Security Advanced Mode Quick Start

APPLICATIONS NOTE

August 2004

Description: The security server allows you to protect your SCADA/HMI and WebHMI applications against unauthorized access.
OS Requirement: The operating system required is Win XP/2000/NT.
General Requirement:
Working knowledge of Genesis32 and Genesis32 terminology.

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 forget your administrator password and would like to receive a backdoor password from support@iconics.com.

Fig. 1 Administrator Login

3. When creating a new security configuration you will see the next dialog. Click **No** since you want to configure in Advanced mode.

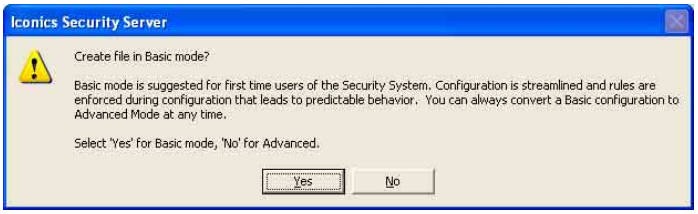

Fig. 2 Configure in Advanced mode

4. You could use the NT security database from your computer or a Domain server, but click **Cancel** since you would like to manually add groups and users.

Fig. 3 Optionally integrate NT security

5. Specify a file name for your security configuration e.g. **mySecurity.sec** and click the **Save** button.

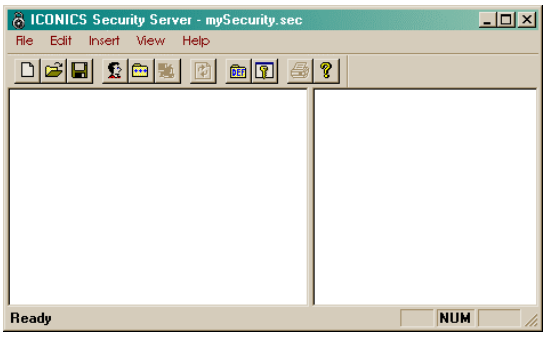

Fig. 2 Security Configurator

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

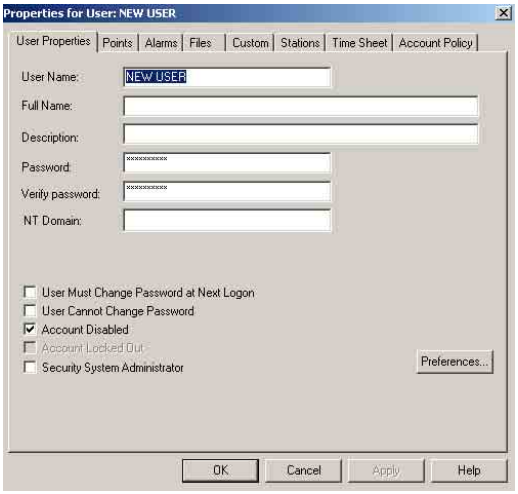

Fig. 3 Administrator Settings

7. Select from the menu **Insert, New User** in order to add a user called **JOHN**, and specify his password. Don't forget to **uncheck** the **Account Disabled** checkbox.
8. Select from the menu **Insert, New Group** in order to add groups called **Engineers, Operators** and **View Only**
9. To assign John to be a member of the View Only Group, click on the **View Only** group, click on **JOHN** and click the **Associate User & Group-icon** on the toolbar.
10. To give write protection to all OPC Tags, double-Click the **View Only** group, select the **Points** tab and configure it to Exclude: *****

