



AnyRouter Tech, TUP Software Ltd.

User's Manual

TopView 2.2



Last revised: Sept. of 2006

WWW.TUPSOFT.COM

Contents

1	INTRODUCTION	3
2	INSTALLATION PROCEDURE	5
2.1	PRE-INSTALLATION PREPARATION.....	5
2.2	INSTALLATION STEPS.....	5
2.3	REGISTERING TUPVIEW	6
3	OPERATION GUIDE	8
3.1	STARTING TUPVIEW SYSTEM.....	8
3.2	CONNECTING TO THE SERVER	10
3.3	THE MAIN INTERFACE	11
3.4	HOST INFORMATION AND ADMINISTRATION.....	11
3.4.1	<i>Managing Workgroups</i>	12
3.4.2	<i>Managing Computer Hosts</i>	13
3.4.3	<i>Exporting/Importing System Settings</i>	17
3.4.4	<i>General Filtering Settings</i>	18
3.5	OPERATOR PASSWORD	18
3.6	MONITORING OPERATIONS.....	19
3.7	LOOKING UP RUNNING RECORDS AND SYSTEM INFORMATION	22
3.8	ACTIVITY RESTRICTION	26

1 Introduction

The fusion of computer and communications technology is just bringing a radical structural transformation to the business society. The dimensions of this revolution are so vast that none can easily discern. The emergence of a new networked computerized workplace will finally fulfill the mission of information integration where the weaving together of all the computers enables every authorized employee in a company to exploit fully the resources scattered all over the information environment. TupView 2.2, the latest product developed by the Tup Software Ltd., is intended to provide a topview for a small & medium business owner/executive who is in need gaining real-time insight/control over the every detailed activity on a PC host over the whole LAN. This is an essential step forward in the process of evolving a business into an organic living entity, since it abolishes space and time, making everywhere here and anytime now, for the executive (brain) to make day-to-day decisions based on the information fed by every PC host (neuron) in real time manner, with direct and remote software and hardware management over the whole organization.

TupView 2.2 logs every meaningful action performed on a PC host to enforce acceptable-use computing and record keeping; it generates statistical reports on software and hardware uses to give a quick glance into overall resource effectiveness and employees' work habits; it is able to record, track, and play back continuously the screen activities appearing on a specific PC host for appropriate investigative operation; it restricts installation and use of computer applications and peripherals for the purposes of software compliance and data protection and security; and it automatically acquires the system information (both software and hardware) of PC hosts over the whole LAN for better management of information technology environment.

More specifically, the main functions of TupView 2.2 can be summarized as follows:

- 1) Logging activities on a PC host in real time, so you can know what the employee is doing right now.
- 2) Taking a snapshot of an active screen for further information and investigation.
- 3) Tracking down and recording continuously the screen activities at a preset time interval (default 3 seconds and 4 PC hosts simultaneously).
- 4) Recording the use of applications such as time opened and closed and the total running period, and giving statistical analysis on how effectively the application is used.

- 5) Logging window switch events so as to calculate the active time spent on an application.
- 6) Recording printing events including the user, time, file name, and total pages.
- 7) Logging in detail how a file and its content are modified by an employee.
- 8) Logging software and hardware changes such as when an application is deleted or a device removed, and listing the software and hardware installation details on a computer.
- 9) Regulating and restricting the use of applications with a preset blocking list, and enforcing through application identification, effectively preventing bypass via renaming or application modification.
- 10) Limiting the use of some hardware devices such as removable storages and CD drives for data protection.

2 Installation Procedure

This procedure provides instructions for installing a TupView system and its registration.

2.1 Pre-installation Preparation

- (1) Download the latest version of the TupView program from www.tupsoft.com.
- (2) TupView must be installed on a PC host with one of the following operation systems, i.e., Windows 2000 Pro/2000 Server/XP/2003.
- (3) The minimum requirements for the hardware are Pentium III 500 MHz (or higher) with 256 MB memory and 1GB storage. The suggested systems are:

	CPU	Memory	Free Hard Disk Space
Server (10 licenses)	Pentium IV 2.8 GHz	512 MB	20 GB
Server (100 licenses)	Pentium IV 2.8 GHz	1024 MB	40 GB
Server (>200 licenses)	Pentium IV 2.8 GHz	1024 MB	80 GB
Console	Pentium III 800 MHz or higher	512 MB	30 GB
Workstation	Pentium III 500 MHz or higher	256 MB	1 GB

2.2 Installation Steps

The TupView 2.2 package comprises three modules: the server, console, and workstation (Agent). They are independent from each other and can be installed on the same PC or separate PC hosts. The workstation (Agent) is to be installed on the PC hosts to be monitored for collecting and forwarding data; multiple consoles can be installed on different PC hosts that are used to look up the captured data; and one local area network (LAN) must have one and only one server installed for the monitoring purposes.

Installation of a server:

- 1) Back up the data and files using **backuptool.exe** in the server installation package, if

an early version of TupView had been installed (before Ver. 2.0).

- 2) Download the newest package from www.tupsoft.com.
- 3) Double-click on the installation file and follow the instructions.
- 4) After the installation, restore the settings using the backup tool.

Installation of consoles:

- 1) Uninstall the existing console program.
- 2) Download the newest version from www.tupsoft.com
- 3) Double-click on the installation file and follow the instructions.

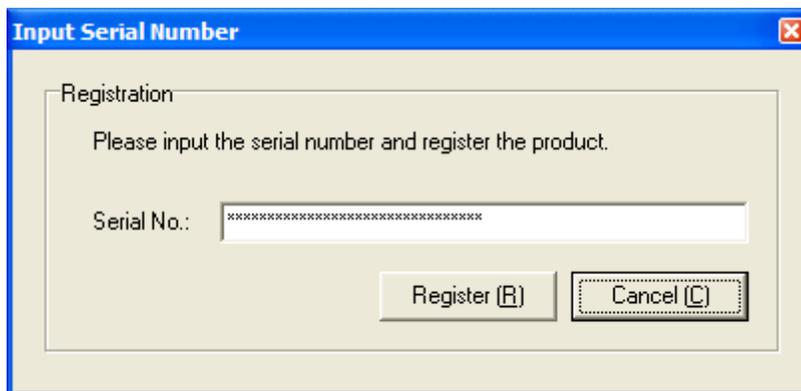
Installation of workstations:

- 1) Download the newest packages from www.tupsoft.com.
- 2) Double-click on the installation file and follow the instructions.
- 3) There is no need to uninstall the existing program on the PC host to be monitored. Rather, download the patch and then follow the instructions to upgrade on a console.

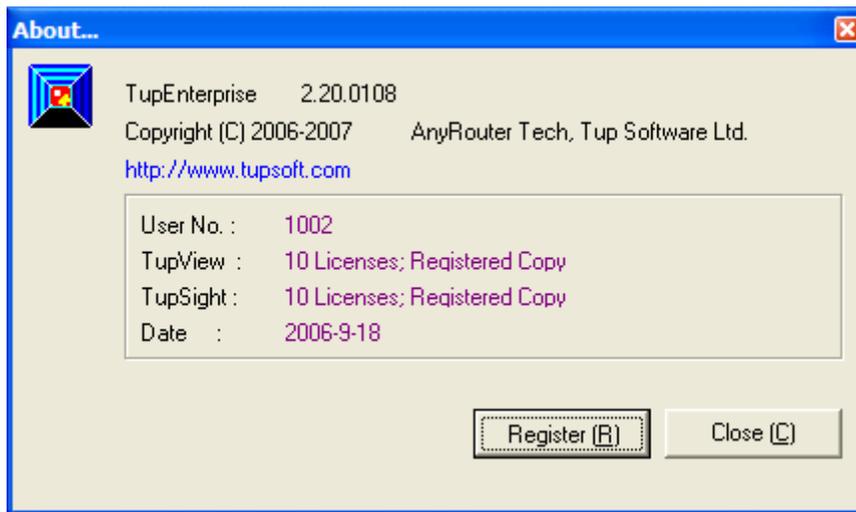
2.3 Registering TupView

After the installation, you can go ahead to register the product at www.tupsoft.com. The evaluation copy will expire in 15 days and is limited to monitoring up to 5 computers.

