

Technical Note

# ETHERNET CONFIGURATION FOR OPHIR- SPIRICON GIGEVISION PRODUCTS

3050 NORTH 300 WEST  
NORTH LOGAN, UT 84341  
PHONE (435) 753-3729

E-MAIL: [SERVICE.OPHIR.USA@MKSINST.COM](mailto:SERVICE.OPHIR.USA@MKSINST.COM)  
[WWW.OPHIROPT.COM/PHOTONICS](http://WWW.OPHIROPT.COM/PHOTONICS)

In the default configuration of most GigE Vision systems the camera device is connected directly to a single PC, and the network adapter and camera negotiate an IP address automatically (known as Link Local Addressing). In many Gigabit Ethernet network configurations this is sufficient to provide full functionality of the GigE Vision camera. However, depending on the network configuration and policies present, additional configuration may be required. This document provides an in-depth review of the most common configuration issues and steps to resolve them.

In many organizations, configuration of GigE Vision devices will require the assistance of IT administrators/network engineers. Care must be taken when implementing the network configuration below to prevent the introduction of security risks into the network environment.

### I. Product Matrix

Configuration of network interfaces can be unfamiliar or complicated for novice users. The software tools required to optimally configure a GigE Vision camera also vary by the device manufacturer. This matrix will direct you to sections of this guide useful for configuring each Ophir-Spiricon GigE Vision product.

Product	GigE Vision Camera Model	Sections
BeamGage Beam Profiler Cameras	Pyrocam IV or Pyrocam III-HR	<a href="#">IV</a> , <a href="#">V</a> , <a href="#">VI.a</a> , <a href="#">VII.a</a>
	SP1201 or SP1203	<a href="#">IV</a> , <a href="#">V</a> , <a href="#">VI.a</a> , <a href="#">VII.a</a>
	SP504S	<a href="#">IV</a> , <a href="#">V</a> , <a href="#">VI.b</a> , <a href="#">VII.a</a>
BeamWatch Non-Contact Laser Profilers	BeamWatch Dual Axis (acA2000-50gmNIR)	<a href="#">IV</a> , <a href="#">V</a> , <a href="#">VI.a</a> , <a href="#">VII.a</a>
	BeamWatch Integrated	<a href="#">IV</a> , <a href="#">V</a> , <a href="#">VI.d</a> , <a href="#">VII</a>

### II. Hardware Selection for GigE Vision Devices

The network adapter selected for use with GigE Vision cameras has a significant impact to the effective throughput of the camera. Selecting an incompatible or less compatible gigabit Ethernet network adapter, such as many that are embedded into laptops, is not adequate for running every camera at its full format and frame rate. If an optimal network adapter cannot be supplied to the system, it may be necessary to reduce the frame format or frame rate of the beam analysis system to ensure reliable frame transmission.

Only Gigabit PCI Express network adapter cards should be used with GigE Vision cameras. Older PCI adapters are not supported.

- Intel Pro 1000 series adapters are recommended by most GigE Vision camera manufacturers and have been found to work reliably in more configurations than other adapters. Changing the installed driver may be required for optimal performance.
- Intel Gigabit CT series adapters use the same chipset as one of the Pro 1000 series adapters but may not work well with all drivers.
- Realtek brand adapters have found to often be less reliable for GigE Vision use. These are often provided as laptop Gigabit ethernet adapters.
- At the time of writing, no Marvell-Yukon brand adapters are known to be reliable for GigE Vision use.

- Use of a USB 3.0 to Gigabit adapter may be possible depending on the data throughput required in the beam analysis application. If a suitable adapter cannot be supplied on the laptop an alternate desktop computer is recommended.
- StarTech brand USB 3.0 to GigE adapters are reliable for use with Pyrocam cameras and lower throughput applications of other GigEVision cameras.

### III. Driver Selection for GigEVision Devices

The driver for a network adapter is a potential source of instability of GigEVision cameras.

The latest version of a driver is most often the best version, since it has the latest bug fixes from the manufacturer. The driver that is distributed with the operating system is often not the most recent and a later version can be obtained from the manufacturer. We recommend using the latest version of the driver provided by the manufacturer.

### IV. Network Adapter IP Configuration

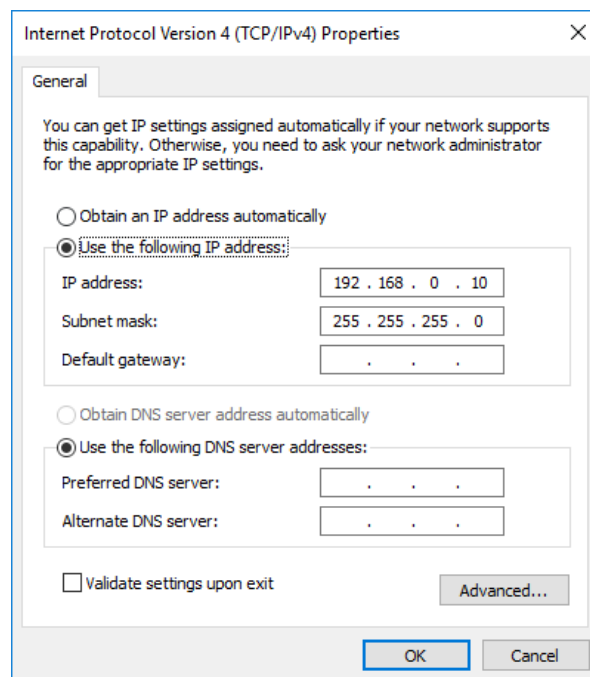
The two most common ways to configure the IP addresses of network adapters are:

- Assigning a static IP address (also "fixed" or "persistent")
- Configuring automatic addressing via DHCP (Dynamic Host Configuration Protocol) or Auto IP (Automatic Private IP Addressing, based on link-local addresses (LLA)).

#### a. Assign a Static IP Address

To assign a static IP address to a network adapter:

1. Open the **Network Connections** window in the Windows Control Panel. For quick access:
  - a. Press **⊞+R**.
  - b. Type **ncpa.cpl**.
  - c. Press **Enter**.
2. Right-click the network adapter connection that is used with the GigEVision device and then click **Properties** to open the **Properties** window.
3. Double-click **Internet Protocol Version 4 (TCP/IPv4)** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.
4. Click **Use the following IP address**.
5. In the **IP address**, **Subnet mask**, and **Default gateway** fields, type the IP address, subnet mask, and default gateway addresses.
6. In the **Preferred DNS server** and **Alternate DNS server** fields, type the primary and secondary DNS server addresses. Normally, a domain name server is not required.
7. Click **OK** to confirm your changes.



8. Repeat steps 2-7 for each applicable network adapter that will support a GigE Vision camera.

#### *Additional Static IP considerations:*

During preliminary configuration of one or more GigE Vision systems, the following settings may be used to establish a network connection very quickly:

- Configure a static address for the network adapter in the automatic IP address range.
  - IP address: 169.254.0.1 to 169.254.255.254
    - Subnet mask: 255.255.0.0
- Configure LLA or Auto IP address assignment for the GigE Vision camera.
- If the computer has multiple network adapters, each adapter must be in a different subnet.
- These address ranges have been reserved for private use according to IP standards. The recommended ranges for static IP addresses are:
  - IP address: 172.16.0.1 to 172.32.255.254
    - Subnet mask: 255.255.0.0
  - IP address: 192.168.0.1 to 192.168.255.254
    - Subnet mask: 255.255.255.0
- When assigning static IP addresses to GigE Vision systems, keep in mind that for the internal camera to communicate properly with a network adapter, it must be in the same subnet as the adapter to which it is attached. Moving systems between network adapters with static IP addresses will cause communication failures.

#### **b. Automatic assignment via DHCP or LLA**

With the default settings, a network adapter will use automatic IP addressing to assign itself an IP address.

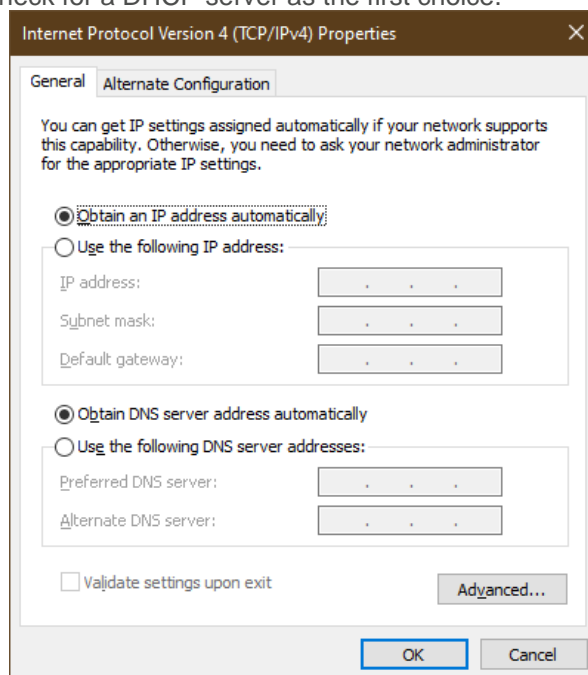
When the network adapter is configured to receive its IP address via DHCP or LLA addressing, it operates as follows:

- The network adapter tries to obtain an IP address from a DHCP server. If a DHCP server is available, it receives an IP address from the server and uses it.
- If no DHCP server is available, the adapter uses a built-in routine to assign itself a Link Local Address (LLA) IP address
  - IP address: 169.254.0.1 to 169.254.255.254
    - Subnet mask: 255.255.0.0

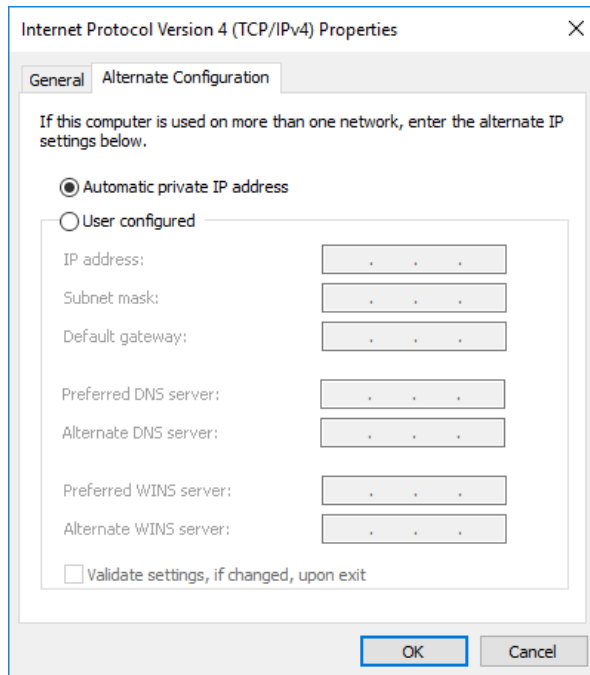
In most cases, the adapter used with a GigEVision device will not have a DHCP server available.