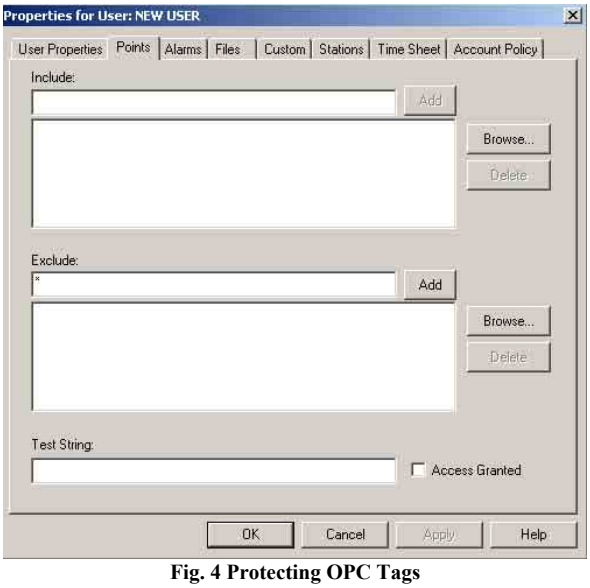

Fig. 4 Protecting OPC Tags

11. Select from the menu **Edit, Default Group** and give write protection to all OPC Tags by selecting the **Points** tab and configure it to **Exclude**: *****
12. In order to give members of the **Engineers** group write access, you select its **Points** tab and configure it to **Include**: *****
13. Select from the menu **Edit, Default Group**. To give access to your mainmenu.gdf display, select the **Files** tab and add **mainmenu.gdf** to the include list.

Fig. 5 Provide access to the MainMenu.gdf

14. Select from the menu **Edit, Application Actions…**. Click on **Gwx32** in the **Actions** list box, click on **ADMINISTRATORS** in the **Users/Groups** list box and click on the <<**MOVE>>** button.

Fig. 6 Allow Application actions to Administrators

15. Click on **Gwx32** in the **Actions** list box, click on **DEFAULT** in the **Users/Groups** list box and click on the <<**MOVE>>** button.
16. Select the Next GraphWorX actions in **DEFAULT** and **Delete** them:
    - **Exit Application**
    - **Menu: Exit Runtime**.

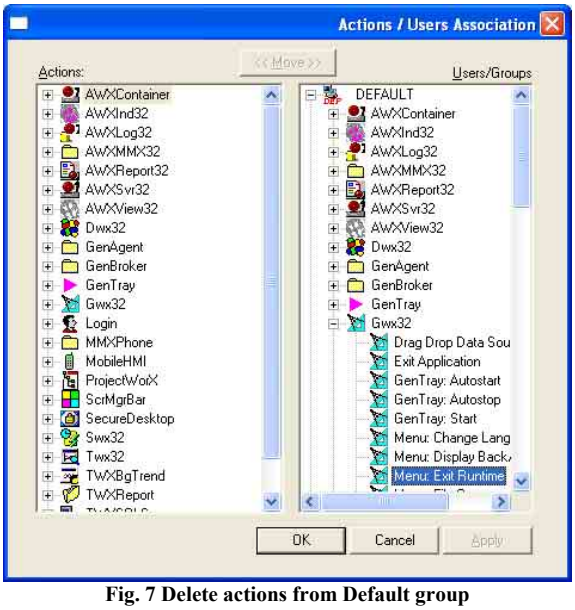

Fig. 7 Delete actions from Default group

NOTE: This protects GraphWorX32 from being stopped by any unauthorized person. Similar to the steps performed for GraphWorX32 (step 14 and 15) you can also protect access to your computer's Desktop.

17. Click on **Secure Desktop** in the **Actions** list box, click on **DEFAULT** in the **Users/Groups** list box and click on the <<**MOVE**>> button.
18. Select the Secure Desktop action **Full Desktop Access** in **DEFAULT** and **Delete** it.
19. In order for secure desktop to function, the secure desktop application needs to be started by using **GenTray**

NOTE: Please avoid making any mistakes when trying the Secure Desktop. Your Windows Start button, Ctrl-Alt-Del, Alt-Tab will not allow any access until a person with the appropriate security rights (Step 14) is logged in.

Fig. 8 Login dialog during runtime

NOTE: In order to **Login**, you can select **Tools → Security Login …** from the **GraphWorX32** menu. 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.