any other issues or problems regarding WYX.B virus, then please write e-mail to support@mspl.net

After the installation is complete and the machine is restarted, certain applications don't seem to function.

To make the applications function, please edit c:\program files\escan95\log\tsp.log. Here you will find all the names of the EXE files of the application that are run and are giving a problem. This log file provides the entire path and the names of the EXE files.

Thereafter, edit c:\program files\escan95\exclude.dat file and add the names of the concerned EXE files of the application that are not functioning; then save this file and finally start that program. The same applies to Windows NT Server and Workstation.

Note - In case of Windows NT Server and Workstation, the path will be c:\program files\escannt\exclude.dat]

What should I do if some viruses could not be removed while scanning the computer?

This might happen because some files might be in use. To clean those file, restart the computer in MS-DOS mode and run the DOS scanner of eScan. Then follow the steps below:

```
c:\>cd avpdos
c:\avpdos>avpdos32 * /-
```

This will clean all the viruses that could not be removed from the Windows mode.

What should I do if there is cross mark on the Monitor icon?

This can happen because of two reasons, viz.:

a) either the Monitor has been disabled or

b) the License period is over (expired).

This can be rectified in two ways:

Right click on Monitor icon in the System Tray and then click on Enable eScan Monitor option. This will enable the Monitor and the cross mark will disappear.

Double click on the e icon in the System Tray and then go to the Monitor section from Task Bar (left side of the screen). There will be an option to turn the Monitor On or Off. Check the "On" option and then click on the "Apply" button and exit. This will enable the Monitor and the cross mark will disappear.

I drag the mouse pointer on the e icon and it shows "Unknown Server". What should I do?
This might happen because of two reasons:

eScan Management Console Announcement mechanism has been stopped.

eScan server is on a different network.

To rectify this, first check if eScan Management Console icon is present in the System Tray. Double click on the icon to select the Services option in order to check if the announcement is "ON".

"Stop Announcement" should be active in case the announcement is ON.

Starting the announcement should solve your problem. In case the problem still persists, then go to c:\program files\escan95 directory of the client machine and then edit eupdate.ini. Edit the following entries in the EUpdate.ini in the following sections:

[Config]

Servers=
Save the file. Right click on the e icon and click on "Exit". Then click on Start> Programs> eScan for Windows and thereafter click on eScan Client updater option. Now the e icon will be displayed in the System Tray. Just point the cursor on it to check if the TCP/IP address of the eScan server is displayed.

What should I do when the message "License period over" is displayed whenever I start the computer?
There are two different ways to enter the License key:

Right click on e icon to select eScan Content Administrator option. Once the screen appears, click on the License button on the Task Bar (left side of the screen). Then enter the License key in upper case only.

Go to c:\Program files\eScan95 directory from MS-DOS prompt to edit License.ini. Just delete the old key specified in the "Key =" section and then enter the new License key in upper case only.

Where can I check the renewal/expiry date of eScan?
Right click on e icon in the System Tray to select eScan Content Administrator option. Once the screen appears, click on the License button on the Task Bar (left side of the screen). The date when eScan has to be renewed is displayed there.

How do I know that the client machine is updated or has pulled the updates from the eScan

server?

Right click on the e icon in the System Tray to select View log files option. Further, click on View Download log to view the date, time and the list of all successfully downloaded files from the eScan server.

When I try to scan the hard disk using eScan for Windows, it displays the message "An error was found at checking the virus database: some AVC files are missing. Please call our hotline."

This might happen if some database files (AVC files) of eScan are either corrupted or not being copied properly during installation. In this case, simply download the latest eScan updates from the eScan server. This should solve the problem

How do I remove Boot Sector and macro viruses from a floppy disk?

Right click on the e icon in the System Tray to select Scan Floppy disk option. Ensure that the floppy is not write-protected before inserting it in the floppy drive. Then click on "Scan Now" button. eScan will then start the scan process to remove the viruses from the floppy disk.

What should I do if I don't see the Monitor settings menu when I right click on the Monitor icon in the System Tray?