- 1) Connect the console to the TupView server to be registered.
- 2) Select **About** from the main menu and open **Registration**.
- 3) When the following window appears, input the serial number.



4) Press the **“Register”** button to display the license information.



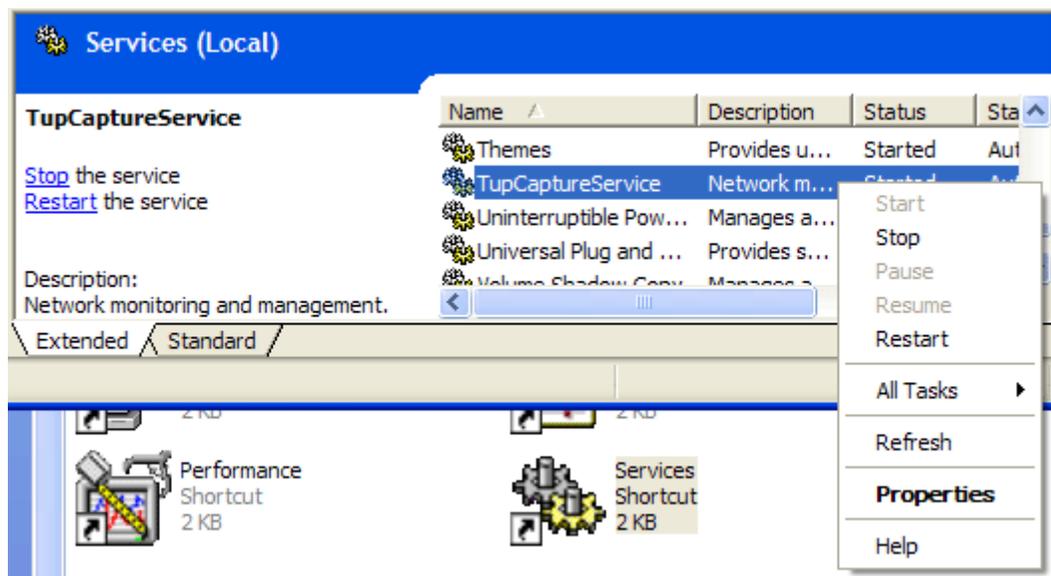
3 Operation Guide

3.1 Starting TupView System

When the host computer is turned on, the TupView server will auto-start. The TupView console can be executed at any later time you want. The server module is used to store and manipulate the configuration settings and collected data from all the workstations. On a local area network where each PC host can directly visit each other, there is only one server is needed. If there are many server modules installed on a LAN, only the one started earliest will be running and the others will be deactivated.

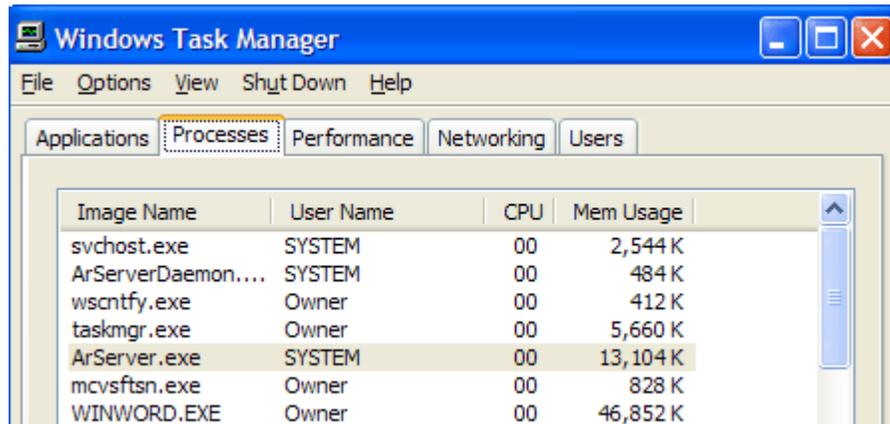
After the installation, the server will run automatically without the need for a user to intervene.

You can also manually start the server from Services in the Administrative Tools dialog from the Windows Control Panel, as shown below.



After the first running, there will be two processes shown for the TupView system inside the Windows Task Manager, i.e.,

- 1) **ArServer.exe** --- TupView Server Process
- 2) **ArServerDaemon.exe** --- TupView Server Protection Process

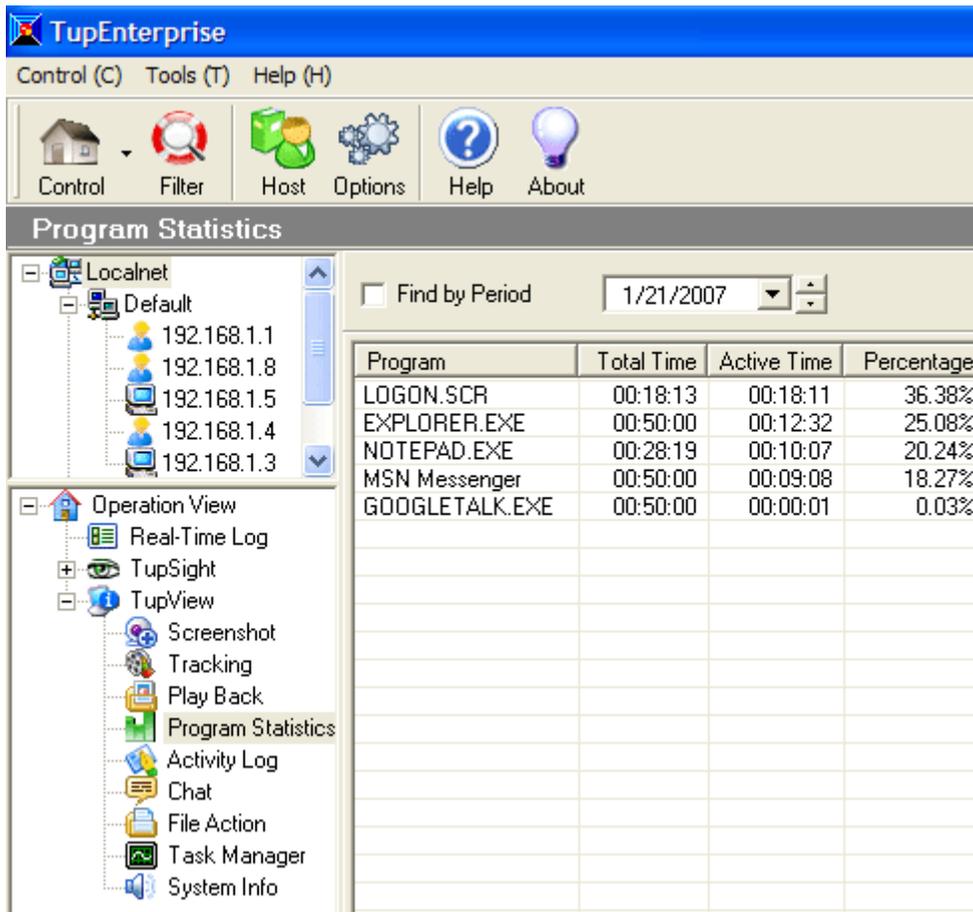


Unlike TupSight, another monitoring system also developed by Tup Software Ltd., workstation modules, called the Agents, must be installed on the PC hosts to be monitored for TupView. The installed modules are so designed that they automatically hide themselves and are highly unlikely to be detected/deleted from the PC hosts. In case that it is removed from a PC host, the console will be warned of the deletion for further action.

