
**NETSAFA POLICY CONTROL
VERSION 2007.2**

USER MANUAL

Today's better software™

Copyright © DTM Technology Limited

Document Version: 20080120

Please email any comments to:

info@netsafa.com

Warranty

DTM Technology Limited does not warrant that:

- a. the software or services provided under this agreement will be uninterrupted or error free; or
- b. the software or services will meet the End User's requirements, other than as expressly set out in this agreement.

Except where stated to the contrary in this agreement, all warranties whether express, implied, statutory or otherwise are excluded. Where the exclusion, restriction or modification of certain warranties, guarantees, conditions, rights or remedies is prohibited under applicable legislation, then such a term will be taken to be included in this agreement. However, the liability of DTM Technology Limited for any breach of any such term will be limited, at the sole discretion of DTM Technology Limited.

The End User warrants that, at the time of entering into this agreement, they are not relying on any representation made by DTM Technology Limited which has not been stated expressly in this agreement, or on any information contained in any other document produced by DTM Technology Limited, including any brochures, catalogues, publicity material or information available on the DTM Technology Limited or NetSafa Policy Control software Internet site.

Disclaimer

DTM Technology Limited denies any and all responsibility for damages caused directly or indirectly as a result of any faults with the enclosed programs and/or documentation.

License

DTM Technology Limited retains the copyright to the user manual. All patent, copyright and other proprietary rights in and to the programs will remain with DTM Technology Limited.

Your purchase gives you the right to copy and use the programs as described on your DTM Technology Limited License Certificate included in your package.

Please save your DTM Technology Limited License Certificate, which contains your CD key. They serve as your legal right to use the software. You may also need them in order to receive future updates to the product.

Please be careful not to install or run the software on more PCs than your DTM Technology Limited License Certificates permits you to do.

The programs may be copied for backup purposes only, and only as long as the above-mentioned rules are adhered to.

Trademarks

NetSafa® and Today's better software™ are registered trademarks of DTM Technology (Pte) Limited. All other products mentioned in this manual are trademarks of their respective manufacturers.

Table of Contents

Warranty	3
Disclaimer	3
License	3
Trademarks	3
1 Introduction	
1.1 Welcome to NetSafa Policy Control	6
1.2 Documentation Updates	6
1.3 Operating Systems	6
1.4 Communication Devices	6
2 Installation	
2.1 <i>Server Installation</i>	
2.1.1 Setup	7
2.1.2 Install	7
2.1.3 Welcome	7
2.1.4 License Agreement	8
2.1.5 Installation Folder	8
2.1.6 Browse for Folder	8
2.1.7 Disk Cost	9
2.1.8 Confirm Installation	9
2.1.9 Installing	9
2.1.10 Installation Complete	10
2.2 <i>Client Installation</i>	
2.2.1 Setup	10
2.2.2 Install	10
2.2.3 Welcome	11
2.2.4 License Agreement	11
2.2.5 Installation Folder	12
2.2.6 Browse for Folder	12
2.2.7 Disk Cost	12
2.2.8 Confirm Installation	12
2.2.9 Installing	13
2.2.10 Installation Complete	13
2.3 <i>Windows Media Encoder 9 Installation</i>	
2.3.1 Setup	13
2.3.2 Install	14
2.3.3 Welcome	14
2.3.4 License Agreement	14
2.3.5 Installation Folder	15
2.3.6 Ready to Install	15
2.3.7 Installing	15
2.3.8 Installation Complete	16
3 Server Module	
3.1 Run the Server Module	16
3.2 Login Information	16
3.3 <i>Overview</i>	
3.3.1 Menu Bar	17
3.3.2 File	17
3.3.3 View	17
3.3.4 <i>Tools</i>	
3.3.4.1 Control Panel – Password	18
3.3.4.2 License Key	18
3.3.5 <i>Help</i>	
3.3.5.1 Web Update	19
3.3.5.2 About NetSafa Server	19
3.3.6 Auto Scan	19
3.3.7 <i>Feature Buttons</i>	
3.3.7.1 Scan	20

3.3.7.2	Communicate	
3.3.7.2.1	Communicate – Chat Session	20
3.3.7.2.2	Communicate – Send Message	21
3.3.7.3	Files	
3.3.7.3.1	Files – Send File	21
3.3.7.3.2	Files – Collect File	22
3.3.7.4	Control	
3.3.7.4.1	Control – Shutdown	22
3.3.7.4.2	Control – Restart	23
3.3.7.4.3	Control – Logoff	24
3.3.7.4.4	Control – Run Application	24
3.3.7.4.5	Control – Open Website	25
3.3.7.4.6	Control – Run Command	25
3.3.7.5	Settings	
3.3.7.5.1	Settings – Device Control	26
3.3.7.5.2	Settings – Internet Policy	27
3.3.7.5.3	Settings – Application Policy	29
3.3.7.6	Report	30
3.3.7.7	Record	30
3.3.8	<i>Real-Time Monitoring</i>	
3.3.8.1	Process	32
3.3.8.1.1	Process – Kill	32
3.3.8.2	Internet	32
3.3.8.2.1	Internet – Kill	32
3.3.8.3	Application	33
3.3.8.3.1	Application – Kill	33
3.3.8.4	Device	33
3.3.9	<i>Control Panel</i>	
3.3.9.1	Control	34
3.3.9.2	Protection	35
3.3.9.3	Connection	36
3.3.9.4	Send Message	36
3.3.9.5	Pop-Up Message	37
3.3.9.6	Scan	37
3.3.10	<i>Remote Client Area</i>	
3.3.10.1	Client PC Status	37
3.3.10.2	Short Cut Menu	37
3.3.10.2.1	Active PC	38
3.3.10.2.2	Offline PC	38
4	Client Module	
4.1	Run the Client Module	39
4.2	Taskbar	39
4.3	The Client Module	39
4.4	NetSafa Client Chat	40
5	Uninstallation	
5.1	<i>Server Uninstallation</i>	
5.1.1	Uninstall	41
5.1.2	Welcome	41
5.1.3	Removing	41
5.1.4	Uninstallation Complete	42
5.2	<i>Client Uninstallation</i>	
5.2.1	Uninstall	42
5.2.2	Welcome	42
5.2.3	Removing	43
5.2.4	Uninstallation Complete	43
5.2.5	Restart	43
6	INDEX	44

1 Introduction

1.1 Welcome to NETSAFA Policy Control

NetSafa® Policy Control is centrally-managed security software, allowing and enabling administrators to have control of all the computers running in the network and at the same time, protecting every workstation with a strong policy control. It is the only security software in the market today to heed the call of companies and businesses alike, which are reviewing their processes to ensure strict adherence to the instructions and procedures in place to control access to any particular material.

NetSafa® Policy Control helps IT manager, administrators, school principals/directors, company CEOs, and owners to eliminate threats that so as to prevent misuse of their corporate network systems and servers and also protect individual employee from unintentional misuse that could break the respective law of each country.

This software, apart from all the other features included, isolates 4 main threats, i.e., External Devices, Internet, Processes and Applications. This software is also available in 3 different editions, i.e., Basic, Standard and Professional. For schools, however, only the Professional Edition is available at a discounted rate.

1.2 Documentation Updates

From time to time, NetSafa® Policy Control is improved through the release of updated builds of the product.

Note: The most recently released build of NetSafa® Policy Control should always be installed in order that the installed product is up to the current standard. It can be downloaded from the www.netsafa.com website (Downloads - Latest builds), and installed provided that a valid license number for the downloaded version of the product is specified. NetSafa® Policy Control includes a Web Update facility that can automatically check for updated builds of installed NetSafa® Policy Control products and download and install them.

Updated builds are documented in the 'README.TXT' file that is installed with the updated build and can be opened from the download page in the website.

Help systems and User Manuals will be updated less frequently. When help systems are updated with changes documented in the 'README.TXT' file, they will accompany an updated build.

Updates of User Manuals are designated by a document revision number on page 2 in the format YYYYMMDD (Y=year digit, M=month digit, D=day digit).

1.3 Operating Systems

NetSafa® Policy Control version 2007.2.0 can run on computers using the operating systems Microsoft Windows XP, 2000, and Vista. You may experience insufficient support for Windows Vista as well as the latest service packs on other platforms.

1.4 Communication Devices

NetSafa® Policy Control functionality relies upon sending data packets between networked computers. These communication devices (protocols) are supported:

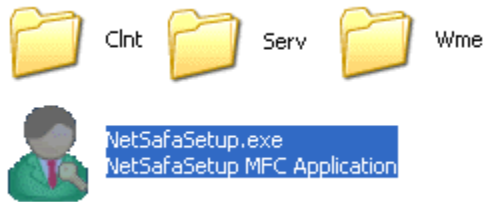
TCP/IP (UDP)

Wireless

2 Installation

2.1 Server Installation

2.1.1 Setup



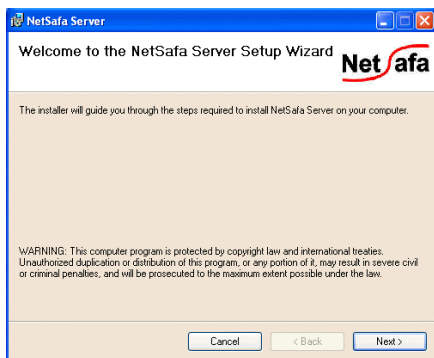
Select NetSafaSetup.exe to run installation in the computer you intended to install the Server module.

2.1.2 Install



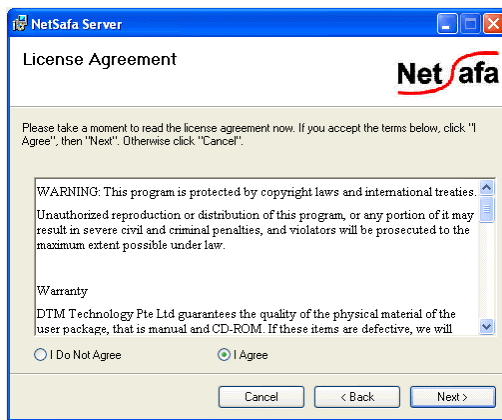
To install the Server module in your computer, select Install Server.

