RECOMMENDED KEPServerEX SETTINGS FOR *groov*

Use this technical note to make sure that you are using Opto 22's recommended settings in the KEPServerEX® communication platform for successful communication with *groov*.

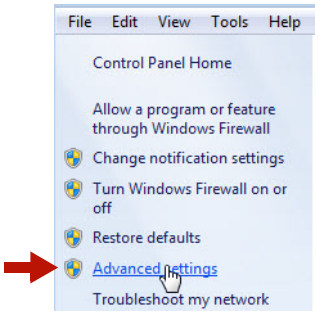
In this technical note:

CONFIGURING THE WINDOWS FIREWALL

If your OPC UA server is not on the same computer as *groov*, inbound traffic to the OPC UA server needs to be able get through the firewall on the port used by the server. To allow access through the firewall requires adding an Inbound Rule to the Windows Firewall on the computer where the OPC UA server is installed.

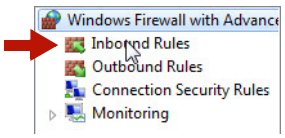
As an example, the following instructions describe how to add in Windows 7 the Inbound Rule for port 49320, the default port for the KEPServerEX 5 server.

1. After you have successfully installed the 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.

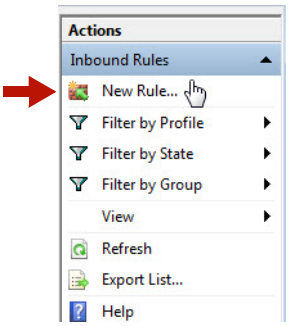


The Windows Firewall with Advanced Security dialog box opens.

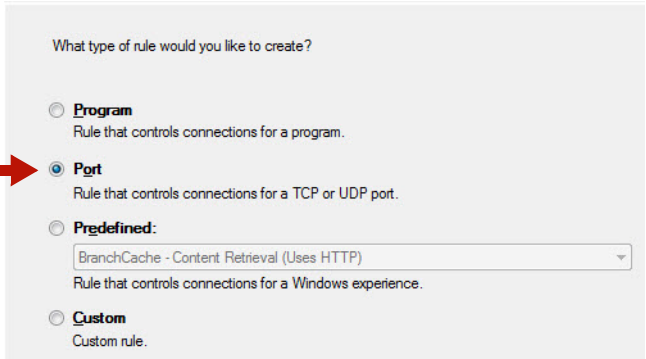
4. In the left panel, click Inbound Rules.



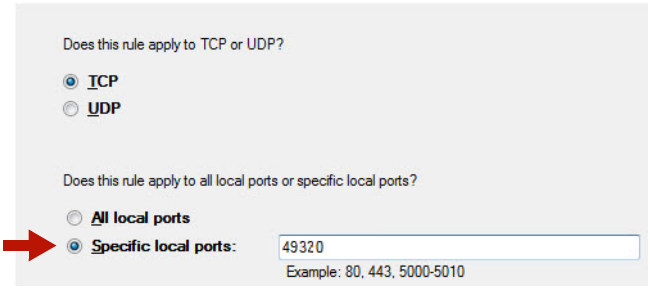
5. In the right panel, click New Rule.



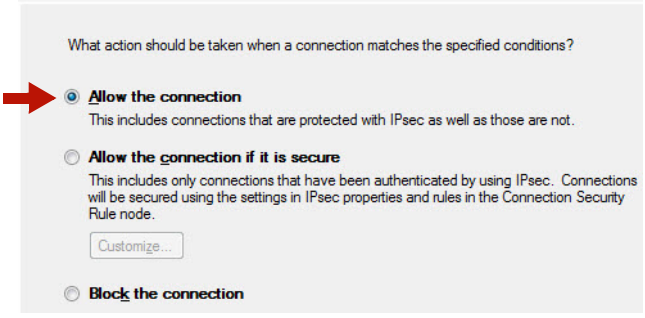
6. For Rule Type, select Port. Click Next.



