GenBroker – Securing Communications with GenBroker

APPLICATIONS NOTE

April 2010

Description: Guide to configuring GenBroker to secure WebHMI and other OPC-DA communications
OS Requirement: Win 2000, XP Pro, Server 2003, Vista, Server 2008, Windows 7
General Requirement: A working knowledge of GenBroker communications and GENESIS, WebHMI, or BizViz version 9 and above.

Introduction

With the recent cyber security concerns – especially when public and private networks are interconnecting – it is extremely important to implement very tight security. ICONICS products architecture has a built in security feature that is very powerful yet simple to configure.

GENESIS32 has a networking module called GenBroker that is fully integrated with ICONICS Security Server. Apart from GenBroker Security, you may also apply additional IIS and Windows security.

The first recommendation is to use the SOAP/XML option from GenBroker and WEBHMI Server, even though the SOAP/XML is slightly slower than the communication over TCP/IP. See separate the *GenBroker - Setup for SOAP/XML* application note for more details on how to implement the SOAP/XML communication channel.

GenBroker communications carry OPC data, alarms and events, historical trend data, licensing, security, and aliasing information over TCP/IP. Unwanted viewing and modification of this data is secure from non-ICONICS components because it is a binary data stream only readable by ICONICS products.

However, since all ICONICS products can read and write to the GenBroker data stream we need to be able to protect our communications from old or rogue installations of ICONICS products and from users that should not be able to access certain GenBroker data.

In order to accomplish this, we can use the enhanced security settings available from the GenBroker Configurator. Under the Advanced → Server branch of the configurator, there are two sections that we will configure to enhance security: Security and Client IDs. This document will discuss these options and how they help to secure your data.

Configuring GenBroker

1. Go to Start → Programs → ICONICS Tools → GenBroker Configurator and you should see a screen similar to Figure 1.

Figure 1 - GenBroker Configuration Selection Screen

2. Click on Edit if you already have an active configuration, or New to open a new one. When the configurator opens, expand down to Advanced → Server → Security.

Figure 2 - Security Branch

3. Check the "Read Only" checkbox. This will limit clients that communicate with the GenBroker Server from performing a write requests to the OPC Data Server. Clients will have read-only access to the data.
4. Check the "Restricted Functionality" check box. This will limit the type of data that clients may use to communicate with the GenBroker Server. It is recommended to uncheck the "Browsing" option that will disable the network and tag browsing.

Figure 3 - Security Selections

5. If you check the "Require Credentials" check box, the GenBroker Server requests additional user credentials from

the client. The user on the client machine will see a login dialog to enter login credentials as shown in Figure 4 (note, this is NOT the ICONICS Security credentials).

Figure 4 - Login dialog to enter login credentials

NOTE: If you want to define the credentials for automatic login for the client, open client GenBroker file and expand down to Advanced → Client → Security. Check User defined credentials for automatic login check box and specify NT credentials if you want to use them.

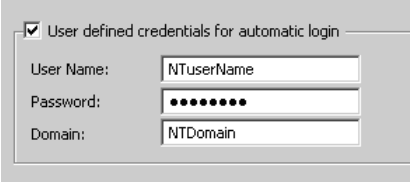

Figure 5 - Automatic Login Credentials

Encryption type specifies if the password will be encrypted when a user on the client machine tries to log in to GenBroker Server. The length of the encryption key can be 40 bits or 128 bits.
The **Lockout** specifies the amount of time (in minutes) that the server will not allow the user to connect if the user had a specified number of unsuccessful login attempts. If a client application, such as GraphWorX32, requests data from GenBroker Server, the server will wait for the specified time period (in seconds) to receive and validate login credentials from the client. If server does not receive the login credentials within the specified time period, then the server rejects the request to the client with an error.

6. In GenBroker Configurator tree control on the left-hand pane, select "Client ID" to restrict connectivity for selected clients only.
7. Check the "Required Client IDs" checkbox. This will open up options that allow you to name specific nodes that can access the GenBroker Server.

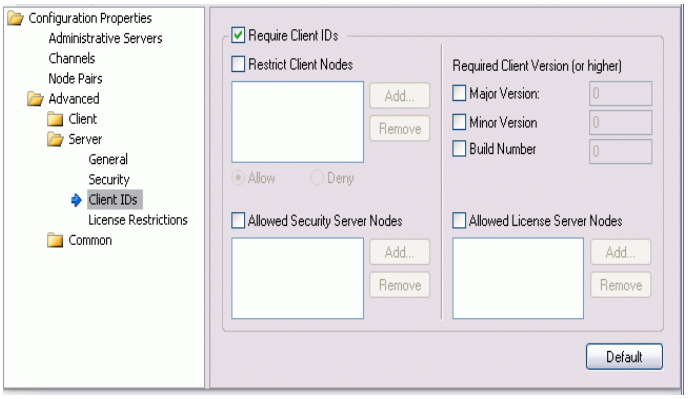

Figure 6 - Client IDs Dialog

8. Check the "Restrict Client Nodes" checkbox, which will allow you to specify clients that are allowed or denied to access the GenBroker Server. You can specify computer name, IP address, or DNS name here.