2.1.3 Welcome



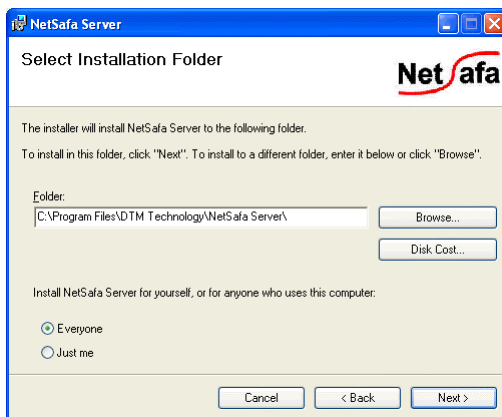
Welcome to the NetSafa Server Setup Wizard.
Click Next to continue.
Click Cancel to cancel installation.

2.1.4 License Agreement



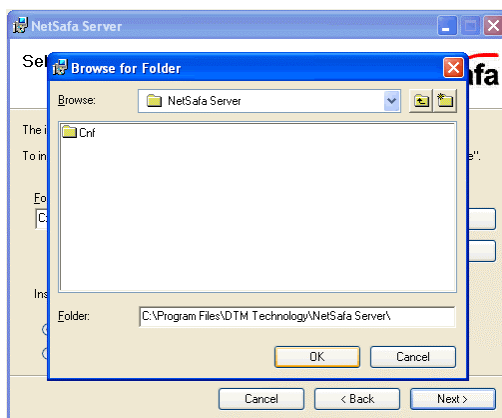
Read the License Agreement carefully.
To continue installation, click the 'I Agree' button.
Click Next.

2.1.5 Installation Folder



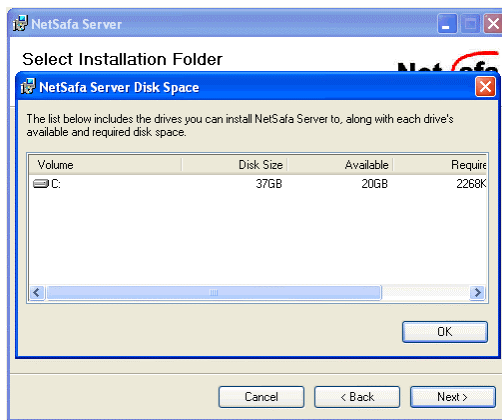
Select the desired Installation Folder. By default, the Server module will be installed in the **C:\Program Files\DTM Technology\NetSafa Server** folder.

2.1.6 Browse for Folder



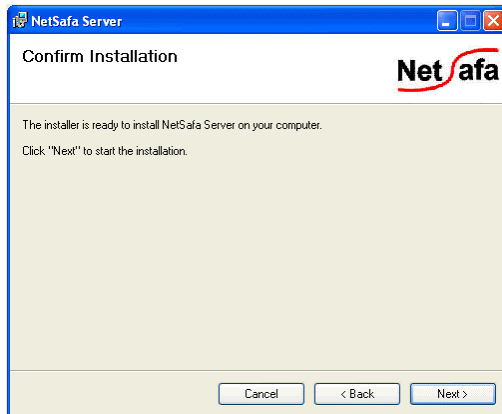
To select a different folder, click the 'Browse' button.
After you have made the changes, click OK.

2.1.7 Disk Cost



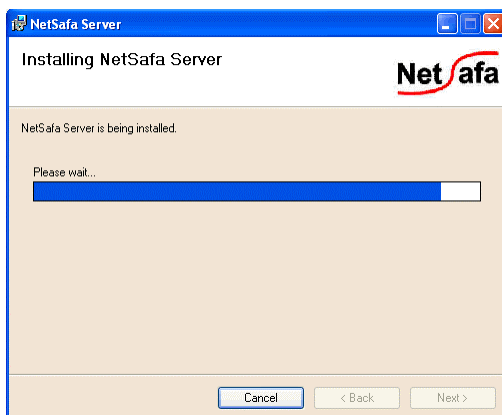
To find out the necessary disk space, click the 'Disk Cost' button. Click OK.

2.1.8 Confirm Installation



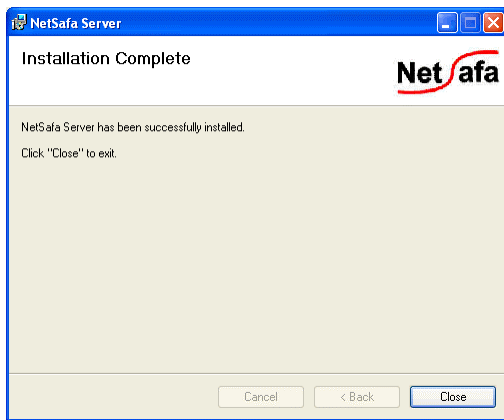
Click Next to confirm installation.

2.1.9 Installing



The wizard will install the Server module. At any point, to cancel installation, click the 'Cancel' button.

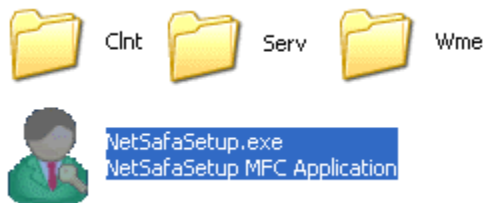
2.1.10 Installation Complete



Installation complete.
Click Close to exit.

2.2 Client Installation

2.2.1 Setup



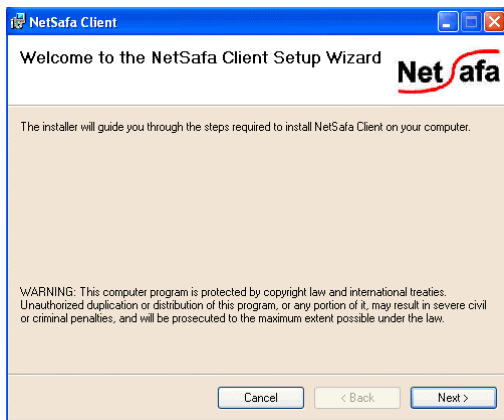
Select NetSafaSetup.exe to run installation in the computer you intended to install the Client module.

2.2.2 Install



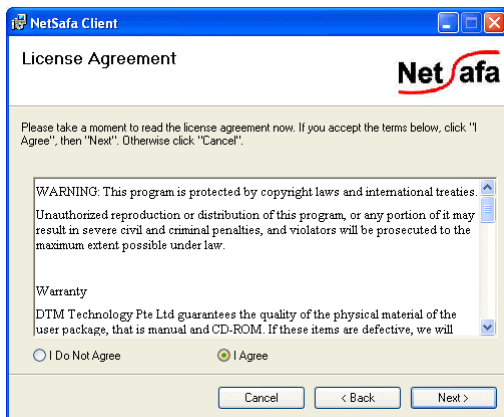
To install the Client module in your computer, select Install Client.

2.2.3 Welcome



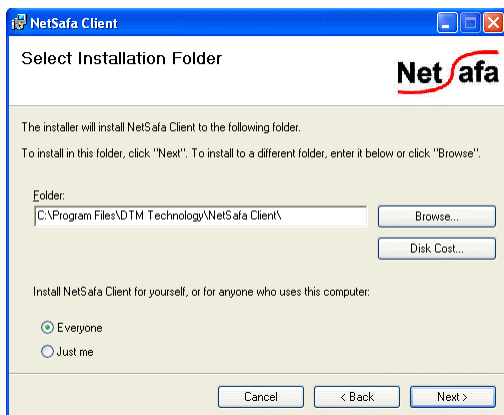
Welcome to the NetSafa Client Setup Wizard.
Click Next to continue.
Click Cancel to cancel installation.

2.2.4 License Agreement



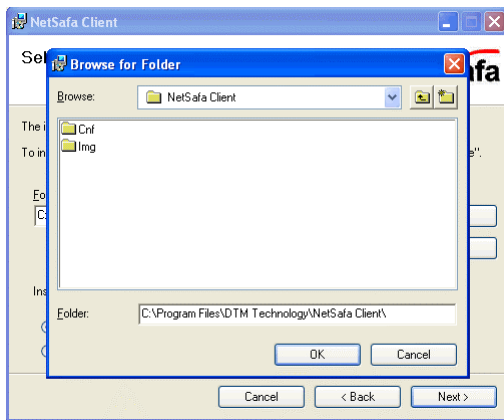
Read the License Agreement carefully.
To continue installation, click the 'I Agree' button.
Click Next.

2.2.5 Installation Folder



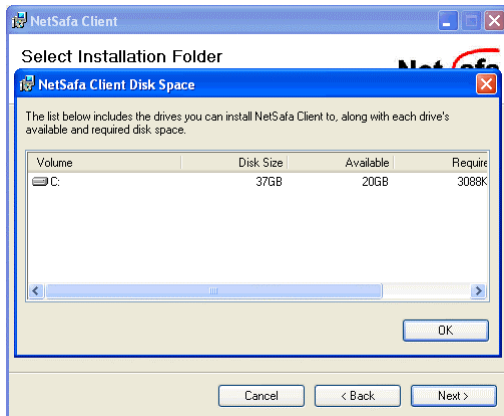
Select the desired Installation Folder. By default, the Client module will be installed in the **C:\Program Files\DTM Technology\NetSafa Client** folder.

2.2.6 Browse for Folder



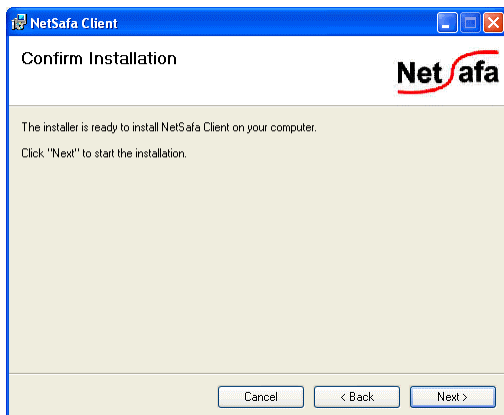
To select a different folder, click the 'Browse' button. After you have made the changes, click OK.

2.2.7 Disk Cost



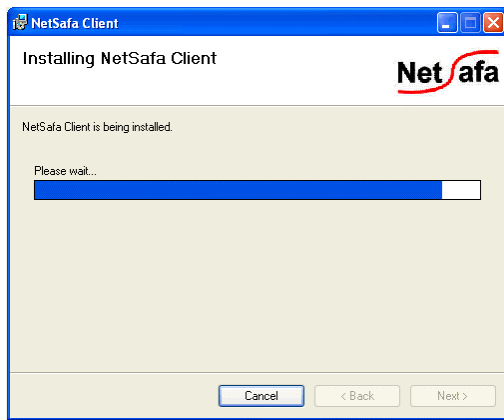
To find out the necessary disk space, click the 'Disk Cost' button. Click OK.

