



Security Basic 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 access Security Configurator, a blank Security application opens up link figure below.

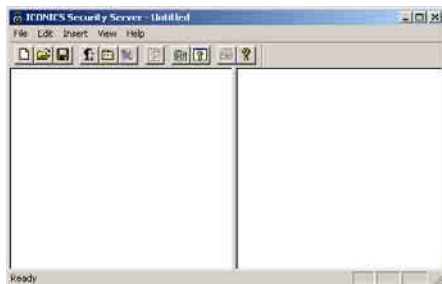


Fig.1 ICONICS Security Configurator

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.

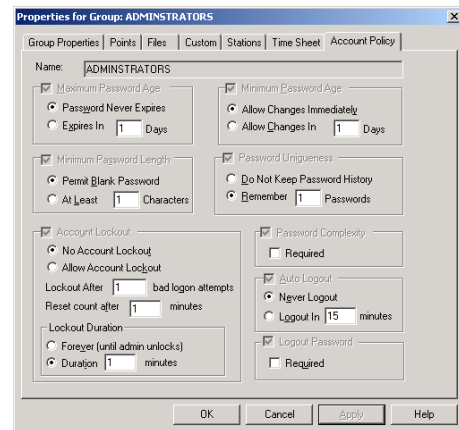


Fig.3 Account Policy Settings

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.

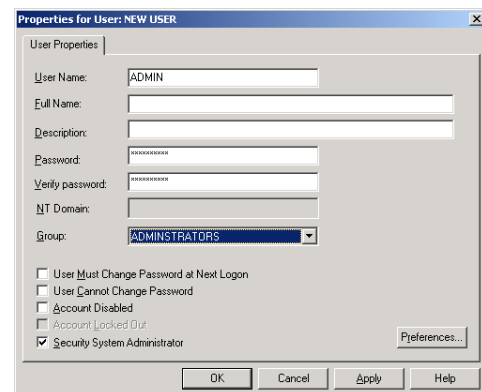


Fig. 4 Administrator Settings

7. Click on the **New Group** icon in the toolbar in order to add groups called **Engineers**, **Operators** and **View Only**
8. Click on the **New User**-icon in the toolbar and add a user called **JOHN**. Specify the password and group,



Security Basic Mode Quick Start

APPLICATIONS NOTE

August 2004



and uncheck the **Account Disabled** checkbox. Assign John to be a member of the View Only Group.

- To prevent users of View Only group from **writing** to OPC Tags, double-Click the **View Only** group, select the **Points** tab and configure it to Exclude: *

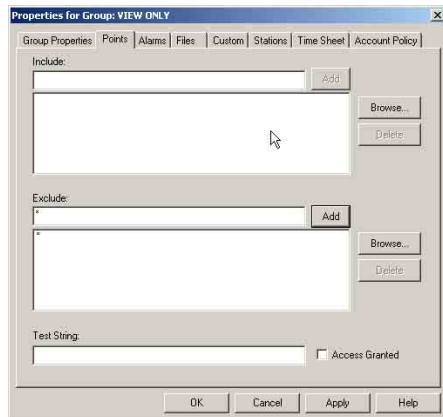


Fig. 5 Protecting OPC Tags

- To give the **View Only** group access to a GraphWorX32 display called **AlarmWorX32_GenEvent.gdf**, double-click on **View Only**, select the **Files** tab and add **AlarmWorX32_GenEvent.gdf** to the include list. Delete "*" from Include list.

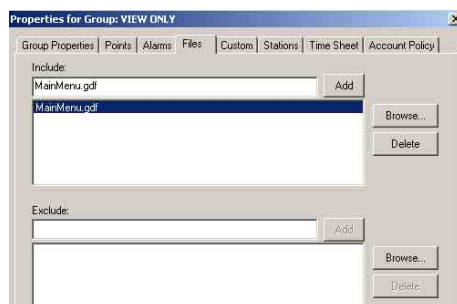


Fig. 6 Provide access to the MainMenu.gdf alone

- 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 GENESIS32 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 GENESIS32 applications. Start by selecting **VIEW ONLY** from the Users/Groups list box and remove all of the entries from that folder, except GWX32, AWWXView32, 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.

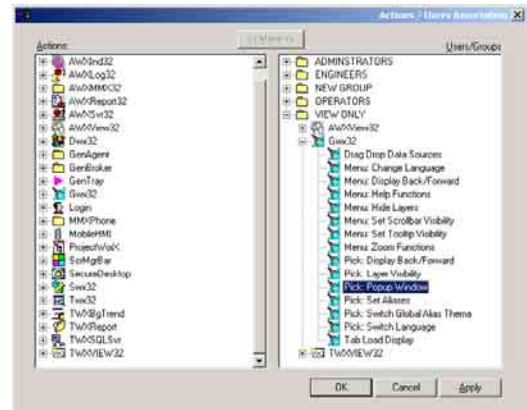


Fig. 7 Restrict Access for VIEW ONLY group

- Try to run GenDemo (from **Start → Programs → ICONICS GENESIS-32 → Gen32Demo**) and you should see the Security Violation screen as below.



Fig. 8 Security Violation screen

- Click on the big center rectangle to bring up the Login dialog. Log in as Administrator with his password.



Fig. 9 Login dialog during runtime

- Since Administrator has access to all GraphWorX32 screens, you will see the Gen32 Demo. Navigate to the **AlarmWorX32_GenEvent.gdf** display.
- Go to **Tools → Security Login** on the GraphWorX32 screen, and Log out Administrator, Login as John.
- Since John has access to **ONLY** the AlarmWorX32_GenEvent.gdf display, he will be able to see the display.



Security Basic Mode Quick Start

APPLICATIONS NOTE

August 2004



19. However John will NOT be able to WRITE to the OPC data Entry field, since the point will be grayed out like below. This is because we excluded all points (*) from Write list for John.



Fig. 10 Security Write protection on Data Entry fields