CHAPTER

13

Useful Utilities

This chapter discusses some advanced level features and utilities that could help administrator to maximize system performance in a security network.

Dynamic DNS

The Dynamic DNS is an application that allows users to register domain names that always point to their GV-systems. This application is only necessary when your GV-system is using a dynamic IP address. If so, the DDNS will update GV-system's IP address to DNS Server in every 10 minutes. Therefore, even if your GV-system's IP address changes, you can still locate it by using the registered domain name.

Dynamic DNS supports Windows XP, Windows 2000, and Windows Server 2003 only, but not supports Windows 95/98 or ME.

Dynamic DNS uses ports 80 and 81 to upload IP address over the Internet. If your GV-system is connected behind a router or firewall, make sure port 80 and 81 are open. Dynamic DNS will only upload global IP addresses. If your GV-system is using virtual IP, NAT port mapping should be done first.

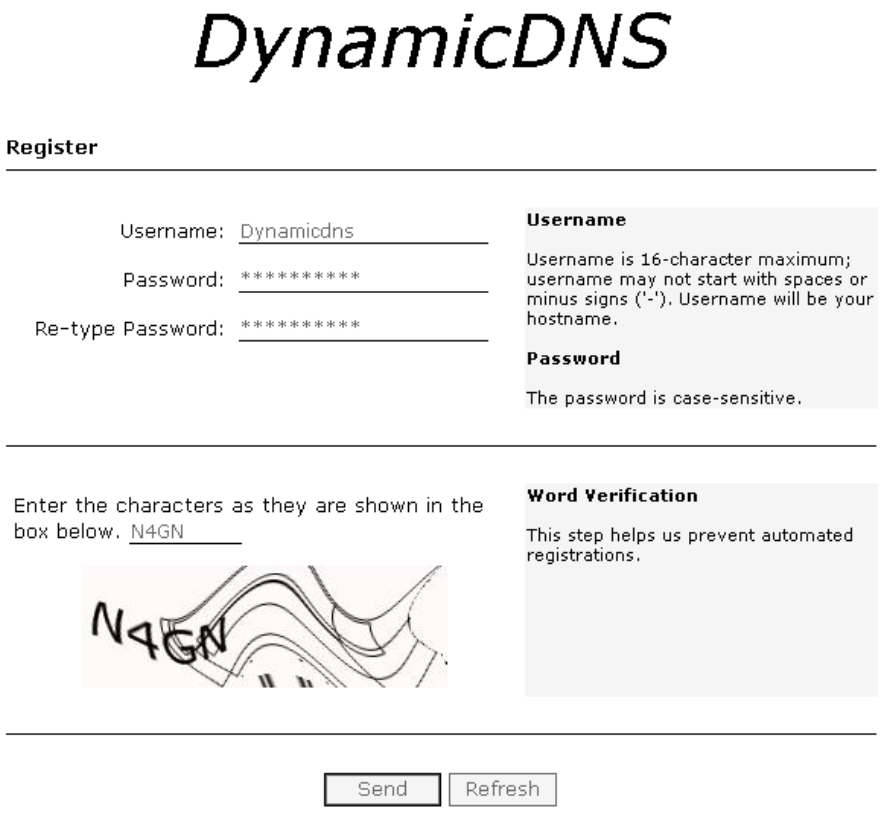
Installing Dynamic DNS

To install Dynamic DNS, follow these steps:

1. Insert the installation CD to your PC. It will automatically run and pop up a window.
2. Select the item of Install Version 7.0 system.
3. Select Dynamic DNS Service in the Install Program 2nd menu, and follow the on-screen instructions. See Figure 1-15.

Registering Domain Name with DDNS

1. Run DNS Client.exe from the system folder to bring up the DNS Client dialog box. Click Register and the following Dynamic DNS register page will appear.
2. Input a username in the Username field. Username can be up to 16 characters. Username will accept “a ~ z”, “0~9”, and “-“, but will not accept space or “-“ as the first character.
3. Enter a password in the Password field. Passwords are case-sensitive and must be at least 6 characters. Re-enter the password in the Re-Type password field for confirmation.
4. In the Word verification section, enter the code within the box. In this example, the code you should enter is *N4GN*. Word verification is not case-sensitive.



5. Click the Send button, and the system will display the following message if the registration is completed successfully.

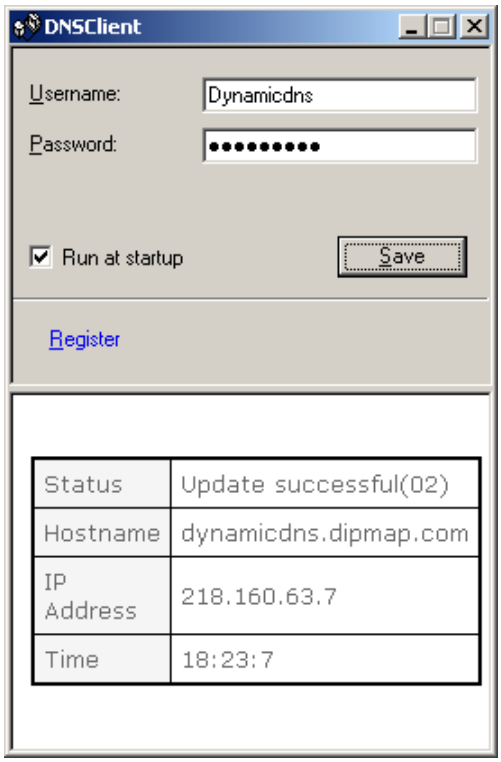
Username: The username you registered. In this example the username is “dynamicdns”

Hostname: The hostname you created. Hostname is made by registered username and “dipmap.com”. In this example the host name is “ http://dynamicdns.dipmap.com ”. This will be the domain name you use for login to GV-system.

IP Address: Your GV-system’s current IP address. This IP address will be updated every 10 minutes.

In DNS Client interface, enter the registered username and password then press the [Save] button. The system will show the connection information as illustrated below. The DNS Client AP is now activated. However, it will not upload IP address unless one of the following applications is running: the main system, Center V2, VSM, Dispatch Server, Twin DVR, and SMS Server. If the IP address of your GV-system is not updated for more than 30 days, your host name will be deleted automatically.

Enable “Run at startup” if you wish to auto run Dynamic DNS AP on the next Windows start-up.



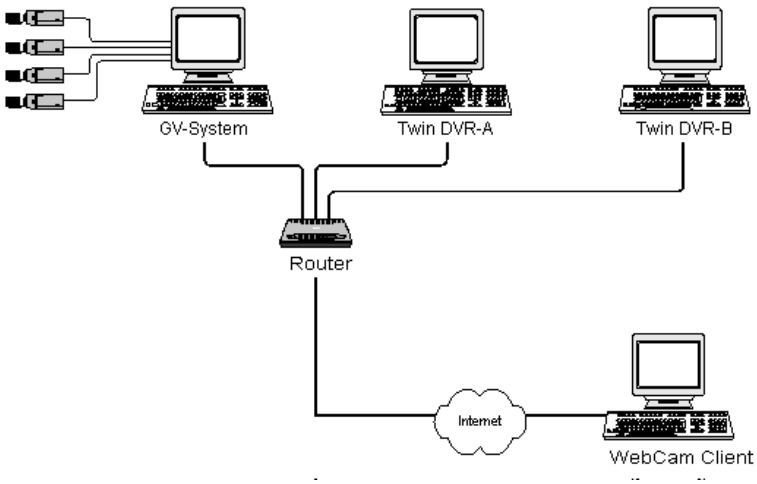
TwinDVR System

TwinServer is an external application that helps sharing the networking liability from the GV-system. A complete TwinServer concept requires at least two computers: a TwinServer, which should be run on the computer where GV-system is installed, and a TwinDVR, which should be run on a separated computer connected to the same LAN as the TwinServer. The TwinServer sends video stream to TwinDVR, while TwinDVR acts as a WebCam Server and serves all WebCam clients over the Internet. One TwinDVR can serve approximately 200 channels over the Internet. Multiple TwinDVRs can be added to the network as online traffic increases.