2.2.8 Confirm Installation



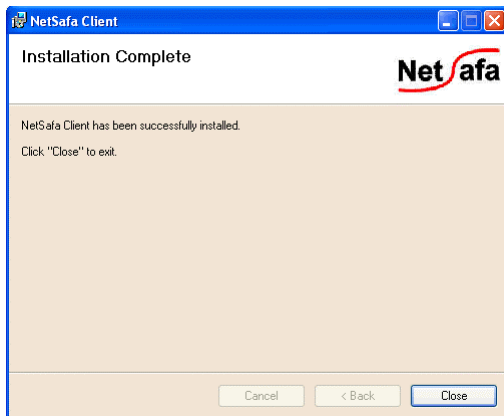
Click Next to confirm installation.

2.2.9 Installing



The wizard will install the Client module. At any point, to cancel installation, click the 'Cancel' button.

2.2.10 Installation Complete

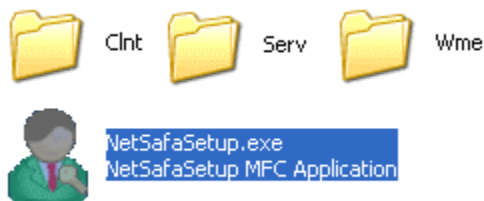


Installation complete.
Click Close to exit.

2.3 Windows Media Encoder 9 Installation

The Windows Media Encoder 9 is a necessary file to install and run in the Client computer in order to run the 'Record' feature in the Professional Edition only. This file is not necessary to be installed if you have the Basic or the Standard Edition, as the 'Record' feature is not available.

2.3.1 Setup



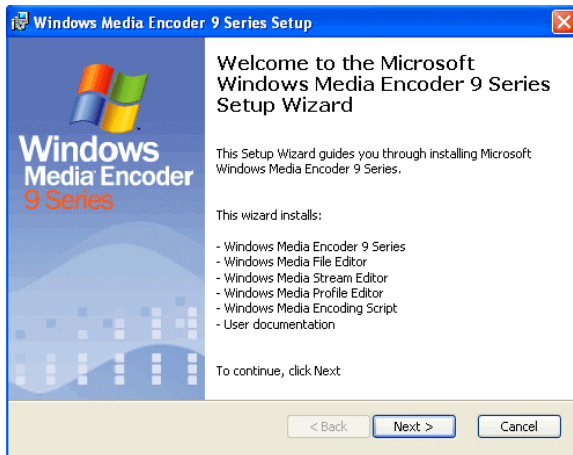
Select NetSafaSetup.exe to install the Windows Media Encoder 9 into the computer that you have installed the Client module.

2.3.2 Install



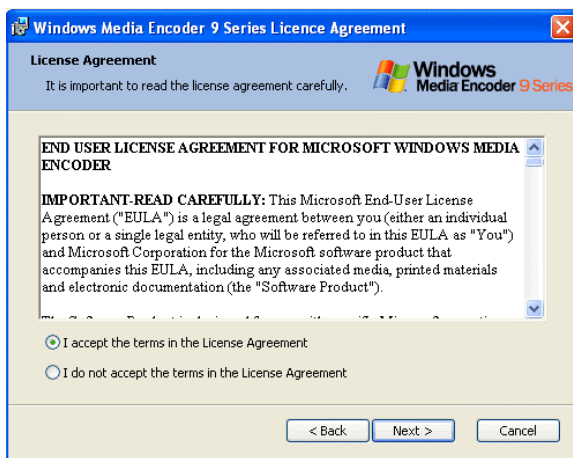
To install the Windows Media Encoder 9 in the computer that you have installed the Client module, select Install Windows Media Encoder 9.

2.3.3 Welcome



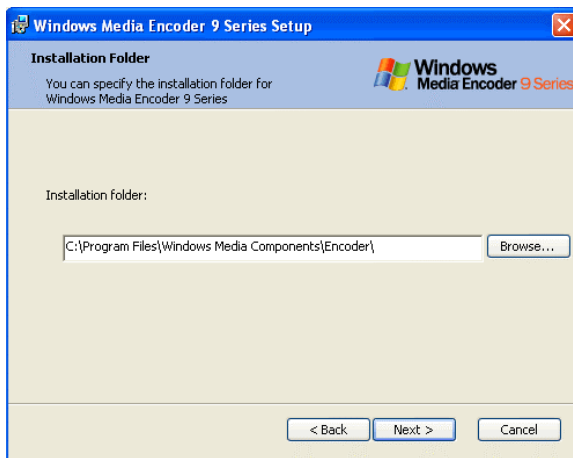
Click Next to continue.

2.3.4 License Agreement



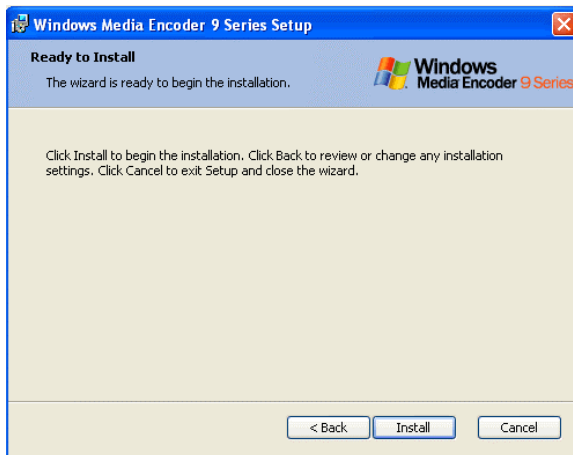
Make sure the "I accept the terms in the License Agreement" is selected. Click Next to continue.

2.3.5 Installation Folder



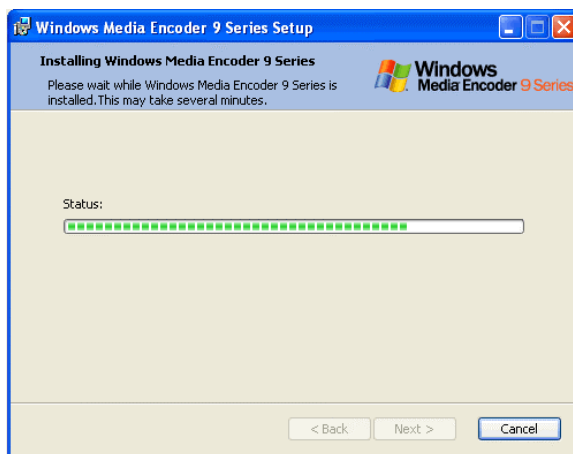
Click Next to install in the default installation folder.
Otherwise, click Browse to define a new installation folder.

2.3.6 Ready to Install



Click Install to begin the installation.

2.3.7 Installing



Installation in progress.
Click Cancel to cancel installation.

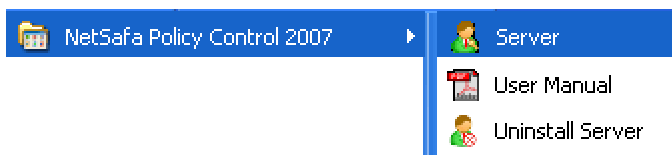
2.3.8 Installation Complete



Click Finish to close Wizard.

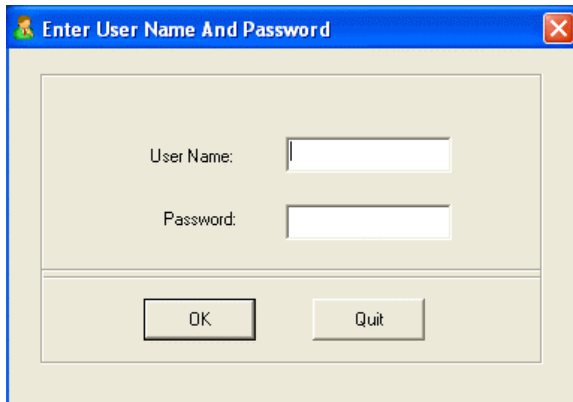
3 Server Module

3.1 Run the Server Module



To run the Server module application, simply select Server in the Start -> All Programs menu.

3.2 Login Information



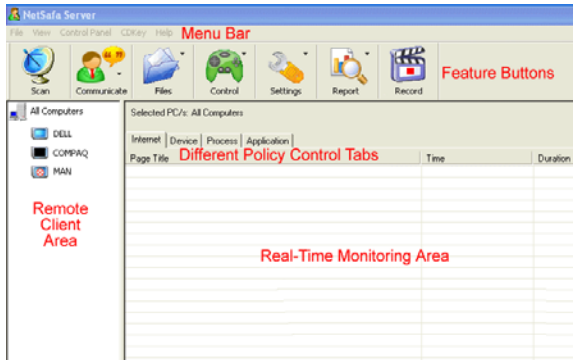
By default,

Username: admin

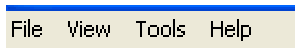
Password: password

You may create a new Username and Password in the Server Control Panel.

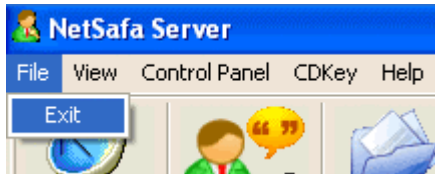
3.3 Overview



3.3.1 Menu Bar



3.3.2 File



Select **File** → **Exit** to exit from NetSafa Server module.

3.3.3 View



Select **View** → **Status Bar** to either enable or disable the status bar.

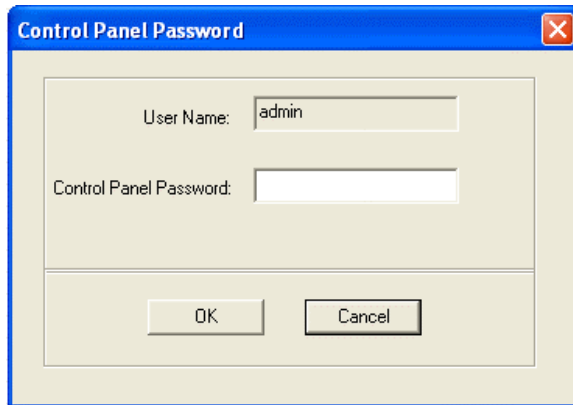


3.3.4 Tools



Select **Control Panel** to configure your Server settings.

3.3.4.1 Control Panel - Password



Enter the Username and Password to enter the **Control Panel**.

