govcomm
A SynapseITS™ company

GC-WWVDS Series Configuration Manual

PN:	350-163
Revision:	A
Issued:	10/15/2025

Quality Record

ISO 9001 is the international standard that demonstrates the ability of a company to consistently meet customer and regulatory requirements. GovComm is ISO 9001:2015 certified.

Approval

The signatures below certify that this document has been reviewed and accepted and demonstrate that the signatories are aware of all the requirements contained herein and are committed to ensuring their participation.

	Name	Signature	Position	Date
Prepared by	Alex Ivanov	*Alex Ivanov*	Technical Writer	July 29, 2024
Reviewed by	Svet Veltchev	*Svet Veltchev*	CTO	August 2, 2024
Approved by	Craig Waltzer	*Craig Waltzer*	CEO	August 7, 2024

Amendment Record

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Page #	Context	Revision	Date
8, 9	IP addresses updated	2	December 05, 2024
9, 10, 13	RTSP connections updated	2	December 05, 2024
9, 10, 11, 12, 13, 19, 20	Screenshots updated/added	2	December 05, 2024
11, 12	Multipoint detection zone configuration explained	2	December 05, 2024
14	Confirmation zone configuration instructions updated	2	December 05, 2024
16	Sign testing instructions updated	2	December 05, 2024
17	Reporting instructions and screenshots updated	2	December 05, 2024
19	Wrong-way event simulation instructions updated	2	December 05, 2024
24	Recommended network settings updated	2	December 05, 2024

Company Proprietary Information

The electronic version of this document maintained on GovComm's online server in PDF format contains the latest revisions. It is the responsibility of the user to ensure that the document they are reading is the current version. Downloaded and printed versions of this document are uncontrolled.

Contents

About This Document

The purpose of this document is to provide step-by-step instructions for configuring the Wrong-Way Vehicle Detection System (WWVDS, also referred to as “the system”), including configuration instructions for:

- Detection and confirmation cameras
- Detection and confirmation zones
- AI engine
- Connected signs
- Network switch

The document also explains how to:

- Export configuration settings for backup and recovery purposes
- Import previously saved configuration settings

Additional Resources

Additional information about the WWVDS can be found in the following documents:

- “WWVDS Installation Manual”

Prerequisites and Tools

The key items you will need to set up a WWVDS are as follows:

- WWVDS and signs
- Computer with a network interface card
- 4 IP addresses
- Ethernet cable

WWVDS and Signs

The system and signs must be properly installed and connected to the power source.

For more information, see the “WWVDS Installation Manual”.

Computer

To set up the system, you will need a computer with an Internet browser.

This manual assumes that your computer has the following configuration:

- Operating system (OS):
  - Windows 10 or 11
- Internet Browser, e.g.:
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- Screen resolution: at least 720×480 pixels
- Connection to the same network switch as WWVDS unit using an Ethernet cable

GovComm has tested the WWVDS web interface only with the software listed above. If you are using a different OS and/or browser, the results may vary.

IP addresses

You will need at least 4 IP addresses allocated in the same IP subnet:

- 1 IP address for the WWVDS
- 2 IP addresses for IP cameras
  - 1 IP address for detection camera
  - 1 IP address for confirmation camera
- 1 IP address for the computer you will use to configure the WWVDS

If you are not sure what these addresses are, contact the network administrator at the appropriate Department of Transportation (DOT) office to confirm that IP addresses have been allocated and are valid.

Without prior configuration of IP addresses by the DOT network administrator, the system cannot be configured and operational. Allocation and assignment of IP addresses may take some time, so request IP addresses in advance.

Cables

You will need an Ethernet cable (CAT5 or CAT6) to connect your computer to the WWVDS network interface.

Network Interface with Ethernet Port

If your computer has a built-in Ethernet port (RJ 45 connector), use the Ethernet port to directly connect your computer to the WWVDS network interface.

If your computer does not have an Ethernet port, you can still connect to the WWVDS using, for example, a USB to Ethernet adapter or another adapter that adds an Ethernet port to your computer.

Updated Software and Firmware

In most cases, you do not need to install or update software or firmware for the system or its components, such as cameras, unless the system is not working properly.

However, given that there is sometimes a gap between the time systems are shipped and the time they are configured after installation, software updates may be required even during the initial configuration.

To check if software and/or firmware needs an update, call GovComm Technical Support at (305) 937-2000.

Supplemental Software Tools

To find the IP addresses of cameras connected to WWVDS, you may use the **DeviceManager** software that is provided for free by GovComm.

Configuration Manual

Print this manual or download it to your computer or mobile device and keep it handy when using the system.

Connect Computer's Network Interface to the WWVDS

Connect your computer to the WWVDS unmanaged network switch by using an Ethernet cable. Your WWVDS network interface has been pre-configured with the following settings:

- IP address: `10.1.10.64`
- Subnet mask: `255.255.255.0`
- Gateway: `10.1.10.1`
- Port: `8000`

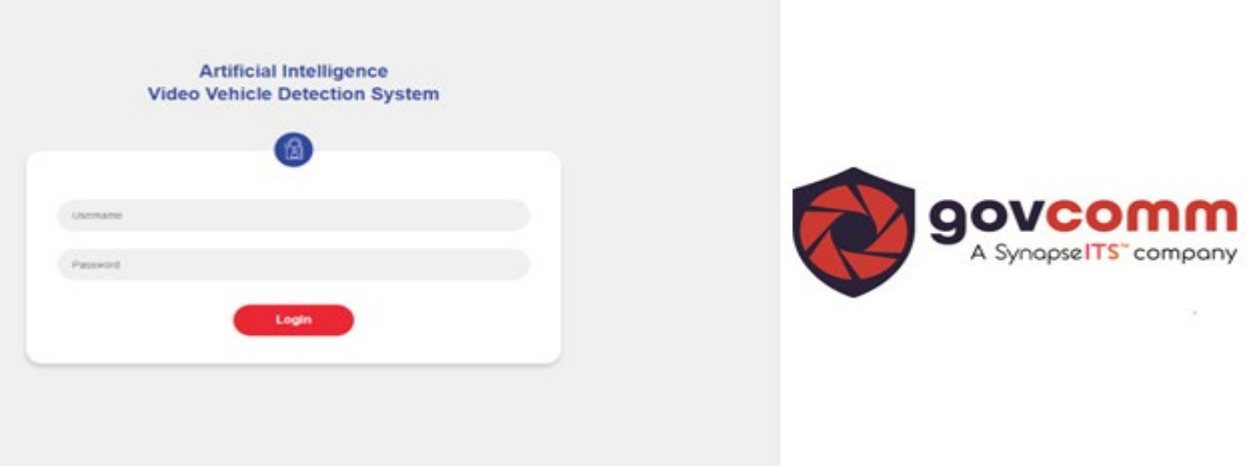
Configure WWVDS cameras to be accessible at IP addresses within the same subnet.

In this manual, the detection camera is configured to use 10.1.10.77 and the confirmation camera is configured to use 10.1.10.95.

To ensure that the WWVDS equipment and your computer are on the same TCP/IP subnet, you need to assign your computer's network interface the following settings as described in "Appendix A. Configuring IP":

- IP address: `10.1.10.100`
- Subnet mask: `255.255.255.0`
- Gateway: `10.1.10.1`

Check if you can access the WWVDS web interface at `http://10.1.10.64:8000`



If you cannot access the web interface, check the TCP/IP settings of your computer: to communicate, both your computer and WWVDS should belong to the same TCP/IP subnet. For information on how to configure your computer's IP address, see "Appendix A. Configuring IP Addresses".

Configure WWVDS Settings

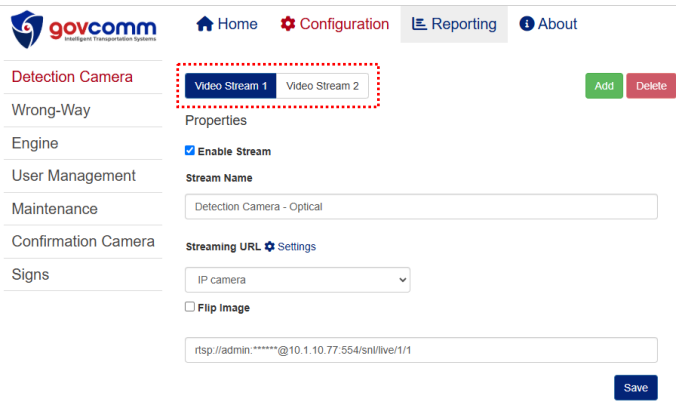
Log in to the WWVDS web interface at `http://10.1.10.64:8000` using the default credentials:

- Username: `admin`
- Password: `GovComm1`

You will see the system home page:

Configure Detection Camera

Navigate to **Configuration > Detection Camera**. You will see the optical video stream settings for the detection camera (**Video Stream 1**):



Note: If you do not see any video streams configured, click **Add** to create a new video stream from the connected bi-spectrum camera. Configure this new stream using the same settings as shown in the screenshots provided in this section.

