



The Cup Software Ltd.

User's Manual

TuplInsight 3.0

Last revised: July of 2005

WWW.TUPSOFT.COM

Contents

1	INSTALLATION PROCEDURE	3
1.1	PRE-INSTALLATION PREPARATION.....	3
1.2	HARDWARE PREPARATION	3
1.3	INSTALLATION STEPS	5
1.4	REGISTERING TUPINSIGHT	6
1.4.1	Upgrading to Unlimited Version	8
2	OPERATION GUIDE	9
2.1	STARTING TUPINSIGHT SYSTEM	9
2.2	CONNECTING TO THE ENGINE	11
2.3	THE MAIN INTERFACE	12
2.4	EXPORTING/IMPORTING MONITORING SETTINGS.....	14
2.5	OPERATOR ADMINISTRATION.....	15
2.6	CUSTOMIZATION.....	15
2.7	INTERNET ACCESS CONTROL.....	17
2.7.1	Restricting Web Access.....	17
2.7.2	MAC Lockup	20
2.8	HOST INFORMATION AND ADMINISTRATION.....	20
2.8.1	Managing Workgroups	20
2.8.2	Modifying Hostnames.....	22
2.8.3	Deleting Hosts.....	22
2.8.4	Exporting/Importing Host and Workgroup Information.....	22
2.8.5	Selecting Hosts to Be Monitored	23
2.9	SETTING UP SYSTEMS.....	24
2.9.1	Configuring the Server.....	24
2.9.2	Configuring the Console	26
2.9.3	Subnetting.....	27
2.9.4	Specifying Connection Ports to Be Monitored	27
2.10	MANAGING THE DATA.....	28
2.10.1	Previewing Messages	28
2.10.2	Reading Messages.....	28
2.10.3	Deleting Messages	29
2.10.4	Saving Messages	30
2.10.5	Opening/Saving Attachments	30
2.10.6	Backing Up Messages	32
2.10.7	Restoring Messages.....	32
2.10.8	Exporting Messages	33
2.11	MONITORING CHAT SESSIONS	34
2.11.1	Looking Up Chat Log Files.....	35
2.12	SEARCHING MESSAGES	35
2.13	FILTERING MESSAGES.....	37
2.13.1	General Filtering Settings.....	37
2.13.2	Filtering URLs	38
2.14	TECHNICAL SUPPORT	39

1 Installation Procedure

This procedure provides instructions for installing a TuplInsight system and configuring in its first running.

1.1 Pre-installation Preparation

- (1) Download the latest version of the TuplInsight program from www.tupsoft.com.
- (2) Select a computer host to install the TuplInsight engine. Whenever possible, the host is the one directly connected to the Internet, e.g., a proxy server. For the operation system (OS) on the host, we recommend Windows 2000.
- (3) The TuplInsight console depends on Microsoft Access Database Components (MDAC) for data access, which are a part of the Windows 98SE, Windows 2000, and Windows XP operating systems. You may need to download and install these MDAC files yourself (they are free) from www.microsoft.com if those files on your system have been damaged.
- (4) Make sure the network is functioning correctly. To check your network connectivity, you can ping a network adapter by name or IP address.
- (5) To avoid any possible conflicts, we recommend temporarily disabling the firewall, antivirus, and proxy software.

1.2 Hardware Preparation

TuplInsight is an eavesdropping program and, in principle, can be installed on any computer host on the local area network (LAN) with or without the help of a shared hub. Due to different networking technologies on each LAN, whenever possible the TuplInsight engine is always installed on the gateway machine (using NAT or proxy) so as to capture data from all the computer hosts on the local network. If the gateway device is a router rather than a computer, the engine should be installed on a host sharing the same network segment with the router.

The following three schemes show how to select a computer host for the installation, with Fig. 3 representing the most common solution.

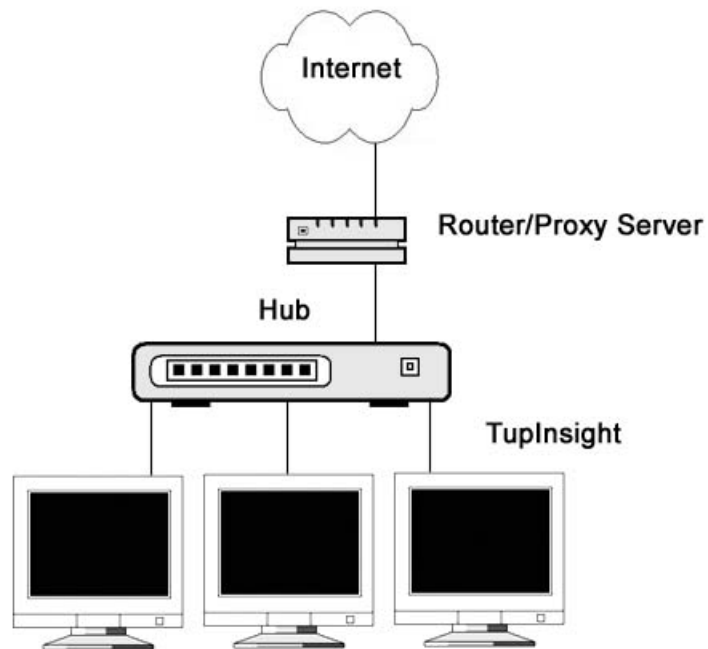


Fig.1. On a traditional shared hub-based LAN, the engine can be installed on any host machine.

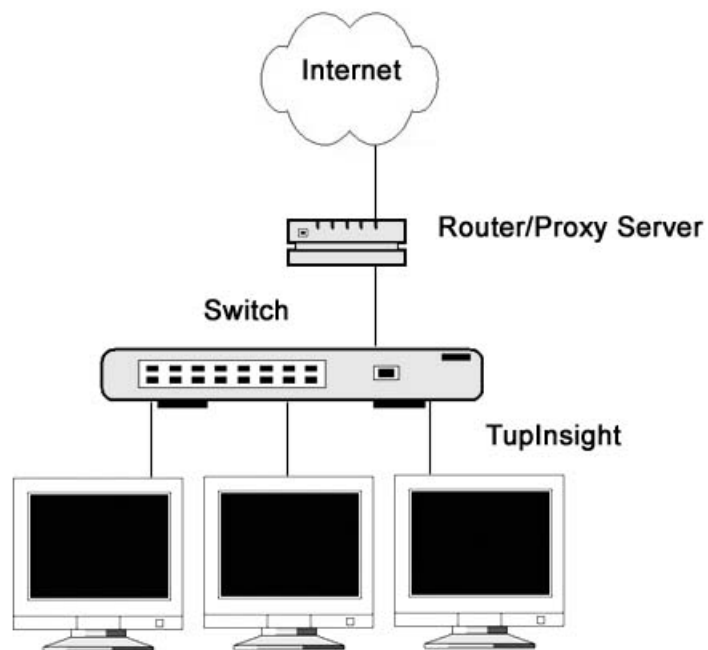


Fig. 2. On a switched LAN, the engine is installed on the gateway machine or a host connected to the "management port" of the top-level switch.

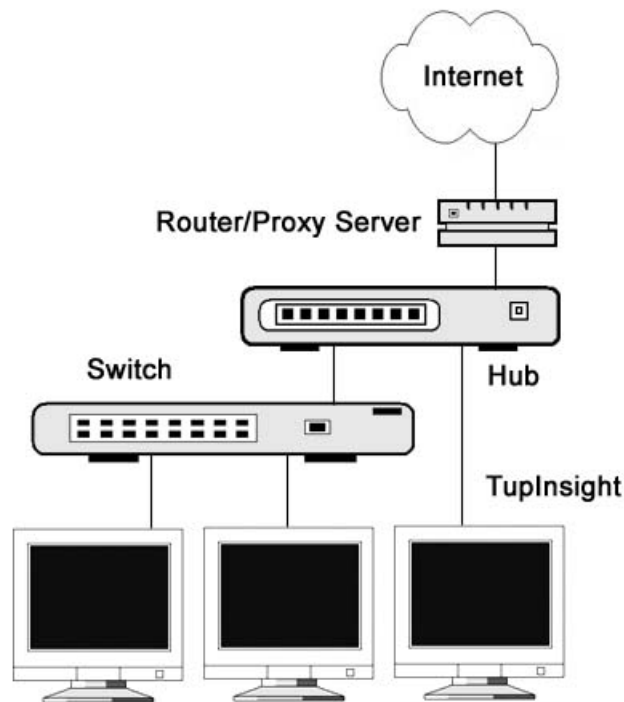


Fig. 3. The most common solution is to add a shared hub between the router and the top-level switch.

To determine the network characteristics, you can follow these steps:

- 1) Select **Computers Near Me → Properties → Local Area Connection → Properties**.
- 2) Look up TCP/IP properties to see whether there is a default gateway.
- 3) If there is an IP address to the right of the words **Default Gateway**, see whether it belongs to a router or a computer.
- 4) If that is a computer, install the TupInsight engine on this gateway machine; otherwise, place a shared hub to the nearest Ethernet port to the Internet connection, as shown in Fig. 3.
- 5) If there is no default gateway, open from the IE browser menu **Tools → Internet Options → Connections → Local Area Network (LAN) settings**, check whether your browser is using a proxy server.
- 6) If this is the case, install the engine on the proxy server and go to the TupInsight console to configure the HTTP proxy by selecting **Tools → Options → Server → Proxy**.

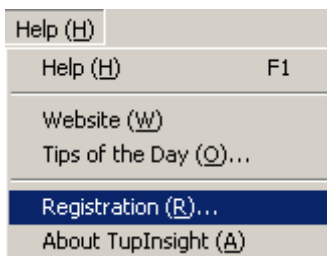
1.3 Installation Steps

- 1) Double-click on the installation file and follow the installation instructions.
- 2) The system comprises two parts, the engine and the console. They can be installed on the same computer host or separately on two different machines.
- 3) After the installation, run the TupInsight engine first and then the console for registration.
- 4) Since TupInsight is an eavesdropping program, no configuration of Outlook and/or FoxMail consoles is needed.

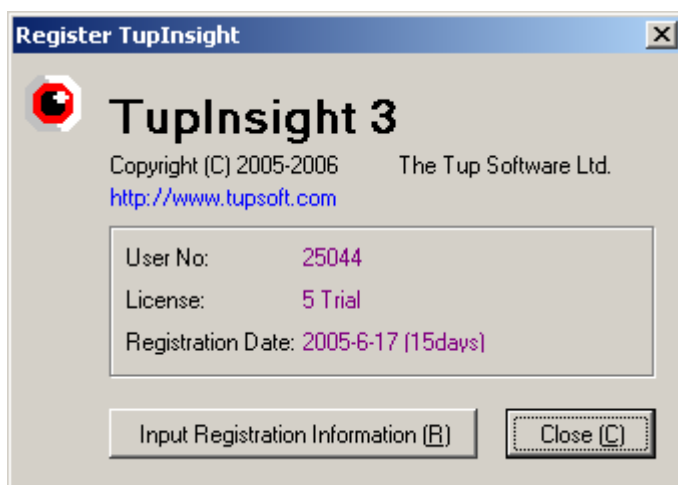
1.4 Registering TupInsight

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.

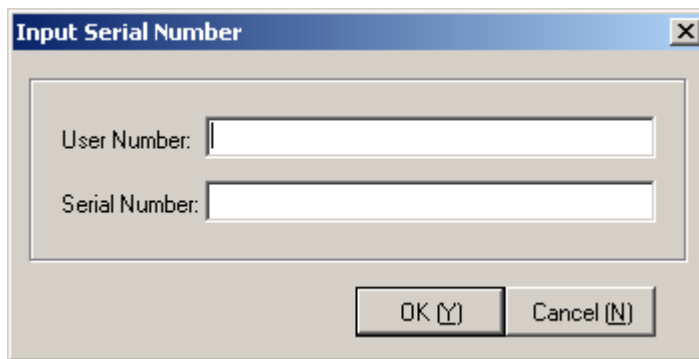
- 1) Connect the console to the TupInsight engine to be registered.
- 2) Select **Help** from the main menu and open **Registration**.



- 3) When the following window appears, select **Input Registration Information**.

