9.4 Authentication Server

The Authentication Server is a password and account management system for multiple GV-VMS. Through the Authentication Server, the administrator can create the accounts with different access rights to a group of GV-VMS. Once any GV-VMS is connected to the Authentication Server, the previous password settings in local GV-VMS will be invalid. Local GV-VMS will submit to the full control of the Authentication Server.

Note: In addition to the GV-VMS, the Authentication Server also supports GV-System, E-Map Server and GV-Control Center V3.1.2.0 or earlier for central credential management. Up to 20,000 client accounts can be created.

9.4.1 Installing the Server

You can install the Authentication Server from Software DVD or GeoVision Website.

Installing from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-Authentication Server** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website: http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, select GV-VMS, find the **Supplemental Utilities** section and click the **Download** icon 

of **GV-Authentication Server**.

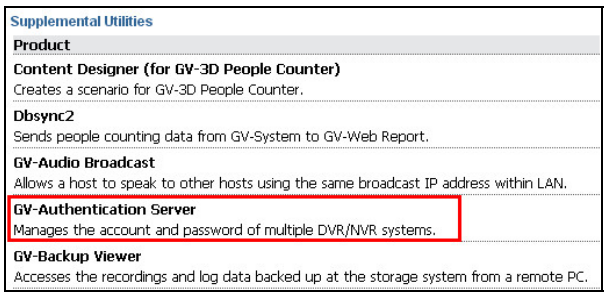


Figure 9-13

9.4.2 The Main Window

Go to Windows **Start**, click **Programs**, select **AuthServer** and click **AuthServer**. This window appears.

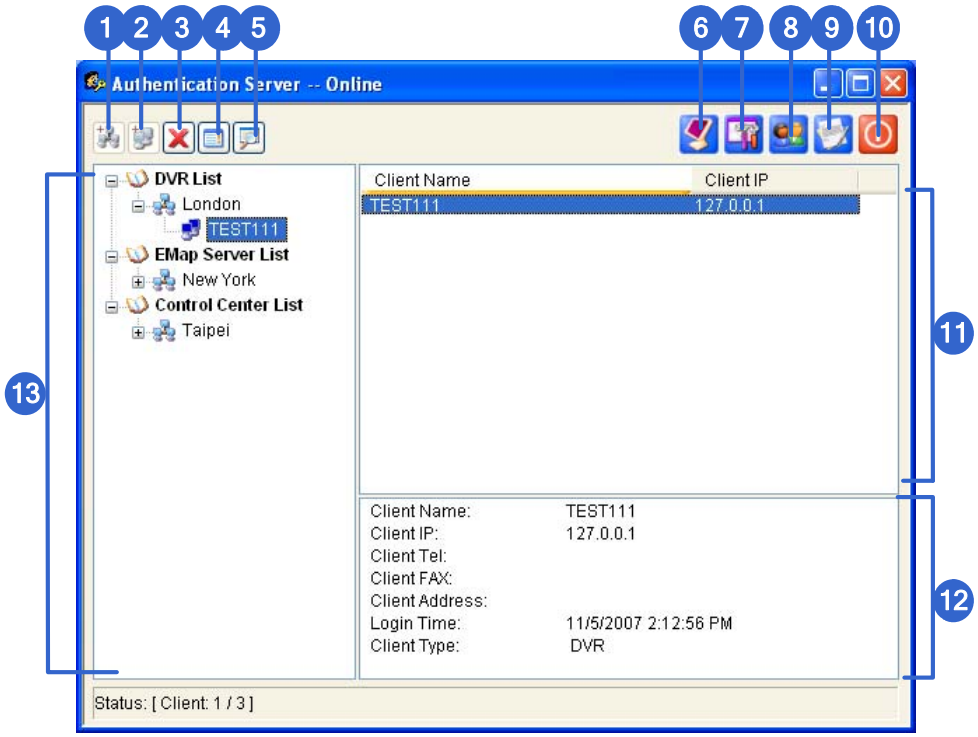


Figure 9-14

The controls in this window:

No.	Button	Description
1	Add An Area	Creates an Area group.
2	Add A Client	Creates a client account.
3	Delete An Area / Client	Deletes an existing group or client.
4	View/Edit A Client	Select a client from the Client List, and click to view / edit it.
5	Find A Client	Finds an existing client.
6	Start/Stop Service	Starts/Stops the Authentication Server.
7	Server Setup	Configures the Authentication Server.
8	Account Setup	Configures passwords and grants permissions to clients. Imports groups from Active Directory.

No.	Button	Description
9	Log	Sets up the Authentication Server Log and opens the log browser.
10	Exit	Exits this window; Logs out Administrator; Changes Password, imports or exports account information.
11	Connected Client List	Lists the connected GV-VMS, GV-System, E-Map Server or GV-Control Center.
12	Client Information	Lists the information of the selected GV-VMS, GV-System, E-Map Server or Control Center.
13	Client List	Lists the created clients and area groups.

9.4.3 Creating Clients

You must create and arrange the clients first which user credentials will be centrally managed by the Authentication Server. To create a list of GV-VMS clients, follow the steps below.

1. To create a GV-VMS client, highlight the **DVR List** from the left panel and click the **Add A Client** button (No. 2, Figure 9-14).

