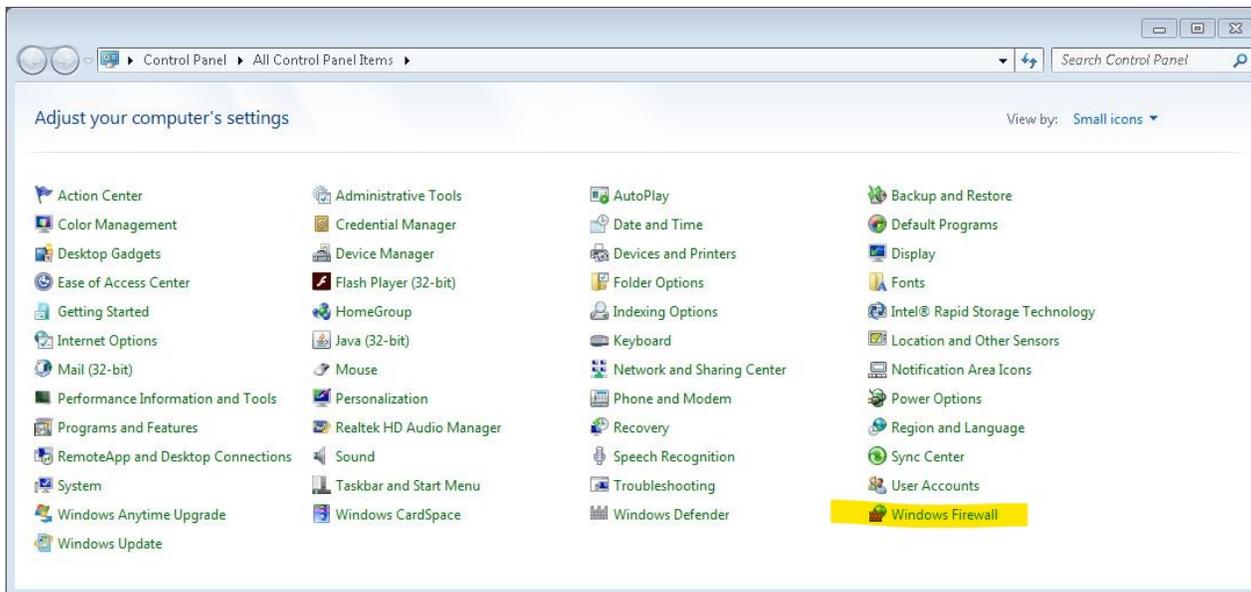


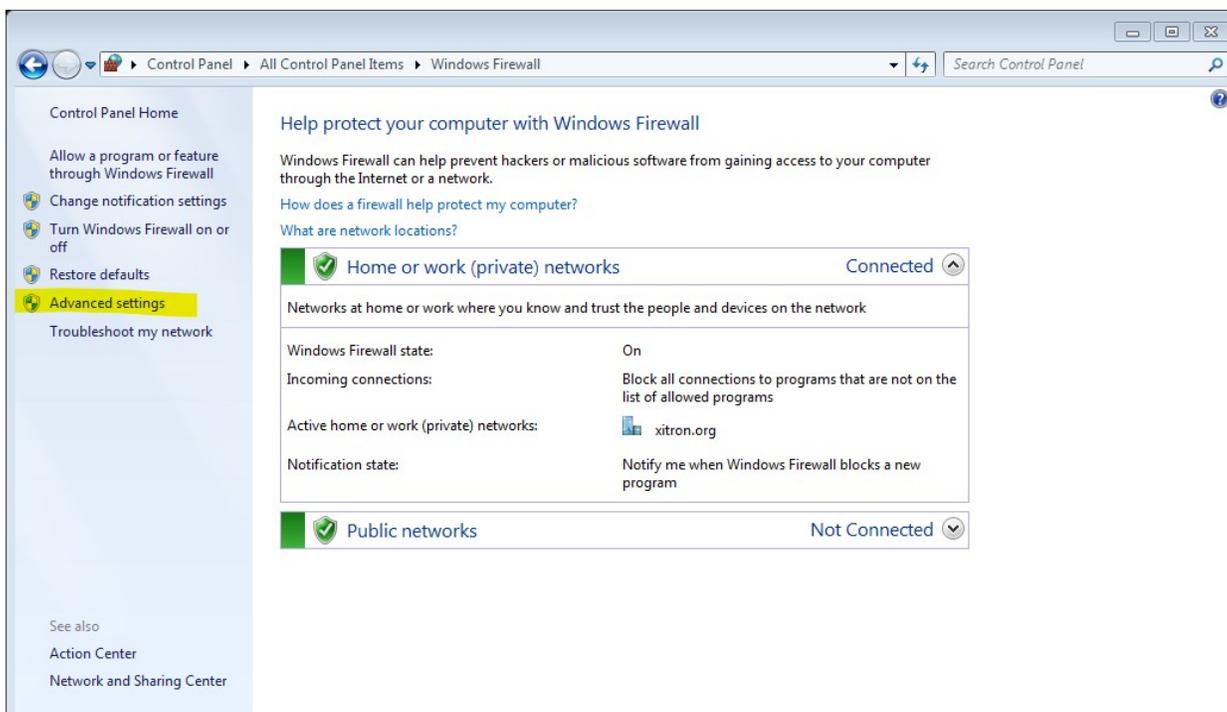
Allowing Computer IP number through Windows Firewall

