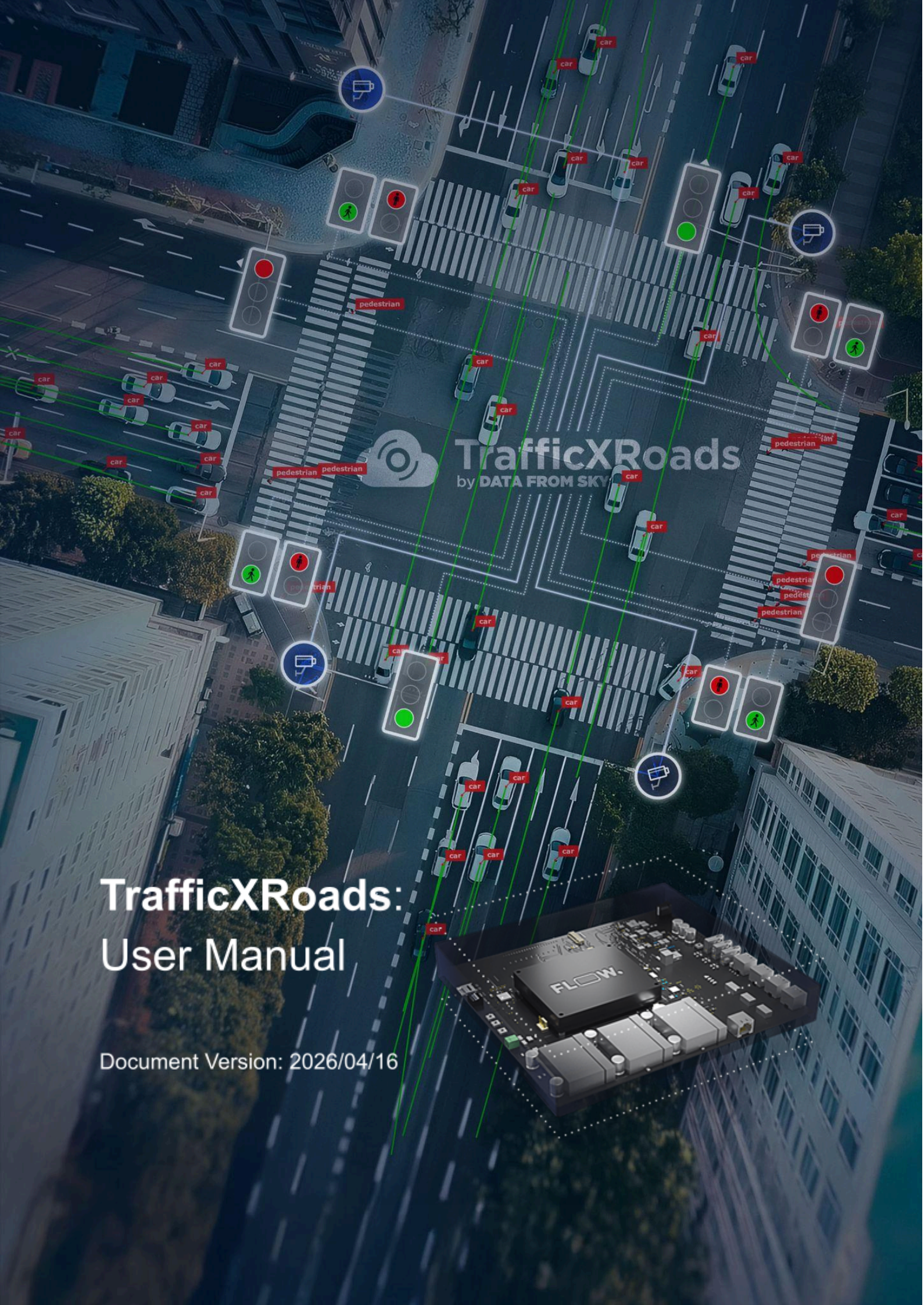


TrafficXRoads: User Manual

Document Version: 2026/04/16

DATA FROM SKY

TrafficXRoads: User Manual

Your guide to getting started with the TrafficXRoads unit.

Thank you for choosing the TrafficXRoads solution and becoming part of the DataFromSky family, pioneers in next-generation traffic analytic intelligence. You have acquired the most advanced and versatile traffic AI system, ready to unlock limitless possibilities with your ingenuity.

We look forward to supporting your journey toward creating smoother, safer, and smarter traffic solutions. Let the traffic FLOW!

On behalf of the DataFromSky team

David Herman, CEO

DATA FROM SKY

Table of Contents

Introduction

The **TrafficXRoads** product line is a range of advanced video analytics embedded computers designed for modern traffic management. These systems excel in real-time detection tasks, enabling dynamic traffic light control and comprehensive data collection from IP cameras. With industrial-grade NVIDIA processors and AI-based detection algorithms, TrafficXRoads devices transform video streams into high-quality trajectory data, providing actionable insights for various applications.

Applications of TrafficXRoads Devices

TrafficXRoads devices are designed to address a wide range of applications in traffic management, safety, and data-driven decision-making. They are specifically built to integrate with the FLOW AI software, which serves as the core engine for all computational tasks across the use case areas listed below. TrafficXRoads devices, together with the FLOW framework, empower operators with advanced capabilities, including:

- Traffic Monitoring and Data Collection
- Actuated Adaptive Traffic Control
- Automated Incident Detection
- Intersection Safety
- Parking Management
- Traffic Violations
- Vulnerable Road Users and Active Mobility
- Emissions
- Security
- Retail

TrafficXRoads can be provided as a standalone hardware device without the FLOW software.

TrafficXRoads Product Line Overview

This section provides technical specifications of TrafficXRoads hardware and analytics capabilities and follows a breakdown by Product Model with dimensions, panel layouts, mounting options, field installation instructions, and other specifics.