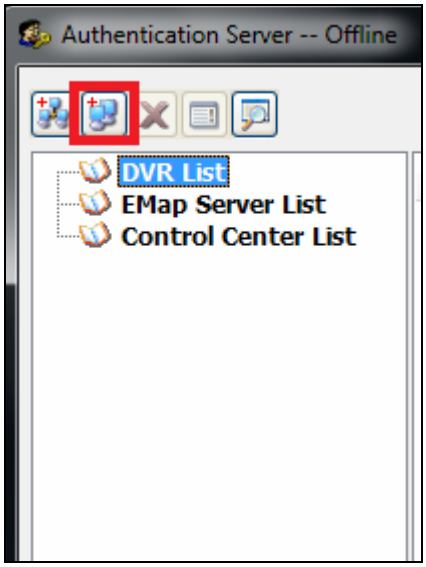


Figure 9-15

2. Type the client's information and click **OK**. The **Name** must match that of local GV-VMS.

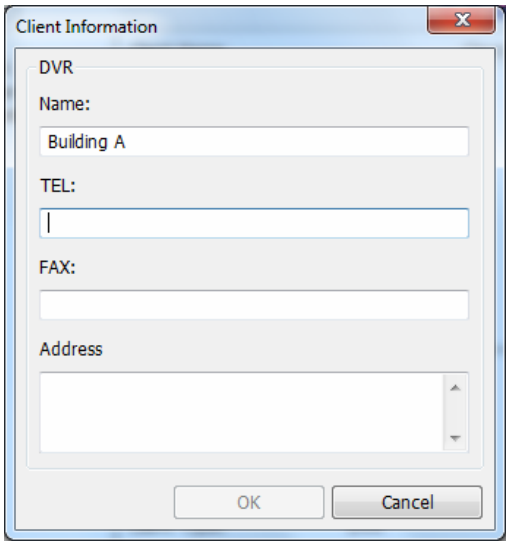
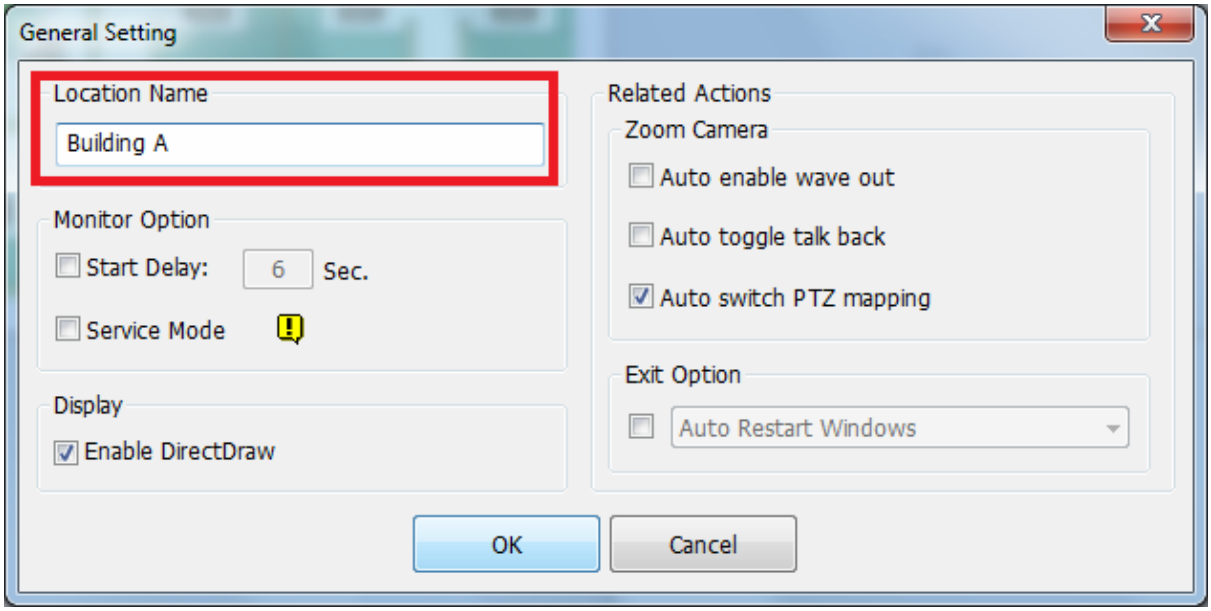


Figure 9-16

Tip: To view the name of your GV-VMS server, select **Toolbar** , click **Configure** , select **System Configure** and click **General Setting**.



3. To create another client, repeat the steps above.
4. You can also arrange multiple clients under a group by highlighting a list and clicking the **Add An Area** button (No. 1, Figure 9-14). The created group appears under the selected List.

9.4.4 Creating User Accounts

To create user accounts with different access rights and assign the user accounts to a group of GV-VMS clients, follow the steps below. Up to 20,000 accounts can be created.

1. Click the **Account Setup** button (No.8, Figure 9-14) and select **Password Setup**. The Password Setup dialog box appears.
2. To create and edit a user account, refer to *Account and Password* in Chapter 1.

Note: The Administrator has the authority of changing the password of any accounts.