Windows inherent Firewall filters incoming network traffic to help block unwanted network connections. Optionally, the Windows Firewall can also filter outgoing traffic to help limit the risk of malware. Although Windows Firewall default settings work well with components built into the operating system, they might prevent other applications from functioning correctly. Xitron has included this technote as a way for troubleshooting Client connection issues for both our Navigator GPS/Elite and Sierra workflow products. We are using Windows 10 Pro for our directions. Older operating systems or server editions may differ.

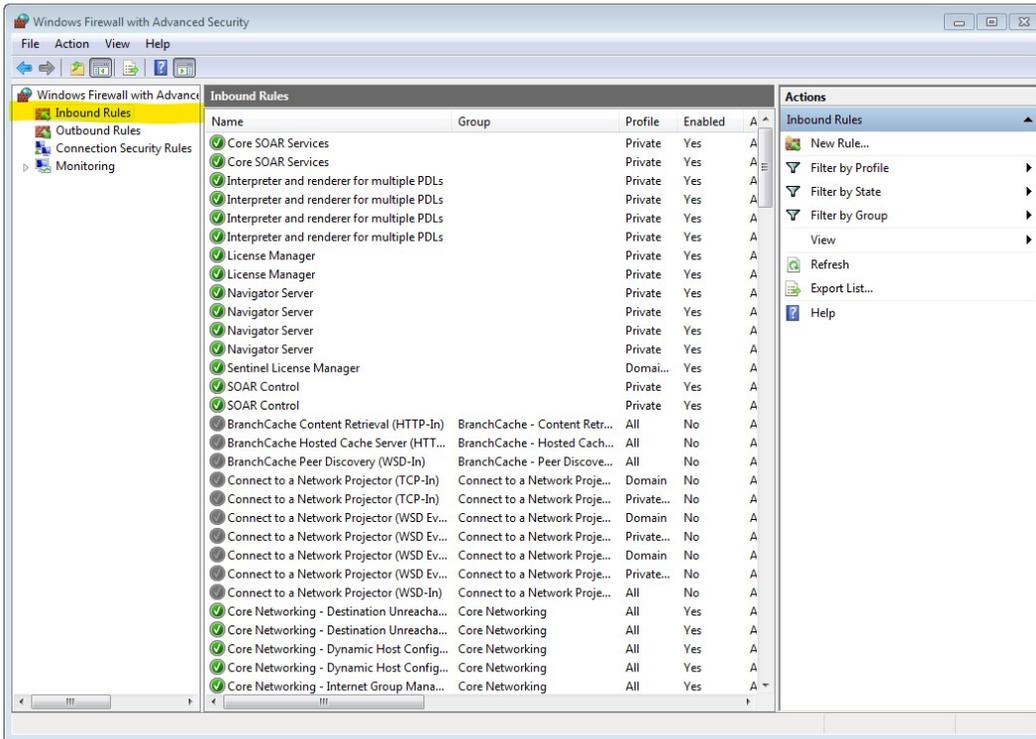
Step 1: Open Windows Control Panel -Double-click Windows Firewall



