

RECOMMENDED IGNITION SETTINGS FOR *groov*

IMPORTANT: If you are using the Ignition® Edge OPC-UA server and drivers included in the *groov* Box, do not use this technical note. See instructions in the *groov* Box User's Guide (form 2104) instead.

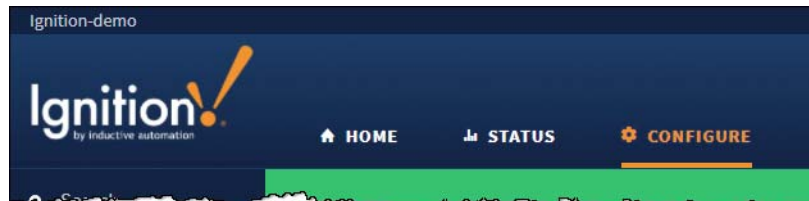
This technical note is intended for *groov* customers who want to use an external Ignition Enterprise OPC-UA tag server by Inductive Automation®. Examples:

- If you're using *groov* Server for Windows with Ignition Enterprise
- If you have a *groov* Box with the internal Ignition Edge OPC-UA server, and you also want to use Ignition Enterprise, for example to use additional drivers

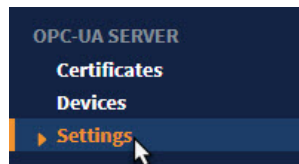
In cases like these, follow the steps below to use Opto 22's recommended settings for successful communication with *groov*.

CONFIGURING IGNITION

1. After installing Ignition, open the Ignition webpage.
2. Click the Configure tab.



3. Scroll down and find OPC-UA Server in the left panel. Click Settings.



4. In the Settings page, check Allow Anonymous Access.

Settings

Authentication	
Authentication Profile	<input type="text" value="opcua-module"/> The name of the authentication profile to authenticate against.
Allowed Roles	<input type="text" value="ReadWrite"/> Separate multiple roles with a comma (ex: Administrator,user,manager)
Allow Anonymous Access	<input checked="" type="checkbox"/> Allow users to connect whether or not they possess authentication credentials. (default: false)

5. Scroll down farther in the page and check Expose Tag Providers.

Expose Configured Tags	
Expose Tag Providers	<input checked="" type="checkbox"/> If enabled, Ignition tag providers will be exposed through the OPC-UA server, allowing third party clients to access the tags configured in the system. (default: false)
Auditing Enabled	<input type="checkbox"/> (default: false)
Audit Profile	- none - If enabled, writes to exposed tags will be audited to the selected profile.

6. At the bottom of the page, click Save Changes.
7. Exit the Ignition webpage.

WHAT'S NEXT

If you are running *groov* Server for Windows on the same computer as Ignition Enterprise, your communications are secure because they use a port on localhost (127.0.0.1:4096).

If *groov* Server for Windows and Ignition Enterprise are on different computers, inbound traffic to the Ignition OPC-UA server must be able get through the firewall on the TCP/IP service port *groov* uses to access this server. In this case, work with your IT Department to set up security and establish an Inbound Rule to the Windows Firewall for the Ignition service port on the computer where Ignition is installed.