3. To assign the created user to a group of GV-VMS clients:

A. Click the **Group Setting** button.

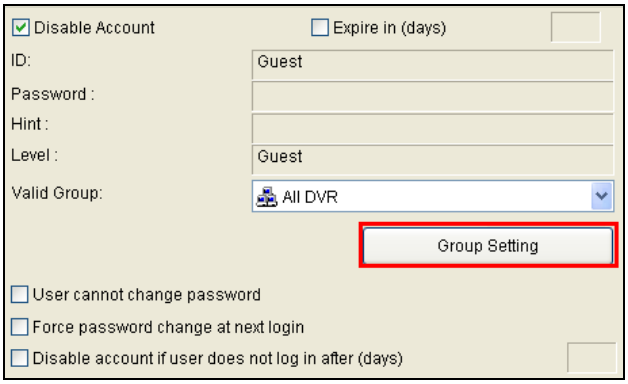


Figure 9-17

B. In the Valid Group List window, click the **New Group** button.

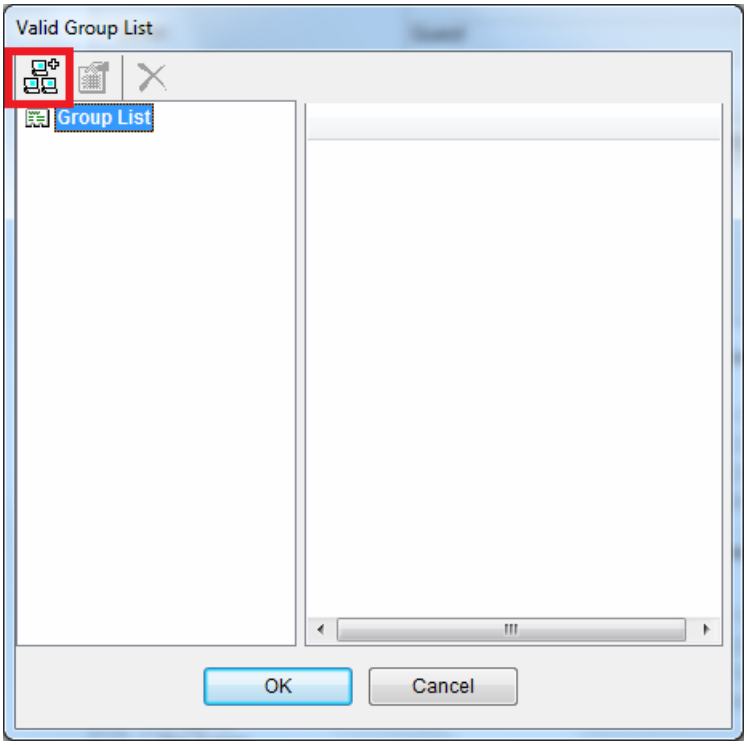


Figure 9-18

C. In the DVR Group Information window, give a name to the group, select the desired GV-VMS clients to be added to the group. Click **OK**.

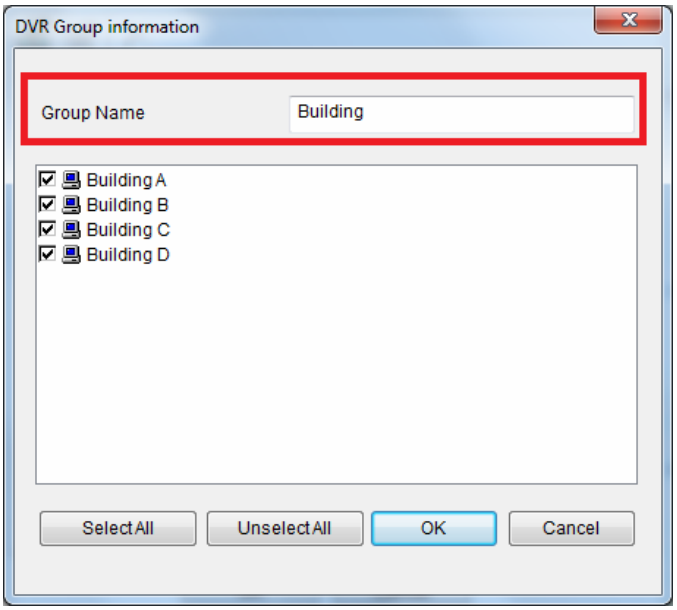


Figure 9-19

D. Click **OK** again to go back to the Password Setup window.

E. Use the **Valid Group** drop-down list to select the created group. The user will be able to log in the assigned GV-VMS clients.

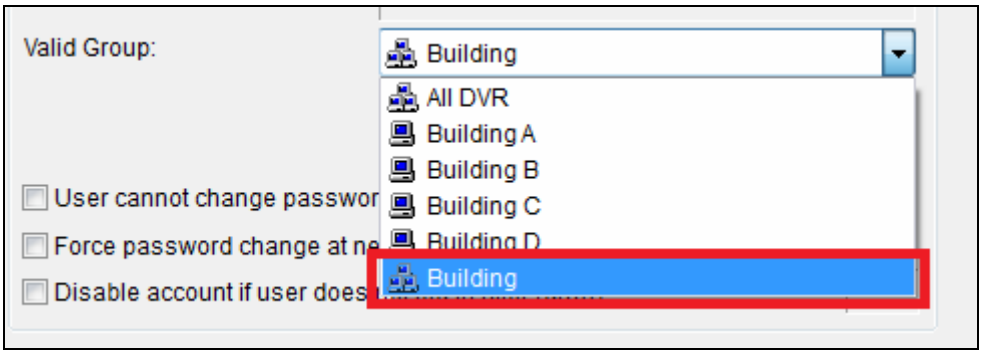


Figure 9-20

4. Optionally, you can use the following functions to arrange the user and client accounts.

A. Right-click a user account to have two options. The **Apply setting to** option allows you to apply the same settings to a specific user account. The **Apply setting to group** option allows you to apply the same settings to all user accounts under the same account level.

