Recommended Ignition OPC-UA Server Settings for *groov*

This technical note is intended for *groov* customers who want to use the Ignition® OPC-UA tag server by Inductive Automation®. Follow the steps below to use Opto 22's recommended settings for successful communication with *groov*.

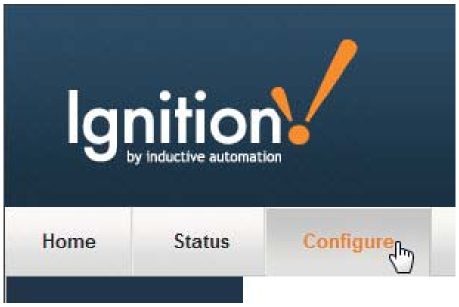
In this technical note:

Configuring Ignition 1

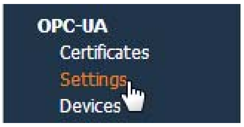
Configuring the Windows Firewall 3

Configuring Ignition

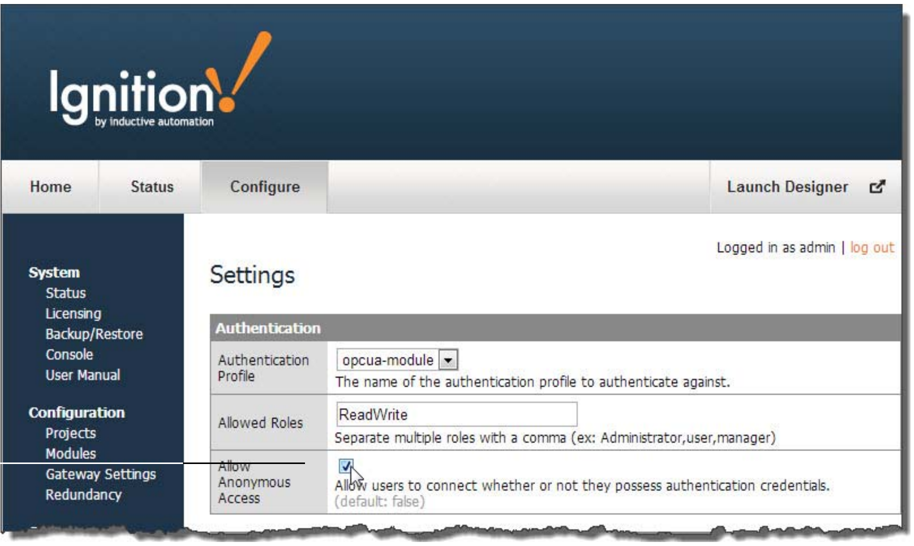
1. After installing Ignition, open the Ignition webpage.
2. Click the Configure tab.



3. Under OPC-UA in the left panel, click Settings.



4. In the OPC-UA Settings, make sure that Allow Anonymous Access is checked.



Settings

Authentication

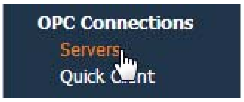
Authentication Profile: opcua-module
The name of the authentication profile to authenticate against.

Allowed Roles: ReadWrite
Separate multiple roles with a comma (ex: Administrator,user,manager)

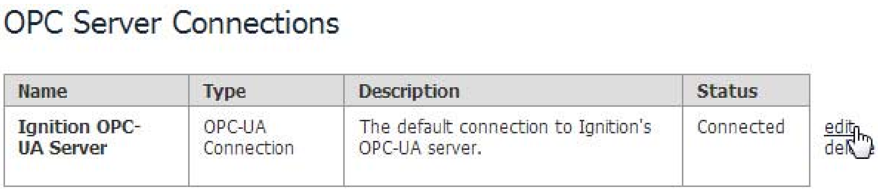
Allow Anonymous Access: ☑ Allow users to connect whether or not they possess authentication credentials.
(default: false)