Ensure, an RTSP connection line is specified for channel 1, similar to the following (replace 10.1.10.77 with the IP address you assigned to the detection camera):

```
rtsp://admin:******@10.1.10.77:554/snl/live/1/1
```

The asterisks (******) mask the password, in the example above, the **admin** user password.

Click **Save** after making changes.

Click **Video Stream 2** to check the thermal video stream settings:

Verify the second (thermal) video stream points to channel 2 of the bi-spectrum camera (replace `10.1.10.77` with the IP address you assigned to the detection camera):

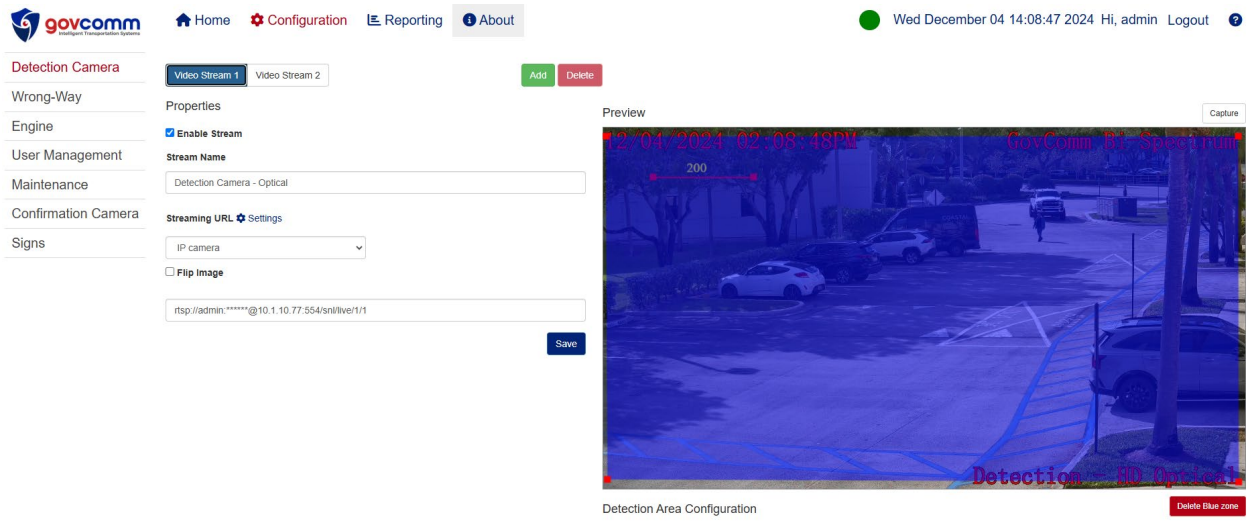
```
rtsp://admin:******@10.1.10.77:554/snl/live/2/1
```

Click **Save** after making changes.

Once you have completed the configuration process, you should be able to view live video feeds from both the optical and thermal sensors of the detection camera.

Customize the Detection Area

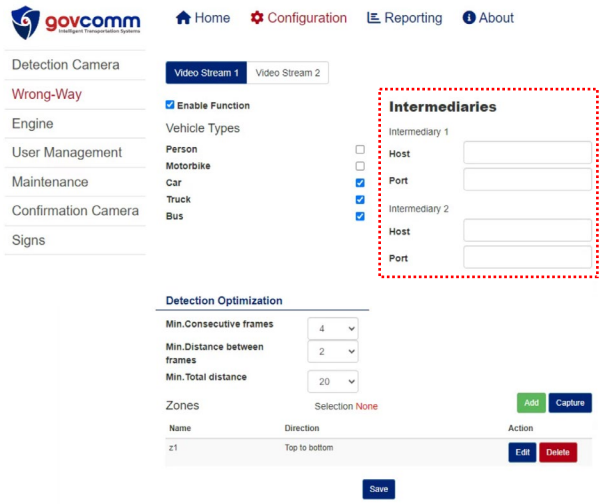
The detection area is represented by a blue rectangle in the camera preview. To customize its size and position, drag the red square markers located at the corners of the rectangle. Don't forget to click **Save** to apply your changes.



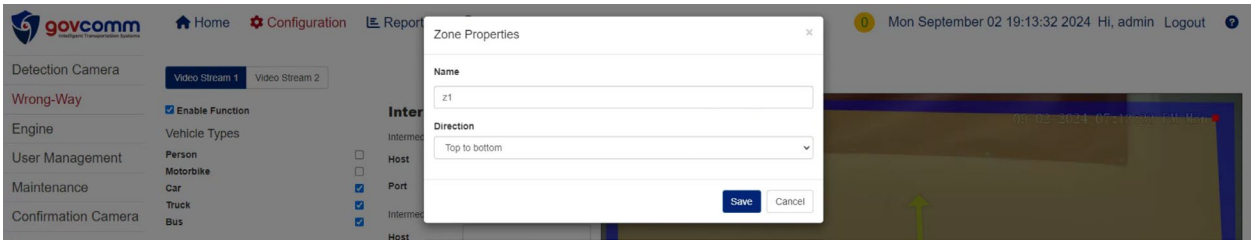
You can independently adjust the detection areas for both optical and thermal video streams.

Configure Wrong-Way Detection Parameters

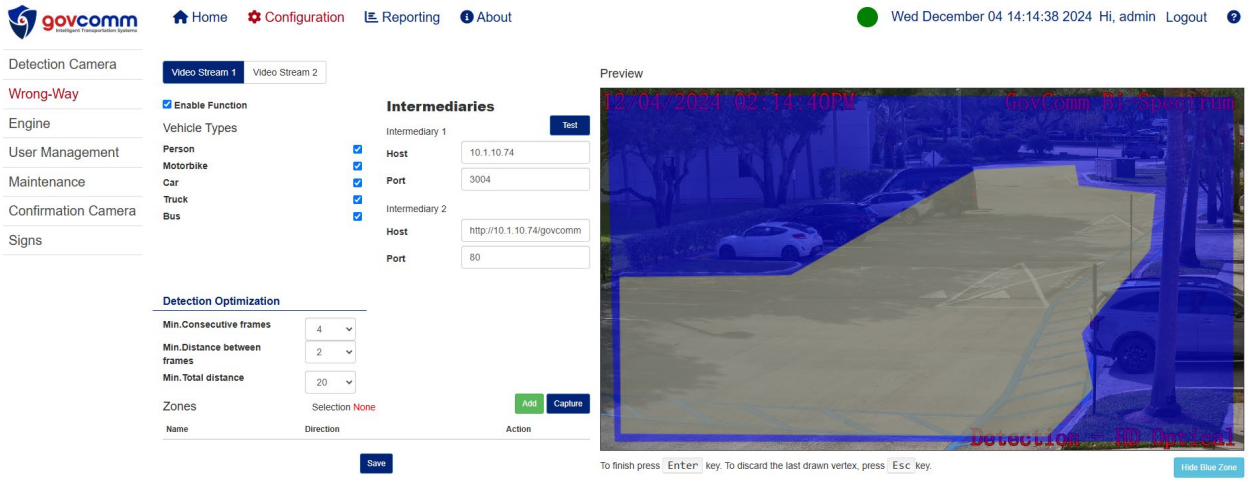
Navigate to **Configuration > Wrong-Way**. You will see the detection zone settings for the optical video stream (**Video Stream 1**). Enter the traffic management center (TMC) server parameters in the **Intermediaries** pane:



If there are no detection zones configured, click **Add** to create a new detection zone:

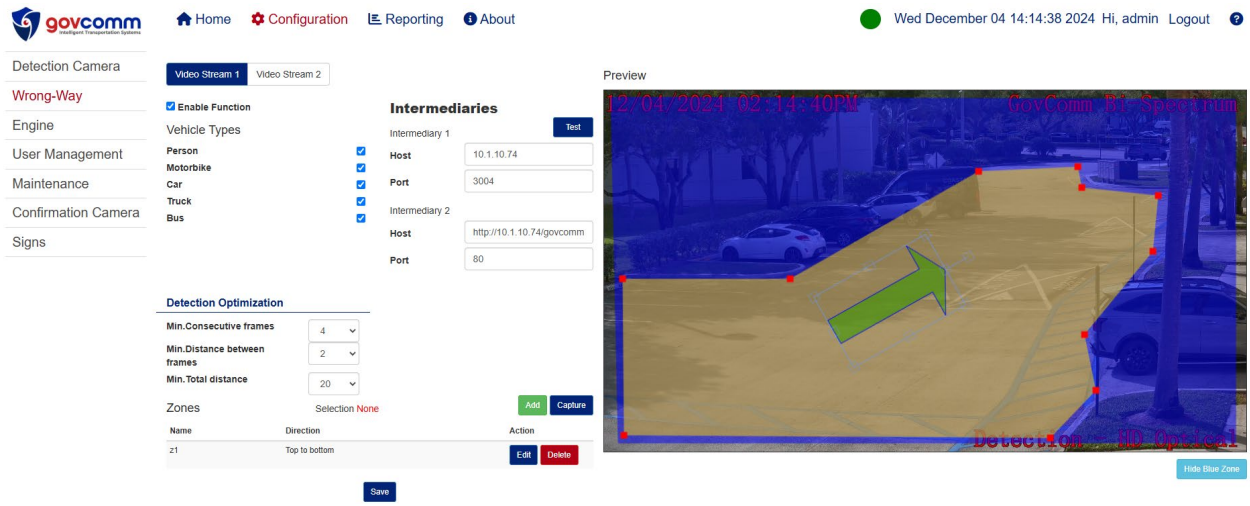


Click inside the blue area to add edge points for the detection zone. The yellow area indicates the detection zone. Press **Enter** to finish editing.