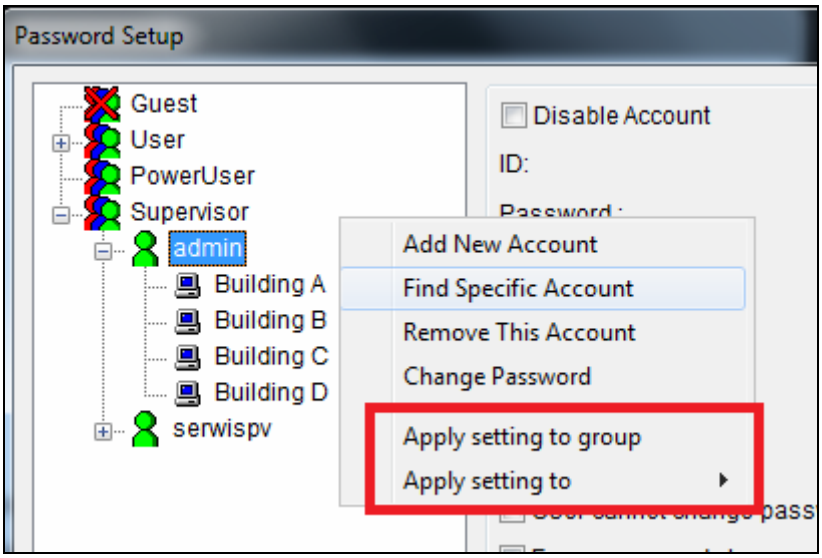


Figure 9-21

B. Right-click a client account to have two options. The **Apply setting to other DVR(s)** option allows you to apply the same settings to all clients under the same user account. For this example, the settings of Building A client will be applied to all Building B, C and D clients. The **Copy** option allows you to copy and paste one client's settings and any client.

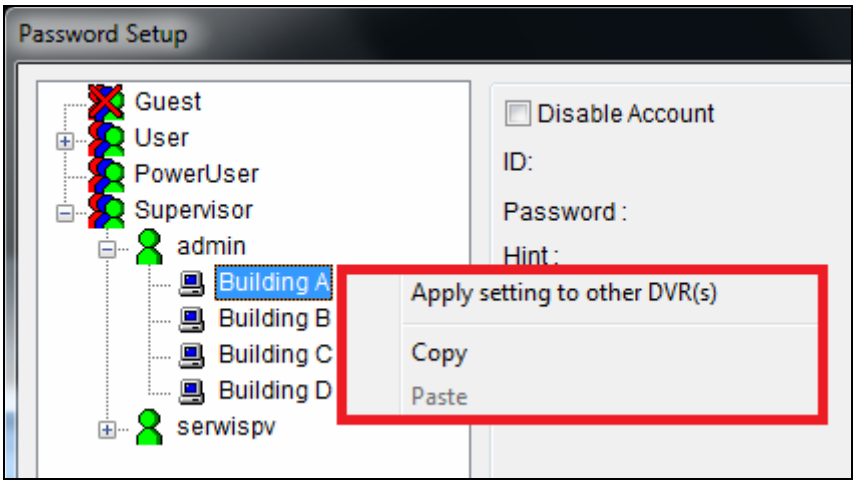


Figure 9-22

9.4.5 Importing Groups and Users from Active Directory

To create user accounts efficiently, you can import groups and users from Microsoft's Active Directory to Authentication Server. You will need to install Active Directory on Windows operating system and set up users into groups before following the steps below.

Note: User accounts in Active Directory need to be grouped into Groups settings first as only groups can be imported into Authentication Server.

---

1. Run **Active Directory Domains and Trusts** in Windows Server 2008 / 2012 by clicking the **Start** menu and opening **Administrative Tools**.
2. Right-click your local Active Directory system and select **Manage**. The Active Directive Users and Computers dialog box appears.