To assign an IP address using DHCP/LLA:

1. Open the **Network Connections** window in the Windows Control Panel. For quick access:
  - a. Press **⊞+R**.
  - b. Type **ncpa.cpl**.
  - c. Press **Enter**.
2. Right-click the network adapter connection that is used with the camera and click **Properties** to open the **Properties** window.
3. Double-click **Internet Protocol Version 4 (TCP/IPv4)** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.
4. Make sure that **Obtain an IP address automatically** is selected. This makes the adapter check for a DHCP server as the first choice.



5. Click the **Alternate Configuration** tab. The settings on this tab are applied when moving between two networks and allows a second configuration. This is unneeded in most GigEVision device applications.
6. Make sure that **Automatic private IP address** is selected.



7. Click **OK** to confirm your changes.

## V. Network Adapter Configuration

All network adapters used to connect to a GigEVision device must use a filter driver installed to the network adapter. Filter drivers are installed with the Spiricon Driver Manager.

The following filter drivers may be installed with Ophir-Spiricon products.

Filter Driver Name	GigEVision Camera Model
eBUS Universal Pro for Ethernet Driver	Pyrocam IV, Pyrocam III-HR SP1201, SP1203 BeamWatch Dual Axis, BeamWatch Integrated
Vimba GigE Transport Layer	SP504S
Pylon GigE Vision Driver	

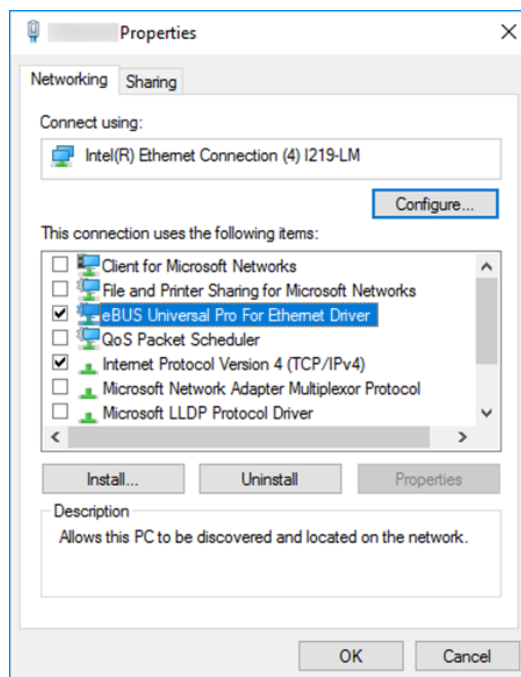
The following settings ensure optimal connection and data transfer for a Gig-E camera.

### a. Changing the Network Adapter Filter Drivers in Windows

Filter drivers are normally applied to all installed network adapters, but do not need to be active unless the adapter is used for that type of device. Generally, there is no adverse effect of having filter drivers installed and unused on an adapter. However, it is recommended to disable protocols or services that may interfere with the GigEVision device being used with each adapter.

To disable protocols or services:

1. Open the **Network Connections** window in the Windows Control Panel. For quick access:
  - a. Press **⊞+R**.
  - b. Type **ncpa.cpl**.
  - c. Press **Enter**.
2. Right-click the network adapter connection that is used with the camera and click **Properties** to open the **Properties** window.
3. Clear all check boxes except **eBUS Universal Pro for Ethernet Driver** and **Internet Protocol Version 4 (TCP/IPv4)**. See the figure below.



4. Repeat steps 2 and 3 for all applicable network adapters that will support a GigEVision camera.

## b. Changing the Network Adapter Properties in Windows

We recommend optimizing the adapter properties for GigEVision use for all network adapters used for GigEVision devices. In some hardware configurations the features, names, and values available may be different. Configure the following settings below to their most equivalent setting available on the network adapter in use. Missing features may indicate that the network adapter is not compatible for GigEVision use.

To optimize the adapter properties:

1. Open the **Network Connections** window in the Windows Control Panel. For quick access:
  - a. Press **⊞+R**.
  - b. Type **ncpa.cpl**.
  - c. Press **Enter**.
2. Right-click the network adapter connection that is used with the GigEVision device and click **Properties** to open the **Properties** window.

3. Click **Configure** to open the **Configuration** window of the network driver.
4. Click **Advanced**.
5. Adjust the following properties (see notes below):
  - a. Set the **Jumbo Frames/Packet** property to its maximum value. If there is no **Jumbo Frames** property, select the parameter that relates to frame size and set it to the maximum value.
  - b. Select the parameter that relates to the receive (Rx) ring buffer or number of receive descriptors (e.g. **Receive Descriptors or Receive Buffers**) and set it to the maximum value.
  - c. Select **Interrupt Moderation** and set value to **Enabled**.
  - d. Select the parameter that relates to the interrupt moderation rate or number of CPU interrupts (e.g. **Interrupt Moderation Rate**) and set it to Extreme value (ITR=3600). The way to set the number of CPU interrupts may differ for the network adapter.
  - e. Select the parameter that relates to speed and duplex mode (e.g. **Speed and Duplex Mode**) and set it to automatic (e.g. **Auto Negotiation**).
6. Repeat steps 2-5 for all applicable network adapters that will support a GigEVision camera.

Depending on the network adapter model, the parameter names of the network adapter may differ from the ones used above. Also, the way to set the parameters may differ, and some parameters may not be available.

- Using jumbo frames is important for reducing the overhead and the CPU load. The bigger the frame size, the less CPU interrupts are generated, and thus, the lower the CPU load.
- The receive (Rx) ring buffer defines the number of buffers used by the NIC driver to receive and process received image data from the camera. Usually, the ring buffer is set to a small value and might need to be increased on systems receiving a high volume of network traffic.
- The interrupt moderation rate (IMR) defines the trade-off between latency and performance. The IMR controls the interrupt throttle rate (ITR), the rate at which the controller moderates interrupts. A lower ITR leads to a more responsive driver, but also leads to a higher CPU load because more interrupts are generated. Conversely, a higher ITR leads to a higher latency for processing interrupts, but a lower CPU load. For most applications, higher values for IMR (e.g. Extreme or 3600) are recommended by Ophir. If lower latency is needed, use a lower value.

## VI. IP Configuration

Most GigEVision devices should follow the GenICam standard and so any tool that follows the standard can be used to configure any GenICam compliant device. There can be nuances when mixing the tools and devices from different manufacturers. These instructions provide the optimal or intended tool for each type of device.



*Note: These changes will stay in place even when the camera is powered off and back on again.*



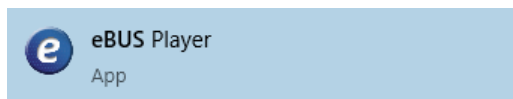
### a. Using the Pleora eBUS Player

The Pleora eBus Player is installed via the Spiricon Driver Manager utility with the camera drivers for several products. This tool is optimal for configuring the settings for the following devices:

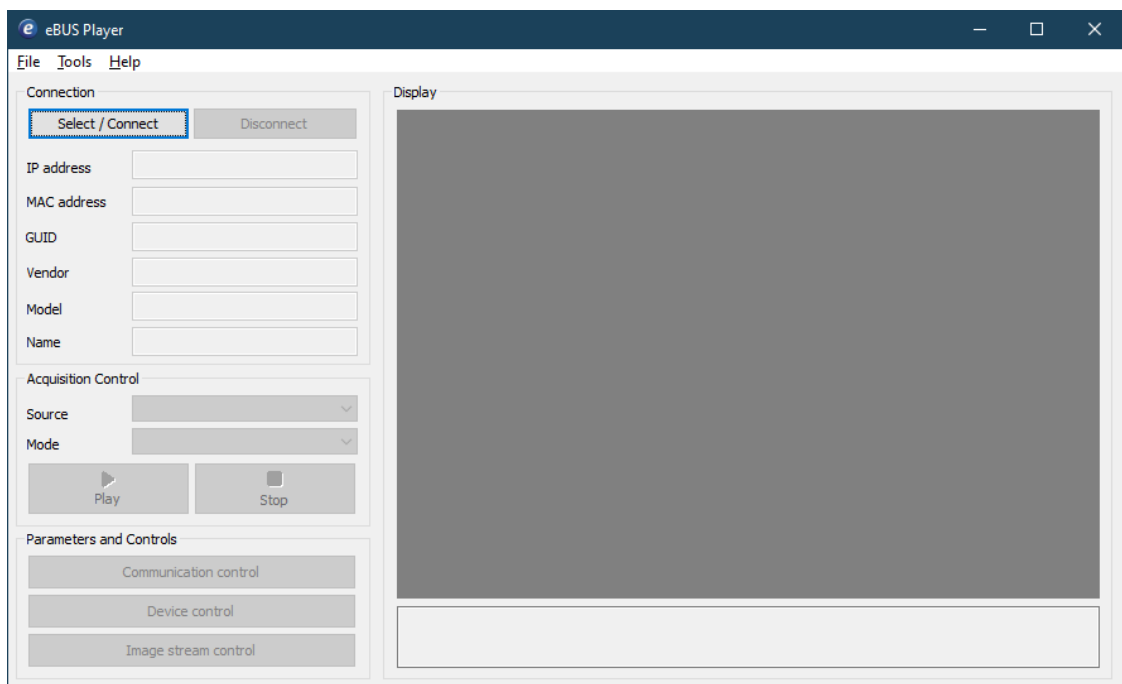
- Pyrocam IV
- Pyrocam III-HR
- SP1201
- SP1203
- BeamWatch Dual Axis