Ensure the detection zone remains within the blue detection area boundary.

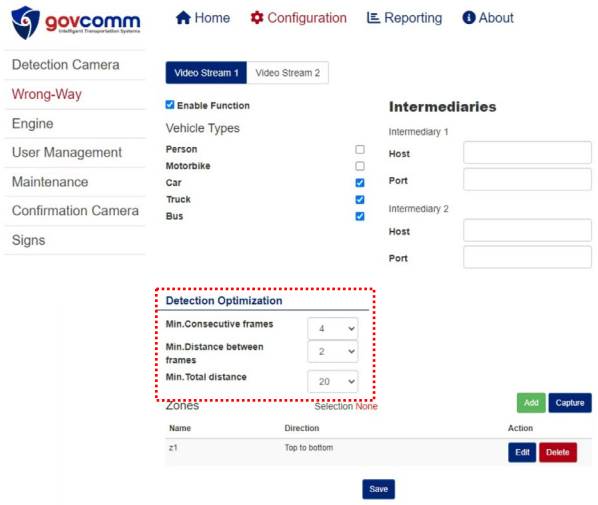
To set the traffic direction, click outside the yellow zone in the camera view, click the green arrow, and drag the marker near the arrow point to indicate the traffic flow:



Click **Save** to save changes. To apply these changes, you need to perform steps described in the “Restart AI Engine” section.

Note: Depending on the software version, multipoint detection zones may not be available. In such cases, rectangular detection zones can be used, which are suitable for most scenarios. If your project requires multipoint detection zones but your system only supports rectangular zones, please contact GovComm for a software update.

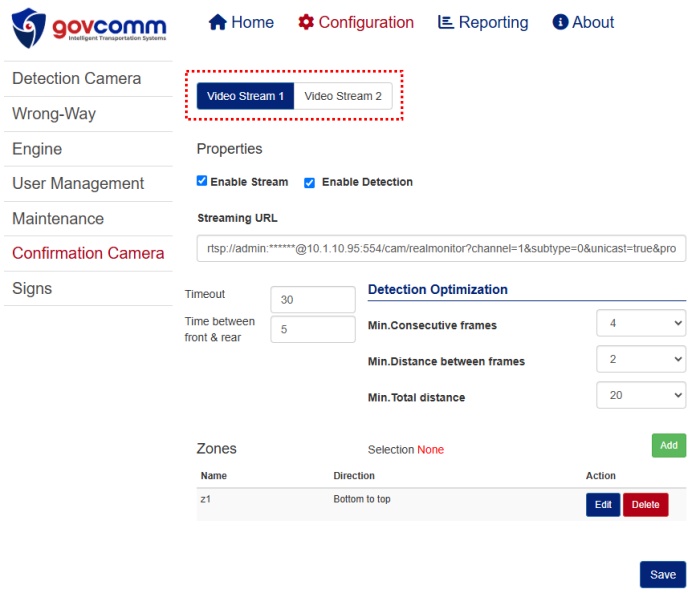
Ensure the detection parameters in the **Detection Optimization** pane are configured as shown on the screenshot below:



Repeat the same steps for **Video Stream 2** (thermal). You can independently adjust the detection optimization parameters for both optical and thermal video streams.

Configure Confirmation Camera

Navigate to **Configuration > Confirmation Camera**. You will see the optical video stream settings for the confirmation camera (**Video Stream 1**):



Note: If you do not see any video streams configured, click **Add** to create a new video stream from the connected bi-spectrum camera. Configure this new stream using the same settings as shown in the screenshots provided in this section.

Ensure, an RTSP connection line is specified for channel 1, like the following (replace `10.1.10.66` with the IP address you assigned to the confirmation camera):

```
rtsp://admin:******@10.1.10.95:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif
```

The asterisks (******) mask the password, in the example above, the **admin** user password.

Click **Save** after making changes.

Click **Video Stream 2** to check the thermal video stream settings. Verify the second (thermal) video stream points to channel 2 of the bi-spectrum camera (replace 10.1.10.65 with the IP address you assigned to the confirmation camera):

```
rtsp://admin:******@10.1.10.95:554/cam/realmonitor?channel=2&subtype=0&unicast=true&proto=Onvif
```

Click **Save** after making changes. Once you have completed the configuration process, you should be able to view live video feeds from both the optical and thermal sensors of the confirmation camera.

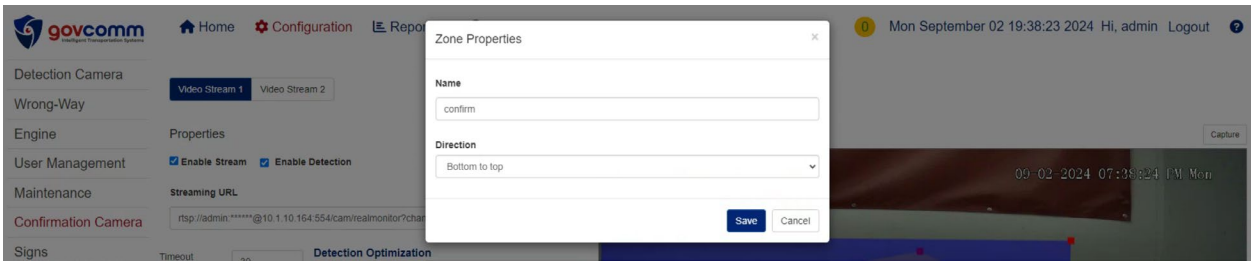
Customize the Confirmation Area

The confirmation area is represented by a blue rectangle in the camera preview. To customize its size and position, drag the red square markers located at the corners of the rectangle. Don't forget to click **Save** to apply your changes.

You can independently adjust the confirmation areas for both optical and thermal video streams.

Configure Wrong-Way Confirmation Parameters

If there are no confirmation zones configured, click **Add** to create a new confirmation zone:

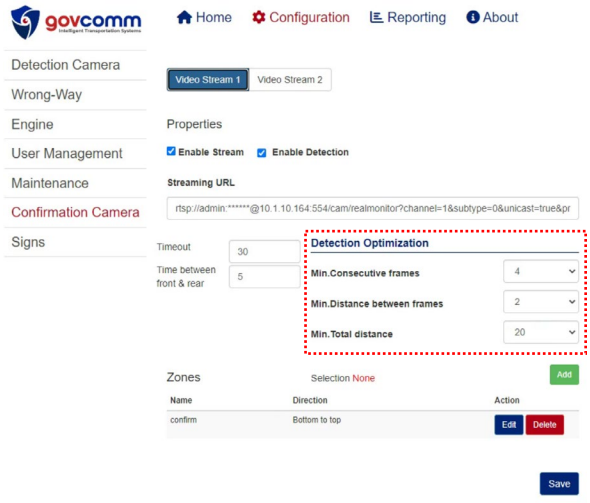


Adjust the confirmation zone size and position following the same steps as outlined in the “Configure Wrong-Way Detection Parameters” section to encompass the desired confirmation area. Ensure the confirmation zone stays within the blue boundary.

Note: Depending on the software version, multipoint confirmation zones may not be available. In such cases, rectangular detection zones can be used, which are suitable for most scenarios. If your project requires multipoint confirmation zones but your system only supports rectangular zones, please contact GovComm for a software update.

Click **Save** after making changes. To apply these changes, you need to perform steps described in the “Restart AI Engine” section.