Important: Information contained in this section is tied to standard product deployments only. Any non-standard deployments may result in variations in the below specifications, instructions or other product details.

General Overview

The TrafficXRoads product line currently comprises these available models. These may change over time:

- **TrafficXRoads 30N**
- **TrafficXRoads OV008**
- **TrafficXRoads I132 (replacing I131)**

Each model offers unique specifications tailored to specific needs, such as processing power, camera capacity, and power configurations, ensuring scalability and compatibility with diverse operational requirements.

Important: Not all listed hardware capabilities, configurations, or interfaces are necessarily supported by FLOW.

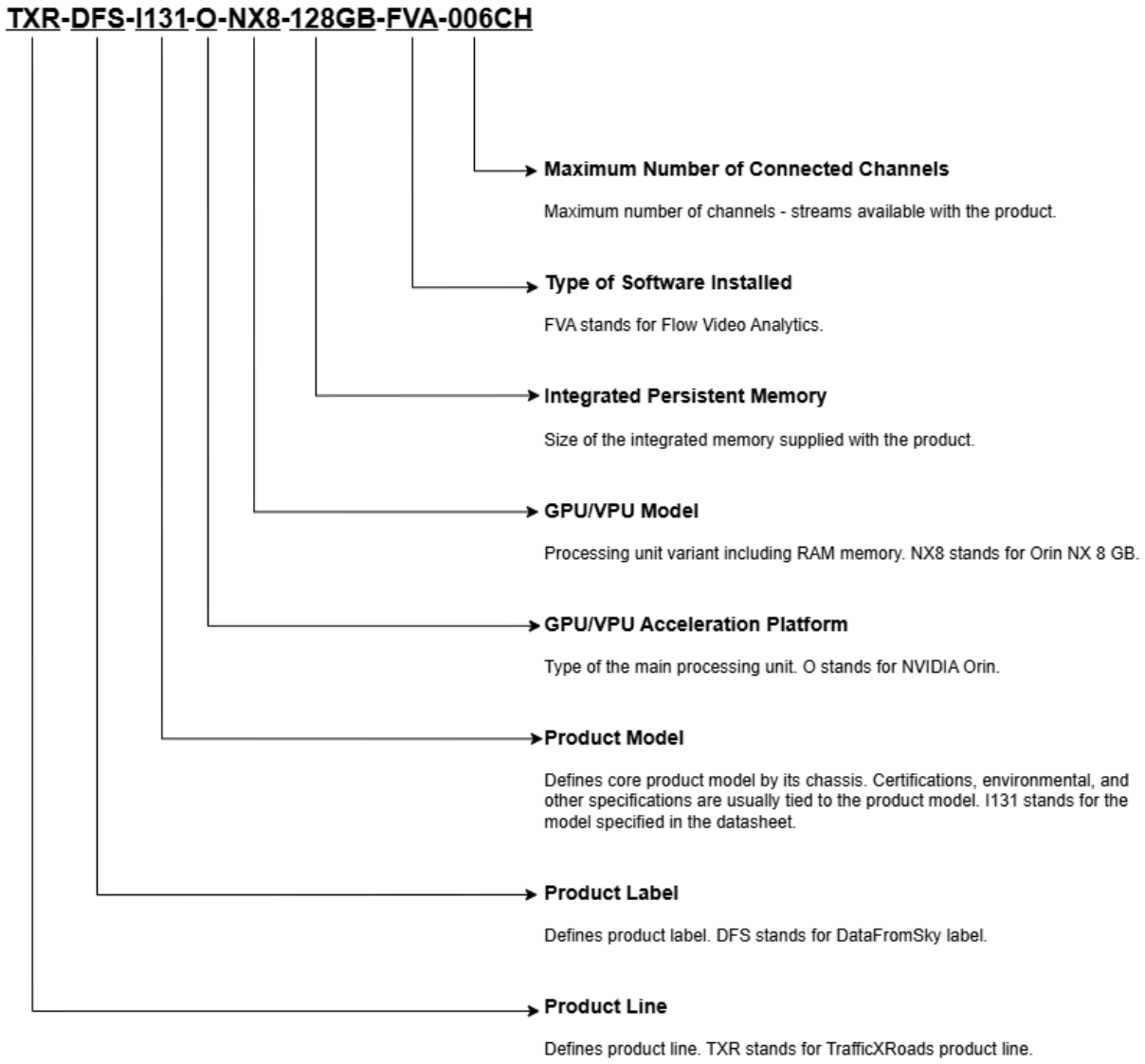
Hardware Overview

The tables below highlight the key differences between models to help you select the best device for your needs.

TrafficXRoads Model	TrafficXRoads 30N	TrafficXRoads OV008	TrafficXRoads I132
Processor	NVIDIA Orin NX	NVIDIA Orin AGX	NVIDIA Orin NX
Memory *(*RAM and storage may differ per model)*	8 GB 128-bit LPDDR5x; 128 GB nVME SSD storage*	32 GB 256-bit LPDDR5x; 64 GB eMMC*	8 GB 128-bit LPDDR5x; 128 GB NVMe SSD storage*
Network Ports	2x 1GbE	1x 10GbE; 1x 1GbE; 8x PoE (10/100 MbE)	2x 1GbE PoE
Power Range	9–36V DC, 50W recommended	9–55V DC, 100W recommended	12V DC, 50 W recommended

Product Coding

The following breakdown describes the product coding approach in detail.