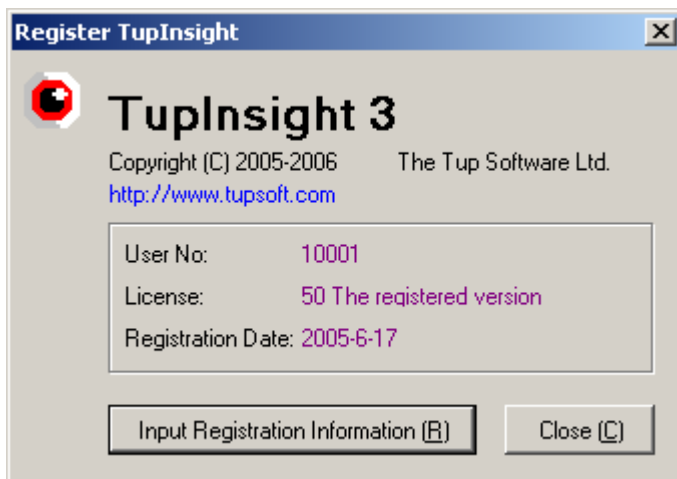


- 4) Enter the user number and serial number in the corresponding field and press the **OK** button.



A dialog box titled "Input Serial Number" with a close button (X) in the top right corner. It contains two text input fields: "User Number:" and "Serial Number:". At the bottom, there are two buttons: "OK (Y)" and "Cancel (N)".

- 5) Click the **OK** button on the following window to display the license information.

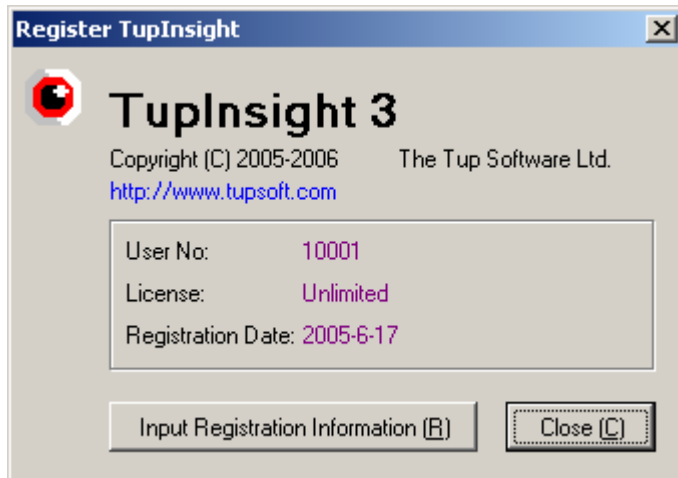


A dialog box titled "Register TupInsight" with a close button (X) in the top right corner. It displays the TupInsight 3 logo (a red circle with a white 'T' and a black dot) on the left. To the right of the logo, the text reads "TupInsight 3", "Copyright (C) 2005-2006 The Tup Software Ltd.", and "[http://www.tupsoft.com](\"http://www.tupsoft.com\")". Below this, there is a table with registration details:

User No:	10001
License:	50 The registered version
Registration Date:	2005-6-17

At the bottom, there are two buttons: "Input Registration Information (R)" and "Close (C)".

- 6) If you have purchased an unlimited version of TupInsight, the window changes to the following one.



7) Click the **Close** button to exit.

1.4.1 Upgrading to Unlimited Version

If you want to upgrade a product with limited licenses to an unlimited one, follow the similar procedure of Registering TupInsight.

2 Operation Guide

When the host computer is turned on, the TuplInsight engine will auto start. The TuplInsight console can be executed at any later time you want. The console is connected to the engine via TCP protocol with the default data connection port number range 12881-12885. (They are changeable if conflict with your other programs.)

The Emails, webpages, and FTP files captured by the engine are transferred to the console through a TCP connection. When logging on the console, enter or locate the IP address or host name for the machine where the engine is installed.

TuplInsight is based on the client/server architecture and allows multiple clients logging on the server at the same time. A client identifies itself by its logon ID. Each operator (or user) may have a different level of access privilege. Admin is the default system administrator with full access and has authority to configure the system settings.

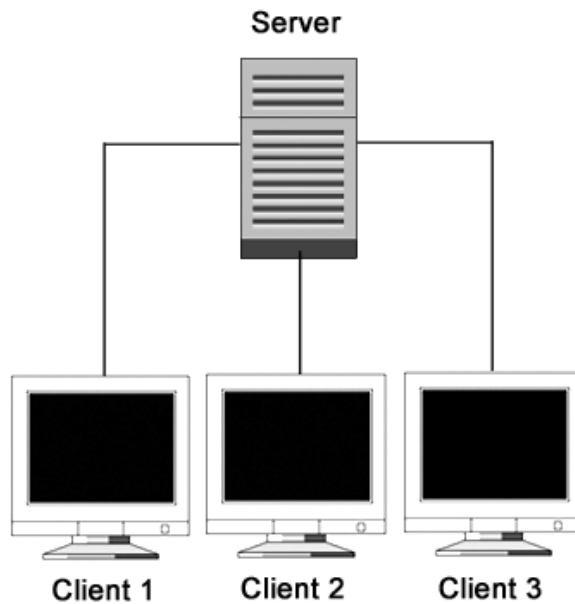


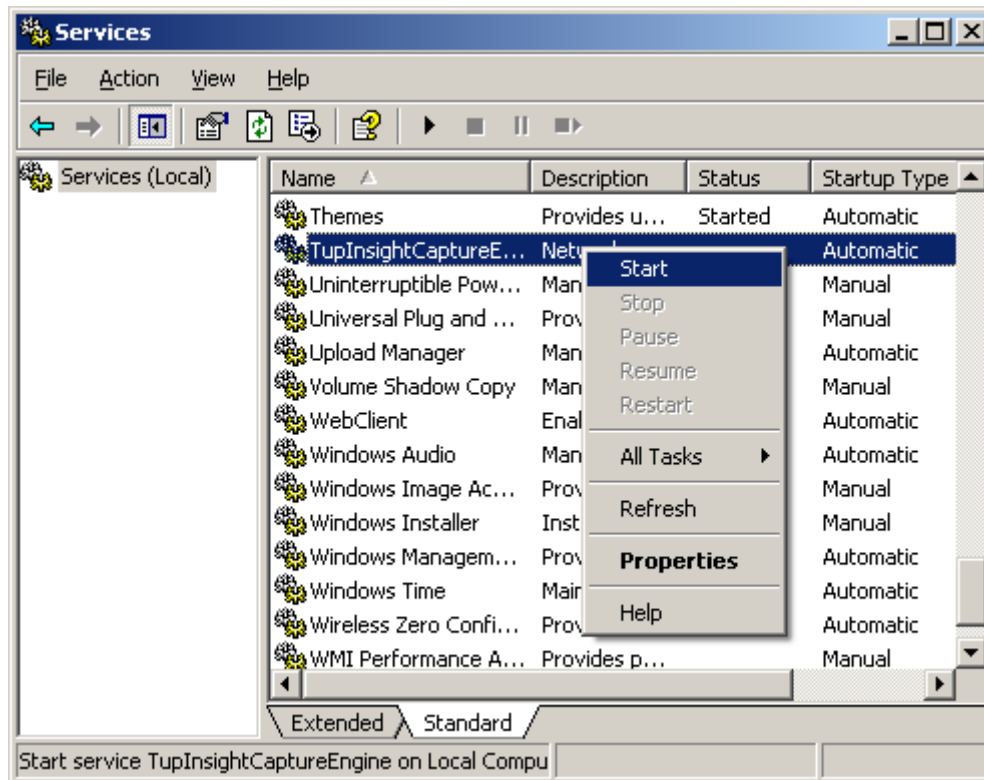
Fig. 4. The client/server architecture and distributed management of data.

2.1 Starting TuplInsight System

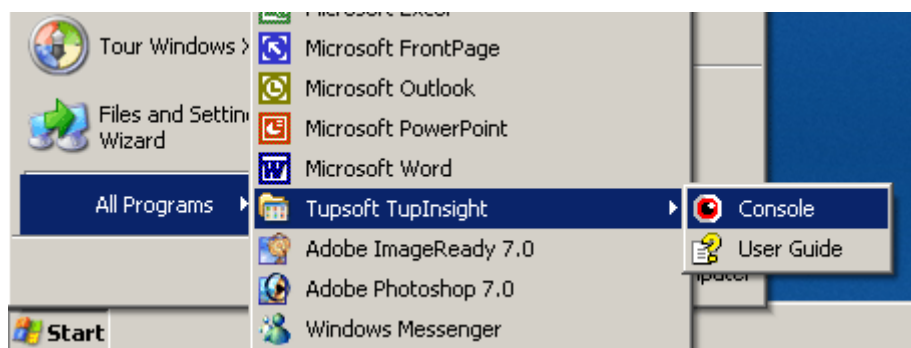
The system comprises an engine and a console. After the installation and restart, the

engine will run automatically without the need for a user to intervene.

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

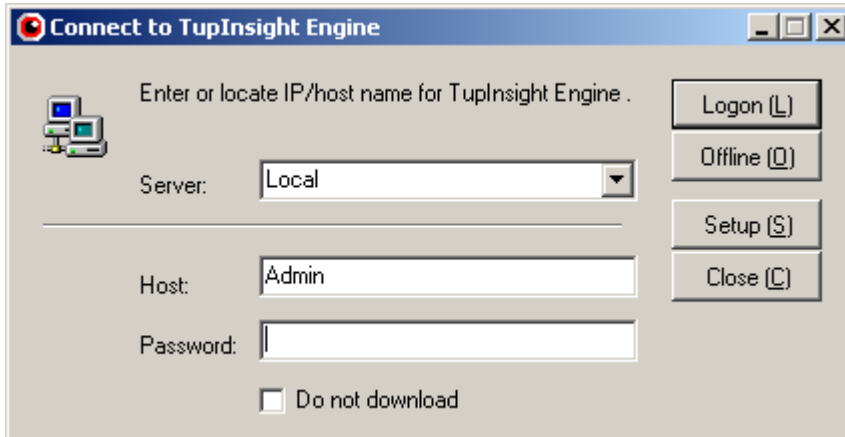


To run the console, Click on **Start, All programs, Tupsoft TupInsight**, and select **Console**, as shown below.

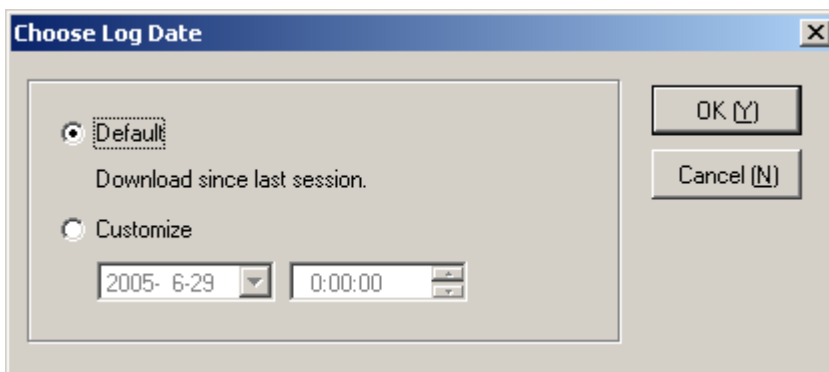


2.2 Connecting to the Engine

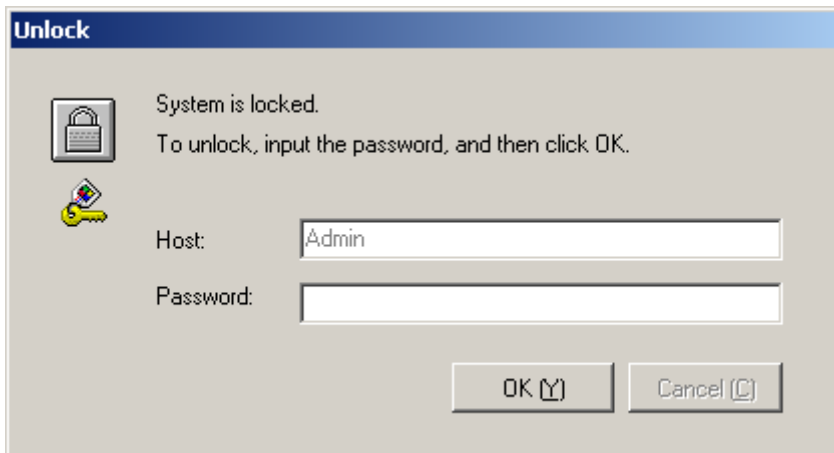
- 1) After starting the TupInsight console, you need to connect it to the engine from the following logon window. By default, the server is Local, user name Admin, and password blank (NULL).