Ensure the detection parameters in the **Detection Optimization** pane are configured as shown on the screenshot below:

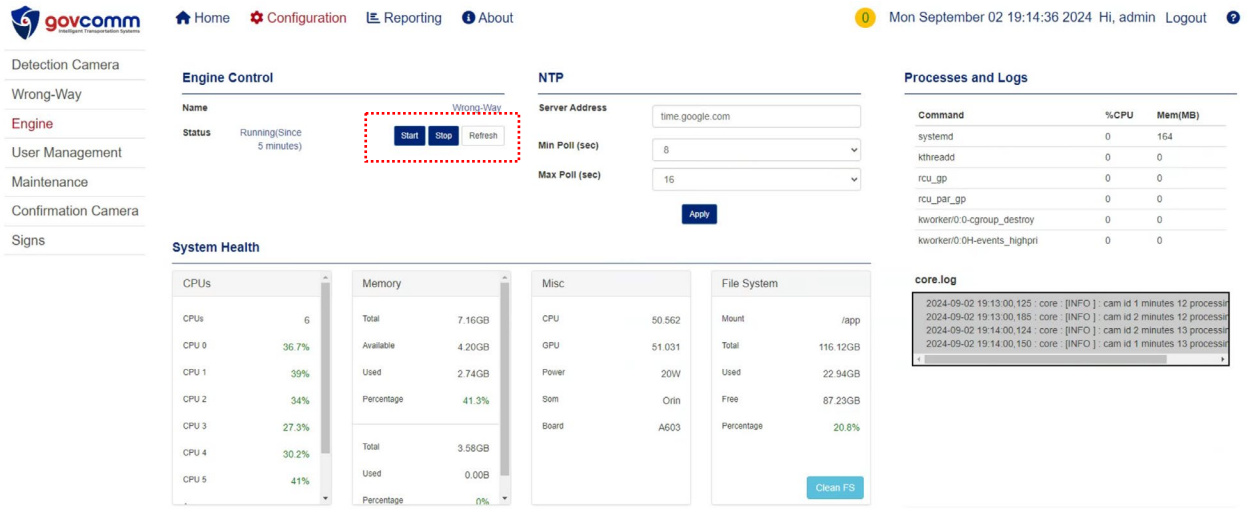


Repeat the same steps for **Video Stream 2** (thermal).

You can independently adjust the detection optimization parameters for both optical and thermal video streams.

Restart AI Engine

To apply new parameters, you must restart the AI engine. In the WWVDS web interface, navigate to **Configuration > Engine**.

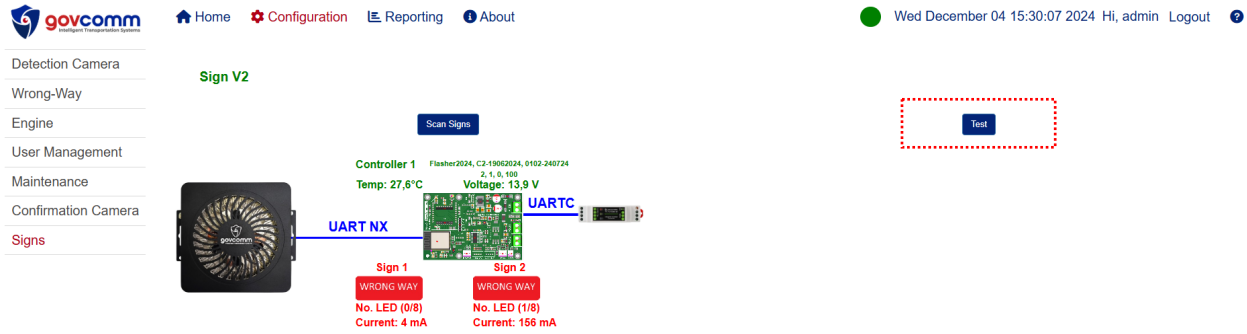


In the **Engine Control** pane, click **Stop** to halt the engine, then click **Refresh** to verify its stopped status. Finally, click **Start** to restart the AI engine.

Following the AI engine restart (that may take up to 20 seconds), you might need to log out of the WWVDS web interface and then log back in.

Test the Highlighted Signs

Navigate to **Configuration > Signs** in the WWVDS web interface. If no sign information is displayed, click the **Scan Signs** button to view the connected signs status.

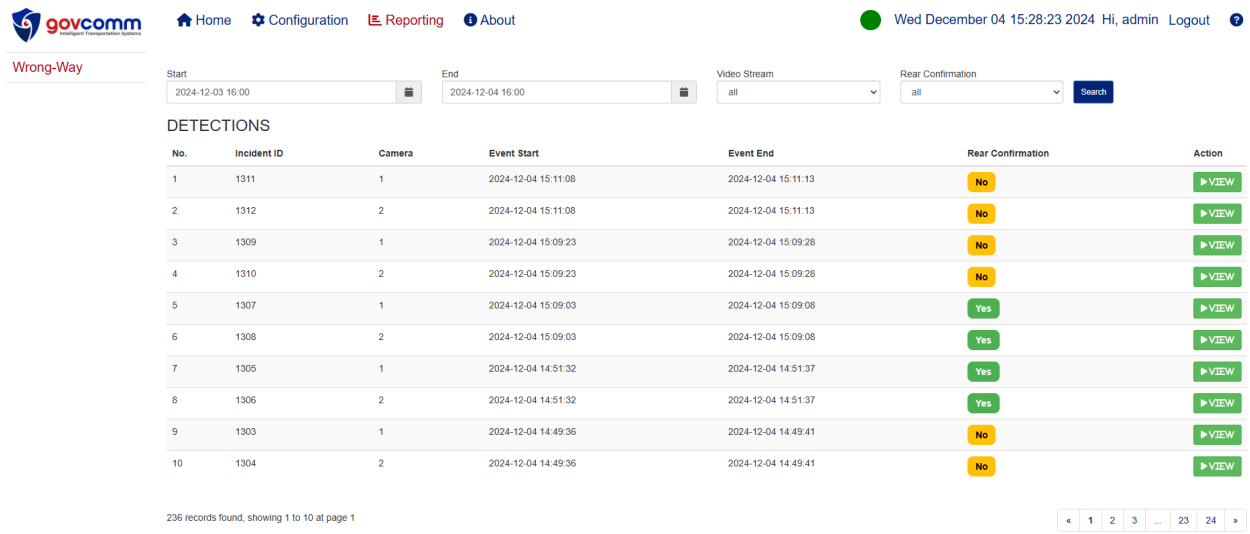


Click the **Test** button to test the signs. The highlighted signs will flash for approximately 30 seconds.

Maintenance Tasks

Reporting

The **Reporting** page, accessible from the top-level menu, allows you to search through the incident database. You can filter events by start and end time, source video stream (e.g., optical or thermal camera), and confirmation status (confirmed or unconfirmed). Confirmed events indicate the vehicle passed the confirmation zone, while unconfirmed events indicate the vehicle changed direction before reaching the confirmation zone.

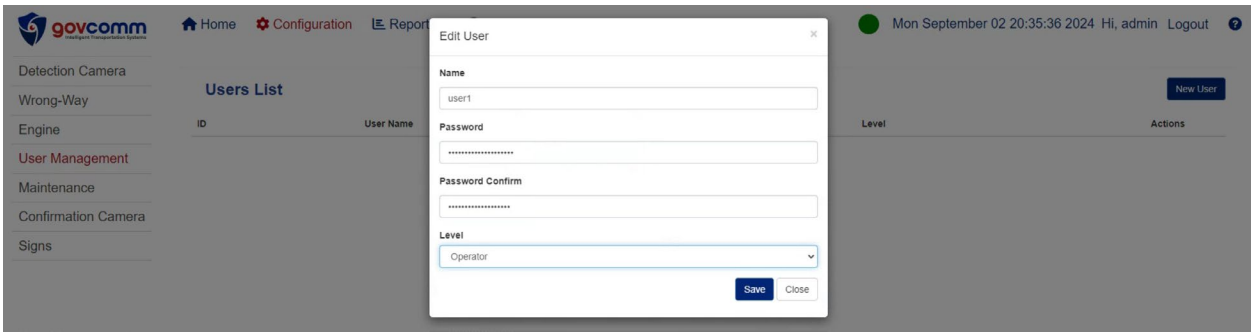


To view detailed information about an incident, including timestamps and associated images, click the **View** button:

Note: Depending on the software version, the Rear Confirmation filter may not be available. If your project requires this filter, please contact GovComm for a software update.