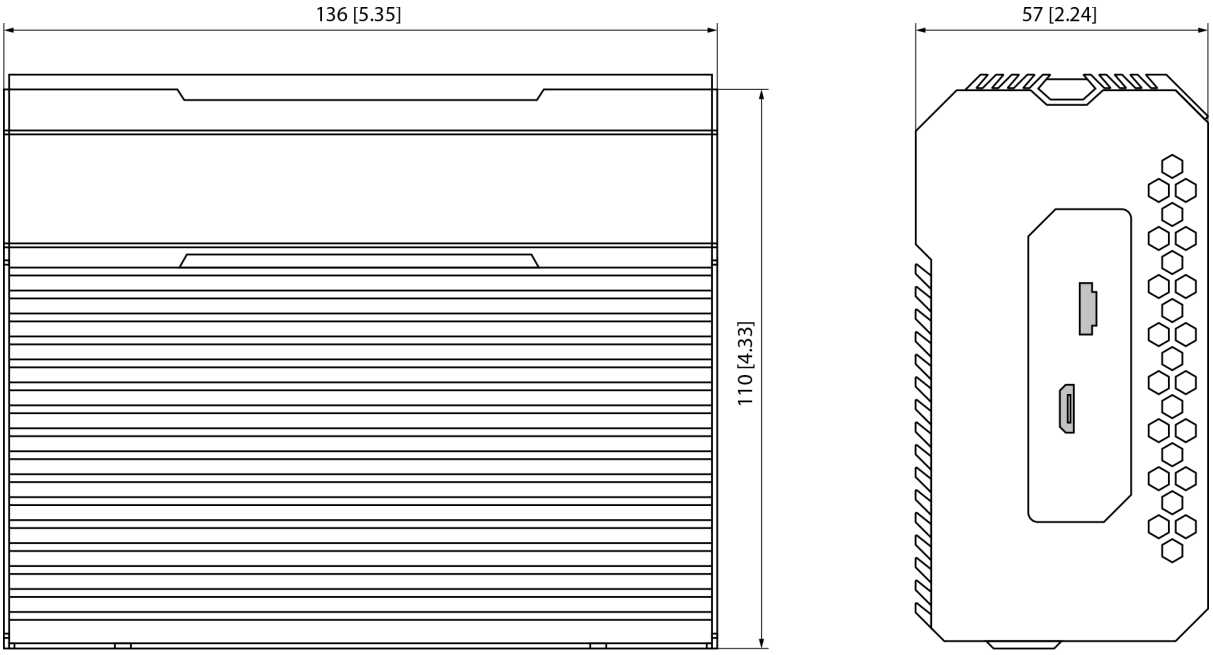

TXR-DFS-I131-O-NX8-128GB-FVA-006CH
Maximum Number of Connected Channels
Maximum number of channels - streams available with the product.
Type of Software Installed
FVA stands for Flow Video Analytics.
Integrated Persistent Memory
Size of the integrated memory supplied with the product.
GPU/VPU Model
Processing unit variant including RAM memory. NX8 stands for Orin NX 8 GB.
GPU/VPU Acceleration Platform
Type of the main processing unit. O stands for NVIDIA Orin.
Product Model
Defines core product model by its chassis. Certifications, environmental, and other specifications are usually tied to the product model. I131 stands for the model specified in the datasheet.
Product Label
Defines product label. DFS stands for DataFromSky label.
Product Line
Defines product line. TXR stands for TrafficXRoads product line.

TrafficXRoads 30N Model

The TrafficXRoads 30N is a compact and lightweight unit designed for straightforward installations. Powered by the NVIDIA Orin NX processor, it features two Ethernet ports (non-PoE) and is ideal for simple setups or space-constrained environments. Active cooling is recommended for optimal performance.

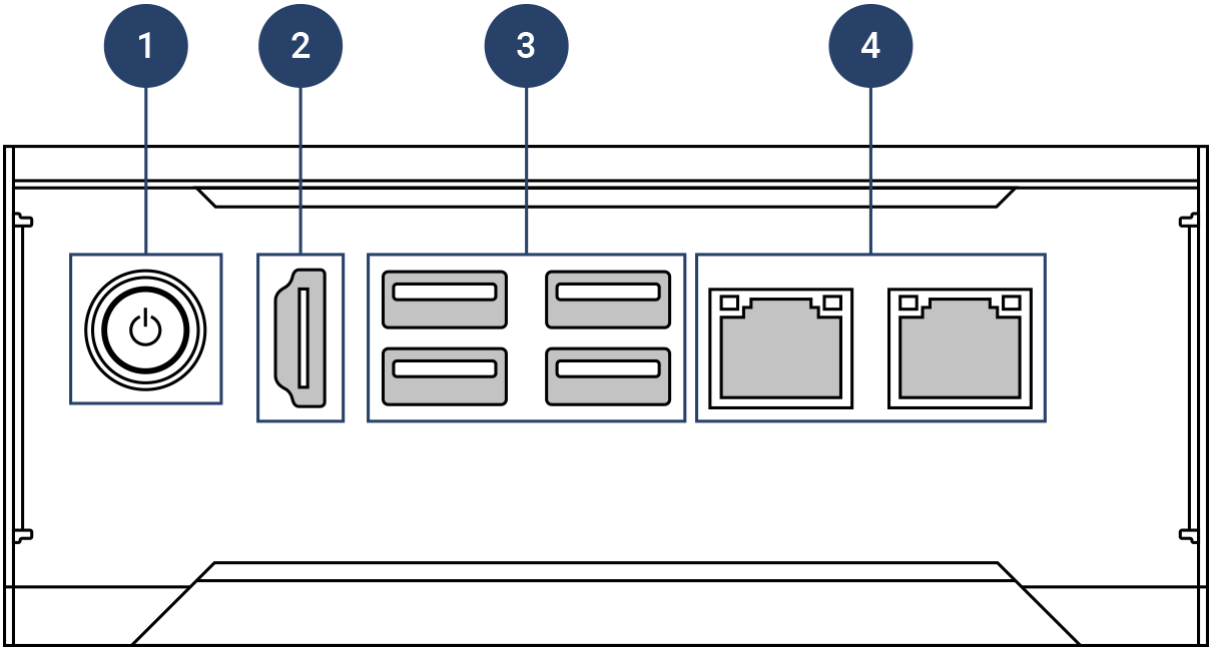
Dimensions

The diagram below shows the device dimensions in millimeters [inches].