- 2) If the engine 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) Click on the **Setup** button to select the date from which the captured data should be transferred. By default, the console will fetch the data since last session.

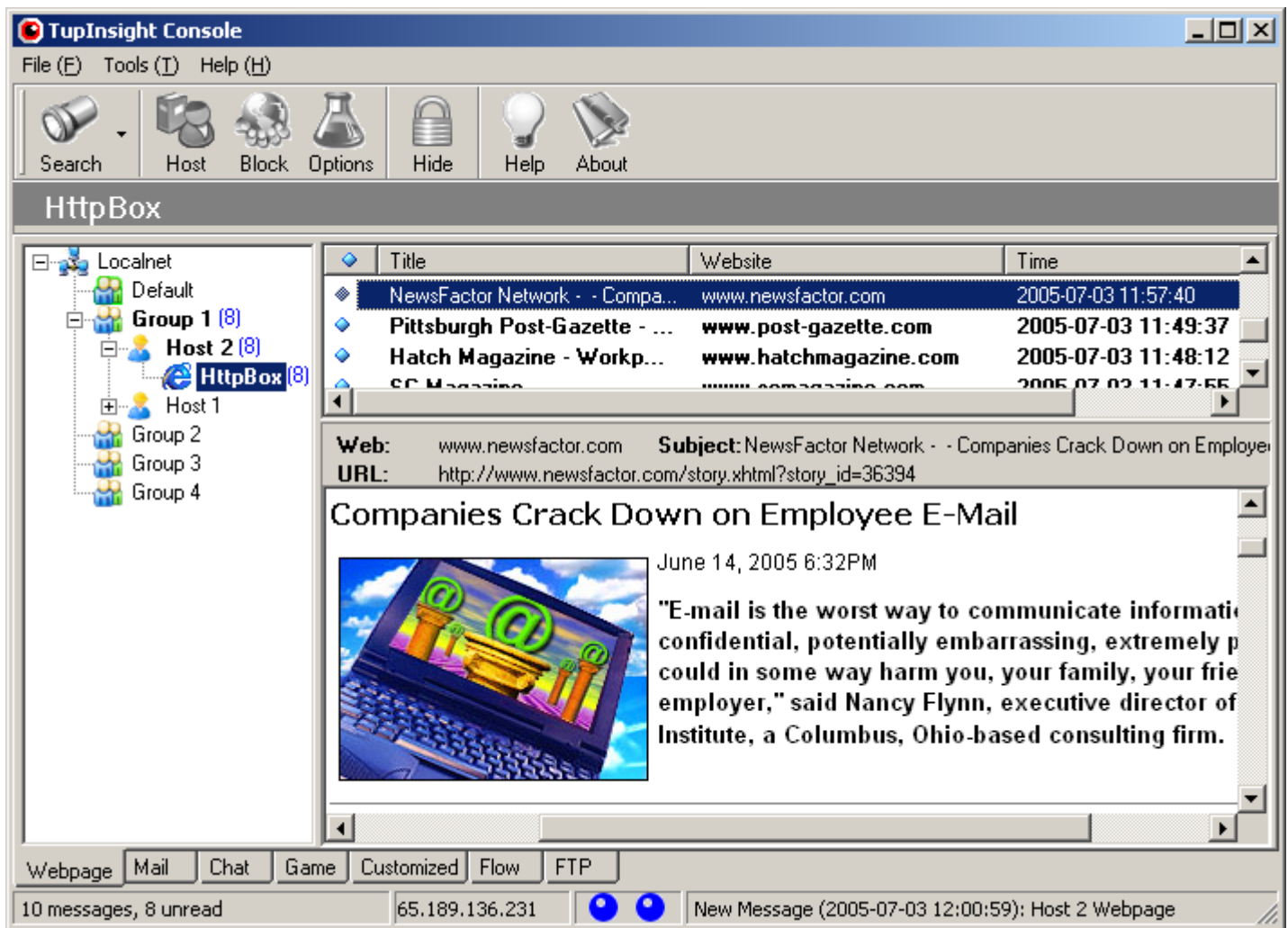


- 4) Enter your user ID and password, and then click **Logon**. (If you are to backup/restore the captured messages, also mark the box **Do not download**).
- 5) After successfully logging on, the main interface will appear.
- 6) If the **Offline** button is pressed, another logon window appears. This window, with the default password also blank (NULL), is designed to prevent invalid users from viewing the data.



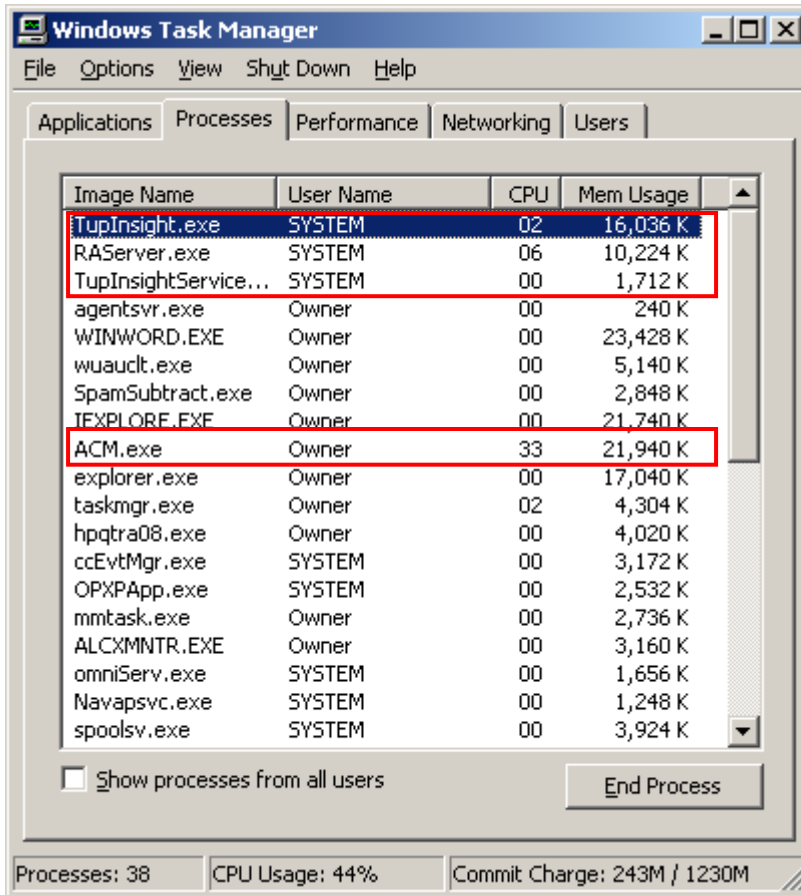
2.3 The Main Interface

After logging on the console, the main interface displays the captured webpage messages by default. You can switch to another monitoring action using the buttons in the action area on the bottom left of your screen.

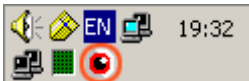


If the engine and console are installed on the same PC, there will be four processes running for the TupInsight system shown inside the Windows Task Manager, i.e.,

- 1) TupInsight.exe --- TupInsight Engine Process
- 2) TupInsightService.exe --- TupInsight Engine Service Process
- 3) RAServer.exe --- TupInsight Database Service Process
- 4) ACM.exe --- TupInsight Console Process.



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



2.4 Exporting/Importing Monitoring Settings

When upgrading the TupInsight system, the monitoring 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:

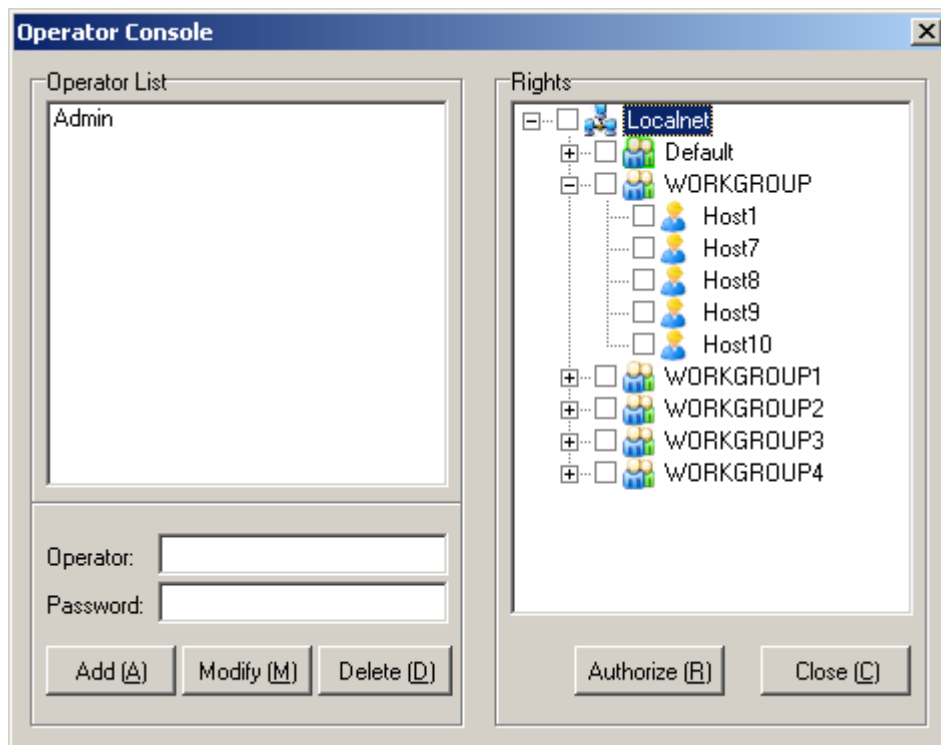
- 1) Run the TupInsight console.
- 2) Open **File** from the main menu and select **Backup Settings**.
- 3) Enter the file name to be saved and then click **OK**.

After installing the upgraded TuplInsight engine, the settings are restored by the following steps:

- 1) Run the TuplInsight console.
- 2) Open **File** from the main menu and select **Import Settings from File**.
- 3) Locate the file name to be restored and click **OK**.

2.5 Operator Administration

In the TuplInsight system, the only default operator is Admin (the system administrator) with full access. Additional operators can be authorized and are granted different levels of access. Through the operator administration console, as shown below, operators are added or deleted, passwords changed, and access rights modified.



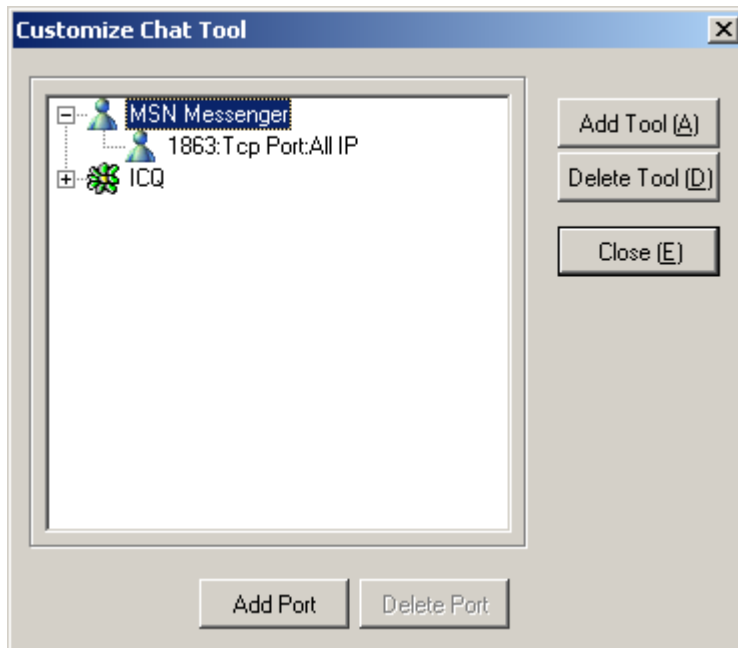
2.6 Customization

Monitoring online activities such as chat, game, or other definable online tools can be customized by the user.