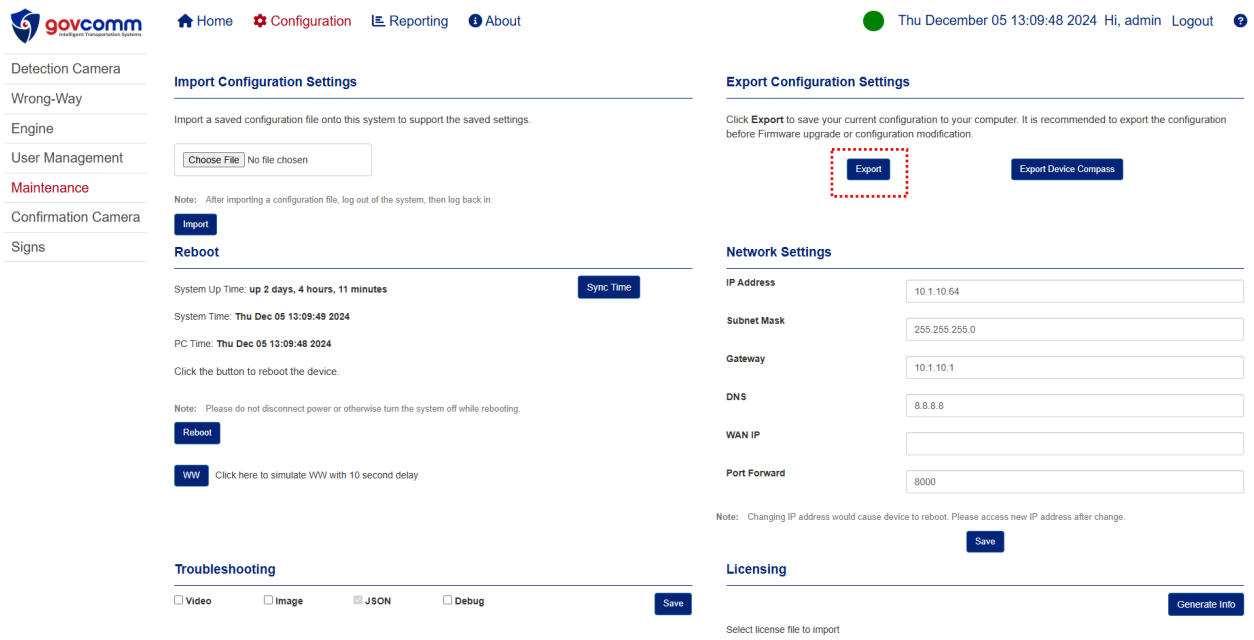
User Management

The **Configuration > User Management** page allows you to add and manage users who have access to the system.



Backing Up & Restoring Your Configuration

Once you have confirmed that the system is functioning properly, it is important to export the configuration settings for backup purposes. Navigate to **Configuration > Maintenance** and click **Export**. Your browser will download the configs.zip file.

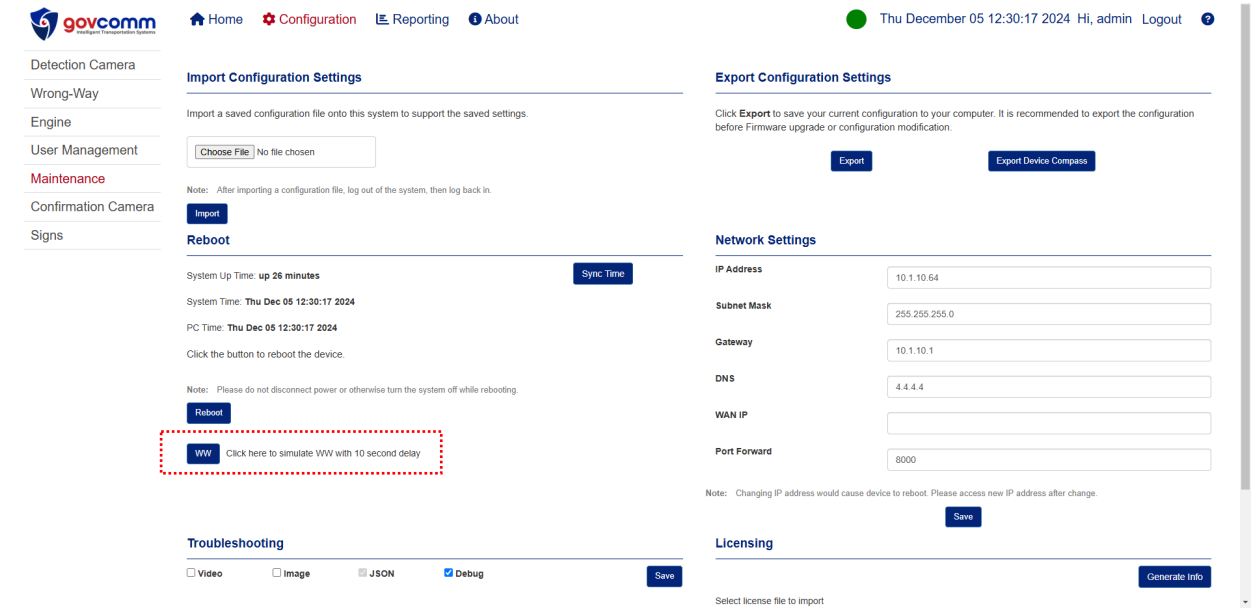


If you need to set up another system with the same configuration, you can import the previously exported zip file: navigate to **Configuration > Maintenance**, click **Import Configuration Settings** and select the previously exported zip file.

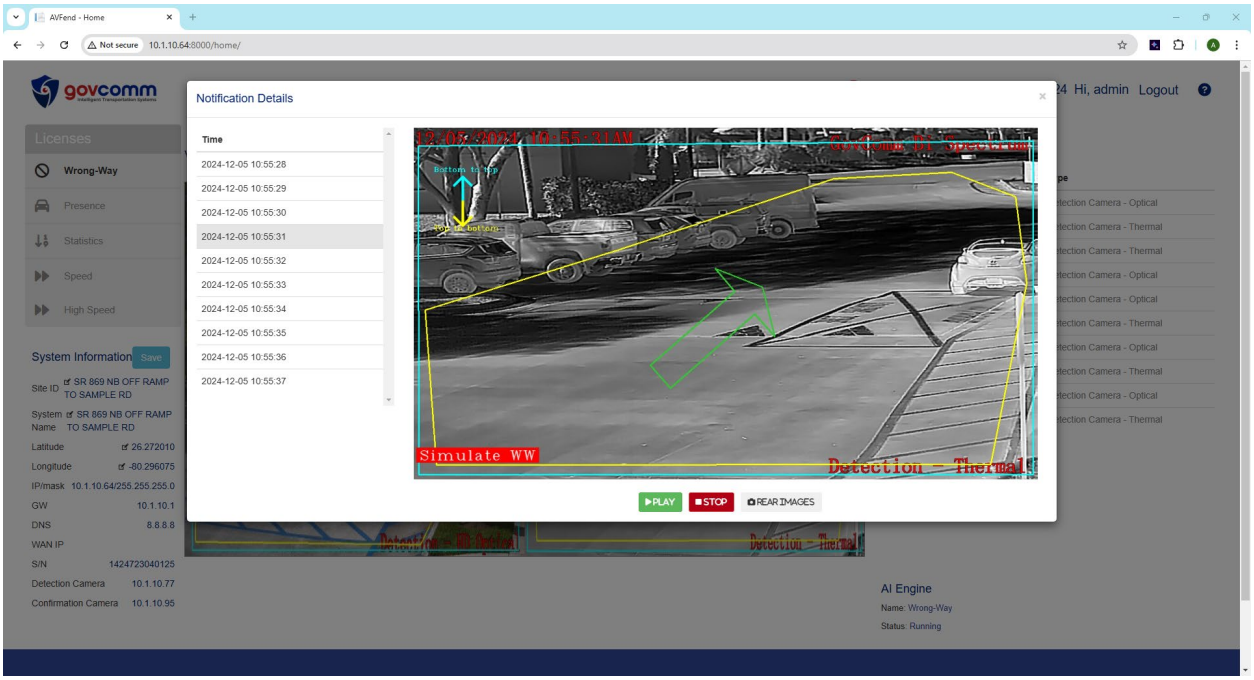
After importing the configuration, you will need to log out and log back in for the new settings to take effect and the updated configuration to be visible.

Wrong-Way Event Simulation

The **WW** button simulates a wrong-way event. This will activate the highlighted signs and generate corresponding records in the **Reporting** menu and on the **Home** page.



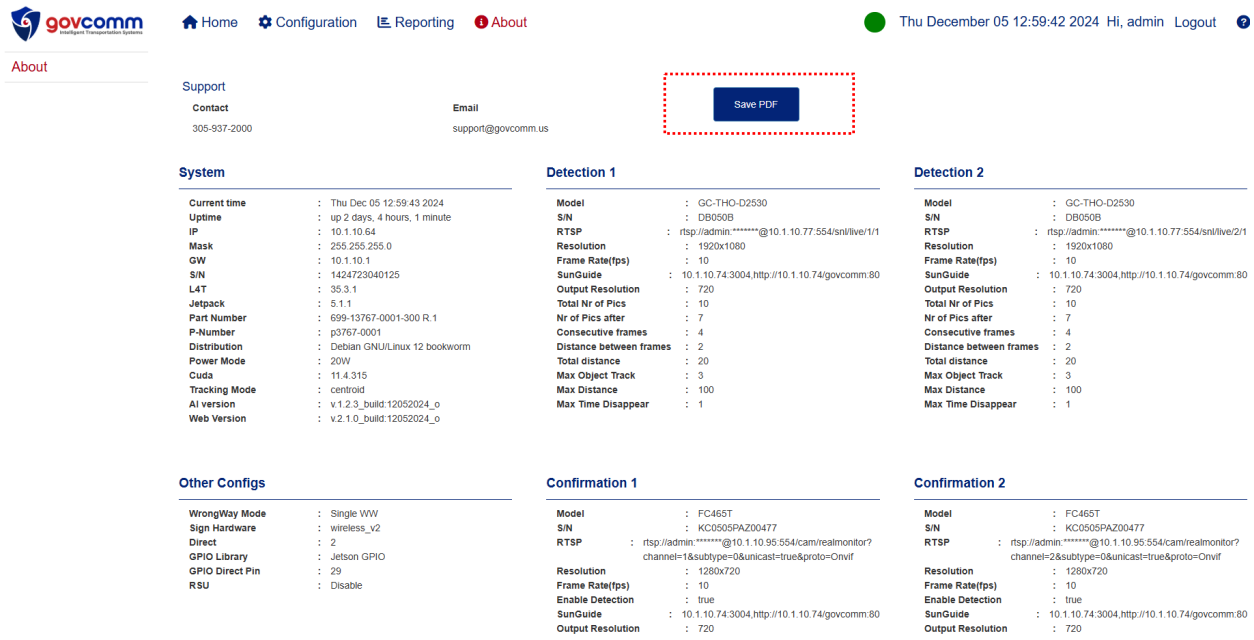
The simulated wrong-way events will be labeled accordingly on the associated images.