When a host PC is turned on, the workstation will auto-start itself and cannot be stopped manually. The main task of an agent module is to collect data and forward them to the server. It consists of the application running information, network data, file action, printer activity, and PC system (software and hardware) information. Since it adopts high-speed image capture, high compression storage, and efficient remote file transmission, the workstation uses very little system resources of a PC host.

An agent module can be started and stopped via the console interface (**Tools → Host → Upgrade Agent**). It can be automatically upgraded via the console ever since installed on a PC host.

The console is the operation interface of the TupView system. All the functions of TupView can be realized through the interface. To run the console, Click on **Start, All programs, Tupsoft TupView**, and select **Console**.



When the console is started, a process will be added into the Windows Task Manager:

ArConsole.exe

There will be also a TopView icon inside the Windows Toolbar, as shown below.



3.2 Connecting to the Server

- 1) After starting the TopView console, you need to connect it to the server from the following logon window. By default, the server is Local, user name Admin, and password blank (NULL).



The screenshot shows a Windows-style dialog box titled "Logon" with a blue title bar and a close button (X) in the top right corner. The dialog has a light beige background. At the top left, there is a small icon of a computer monitor and tower. To the right of the icon, the text reads "Input/select the host name/IP address for the server." Below this, there is a "Server:" label followed by a dropdown menu currently showing "Local Server". To the right of the dropdown are two buttons: "Logon (L)" and "Logoff (O)". Below the dropdown is a checkbox labeled "Internet Server" which is currently unchecked. A horizontal line separates the server selection section from the user information section. Below the line, there is a "User Name:" label followed by a text input field containing "Admin". Below that is a "Password:" label followed by a text input field which is empty. To the right of the password field, the text "(Null Default Password)" is displayed in blue. At the bottom of the dialog, there is a checkbox labeled "Save the password and auto logon" which is currently unchecked.

- 2) If the server and console are installed on different host machines, in the Server field locate/enter the IP address or hostname for the computer. The console can display IP addresses in the drop-down menu by automatically scanning the whole LAN.
- 3) Enter your user ID and password, and then click **Logon**. (If you want to logon automatically next time, also mark the box **Save the password and auto logon**).

3.3 The Main Interface

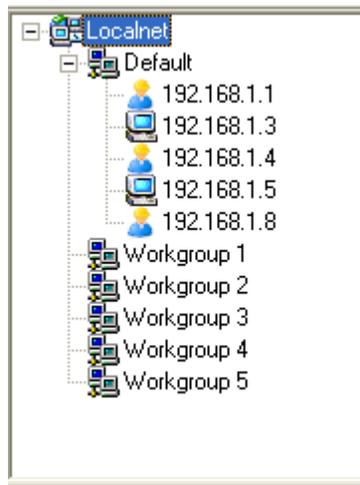
After successfully logging on the console, the main interface will look like the above shown.

3.4 Host Information and Administration

TopView's simple and straightforward administration panel makes it easy for the user to manage the data and information of hosts.

3.4.1 Managing Workgroups

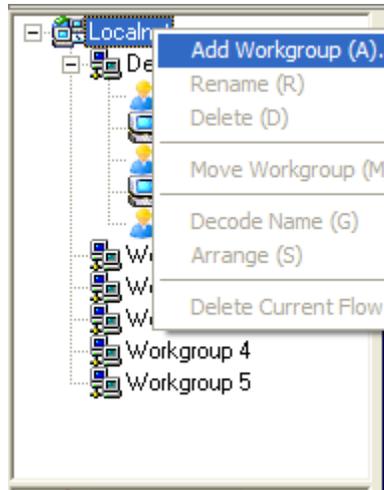
TupView simplifies the management tasks by dividing hosts into meaningful groups, and you have the flexibility to select/combine hosts into different workgroups. Initially, TupView automatically sets up a workgroup called “**Default**” containing all the hosts on the LAN, and whenever a new host is detected, it will also add that host into the “**Default**.” The console program can scan and automatically display the workgroups it has detected. To disable this auto-scan function, you can uncheck the box of “**The server will automatically scan PC hosts over the whole LAN**” through the **Host Info** interface.



1) Creating a New Workgroup

You can set up a new workgroup manually by doing the following:

1. From the host tree list area, select **Localnet** and then right-click the mouse.
2. Select **Add Workgroup**, enter a name, and click on **OK**.



2) Transferring a Host to Another Workgroup

Whenever a new host is connected to the network, the TopView console scans automatically and moves it into a workgroup where it belongs. You can also move manually a host from one workgroup to another by doing the following:

1. From the host tree list area, highlight a host (or hosts using CTRL key) and right-click the mouse to select **Move Workgroup**.
2. From the sub-menu, select the destined workgroup.

3) Deleting a Workgroup

From the host tree list area, highlight the workgroup to be deleted and click on the “**Delete**” button. When a workgroup is deleted, all the hosts inside the workgroup will be moved into the workgroup “**Default**” first. The “**Default**” is un-deletable by default.

3.4.2 Managing Computer Hosts

1) Scanning Computer Hosts

In its first running TopView will automatically scan computer hosts over the whole LAN. You can also manually scan the network by the following steps:

1. From the main menu, select **Host** and then click on the “**Scan & Renew**” button.

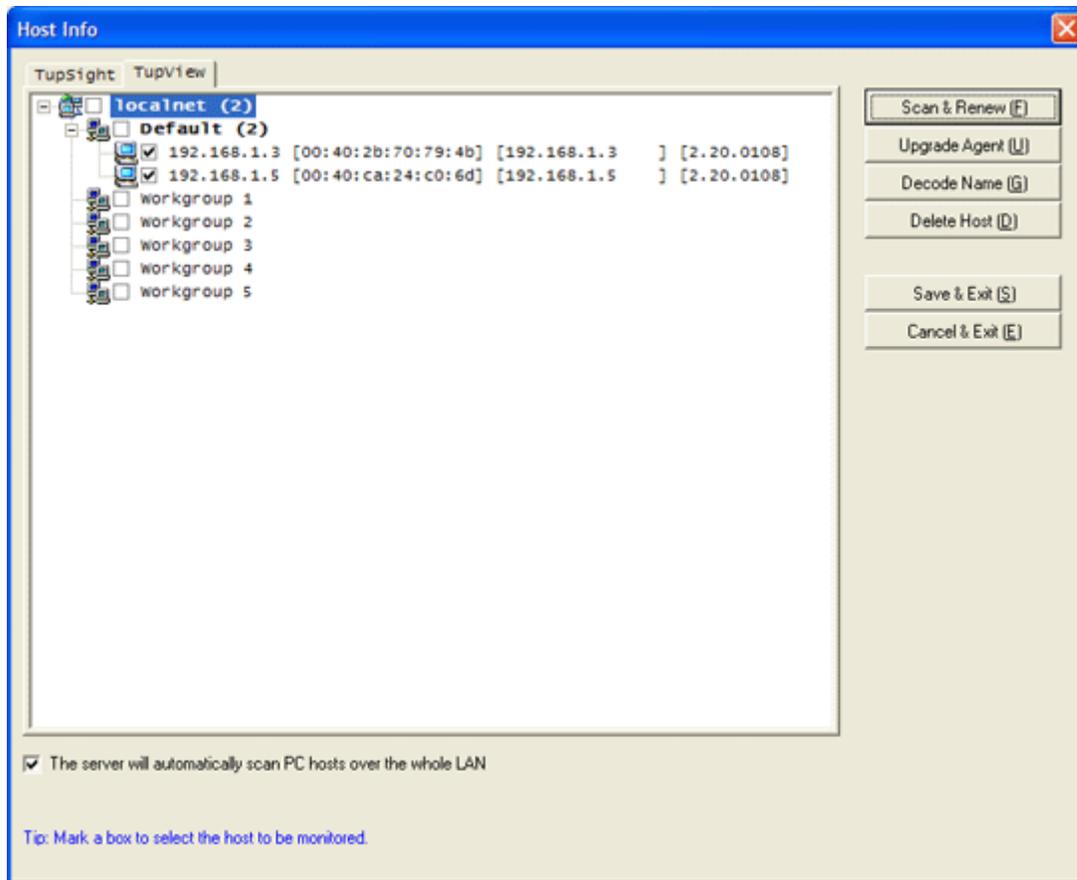
2. Input the starting and ending addresses and single-click the “**Begin**” button on the pop-up screen.
3. Select those hosts that you want to add from the scanned results and click on the “**Confirm**” button.