The eBUS Player application is installed with the Pleora drivers and can be opened via the Windows Start Menu:

1. Search for "**eBus Player**" or Navigate to **Pleora Technologies, Inc -> eBus Player**.

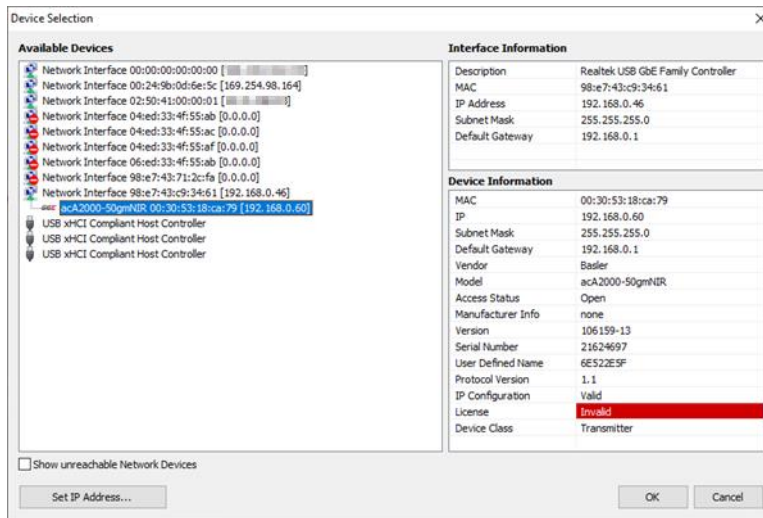


2. The **eBUS Player** opens an empty viewer with disabled controls.

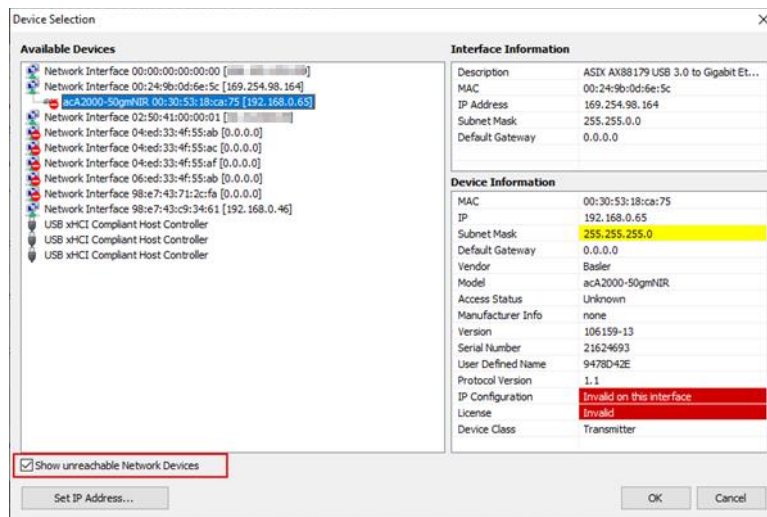


### i. Selecting the Camera

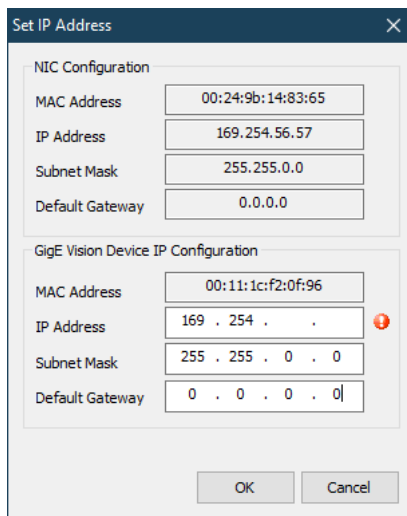
1. Press **Select/Connect**.
2. The **Device Selection** dialog displays.
3. If the camera has a valid IP configuration, it will be visible as a child of one of the available network adapters on the PC.



4. If the GigEVision camera is found, click its entry, click **OK**, and proceed to the next section of this guide.
  - Otherwise follow these steps:
    - a. Check the power and Ethernet connections.
    - b. Check the **Show unreachable Network Devices** checkbox.
    - c. After a few moments, the camera displays. The IP Configuration property on the right pane will be red and display **Invalid on this interface**.



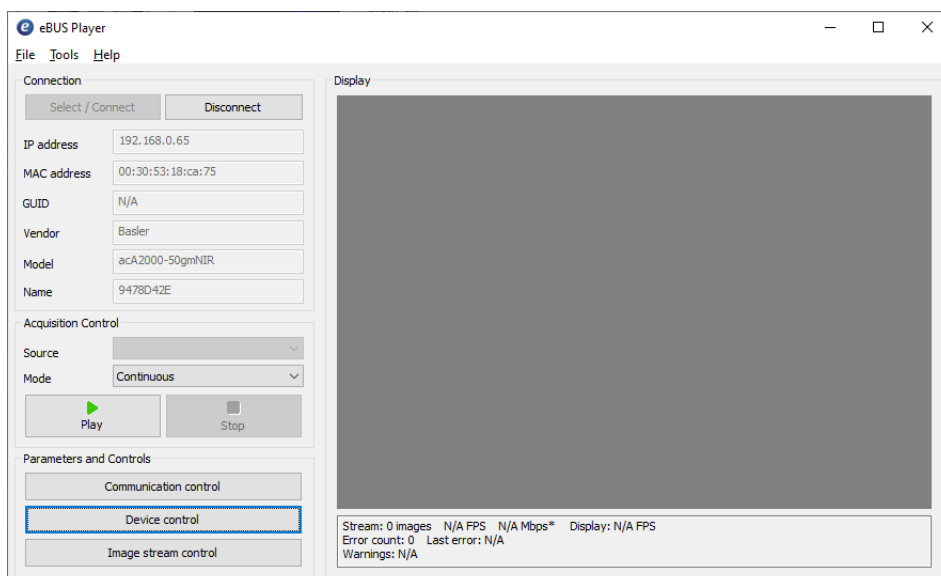
- d. Either disconnect and reconnect the camera connection to a network adapter with a compatible IP configuration, or set a new temporary IP configuration by clicking **Set IP Address....**
- e. The **Set IP Address** dialog will open, and the IP configuration of the attached network adapter will display.



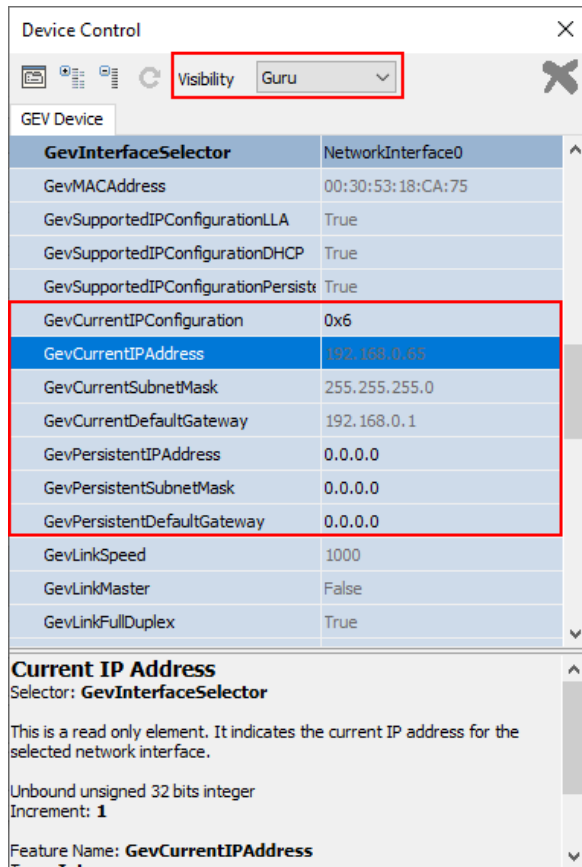
- f. Set a valid IP configuration for the camera.
  - When configuring a camera to use a temporary IP address, keep the following in mind:
    - For a camera to communicate properly, the IP address must be in the same subnet and have the same subnet mask as the adapter to which it is connected.
    - The camera must have an IP address that is unique within the network.
    - See the individual sections below for recommendations on common IP address reservations.
- g. Click OK to save the temporary IP address.
- h. On the Device Selection dialog, the IP Configuration property must read as Valid.
- i. If the GigEVision camera is found, select the entry and click OK.
- j. If no device can be found, contact the Ophir-Spiricon Service department.

## ii. Device Control Properties

Once a camera with a valid IP configuration has been selected, the eBUS Player viewer will connect to the camera.



1. To change the device IP configuration, click **Device Control**.
2. On the toolbar, change the **Visibility** to **Guru** and click **Collapse** to close the property groups.
3. Expand the **TransportLayerControl** group.
4. Scroll down to locate the **GevCurrentIPConfiguration** property. This is the first of the IP configuration properties that will be used.



### iii. IP Configuration Options

When configuring the device IP address, the following options are available:

- **Auto IP (LLA):** Auto IP (Link Local Address) means the camera uses automatic IP address assignment and assigns itself an IP address.
- **Static IP:** The IP address assigned to the camera will not change, even when the camera is powered off and on. A subnet mask and a gateway may be required. Make sure that the camera is in the same subnet as the adapter and that the camera has a unique IP address. Coordination with local IT is recommended.
- **DHCP:** A DHCP server assigns an IP address to the camera.

In the **eBUS Player Device Control properties**, these modes are configured by the **GevCurrentIPConfiguration** property per the following table. Depending on the camera type either the mode column or the value column will be displayed.