About

The **About** menu item allows you to view and save a PDF file containing a detailed summary of the system's configuration. This information is useful for reporting and archiving purposes.

Note: The software may take up to 30 seconds to populate the page with all WWVDS parameters. Please wait until the information is fully displayed before saving the PDF file.



Appendix A. Configuring IP Addresses

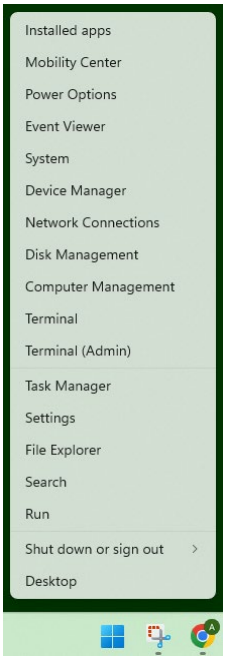
To communicate, your computer and the system must have compatible IP protocol settings, namely, they must belong to the same TCP/IP subnet.

Open the Run Window

The **Run** window is used to launch applications on Windows computers.

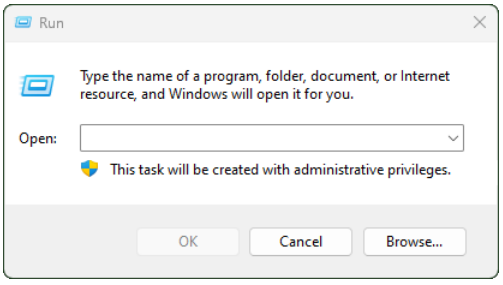
To open the **Run** window:

- Right-click the Windows **Start** button, then select **Run** from the pop-up menu.



- Or, if your keyboard has a **Windows** logo key (usually between **CTRL** and **ALT** in the lower left corner), press **Windows + R** on your keyboard (press the **Windows** logo key and the **R** key on your keyboard at the same time).

You will see the **Run** window:



Configuring Network Settings

Depending on your preference you can use:

- Windows Graphical User Interface (GUI) by following the instructions in the "Changing Network Interface Settings Using GUI" section
- Or Windows Command Line Interface (CLI) by following the instructions in the "Changing Network Interface Settings Using CLI" section

Regardless of the method you choose, the result will be the same: your computer's network interface will be configured to communicate with the system.

Changing Network Interface Settings Using GUI

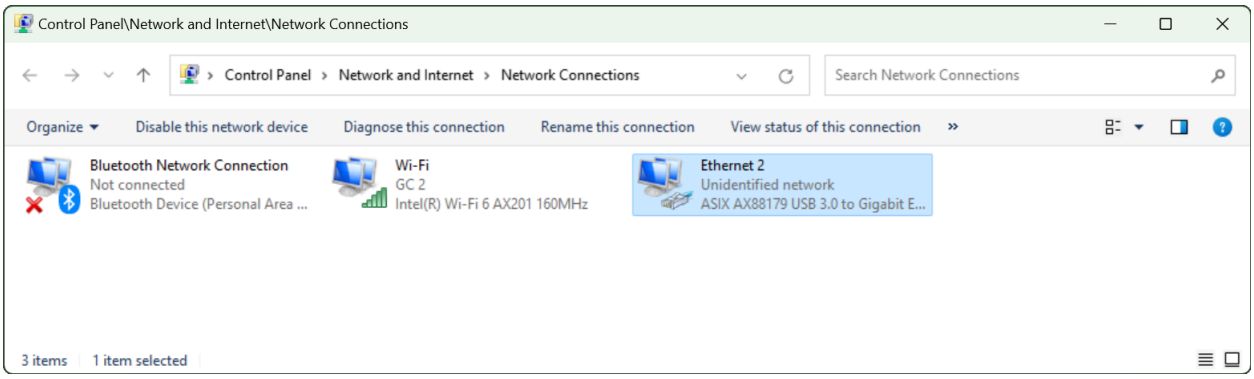
Network interface parameters are set using the IP protocol properties window.

Open the IP Protocol Properties Window

Open the **Run** window as described in the "Open the **Run** Window" section above.

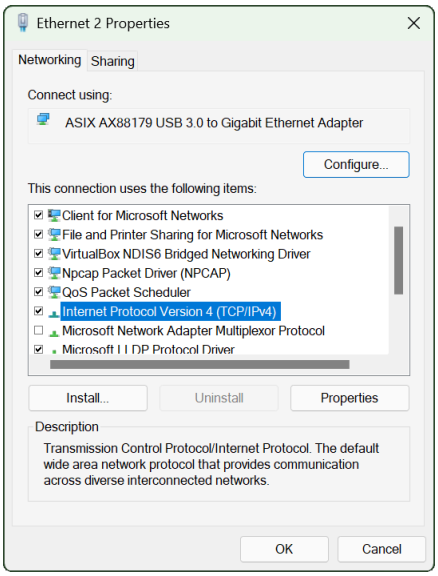
In the **Run** window, type `ncpa.cpl` and press **Enter** or click **OK**.

You will see the **Network Connections** window:



Right-click the Ethernet connection and click **Properties** from the pop-up menu to open the connection properties window.

In the connection properties window, select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties** below the list of items.

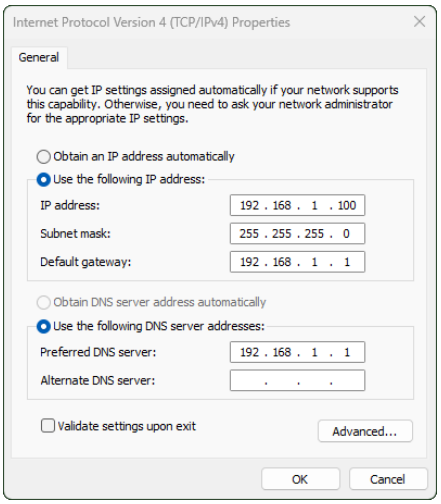


Save Your Current Network Settings

After changing your computer's network interface settings, you may lose your Internet connection. If you are using a GUI, write down the original settings, save a screenshot of the network connection properties window on your computer, or take a screenshot using your phone. To restore the original network settings, follow the steps in the “Restoring Network Interface Settings Using GUI” section.

Set the Recommended Network Settings

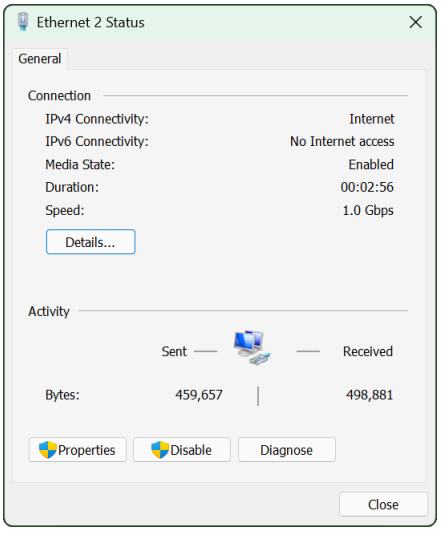
In the Internet protocol properties window, enter the settings and click **OK** (replace the addresses with the ones that are relevant for your configuration, e.g. `10.1.10.100` if you need to connect to the main WWVDS unit, or `192.168.1.100` if you need to connect to the cameras).



