

Description: Guide to setup the Security Server to protect your SCADA/HMI and WebHMI applications against unauthorized access.

OS Requirement: Win XP/2000/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

Basic mode does not allow us to do the following things that we can do in Advanced mode:

- 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 → SecurityConfigurator to launch the Security Configurator.
2. The first time you access Security Configurator, a blank Security application opens up.
3. Click on File → New to create a new configuration. When you are asked to choose a security type, select Basic Mode. Give the configuration a name and save the file.
4. Click on the **New Group** icon  in the toolbar and add a group called ADMINISTRATORS
5. You may edit the group's **Account Policy** settings by clicking on the Account Policy tab.

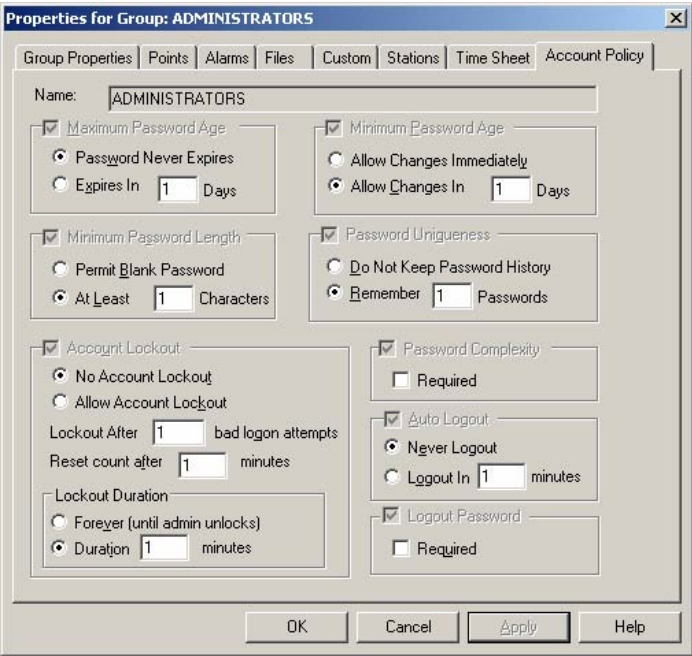


Figure 1 - Account Policy Settings

6. Click OK when you are done editing.
7. Click on the **New User** icon  in the toolbar and add a user called **Admin**. Specify a password that you will remember.
8. Select the ADMINISTRATOR group you have created in step 4 for Group.
9. Check the **Security System Administrator** checkbox and uncheck the **Account Disabled** checkbox as shown in Figure 2. Click OK when done.

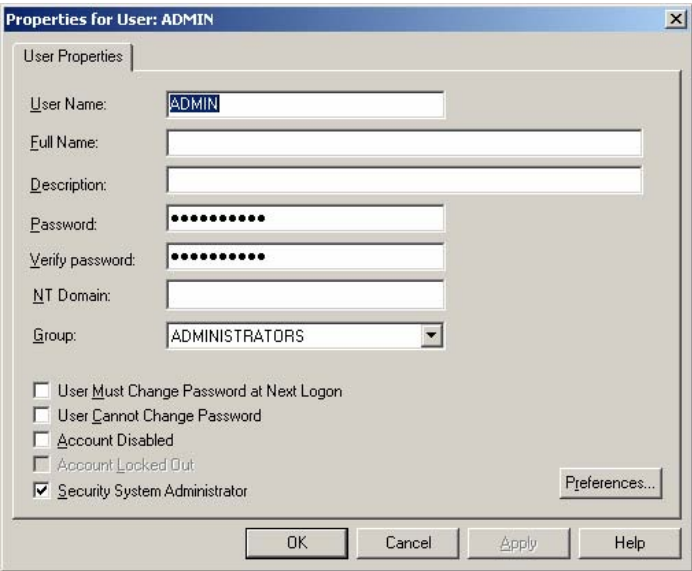


Figure 2 - Administrator Properties



Security – Basic Mode Quick Start



APPLICATIONS NOTE

December 2007

10. Click on the **New Group** icon  in the toolbar in order to add a group called **View Only**.
11. Click on the **New User** icon  in the toolbar and add a user called **JOHN**. Specify a password, select the View Only Group, and uncheck the **Account Disabled** checkbox.
12. To prevent users of View Only group from writing to OPC Tags, double-Click the **View Only** group, select the **Points** tab and add “*” to the Deny Write field, then click on the add button.
13. 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 allow writing list. Delete “*”.