By default,

Username: admin

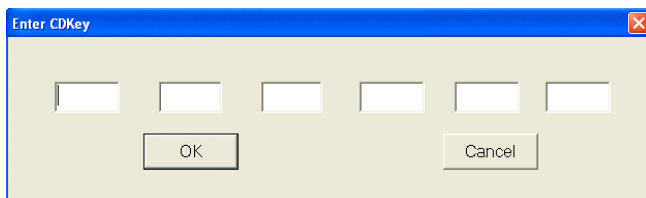
Password: password

SEE SECTION ON CONTROL PANEL 3.3.9 PAGE 33

3.3.4.2 License Key

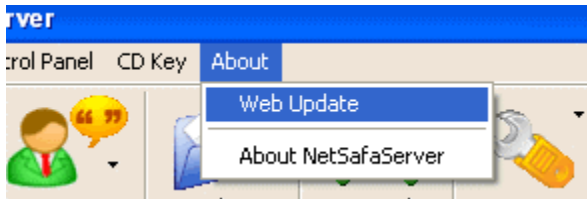


By default, the Free Download software entitled you to 1 Client license only. After you made your purchase to the respective license number, you will be given a license certificate that includes your License Key number. Enter that **License Key** into the boxes below in its correct sequence. Click OK once done.



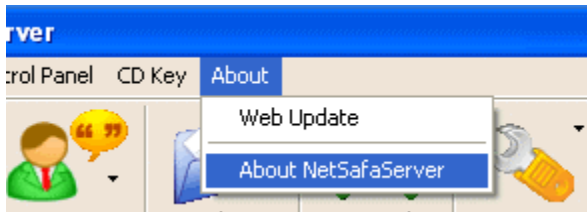
3.3.5 Help

3.3.5.1 Web Update

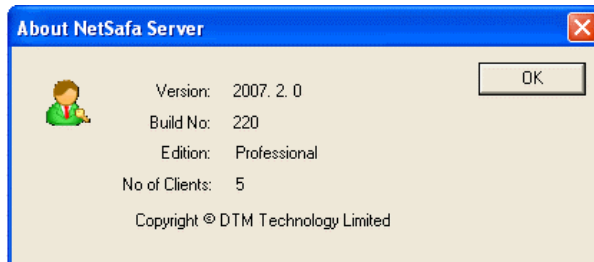


Get the latest builds and updates from NetSafely Web Server with Web Update.

3.3.5.2 About NetSafely Server

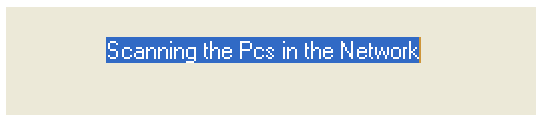


Click **About** → About NetSafely Server to find out your license information.



Click OK to close.

3.3.6 Auto Scan



The Server will automatically scan all the IP addresses available in your network when you start the Server Module.

3.3.7 Feature Buttons



3.3.7.1 Scan



The **Scan** button is to refresh the network scanning.

3.3.7.2 Communicate

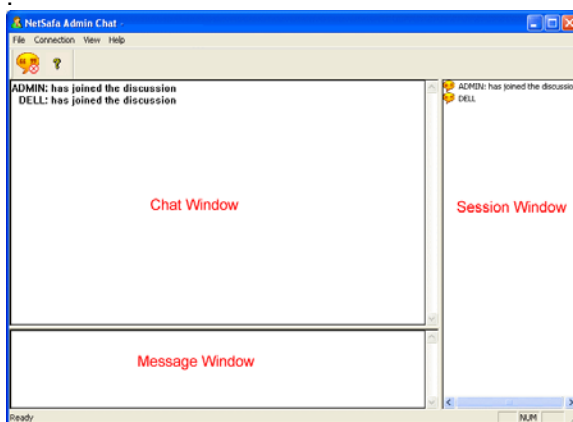


Select the **Communicate** button to open the down menu.

3.3.7.2.1 Communicate – Chat Session



To start a chat sessions with clients, firstly select the Client computer that you want to chat with. Next select **Communicate** → **Start Chat** feature to open the window as follows.



Type in your message in the *Message Window*. Press the Enter key on your keyboard to send the message.

Your message will appear on the *Chat Window*, which is visible to the Client.

The *Session Window* shows which Client computers you are currently in engaging in.

On the client computer, the same Chat window will open at the same time.

To stop the Chat session, click the



button.

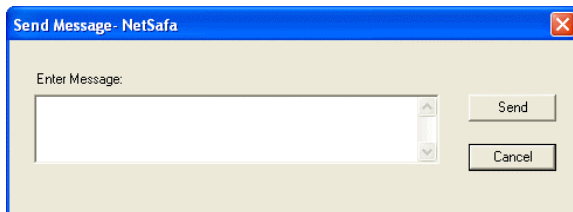
Once you (the Server) decided to close and exit the Chat session, you are automatically asked to save the session.

3.3.7.2.2 Communicate – Send Message



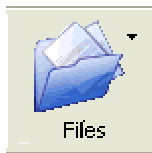
To send messages to clients, firstly select the Client computer that you want to send your message to.

Next select **Communicate** → **Send Message** feature to open the window as follows.



Type in your message in the space provided.
Click Send to send your message.

3.3.7.3 Files



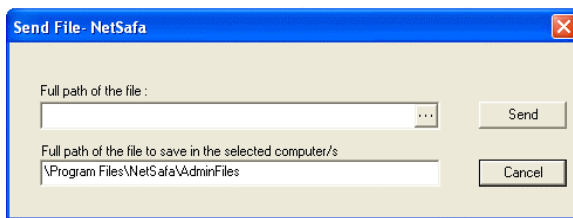
Select the **File** button to open the down menu.

3.3.7.3.1 Files – Send File



Send files to your clients using the Send File feature.

Select **Files** → **Send File** feature to open the window as follows.



Key in the *Full path of the file* to be sent. Click the  button to browse for the file in the Server module.

Select the *Full path of the file* to save in the selected computer.

By default, the file will be sent to *\\Program Files\\NetSafa\\AdminFiles* in the client computer. You may change this to your desired location.

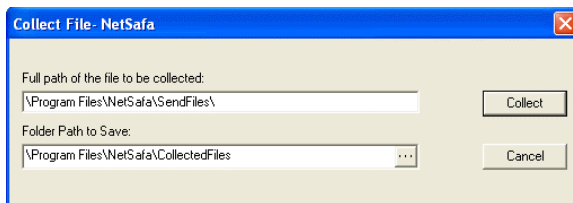
Click Send to send the file.

3.3.7.3.2 Files – Collect File



Collect files from your clients using the Collect File feature.

Select **Files** → **Collect File** feature to open the window as follows.



Key in the full path of the file to be collected.

By default, the file will be collected from *\\Program Files\\NetSafa\\SendFiles* in the client computer. You may change this from the client location.

Select the folder path to save in the Server computer.

By default, the file will be saved in the *\\Program Files\\NetSafa\\CollectedFiles*. Click the  button to browse for another location in the Server module.

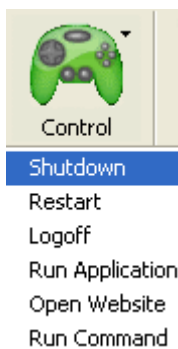
Click Collect to collect the file.

3.3.7.4 Control



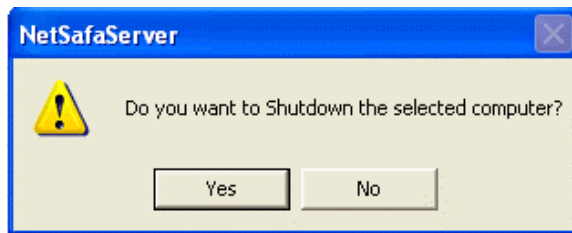
Select the **Control** button to open the down menu.

3.3.7.4.1 Control - Shutdown



To shutdown the client computers, firstly select either one or several or all-available computers in the network.

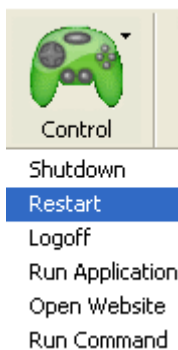
Next select the **Control** → **Shutdown** feature to open the window as follows.



Click Yes to shutdown.

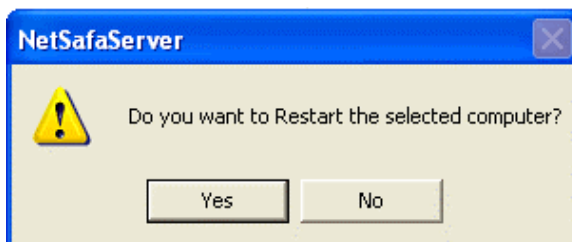
Click No to cancel the operation.

3.3.7.4.2 Control - Restart



To restart the client computers, firstly select either one or several or all-available computers in the network.

Next select the **Control** → **Restart** feature to open the window as follows.



Click Yes to restart.

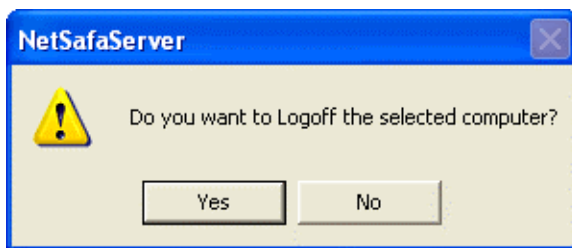
Click No to cancel the operation.

3.3.7.4.3 Control – Logoff



To logoff the client computers, firstly select either one or several or all-available computers in the network.

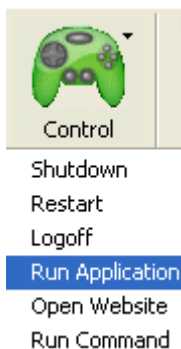
Next select the **Control → Logoff** feature to open the window as follows.



Click Yes to restart.

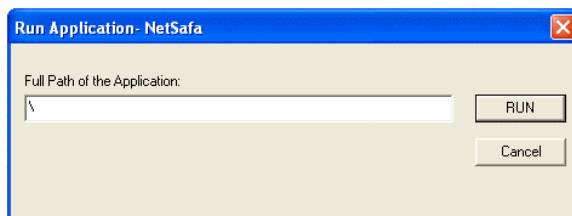
Click No to cancel the operation.

3.3.7.4.4 Control – Run Application



To run applications in the client computers remotely, firstly select either one or several or all-available computers in the network.

Next select the **Control → Run Application** feature to open the window as follows.

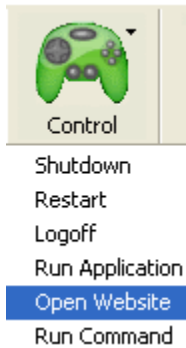


Type in the *Full path of the Application* in the space provided.

