

Description: Guide to setup your SCADA/HMI and WebHMI applications against unauthorized access using ICONICS Security Server

OS Requirement: Win 2000 Pro/Server, XP Pro, Server 2003

General Requirement: Working knowledge of Genesis32 and Genesis32 terminology.

Introduction

For security and management purposes, sometimes it is necessary to create users with specific privileges to perform certain tasks. The ICONICS Security Server allows you to have such a configuration and level of security. Below is a list of what the security server can do:

- 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.

Advanced vs. Basic Mode

Advanced mode allows to do a few things that we cannot do in Basic mode such as:

- Use NT Integrated security
- Configuring the default (non-logged-in) user permissions
- Configure permissions on both a group and user basis
- Associating users with more than one or no groups

NOTE: Whenever permissions overlap, the permissions that are **LEAST** restrictive take precedence.

Configuring the Security Server

1. Go to Start → Programs → ICONICS Tools → Security Configurator to launch the Security Configurator.
2. When creating a new security configuration, you will see the next dialog show in Figure 1. Select Advanced Mode and click “OK”.

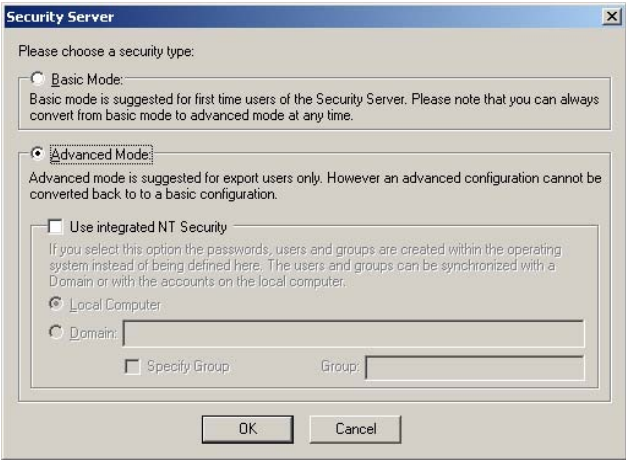


Figure 1 - Selecting Configuration Mode

3. Specify a file name for your security configuration and click the **Save** button. A blank configuration will appear.
4. Click Edit → Default Group from the menu options. To Prevent anyone who does not have permission from writing to a point, an alarm, or seeing a display, delete the “*” under the “Allow Writing” area.

NOTE: The Default Group settings applies to EVERYONE except those users and groups that has included permissions in the configuration. This set up will NOT allow any one who does not log in to view any files.

5. Click on the **New User** icon  in the toolbar and add a user called **Administrator**.
6. Specify a password that you will not forget, **uncheck** the **Account Disabled** checkbox and **check** the **Security System Administrator** checkbox as shown in Figure 2.

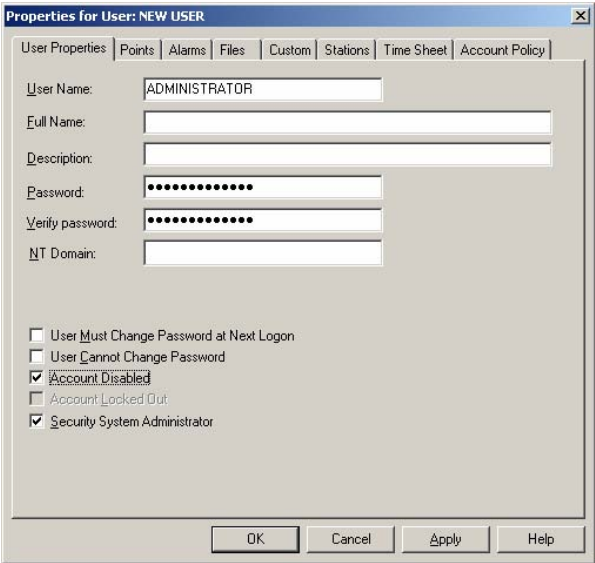


Figure 2 - Administrator Settings

7. Click on the Points tab and add a “*” to the **Allow Writing** area by typing in “*” in the text box and click on the **Add** button. Do the same for the Alarms Tab.
8. Add a “*.*” to **Allow Writing** are to grant permission for viewing all displays.
9. Add another user called **JOHN**, and specify his password. Don’t forget to **uncheck** the **Account Disabled** checkbox.
10. Click on the Files tab and type in one of the displays that you have on your machine (i.e. AlarmWorX32_GenEvent.gdf).
11. Click on the **New Group** icon , to add a group named Engineers. Alternatively, you can select from the menu Insert → New Group to add the Group.
12. Repeat step 7 to create a group named View Only
13. Click on the **View Only** group, then click on **JOHN** and select the **Associate Users with Groups** icon  on the toolbar.
14. Click on Edit → Application Actions... from the menu. The Actions/Users Association window will appear.

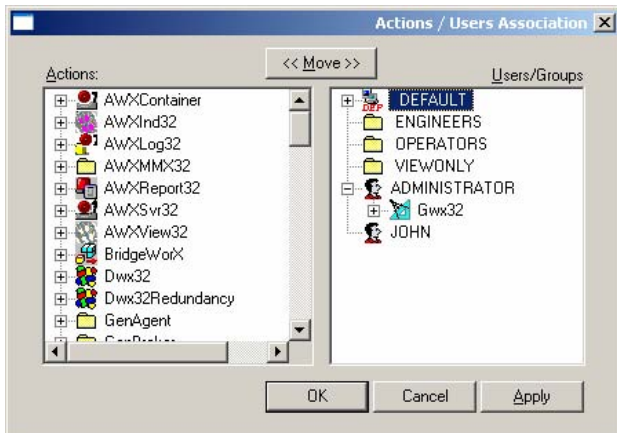


Figure 3 - Application Actions

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

NOTE: This protects GraphWorX32 from being stopped by any unauthorized person.

18. Click on **Secure Desktop** in the **Actions** list box, click on **DEFAULT** in the **Users/Groups** list box and click on the **<<MOVE>>** button.
19. Select the secure Desktop action **Full Desktop Access** in **DEFAULT** and **DELETE** it.

20. 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 is logged in.

21. You can now test your security by opening the Gen32Demo from Start → Programs → ICONICS Tools → Gen32Demo or any other display you would like. Notice that you will not be able to go into runtime to see any displays unless you are logged in. A Warning message pops up and Login dialog shown in Figure 4 appears. Log in as JOHN.



Figure 4 - Login Dialog

22. Notice how you are unable to write any values to an OPC Point.
23. Log in as the Administrator now, by clicking on Tools → Security login in the GraphWorX32 runtime menu. You should be able to write to any points once you are log in.

NOTE: Remember that we only grant JOHN access to view one display (the AlarmWorX32_GenEvent.gdf display). You will need to log in as the Administrator to see any other displays or give JOHN the permissions to view other displays.