Front Panel

The front panel description is below.

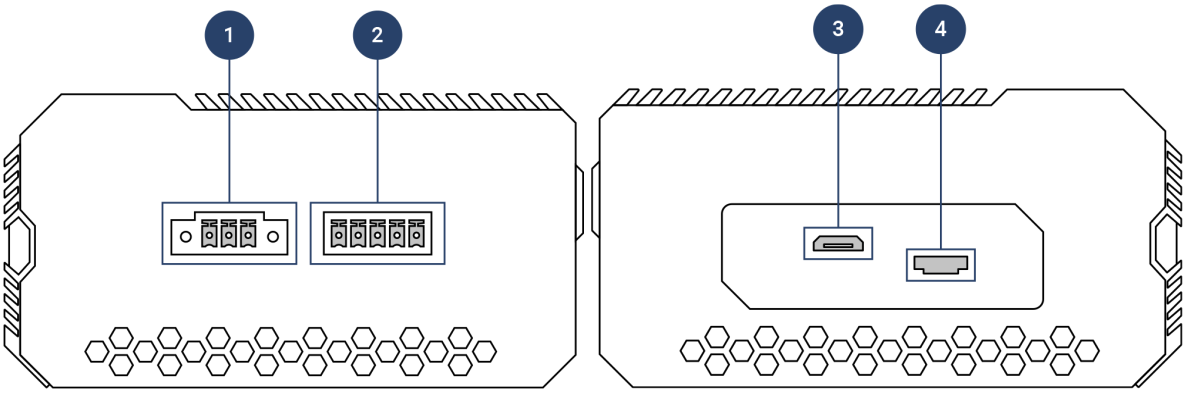


No.	Name	Description
1	Power Button	On/Off

2	HDMI Port	HDMI display output.
3	USB 3.1	4x USB 3.1 Type A port.
4	LAN/WAN	2x 1 Gigabit Ethernet RJ45 port.

Side Panels

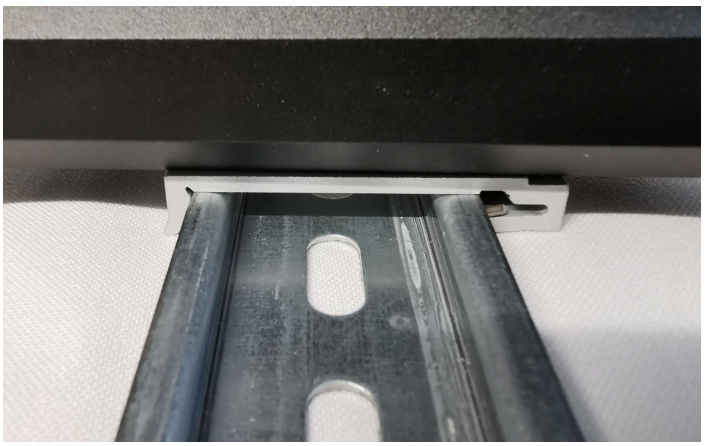
The side panels description is below.



No.	Name	Description
1	DC Power Input	Connecting to the power source.
2	CAN-FD / RS-485	5-pin port for RS-485 and CAN bus communication.
3	Micro USB	Micro USB port.
4	SIM Card Slot	Insert a SIM card into the card slot.

Mounting

- This model can be mounted via DIN rails.



Field Installation

Power source

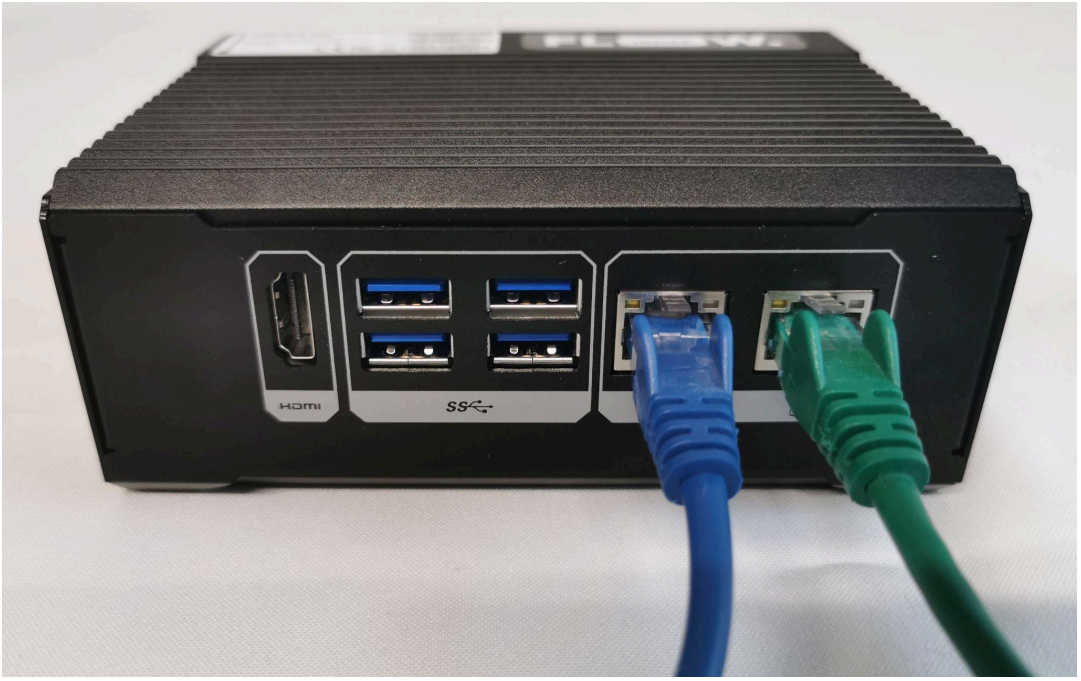
The device is powered by a 9–36V DC power source with a minimum power requirement of 25W (50W recommended).

