Security – Security Configuration Settings

APPLICATIONS NOTE

April 2010

Description: Guide to using ICONICS Security with GENESIS32
OS Requirement: Win 2000, XP Pro, Server 2003, Vista, Server 2008, Windows 7
General Requirement: ICONICS GENESIS32 v9.x Installation, basic GENESIS32 knowledge, and ICONICS Security knowledge

Introduction

GENESISS32 comes with a Security Server, a software component for providing user and group-level security for your entire GENESIS32 system. You can define as many groups and individuals as required by your project. Each user can have unique access restrictions on OPC Data Point, files, workstations, and more. Further restrictions can be placed on individual actions with the various components of GENESIS32 (e.g., GraphWorX32, TrendWorX32, AlarmWorX32, etc.) on a per-user basis. For example, only Engineers can enter the development environment, and only Managers can add points to a Trend View. Simply add or subtract permissions from the action list.

During runtime, the Security Server takes care of logging people into (and out of) the system, as well as reporting this information to the GenEvent server. This way audit trails can be logged and/or printed as well as viewed on GENESIS32 workstations.

This application note is a supplement to the *Security – Advanced Mode Quick Start* application note. We aim to describe some of the additional security settings available as well as demonstrate how you might use ICONICS Security.

The Default Group

The system **Default Group** (available in advanced security configuration mode only) contains access rights when no one is logged into the system. When you first create an Advanced Security Configuration, the default group has full access to everything. The first step in configuring the security system is to remove most if not all access rights assigned to the default group.

> **NOTE:** The default group should have the minimum access rights, because all users will inherit the rights configured in the default group. Furthermore, you cannot remove rights already granted in the default group in configured users or groups.

To edit the default group, select Default Group from the Edit menu in the Security Configurator. This opens the Properties dialog for the default group, as shown in Figure 1. The same property pages used to edit ordinary groups are used for the default group, with the following differences:

> There is no Stations property tab. Default access is valid for all stations.
> There is no Time Sheet property tab. Default access is valid for all hours.
> Account Policy must be set in the default group. This is the policy that new groups and users will default to when creating them.

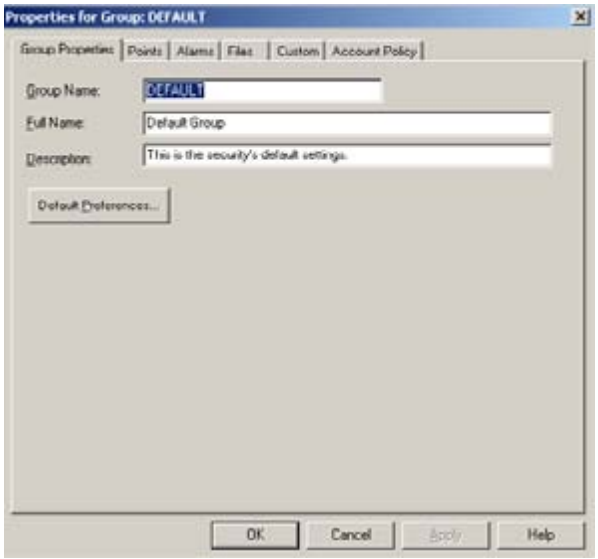

Figure 1 - Properties for Default Group

Global Settings

Sometimes it is necessary to customize the Global Security Settings (e.g. Simultaneous Logins, Allow User Lists). You can access these options from menu Edit → Global Settings.

You will find the following options on the Policy tab of the Global Settings dialog:

> **Allow Auto NT Login**: If you are using Windows security, you can enable this option to log in the user when he logs into Windows.
> **Allow User List**: this option allows you to see the list of predefined users in the Security Login dialog.
> **Display Last User**: when enabled, this option will show the last logged in user in the Security Login dialog.
> **Include User's Full Name in Events**: Security user events are reported to the GenEvent server, you can enable this option to report the user's full name in the event as oppose to the login name.

Simultaneous Logins: when enabled, this option allows you to login multiple users at the same time. Without this option checked, the security system will always only allow one user to log in at a time.

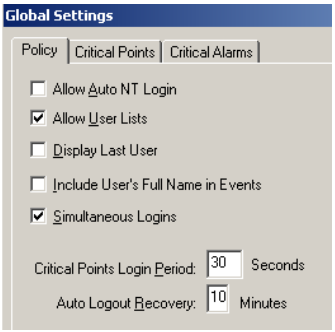

Figure 2 - Global Settings

Aside from the Policy tab, there are two more tabs on the Global Setting dialog: Critical Points and Critical Alarms. Sometimes, there will be very important OPC points and alarms that you want to make sure that the person writing to the point or acknowledging the alarm to provide credentials again. In such cases, you can add those points and alarms into the configuration using the respective tabs.