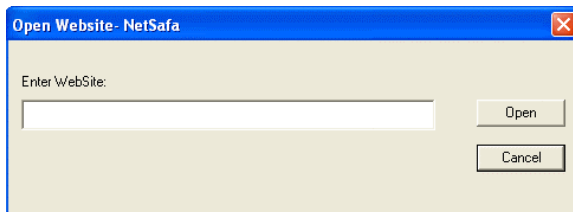
Click the 'Run' button.

***Important:** Make sure the full path of the application residing in the client computer is correct, or else the application will not run. Also make sure the path is not blocked by the Application settings.

3.3.7.4.5 Control – Open Website



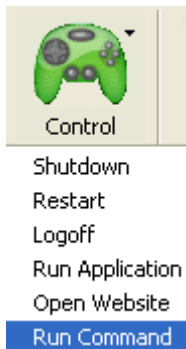
To open websites in the client computers remotely, firstly select either one or several or all-available computers in the network.
Next select the **Control → Open Website** feature to open the window as follows.



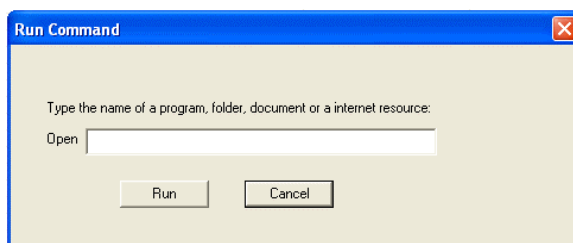
Type in the *URL (web address)* in the space provided.
Click the 'Open' button.

***Important:** Make sure the correct URL is typed or else the website will not open. Also make sure the path is not blocked by the Internet Policy settings.

3.3.7.4.6 Control – Run Command



To run specific command in the client computers remotely, firstly select either one or several or all-available computers in the network.
Next select the **Control → Run Command** feature to open the window as follows.



Type in the name of a *Command* in the space provided.

Click the 'Run' button.

***Important:** Make sure the correct command is typed or else the command will not run. Also make sure the path is not blocked by the Application settings.

3.3.7.5 Settings

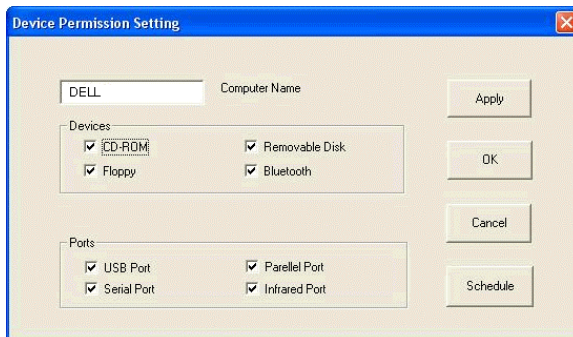


Select the **Settings** button to open the down menu.

3.3.7.5.1 Settings – Device Control



To set Device Settings to client computers, select the **Settings** → **Device Control** feature to open the window as follows.



Computer Name

Name of computer in your network that you have selected to apply the device settings to.

Devices

Current devices that the settings can be applied to.

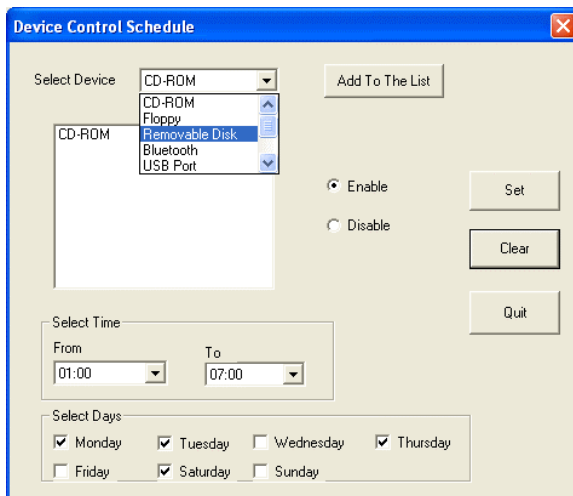
By default, all are selected, i.e. all devices are enabled. To disable, remove the check from respective box. Click the 'Apply' button to apply the settings. Click OK to close the window.

Ports

Current ports that the settings can be applied to.

By default, all are selected, i.e. all ports are enabled. To disable, remove the check from respective box. Click the 'Apply' button to apply the settings. Click OK to close the window.

'Schedule' button is to schedule the time and day to set the settings.



First, select *The Device* and 'Add To The List'.

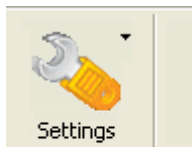
Select either to *Enable* or *Disable* the devices you have added.

Next *Schedule* the time and day.

***Note:** The *From* time cannot be later than *To* time, and *To* time cannot be sooner than the *From* time. Also make sure you select the Week Days to apply the settings to.

Click 'Set' button to set the schedule settings, 'Clear' button to clear the schedule settings.

3.3.7.5.2 Settings – Internet Policy



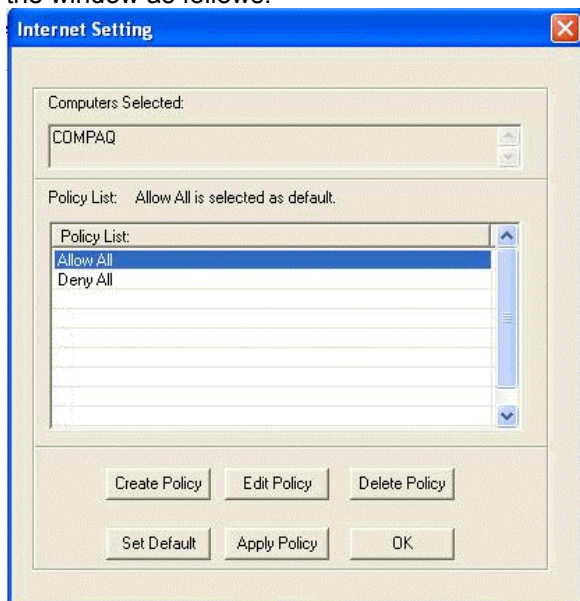
Settings

Device Settings

Internet Policy

Application Policy

To set Internet policy to client computers, select the **Settings → Internet Policy** feature to open the window as follows.



Computers Selected:

Indicates the computers that the Server has selected to apply the policy to.

Policy List:

Shows which policy is the default. Only the Allow All or the Deny All policy can be set as default.

Create Policy:

In the *Create Policy* window, first enter a *Name of the new policy* such as 'Disable yahoo website'.

Next type in the name of the website you want to set the policy. You can even just type in the keyword like google instead of www.goggle.com.

Then click the 'Add' button to add it to the *Except* list.

Next select either to 'Allow All' or 'Deny All' websites except the items in the list.

Click 'OK'.

To delete in the except list, select the item in the except list and click 'Delete'. Or click 'Delete All' button to delete all the items in the except list.

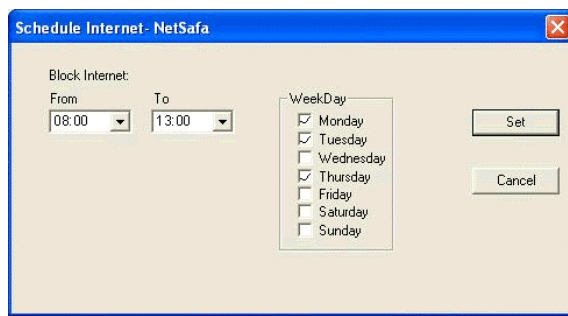
***Note:** The 'Schedule to block internet' button is disable if you select the 'Allow All' or 'Deny All' button. To select the 'Schedule to block internet' button, do not put a check on either the 'Allow All' or 'Deny All' button.

Edit Policy

To edit a policy you have created, select that policy in the *Policy List* and click the 'Edit Policy' button.

***Note:** The 'Allow All' and 'Deny All' policy cannot be edited.

To Schedule to block (Deny All) Internet, check the box and click the button that will open the window as follows.



Select the time and day you want to Block (Deny All) Internet and click 'Set'.

Set Default

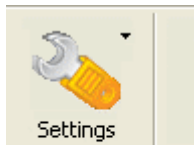
Select the policy you want to set it as default.

***Note:** Only Allow All or Deny All can be set as default.

Apply Policy

Click 'Apply Policy' button after you have selected which policy to apply.

3.3.7.5.3 Settings – Application Policy

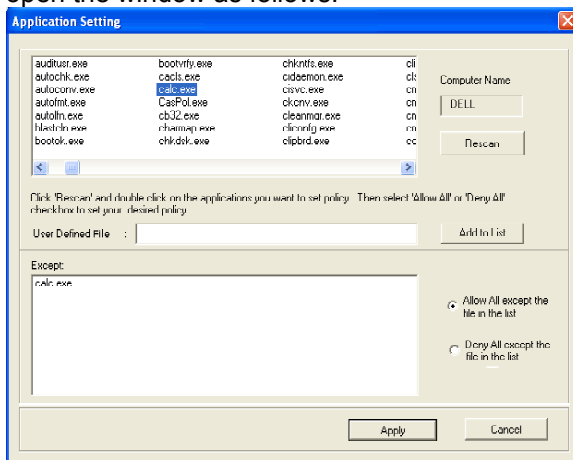


Device Settings

Internet Policy

Application Policy

To set Internet policy to client computers, select the **Settings → Application Policy** feature to open the window as follows.



Computer Name

Name of computer in your network that you have selected to apply the device settings to.

Click 'Rescan' button to scan all the .exe files in the client computer.

Double-click on the .exe file you want to set the policy to.

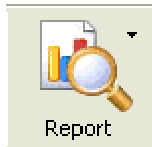
Next select either 'Allow All' or 'Deny All' in the check box.

Click 'Apply' to confirm the settings.

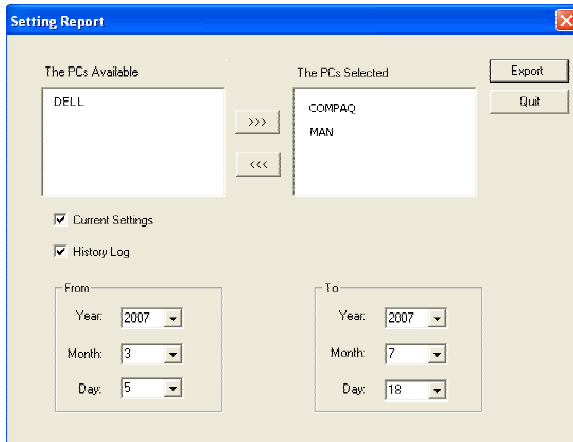
User Define File

This option is for the Server to define any files that you want to set the policy that do not appear in the Rescan area, not necessarily in .exe format.