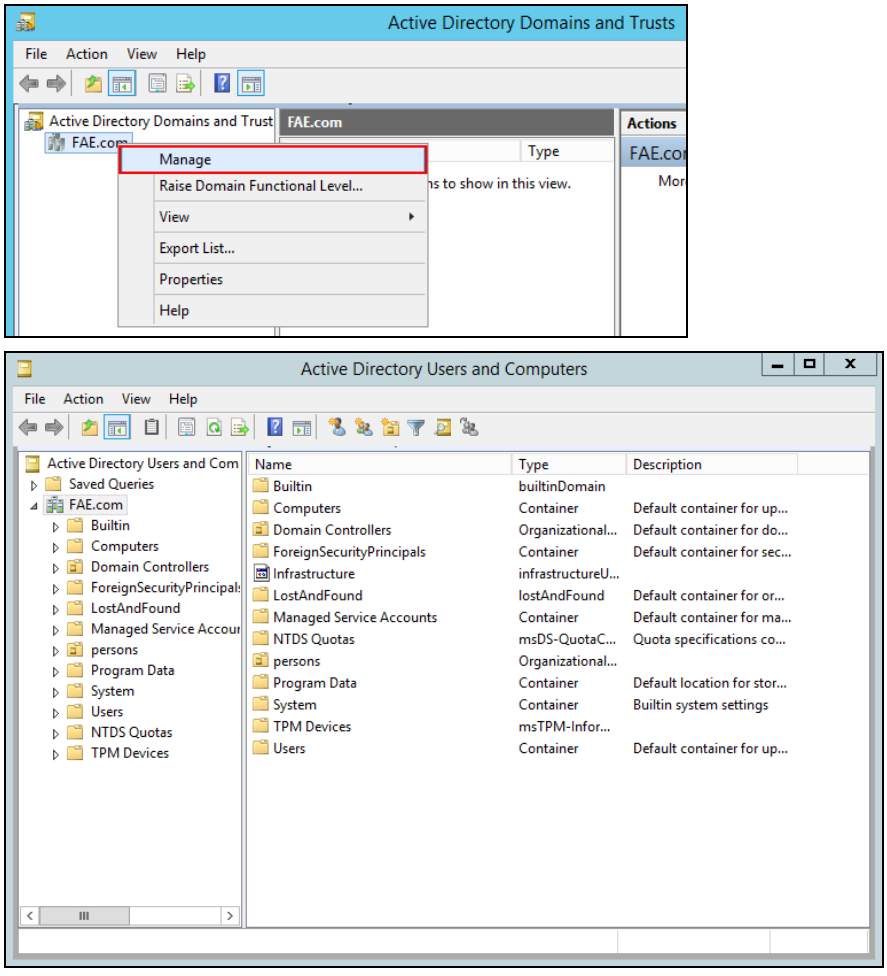


Figure 9-23

3. On the **View** menu, select **Advanced Features**.

Note: If you use Windows Server 2008 instead of Server 2012, skip this step.

4. Right-click the folder saved with the user accounts or groups and select **Properties**.

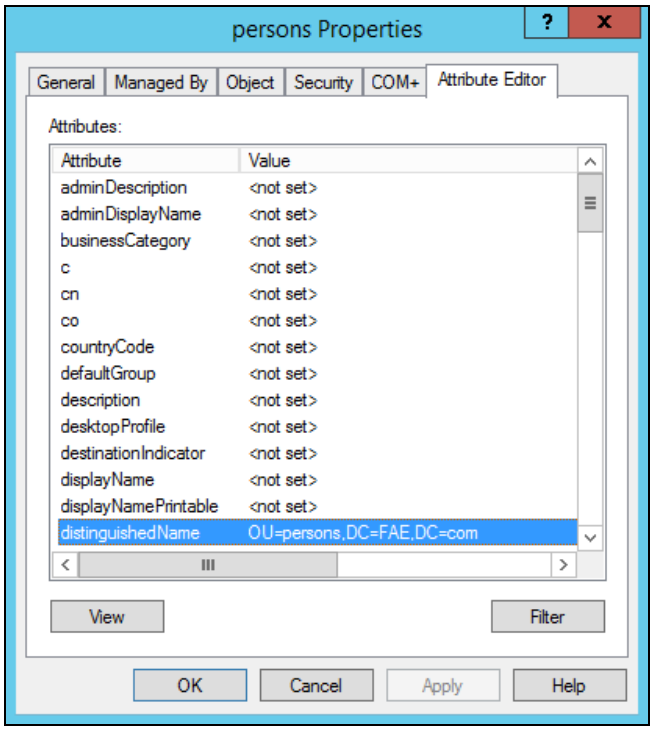


Figure 9-24

Tip: You can change the query parameters or show all items for each folder by clicking **View** and selecting **Filter Options**.

5. Select the **Attribute Editor** tab, double-click the attribute **distinguishedName** and copy the value like **OU=persons,DC=FAE,DC=com**. You will need to paste the value at *step 8, C* to assign the folder to import the user accounts or groups.

6. In AuthServer, click the **Account Setup** button (No.8, Figure 9-14) and select **Active Directory Setup**. This page appears.