Wiring

- Red wire: Positive DC pole (+)
- Black wire: Negative DC pole (-)

Connection

1. Connect port 2 (green cable) to your camera network.
2. Connect your computer to port 1 (blue cable), which is used as a service port by default. A detailed description follows in the section TrafficXRoads Initial Setup.



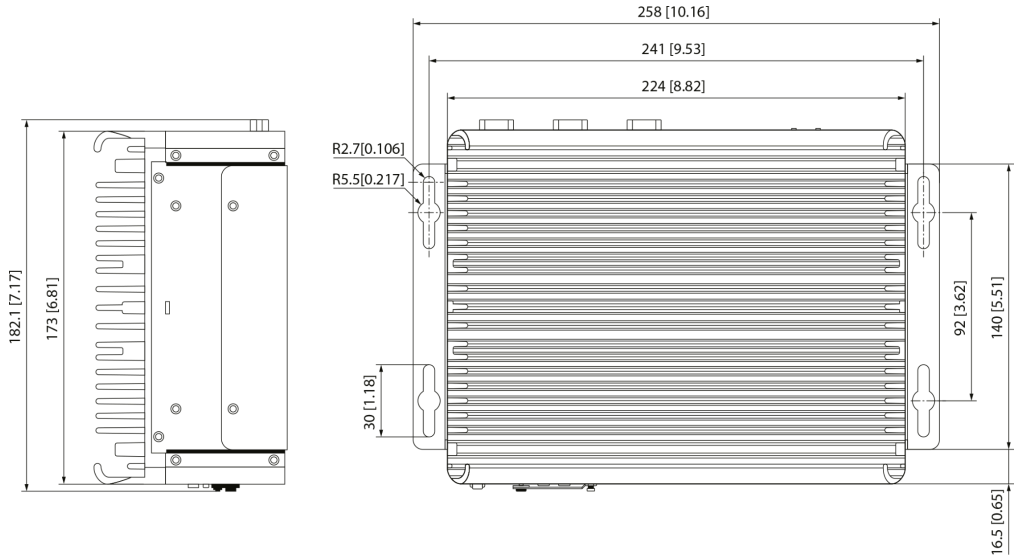
For setups involving multiple IP cameras, it is recommended to use an external PoE switch to ensure stable performance and adequate power distribution.

TrafficXRoads OV008 Model

The TrafficXRoads OV008, powered by the NVIDIA Orin AGX 32 GB processor, is designed for demanding applications. It offers up to eight PoE ports, making it ideal for larger camera networks and handling more video streams (up to 14, depending on the license/configuration).

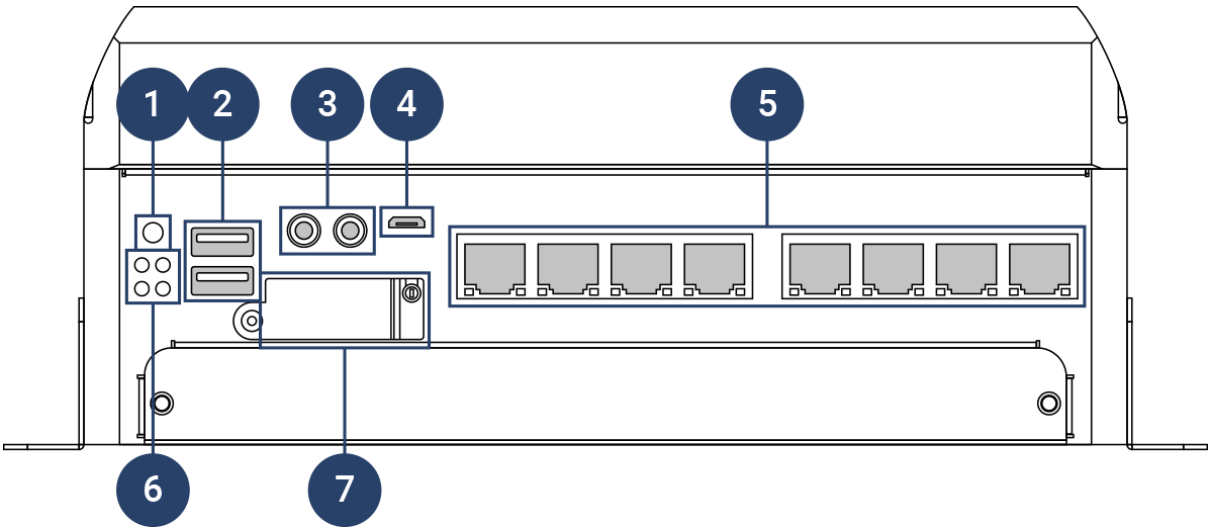
Dimensions

The diagram below shows the device dimensions in millimeters [inches].