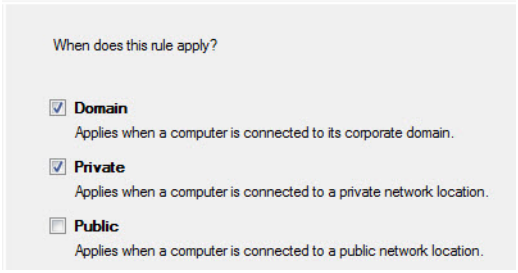
7. For Protocol and Ports, select Specific local ports and enter 49320 (the default Kepware port). Click Next.



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



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



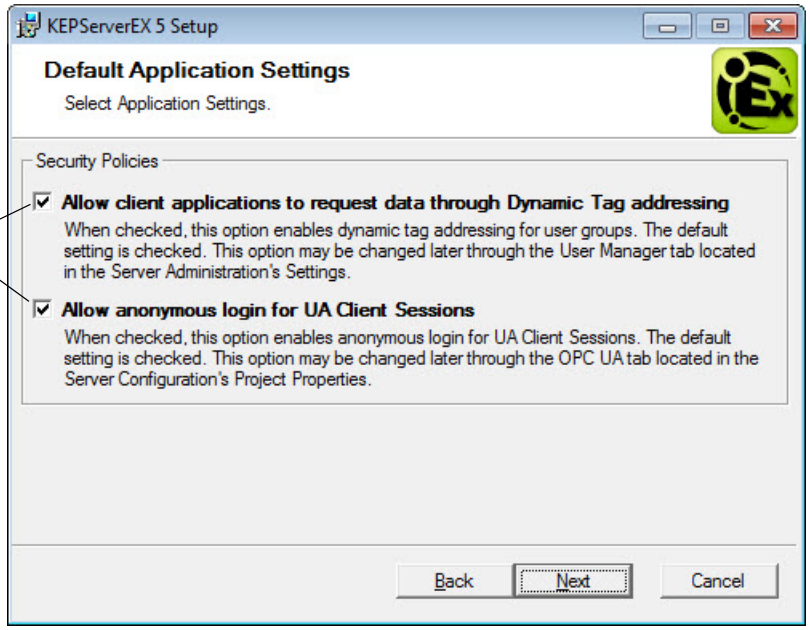
10. For Name, enter a descriptive name such as "Kepware OPC-UA Server."
11. Click Finish.
12. Exit the Windows Firewall and Control Panel dialog boxes.

DEFAULT APPLICATION SETTINGS

When you install KEPServerEX, make sure to select the following settings on the Default Application Settings page:

- **Allow client applications to request data through Dynamic Tag addressing**: This option must be selected so that *groov's* Dynamic Tag feature will work.
- **Allow anonymous login for UA Client Sessions**: This option must be selected in order for *groov* to work at all.