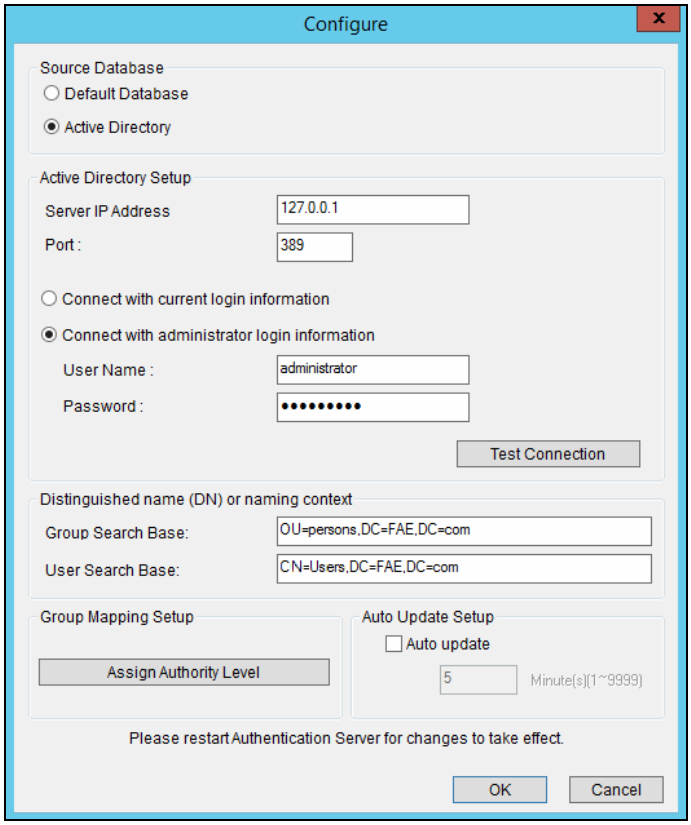


Figure 9-25

7. Under Source Database, select **Active Directory** to enable the function.
8. To connect to the server with Active Directory:
   A. Type the **Server IP Address** and the **Port** number of the server.
   B. To log into the server using your current login information, select **Connect with the current login information**. To log into the server using the login information of its administrator, select **Connect with administrator login information** and type the user name and password.
   C. Paste the value of distinguished name you copied at step 5 respectively to **Group / Users Search Base**.
   D. Click **Test Connection** to see if you can connect to the server with Active Directory.

9. To assign groups in Active Directory to User, Power User or Supervisor authority levels:

   A. Click the **Assign Authority Level** button. This dialog box appears.

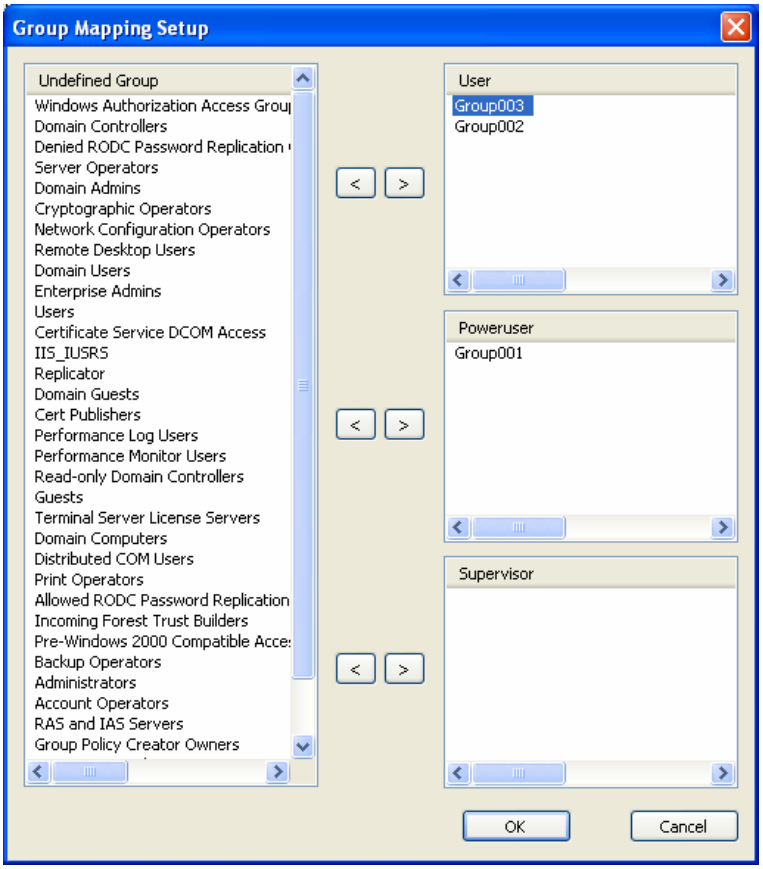


Figure 9-26

   B. Select the groups detected in Active Directory from the Undefined Group list and use the arrow buttons < > to assign the groups to User, Power User or Supervisor level.

   C. Click **OK** to import the user data into the Password Setup window.

10. To automatically update changes to user data in Active Directory, click **Auto Update** and specify the update frequency in minutes.

11. Click **OK** and restart Authentication Server to apply the settings.

9.4.6 Starting the Server

To configure the server and start the service, follow the steps below.

1. Click the **Server Setup** button (No. 7, Figure 9-14). This dialog box appears.

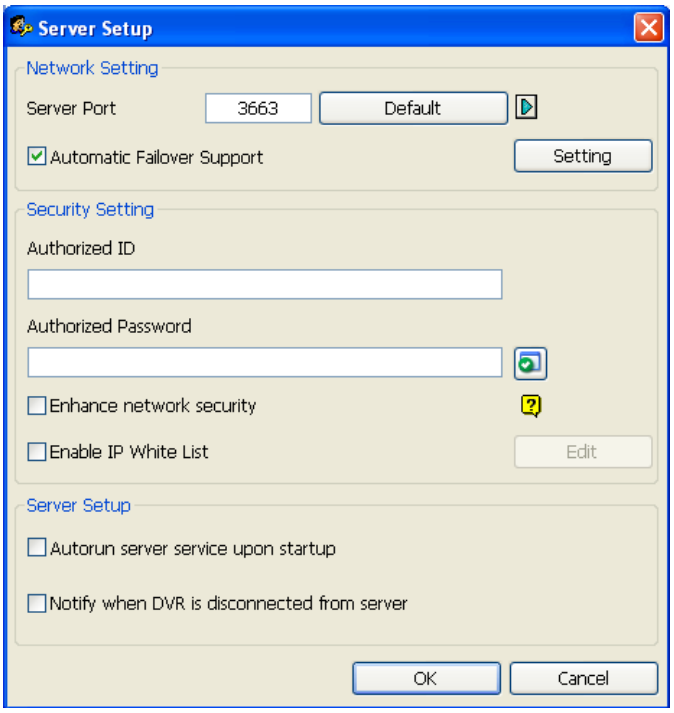


Figure 9-27

2. Under Security Setting, type the **Authorized ID** and **Authorized Password** which will be used for the client GV-VMS to log into the Authentication Server.
3. Click **OK** to apply the settings.
4. Click the **Start/Stop Service** button (No. 6, Figure 9-14) to start the services.