There are two ways to connect TwinServer and TwinDVR: TCP/IP mode and Multicast mode. Both have its advantages and disadvantages; choose the one that suits your application mostly.

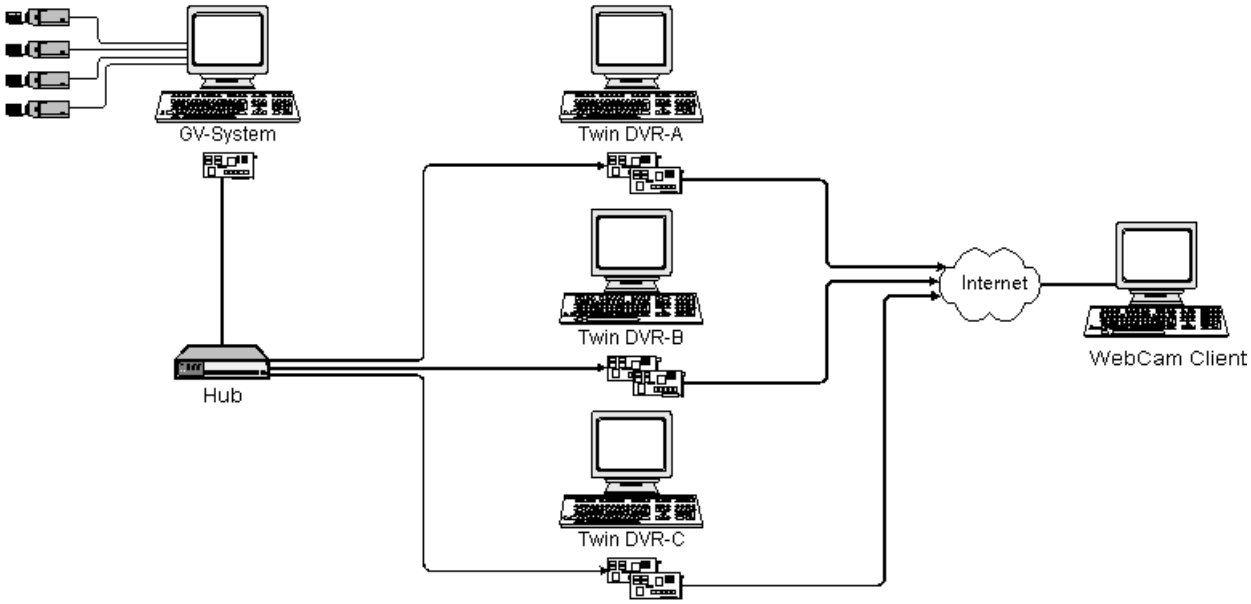
TCP-IP Mode

TCP/IP is a simpler and cost-effective solution. In the TCP/IP mode, the TwinServer and TwinDVRs are connected in a point-to-point connection. It means that video streams are sent from TwinServer to TwinDVR-A, then TwinDVR-A duplicates the video streams and sends them to TwinDVR-B. If the connection between TwinServer and TwinDVR-A is broken, TwinDVR-B will not be able to receive video streams as well.



MultiCast Mode

Multicast Network is more complicated and expensive to setup. In the Multicast mode, the TwinServer transmits video streams in packets to a virtual buffer of the Multicast network. The virtual buffer then broadcasts the video streams to all TwinDVRs under the network. Each TwinDVR should be installed with two network cards. One is for the hub where TwinServer is plugged in, and the other for a DSL or ISDN modem with dedicated ISP service to the Internet. Each TwinDVR serves its own group of WebCam Clients.



Starting TwinServer

1. In the main system, click the Network button, and then select TwinServer. This TwinServer setup dialog box appears.

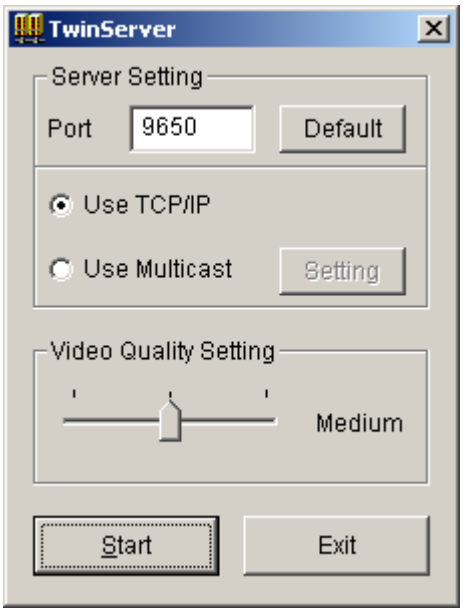


Figure 13-1 *TwinServer Settings*

2. The default port 9650 is for video transmission. Keep it as default or modify it if necessary.
3. Select the type of network to be used: Use TCP/IP or Use Multicast. If Use Multicast is enabled, click the Setting button to display Multicast Setting dialog box. See *Multicast Settings* below.
4. Use the Video Quality Setting slider to adjust video quality for Low, Med, or High.
5. Click the Start button to activate the TwinServer.

Multicast Settings

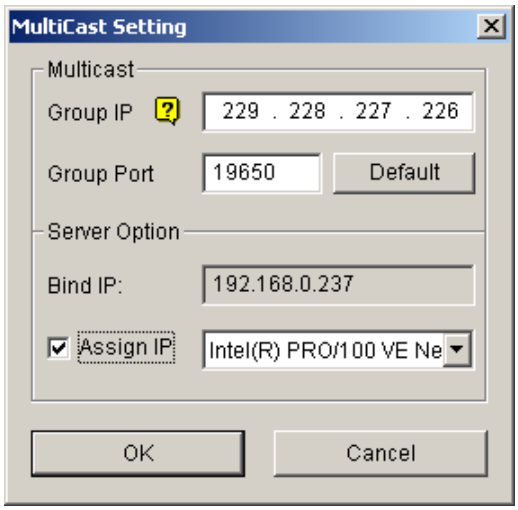


Figure 13-2 *MultiCast Settings*

[MultiCast]

- **Group IP:** Displays the IP address for the virtual buffer that stores the video streams in Multicast network.
- **Group Port:** Used for transferring video streams over the Multicast network.

[Server Option] Only necessary if your GV-system is installed more than one network card. Enable Assign IP and select one network card. This will automatically bring up Blind IP of the network card.

Installing TwinDVR

The TwinDVR is included in the installation CD. This application should be installed in a separate PC within the same Local Area Network as the TwinServer. Before the installation, make sure your PC meets the following minimum system requirements:

OS	Win 2000, XP, Server2003
CPU	Pentium4 2.0GHz (minimum)
Memory	256 MB RAM
Hard Disk	40 GB (minimum)
VGA	NVIDIA GeForce II 32MB
Network	TCP/IP

1. Insert the installation CD to the PC where TwinDVR will be installed.
2. Select the Install Version 7.0 system item from the pop-up window.
3. Select the TwinDVR system item, and follow the on-screen instructions. Refer to Figure1-15. During the installation, you may be prompted to install GeoMPEG4 codec; simply press Yes.