Customizing Chat Tools

In TuplInsight, some chat tools such as MSN and ICQ are defined by default. You can add more by the following procedure.

- 1) Right-click the mouse in the host tree list area and select **Customize chat tool**.
- 2) Add the tools to be monitored or modify/add their connection ports. (Most of the chat tools nowadays allow multiple ports to be used for connections.)



Customizing Game Tools

The operation is similar to that of how to customize chat tools. Please refer to [Customizing Chat Tools](#).

Customizing Other Online Tools

The operation is similar to that of how to customize chat tools. Please refer to [Customizing Chat Tools](#).

2.7 Internet Access Control

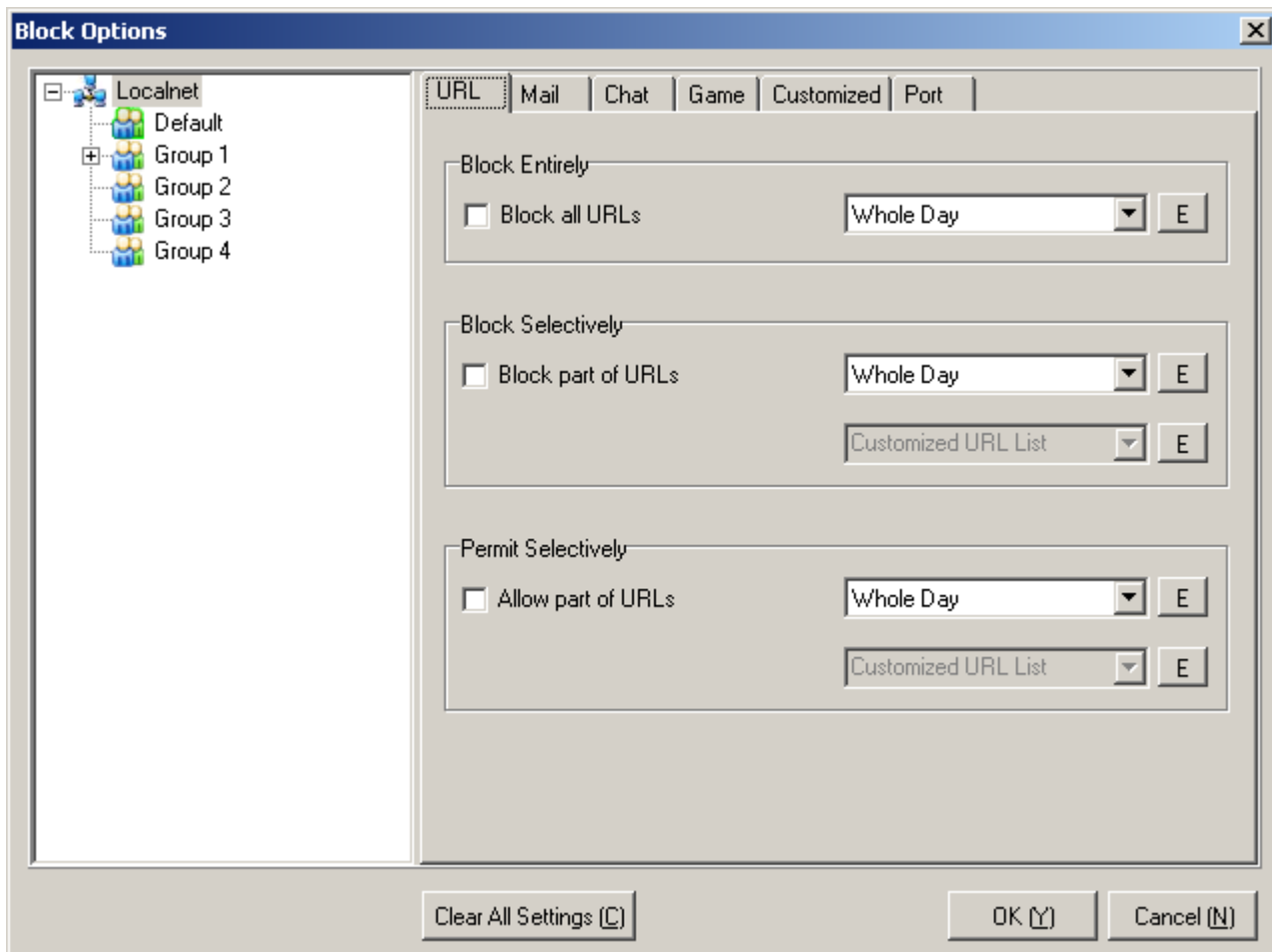
Another important function of TuplInsight is its ability to restrict online activities according to the user's customization and lock up MAC (Media Access Control) addresses.

Restriction of web access: You can use TuplInsight to set time schedules (Internet access or specific online activities can be disabled at certain times of day for a host, group, or the whole local network), block/filter URLs (web-sites) by user-defined keyword, disallow Email servers, and regulate chat/game or customized tools.

Lockup of MAC addresses: You can use TuplInsight to disallow the change of MAC and IP addresses on the LAN. (Note: Lockup of IP addresses in a DHCP system will lead to the network failure.)

2.7.1 Restricting Web Access

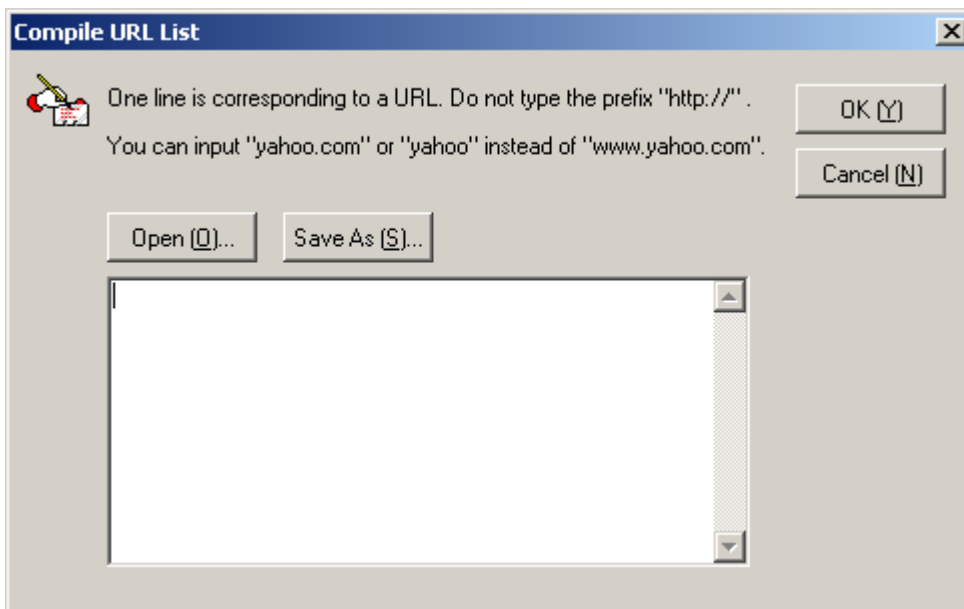
The restrictions are set only by the system administrator (Admin).



2.7.1.1 Blocking/Filtering URLs (Websites)

There are three modes to block/filter URLs: Disallow/allow all the websites; disallow/allow part of websites by user-defined keyword; and the combination thereof. For every blocking/filtering mode you can set specific time schedules.

A URL block/allow list can be customized by Admin for a host, group, or the whole network.

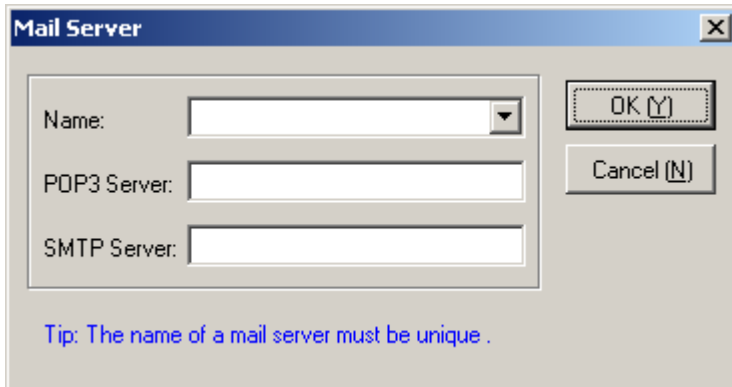


2.7.1.2 Blocking Emails

This blocking/filtering function can set rules such as what kind of Email tools, for instance, FOXMAIL or OUTLOOK, are allowed and which mail server the host(s) can use for sending and/or receiving mails at certain times of day.

The customizable mail servers consist of POP3 and SMTP servers. To locate the addresses of specific POP3 and SMTP servers, you can lookup the corresponding websites for details. For example, for yahoo.com the mail servers are pop.mail.yahoo.com and smtp.mail.yahoo.com, respectively.

If there are several mail servers should be blocked, you must input them one by one.



2.7.1.3 Blocking Chat Sessions

You can define which chat tool is disallowed for a host, group, or the whole network by the following procedure.

- 1) Right-click the mouse in the host tree list area and select **Customize chat block**.
- 2) Add the tools to be blocked inside the dialog window.

2.7.1.4 Blocking Game Activities

The procedure is similar to that of Blocking Chat Sessions.

2.7.1.5 Blocking Customized Online Tools

The procedure is similar to that of Blocking Chat Sessions.

2.7.1.6 Blocking Connection Ports

The availability of blocking at connection port level of TuplInsight gives the system administrator more flexibility for web access control.

2.7.2 MAC Lockup

To lock up MAC addresses, TupInsight views a host as invalid if it is not in the list previously compiled. Thus, whenever a new host is detected it will block the network connection by IP conflict. Before you start the lockup, make sure all the hosts are in the list by scanning the whole network.

Similarly, to prevent any host from modifying the IP address, TupInsight will ban the network connection by IP conflict until the correct IP address is returned.

2.8 Host Information and Administration

TupInsight's simple and straightforward administration panel makes it easy for the user to manage the data and information of hosts. It allows the user to do the following manipulations.

- 1) Managing workgroups
- 2) Modifying hostnames
- 3) Deleting hosts and workgroups
- 4) Exporting/importing host and workgroup information
- 5) Selecting hosts to be monitored.

2.8.1 Managing Workgroups

TupInsight simplifies the management tasks by dividing hosts into meaningful groups, and you have the flexibility to select/combine hosts into different workgroups. Initially, TupInsight 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-add function, you can change the settings through the Group and Host Information interface.

