



Security Basic Mode Quick Start

APPLICATIONS NOTE

January 2003

The security server allows you to protect your SCADA/HMI and WebHMI applications against unauthorized access.

Security Server Capabilities:

- Manage security access for users and groups of users.
- Grant or restrict write access to OPC Data Access tags
- Grant or restrict access to Display Files (*.gdf)
- Grant or restrict access based on time.
- Grant or restrict access from specific nodes on the network.
- Allow security to be used for a custom automation purpose.
- Grant or restrict access to application actions such as Exit Application, Ack Alarms, Add Trend Pens, etc.

Configure Security Server

To configure the Security server, the following steps have to be completed.

1. To start the Security Configurator click **Start, Programs, ICONICS GENESIS-32, Tools, Security Configurator**
2. The first time you login with an empty user name and password **ICONICS**. The challenge number can be used when you forgot your administrator password and would like to receive a backdoor password from support@iconics.com



Fig. 1 Administrator Login

3. Select from the menu File, New. When you are asked to create the file in Basic mode, choose YES to create a configuration in Basic Mode. Then save the file as **MySecurity.sec**
4. Click on the **New Group** icon in the toolbar and add a group called **Administrators**, then press OK.



Fig.2 Add Administrators Group

5. You may then wish to change the group's **Account Policy** settings as shown in the figure below.

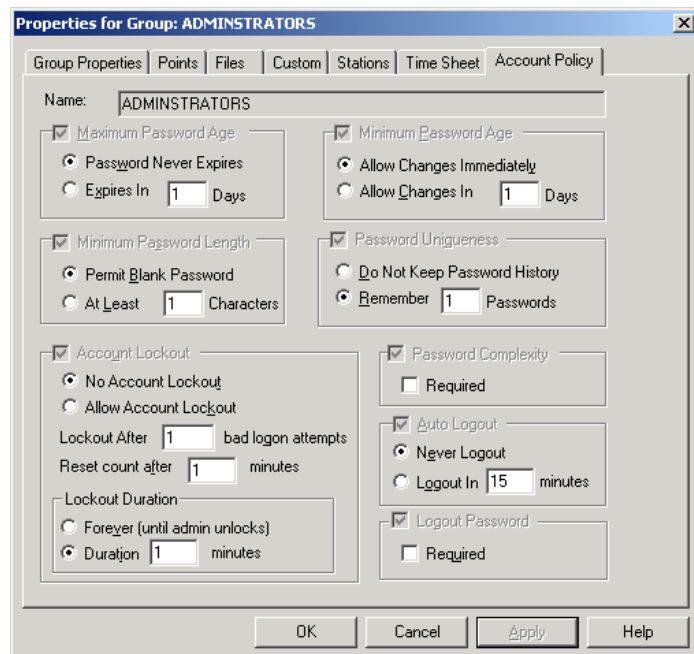


Fig.3 Account Policy Settings

6. Click on the **New User**-icon in the toolbar and add a user called **Administrator**. Specify a password that you will not forget. Add this user to the Group called **Administrators**. Also check the **Security System Administrator** checkbox and uncheck the **Account Disabled** checkbox as shown in Fig. 3.



Security Basic Mode Quick Start

APPLICATIONS NOTE

January 2003

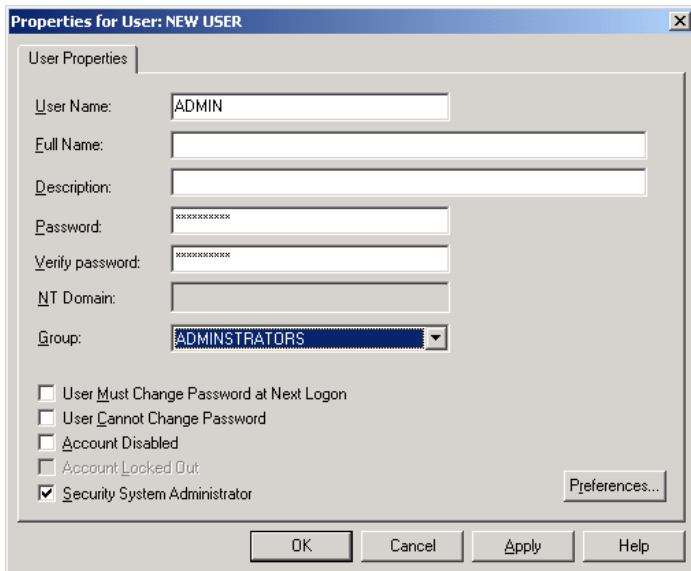


Fig. 4 Administrator Settings

- Click on the **New Group** icon in the toolbar in order to add groups called **Engineers, Operators** and **View Only**
- Click on the **New User**-icon in the toolbar and add a user called **JOHN**. Specify the password and group, and uncheck the **Account Disabled** checkbox. Assign John to be a member of the View Only Group by clicking on the **View Only** group, then click on **JOHN** and click the **Associate User & Group** icon on the toolbar.
- To give write protection to all OPC Tags, double-Click the **View Only** group, select the **Points** tab and configure it to Exclude: *