While installing eScan the option "Should the user be given the option to DISABLE background monitoring for viruses?" is provided. If you would have clicked on the NO button during installation, the Monitor settings will be disabled.

To activate the Monitor, click on Start> Run, type the command "killmon" and finally press the Enter key. This will restart the eScan Monitor and activate it.

If I make one machine as an eScan server and it is not having an Internet connection, will it pick up the updates from the Internet?

In this scenario, you can have an Internet connection through a proxy or a dial-up modem. Else, you will not be able to download the latest virus signatures.

Once I install an eScan server, will I have to do any additional settings in eScan?

No. When you install eScan as a server, it automatically detects the settings of the proxy server. If you have a modem, it will download the updates/signature files and push these to the clients whenever you connect to the Internet.

What will happen if I disable the eScan server?

In this case, the clients will not be able to communicate with the eScan server and as a result the logs from the clients will not be uploaded to the eScan server. Likewise, the clients will not be able to pull the updates from the server.

How does a client know which is the eScan server?

eScan server has an announcement mechanism that keeps broadcasting 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.

In eScan Management Console some of the users' icons are shown in red color. What does this indicate?
This indicates that those computers have been found with infections. Therefore, you need to check the logs.

What should I do if eScan is unable to remove a new virus?
In case a new virus strikes and eScan is unable to remove it, please send a copy of the infected file to support@mspl.net (only after password protecting it in the form of a ZIP file).

Note - Under no circumstances, the virus-infected file that is detected (but cannot be disinfected) will be forwarded to the end users in your organization; it will be quarantined.

If eScan quarantines *.exe and *.com files and thereafter eScan is uninstalled, will these files get deleted?
No, these files will not get deleted.

How do I change the directory of eScan after the installation process is over?
No, you cannot move/change the directory of eScan. For this you will have to reinstall the software with the desired path.

Support

This section gives details to obtain support from MicroWorld. We offer 24-hour x 6 support to our customers through e-mail, telephone and Chat.

Chat Support

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

E-Mail support

We provide e-mail support.

- Drop us a line at support@mwti.net

Telephone Support

- ▪ We provide telephone support.
- Call us at +91 - 22 - 8265701 (5 lines)   Fax: +91 - 22 - 8304750

Our offices

MicroWorld Technologies Inc.

109, White Oak Lane, Suite # 200-P, Old Bridge, NJ 08857,

USA

Tel: (+1)-732-607 7501/02

Fax: (+1)-732-607 7503

MicroWorld Software Services Pvt Ltd.

14-A,

Pocket 2, EHS DDA Flats,

Mayur Vihar, Phase 3,

New Delhi-110096, India.

Tel Fax: (011) 2618892

MicroWorld Software Services Pvt Ltd.

Plot No. 80, Road No. 15,

MIDC - Marol, Andheri (E),

Mumbai - 400 093, **India.**

Tel: (+91-22) 8265701 - 05

Fax: (+91-22) 830 4750

For more information about our products please visit: www.mwti.net

Glossary

This section provides a glossary of terms related to our application.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Access 97 macro virus Affects MS Access 97 or later on any operating system. Written in VBA macro language.

Address Coded representation of the origin or destination of data.

AppleScript worm Is a script that uses the functionality of AppleScript to spread to other computers or scripts an email application to send itself out.

ASCII American Standard Code for Information Interchange - A seven-level code (128 possible characters) used for data transfer.

Anonymous FTP Downloading public files using the File Transfer Protocol (FTP). Called anonymous because you don't need to identify yourself before accessing files.

Attachment A file attached to an e-mail message.

Anti-Virus Software Scans computer's memory and disk drives for viruses. When it finds one, it informs you and allows you to clean, delete or quarantine files, directories or disks infected by it.

Armored Virus Tries to prevent analysis of its code.

Attack An attempt to compromise or bypass a system's security.

B

Batch file worm Affects Computers connected to a network with DOS, Windows 95/98/Me and Windows NT/2000 operating systems. Spreads by searching for shared areas on remote computers to which it can copy itself.

Bandwidth Range of frequencies passing through a given circuit. Greater the bandwidth faster is the information sent or accessed through the circuit.