Mode	Hexadecimal Value
Auto IP or LLA Mode	0x4
Persistent Mode	0x5
DHCP Mode	0x6

#### iv. Configuring the Persistent (Static), LLA, or DHCP IP Address Modes

To change the IP configuration of the camera:

1. Set the **GevCurrentIPConfiguration**
  - a. For a Persistent or Static address, set to **0x5** or equivalent.
  - b. For an Auto IP (LLA) address, set to **0x4** or equivalent.
  - c. For a DHCP address, set to **0x6** or equivalent.



When configuring a camera to use either a temporary or a static IP address, keep the following in mind:

- For a camera to communicate properly, it must be in the same subnet as the adapter to which it is connected.
- The camera must have an IP address that is unique within the network.
- Recommended ranges of static IP addresses for local networks are:
  - 172.16.0.1 to 172.32.255.254
  - 192.168.0.1 to 192.168.255.254
- These address ranges have been reserved for private use according to IP standards.
- If the computer has multiple network adapters, each adapter must be in a different subnet.
- A network gateway is not required in some configurations. If not required, enter 0.0.0.0.

2. If configuring a Persistent IP address, set the desired values for the following fields:

**GevPersistentIPAddress**  
**GevPersistentSubnetMask**  
**GevPersistentGateway**

GevCurrentIPConfiguration	0x5
GevCurrentIPAddress	169.254.10.10
GevCurrentSubnetMask	255.255.0.0
GevCurrentDefaultGateway	0.0.0.0
GevPersistentIPAddress	192.168.100.105
GevPersistentSubnetMask	255.255.255.0
GevPersistentDefaultGateway	0.0.0.0

If configuring DHCP or LLA addresses it is recommended to clear the three persistent IP values to 0.0.0.0 for clarity, but it is not necessary to do so.

The eBUS Player will automatically save changes as they are made.

3. Close the Device Control dialog and click Disconnect.
4. To verify the IP Address change, power-cycle the GigEVision device and reconnect.

### b. Using the Allied Vision Vimba Viewer

The Vimba Viewer application is installed with the SP504S driver installation provided by the Spiricon Driver Manager. This tool is optimal for configuring the settings for the following devices:

- SP504S
- SP1201 (optional)
- SP1203 (optional)



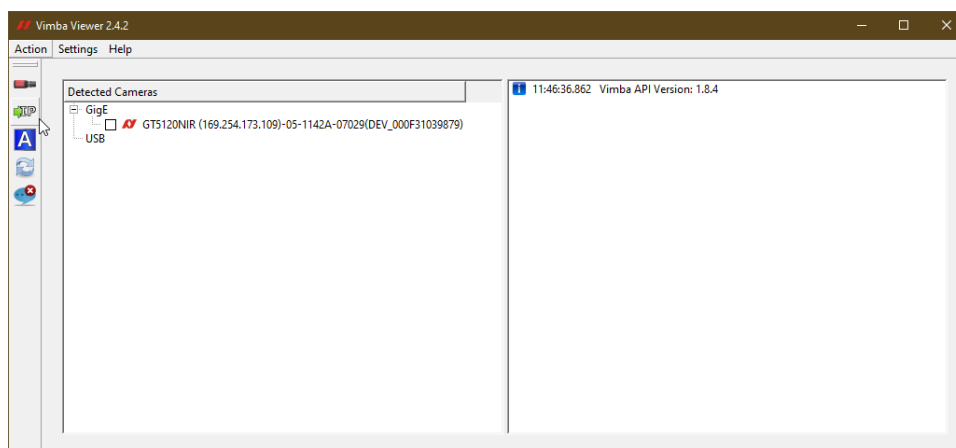
*Note: These changes will stay in place even when the camera is powered off and back on again.*

After installation the application can be opened via the Windows Start Menu:

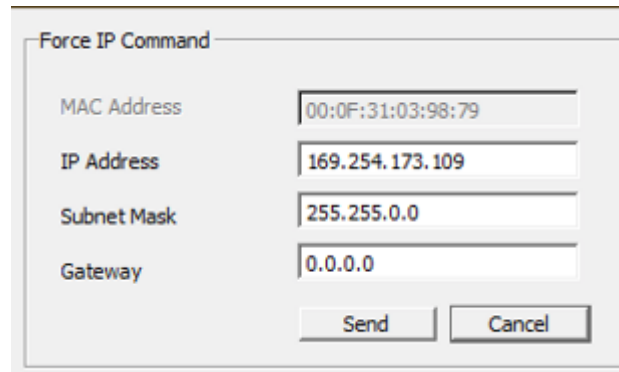
1. Search "Vimba Viewer" or Navigate to **Allied Vision Vimba -> Vimba Viewer**



2. The Vimba Viewer opens displaying each network adaptor and any detected cameras.

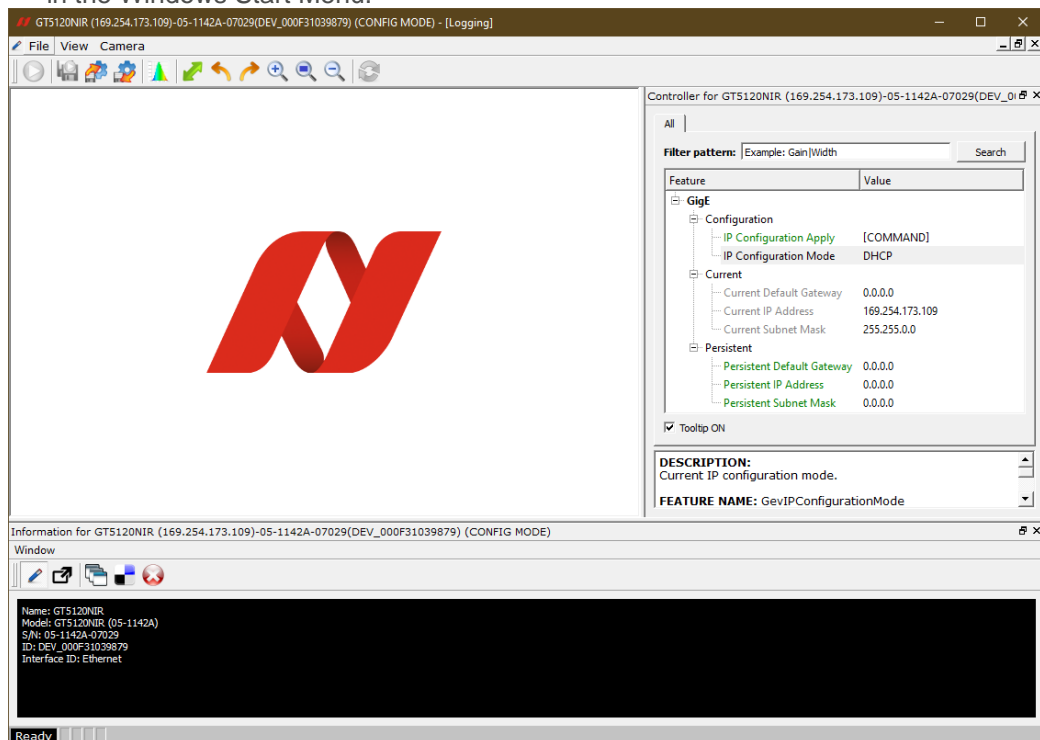


- a. If no device is found, check all connections, verify that Link and Activity LED's on the Gigabit ports are active, and in the Action Menu click Refresh.
- b. In the Action Menu the Send Force IP Command may allow an unreachable camera to be found by forcing at temporary IP address to the camera that is compatible with the configured network adapter.
  - i. In the **Send Force IP Command** dialog, select the desired network interface, select the device ID, enter a valid IP configuration and click **Send**.



A dialog box titled "Force IP Command" with four input fields and two buttons. The fields are: MAC Address (00:0F:31:03:98:79), IP Address (169.254.173.109), Subnet Mask (255.255.0.0), and Gateway (0.0.0.0). The buttons are "Send" and "Cancel".

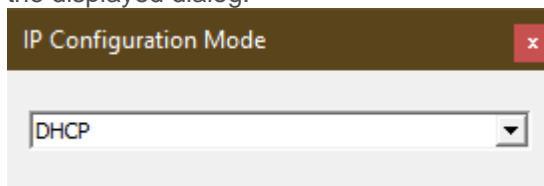
- ii. This IP address is temporary and will not persist when power cycling the camera but will allow configuration of the camera to a valid state.
- c. If the problem persists, contact the Ophir-Spiricon Service department.
- d. Clicking on a camera in the Detected Cameras list will display the camera window. Video output may be tested using the controls provided by the Vimba Viewer.
  - i. For full instructions about using Vimba Viewer, the Vimba Viewer Guide can be found in the Windows Start Menu.



- 3. In the right-hand pane the camera feature list is displayed. Under the GigE node, the IP configuration settings are found.

Feature	Value
<b>GigE</b>	
<b>Configuration</b>	
IP Configuration Apply	[COMMAND]
IP Configuration Mode	DHCP
<b>Current</b>	
Current Default Gateway	0.0.0.0
Current IP Address	169.254.173.109
Current Subnet Mask	255.255.0.0
<b>Persistent</b>	
Persistent Default Gateway	0.0.0.0
Persistent IP Address	0.0.0.0
Persistent Subnet Mask	0.0.0.0

- The IP Configuration Mode can be set by clicking on the entry and selecting the desired mode in the displayed dialog.



- Persistent IP address settings may be configured by clicking on the field.
- Once the desired settings are configured, close the Vimba Viewer software.
- To verify the IP Address change, power-cycle the GigEVision device and reconnect.

### c. Using the Basler pylon IP Configurator

Optionally, the Basler pylon IP Configurator is available for download from Basler to assign an IP address to BeamWatch Dual Axis. This software is not currently provided in the Spiricon Driver Manager but can be useful for working with this system.