1) Creating a New Workgroup

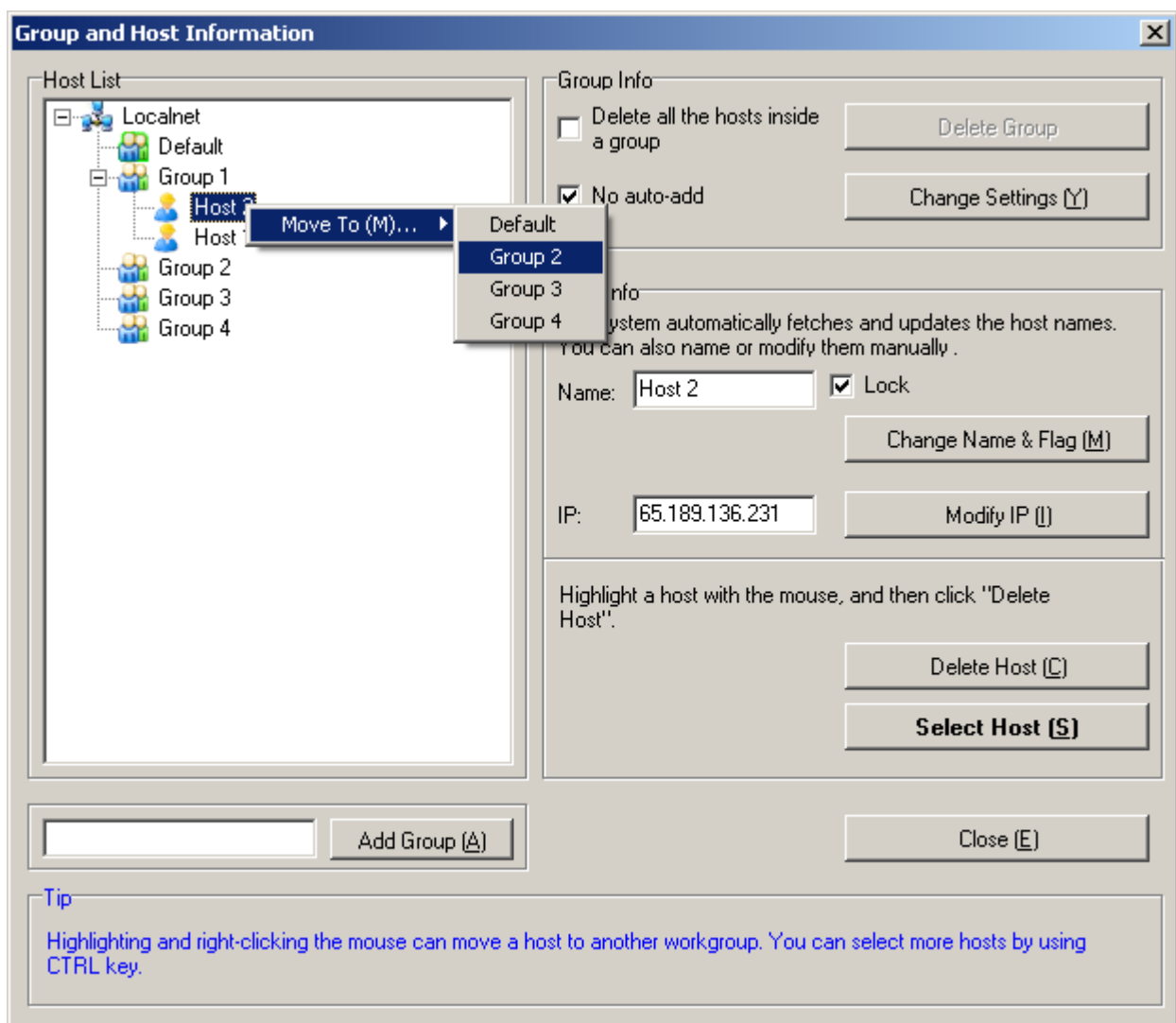
You can set up a new workgroup manually by doing the following:

1. From the main menu, select **Tools** and then **Host Info**.
2. Enter a name for a workgroup and click on **Add Group**.

2) Transferring a Host to Another Workgroup

Whenever a new host is connected to the network, the TupInsight 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 main menu, select **Tools** and then **Host Info**.



2. Highlight a host (or hosts using CTRL key) and right-click the mouse to select **Move to ...**

3. From the sub-menu, select the destined workgroup.

3) Deleting a Workgroup

From the Group and Host Information panel, highlight the workgroup to be deleted and click on the **Delete Group** button. Before making the decision, make sure you want to delete all the hosts inside the workgroup. To retain some, move them into the workgroup “Default” first. The “Default” is un-deletable by default.

4) Disabling Auto-Add Function

From the Group and Host Information panel, mark **No auto-add** and click on the **Change settings** button.

2.8.2 Modifying Hostnames

A hostname is the computer name corresponding to a specific IP address. By default, the TuplInsight console will automatically fetch the computer name for a host. Due to a great variety of networking systems, the console might not get the name for some reason. If this is the case, just rename the host corresponding to the IP address by doing the following:

1. Run the TuplInsight console.
2. From the main menu, select **Tools** and then **Host Info**.
3. Highlight the host to be renamed and edit the name displayed inside the open field.
4. Click on the **Change Name & Flag** button.
5. Mark the box **Lock** to disable auto-modification by the console in case it detects the computer name later.

2.8.3 Deleting Hosts

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

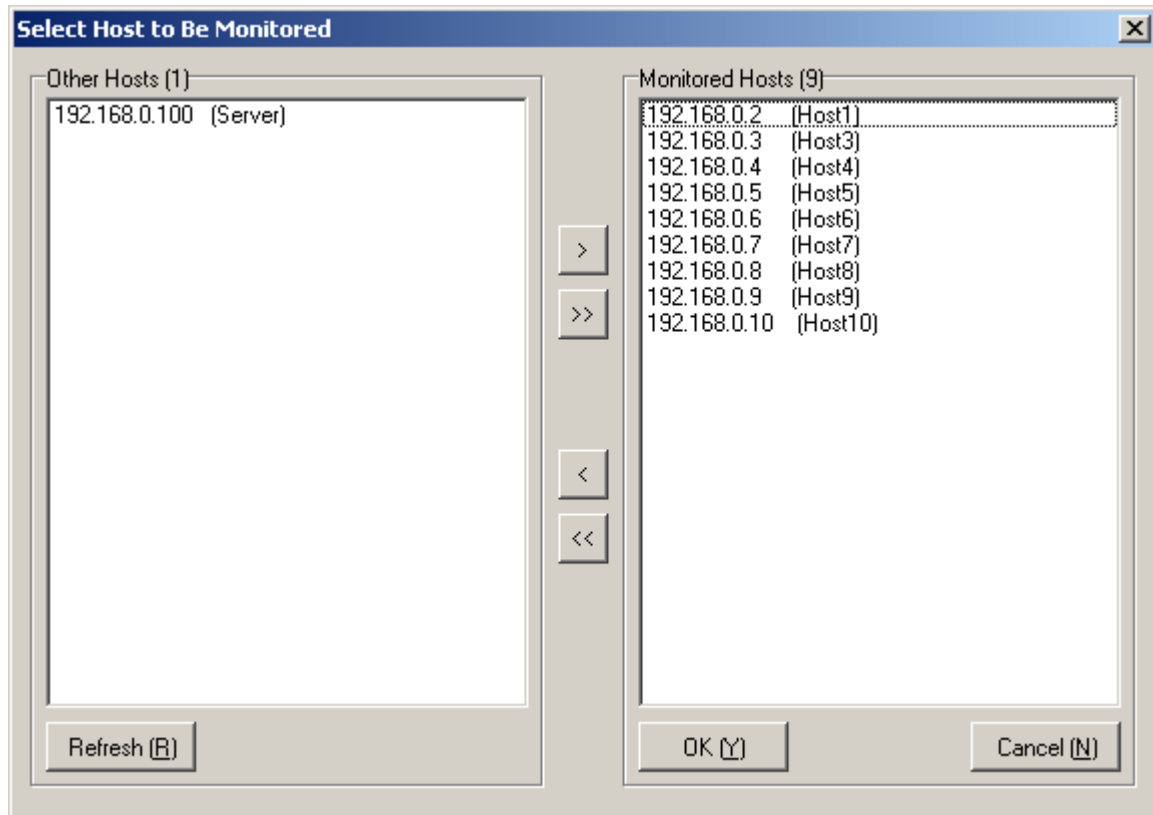
2.8.4 Exporting/Importing Host and Workgroup Information

The host and workgroup information can be reused when upgrading the TuplInsight system. Since the monitoring settings contain the information of hosts and workgroups, please refer to the steps in [Exporting and Importing Monitoring Settings](#).

2.8.5 Selecting Hosts to Be Monitored

By default, the TuplInsight system will automatically capture all the messages sent and received regardless of the hosts for the whole network. If you purchase a copy with limited licenses, you might need to select the hosts to be monitored.

1. Run the TuplInsight console, and logon and connect to the engine as the system administrator.
2. From the main menu, select **Tools** and then **Host Info**.
3. Click on the **Select Host** button, and a window that looks similar to the following appears on the screen.



4. Highlight the host and then click on one of the arrow buttons to transfer from one side to the other.
5. When you are done, click on the **OK** button.

On the console, the monitored hosts are represented using blue icons, while the unmonitored ones red icons.

2.9 Setting Up Systems

The system settings of TuplInsight consist of two parts, the engine and the console, and both of them are done through the console.

To set up the engine, you need to select a monitoring network adapter and choose a password. You can also change the data retention period, define subnets, and configure connection ports to be monitored. The console also needs password protection and configuration such as how to mark a message read.

The monitoring adapter: Here, the monitoring adapter is the network card on the host where the TuplInsight engine is installed. The TuplInsight system currently does not support multi-adapter monitoring. Thus, if the host has two adapter cards for the internal and external connection, respectively, you should select the one connected to the local network.

Subnets: The TuplInsight can automatically do subnetting for a host based on the IP address. If there are many subnets on the local network, you might need to define manually.

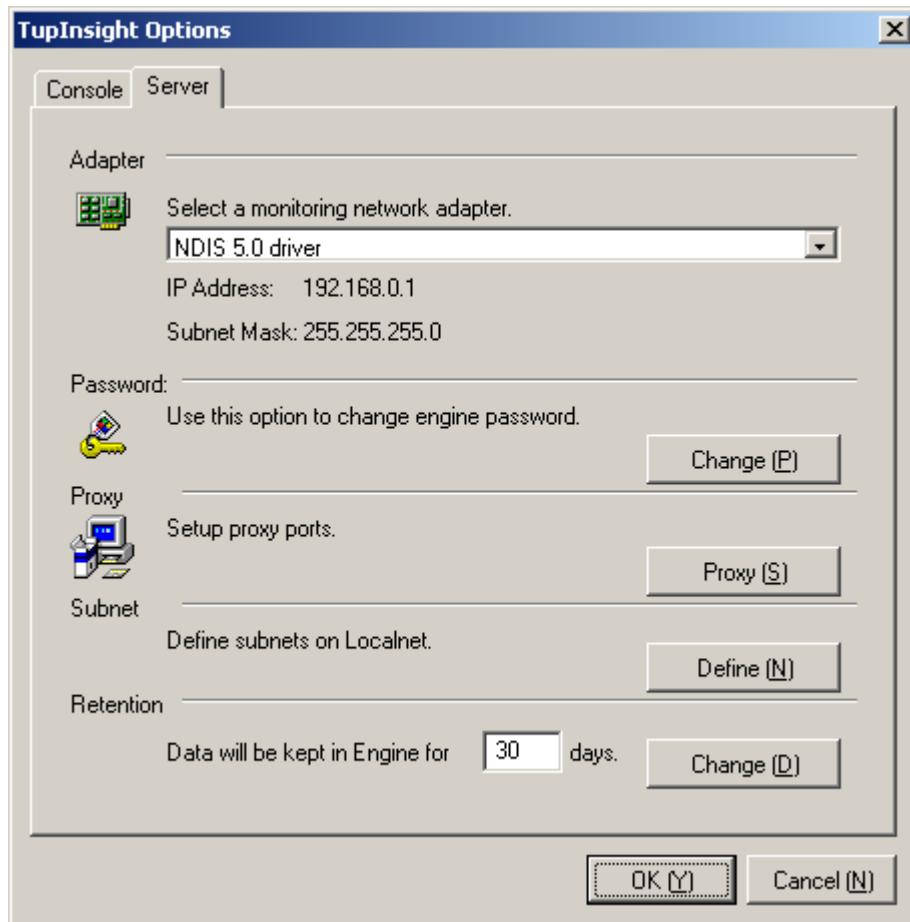
Connection ports to be monitored: If the Internet connection sharing is via proxy, you need to configure the connection ports to be monitored, i.e., proxy ports.

Note: Only the system administrator has the authority to configure the system settings.

2.9.1 Configuring the Server

The configuration includes selecting a monitoring adapter, setting up a password, defining subnets, and specifying connection ports to be monitored if the Internet sharing is via proxy

with non-default ports. For well known port numbers, HTTP: 80; FTP: 21; POP3: 110; and SMTP: 25.



The monitoring adapter: Here, the monitoring adapter is the network card on the host where the TupInsight engine is installed. The TupInsight system currently does not support multi-adapter monitoring. Thus, if the host has two adapter cards for the internal and external connection, respectively, you should select the one connected to the local network.