Enable Allow Anonymous Access

5. Under OPC-UA Connections in the left panel, click Servers.



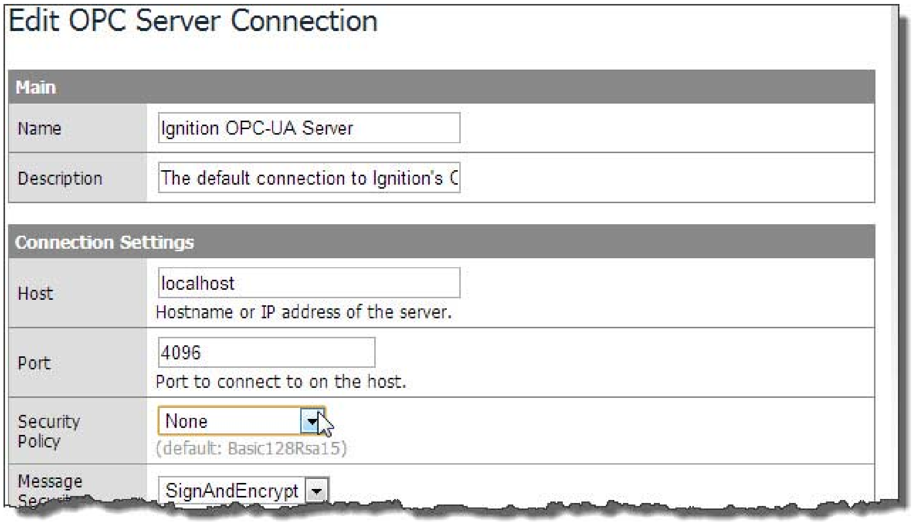
6. Next to the Ignition OPC-UA Server you are using, click "edit."



OPC Server Connections

Name	Type	Description	Status	
Ignition OPC-UA Server	OPC-UA Connection	The default connection to Ignition's OPC-UA server.	Connected	edit delete

7. Change the Security Policy to None.



Edit OPC Server Connection

Main

Name: Ignition OPC-UA Server

Description: The default connection to Ignition's C

Connection Settings

Host: localhost
Hostname or IP address of the server.

Port: 4096
Port to connect to on the host.

Security Policy: None
(default: Basic128Rsa15)

Message Security: SignAndEncrypt

8. Exit the Ignition webpage.

Configuring the Windows Firewall

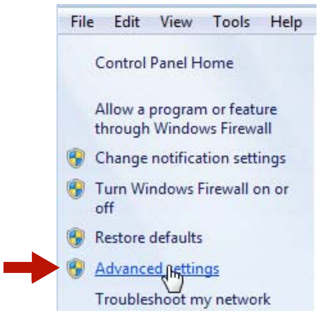
If you are using a GROOV-AT1 or running *groov* Server for Windows on a different computer, inbound traffic to the Ignition OPC-UA server needs to be able get through the firewall on the TCP/IP service port *groov* will use to access this server. This requires adding an Inbound Rule to the Windows Firewall for the Ignition service port on the computer where Ignition is installed.

NOTE: If you are using groov Server for Windows and it is installed on the same computer as the OPC-UA server, you do not need to configure the Windows Firewall as described here.

The following instructions describe how to add in Windows 7 the Inbound Rule for port 4096, Ignition's default.

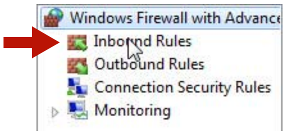
1. After you have successfully installed the Ignition OPC-UA server, open the Windows Control Panel.
2. If icons are displayed in the Control Panel, click Windows Firewall. If categories are displayed in the Control Panel, click System and Security and then click Windows Firewall.

3. In the left panel, click Advanced settings.

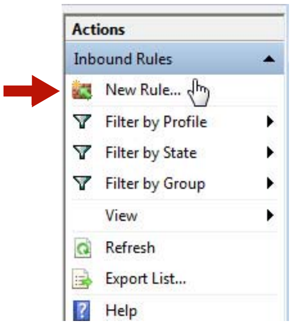

File
Edit
View
Tools
Help
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

The Windows Firewall with Advanced Security dialog box opens.