3.3.7.6 Report



To view the report settings assigned to client computers, select the **Report** feature to open the window as follows.



The PCs Available

These are client computers in your network that are available.

The PCs Selected

Click the  button to move the computers from the *Available* to *Selected* box. To undo, simply select the computer and click the  button.

Current Settings

To view the current settings, put a check on the box.

History Log

This option is to view all the settings taken place prior to the current date. Once you have selected this option, select the *From* and *To* date.

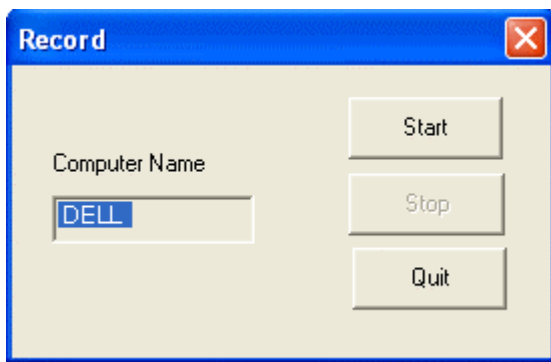
***Note:** The *From* date cannot be later than *To* date, and *To* date cannot be sooner than the *From* date.

Click the 'Export' button once done. The report will be exported as Microsoft Excel .csv format.

3.3.7.7 Record



To record client's screen activities, select the **Record** feature to open the window as follows.

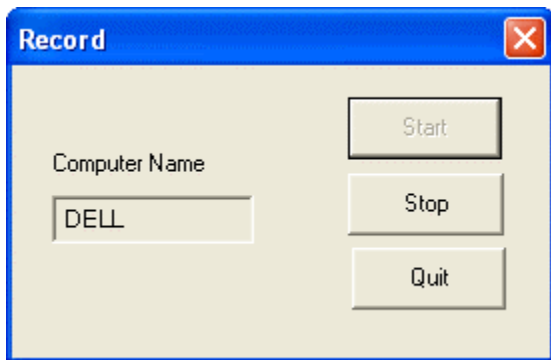


Computer Name

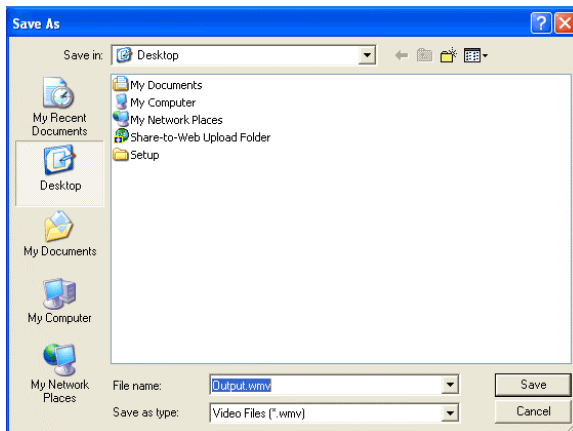
Name of computer in your network that you have selected to record the screen activities.

Click 'Start' button to start the recording.

***Important:** You must install the Windows Media Encoder 9 in the client computers to use this feature. Otherwise, the recording will not function.



Click 'Stop' button to stop all recording sessions.



Once done, you may save the session in Video Files (.wmv) format.

3.3.8 Real-Time Monitoring

3.3.8.1 Process

Selected PC/s: DELL	
Internet	Device
Process	Application
Internet policy selected: NONE	
Process ID	Process Name
0	[System Process]
4	System
1028	smss.exe
1080	csrss.exe
1104	winlogon.exe
1148	services.exe
1160	lsass.exe
1332	svchost.exe
1384	svchost.exe
1420	svchost.exe
1456	EvtEng.exe
1560	S24FvMnn.exe

Select a client computer.

Then select the *Process* tab to view all the current processes that is currently running in that computer in real-time.

3.3.8.1.1 Process – Kill

Selected PC/s: DELL	
Internet	Device
Process	Application
Internet policy selected: NONE	
Process ID	Process Name
0	[System Process]
4	System
1028	smss.exe
1080	csrss.exe
1104	winlogon.exe

During your monitoring of the processes, you are able to terminate the process on the client computer by simply right click your mouse on the process that you want to do so and select '*Kill This Process*'. The process will automatically be terminated at once.

3.3.8.2 Internet

Selected PC/s: DELL		
Internet	Device	Process
Application	Internet policy selected: NONE	
Page Title	Time	Duration
NetScape Security Software - Windows Internet Explorer provided by Yahoo!	13:14:4	0:2:14
Yahoo! Mail - The best web-based email - Windows Internet Explorer pro...	13:14:4	0:2:14

Select a client computer.

Then select the *Internet* tab to view all the current websites that is currently running in that computer in real-time.

Time indicates the time that that particular website is opened.

Duration indicated the length of time that the website has been opened.

3.3.8.2.1 Internet - Kill

Selected PC/s: DELL		
Internet	Device	Process
Application	Internet policy selected: NONE	
Page Title	Time	Duration
NetScape Security Software - Windows Internet Explorer provided by Yahoo!	13:14:4	0:4:5
Yahoo! Mail - The best web-based email - Windows Internet Explorer pro...	13:14:4	0:4:5

During your monitoring of the URL (web address), you are able to terminate the website on the client computer by simply right click your mouse on the website that you want to do so and select '*Kill This Website*'. The website will automatically be terminated at once.

3.3.8.3 Application

Selected PC/s: DELL					
Internet	Device	Process	Application	Internet policy selected: NONE	
Active Window			Application Path	Time	Duration
NetScape Server			NetScapeServer.exe	12:23:14	1:1:35
Fireworks - [Untitled-9.png @ 100%]			Fireworks 4.exe	12:21:13	1:3:56
Internet Manuals			explorer.exe	12:19:9	1:5:48

Select a client computer.

Then select the *Application* tab to view all the current application that is currently running in that computer in real-time.

Time indicates the time that that particular application is running.

Duration indicated the length of time that the application has been running.

3.3.8.3.1 Application - Kill

Selected PC/s: DELL				
Internet	Device	Process	Application	Internet policy selected
Active Window				App
NetScape Server				Net
Fireworks - [Untitled-9.png @ 100%]				Fire
Kill This Application				

During your monitoring of the applications, you are able to terminate the application on the client computer by simply right click your mouse on the application that you want to do so and select 'Kill This Application'. The application will automatically be terminated at once.

3.3.8.4 Device

Selected PC/s: DELL			
Internet	Device	Process	Application
Device Name	Device Type	Total Size	Free Space
Local Disk (C:)	Local Disk	37.21 GB	20.99 GB
(3:) Drive (D:)	(3:) Drive		

Select a client computer.

Then select the *Device* tab to view all the devices that is currently available in that computer in real-time.

Total Size indicates the total space size available in that device.

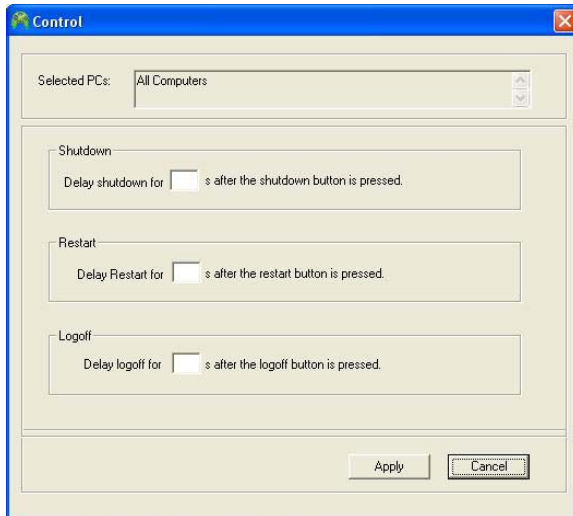
Free Space indicates the total free space available in that device.

3.3.9 Control Panel



3.3.9.1 Control

To change configurations in the Control settings, double-click the icon.



Selected PCs

Name of computer(s) in your network that you have selected.

Shutdown

Enter the time in seconds for the shutdown command delay to take in effect after the shutdown option is selected. This is to prevent loss of data on the client computer before saving can take place.

Restart

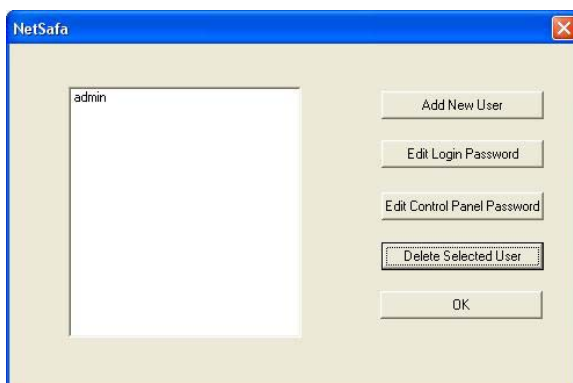
Enter the time in seconds for the restart command delay to take in effect after the restart option is selected. This is to prevent loss of data on the client computer before saving can take place.

Logoff

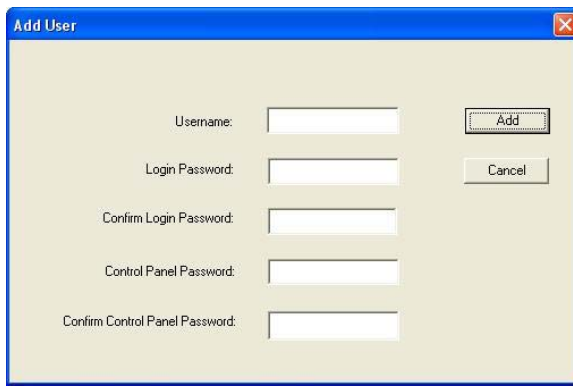
Enter the time in seconds for the logoff command delay to take in effect after the logoff option is selected. This is to prevent loss of data on the client computer before saving can take place.

3.3.9.2 Protection

To add and/or edit users and passwords, double-click the icon.