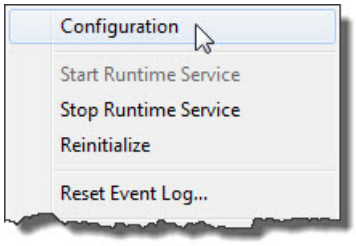
Check these items



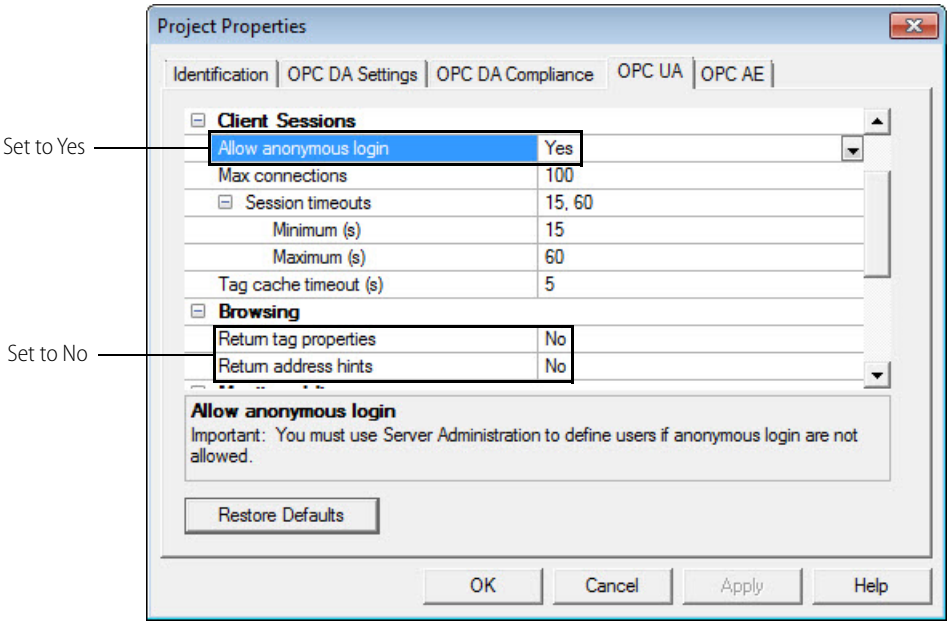
RUNTIME CONFIGURATION SETTINGS

Once KEPServerEX has been installed, follow these steps to make sure the Runtime configuration options that affect *groov's* functionality are set correctly.

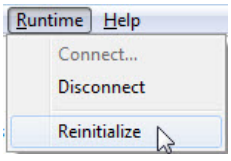
1. Click Start > KEPServerEX 5 Configuration, or right-click the KEPServerEX icon in the system tray and choose Configuration.



2. Select File > Project Properties, and then click the OPC UA tab.
   - **Allow anonymous login:** Set to Yes.
   - **Return tag properties:** Set to No. Setting this item to Yes can greatly increase the number of tags imported by *groov*.
   - **Return address hints**: Set to No.



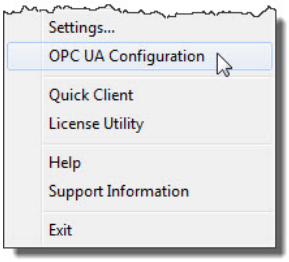
3. Click OK.
4. Select Runtime > Reinitialize.



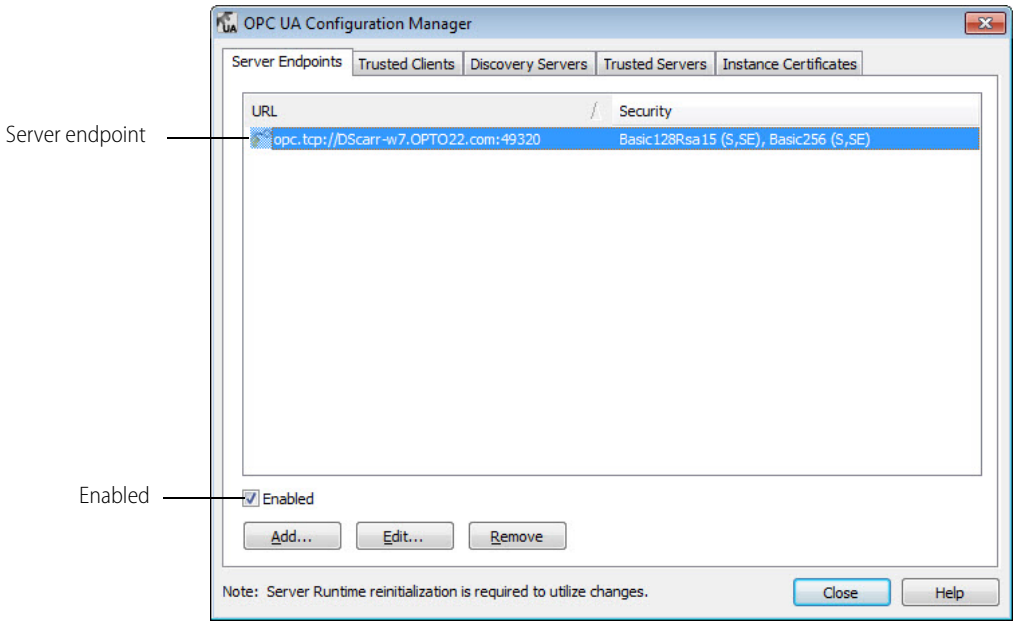
SERVER ENDPOINT SETTINGS

You must configure at least one server endpoint that can be reached by *groov,* but you might have more depending upon your PC and its network interfaces. You'll want at least one endpoint for the PC's hostname (e.g. opc.tcp://yourhostname.OPTO22.COM:49320). The default Kepware port is 49320.