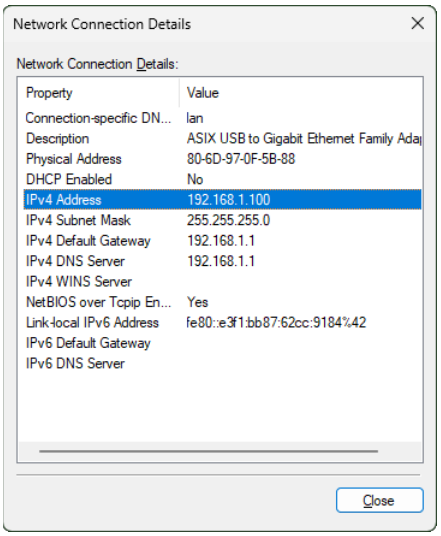
In the connection properties window (shown above), click **OK** to apply the settings and close the connection properties window.

Make Sure the Settings Have Been Applied

In the **Network Connections** window, double-click the Ethernet connection to open the connection status window:



Click **Details** to check that the Ethernet network interface has the recommended network settings:



Click **Close** to close the network connection details window.

Click **Close** once again to close the connection status window.

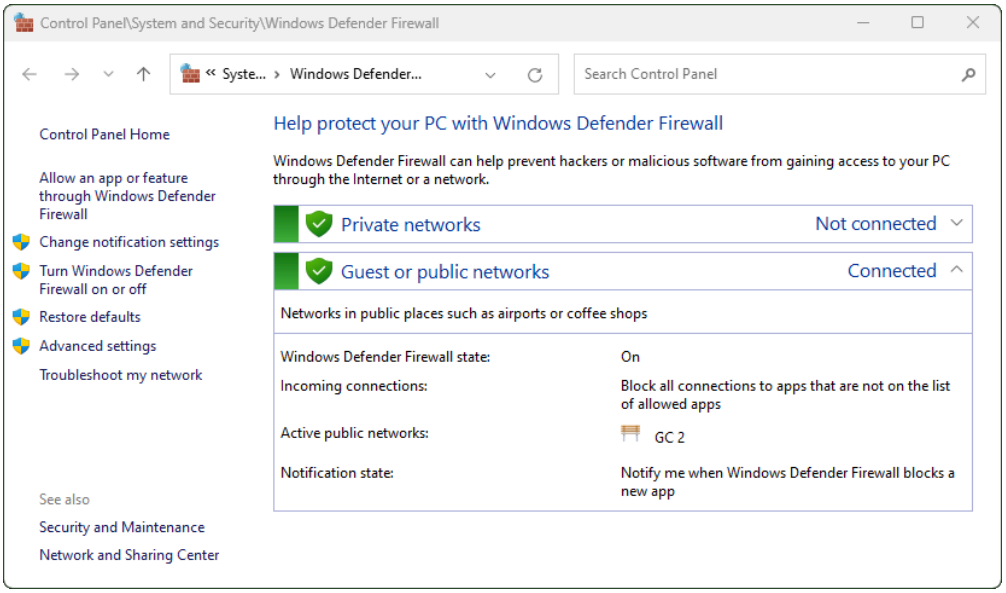
Disabling Windows Firewall Using GUI

It is recommended to disable Windows Firewall during system configuration.

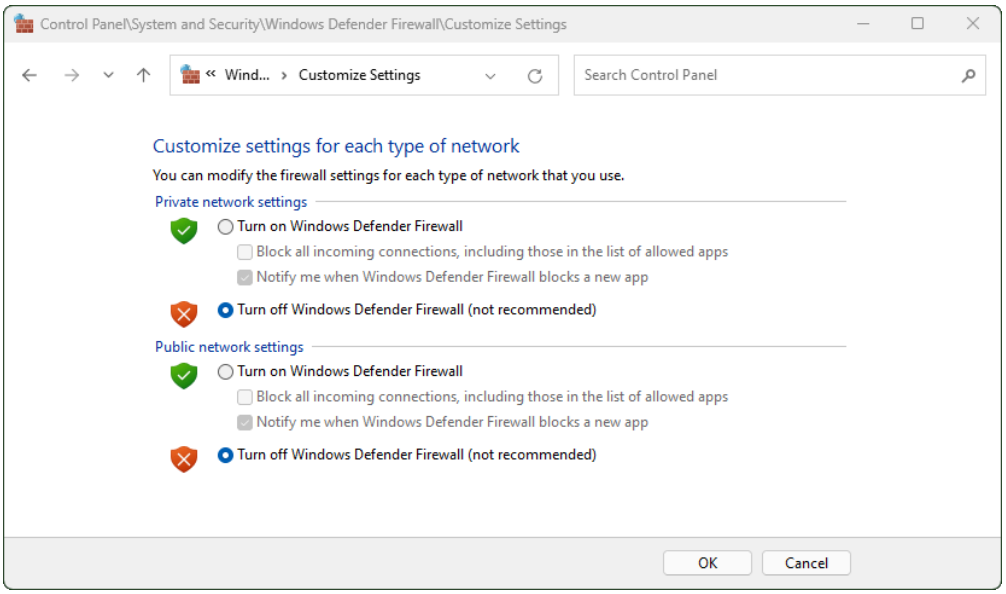
Open **the Run** window as described in the “Open the Run Window” section.

In the **Run** window, type firewall.cpl and press **Enter** or click **OK**.

You will see a **Windows Firewall** control panel similar to the following:



Select Turn **Windows Defender Firewall** on or off on the left and configure the firewall settings as shown in the screenshot below:



Click **OK** to save settings.

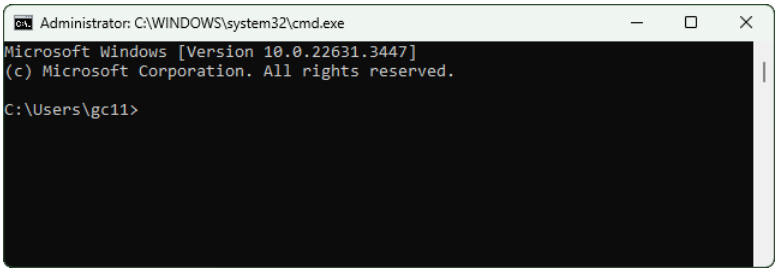
To enable the firewall, follow the steps in the "Enabling Windows Firewall Using GUI" section.

Changing Network Interface Settings Using CLI

Open the “**Run**” window as described in the “Open the Run Window” section.

In the **Run** window, type `cmd` and press **Enter** or click **OK**.

You will see the Windows command prompt window:



List Available Ethernet Network Interfaces

To view a list of Ethernet interfaces available on your computer, type the command and press **Enter**:

```
netsh interface ip show config | findstr "Ethernet"
```

Be sure to enter Ethernet with the first capital letter.

Depending on your computer configuration, you will see output similar to the following:

```
Configuration for interface "Ethernet 2"
```

Make a note of the network interface name. In the example above it is Ethernet 2 (case sensitive), but it may be different in your configuration. In the next steps we will use this name to configure your computer's network settings.

Save Your Current Network Settings

After changing your computer's network interface settings, you may lose Internet connection.

Once setup is complete, you can apply your computer's original network settings to restore access.

To save your current network configuration, use the command:

```
netsh -c interface dump > <drive_letter>:\<path>\<settings_file>
```

For example, to save the network configuration to the file original_ip_config.txt in the root folder of drive C:, run the command:

```
netsh -c interface dump > c:\original_ip_config.txt
```

To restore the original settings, follow the steps in the "Restoring Network Interface Settings Using CLI" section.

Set the Recommended Network Settings

To set network settings, use the `netsh` command:

```
netsh interface ip set address name="<interface name>" static
<computer_ip_address> <subnet_mask> <gateway_ip_address> <gateway_metric>
```

To configure an interface named Ethernet 2 with a static IP address of `192.168.1.100`, a subnet mask of `255.255.255.0`, and a default gateway of `192.168.1.1`, run the command:

```
netsh interface ip set address name="Ethernet 2" static 192.168.1.100
255.255.255.0 192.168.1.1 1
```

Or you can use a simplified version of the command (without specifying the gateway):

```
netsh interface ip set address name="Ethernet 2" static 192.168.1.100
255.255.255.0
```

Disabling Windows Firewall Using CLI

It is recommended to disable Windows Firewall during system configuration.

To disable Windows Firewall, run the following commands:

```
netsh advfirewall set domainprofile state off
netsh advfirewall set privateprofile state off
netsh advfirewall set publicprofile state off
```

To enable the firewall, follow the steps in the "Enabling Windows Firewall Using CLI" section.

Restoring Computer Settings

Restoring Network Interface Settings Using GUI

Open the **Run** window as described in the “Open the **Run** Window” section.

In the **Run** window, type `ncpa.cpl` and press **Enter** or click **OK**.

You will see the **Network Connections** window.

Right-click the **Ethernet** connection and select **Properties** from the pop-up menu to open the connection properties window.

In the connection properties window, select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties** below the list of items.

In the Internet protocol properties window, enter the original settings of your computer’s network interface and click **OK**.

In the **Network Connections** window, double-click the **Ethernet** connection to open the connection status window.

Click **Details** to check that the **Ethernet** network interface has the original network settings.

Click **Close** to close the network connection details window.