Optionally, you can configure the following settings before starting the Authentication Server:

[Network Setting]

- **Server Port:** The default port number is **3663**. To use UPnP for automatic port configuration to your router, click the **Arrow** button. For details, see *UPnP Settings* in Chapter 7.

- **Automatic Failover Support:** Select and click the **Setting** button to configure up to 2 Authentication Servers in case the primary Authentication Server fails. Once the primary server fails, the second or the third server will take over the connection from clients and provide uninterrupted services. Note the settings of Authorized ID and Authorized Password on the failover server must match those of the primary server.

Tip: To set up the failover Authentication Server, you can export the current settings by using the **Export Account** and **Import Account** functions in the **Exit** button.

Note: Once the primary Authentication Server is ready to resume the services, it is required to close the failover Authentication Server so the connection from clients can move back to the primary.

[Security Setting]

- **Enhance network security:** Strengthen network security on Authentication Server.
- **Enable IP White List:** Click **Edit** to create a list of IP addresses only which are allowed to establish connection with Authentication Server.

[Server Setting]

- **Auto run server service upon startup:** Allow the server to automatically start service upon Windows startup.
- **Notify when DVR is disconnected from server:** Notify the Authentication Server with a pop-up window when the GV-VMS is disconnected with the Authentication Server.

9.4.7 Connecting GV-VMS to the Server

To configure the GV-VMS in order to access the Authentication Server remotely through a network connection, follow the steps below.

1. On the main screen of GV-VMS, click **User** 1, select **Password Setup** and click **Remote Authentication Setup**. The Setup Remote Authentication Server dialog box appears.

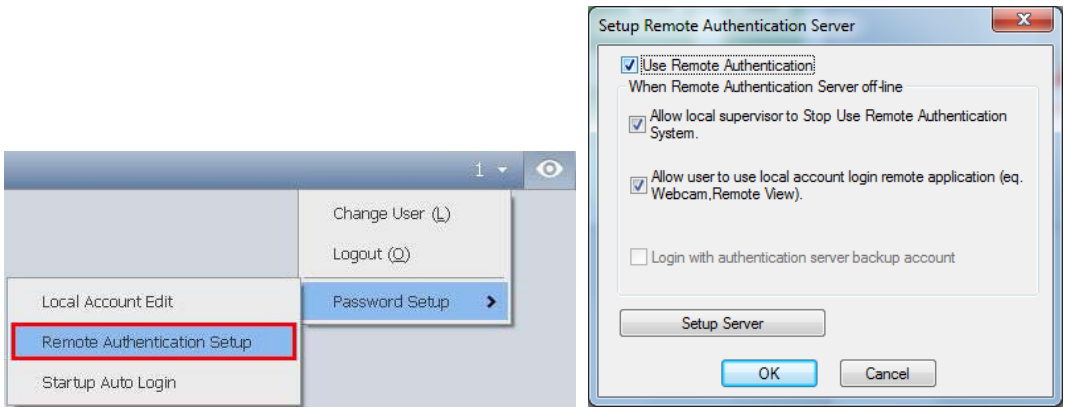


Figure 9-28

2. Select **Use Remote Authentication** and select any of the following options.

[When Remote Authentication Server Off-line]

- **Allow local supervisor to stop use Remote Authentication System:** Allow the local supervisor to stop the Authentication application when the connection with the Authentication Server fails. Note if the option is disabled and the connection with the Authentication Server fails, the local supervisor will not be able to log into the GV-VMS, and the dialog box will not be accessible until the connection resumes.
- **Allow user to use local account login remote application:** Allow local users to access remote applications with their previous password and ID settings when the connection with the Authentication Server fails.
- **Login with authentication server backup account:** Keep using password settings created on the Authentication Server even though the connection with the server fails.

3. Click **Setup Server**. This dialog box appears.

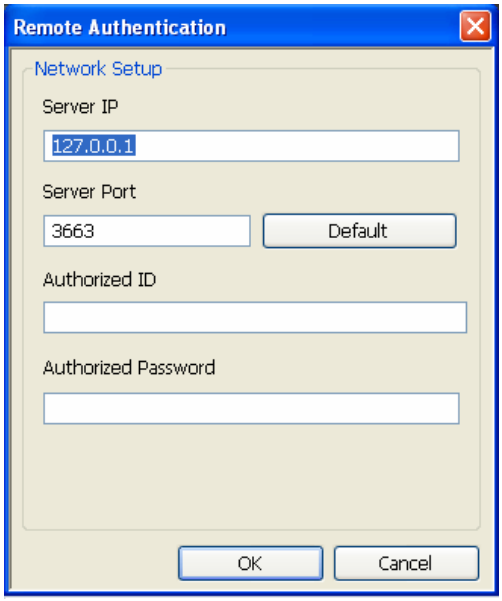


Figure 9-29

4. Type the IP address and port of the Authentication Server.
5. Type the **Authorized ID** and **Authorized Password** of the Authentication Server.
6. Click **OK** to start the connection. When the connection is established, the previous password settings in the GV-VMS will be invalid.
7. Press **[L]** on the keyboard to call up the Login dialog box. The icon  indicates that the connection is established.