Starting TwinDVR

1. Run TwinDVR.exe. This displays the TwinDVR dialog box.

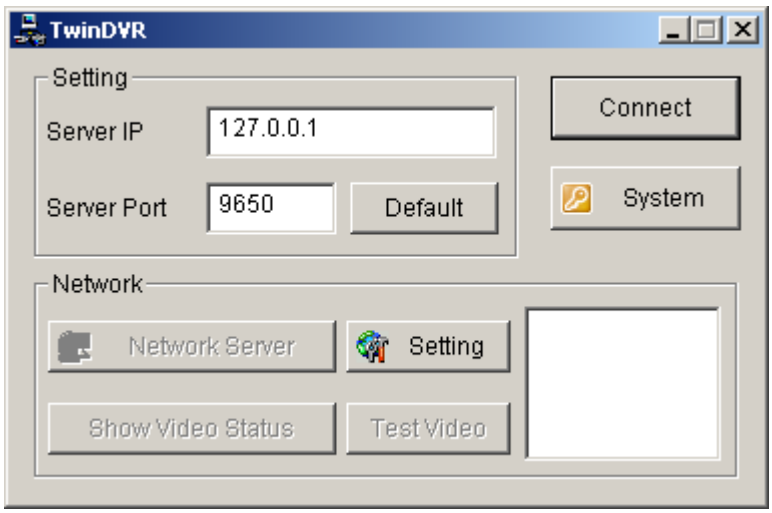


Figure 13-3 *TwinDVR Setup*

2. Input the IP address of TwinServer in the Server IP field.
3. Keep the server port in default, or it should match the TwinServer port. See Figure 13-1.
4. Click the Connect button to establish the connection between TwinDVR and TwinServer. A valid user ID and password are required.

If the connection is established, the Network Server, Show Video Status, and Test Video buttons will be available. You can now use them to set up TwinDVR for:

- Testing Video Stream
- Starting WebCam Server at TwinDVR
- Setting Multiple TwinDVRs in TCP/IP Mode
- Setting Multiple TwinDVRs in Multicast Mode

Testing Video Stream

This function allows you to test the video transmission between TwinServer and TwinDVR. Click the Show Video Status button to display 16 monitoring windows beneath the TwinDVR dialog box. Click the Test Video button and video streams from the connected TwinServer will be streamed to the monitoring windows for 10 seconds. You may click the Hide Video Status button to close the monitoring windows.

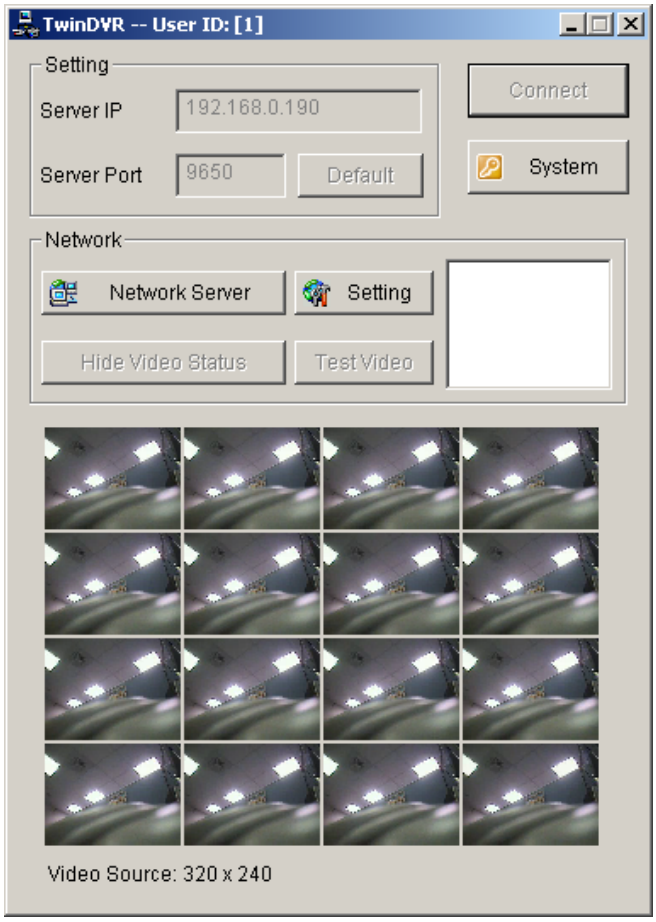


Figure 13-4 *Testing Video Stream*

Starting WebCam Server at TwinDVR

Click the Network Server Button, and then select WebCam Server to display the Server Setup dialog box. See the same dialog box in Chapter 6, Figure 6-1.

Setting Multiple TwinDVRs in TCP/IP Mode

Click the Network Server button, and then select Extended Server. The Extended Server is to duplicate TwinServer's video stream and transmit it to the next TwinDVR in the same network. If there are five TwinDVRs in the network, you should activate the Extended Server function in TwinDVR 1, 2, 3, and 4 respectively. It's not necessary to activate TwinDVR 5 since there are no more TwinDVR running behind it.

Setting Multiple TwinDVRs in Multicast Mode

Click the Network Server button, and then select Use Multicast Mode. The Multicast mode is now activated. The Multicast Server is to instruct TwinDVR to obtain video streams from the virtual buffer. If there are five TwinDVRs connected to the network, all TwinDVRs will be required to select the Use Multicast Mode option.

TwinDVR Settings

Network Card Settings

In Figure 13-3, click the Setting button, and then select Network Setting to display the following dialog box. This option is necessary when your TwinDVR has more than one network card. Enable Assign IP and select one network card. This will automatically bring up Blind IP of the network card. The network card will be used for connecting to TwinServer; the other network card will be assigned for connecting to Internet.

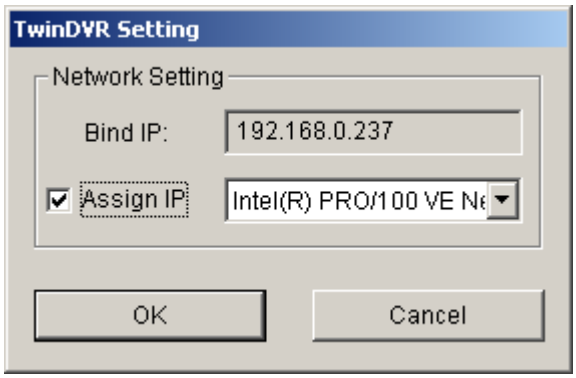


Figure 13-5 *TwinDVR Setting*

System Settings

In Figure 13-3, click the Setting button, and then select System Configure to display the following dialog box. The option is only available when TwinDVR is connecting to TwinServer.

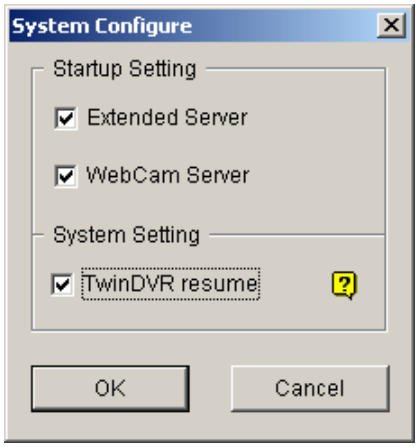


Figure 13-6 *System Settings*

[Startup Setting]

- **Extended Server:** Activates Extended Server on TwinDVR startup.
- **WebCam Server:** Activates WebCam Server on TwinDVR startup.