Click **Close** once again to close the connection status window.

Enabling Windows Firewall Using GUI

Open the **Run** window as described in the “Open the **Run** Window” section.

In the **Run** window, type `firewall.cpl` and press **Enter** or click **OK**.

You will see a **Windows Firewall** control panel.

Select **Turn Windows Defender Firewall** on or off on the left and configure the firewall to turn the firewall on.

Click **OK** to save settings.

Restoring Network Interface Settings Using CLI

Open the **Run** window as described in the “Open the Run Window” section.

In the **Run** window, type `cmd` and press **Enter** or click **OK**.

You will see the Windows command prompt window.

To restore the original network settings, use the command:

```
netsh exec <drive_letter>:\<path>\<settings_file>
```

For example, to restore the network configuration from the file named c:\original_ip_config.txt, run the command:

```
netsh exec c:\original_ip_config.txt
```

To configure a network interface to automatically obtain an IP address from a DHCP server, use the command:

```
netsh interface ip set address "<interface_name>" dhcp
```

For example, if the interface name is Ethernet 2, run the command:

```
netsh interface ip set address "Ethernet 2" dhcp
```

Enabling Windows Firewall Using CLI

To turn on Windows Firewall, run the following commands:

```
netsh advfirewall set domainprofile state on
netsh advfirewall set privateprofile state on
netsh advfirewall set publicprofile state on
```

Appendix B. Updating Passwords for Bi-Spectrum Cameras

Using the DeviceManager Application

Open the **DeviceManager** application and click **Refresh**. You will see a list of bi-spectrum cameras on your network:

In the **DeviceManager** application, in the **Operation** column, click on the pencil icon and in the **Modify network parameters** pop-up window.

Update the administrator password for the camera (the default username is `admin`, and password is `GovComm1!`).

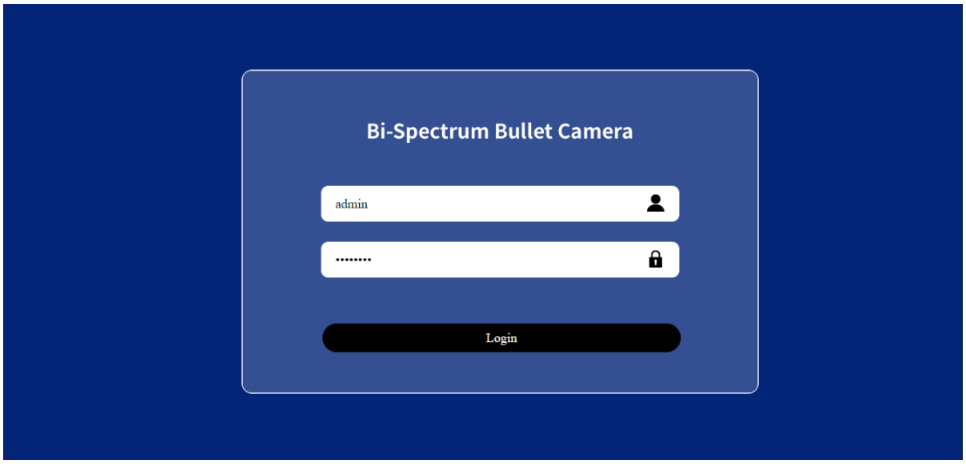
If necessary, you can update the network settings: IP address, subnet mask, and gateway.

Click **Modify** to save the changes.

Click **Confirm** in the **Information** pop-up window. You will see the updated camera settings in the **DeviceManager** application.

Using Web Interface

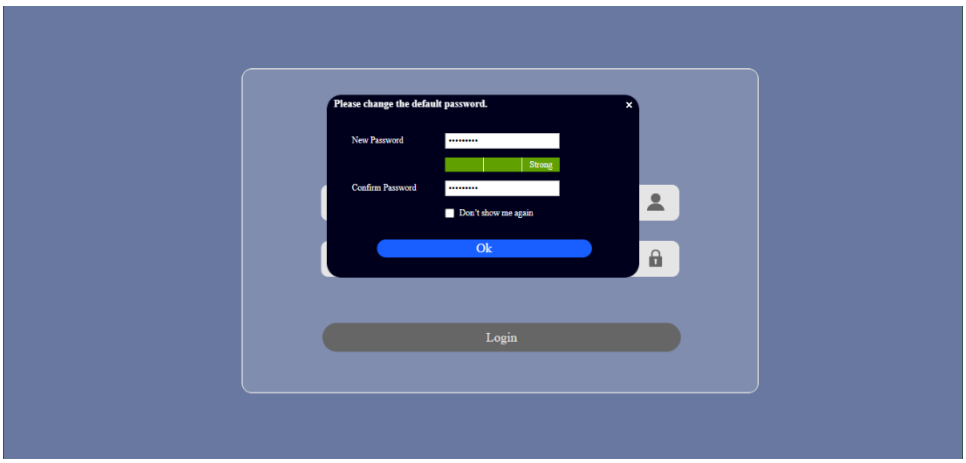
Enter the bi-spectrum camera's IP address in your browser to access the login window:



When connecting to a bi-spectrum camera for the first time, use the default credentials:

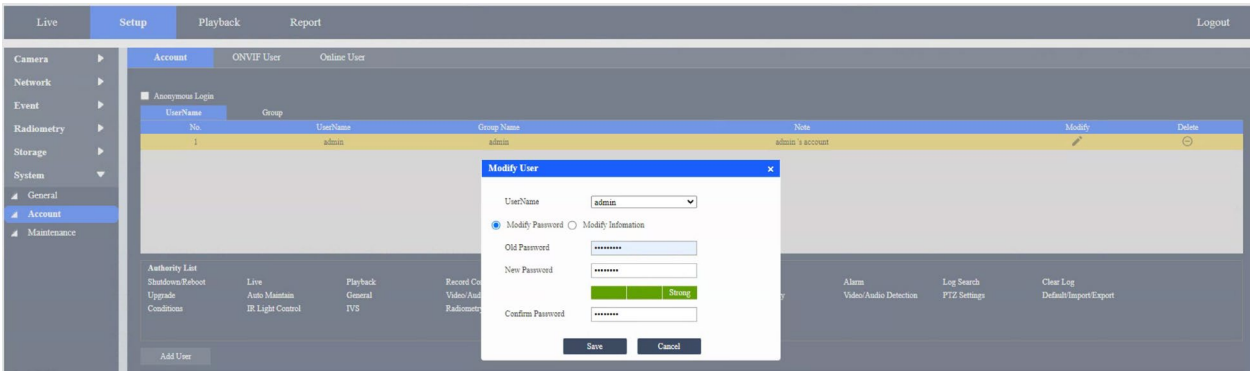
- Username: `admin`
- Password: `GovComm1!`

You will see a pop-up window asking you to change the default password:



Click **OK** to save the changes and open the camera's web interface.

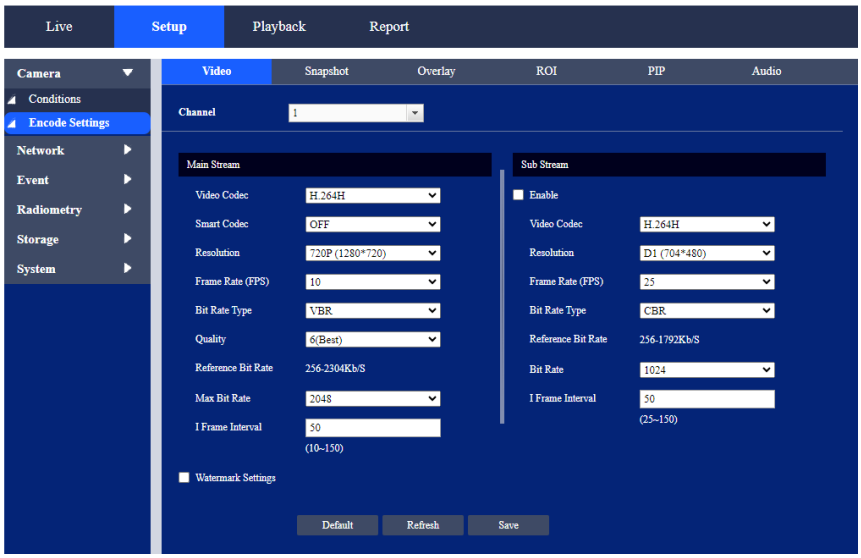
If you need to change the password later, in the web interface, navigate to **Setup > System > Account** and in the list of users click on the pencil icon in the **Modify** column:



Click **Save** to save the changes.

Appendix C. Recommended Video Settings for Bi-Spectrum Cameras

In the camera's web interface, navigate to **Setup > Camera > Encode Settings**. On the **Video** tab, configure the first channel (Optical) of the bi-spectrum camera as shown on the screenshot and click **Save**.



On the **Video** tab, configure the second channel (Thermal) of the bi-spectrum camera as shown on the screenshot and click **Save**.