Figure 9-30

As long as the Authentication Sever is working, every time when you start the GV-VMS, the Login dialog box will appear. Type the user account created on the Authentication Server to log into the GV-VMS.

Note: The disconnection icon  will appear on the Login dialog box (Figure 9-28) when one of the following situations occurs:

1. The login ID and Password do not match any of the user IDs and Passwords created on the Authentication Server.
2. The client name (Figure 9-16) does not match the location name of GV-VMS.
3. The network connection encounters traffic problem.

9.4.8 Remote Access from Control Center and Remote E-Map

The Authentication Server allows you to restrict users of E-Map Server and GV-Control Center to access specific GV-VMS hosts and cameras only. Instead of connecting to GV-VMS hosts directly, the user of E-Map Server and Control Center will connect to the Authentication Server using the user account you created on the Authentication Server.

You must first set up remote authentication on E-Map Server and GV-Control Center. After the E-Map Server and GV-Control Center are connected to the Authentication Server, the user will be prompted to log in with the user ID and password you created on the Authentication Server. Once the user logs in, a list of GV-VMS hosts authorized to the user account will be displayed, and the user will be able to view the assigned cameras.

Setting up Authentication Server

You need to create and arrange E-Map Servers and Control Servers under their separate lists on the Authentication Server window (Figure 9-14).

1. In the Client List field, click the E-Map Server List or Control Center List and click the **Add A Client** button (No. 2, Figure 9-14). The Client Information dialog box appears.
2. Type the name and information of the E-Map Server or Control Center. The name does not need to match the location name of the E-Map Server or Control Center.
3. Click **OK** to add the E-Map Server or Control Center.

Accessing from E-Map Server

The E-Map Server can access the user account setting of the Authentication Server.

1. Run the **E-Map Server**. For details, see *E-Map Sever* in Chapter 8.

2. In the E-Map Server window, click **Tools** on the menu bar, and select **Options**. This dialog box appears.

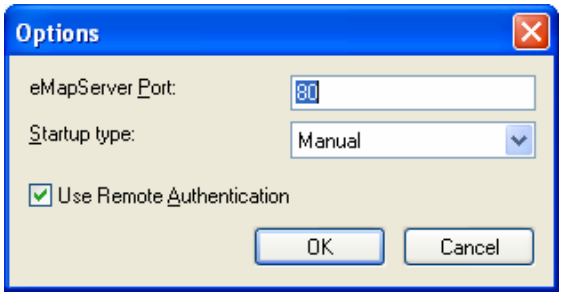


Figure 9-31

3. Select **Use Remote Authentication**.
4. To enable the Authentication Server service to start automatically at Windows startup, select **Automatic**. Keep the E-Map Server Port **80** as default or modify if necessary.
5. Click **OK** to apply the settings.
6. In the E-Map Server window, click **Tools** on the menu bar and select **Remote Authentication**. This dialog box appears.

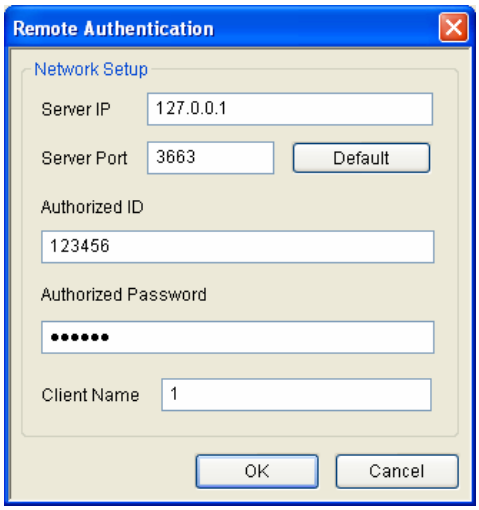


Figure 9-32

7. Type the IP address, authorized ID and authorized password of the Authentication Server, as well as the E-Map Server's client name created on the Authentication Server, and then click **OK**.
8. In the E-Map Server window, click **Tools** on the menu bar and select **Start Service** to start the E-Map Server.
9. When you log into the E-Map Server, type the user ID and password created on the Authentication Server. A list of assigned GV-VMS clients to the user will be displayed.

Accessing from GV-Control Center

The GV-Control Center can access account settings of the Authentication Server.

Note: The Authentication Server only supports GV-Control Center V3.1.2.0 or earlier.

---

1. Run the **GV-Control Center**. For details, see *GV-Control Center User's Manual*.
2. On the Host List, right-click **Host List by ID** and select **Remote Authentication Setup**. A dialog box appears (Figure 11-27).
3. Type the IP address, authorized ID and authorized password of the Authentication Server, as well as Control Center's client name created on the Authentication Server, and then click **OK** to enable connecting to the Authentication Server.
4. To access the Authentication Server account settings, on the Host List, right-click **Host List by ID** and select **Get Host List by ID**. A dialog box prompts you for ID and password.
5. Type a user ID and password created on the Authentication Server, and click **OK**. A list of assigned GV-VMS hosts to the user will be displayed.