Alternately,

1. You can also input an IP address on the bottom of the pop-up window, and then click on the “**Acquire MAC Address**” button.
2. Input a corresponding nickname, and then click on the “**Add to List**” button.
3. If the system is unable to get the MAC address for some reasons, you can also fill in manually.

 Note: In the following cases, the computer hosts are not detectable:

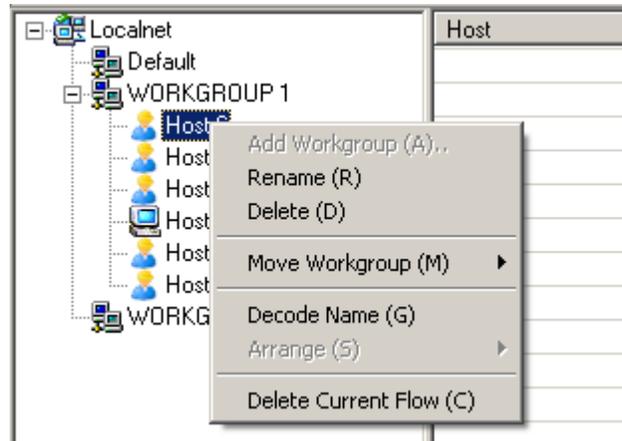
- a) The machine has been turned off.
- b) The computer is not connected to the network.
- c) The computer and the server are not on the same network segment.
- d) The firewall settings of the computer block the scanning of the server.



2) Modifying Host Information

1. Modifying Hostnames

A hostname is the computer name corresponding to a specific IP address. By default, the TupView console will automatically fetch the computer name for a host.



You can decode the hostname manually by right-clicking a host in the host tree list area and select “**Decode Name**.” You can also do that from the “**Host Info**” window by selecting the host(s) and then hit the “**Decode Name**” button.

Due to a great variety of networking infrastructures, the console might not get the name for some reasons. If this is the case, just rename the host corresponding to the IP address by right-clicking a host in the tree list area and select “**Rename**” to input a name.

2. Modifying IP addresses

When an IP address is changed for a computer host on the LAN, TupView will automatically correct the IP address on the console accordingly. This process might take about 1 min.

3. Deleting Hosts

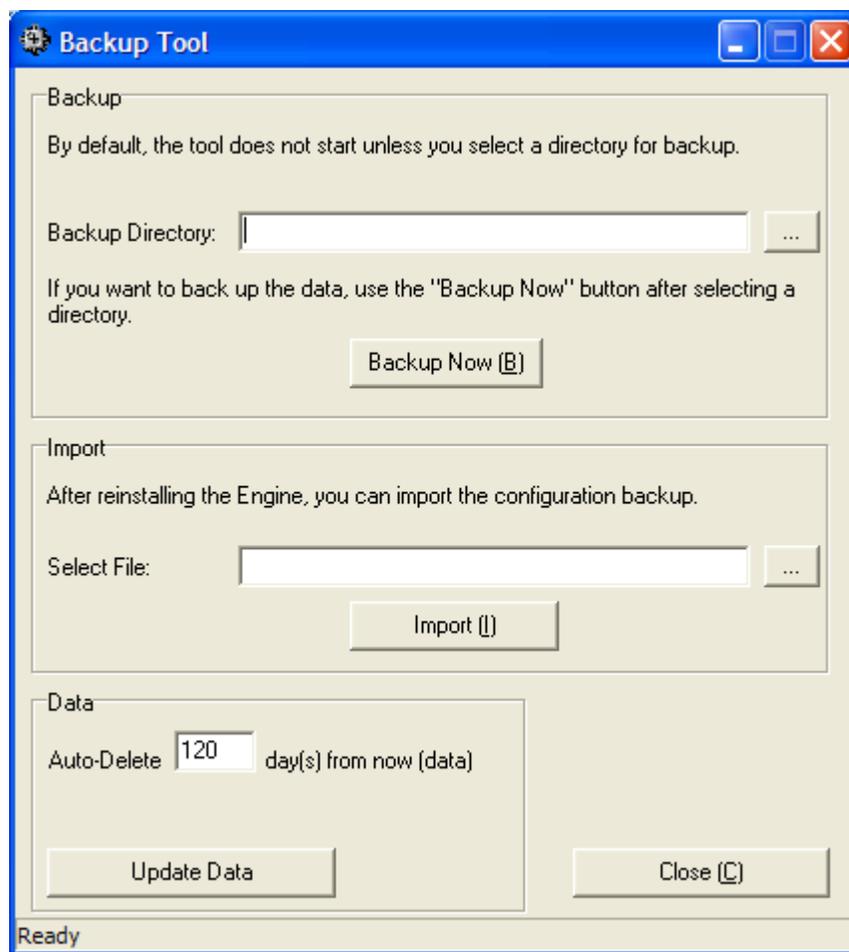
1. From the main menu, select **Tools** and then **Host**.
2. Highlight the host to be deleted and click on the “**Delete Host**” button.

When a workstation is deleted from the list, it does not mean the Agent program is uninstalled from the PC host. Rather, the program will not capture and forward data temporarily. If you want to restart the capture at a later time, you can go to **Host** to select the object to be monitored (**Tools** → **Host** → **Scan & Renew**).

3.4.3 Exporting/Importing System Settings

When upgrading the older TopView system than Ver. 2.0 (No action is required for newer ones), the system settings of the engine must be exported and then imported again. The settings contain the information of hosts and workgroups as well, and blocking and filtering configurations.

Before uninstalling the engine, the settings should be downloaded first using **Backup Tool**.