<https://docs.baslerweb.com/overview-of-the-pylon-ip-configurator>

This is a direct download link of the 64-bit Pylon Software Suite (valid as of May 2022):

[https://www.baslerweb.com/fp-1589378356/media/downloads/software/pylon\\_software/Basler\\_pylon\\_6.1.1.19832.exe](https://www.baslerweb.com/fp-1589378356/media/downloads/software/pylon_software/Basler_pylon_6.1.1.19832.exe)



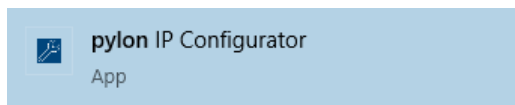
*Note: These changes will stay in place even when the camera is powered off and back on again.*

If manually installing the Pylon Software Suite, only the **Camera User** and **GigE** installation options are required.

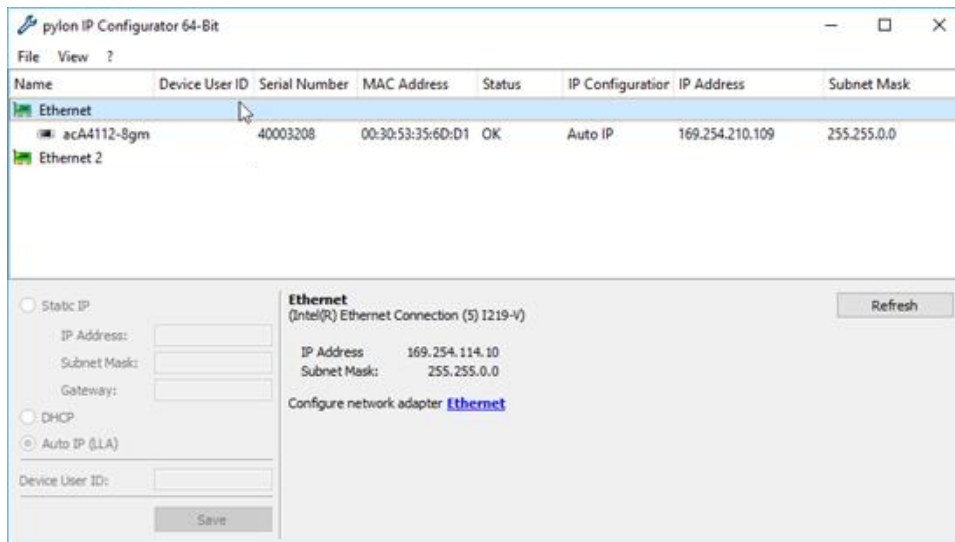
After installation the application can be opened via the Windows Start Menu:

- Search "pylon IP Configurator" or Navigate to **Basler -> pylon IP Configurator**.





2. The pylon IP Configurator opens displaying each network adaptor and any detected cameras.



### i. IP Configuration Options

When configuring the BeamWatch Integrated IP address there are the following options:

- **Auto IP (LLA):** Auto IP (Link Local Address) means that the camera uses automatic IP address assignment and assigns itself an IP address.
- **Static IP:** The IP address assigned to the camera that will stay in place even when the camera is powered off and on. A subnet mask and a gateway may be required. Make sure that the camera is in the same subnet as the adapter and that the camera has a unique IP address. Coordination with local IT is recommended.
- **DHCP:** DHCP means that a DHCP server assigns an IP address to the camera.

### ii. Assigning a Static (Persistent) IP Address

When configuring a camera to use a static IP address, there are some things to keep in mind:

- For a camera to communicate properly, it must be in the same subnet as the adapter to which it is connected.
- The camera must have an IP address that is unique within the network.
- Recommended ranges of static IP addresses for local networks are:
  - 172.16.0.1 to 172.32.255.254
  - 192.168.0.1 to 192.168.255.254
- These address ranges have been reserved for private use according to IP standards.
- If the computer has multiple network adapters, each adapter must be in a different subnet.
- A network gateway is not required in some configurations. If not required, enter 0.0.0.0.

To change the IP configuration of the camera to Static IP:

1. In the top pane of the IP Configurator, select the camera whose IP configuration will be changed.
2. In the lower left pane of the IP Configurator, select **Static IP**.

**Basler acA4112-8gm (40003208)**

Static IP  
 IP Address: 169.254.210.10  
 Subnet Mask: 255.255.0.0  
 Gateway: 0.0.0.0  
 DHCP  
 Auto IP (LLA)

Device User ID:

Save

Vendor: Basler  
 Model Name: acA4112-8gm  
 Device User ID:  
 Serial Number: 40003208  
 MAC Address: 00:30:53:35:6D:7F  
 IP Configuration: Auto IP  
 IP Address: 169.254.210.10  
 Subnet Mask: 255.255.0.0  
 Gateway: 0.0.0.0

3. In the IP Address, Subnet Mask, and Gateway fields enter the desired values.
4. Click the **Save** button.

The IP Configurator will save the changes. This takes a few seconds. When the IP Configurator has finished saving, the information in the top pane and the lower central area will have been updated automatically.

### iii. Assigning an Auto IP (LLA) IP Address

The method for assigning an IP address may be changed to Auto IP (Link Local Address). This means that the camera uses automatic IP address assignment and assigns itself an IP address.

To change the IP configuration of the camera to Auto IP (LLA):

1. In the top pane of the IP Configurator, select the camera whose IP configuration will be changed.
2. In the lower left pane of the IP Configurator, select **Auto IP (LLA)**.

**Basler acA4112-8gm (40003208)**

Static IP  
 IP Address: 169.254.210.10  
 Subnet Mask: 255.255.0.0  
 Gateway: 0.0.0.0  
 DHCP  
 Auto IP (LLA)

Device User ID:

Save

Vendor: Basler  
 Model Name: acA4112-8gm  
 Device User ID:  
 Serial Number: 40003208  
 MAC Address: 00:30:53:35:6D:7F  
 IP Configuration: Auto IP  
 IP Address: 169.254.210.10  
 Subnet Mask: 255.255.0.0  
 Gateway: 0.0.0.0

3. Click the **Save** button.

The IP Configurator will save the changes. This takes a few seconds. When the IP Configurator has finished saving, the information in the top pane and the lower central area will have been updated automatically.

#### iv. Assigning an IP Address via a DHCP Server

The method for assigning an IP address may be changed to DHCP. This means that a DHCP server assigns the IP address to the camera.

To change the IP configuration of the camera to DHCP address assignment:

1. In the top pane of the IP Configurator, select the camera whose IP configuration will be changed.
2. In the lower left pane of the IP Configurator, select **DHCP**.

3. Click the **Save** button.

The IP Configurator will save the changes. This takes a few seconds. When the IP Configurator has finished saving, the information in the top pane and the lower central area will have been updated automatically.

If the settings made in step 2 are not compatible with the IP address configuration of the port or network adapter to which the camera is connected, the **Assign Temporary IP Address (Force IP)** dialog opens. To complete this dialog, go to [Assigning a Temporary IP Address to Older Cameras](#) and follow those steps on screen. Once the procedure is complete, the settings made here will be applied.

If no DHCP server is present or if there is a problem preventing the DHCP server from assigning an IP address to the camera, automatic IP address assignment will be used as a fallback.

#### d. Using the BeamWatch Integrated Web Interface

The BeamWatch Integrated IP address can be customized to better coexist within an existing network via the web interface. Please refer to the *Communication* section in the *Settings* page of the BeamWatch Integrated User Note.

## VII. Firewall Configuration

Software firewalls provide an important barrier to security risks in modern PC's but in most cases also limit the connectivity of GigEVision and Ethernet devices. In Windows 10, the Windows Defender Firewall is enabled by default. Information required for configuration of Windows Defender Firewall for GigEVision

and Ethernet devices is provided below. If other software firewalls are used, the sections below may be used as a reference.

#### a. Disable firewall controls on the network adapter

It is not always necessary to disable the firewall. If the firewall is left enabled, the camera and profiler may be fully operational, with the following exceptions:

- On Windows, when a program opens a Gig-E camera for the first time, a Windows Security Alert will open asking to allow incoming requests, depending on current security settings.
- Gig-E camera identification and communication may be blocked.
- Image streaming may be unstable compared to unrestricted use.

Therefore, it is recommended to disable the firewall for the network connections with GigEVision devices. Alternatively, inbound rules can be configured for specific applications so that they are not blocked by the firewall.



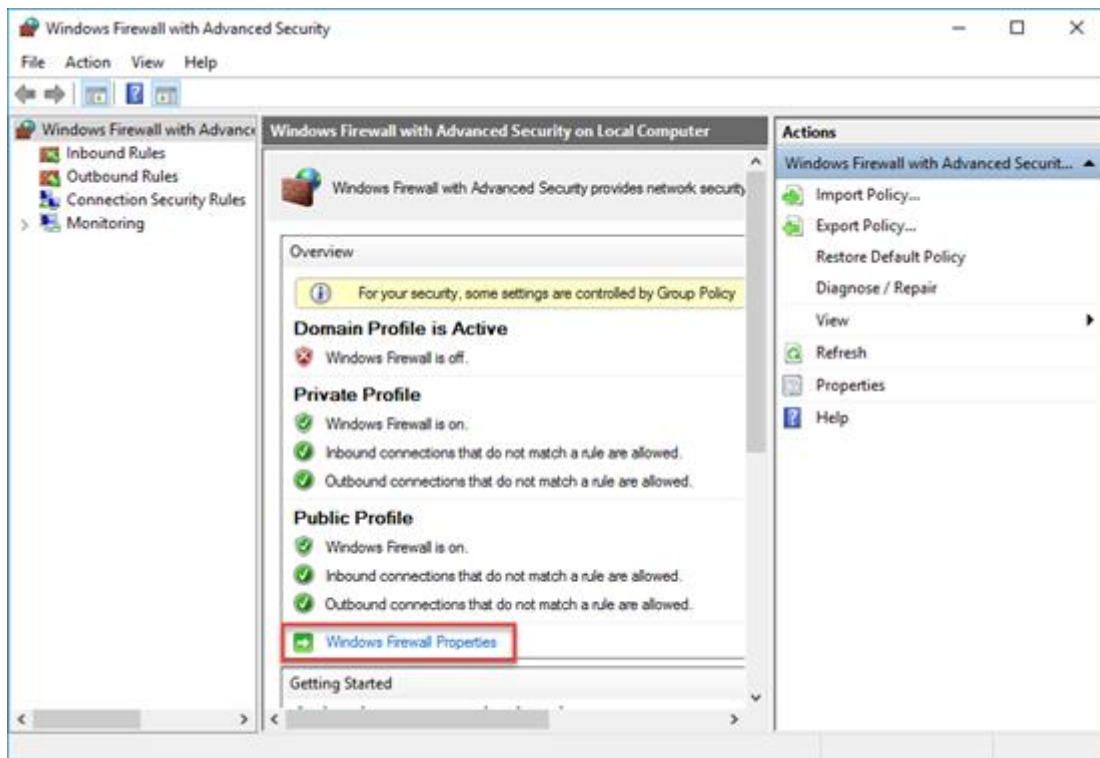
*Care must be taken with this solution to use physical and administrative controls to reserve the physical network adapter port for use only with the GigEVision device. Swapping the Ethernet cables to this network adapter port after this change introduces potential security risks. For example, connecting a LAN or internet connection to this port would not be protected by the firewall.*