Front panel

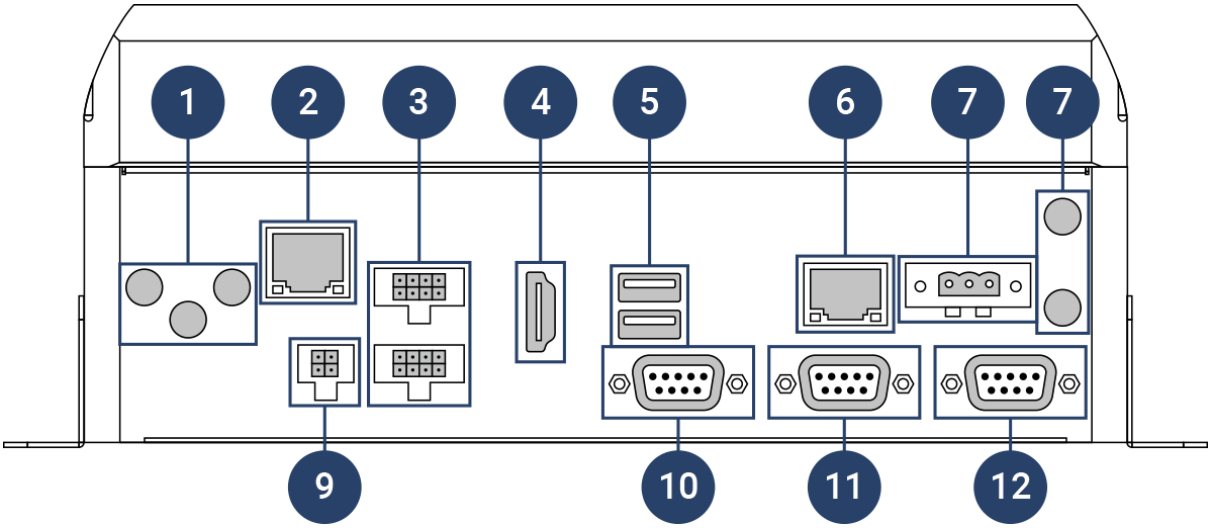
The front panel description is below.



No.	Name	Description
1	Power Button	On/Off.
2	USB 2.0	2x USB 2.0 Type A Port.
3	Audio	Line in and out.
4	OTG USB	Micro USB port.
5	PoE Ports	PoE ports (10/100 MbE) for connecting to the camera network.
6	LED Indicator	
7	SIM/SD Cover	Cover for SIM card and SD card slots.

Rear panel

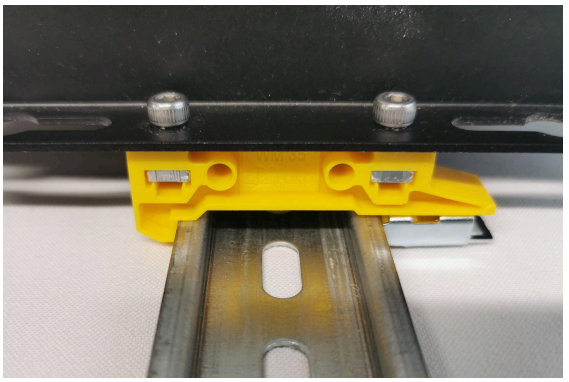
The rear panel description is below.

