GenBroker Security
Advanced server-side security settings
Knowledge Base Article

Keywords   GenBroker, Security
Description   Advanced security settings within GenBroker for protecting GENESIS32 and BizViz servers.
Requirements

Introduction

In addition to the features provided by the ICONICS Security Server application, there are a number of advanced security features within the GenBroker Configurator. These features can help further protect your ICONICS GENESIS32 or BizViz server from unauthorised access.

Security Settings

The GenBroker Configurator has a number of security features under the **Advanced > Server > Security** section of the tree. The following options can all be found here.

Force Read Only

It is possible to force all OPC tags on an ICONICS server to be read-only to all connecting clients. To enable this, simply check the Read Only check box. All tags, regardless of their OPC server defined settings will now become read-only.

Restrict Functionality

By default, a client node can request any type of data from an ICONICS server. You may want to restrict the specific functionality your server provides to clients. This is possible not only for the basic OPC DA, AE and HDA data, but also for specific ICONICS functionality such as Global Aliasing, Licensing and ICONICS Security. Each type of functionality can be independently enabled or disabled.

Client Restrictions

In addition to the settings on the security page of the GenBroker Configurator, there are some additional settings for client restrictions. These can be found under the **Advanced > Server > Client Ids** section of the tree.

Restrict Client Nodes

It is possible to restrict the client nodes that are allowed to connect to your ICONICS Server by adding to this list. By default, the list is empty (and the check box un-ticked) meaning that any client machine can access the server. To add to the list, simply specify the node name or IP address of the clients that will be allowed access. Any clients not in this list will be denied.

Restrict Client Version

Of those clients that are allowed access to your ICONICS server, you can further restrict the client versions that are granted access. Check the options required to start filtering out clients that do not meet the version criteria.

Restrict Security Servers

A very useful feature of the GenBroker security settings is the ability to restrict access based on the client's security server. Typically, a client will pick up its security privileges from your main ICONICS server. It is however, entirely possible that a client can be configured to point to another node for its security. This can be undesirable, especially if the other security server can be configured to open up full access. To prevent this behaviour, you can specify the allowed security nodes in this section of the GenBroker Configurator. Clients that are picking up security from unspecified security servers will be denied access.

Restrict License Servers

In a similar fashion, access can be restricted based on a client's license server. As with the other security settings here, just simply enter the node name or IP addresses of the allowed servers.