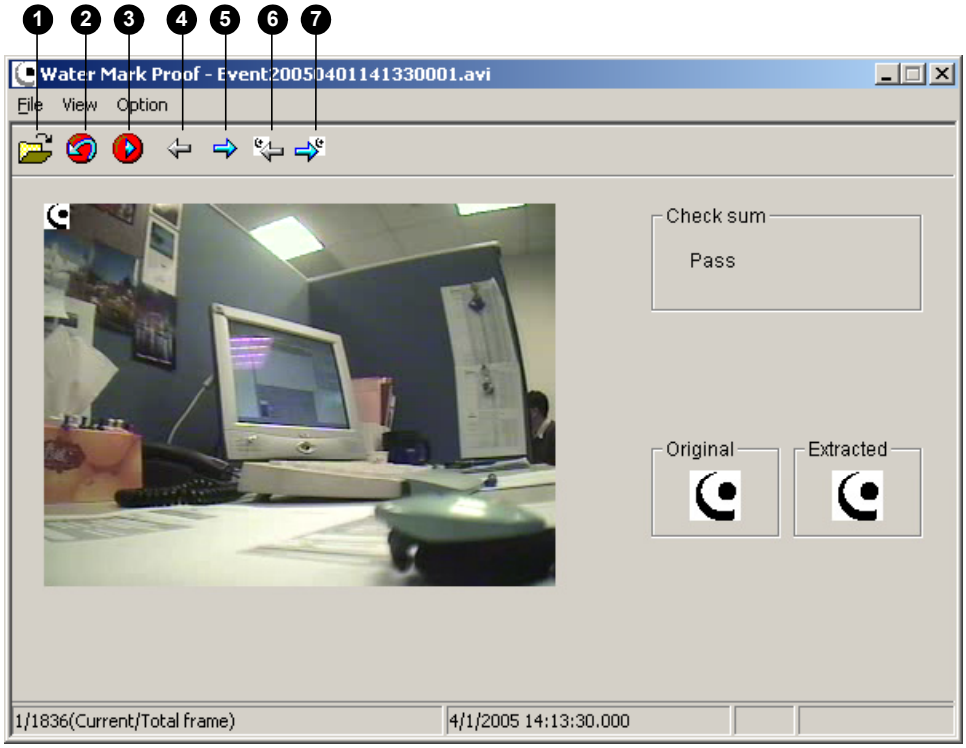
[System Setting]

- **TwinDVR resume:** Resumes TwinDVR connection when the system shuts down unexpectedly.

Watermark Viewer

You can make a watermark proof to protect videos from unauthorized alteration or manipulation. Click the Configure button and then select Use Digital Watermark Protection in the General Setting tab (see the System Configure window on page 20). This allows all recorded videos to be marked with a permanent and inseparable image.

The watermark is invisible to the naked eye. In order to see it, the video stream must be open in a watermarking verification program. Locate and execute WMProof.exe from the system folder. This displays the following windows.



The controls in the window:

No.	Name	Description
1	Open File	Click and find a video file to play.
2	First Frame	Go to the first frame of the file.
3	Play	Play the file.
4	Previous Frame	Go to the previous frame of the file.
5	Next Frame	Go to the next frame of the file.
6	Previous Watermarked Frame	Go to the previous frame that contains watermark.
7	Next Watermarked Frame	Go to the next frame that contains watermark.

The Watermark Viewer displays the verifying result as follows:

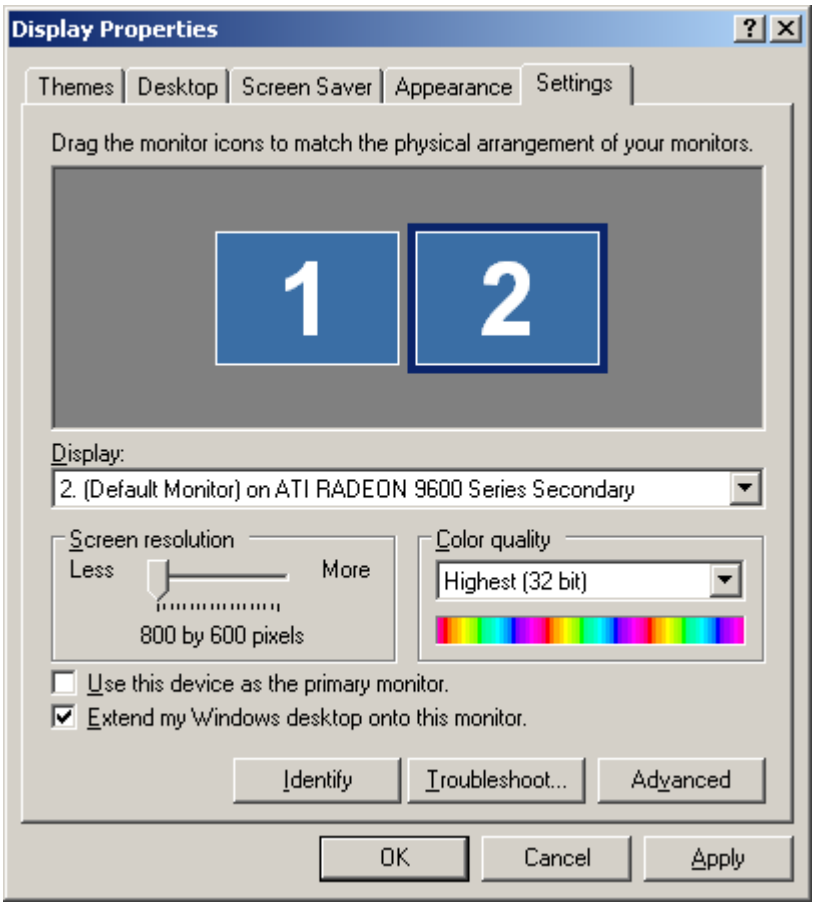
Check sum: If the video stream has not been tampered, the Check sum section displays a Pass message. Otherwise a No Pass message will appear.

Original vs. Extracted: The Extracted section should have the same icon displayed as that in the Original section. If not it indicates the video may have been altered.