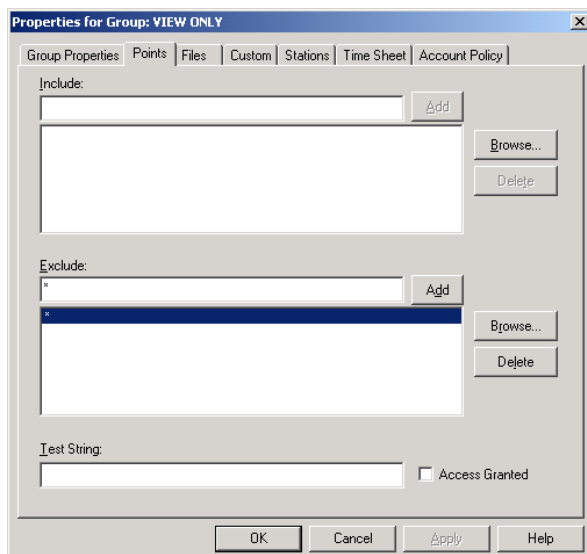


Fig. 5 Protecting OPC Tags

- To give the **View Only** group access to a GraphWorX32 display called "mainmenu.gdf", double-click on **View Only**, select the **Files** tab and add **mainmenu.gdf** to the include list.

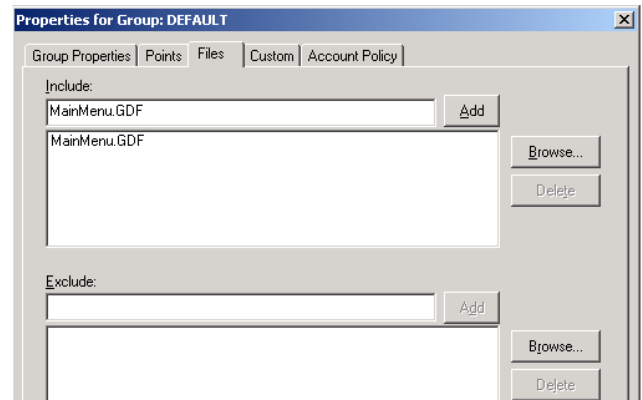


Fig. 6 Provide access to the MainMenu.gdf

- In order to give members of the **Engineers** group write access, you select its **Points** tab and configure it to Include: *
- Now, configure the permissions for GENESIS-32 applications for each user. Click on **Edit, Application Actions** to bring up the Actions/Users Associations screen. By default each user has full access to GENESIS-32 applications. Start by selecting **VIEW ONLY** from the Users/Groups listbox and remove all of the entries from that folder, except GWX32, AWXView32, and TWXView32.
- You can restrict the permissions of the **VIEW ONLY** group within GraphWorX32 by removing permissions from GWX32, such as **Exit Application, GenTray Autostop, Menu: Exit Runtime**, etc.

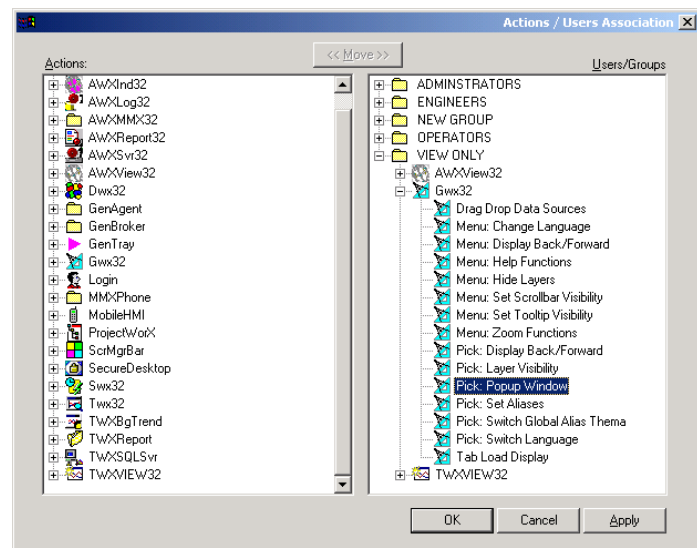


Fig. 7 Restrict Access for VIEW ONLY group



Similar to the steps performed for GraphWorX (steps 12 & 13) you can also protect access to your computer's Desktop.

14. Click on **SecureDesktop** in the Actions listbox, click on **ADMINISTRATORS** in the Users/Groups listbox and click on the **MOVE** button.
15. Add **SecureDesktop** to the **VIEW ONLY**. Then **DELETE** the **Full Desktop** action from the **SecureDesktop** application within VIEW ONLY.
16. In order for secure desktop to function, the secure desktop manager needs to be started by using **GenTray**

Please avoid making any mistakes when trying the Secure Desktop. In action, your Windows Start button, Ctrl-Alt-Del, Alt-Tab will not allow any access until a person with the appropriate security rights (Step 16) is logged in.

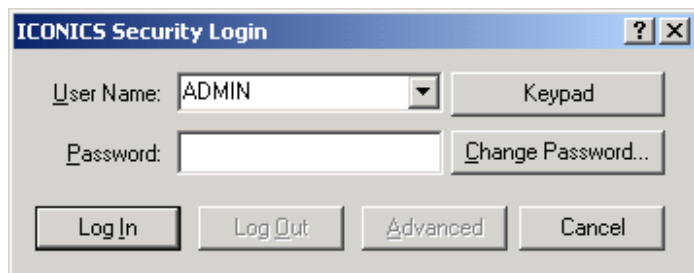


Fig. 8 Login dialog during runtime

In order to **Login**, you can select **Tools, Security Login ...** from the menu bar in **GraphWorX32** during runtime. Alternatively you can also start the Login.exe program by selecting **Start, Programs, ICONICS GENESIS-32, Security Login**. If required the login procedure can also be performed through OLE Automation.