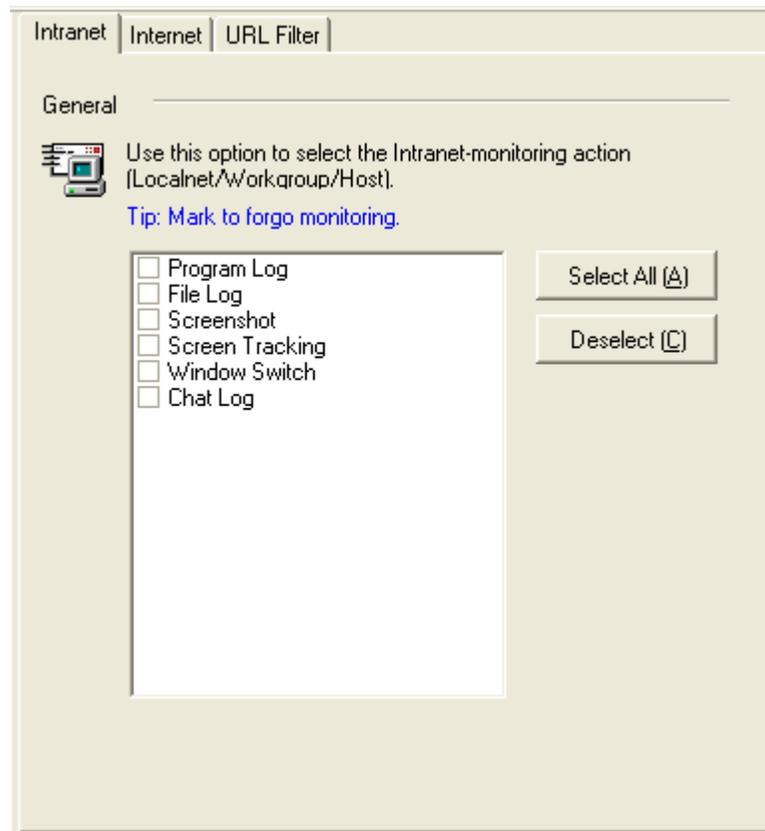


The backup action is to export data or settings from the database file **ArServer.mdb** to a backup directory. When you have set up a backup directory, the tool will automatically back up a file everyday.

To import a file into the system, you simply click the “**Import**” button on the above screen.

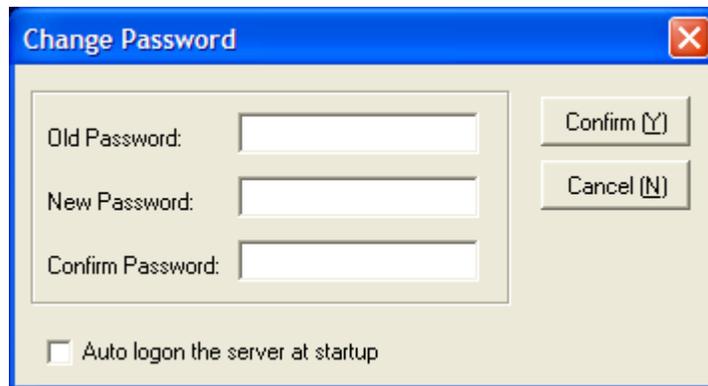
3.4.4 General Filtering Settings

By default, TopView will perform the listed operations, unless you instruct otherwise. Select the settings accordingly on the following window and then click on **Confirm**. For instance, if you are not interested in the everyday screen activities on a specific PC, checking the “**Screen Tracking**” box below will greatly reduce the burdens on both the server storage (about 15 MB per day) and the CPU of the monitored PC (to 1-2% for 512 MB memory).



3.5 Operator Password

To change the console password, from the main menu open **Tools** → **Password**, enter the old and new one and then click on the “**Confirm**” button.



3.6 Monitoring Operations

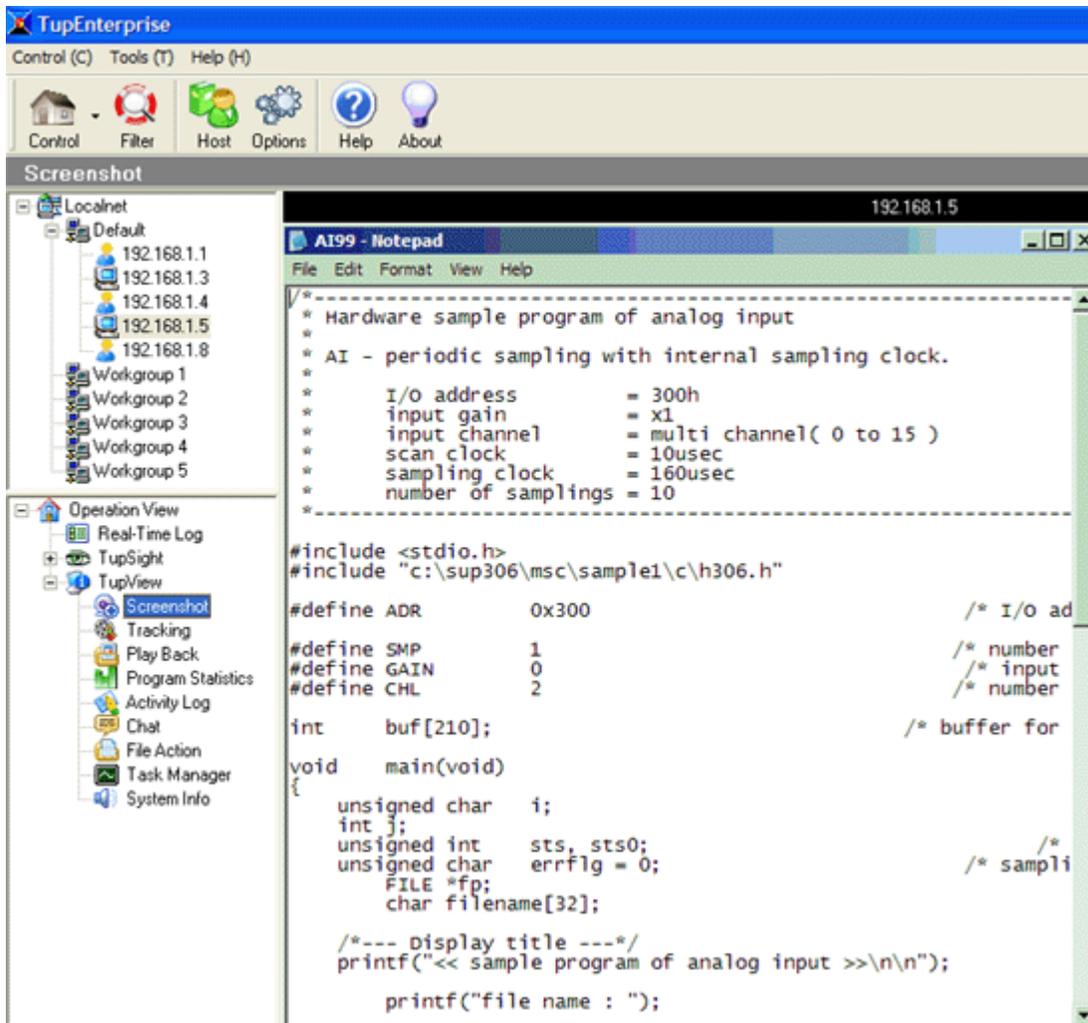
The captured data are classified into the following categories:

Real-Time Log: It displays the activities on a PC host in real time so that you can know what its operator is doing right now. The logged activities include the file action, running applications, window switch, printer events, software and hardware (un)installation, online status, FTP, and Email.