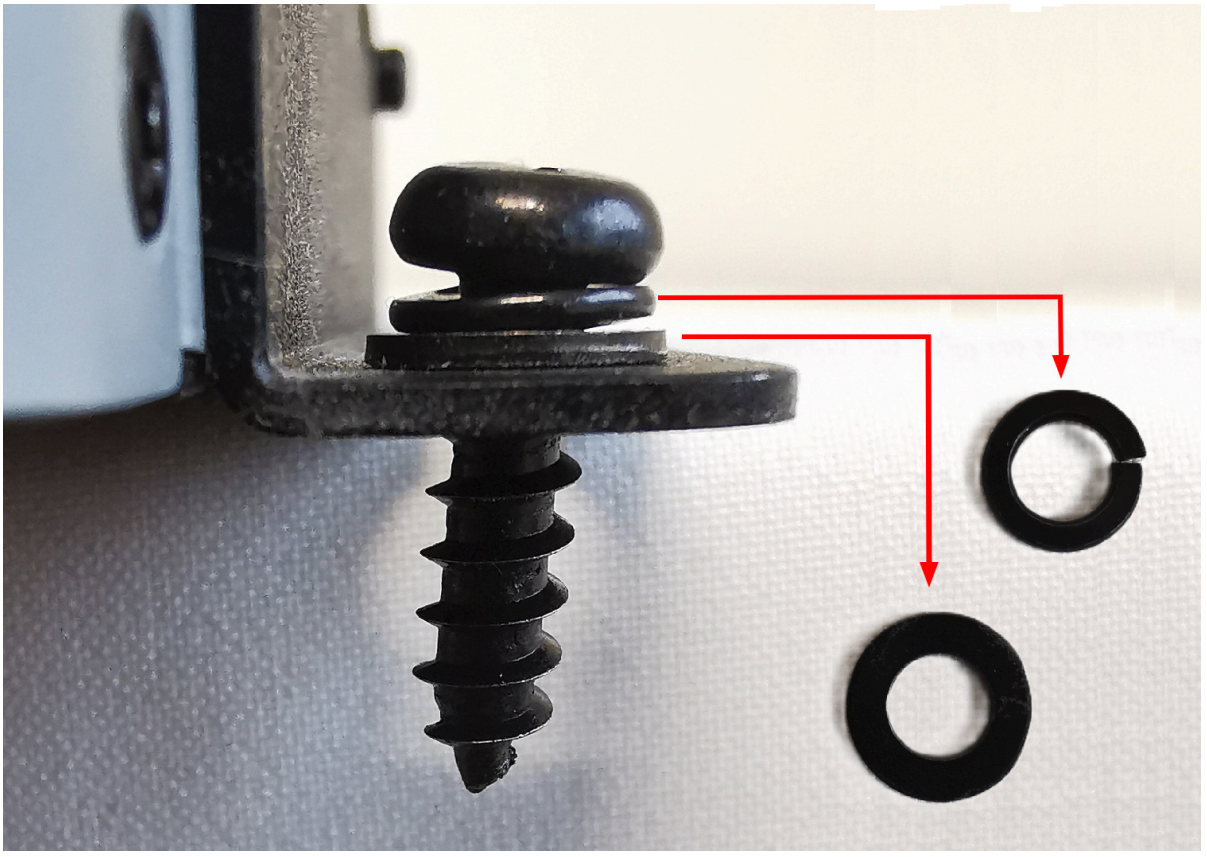


No.	Name	Description
1	Antenna Interfaces	Connects the antenna to the AI mobile NVR for 3G / 4G / WiFi / GPS functions.
2	LAN/WAN	1 Gigabit Ethernet RJ45 port.
3	Alarm IO	Provides 8 alarm inputs and 8 alarm outputs.
4	HDMI Port	HDMI display output.
5	USB3.0	USB 3.0 Type-A port.
6	LAN/WAN	10 Gigabit Ethernet RJ45 port.
7	DC Power Input	Connecting to the power source
8	Antenna Interfaces	Connects the antenna to the AI mobile NVR for 3G / 4G / WiFi / GPS functions.
9	RS-485 Port	COM port for RS-485.
10	CAN Port	COM port for CAN bus.
11	RS-232 Port	COM port for RS-232.
12	RS-232 Port	COM port for RS-232.

Mounting

- This device may be mounted using DIN rails.
- The device may also be mounted using L-bar screws.





Field Installation

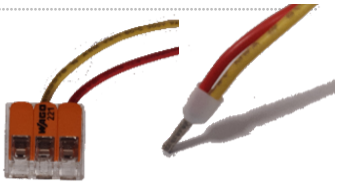
Power source

The device requires a 9–55V DC power source. The minimum power is 65W for the device, with PoE x 8 (10/100 MbE, Single 30W/Total 120W). A 100W power source is recommended (always consider the power requirements of the cameras connected).

Wiring

- Red wire: Positive DC pole (+)
- Black wire: Negative DC pole (-)
- Yellow wire: Turn-on/off wire (connect to Red wire using a WAGO clamp or double bootlace ferrule).

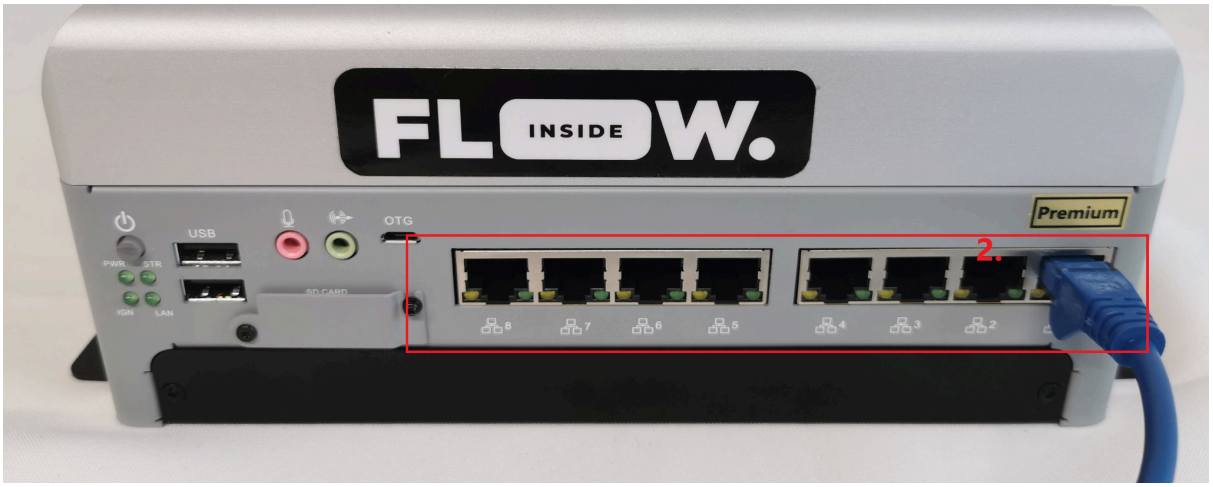
Yellow cable must be connected with the red cable. Use a WAGO clamp or double bootlace ferrule to connect them.



Connection

1. Connect your computer to the LAN 2 port (green cable), which is used as a service port by default. A detailed description follows in the section TrafficXRoads Initial Setup.

2. Connect cameras/camera network to PoE LAN ports (blue cable).

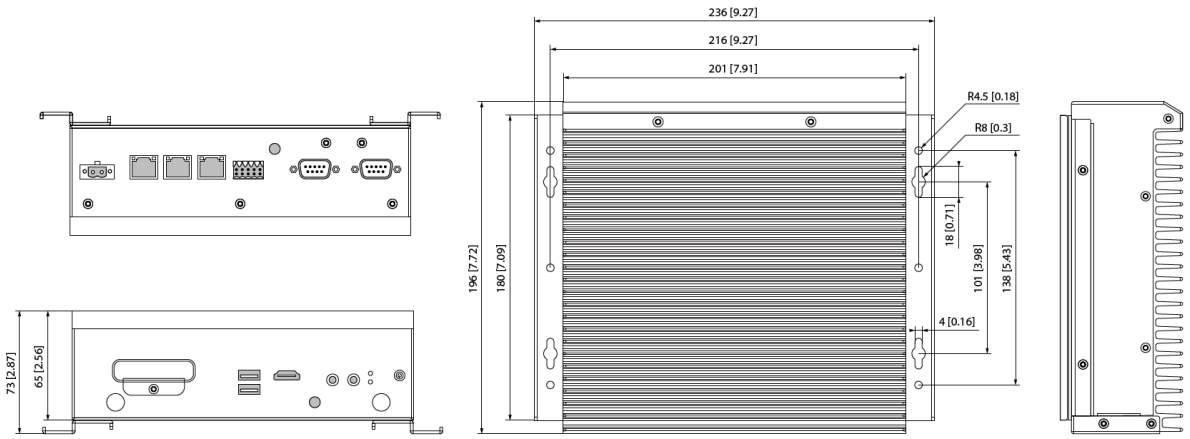


TrafficXRoads I-132 Model

The TrafficXRoads I-132 is equipped with the NVIDIA Orin NX processor to deliver stable and reliable performance. With dual Gigabit Ethernet PoE ports, surge protection, and the widest operating temperature range among the available models, it is built for demanding environments.