#### i. Disable the Windows Defender Firewall via Advanced Security Settings

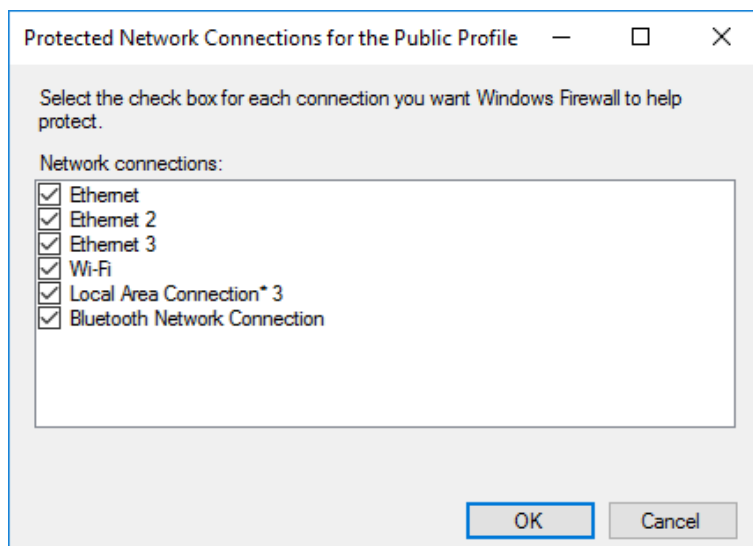
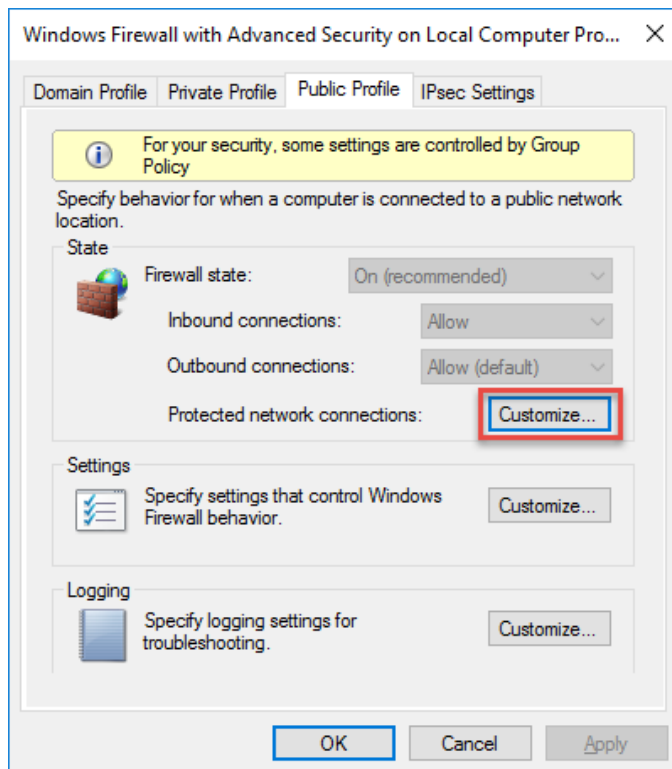
This option allows disabling the firewall for specific network adapters while other methods would disable the firewall completely. *This is the recommended solution for most users.*

To disable the firewall on selected network adapters:

1. Open the **Windows Defender Firewall with Advanced Security** window. For quick access:
  - a. Press **⊞+R**.
  - b. Type **wf.msc**.
  - c. Press **Enter**.
2. Click **Windows Defender Firewall Properties** to open the **Windows Defender Firewall with Advanced Security** properties pane.



3. Click the tab of the profile where firewall protection will be disabled.
  - a. Typically, this is the **Public Profile** tab.
  - b. If using a dedicated network adapter, it is recommended to also disable firewall protection for the other profiles on that network adapter only.
4. Click **Customize** to open the **Protected Network Connections for the Public Profile** window. The window lists connections where the firewall is enabled (see figures below).



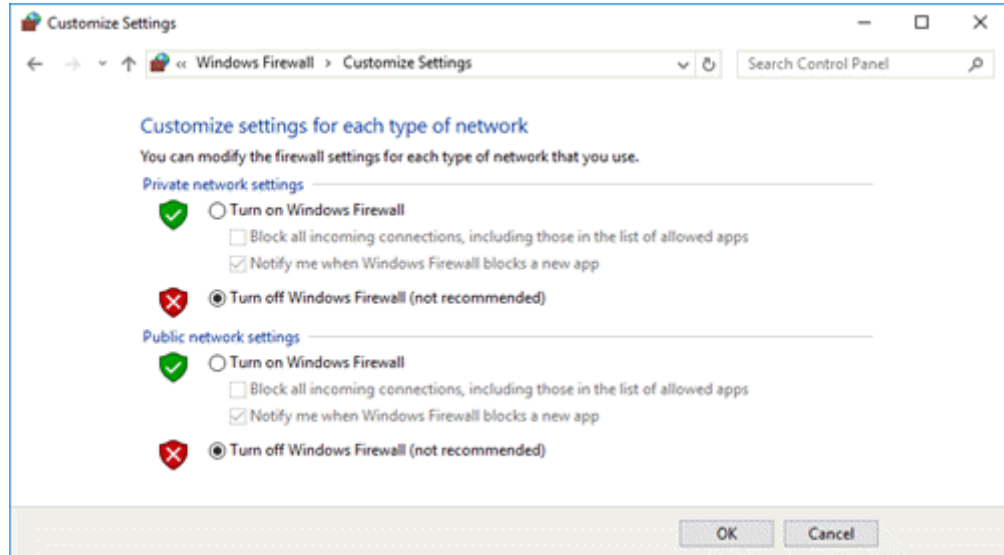
5. Unselect the connections where the BeamWatch is connected. This disables firewall protection for that network adapter.
  6. Repeat steps 3-5 for each profile where firewall protection will be disabled.
- ii. **Disable the Windows Firewall via Windows Control Panel**  
 This option disables the firewall for all connections. This method is not recommended for most users and must be performed with an administrative account.



Take care with this solution to completely disable the firewall on the PC! This solution should only be used on a PC that is isolated from any external network, otherwise the PC may become vulnerable to outside attacks.

To turn off the firewall via Windows Control Panel:

1. Open the **Windows Firewall** window in the **Windows Control Panel**. For quick access:
  - a. Press **⊞+R**.
  - b. Type **firewall.cpl**.
  - c. Press **Enter**.
2. In the left pane, click **Turn Windows Firewall on or off** to open the **Customize Settings** window.
3. Find the network location section for the network adapter where the firewall protection will be turned off.
  - a. Typically, this is the **Public network settings** section.
  - b. If using a dedicated network card, we recommend that you disable firewall protection for the other network zones.
  - c. The specific zone that the dedicated network adapter is configured for can be found in the **Windows Network and Sharing Center**.
4. In the desired sections, click **Turn off Windows Firewall**.
5. Click **OK** to save changes.



### iii. Disable the Windows Firewall via Command Prompt

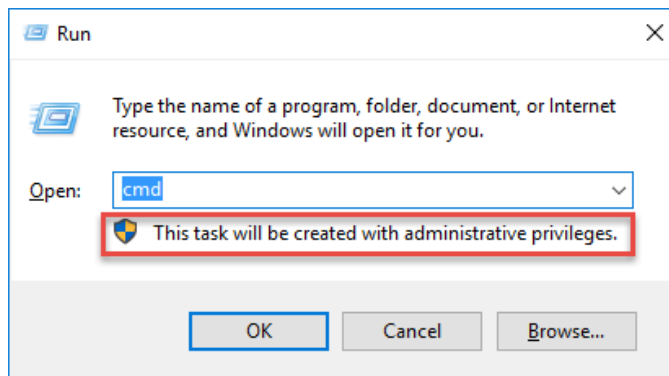
This option disables the firewall for all connections and network zones in a single command. *This is not recommended for most users and must be performed with an administrative account.*



Take care with this solution to completely disable the firewall on the PC! This solution should only be used on a PC that is isolated from any external network, otherwise the PC will be vulnerable to outside attacks.

To disable the firewall via command prompt:

1. Press **⊞+R**.
2. Type **cmd**. Ensure that the message "This task will be created with administrative privileges" is displayed.



3. Press **Enter**. The **Command Prompt** window opens.
4. Type **netsh advfirewall set allprofiles state off**
5. Press **Enter**
6. The firewall is disabled for all profiles.



*Note: It is not possible to use **netsh** to disable the firewall for select connections only.*

## b. Setting Up Inbound Firewall Rules

In some network configurations a firewall can block three areas of communication important to successful operation of the host application for GigE Vision cameras, such as BeamGage or BeamWatch.