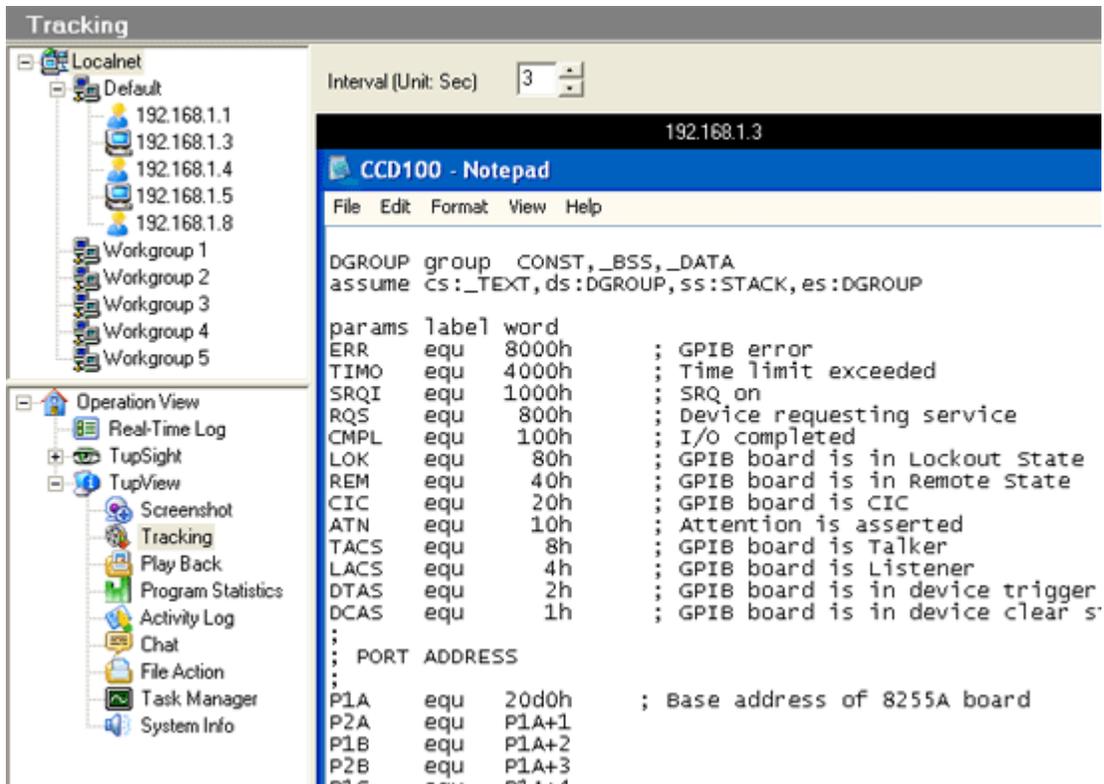
Workgroup	Host	Time	Event	Object
 Default	192.168.1.3	2007-01-21 14:40:55	Window Title	WMPLAYER.EXE
 Default	192.168.1.3	2007-01-21 14:40:53	Program Started	WMPLAYER.EXE
 Default	192.168.1.3	2007-01-21 14:40:47	Window Title	EXPLORER.EXE
 Default	192.168.1.3	2007-01-21 14:40:46	Window Title	EXPLORER.EXE
 Default	192.168.1.3	2007-01-21 14:40:35	Window Title	EXPLORER.EXE
 Default	192.168.1.5	2007-01-21 14:40:33	Window Title	MSHEARTS.EXE
 Default	192.168.1.3	2007-01-21 14:40:32	Window Title	EXPLORER.EXE
 Default	192.168.1.5	2007-01-21 14:40:30	Window Title	MSPAINTE.EXE
 Default	192.168.1.5	2007-01-21 14:40:10	Window Title	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:40:05	Window Title	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:39:32	Window Title	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:39:26	Window Title	MSPAINTE.EXE
 Default	192.168.1.5	2007-01-21 14:38:45	Program Closed	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:35	Window Title	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:35	Program Started	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:33	Window Title	EXPLORER.EXE
 Default	192.168.1.5	2007-01-21 14:38:32	Window Title	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:32	Program Started	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:30	Window Title	EXPLORER.EXE
 Default	192.168.1.5	2007-01-21 14:38:26	Window Title	MSPAINTE.EXE
 Default	192.168.1.5	2007-01-21 14:38:26	Program Closed	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:18	Window Title	MSHEARTS.EXE
 Default	192.168.1.5	2007-01-21 14:38:18	Program Started	MSHEARTS.EXE

Screen Monitoring: It consists of three parts: screenshot taking; screen tracking; and playing back the records.

1. **Screenshot Taking:** It takes a screenshot for a specific PC host at a specific time.



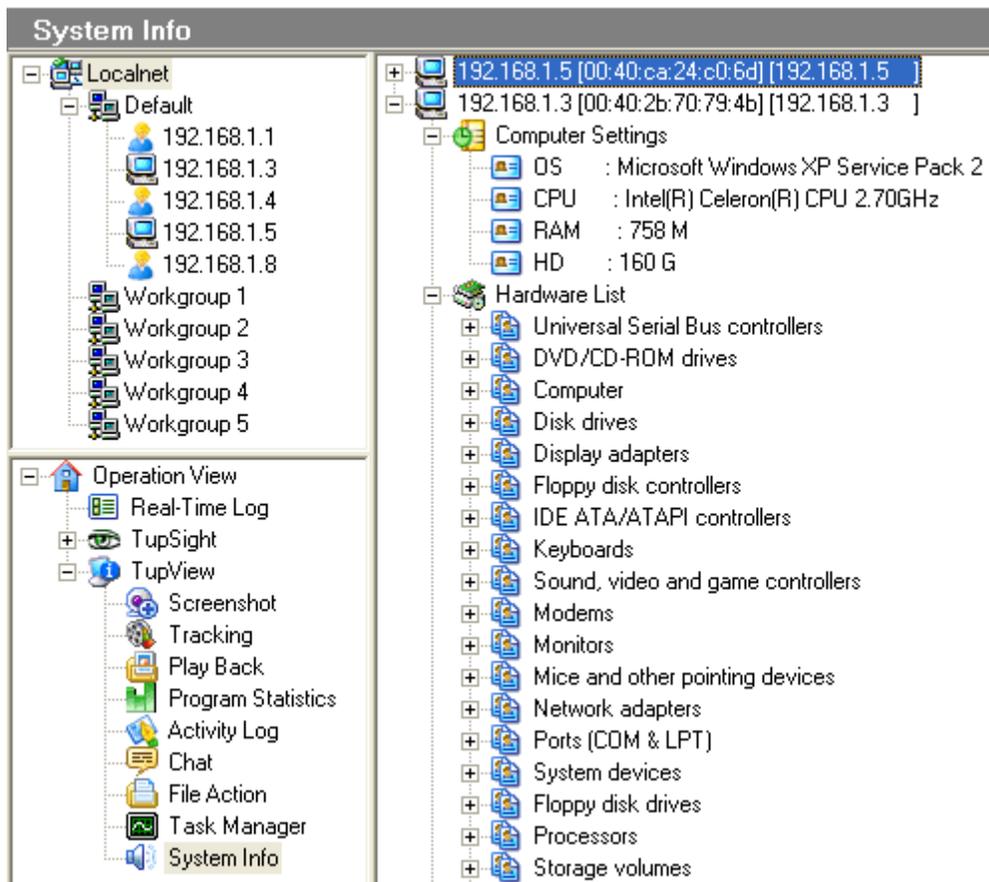
2. **Screen tracking:** It continually tracks one or more screens on the LAN at a given time interval. The tracking interval can be changed arbitrarily.



3.7 Looking Up Running Records and System Information

Printer Event: It logs the activities of both local and network printers.

System Information (Both Software and Hardware): It will remotely acquire the system information of PC hosts for better management of IT resources. When a physical device or application program is installed/uninstalled, the action will be logged in real time.



File Action: It records the creation of a new file and modification/deletion of an existent one.

Host	Operator	Time	Action	Object	Path 1
192.168.1.3	Owner	2007-01-21 12:37:04	File Created	STEP3.C	F:\ADC\STEP3.C
192.168.1.3	Owner	2007-01-21 12:37:04	File Created	STEP3.EXE	F:\ADC\STEP3.EXE
192.168.1.3	Owner	2007-01-21 12:37:05	File Created	TST3.DAT	F:\ADC\TST3.DAT
192.168.1.3	Owner	2007-01-21 12:37:05	File Created	TST4.DAT	F:\ADC\TST4.DAT
192.168.1.3	Owner	2007-01-21 12:37:05	File Created	TST5.DAT	F:\ADC\TST5.DAT
192.168.1.5	Owner	2007-01-21 14:00:13	Folder Creat...	ADC	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI1.C	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI1.OBJ	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI11.C	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI2.C	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI2.DAT	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI2.EXE	C:\Documents and Settings\Own...
192.168.1.5	Owner	2007-01-21 14:00:13	File Created	AI2.OBJ	C:\Documents and Settings\Own...