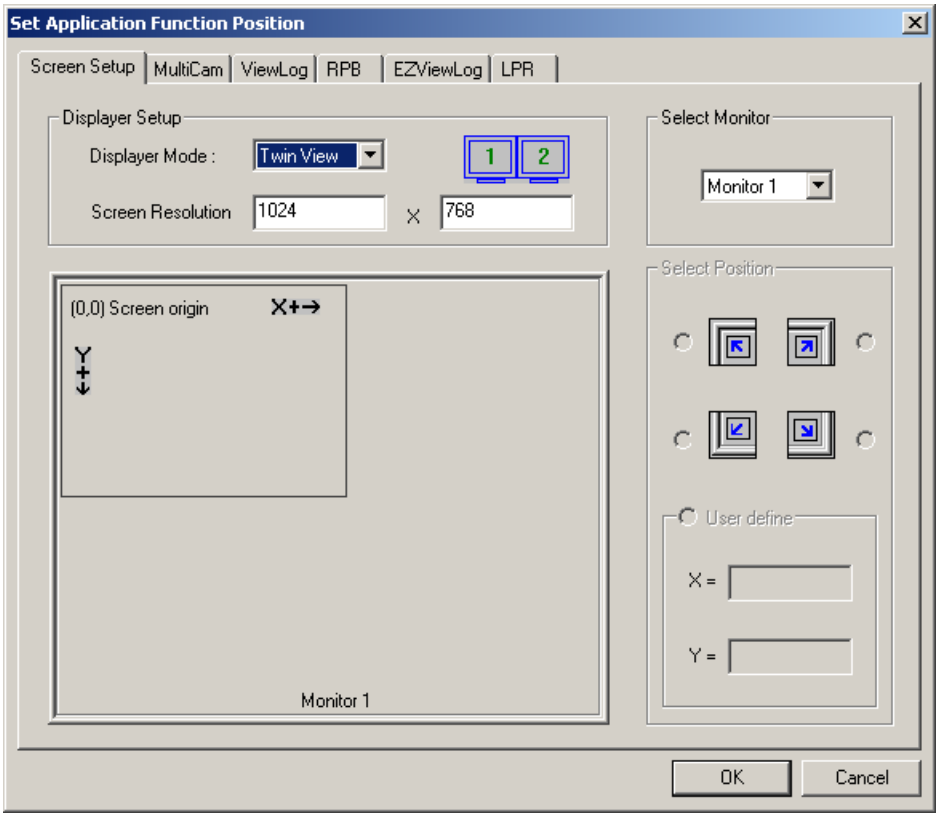
Twin View Display

You can display Main System and ViewLog in two separated monitors. To make this operation possible, your system must equip with VGA card having dual video outputs. Each output should be connected to its own monitor display.

1. Right click on the Windows desktop and select Properties. This displays the Display Property dialog box.
2. Select Settings, enable Extend my Windows desktop onto this Monitor, and then click the Apply button.



3. Locate and execute DMPOS.exe from the system folder. This displays the Set Application Function Position window.



4. In the Screen Setup tab, select TwinView from the Displayer Mode drop-down list.
5. In the MultiCam tab, select Monitor 1 from the Select Monitor drop-down list.
6. In the ViewLog tab, select Monitor 2 from the Select Monitor drop-down list.
7. Click the OK button and start GV-system software, which should appear in monitor 1.
8. Click the ViewLog button on the main panel and select Video/Audio log from the menu. ViewLog should appear in monitor 2.

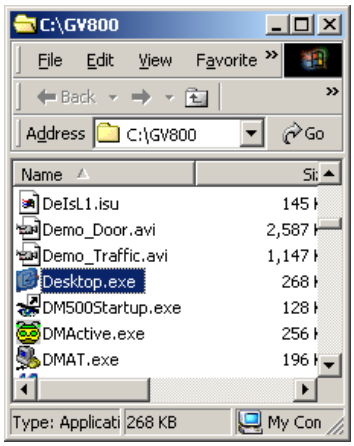
Note: The Select Position option allows you to determine where to position GV software on Windows. It is only necessary if your GV-system is set at 800x600 panel resolution but your Windows desktop is set at 1024x768 or higher. It is recommended that both GV software and Windows desktop to be set at the same resolution. You may refer to *Panel Resolution* on page 21 for details on how to set the resolution for GV-system.

Windows Lockup

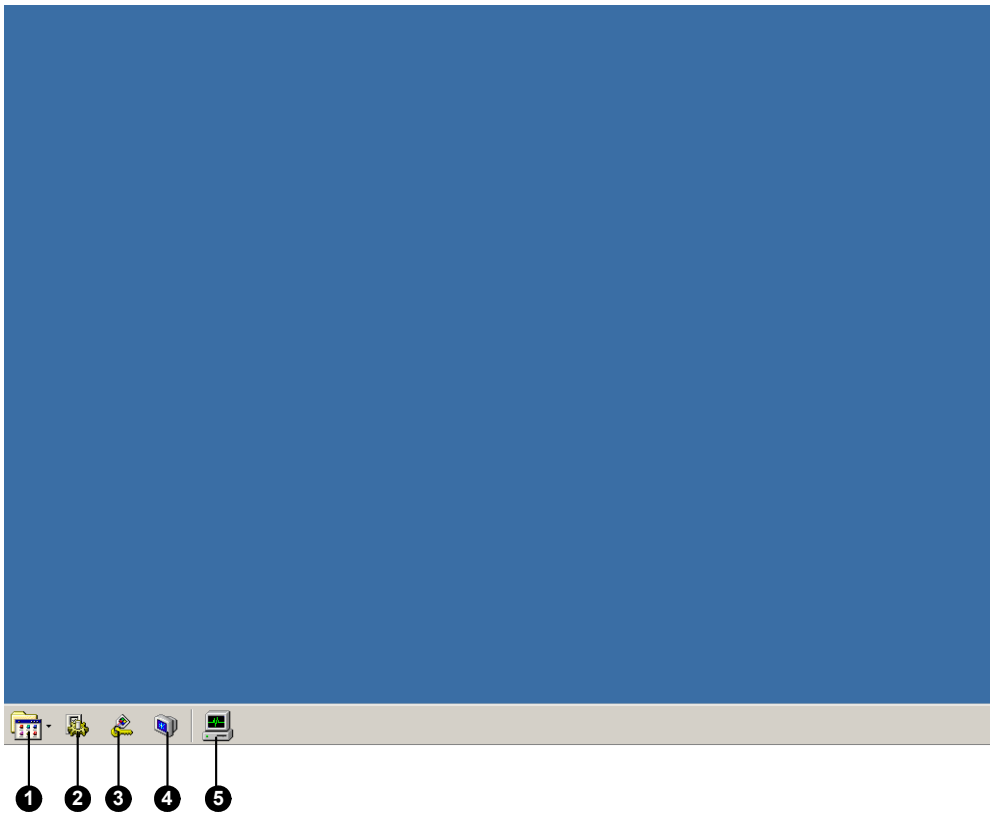
Secure your PC while away from your workstation. With this feature, you may lock up the Windows desktop while launching a customized GV-desktop. The GV-desktop is where operators are limited to run the GV-system and the selected programs.

The GV-desktop Screen

The GV-desktop program is included in the installation of Main System. Go to the system folder and execute Desktop.exe.



The following GV-desktop screen will appear.



The controls in the GV-desktop screen:

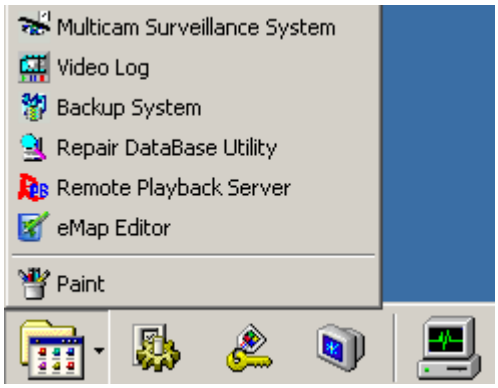
Icon	Name	Description
1	Programs	Click to access programs.
2	Settings	Click to add programs to the programs menu.
3	Log Off	Click to log off GV-desktop.
4	Shut Down	Click to shut down the computer.
5	Task Manager	Click to view the tasks currently running on your computer.

GV-desktop Features

The five buttons on GV-desktop are discussed below.