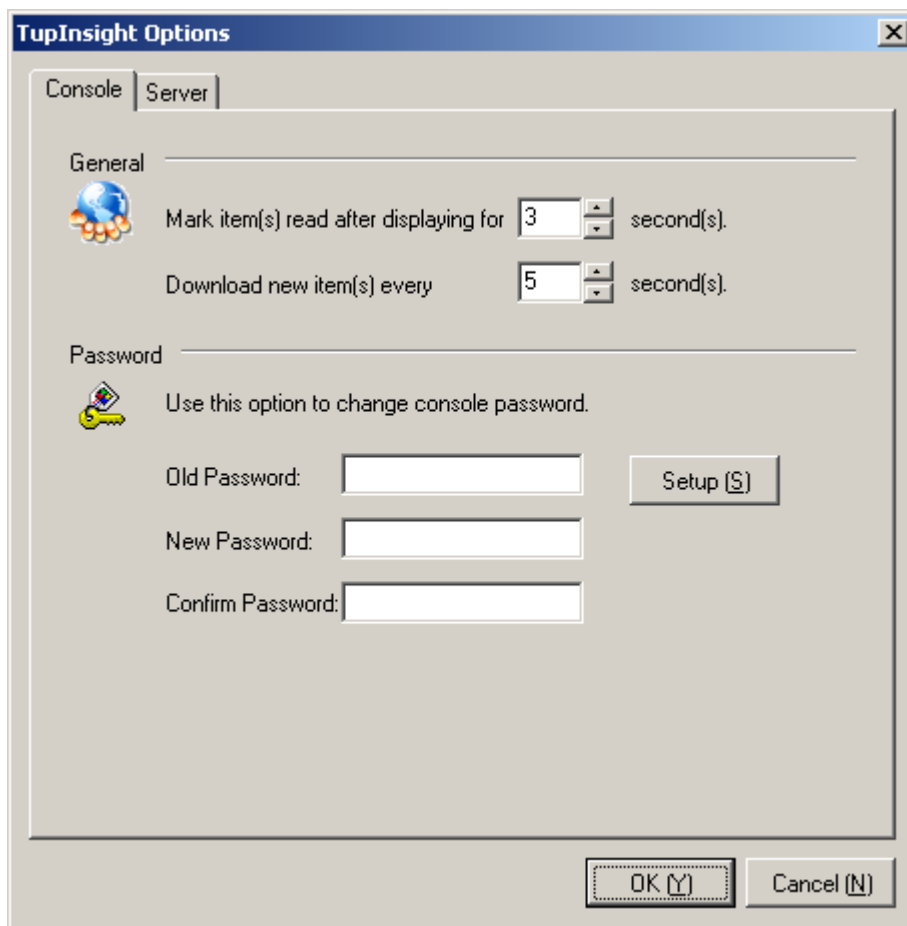
Subnets: The TupInsight can automatically do subnetting for a host based on the IP addresses. If there are many subnets on the local network, you might need to define manually.

Connection ports to be monitored: If the Internet connection sharing is via proxy, you need to configure the connection ports to be monitored, i.e., proxy ports.

2.9.2 Configuring the Console

The configuration includes setting up a password, defining the refreshing time for new messages, and specifying how to mark messages read.

1. Run the TupInsight console.
2. From the main menu, select **Options** to bring up the following window.

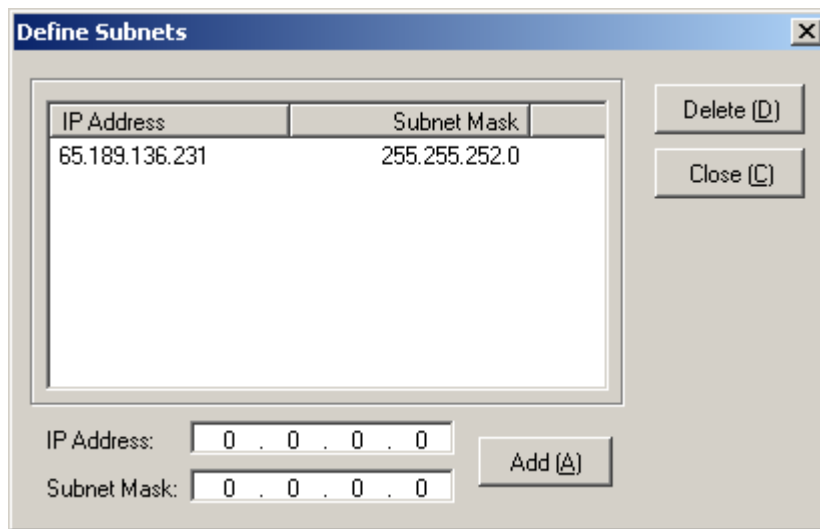


3. By default, the console will mark messages read after displaying for 3 seconds and check for new messages every 5 seconds.
4. To change the console password, enter the old and new one and then click on the **Setup** button.

2.9.3 Subnetting

The TuplInsight can automatically do subnetting for a host based on the IP address. If there are many subnets on the local network, you might need to define manually.

1. Run the console and logon as the system administrator (Admin).
2. From the main menu, select **Options** to bring up a dialog window.
3. From the window, select **Server**, and then click on the **Subnet** button.

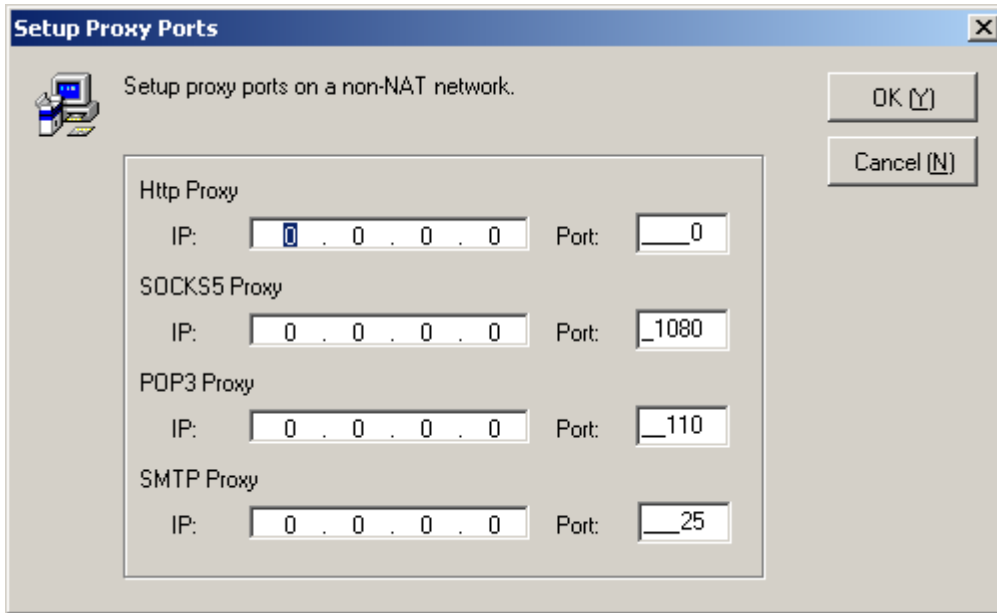


4. Define accordingly.

2.9.4 Specifying Connection Ports to Be Monitored

Generally, there is no need to setup connection ports to be monitored. If you are using a non-NAT proxy server for Internet connection sharing, however, those proxy ports must be specified.

1. Run the console and logon as the system administrator (Admin).
2. From the main menu, select **Options** to bring up a dialog window.
3. From the window, select **Server**, and then click on the **Proxy** button.



4. Specify accordingly and finally click the **OK** button.

2.10 Managing the Data

Data management includes to preview, read, delete, save, backup, restore, search, and filter messages and attachments.

2.10.1 Previewing Messages

The HTTP and Email messages can be previewed through the console.

1. From the host tree list (on the left of the main interface), select the host to be previewed.
2. Select one of the message boxes (HttpBox, InBox, or OutBox).
3. Click on the message to be previewed from the list on the upper right-hand corner.
4. The message will appear inside the bottom right frame.

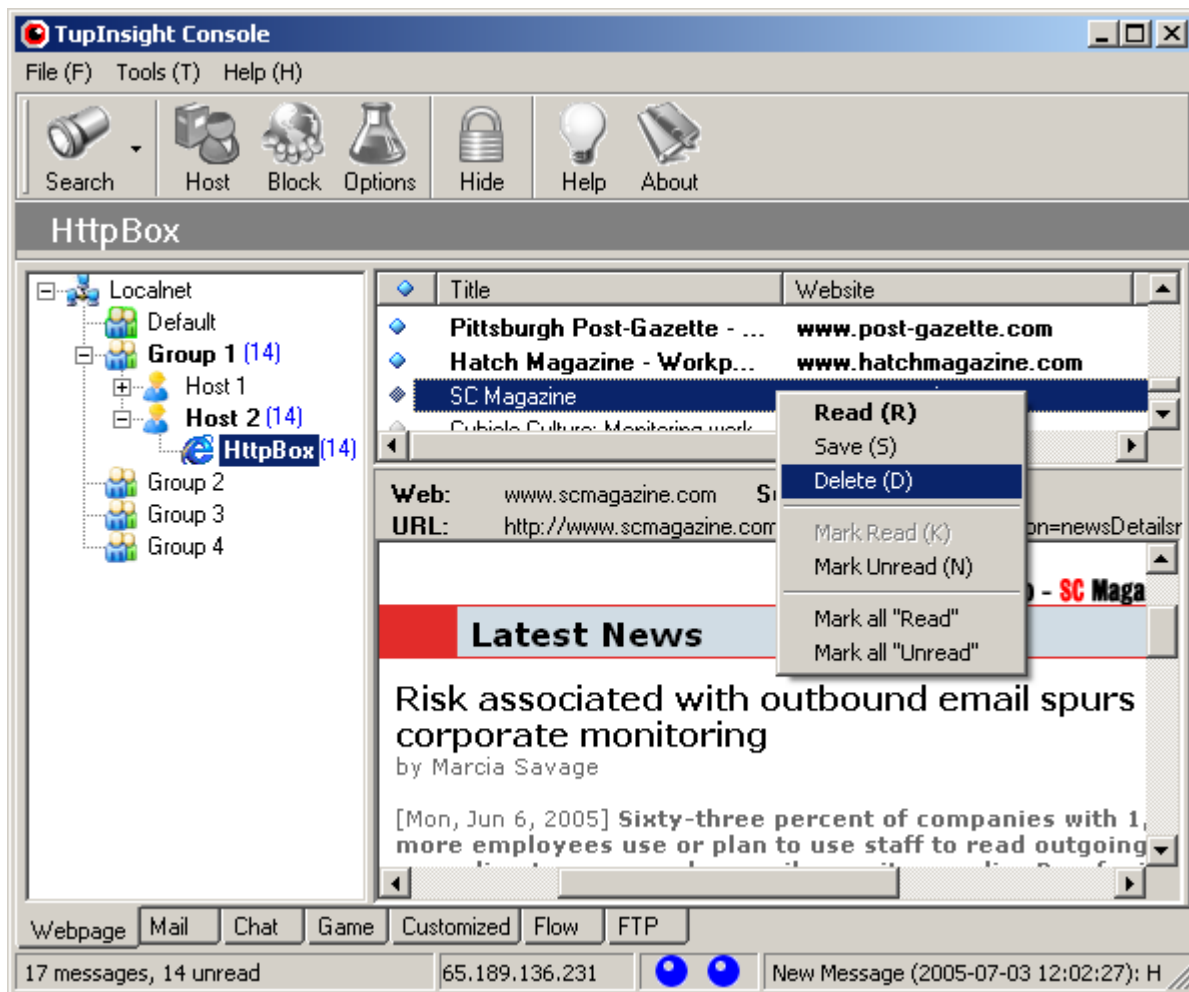
2.10.2 Reading Messages

Double-click to bring up a new window containing the message.

2.10.3 Deleting Messages

Message deletion includes to delete a specific message; all the messages inside a box (HttpBox, InBox, OutBox, or FtpBox); all the messages for a host, group, or the whole network; and history records.