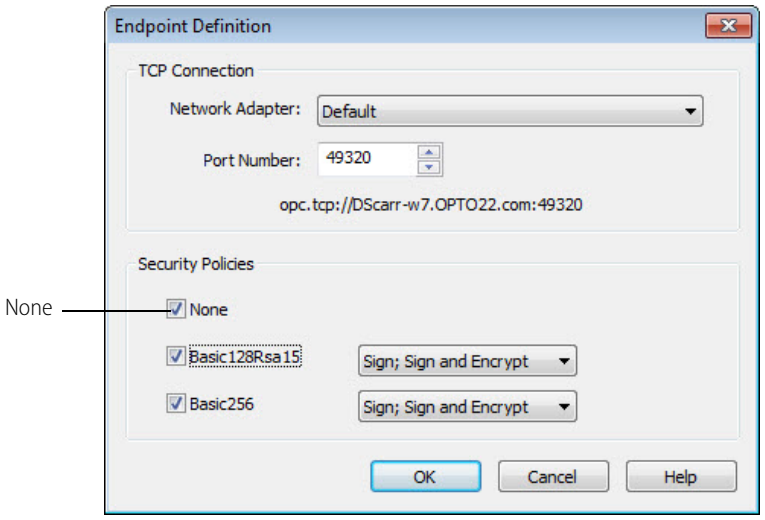
1. Right-click the KEPServerEX icon in the system tray and choose OPC UA Configuration.



2. Click the Server Endpoints tab.



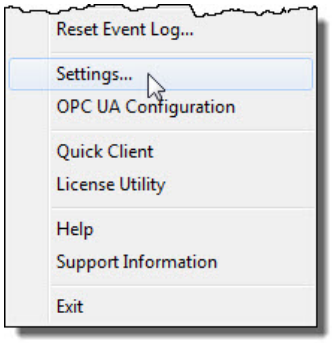
3. Make sure there is a server endpoint and that it is enabled.
4. Highlight the endpoint and click Edit. If you need to add a server endpoint, click Add instead.
5. On the Endpoint Definition dialog box, under Security Policies, make sure None is selected, then click OK.



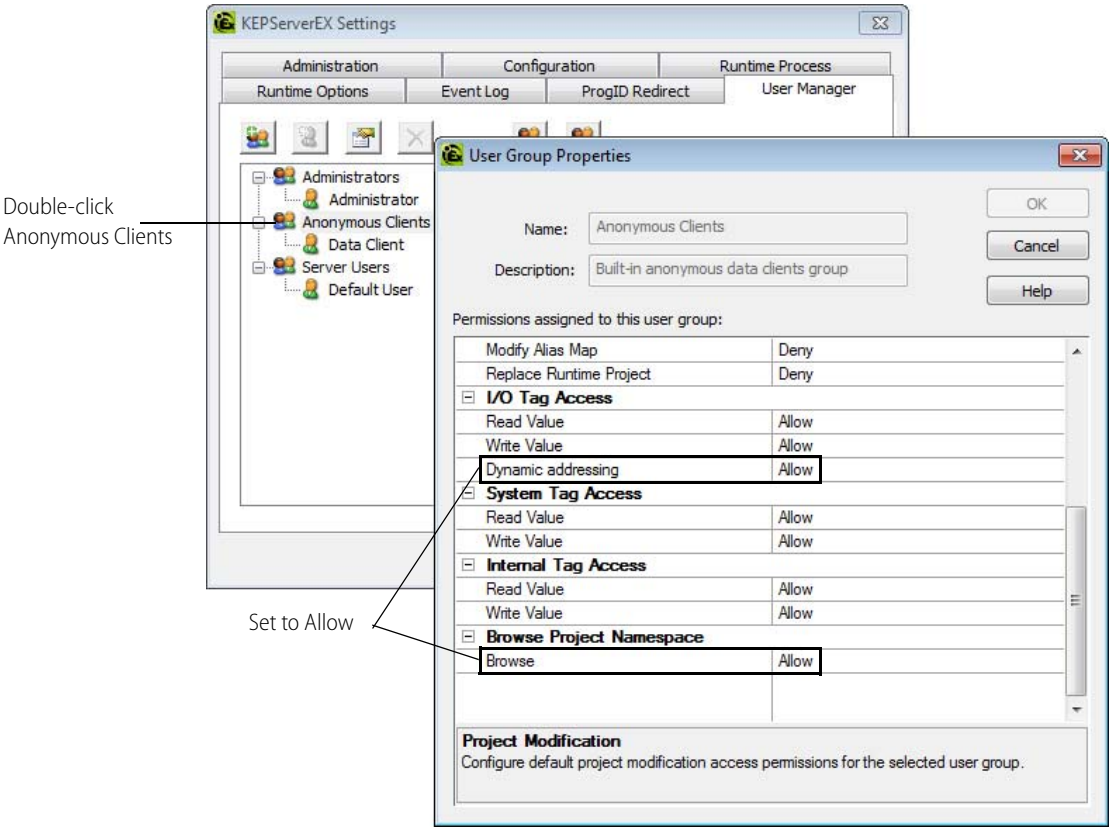
6. Click Close.