Programs

Click the Programs button to see the program menu. The default programs are Multicam Surveillance System (Main System), ViewLog, Backup System, Repair Database Utility, Remote Playback Server, and eMap Editor. You can add or remove new programs to the menu. For the illustration below, Paint is a new program added to the menu.



Settings

Click the Settings button to display the following window. A valid ID and password will be required.

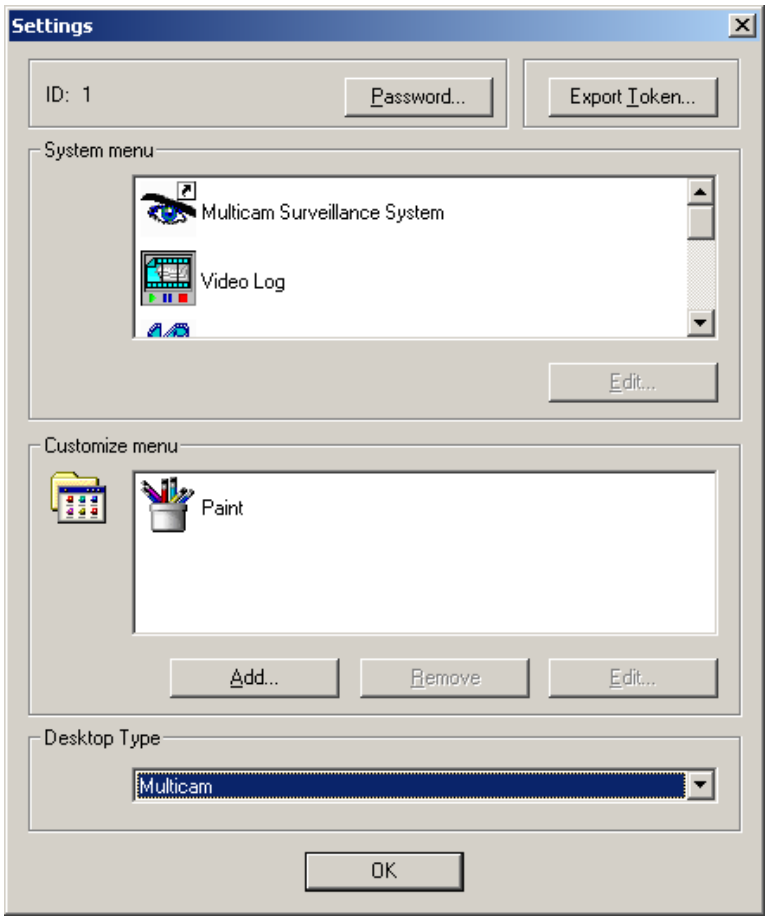


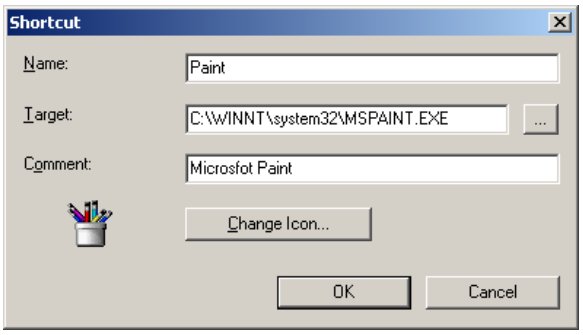
Figure 13-3 *Settings*

[Password] Click to change the password. For the option of Allow Removing Password System, refer to *Setting up Password* in Chapter 2 on page 44.

[Export Token] This option is discussed later in the *Token File for Save Mode* section.

[System Menu] The menu lets you rename system programs. Select a desired program and click the Edit button to change its name.

[Customized Menu] The menu lets you add other programs to the Programs menu. Click the Add button to display the following window. In the Target field, type a path or click the button next to the field to assign a path. Then enter the program name, comment, or even change an icon for the program. Finally, click OK to add the program.



[Desktop Type] Select Windows or GV-desktop (Multicam) from the drop-down menu. The selected desktop will launch the next time when you log in to PC.

Log Off

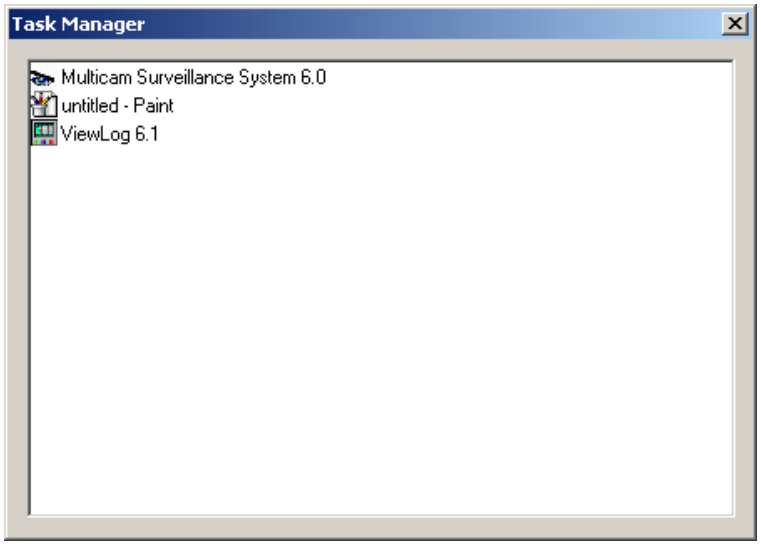
Click the Log off button to log off GV-desktop. A valid ID and password will be required.

Shut Down

Click the Shut Down button to shut down your computer. A valid ID and password will be required.

Task Manager

Click the Task Manager button to view the programs currently running on your computer. When you minimize a program, it will be hiding and working in the background. Double click the program listed in Task Manger to bring the program back to desktop.

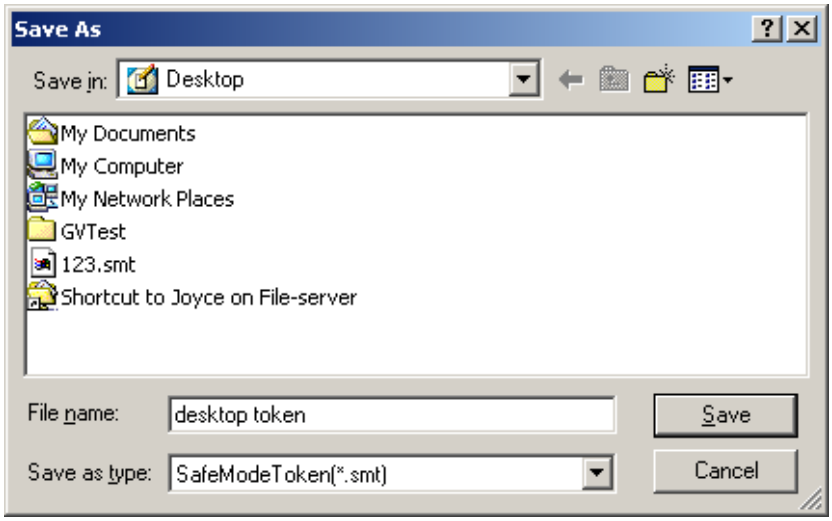


Token File for Save Mode

This option in the Settings section lets you export a token file. In case you enter safe mode and are in the status of the GV-desktop. This token file will let you exit from the GV-desktop and enter the Windows desktop. To export a token file and apply it, follow the steps below.