1. Ophir-Spiricon software communicates between three of its own processes across TCP ports beginning at 10100 and up to a range of 1000 sequential ports.
  - Normally any necessary firewall rules will automatically be generated within Windows Firewall for the host application.
  - Firewall rules may be necessary for the following processes on a PC running the BeamWatch or BeamGage Software.
    - Spiricon.ConsoleService.exe
    - Spiricon.DataServer.exe
    - BeamWatch.exe for BeamWatch, or Spiricon.Version5.exe for BeamGage
  - If necessary, the port range can be customized by modifying the following file.
    - **C:\Program Files\Spiricon\
      - Both the Start and Count properties can be customized
      - A minimum port range of 20 is recommended.**
2. The Ophir EA-1 power meter communicates via TCP and UDP ports.
  - **Discovery:** UDP port 11000
  - **Communication:** TCP port 23 (Telnet mode) or TCP port 80 (HTTP mode)
  - When used with the BeamWatch, the DataServer uses the EA-1's telnet mode.

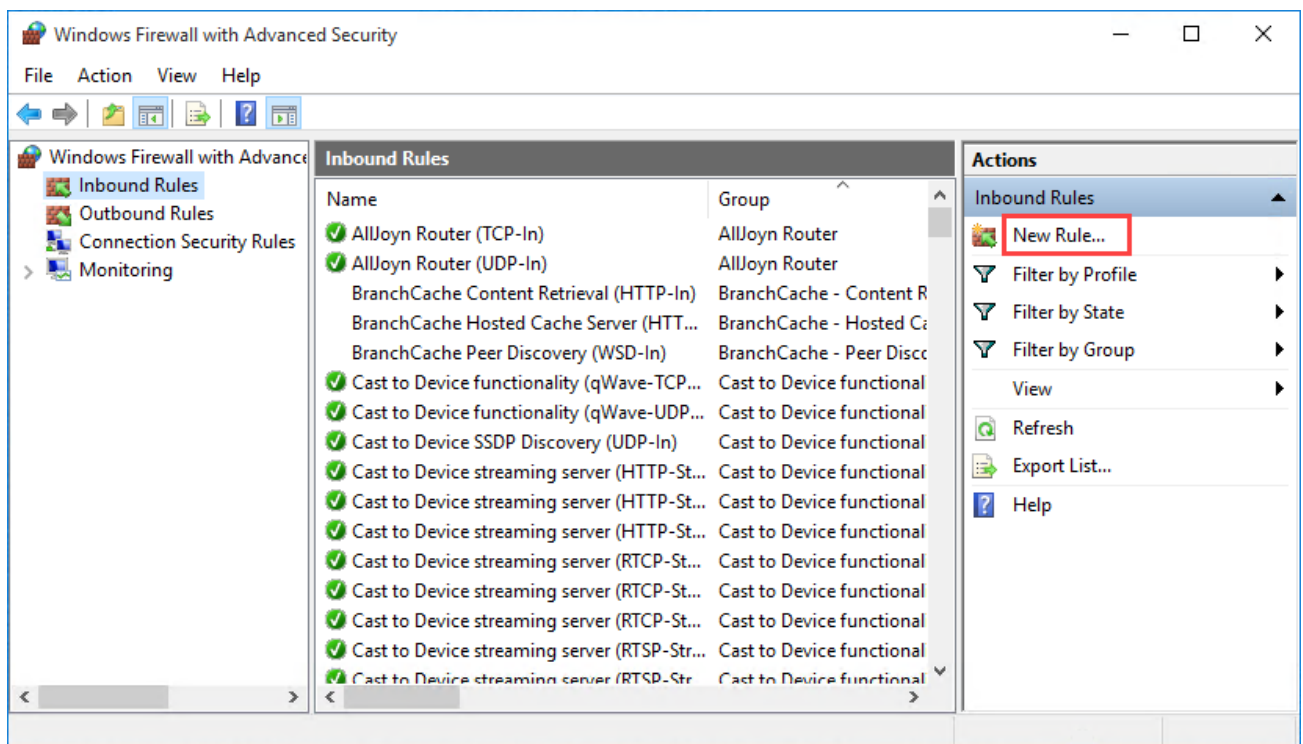


3. The **Basler Pylon Viewer** utility may be used to set the IP Configuration and verify operation of the camera in the BeamWatch.
  - o 64-bit pylon Viewer
  - o **C:\Program Files\Basler\pylon 6\Applications\x64\bin\pylonviewer.exe**

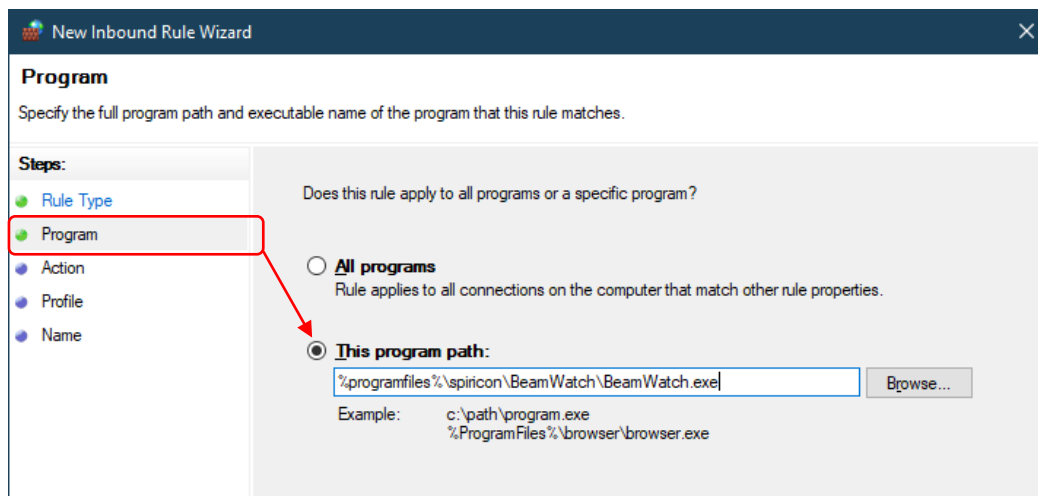
Instead of disabling the Windows Firewall completely, inbound rules can be configured for specific applications so that they won't be blocked by the firewall.

To set up inbound rules:

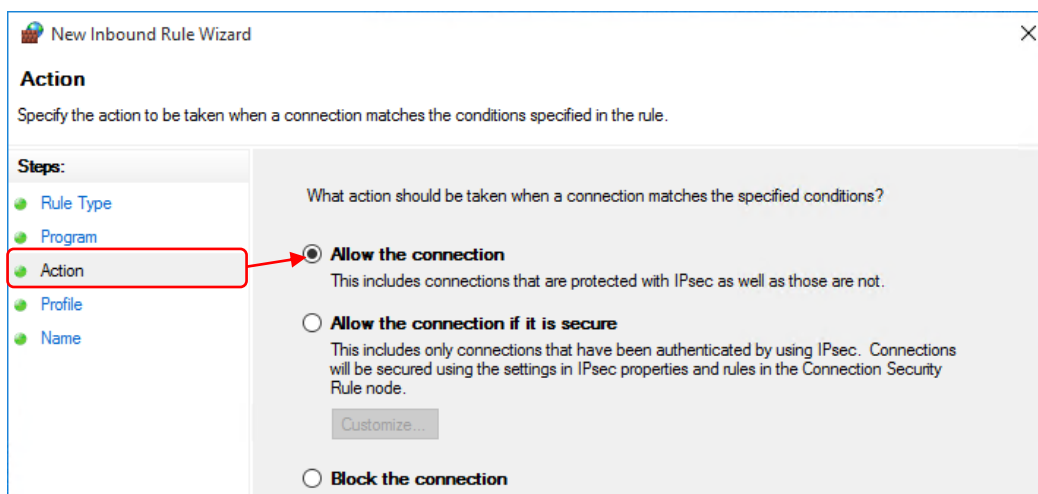
1. Open the **Windows Firewall with Advanced Security** window. For quick access:
  - a. Press **Win+R**.
  - b. Type **wf.msc**.
  - c. Press **Enter**.



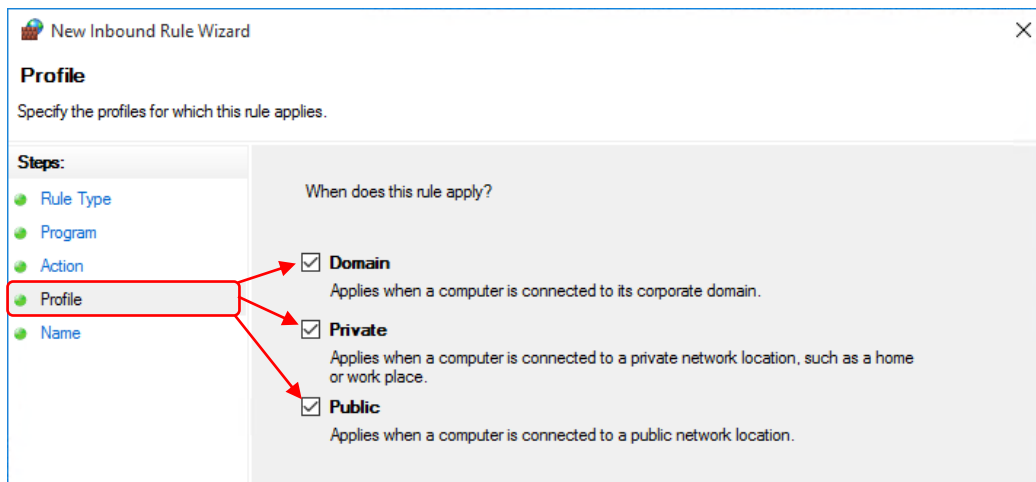
2. In the left pane, click **Inbound Rules**.
3. In the **Actions** pane, expand **Inbound Rules** and click **New Rule** to open the **New Inbound Rule Wizard**.
4. On the **Rule Type** page, select **Program**.
5. On the Program page, select **This program path**.