ANONYMOUS CLIENTS PROPERTIES

1. Right-click the KEPServerEX icon in the system tray and choose Settings.



2. Click the User Manager tab.
3. Double-click Anonymous Clients to open the User Group Properties dialog.



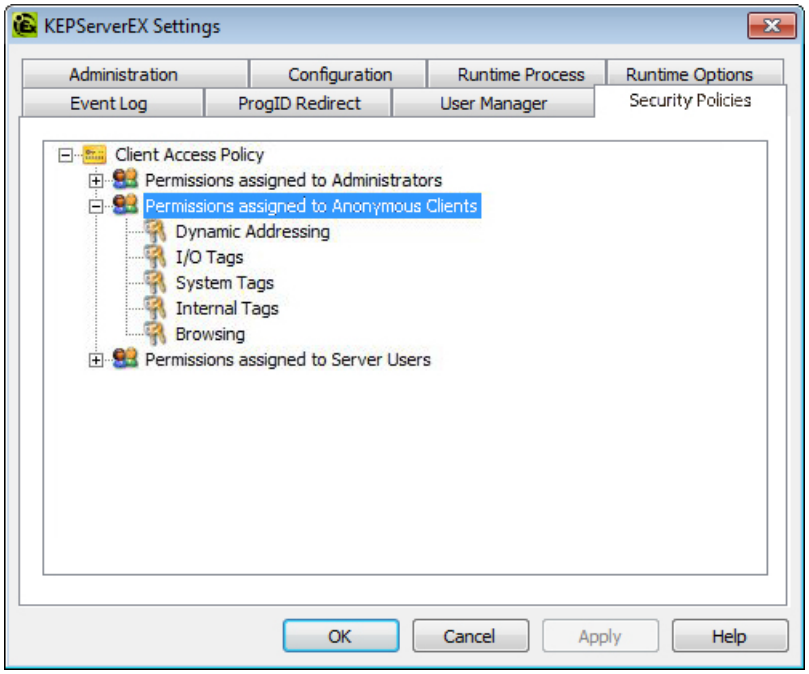
4. Under I/O Tag Access, make sure **Dynamic addressing** is set to Allow.

   If set to Deny, then *groov* cannot use dynamic tags.

5. Under Browse Project Namespace, make sure that **Browse** is set to Allow.

   If set to Deny, then *groov* cannot import any tags. The tags will be imported, but it will look to *groov* like the server is empty.

6. Click the Security Policies tab.



There are many options under Permissions assigned to Anonymous Clients which might affect *groov*. These options provide very precise control, down to individual tags. Review this section if you are having difficulty importing tags or using either imported or dynamic tags.