During runtime, when a user tries to write to that OPC point, he will need to provide his credentials again. The "Critical Point Login Period" parameter specifies the length of time the user has after logging in to write to the Critical Points (or acknowledge Critical Alarms) before he will have to provide his login again.

Demo Security Configuration

Now that we know a bit more about the options available in the Security Configurator, let us create a configuration. If you need help creating the following configuration, you should refer to the *Security – Advanced Mode Quick Start* application note.

For our example, you should remove all permissions in the Default group and configure the global settings as shown in Figure 2.

We will create three groups: Administrators, Engineering, and Operators. Naturally, the Administrators should have all access with no limitations. The Engineering group should have less permissions then the Administrators group, but more than the Operators group. Since the Deny permissions takes precedence over the allow permissions, we are going to use the wild card character * (asterisk) in all of the allow fields for all three groups. The only exception is the operators group. We will add the point:

ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT[1-3]

in the Deny section of the Points tab as well as add a * (asterisk) in the Deny section of the Alarms tab. This will deny the operators from acknowledging alarms. We will also deny the group from accessing Layer1 in Display1.gdf by adding the string "Display1.gdf|Layer1" into the deny section of the Files tab.

> **NOTE:** the syntax to specify a layer is in the form of *file.extension|Layer*. The character between the fie extension and the layer name is a pipe (the character above the back slash \).

Since the Administrators group will have the most permission, we will tighten the account policy to protect the users in this group. You can leave most settings default, and refer to for the settings you should change.

Table 1 - Account Policies

Group	Min Password length	Required Password Complexity	Auto Logout Time
Administrators	At least 6 chars	Yes	10 min
Engineering	At least 1 char	No	30 min.
Operators	At least 1 char	No	30 min.

Now that we have created groups, we will create some users. We will create Administrator, Engineer, and Operator1 as our users. Each of these user should associate to the respective group. They will then inherit the permissions specified in the group.

As the last step, we will add Application Actions into our groups. You should remove all application actions from the Default group and add all actions into the Administrators group.

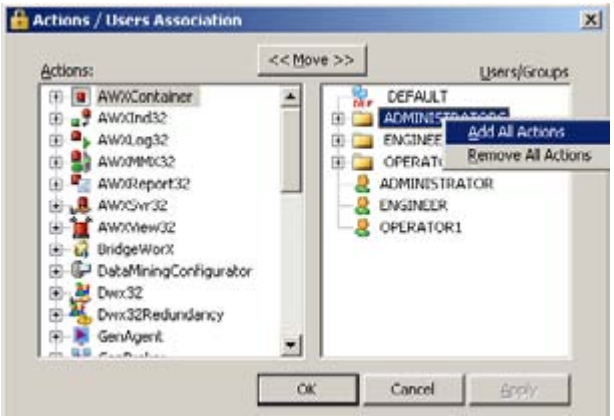

Figure 3 - Application Actions

You can also add all permissions to the Engineering group, but remove the Login → Advance View permission. Since the Operators will have much less permissions, it will be easier to

add just the permissions one by one. You should add the following permissions to the Operators group:

Gwx32 → Exit Application
Gwx32 → Exit Runtime
Secure Desktop → GenTray: Automatic
Secure Desktop → GenTray: Autostart
Secure Desktop → GenTray: Autostop
Secure Desktop → GenTray: NT Service
Login → Advanced View

Testing Your Security Configuration

Now that we have configured our security, you should test your security configuration in steps. Below are the suggested steps to test your security configuration.

Testing Application Access

You can start with standard actions like switching GraphWorX32 from runtime to configuration mode without any user logged into the system. You would see the same security warning as it shows in Figure 4. It is not an error message, but a warning that indicates the user does not have enough permission to complete this action and needs to login with a different user with appropriate permissions.

Figure 4 - Security Warning

If you have denied permissions for accessing other applications, you can also check this with other applications. While the popup warning may word differently, the effect is similar. It will block a user from accessing the application if the logged in user does not have permission.

Testing OPC Point Permissions

You should also verify that Operator does not have enough permission to write into the specific process point, because ICONICS Security (Deny Write) secures it.

When nobody is logged in, then the Guest user (default group settings is applied) cannot write to a process point, but project managers and administrators can.

Figure 5 – Allowed Writes to OPC Points in Display1

Figure 6 - Denied Writes to OPC Points in Display1

NOTE: Notice that there are grayed out buttons in Figure 6. This is because those buttons contains Pick Actions that would write values to the secured OPC points. The grayed out color indicates that those buttons are inaccessible due to lack of security permissions.

Testing Secured Layer

Last test that you should do is to verify that your preconfigured Layer in GraphWorX32 is secured based on user level. See the figure below where Operator1 (Operators group) does not have permissions to see the Layer1 which is part of your Display1.gdf.

Figure 7 - Secured Layer for Guest User