1. Select the message, host, workgroup, or the whole network and then right-click the mouse to bring up a sub-menu.

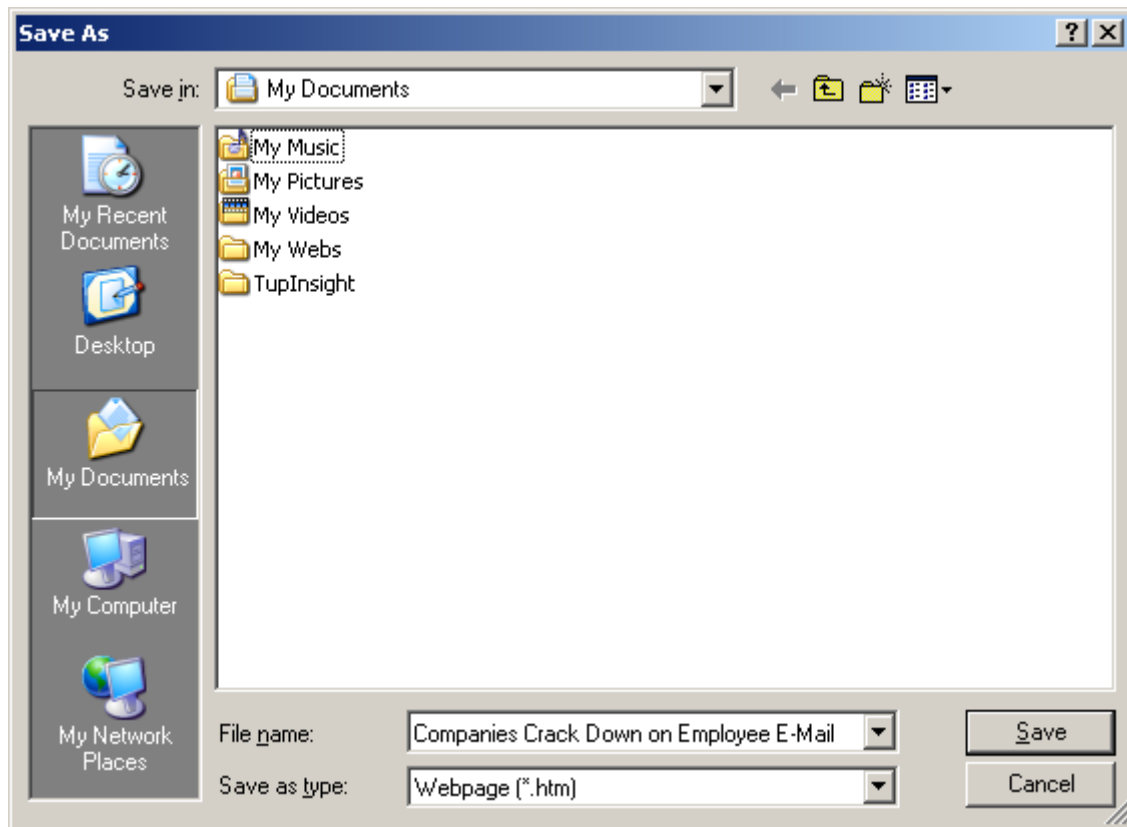


2. Click **Delete** and then **OK**.

Use CTRL or SHIFT key for the multiple selection of messages from the list on the upper right-hand corner, or use CTRL + A to select all.

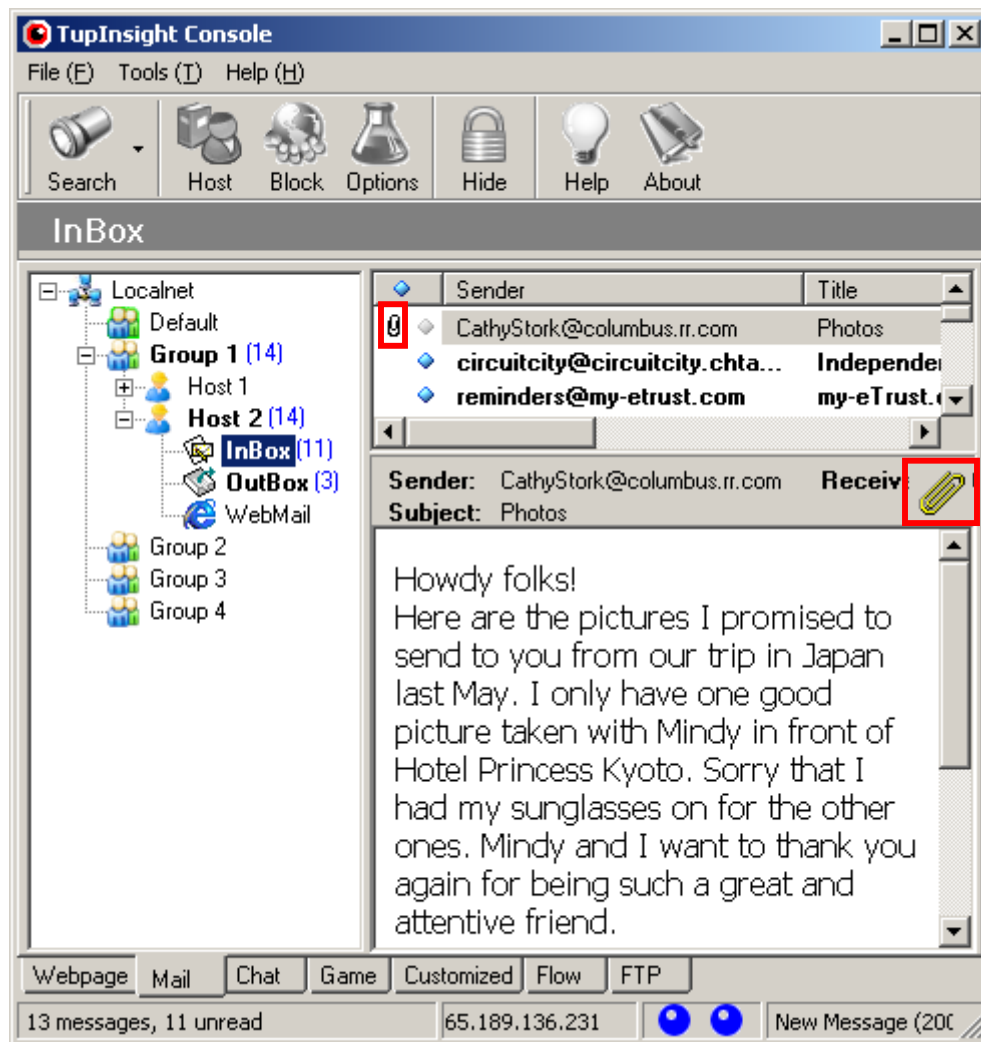
2.10.4 Saving Messages

1. Select the message to be saved and right-click the mouse to bring up a sub-menu.
2. From the sub-menu, select **Save**.
3. In the new window, select a file path, enter a name, and then click on the **Save** button.

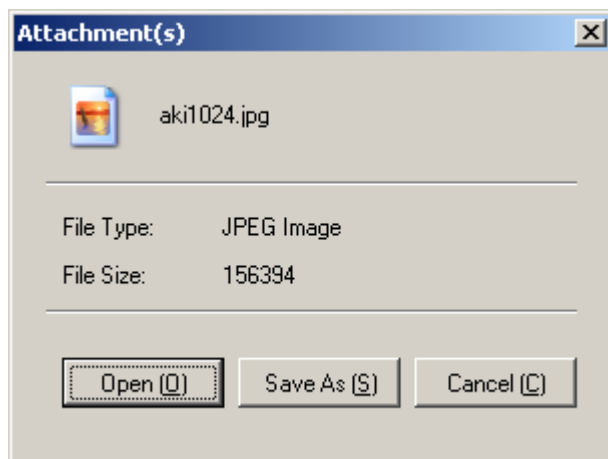


2.10.5 Opening/Saving Attachments

If an Email message contains attachment(s), the attachment “paper clips” will appear as the following.



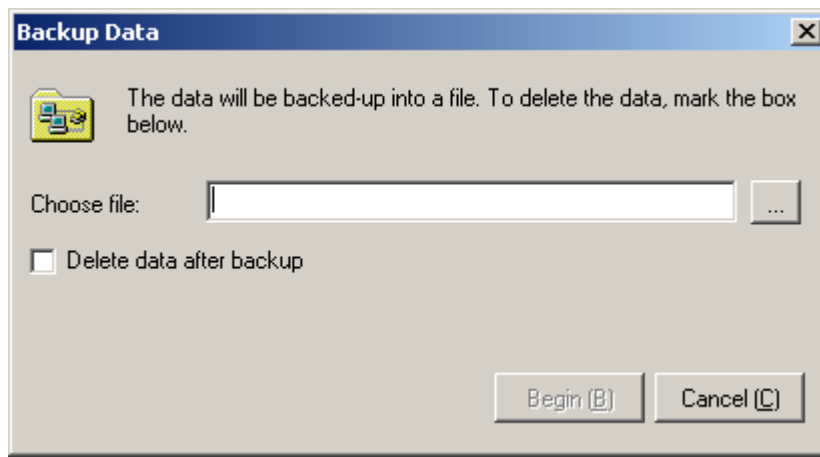
Click the one on the top of the preview frame to bring up the following window, and select accordingly.



2.10.6 Backing Up Messages

To archive the captured messages securely, you need to routinely backup the data. The backup operation should be done when the console is not to download data from the engine. Therefore, you should mark the box **Do not download** on the logon window at the beginning.

1. From the main menu, select **File** and then **Backup Data**.
2. Select the file to be backed up (.abf file) when the following dialog window appears.



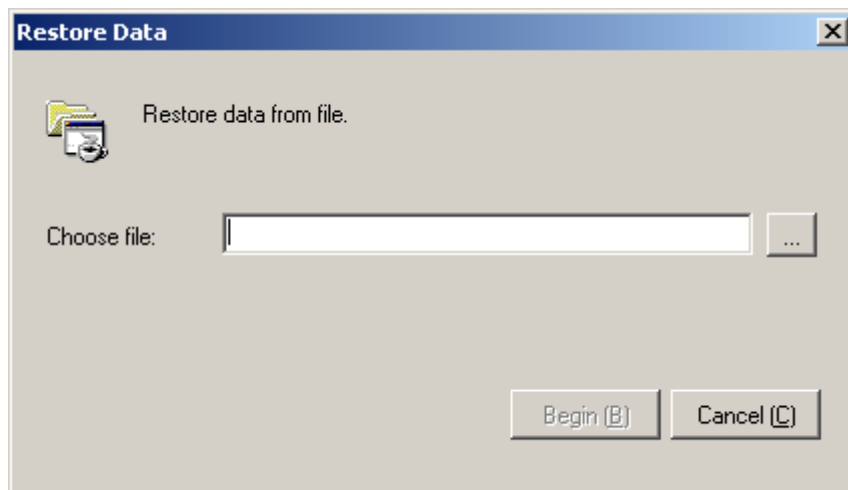
3. Optionally mark **Delete data after backup**.
4. Click on the **Begin** button to start the process.

Since the saving process may take several minutes (depending on the file size), just wait patiently for it to finish.

2.10.7 Restoring Messages

To review the messages backed-up before, you need to restore them first. Similarly, the restoration operation should be done when the console is not to download data from the engine. Therefore, you should mark the box **Do not download** on the logon window at the beginning.

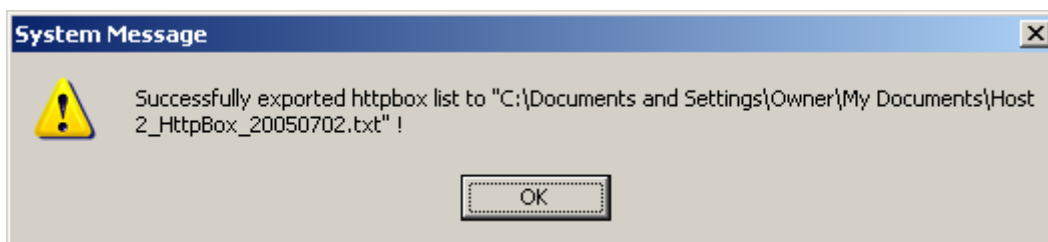
1. From the main menu, select **File** and then **Restore Data**.
2. Select the file to be restored (.abf file) when the following dialog window appears.



3. Click on the **begin** button to start the process.

2.10.8 Exporting Messages

You can export the captured messages from the corresponding message boxes in the format of Excel or Text files.