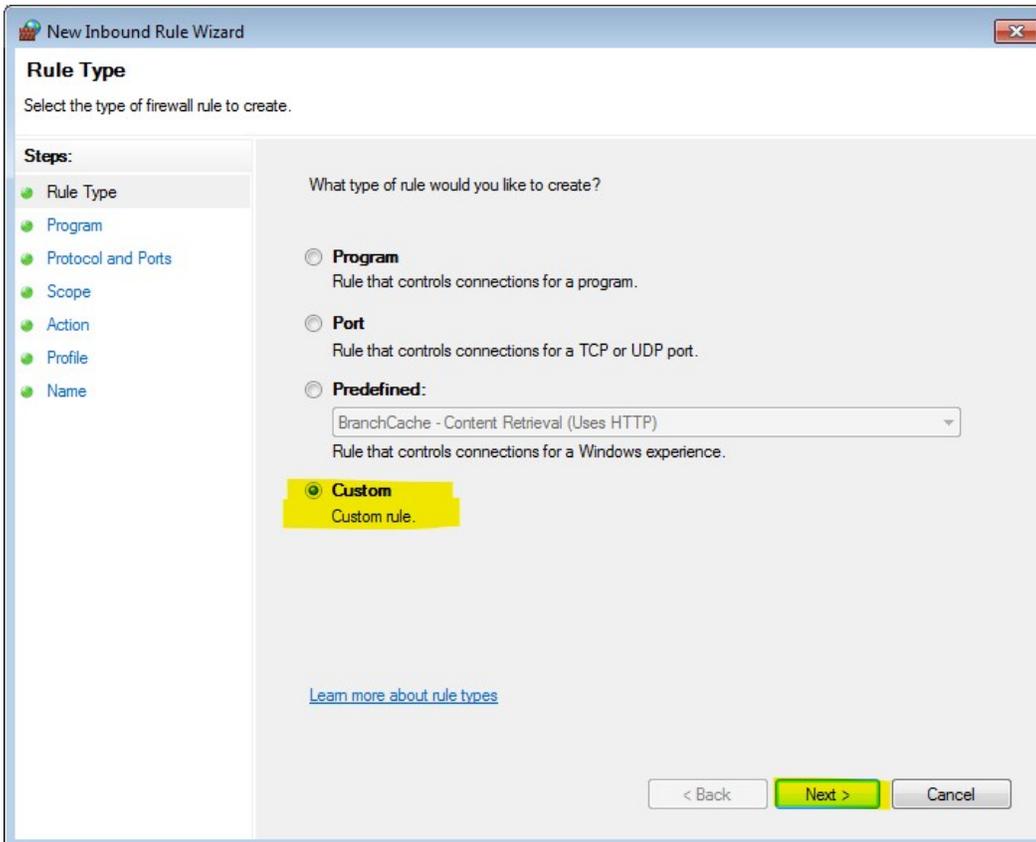
Step 2: Double-click Advanced Settings



Step 3: Select Inbound Rules, then click New Rule.



Step 4: Select Custom Rule, click on Next.



Step 5: Select Scope

New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

Any IP address

These IP addresses:

Add...
Edit...
Remove

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

Any IP address

These IP addresses:

Add...
Edit...
Remove

< Back Next > Cancel

Step 6: Select These IP Addresses and Add

New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

Any IP address

These IP addresses:

Add...
Edit...
Remove

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

Any IP address

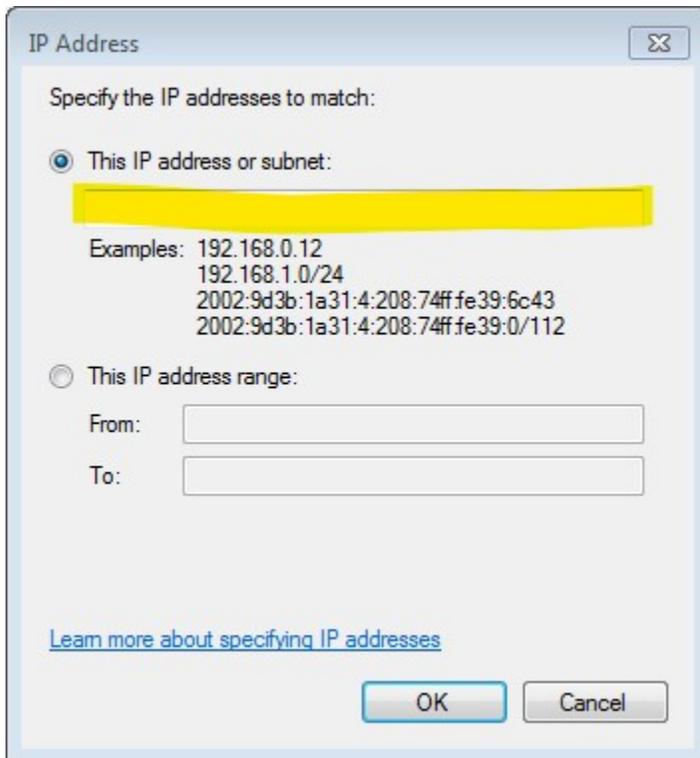
These IP addresses:

Add...
Edit...
Remove

[Learn more about specifying scope](#)

< Back Next > Cancel

Step 7: Add the IP number or IP range you wish to allow through the Windows Firewall



The image shows a Windows Firewall configuration dialog box titled "IP Address". The dialog has a close button in the top right corner. The main instruction is "Specify the IP addresses to match:". There are two radio button options: "This IP address or subnet:" (which is selected) and "This IP address range:". Under the selected option, there is a yellow highlighted text input field. Below this field, there are examples of IP addresses and subnets: "192.168.0.12", "192.168.1.0/24", "2002:9d3b:1a31:4:208:74ff:fe39:6c43", and "2002:9d3b:1a31:4:208:74ff:fe39:0/112". Under the "This IP address range:" option, there are two text input fields labeled "From:" and "To:". At the bottom of the dialog, there is a blue hyperlink that says "Learn more about specifying IP addresses". At the very bottom, there are "OK" and "Cancel" buttons.

Step 8: Make sure that the remote computer whose IP you allowed through the Windows Firewall's set to Static IP and not Dynamic IP. A Dynamic IP number changes at some point, which then revokes your privileges through the firewall.