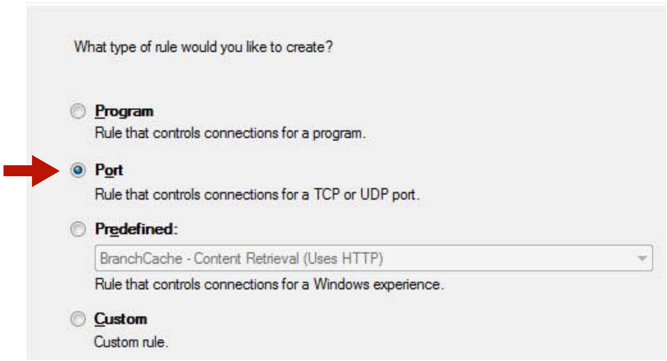
4. In the left panel, click Inbound Rules.



5. In the right panel, click New Rule.



6. For Rule Type, select Port. Click Next.



What type of rule would you like to create?

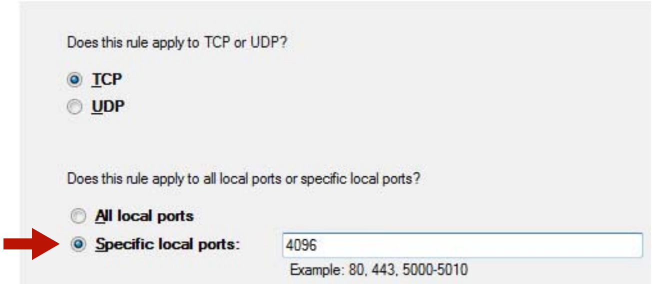
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

7. For Protocol and Ports, select TCP. Then select Specific local ports and enter 4096 (the default Ignition port). Click Next.



Does this rule apply to TCP or UDP?

● TCP

○ UDP

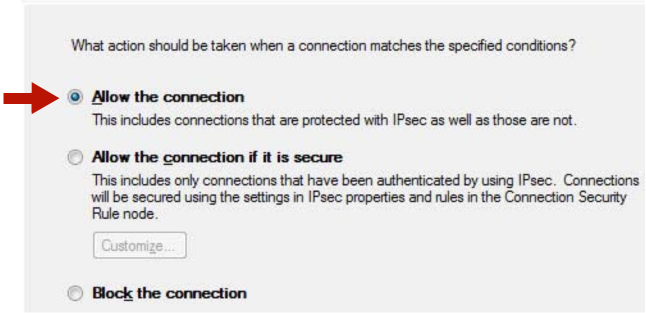
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 4096

Example: 80, 443, 5000-5010

8. For Action, select "Allow the connection." Click Next.



What action should be taken when a connection matches the specified conditions?

● Allow the connection

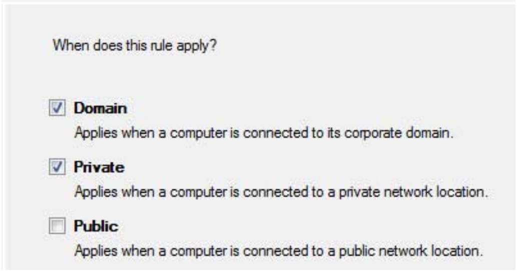
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

9. For Profile, select Domain and Private. Click Next.



When does this rule apply?

☑ Domain

Applies when a computer is connected to its corporate domain.

☑ Private

Applies when a computer is connected to a private network location.

□ Public

Applies when a computer is connected to a public network location.

10. For Name, enter a descriptive name such as "Ignition OPC-UA Server."
11. Click Finish.
12. Exit the Windows Firewall and Control Panel dialog boxes.