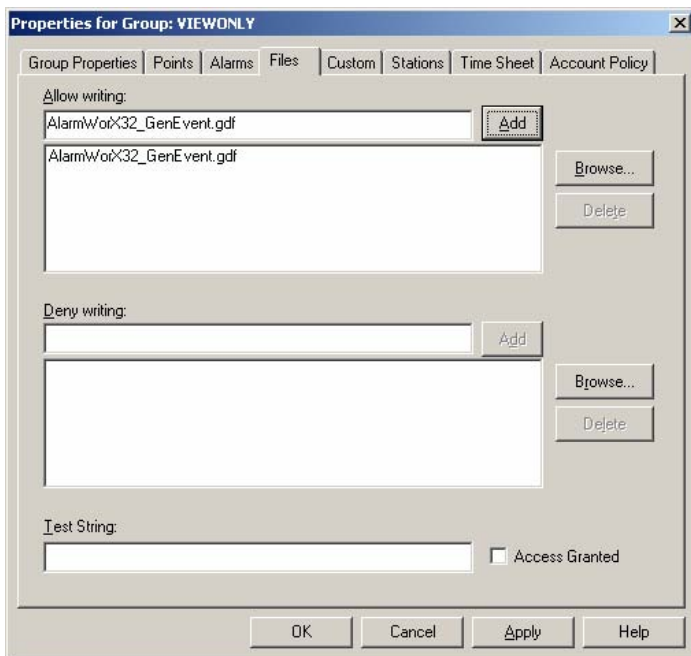


Figure 3 - Provide Access to AlarmWorX32_GenEvent.gdf

14. Now, configure the permissions for GENESIS32 applications for each user. Click on **Edit → Application Actions** to bring up the Actions/Users Associations screen.
15. By default each user has full access to GENESIS32 applications. Start by selecting **VIEW ONLY** from the Users/Groups list box and add entries for GWX32, AWXView32, and TWXView32 from Action List box.
16. 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.

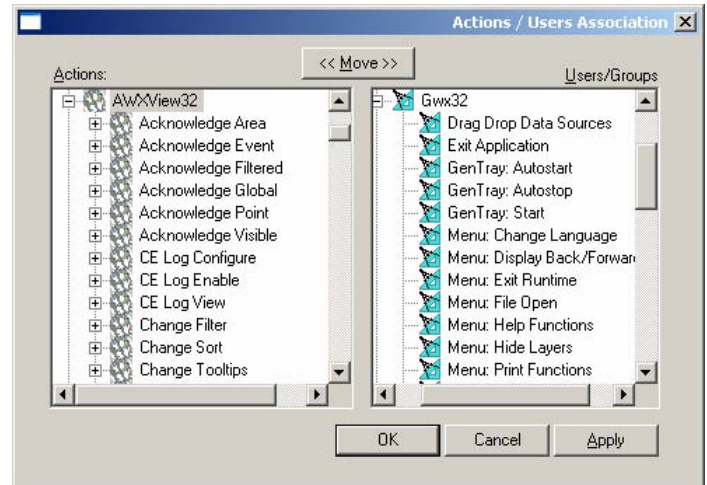


Figure 4 - Restricting Application Access from VIEW ONLY Group

17. Test the configuration by opening Gen32Demo from Start → Programs → ICONICS Tools → Gen32Demo. Select the display AlarmWorX32_GenEvent

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.