2.11 Monitoring Chat Sessions

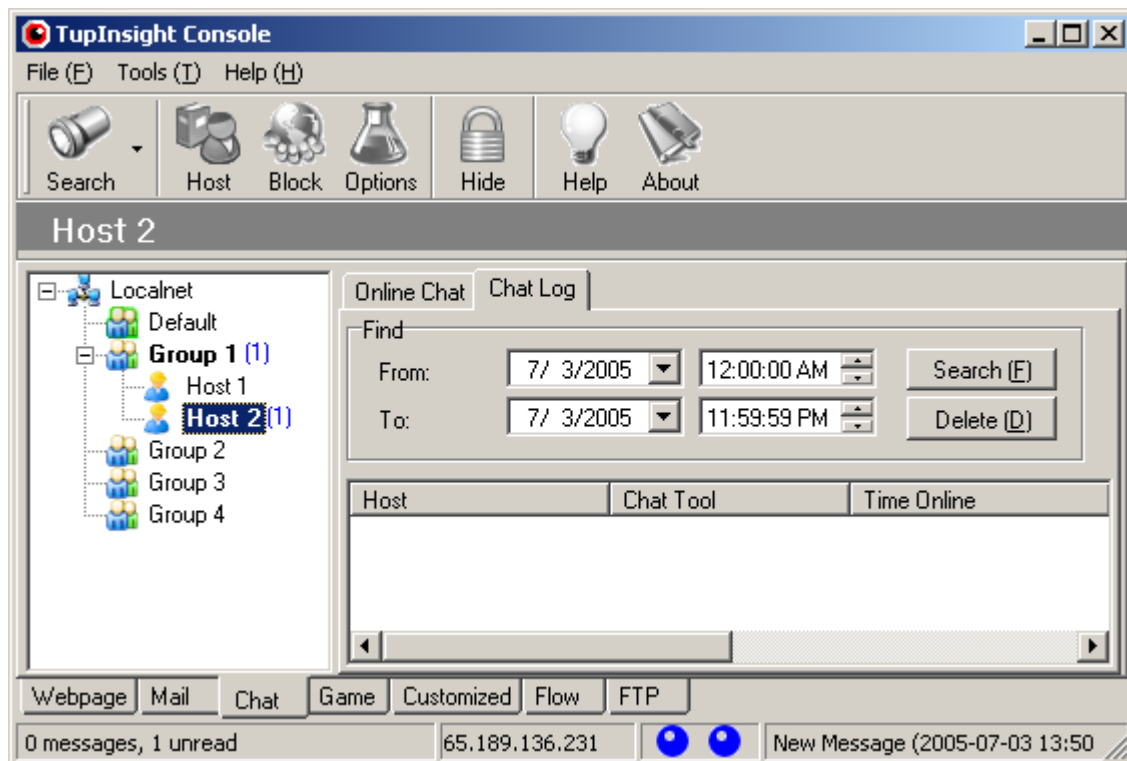
TupInsight shows information such as the host involved, chat tool used, time online, and so on.

1. Run the console and connect to the engine.
2. Select **Chat** from the action area on the bottom left corner.
3. Use the mouse to select a specific host or workgroup from the tree list, and the chat session information will appear on the screen.

The number inside the brackets to the right of a host, workgroup, or the local network indicates how many hosts are chatting online right now.

2.11.1 Looking Up Chat Log Files

TuplInsight records hourly the log data such as the host involved, chat tool used, time online and offline, and sent and received data sizes.



2.12 Searching Messages

You can search Emails and webpages captured.

Email Search: Hit the **Search** button on the user interface to bring up the following window. Type in all or part of a sender name and/or title, and then click on **Search** to display every message that matches. By default, the search only shows the results of the day.

Search Email

Mailbox:InBox

Host:All Hosts

Sender:Cathy

Title:

From:7/ 2/2005

To:7/ 2/2005

☐ Contain attachment(s)

Search (B)

New Search (N)

Close (E)

	Host	Sender	Title	Date Received	Size
0	Host 2	CathyStork@columbus.rr.c...	Photos	2005-07-02 13:54:17	210.86KB

1 records

Webpage Search: Hit the **Search** button on the user interface to bring up the following window. Type in all or part of a sender name and/or title, and then click on **Search** to display every message that matches. By default, the search only shows the results of the day.

Host: All Hosts

Website:

Title: monitor

From: 7/ 3/2005 To: 7/ 3/2005

Search (B)

New Search (N)

Close (E)

	Host	Title	Website	Time	Size
◆	Host 2	Cubicle Culture: Monitoring workers is boss s righ...	www.post-gazette.com	2005-07-03 11:47:32	16.26KB
◆	Host 2	USATODAY.com - Employer monitoring: It s a s...	www.usatoday.com	2005-07-03 13:47:20	53.08KB
◆	Host 2	Companies increasingly monitoring email - ZDNet...	news.zdnet.co.uk	2005-07-03 14:04:02	49.97KB

3 records

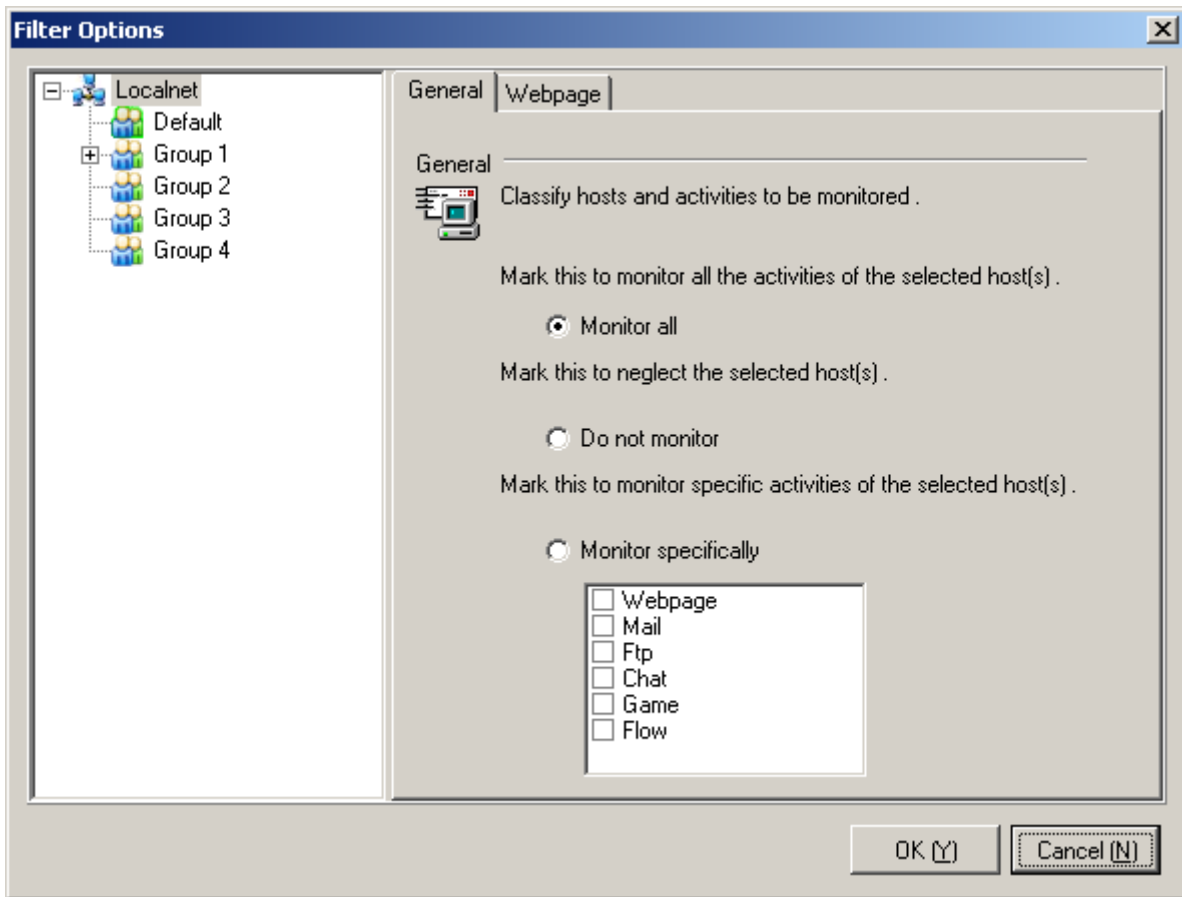
2.13 Filtering Messages

TuplInsight will record all the messages, unless you instruct otherwise. Those instructions are: 1) to neglect a specific host; 2) a specific website; and 3) a specific activity.

Note: Only the system administrator has the authority to configure the settings.

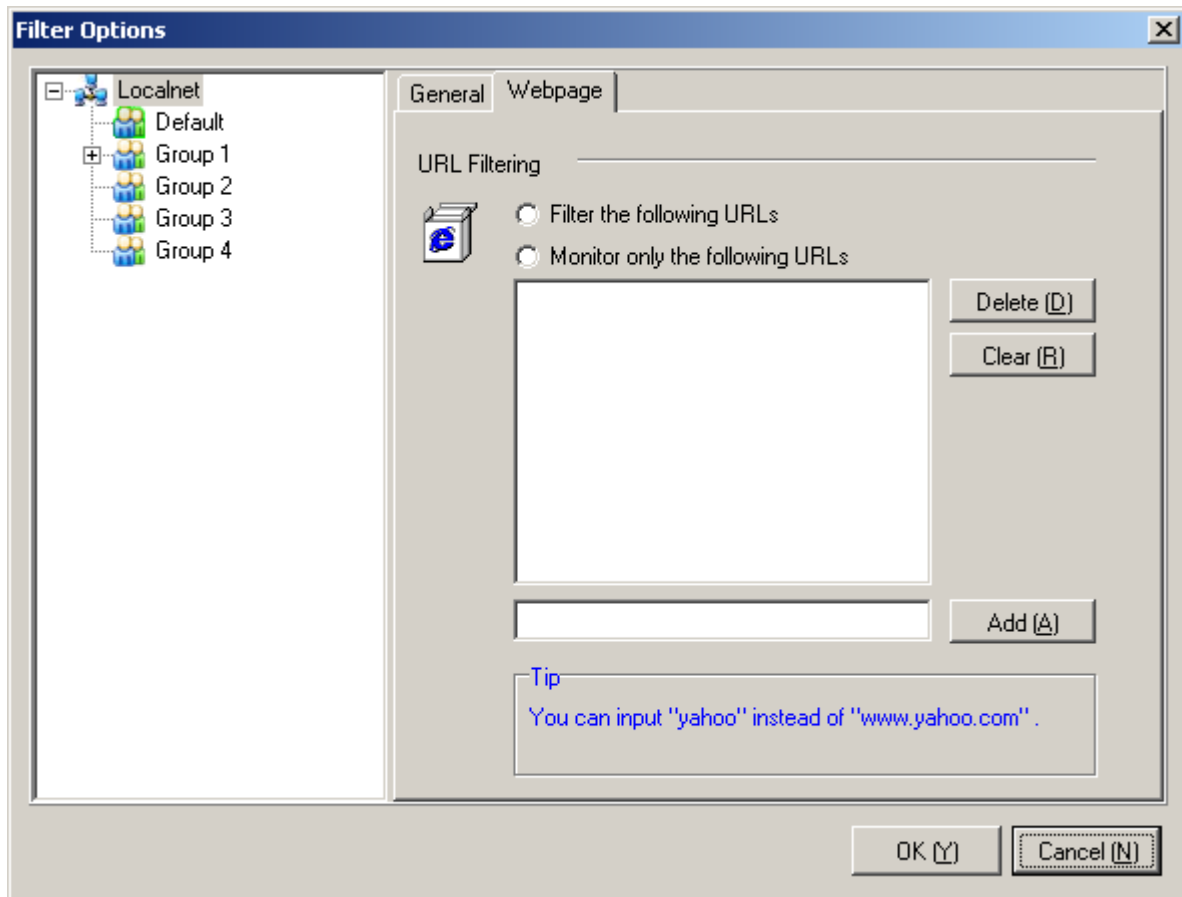
2.13.1 General Filtering Settings

By default, TupInsight will capture all the messages, unless you instruct otherwise. Select the settings accordingly on the following window and then click on **OK**.



2.13.2 Filtering URLs

By default, TupInsight will capture all the webpages, unless you instruct otherwise. Compile a list of websites on the following window and then click on **OK**.



Note: Do not type the prefix <http://>.

2.14 Technical Support

If you have any technical questions, please E-mail support@tupsoft.com.