Add New User



The 'Add User' dialog box has a blue title bar with the text 'Add User' and a close button. The main area is light beige. It contains five text input fields arranged vertically, each with a label to its left: 'Username:', 'Login Password:', 'Confirm Login Password:', 'Control Panel Password:', and 'Confirm Control Panel Password:'. To the right of the first two fields are two buttons: 'Add' (positioned to the right of the Username field) and 'Cancel' (positioned to the right of the Login Password field).

Type in the information, then click 'Add' to add user.

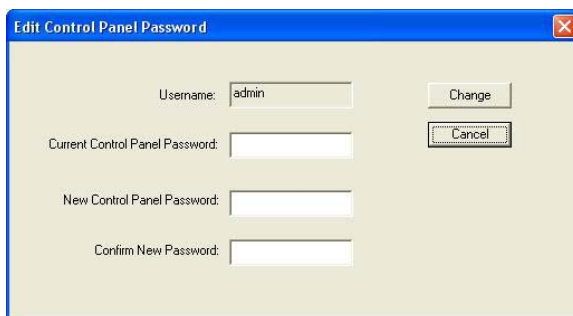
Edit Login Password



The 'Edit Login Password' dialog box has a blue title bar with the text 'Edit Login Password' and a close button. The main area is light beige. It contains four text input fields arranged vertically, each with a label to its left: 'Username:', 'Current Login Password:', 'New Login Password:', and 'Confirm New Password:'. The 'Username' field contains the text 'admin'. To the right of the first two fields are two buttons: 'Change' (positioned to the right of the Username field) and 'Cancel' (positioned to the right of the Current Login Password field).

Select the Username in the main window, then click 'Edit Login Password' button. After you have create new login password, click 'Change'.

Edit Control Panel Password

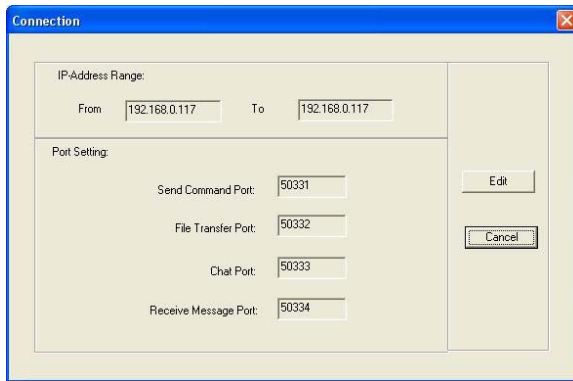


The 'Edit Control Panel Password' dialog box has a blue title bar with the text 'Edit Control Panel Password' and a close button. The main area is light beige. It contains four text input fields arranged vertically, each with a label to its left: 'Username:', 'Current Control Panel Password:', 'New Control Panel Password:', and 'Confirm New Password:'. The 'Username' field contains the text 'admin'. To the right of the first two fields are two buttons: 'Change' (positioned to the right of the Username field) and 'Cancel' (positioned to the right of the Current Control Panel Password field).

Select the Username in the main window, then click 'Edit Control Panel Password' button. After you have create new control panel password, click 'Change'.

3.3.9.3 Connection

To change the connection settings, double-click the icon.



IP-Address Range

This is the IP address range that you want the Server to scan.
Click 'Edit' to change.

Port Settings

By default, the Port Settings are as such:

Send Command Port: 50331

File Transfer Port: 50332

Chat Port: 50333

Receive Message Port: 50334

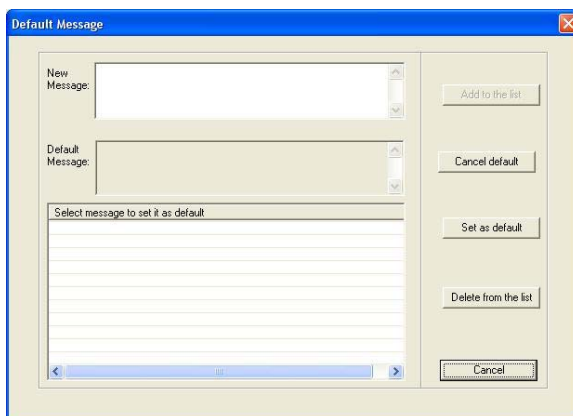
Click 'Edit' to change.

***Important:** Do not change these settings unless the settings are already in use in your company premises. Unauthorized changes can result in the software not functioning properly.

3.3.9.4 Send Message

Send Message

To change the default send messages, double-click the icon.



To create a default message to be sent via Send Message feature, type in your message in the **New Message**.

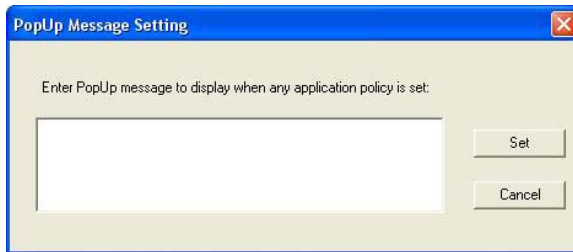
Click 'Add to List'.

You may add in a many messages as you want and you may select anyone as default.

Pop-Up Message

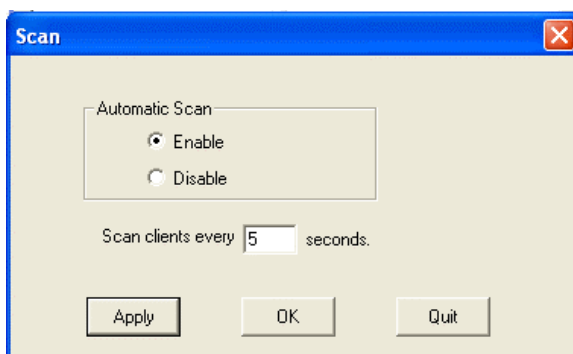
To change the default settings, double-click the icon.

3.3.9.5 Pop-Up Message



Type in the popup message you want to appear on the client computer when the application policy is applied.

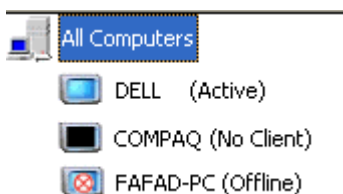
3.3.9.6 Scan



Select 'Enable' to allow the server module to auto scan the Client PCs every few seconds, which you are able to customize. Selecting 'Disable' will allow you to manually scan the Client PCs at your own discretion.

3.3.10 Remote Client Area

3.3.10.1 Client PC Status

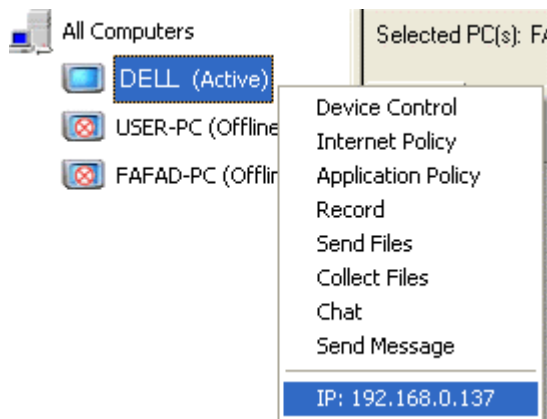


You are able to view all status of the Client PCs:

-  Active – The Client PC is currently logon with the NetSafa client module running.
-  No Client - The Client PC is not installed with the NetSafa client module
-  Offline - The Client PC is currently not logon, but has the NetSafa client module installed.

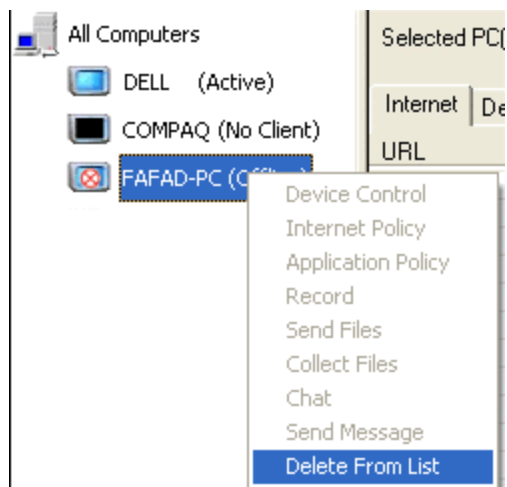
3.3.10.2 Short Cut Menu

3.3.10.2.1 Active PC



Right click on the Active Client PC and a short cut menu pops up. You are able to select all the functions and view the current IP address.

3.3.10.2.2 Offline PC



Right click on the Offline Client PC and you are able to delete it from the list.

4 Client Module

4.1 Run the Client Module



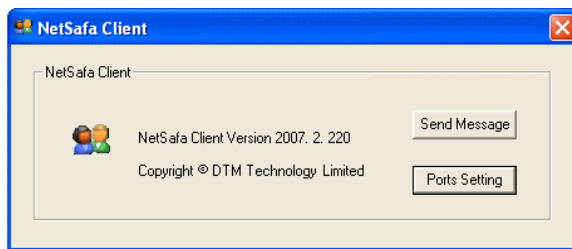
To run the Client module application, simply select Client in the Start -> All Programs -> NetSafa Policy Control 2007 menu.

4.2 Taskbar



Once you run the Client module, it will automatically hide in the taskbar. To open the module, simply double-click the  icon.

4.3 The Client Module



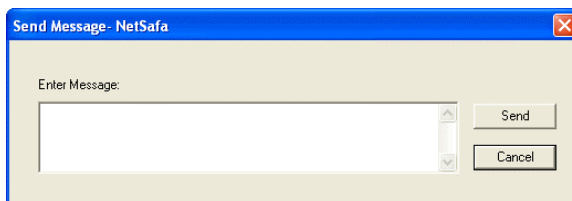
NetSafa Client

Information about the License Version (2007.2) and Build Number: 220

***Note:** 'Send Message' button is disabled as it is waiting for the Server module to be active.

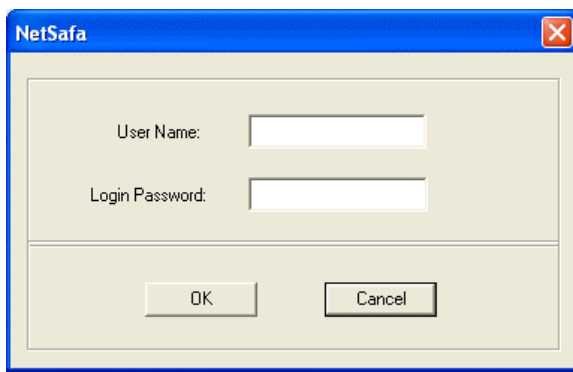
Once the Server Module is active, the 'Send Message' button is enabled.