Background scanning Feature in some anti-virus software to automatically scan files and documents as they are created or run.

Bit Smallest unit of information in a binary system. Represents either a one or zero ("1" or "0").

Bimodal Virus Infects boot records and files.

BIOS (Basic Input/Output System) Part of the operating system that identifies a set of programs used to boot the computer before locating the system disk. It is located in the ROM and is usually stored permanently.

Blended Threat Combines characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to attack the system. Uses multiple means to spread rapidly and cause widespread damage.

Booting Starting the computer. Booting runs various programs to check and prepare the computer for use.

Boot Sector Area on the first track of disk. Contains the boot record.

Boot Record Program in the boot sector. Contains information about characteristics and contents of the disk and booting the computer. If PC is booted with a floppy disk, the system reads the boot record from that disk.

Boot Sector Virus Places its code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus lodges itself in the PC memory and gains control over the PC. From here it spreads to other drives on the system. Once the virus is running, it usually executes the normal boot program, which it stores elsewhere on the disk.

Bugs Are not viruses but are unintentional errors in programs.

Byte A group of bits normally 8 bits in length.

C

Cavity Virus Overwrites part of its host file without increasing the file size.

Checksum Identifying number calculated from file characteristics. Any change in a file changes the checksum.

Cluster Virus Changes directory table entries. Virus starts before other programs so they may appear to infect every program on a disk. Virus code exists in one location, but running any program runs the virus.

Configure To set up a program or computer system for a particular application.

. COM Files Executable file limited to 64 KB with the extension. COM. Used by utility programs and routines. As COM files are executable, viruses can infect them.

Companion virus Renames either itself or its target file to trick the user into running the virus rather than another program. For example, a companion virus attacking a file named MOVIE.EXE may rename the target file to MOVIE.EX and create a copy of itself called MOVIE.EXE.

Corel Script virus Affects Corel SCRIPT files. Uses Corel SCRIPT macro language.

Crack To copy commercial software illegally by breaking (cracking) the various copy protection and registration techniques being used.

Client Application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

Cluster Is a logical disk-partitioning unit. A Cluster consists of one or several logical disk sectors, sequentially located. The Length of the cluster on floppy disks usually equals to 1 or 2, on hard disk - 4 or 8.

D

Daemon Pronounced demon or 'Damon'. Is a process that runs in the background and performs specified operations at predefined times or in response to certain events. Typical daemon processes include print spoolers, e-mail handlers, and other programs that perform administrative tasks for the operating system. The term comes from Greek mythology, where daemons were guardian spirits.

Denial of Service (DoS) Attack preventing normal functioning of a system. Genuine users are denied access. Hackers can cause DoS attacks by destroying or modifying data or by overloading system's servers.

Direct Action Virus Immediately loads itself into the memory, infects other files, and then unloads itself.

Distribution Measure of how quickly a threat spreads

Disassembler A utility performing transformation, reverse to assembling, i.e... transforming machine codes to assembler language. Such utilities are required not only for debugging programs but also for virus analysis.

Downloads Process of copying a file from an online service to one's own computer. Also refers to copying a file from a network file server to a computer on the network. The opposite of download is upload, which means to copy a file from your own computer to another computer.

Dropper A file created specifically to introduce a virus, worm or Trojan into a system. The file may be different type from the virus, worm or Trojan it introduces.

E

Encryption Virus Its code begins with a decryption algorithm and continues with scrambled or encrypted code. Each time it infects, it automatically encodes itself differently, so its code is never the same.

e-mail Name that identifies an electronic post office box on a network where e-mail can be sent.

e-mail Client Application that runs on a personal computer or workstation and enables you to send, receive and organize e-mail. Called a client because e-mail systems are based on client-server architecture.

Exploit Program or technique that takes advantage of vulnerability in software that can be used for breaking security or otherwise attacking a host over the network.

Excel formula virus Affects MS Excel 5 or later running on any operating system. Uses Excel formula language. When an infected document is opened the viral formula sheet is copied into a file in the XLSTART directory. This is automatically loaded into other documents when they are opened.