Program Statistics: It generates the statistical report of active applications.

Program Statistics

Find by Period 1/21/2007

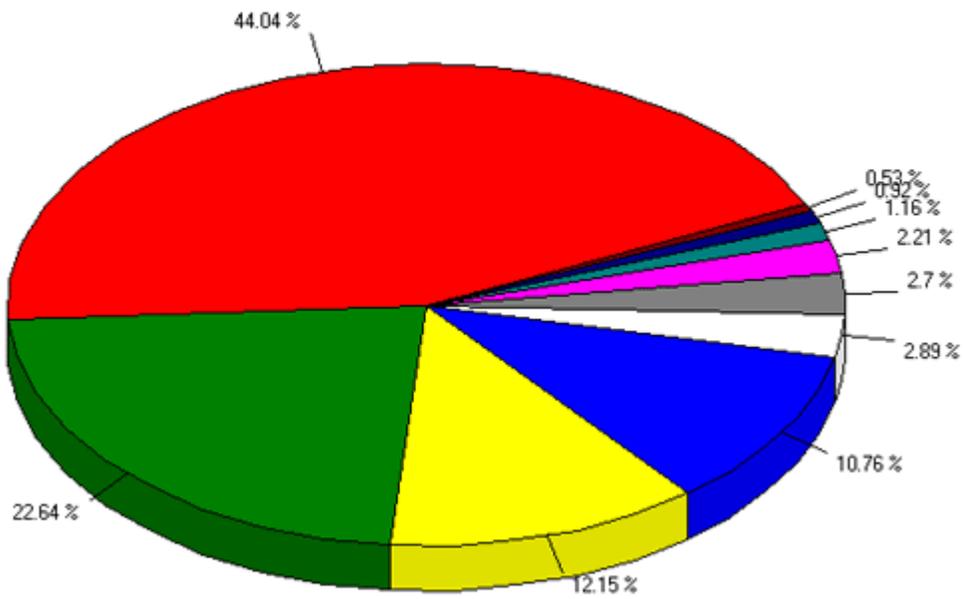
Program	Total Time	Active Time	Percentage
LOGON.SCR	02:19:15	02:19:14	43.58%
EXPLORER.EXE	05:18:00	01:11:34	22.40%
NOTEPAD.EXE	04:46:03	00:38:24	12.02%
MSPAIN.TEXE	01:07:01	00:34:01	10.65%
MSN Messenger	02:40:00	00:09:08	2.86%
Microsoft Word	00:42:12	00:08:32	2.67%
MSHEARTS.EXE	00:09:30	00:07:00	2.19%
WINMINE.EXE	00:03:42	00:03:41	1.15%
PINBALL.EXE	00:02:56	00:02:55	0.91%
Internet Explorer	00:02:09	00:01:41	0.53%
GOOGLE.TALK.EXE	02:40:00	00:01:10	0.37%
WMPLAYER.EXE	00:00:50	00:00:45	0.23%
ICQLITE.EXE	02:35:00	00:00:34	0.18%
SOL.EXE	00:00:23	00:00:23	0.12%
AIM.EXE	02:35:00	00:00:09	0.05%
AIM6.EXE	00:00:58	00:00:05	0.03%
CAVTRAY.EXE	02:35:00	00:00:04	0.02%
ACRORD32.EXE	00:00:08	00:00:03	0.02%
AUTORUN.EXE	00:00:09	00:00:03	0.02%
SPIDER.EXE	00:00:03	00:00:02	0.01%
KAMENU.EXE	00:00:02	00:00:02	0.01%
AGENTSVR.EXE	00:05:00	00:00:00	0.00%

URL Visits: It gives the percentage report of website visits.

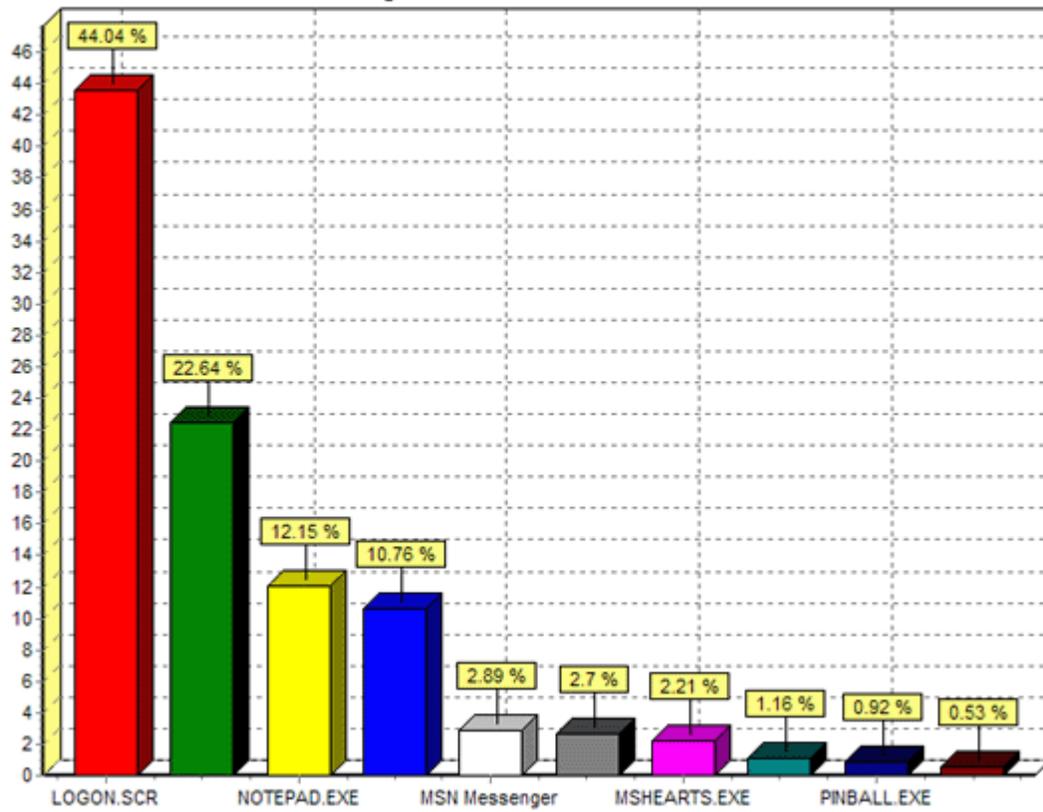
Flow Analysis: It calculates the data flow of each PC host and gives the online statistics.

Each statistical report can be shown in the form of tables, pie charts, and column graphs.