1. Click the Export Toke button to display the following dialog box.

2. Enter a code in the Token Code field.
3. Click OK to display the Save As dialog box.



4. Locate a path, and enter a desired name in the File Name field.
5. Click Save to save the file.

When you enter safe mode and are in the status of the GV-desktop:

6. Click the Settings button on the desktop. You will be prompted to locate the stored token file and enter the set token code.
7. When the Settings window appears (see Figure13-3), select Windows in the Desktop Type field, and then exit from the window.
8. Click the Log Off button to log off the GV-desktop and enter the Windows desktop. The token code and file are also required here.

Authentication Server

The Authentication Server allows a remote server to restrict access to the password settings of local GV-DVR systems. When the Sever is working, the previous password settings in local DVRs will be invalid. Local DVRs will submit to the full control of the Server.

Installing the Server

To install this application in a remote sever, follow these steps:

1. Insert the installation CD. It will run automatically and pop up a window.
2. Select the item of Install Version 7.0 system.
3. Click Authentication Server, and follow the on-screen instructions. Refer to Figure 1-15 on page 15.

The Server Window

Execute AuthServer.exe to display this window.

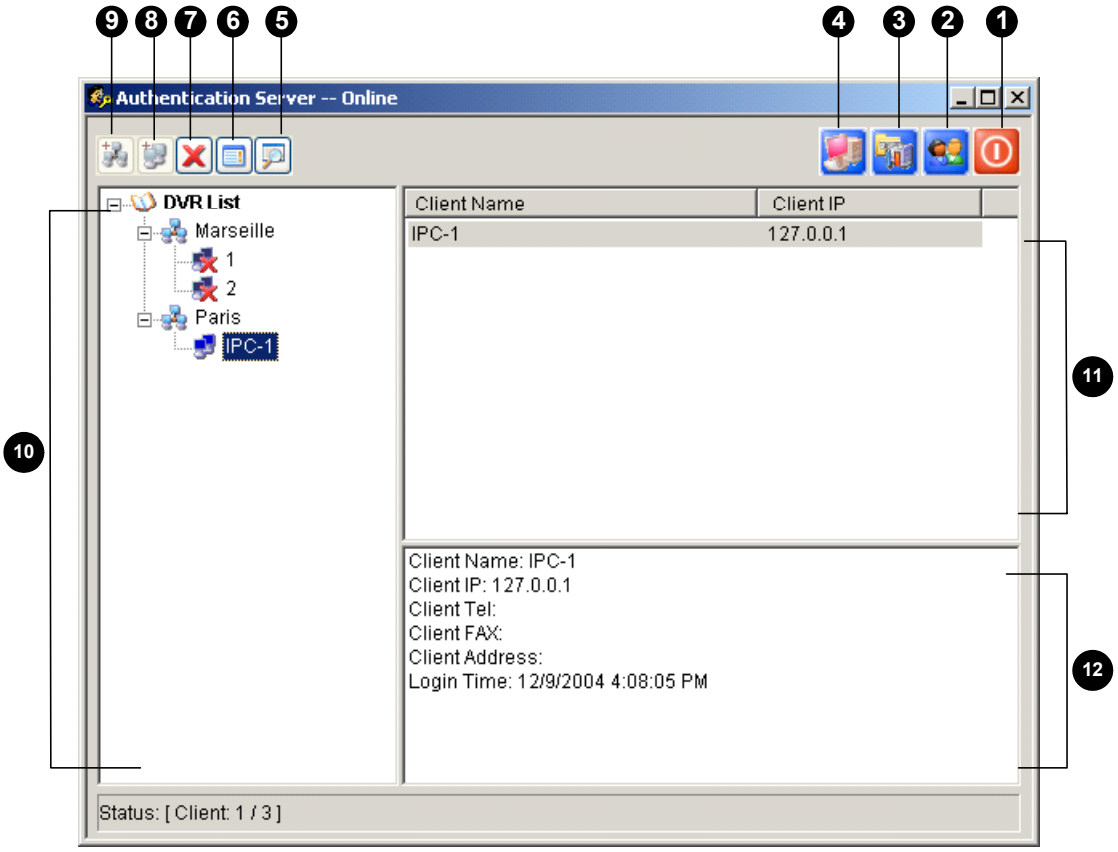


Figure 13-4 *The Authentication Server Window*

The controls in this window:

No.	Button Name	Description
1	Exit	Exits this window; Logs out Administrator; Changes Password
2	PassDll Setup	Configures passwords and grants permissions to clients
3	Server Setting	Configures the Authorization Server
4	Start Server	Starts/Stops the Authorization Server
5	Find A Client	Finds an existing client.
6	View/Edit A Client	Select a client from the DVR List, and click to view /edit it
7	Delete An Area /Client	Deletes an existing group or client
8	Add A Client	Creates a client account
9	Add An Area	Creates an Area group
10	DVR List	Lists the created clients and area groups
11	Connected DVR List	Lists the connected GV-systems
12	DVR Information	Lists the information of the selected GV-system

Creating a DVR List

You can arrange your clients' GV-systems into different groups for a better management. Use the buttons 8 and 9 for the following steps.

1. To create a group, click the Add An Area button.
2. To create a client under the group, click the Add A Client button. This displays the Client Information dialog box.

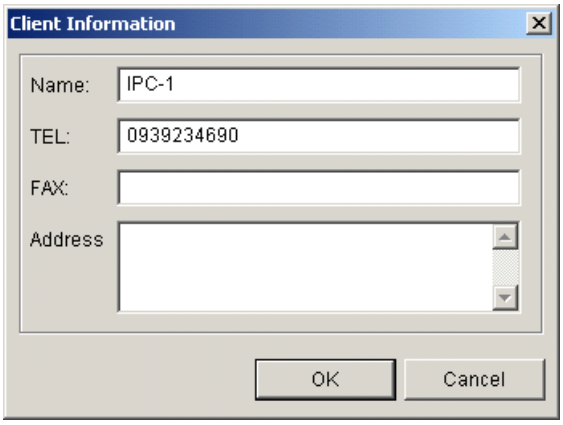


Figure 13-5 *Client Information*

3. Enter the client's information. The Name entered must match that of local GV-system.
4. Click OK.

Editing a User

The supervisor can create users; can grant, deny, or modify permissions; and can allow access to local GV-DVR systems listed in the DVR list.

1. Click the PassDll Setup button to display the Password Setup window. The window is the same as the Password Setup window in Main System (see page 44), except the following section.

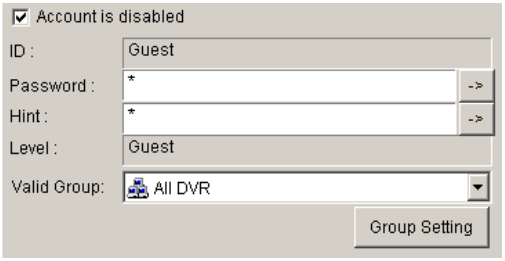


Figure 13-6 *Password Setup*

2. To create and edit a user, refer to *Setting up Password* on page 44.
3. To grant access to local DVRs:
   a. Click the Group Setting button in the window. The Valid Group List window appears.
   b. Click the New Group button. The DVR Group Information window appears.
   c. Give a DVR group name, and check the desired DVRs into the group.
   d. Go back to the Password Setup window. Click the Valid Group drop-down list to select the created DVR group.