.EXE Files Executable file. Run by double-clicking its icon or a shortcut on the desktop, or by entering the program name at a command prompt. Are also run from other programs, batch files or various script files.

F

False Negative Error Occurs when the anti-virus software fails to indicate an infected file is really infected.

False Positive Error Occurs when the anti-virus software wrongly claims a clean file is infected. Error occur when the string chosen for a given virus signature is also present in another program.

FAT (File Allocation Table) Stores the addresses of all the files contained on a disk. In MS-DOS and Windows the FAT is located in the boot sector of the disk. Viruses and normal use can damage the FAT. If damaged or corrupt, the operating system is unable to locate files on the disk.

File Viruses Replace or attach themselves to COM and EXE files. They also infect files with extensions: SYS, RV, BIN, OVAL and COVEY. They can be resident or non-resident, the most common being resident or TSAR (terminate-and-stay-resident) viruses. Many non-resident viruses infect other files when an infected file runs.

Firewall A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the Firewall, which examines each message and blocks those that do not meet the specified security criteria. A Firewall is considered a first line of defense in protecting private information.

FTP (File Transfer Protocol) Protocol used to send files on the Internet.

G

Gateway Points of entrance and exit from a communications network. Viewed as a physical entity, a gateway is the node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture.

H

Heuristic Scanning Behavior-based analysis of a computer program by anti-virus software to identify a potential virus. Anti Virus software sends alerts when a file has suspicious code or content.

Hijack An attack where an active and legitimate session is intercepted and taken over. Remote hijacking can occur via the Internet.

Host File to which a virus attaches itself. Virus is launched when the host file is run.

Hoaxes Are not viruses, but are deliberate or unintentional e-messages, warning people about a virus or other malicious software program. They create as much trouble as viruses by causing massive amounts of unnecessary e-mail.

HTTP (Hypertext Transfer Protocol) Main protocol used by the World Wide Web. Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

I

Internet Address Also known as an IP address. Is a 32-bit hardware-independent address assigned to hosts using the TCP/IP protocol suite.

Infection Length Size of viral code inserted into a program by a virus. If it is a worm or Trojan horse the length represents the file size.

IP (Internet Protocol) Networking protocol for providing connectionless services to the higher transport protocol. It is responsible for discovering and maintaining topology information and for routing packets across homogeneous networks. Combined with TCP, it is commonly known as the TCP/IP platform.

IP Address Uniquely identifies each host on a network or Internet.

J

JavaScript virus Affects JavaScript scripting files, HTML files with embedded scripts, Microsoft Outlook and Internet Explorer.

Joke Programs These are not viruses, but may contain a virus if infected or otherwise altered.

K

Keys The Windows Registry uses keys to store computer configuration settings. When a new program is installed or the configuration settings are altered, values of these keys change. Virus modifies these keys and cause damages.

L

LAN (Local Area Network) Network that interconnects devices over a geographically small area, typically in one building or part of a building. The most popular LAN type is Ethernet, a 10 Mbps standard that works with 10BaseT, 10Base2, or 10Base5 cables.

Library File Contains groups of frequently used computer code shared by different programs. Developers use these codes to make their programs smaller. A virus infecting a library file may appear to infect any program using the library file. In Windows systems, the most common library file is the Dynamic Link Library with extension .DLL.

Linux worm Take advantage of flaws in networking code to gain unauthorized access to remote computers running Linux. They can spread rapidly between computers permanently connected to the Internet because they require no user intervention to function.

Log On To make a computer system or network recognize you so that you can begin a computer session. Most personal computers have no log-on procedure -- you just turn the machine on and begin working. For larger systems and networks, however, you usually need to enter a username and password before the computer system will allow you to execute programs.

M

Macro Set of mini programs that simplify repetitive tasks within a program such as Microsoft Word, Excel or Access. Macros run when a user opens the associated file. Viruses can infect macros.

Macintosh file virus Infect Macintosh computers.

Mailbomb Many e-mails (thousands of messages) or one large message, sent to the system to make it crash.

Master Boot Record A 340-byte program in the master boot sector. It reads the partition table, determines what partition to boot and transfers control to the program stored in the first sector of that partition. There is only one master boot record on each physical hard disk.