To send message or HELP request to the Server, click the 'Send Message' button, which will open the window as follows.

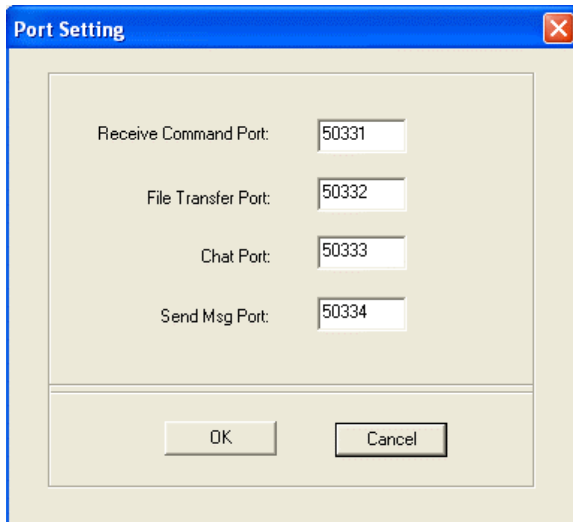


Type in your message in the space provided.
Click Send to send your message.

Click the 'Port Setting' button to set the port settings according the Server module. It will automatically be updated once the Server changes its ports settings. However, should the settings did not take place automatically, the IT Manager has the power and rights to set the settings on individual client computers as it is protected.



Type in the User Name and Password as set in the Server Module. Click OK.



By default, the Port Settings are as such:

Receive Command Port: 50331

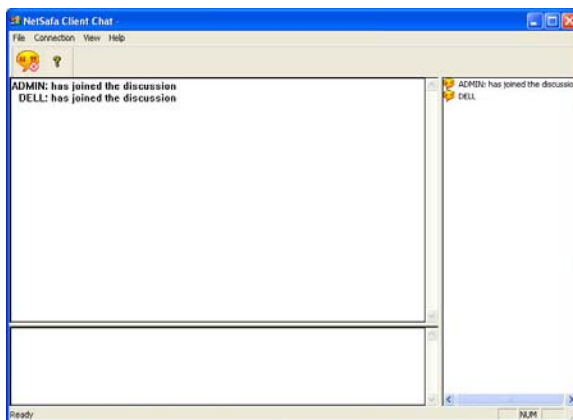
File Transfer Port: 50332

Chat Port: 50333

Send Message Port: 50334

***Important:** Do not change these settings unless the settings are already in use in your company premises. Unauthorized changes can result in the software not functioning properly.

4.4 NetSafa Client Chat



When the Server has selected a particular Client to start chat with, this dialog window will open automatically in that client computer, and can begin to chat with the Server.

5 Uninstallation

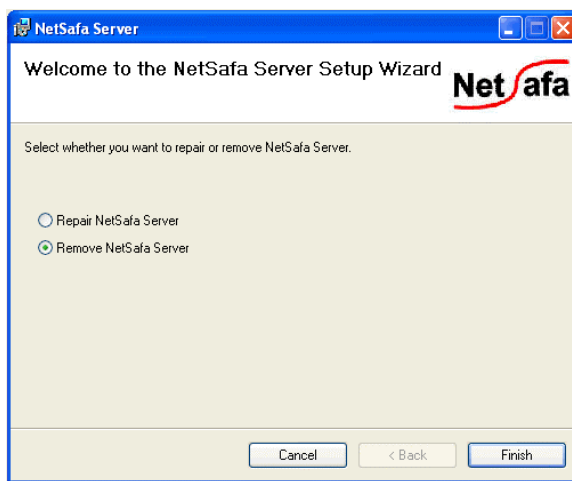
5.1 Server Uninstallation

5.1.1 Uninstall



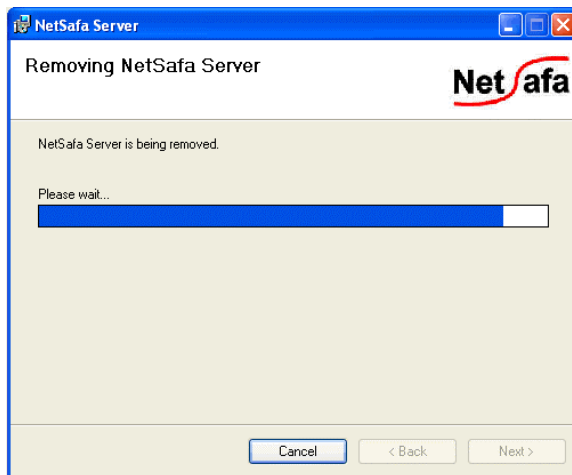
Select Uninstall Server.

5.1.2 Welcome



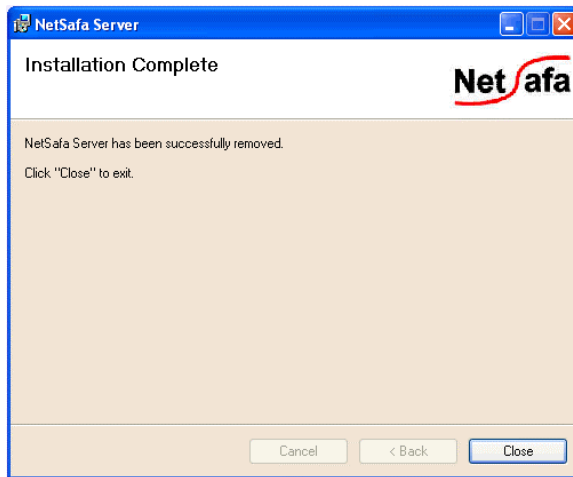
Click *Remove NetSafa Server*.
Click 'Finish'.

5.1.3 Removing



Please wait while the Server module is being removed from your computer.

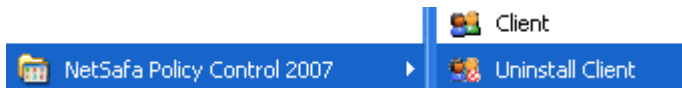
5.1.4 Uninstallation Complete



Click 'Close' to exit.

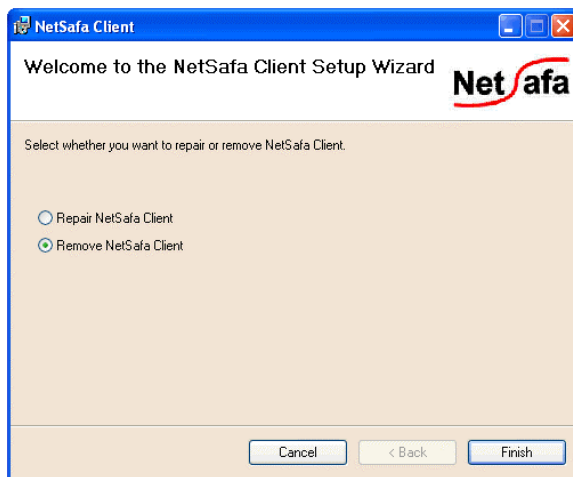
5.2 Client Uninstallation

5.2.1 Uninstall



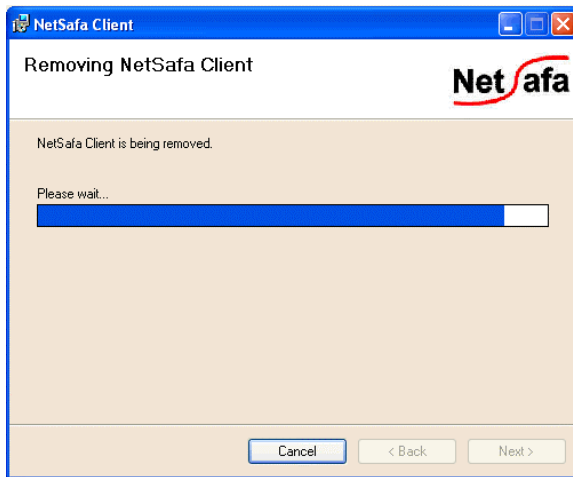
Select Uninstall Client.

5.2.2 Welcome



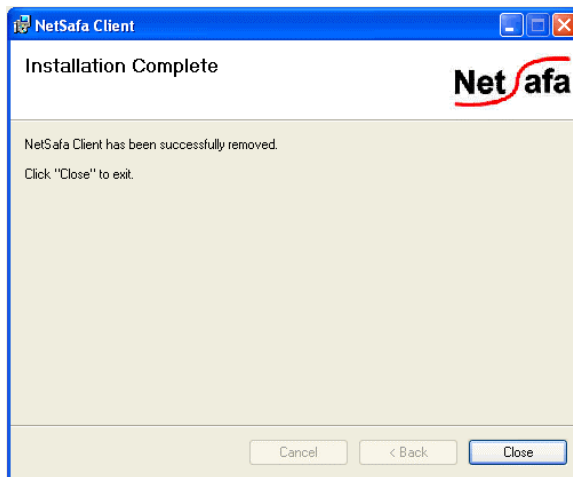
Click *Remove NetSafa Client*.
Click 'Finish'.

5.2.3 Removing



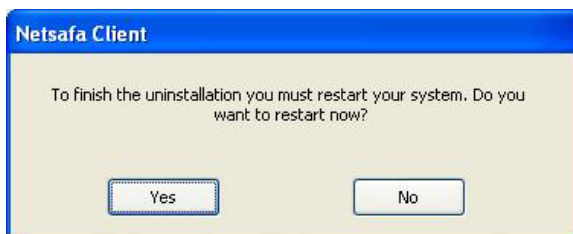
Please wait while the Server module is being removed from your computer.

5.2.4 Uninstallation Complete



Click 'Close' to exit.

5.2.5 Restart



Click 'Yes' button to restart your system in order to finish the uninstallation.

***Important:** Without restarting, the client file may still be running in your system. Thus it is advisable to restart your system.

6 Index

A

About
 NetSafa Server 19
Auto Scan 19
Application
 Monitoring 33

B

C

Control Panel 18, 34
Communicate
 Button 20
Control
 Button 22
Client 10, 39, 42

D

Device
 Monitoring 33

E

F

File
 Menu 17
Files
 Button 31

D

H

I

Installation
 Server 7
 Client 10
 Windows Media Encoder9 13

J

K

L

Login
 Information 32
License
 Key 18

M

Menu
 Bar 17

N

O

Overview
 Server 17

P

Process
 Monitoring 32

Q

R

Report 30
Record 30

S

Server 16
Scan 20
Settings
 Buttons 26

T

Tools 18

U

V

View 17

W

X

Y

Z