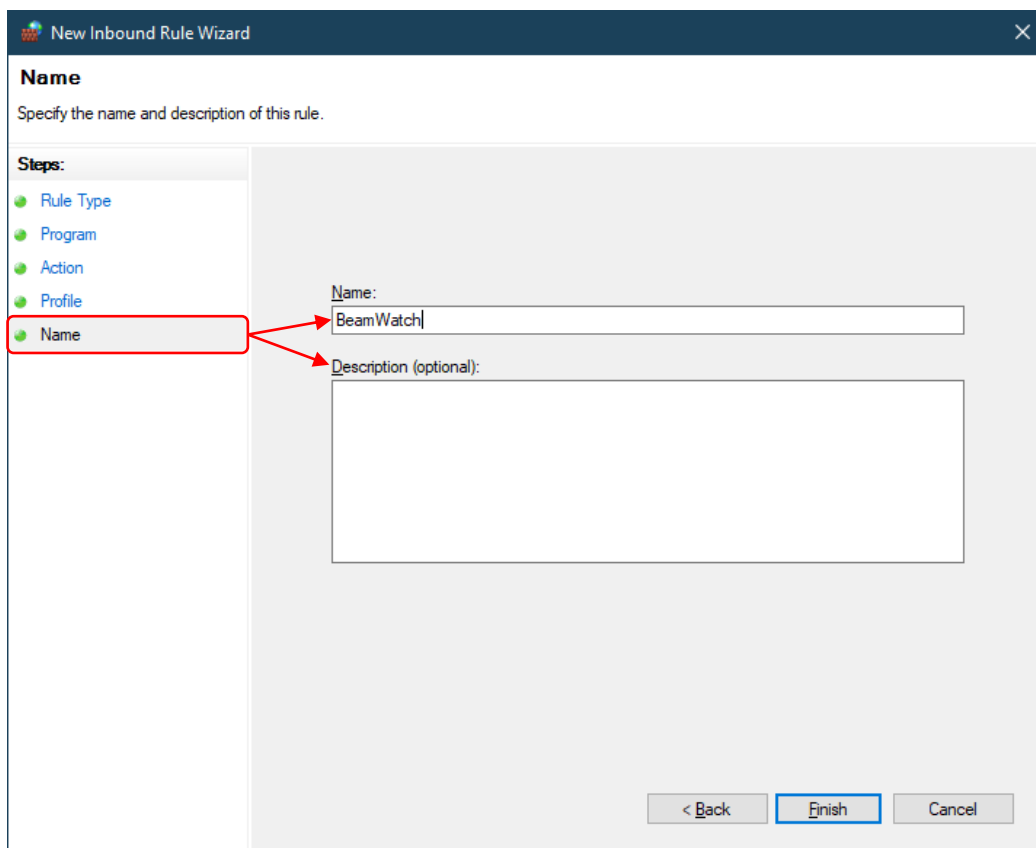
6. Click **Browse** and navigate to the program executable for the new rule.
  - a. Example: To set up a rule for the BeamWatch, navigate to:  
**C:\Program Files\Spiricon\BeamWatch\BeamWatch.exe.**
7. Click **Next**.
8. On the **Action** page, select **Allow the connection**.



9. Click **Next**.
10. On the **Profile** page, select the profile where the rule is to be applied. If you are unsure which profile to choose, select all three options.
  - Setting all three options is safe as the non-volatile storage in the BeamWatch cameras does not carry viruses.



11. Click **Next**.
12. On the **Name** page, enter a name for the rule and, if required, a description.



13. Click **Finish**. The new rule now appears in the **Inbound Rules** pane.

### c. Creating Custom Inbound Firewall Rules for the EA-1

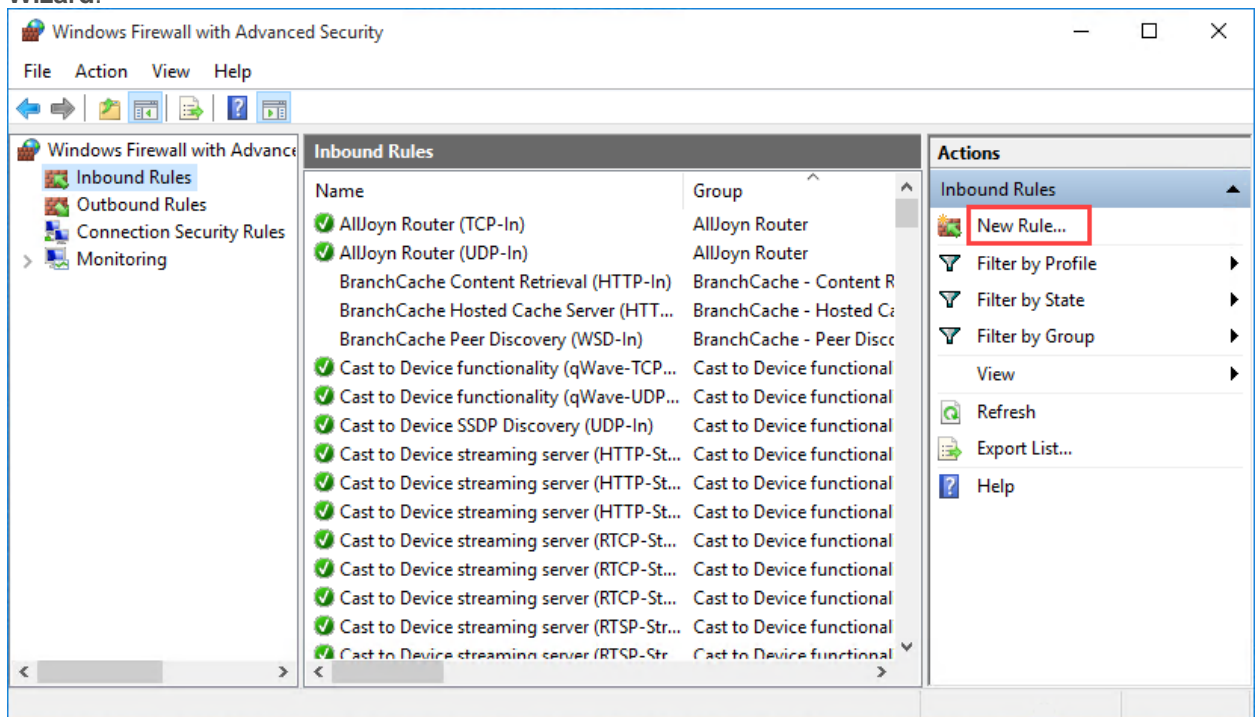
In most cases a firewall rule that creates the least port exposure is preferred. By default, the firewall rules that are created with the **New Inbound Rule Wizard** are as minimal as they can be, but additional options are available.

It may be necessary to create a custom firewall rule to allow a GigE Vision device to be discovered and to communicate, or other ethernet devices such as the EA-1 power meter in the BeamWatch Integrated.

These steps may also be used to create explicit rules for other port ranges used by BeamWatch.

To set up custom inbound rules:

1. Open the **Windows Firewall with Advanced Security** window. For quick access:
  - a. Press **Win+R**.
  - b. Type **wf.msc**.
  - c. Press **Enter**.
2. In the left pane, click **Inbound Rules**.
3. In the **Actions** pane, expand **Inbound Rules** and click **New Rule** to open the **New Inbound Rule Wizard**.



4. On the **Rule Type** page, select **Custom**.
5. On the **Programs** page, select **This Program Path** and enter the suggested path below. Click **Next**.
6. On the **Protocols and Ports** page, configure the **Protocol type**, **Local Port**, and **Remote Ports** fields according to the suggested rules tables below.
7. On the **Scope** page, only configure the local and remote IP scopes **if necessary** in your network environment, otherwise leave set to **Any IP address**.
8. On the **Action** page, select **Allow the connection**.

9. On the **Profile** page, select the profile where the rule is to be applied: **Domain**, **Private**, or **Public**.
  - This should match the designation assigned to the network adapter, which can be found for each adapter in the **Windows Network and Sharing Center**.
  - If you are unsure which profile to choose, use the default selection of all three options.
10. On the **Name** page, provide a recognizable **Name** (required) and **Description** (optional).
11. Click **Finish**. The new rule now appears in the **Inbound Rules** pane.

<p><b>Name:</b> BeamWatch or BeamGage</p> <p><b>Protocol type:</b> UDP</p> <p><b>Local Port:</b> Specific Ports; 11000</p> <p><b>Remote port:</b> Specific Ports; 11000</p> <p><b>Program Path:</b> %ProgramFiles%\Spiricon\<applicationname&gt;\spiricon.dataserver.exe< p=""></applicationname&gt;\spiricon.dataserver.exe<></p>
--

## VIII. Additional Resources

### a. Pleora

- <https://supportcenter.pleora.com/s/article/Configuring-the-Network-Settings-for-a-GigE-Vision-Device-KBase>
- <https://supportcenter.pleora.com/s/article/Configuring-Your-Computer-and-Network-Adapters-for-Best-Performance-KBase>

### b. Allied Vision

- [https://www.alliedvision.com/fileadmin/content/documents/products/cameras/various/installation-manual/GigE\\_Installation\\_Manual.pdf](https://www.alliedvision.com/fileadmin/content/documents/products/cameras/various/installation-manual/GigE_Installation_Manual.pdf)

### c. Basler

- [https://docs.baslerweb.com/network-configuration-\(gige-cameras\)](https://docs.baslerweb.com/network-configuration-(gige-cameras))
- [https://docs.baslerweb.com/hardware-installation-\(gige-cameras\)#recommended-gige-network-adapters](https://docs.baslerweb.com/hardware-installation-(gige-cameras)#recommended-gige-network-adapters)

### d. National Instruments NI-IMAQdx

- <https://knowledge.ni.com/KnowledgeArticleDetails?id=kA03q000000YM6JCAW&l=en-US>





Copyright © 2022 by MKS Instruments, Inc.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as may be expressly permitted in writing by MKS Instruments, Inc. mksinst™ is a trademark of MKS Instruments, Inc.

Document No 50349-001 Rev C 27 Jul 2022

For latest version, please visit our website: [www.ophiropt.com/photonics](http://www.ophiropt.com/photonics)