Master Boot Sector First sector of a hard disk located at sector 1, head 0, and track 0. Contains the master boot record.

Master Boot Sector Virus Infects the master boot sector of hard disks. They spread through the boot record of floppy disks. The virus stays in memory and infects the boot record of floppy read by DOS.

Mid infecting A prefix to denote viruses that infect the middle of a file.

Mime (Multipurpose Internet Mail Extensions) Specification for formatting non-ASCII messages so that they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

MPEG (Moving Picture Experts Group) Pronounced MPEG is a working group of ISO. Term refers to the family of digital video compression standards and file formats developed by the group. MPEG generally produces better-quality video than competing formats, such as Video for Windows, Indeo and QuickTime. MPEG files can be decoded by special hardware or software.

Multipartite Virus Infect documents, executables and boot sectors. They first become resident in system memory and then infect the boot sector of the hard drive and the entire system.

Mutating Virus Changes or mutates as it runs through its host files. Disinfection is more difficult.

MWL (MicroWorld Winsock Layer) Anti Virus and content security concept introduced and used by MicroWorld technologies Inc. MWL is placed above the Winsock layer and acts as a secure blanket between the Internet and your system. Any type of data exchanged through your system is monitored by MWL. This stops potential threats from entering your system. While other products allow threats to enter your system and then try to diffuse them, MWL technology has the key advantage of barring them from entering.

N

Network Group of computers connected to each other within an organization. Organization may be spread across a wide geographical area.

O

Operating System The underlying software that allows you to interact with the computer. It controls the computer storage, communications and task management functions. Examples: MS-DOS, MacOS, Linux, Windows 98, UNIX etc.

Overwriting Virus Copies its code over the host file's data destroying the original program. Disinfections are possible, although files cannot be recovered. It is usually necessary to delete the original file and replace it with a clean copy.

P

Payload Defines extent of damage caused by a virus.

Port Interface of a computer from where an application or physical devices connect.

Protocol Formal set of conventions governing the formatting and relative timing of message exchange between two communicating systems.

POP (Post Office Protocol) Protocol used to retrieve e-mails from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

Password Secret series of characters that enables a user to access a file, computer, or program. Password can be a combination of numbers and alphabets in a random sequence.

Polymorphic Virus Creates varied copies of itself to avoid detection from anti-virus software. Some use different encryption schemes and require different decryption routines. So the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands to mislead anti-virus software. Some use mutation-engines and random-number generators to change their virus code and decryption routine.

Program Infector Infects other program files after an infected application is run.

Q

Quarantine To move an infected file, such as a virus, into an area where it cannot cause more harm. Anti-Virus software's come with quarantine options so that the user also can keep track of virus activity.

R

Register Storage device capable of receiving and holding a number of digits

Real-time Scanner An anti-virus software application that operates as a background task. Computer continues working at normal speed.

Resident Virus Loads into memory and remains inactive until a trigger event occurs like date or time. When this event occurs the virus is activated. All boot and file viruses are of this type.

Removal Measure of skill level needed to remove the threat. The three levels are difficult (requires an experienced technician), moderate (requires some expertise), and easy (requires little or no expertise).

Rogue Program Malicious program intended to damage programs or data, or to breach system security. It includes Trojans, logic bombs, viruses etc.

S

Scalable Allows to be changed in size or configuration to suit changing conditions. For example, a scalable network can be expanded from a few nodes to thousands of nodes.

Self-encrypting Virus Conceal themselves from anti-virus programs. Most anti-virus programs attempt to find viruses by looking for certain patterns of code (known as virus signatures) that are unique to each virus. Self-encrypting viruses encrypt these text strings differently with each infection to avoid detection.

Self-garbling Virus Attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way their code is encoded so anti-virus software cannot find them. A small portion of the virus code decodes the garbled code when activated.

Signature A search pattern, often a simple string of characters or bytes, expected in every instance of a particular virus. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses.

Sparse-infector Virus Uses conditions before infecting files. Examples include files infected only on the 12th execution or files of 128kb.