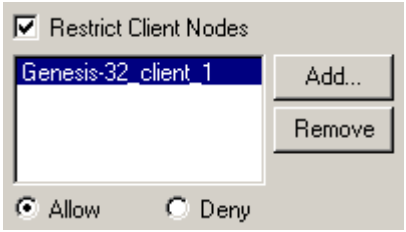

Figure 7 – Setting-up the Allowed Nodes

NOTE: All nodes specified are either all allowed or all denied. You may not have one allowed node and one denied node.

9. With the "Required Client Version" configuration you can also allow only specific versions of client nodes to connect. For example, you may want to only allow clients with GenClient version 9.0.156. **Error! Reference source not found.** shows the different parts of the version number.

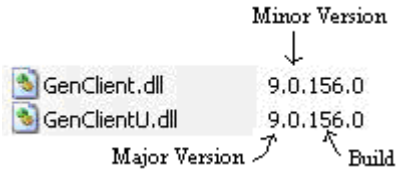

Figure 8 - Verifying Versioning

10. In order to verify what version your client may be running, open a Windows Explorer and browse to *C:\Windows\System32* and find the version number for "GenClientU.dll" by right-clicking on the file and looking at its properties. This version can be input into the configuration as seen in the figure below.

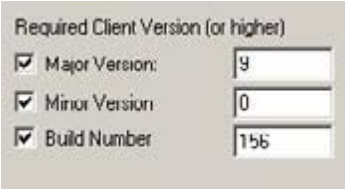

Figure 9 - Configuring for a Specific Version of GenClient

11. Check the "Allow Security Server Nodes" checkbox in order for a specific security server to connect to your GenBroker server.
12. Add the name or IP Address of your ICONICS Security Server. Using this method, only clients logged onto the specified ICONICS Security server(s) will have access to data via your GenBroker server.

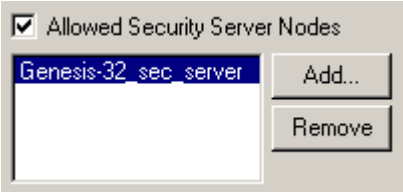

Figure 10 - Setting up a Specific Security Server Node

13. For example, you may have two GENESIS32 servers A and B each with its own security configuration. Clients logged to system A with valid credential may try to access application of system B. If you have set up GenBroker as in Figure 9 then it will force all clients to login to "Genesis-32_sec_server" security for access before any data will be served. This makes the GenBroker server to be more secure.

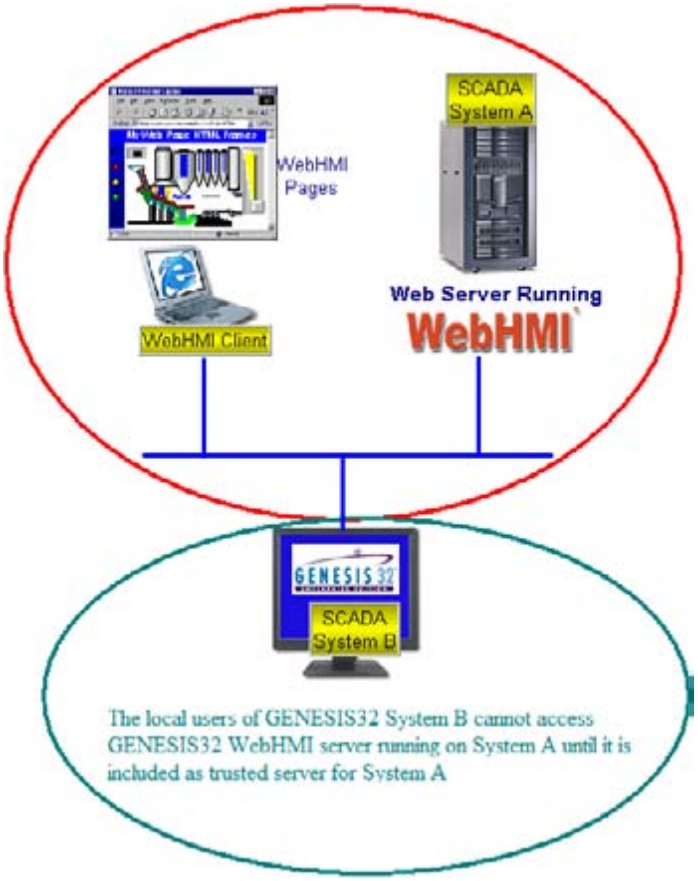

Figure 11 - Example System Architecture

14. Check the "Allow License Server Node" to specific set of licensing servers that could connect to your GenBroker server.
15. Then add the node name or IP Address of those servers into the list.