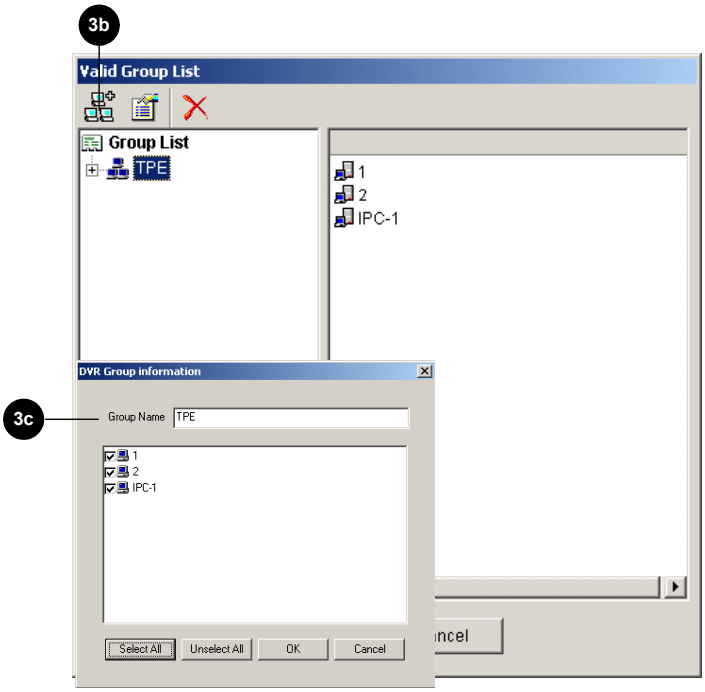


Figure 13-7 *Valid Group List and DVR Group Information*

Starting the Server

To configure the server and start the service, follow these steps:

1. Click the Server Setting button. This dialog box appears.

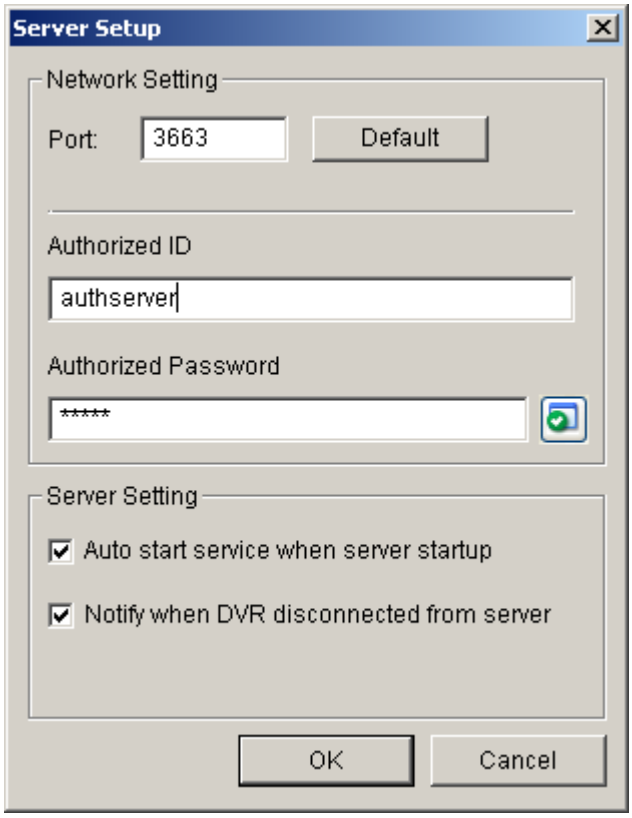


Figure 13-8 *Sever Setup*

[Network Setting] The default port number is 3663.

[Authorized ID and Password] The ID and password entered will be those for the local DVRs to log in the server.

[Server Setting]

- **Auto start service when server startup:** Starts automatically the service when Windows starts.
- **Notify when DVR disconnected from server:** Notifies the Authorization Server with a popup window when the DVR and server loss connection.

2. Click OK to apply above settings.
3. Click the Start Service button to start the connection.

Connecting GV System to the Server

To configure the GV-system in order to access the Authorization Server remotely through a network connection, follow these steps:

1. Click the Configure button, point to Password Setup, and then select Remote Authentication Setup. This dialog box appears.

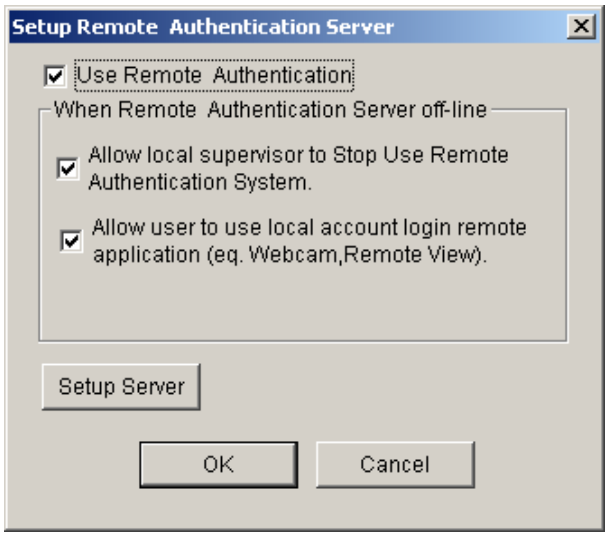


Figure 13-9 *Setup Remote Authenticator Server*

- **Use Remote Authenticator:** Enable the connection with the Authentication Server.
- **Allow Local supervisor to stop use remote authentic system:** Allows the local supervisor to stop the Authentication application when the connection fails. If the option is disabled and the connection fails, the dialog box won't be accessible until connection resumes.
- **Allow user to use local account login remote application:** Allows the local users to access other remote applications with their previous password and ID settings when the connection fails.

2. Click the Setup Server button in Figure 13-9. This dialog box appears.

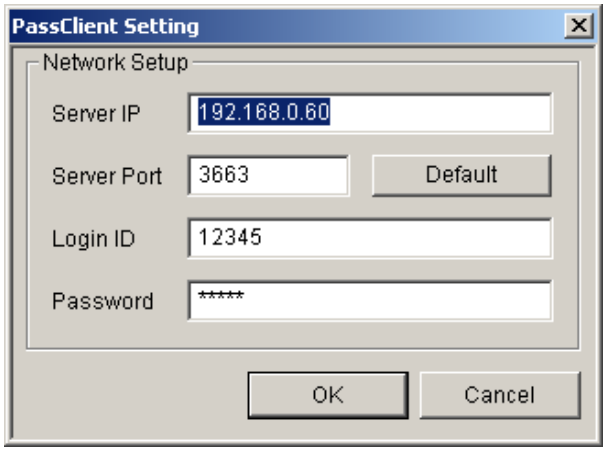


Figure 13-10 *PassClient Setting*

3. Enter the IP address and port of the Authorization Server. Enter the valid ID and password created in the Authorization Server (See Figure 13-8).
4. Click OK to start the connection. **When the connection is established, the previous password settings in the GV-system will be invalid.**
5. Press the shortcut key [L] on the keyboard to call up the Login dialog box. The icon  indicates the connection is established.

6. Enter a valid User ID and password for login.

As long as the Authentication sever is working, every time when you start the GV-system, the Login dialog box will appear.

Note: When the disconnection icon  appears, there might be three reasons:

1. The valid ID and password created in the Authorization Server (see Figure 13-8) don't match those in the GV-system (see Figure 13-10).
2. The client's given name (see Figure 13-5) doesn't match the GV-system's.
3. The network media and traffic problem.