Stealth Virus Conceal their presence from anti-virus software. Many stealth viruses intercept disk-access requests, so when an anti-virus application tries to read files or boot sectors to find the virus, the virus feeds the program a "clean" image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection. Stealth viruses must be running to exhibit their stealth qualities.

Subject of e-mail Indicates the subject line of the email sent by the worm.

Synchronous Transmission Transmission in which data bits are sent at a fixed rate, with the transmitter and receiver synchronized.

SMTP (Simple Mail Transfer Protocol) Protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Spam Electronic junk mail, junk newsgroup postings or unsolicited mail.

T

TCP/IP (Transmission Control Protocol/Internet Protocol) – Also known also as the Internet protocol suite. Combines both TCP and IP. Widely used applications, such as Telnet, FTP and SMTP, interface to TCP/IP.

Technical Description Describes technical details of the virus such as registry entry modifications and files that are manipulated by the virus.

Threat Assessment Gives severity rating of the threat. Includes damage that the threat causes, how quickly it can spread and how widespread the infections are known to be (wild).

Threat Containment Measure of how well current Anti virus technology can keep the threat from spreading. The measures are Easy (the threat is well-contained), Moderate (the threat is partially contained), and Difficult (the threat is not currently containable).

Time Bomb Malicious action triggered at a specific date or time.

TOM (Top of Memory) A design limit at the 640kb-mark on most PCs. Often the boot record does not completely reach top of memory, thus leaving empty space. Boot sector infectors often try to conceal themselves by hiding here. Checking the TOM value for changes can help detect a virus. The value can change for non-viral reasons also.

Trojan Destructive program that masquerades as a benign application. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

TSR (Terminate and Stay Resident) TSR programs stay in memory after being executed. Allow user to quickly switch back and forth between programs in a non-multitasking environment, such as MS-DOS. Some viruses are TSR programs that stay in memory to infect other files and program.

Tunneling Virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system actions before the OS can execute a virus. Tunneling viruses try to intercept the actions before the anti-virus software can detect the malicious code. New anti-virus programs can recognize many viruses with tunneling behavior.

U

User Name Name used to gain access to a computer system. Usernames, and often passwords, are required in multi-user systems. In most such systems, users can choose their own usernames and passwords.

UNC (Universal Naming Convention) Is the standard for naming network drives. For example, UNC directory path has the following form: \\server\microworld\\subfolder\filename.

Unix worm Takes advantage of flaws in networking code called buffer overflows to gain unauthorized access to remote computers running Unix.

V

Vaccination Technique of some anti-virus programs to store information about files in order to notify user about file changes. Internal vaccines store the information within the file itself, while external vaccines use another file to verify the original for possible changes.

Variant Modified version of a virus. Usually produced on purpose by the virus author or person amending the virus code. If changes to the original are small, most anti-virus products will also detect variants. If the changes are major, the variant may be undetected by anti-virus software.

Virus Program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus Signature A unique string of bits, or the binary pattern, of a virus. The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses. Anti-virus software uses the virus signature to scan for the presence of malicious code.

Vulnerability Characteristic of a system that will allow someone to keep it from operating correctly, or that will let unauthorized users take control of the system.

W

WAN (Wide Area Network) Network that typically spans nationwide distances and usually utilizes public telephone networks.

WinSock (Windows Socket) Is an Application Programming Interface (API) for developing Windows programs that can communicate with other machines via the TCP/IP protocol. Windows 95 and Windows NT comes with Dynamic Link Library (DLL) called winsock.dll that implements the API and acts as the glue between Windows programs and TCP/IP connections.

Wild Measures the extent to which a virus is spreading. Asses number of independent sites and systems infected, geographic distribution of infection, ability of current technology to combat the threat, and the complexity of the virus. When a virus has attacked an external system it is termed as being 'in the wild'.

Worm A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

X

XML (Extensible Markup Language) A specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Y

Yankee Doodle Type of memory resident virus. Plays the tune Yankee Doodle when activated.

Z

Zombie A computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks. The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies.

Zoo Collection of viruses used for testing by researchers.

Zoo Virus Exists in the collections of researchers.

Index