Program Statistics-Localnet



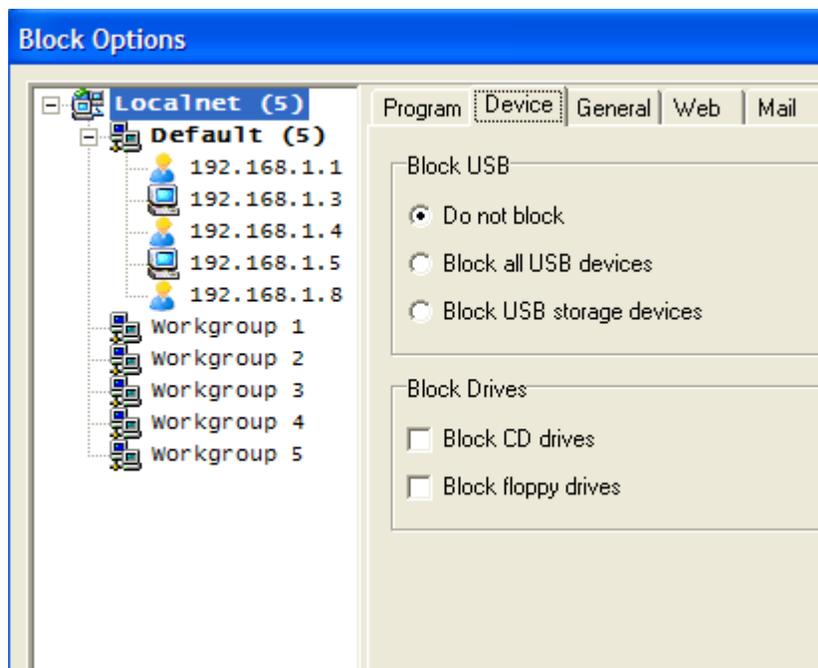
Program Statistics-Localnet



3.8 Activity Restriction

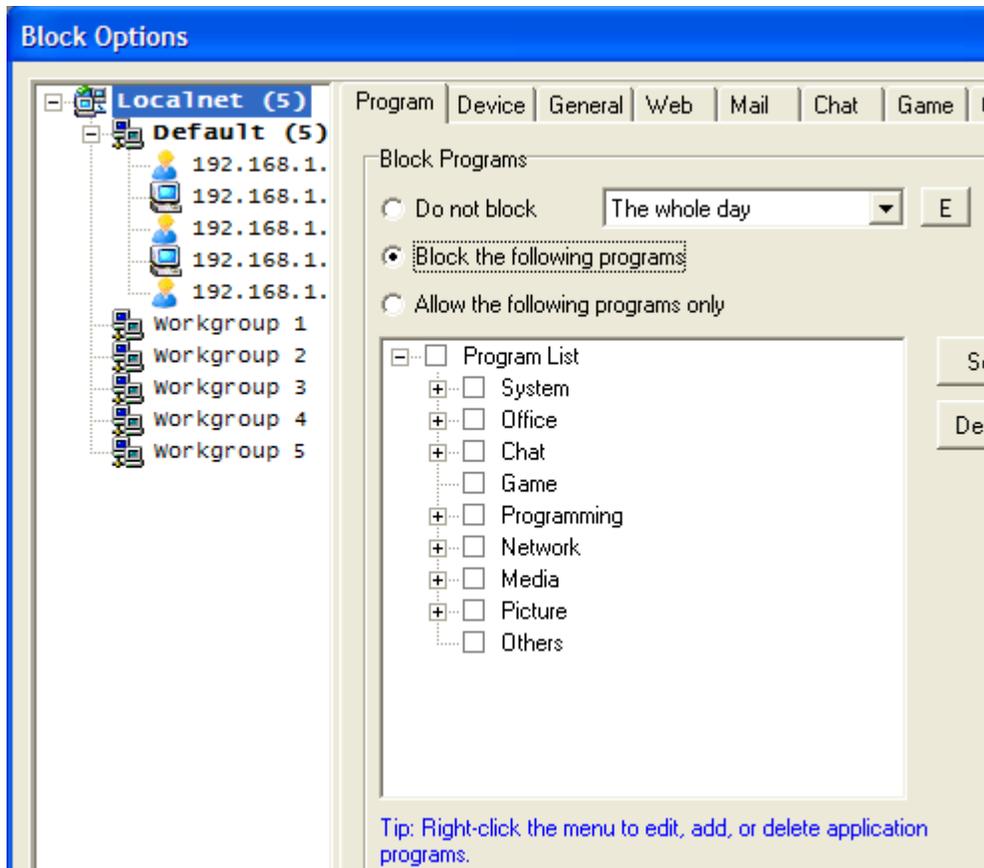
The computer activities can be limited or blocked in the following ways:

1. Blocking Programs
2. Blocking Devices
3. Limiting Data Flow
4. Blocking URLs
5. Blocking Emails
6. Blocking Ports

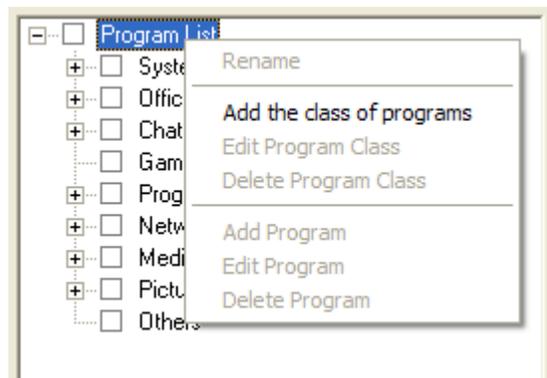


The computer can be controlled in the following ways:

1. Locking Computer
2. Unlocking Computer
3. Logging Off User
4. Restarting Computer
5. Shutting Down Computer



The class of programs can be added, deleted, or renamed.



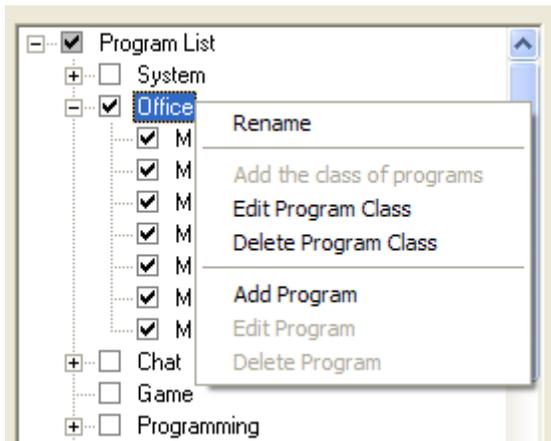
Adding Program Class: Highlight **“Program List”**, right-click the mouse, select **“Add the class of programs,”** input a name, and then hit **“OK.”**

Deleting Program Class: Highlight the class to be deleted, right-click the mouse, and select **“Delete Program Class.”**

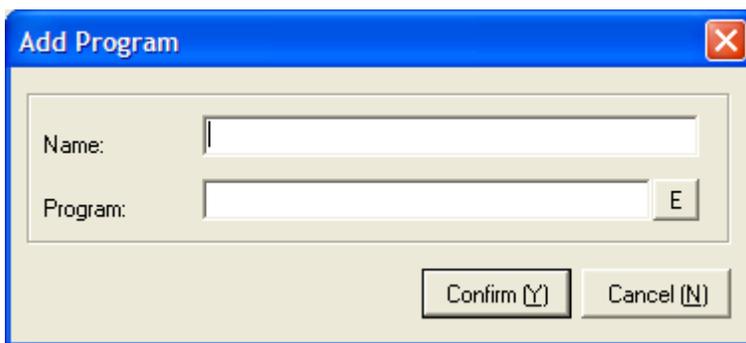
Renaming Program Class: Highlight the class to be renamed, right-click the mouse, select “Rename Program Class,” input a name, and hit “OK.”

Accordingly, the applications can be also added, deleted, and renamed.

Adding Application: Highlight the program class, right-click the mouse, and select “Add Program.”



In the pop-up window, click the “E” button to select the program.



 Note: The name of a program should not be input directly. Rather, you must browse into the corresponding program folder to select it. In this way, the system will record the characterization of the application, effectively preventing bypassing via renaming or program modification.

Deleting Application: Highlight the application to be deleted, right-click the mouse, and select "**Delete Program.**"

Renaming Application: Highlight the application to be renamed, right-click the mouse, select "**Rename Program,**" input a name, and then hit "**OK.**"