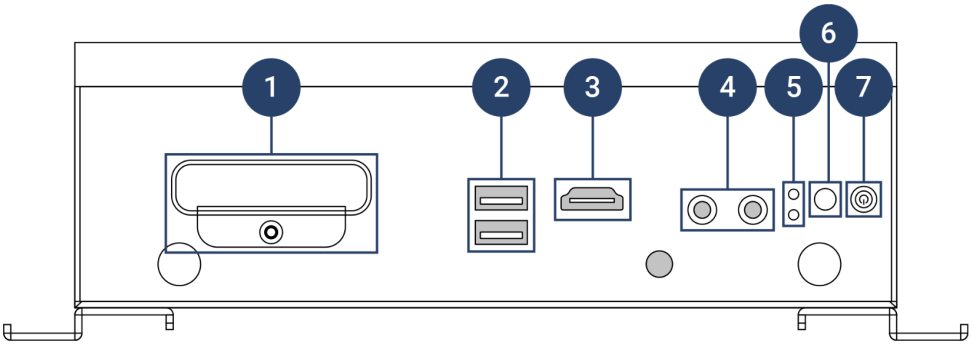
Dimensions

The diagram below shows the device dimensions in millimeters [inches].



Front panel

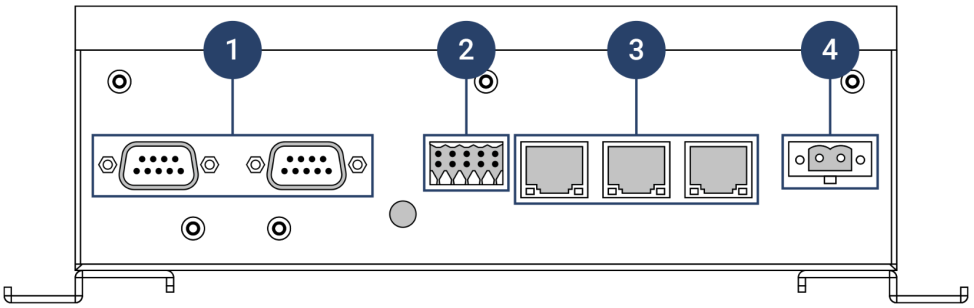
The front panel description is below. **Interfaces (1) - (4) are not used.**



No.	Name	Description
1	SIM Cover (Not used.)	Cover for 2x Nano SIM cards.
2	USB 2.0 (Not used.)	2x USB 2.0 Type-A Port.
3	HDMI Port (Not used.)	HDMI display output.
4	Audio (Not used.)	Line in, Line out.
5	LED Indicators	Upper – HDD status, lower – Power status.
6	Reset	Reset hole.
5	ON/OFF	Power button.

Rear panel

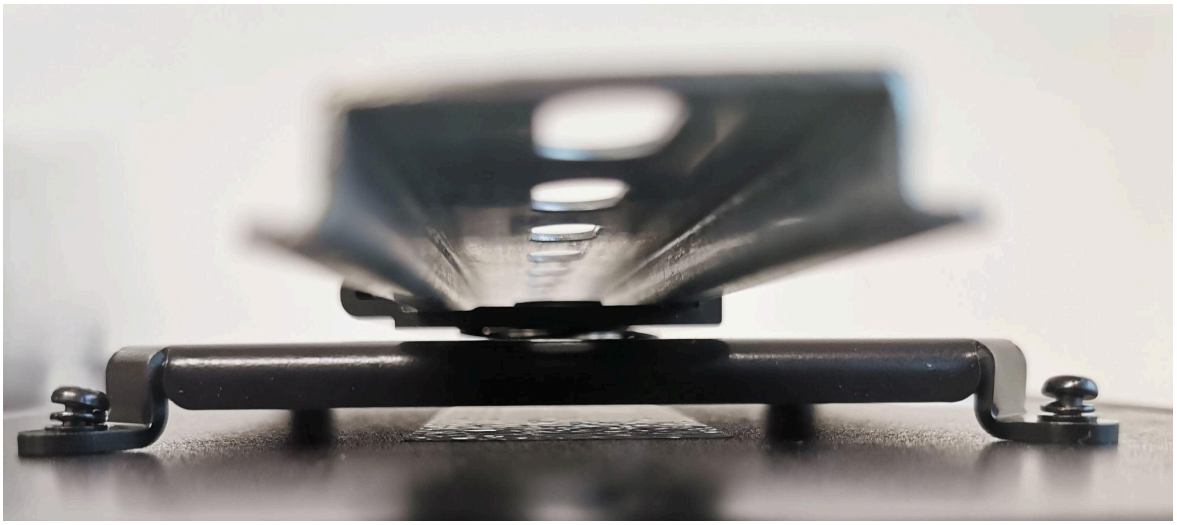
The rear panel description is below.



No.	Name	Description
1	COM Ports	2x COM port.
2	DI/DO (Not Used)	2x5-pin Terminal Block 4x DI (support PNP/NPN/dry contact) 2x DO (support dry/sink contact)
3	LAN & POE	From the left: LAN port, POE1 and POE2 camera network ports.
5	DC Power Input	Connecting to the power source.

Mounting

- This model may be mounted via DIN rails.
- The device may also be mounted using L-bar screws.



Field Installation

Power source

A provided 12V DC power source powers the device.

Wiring

- White wire: Positive DC pole (+)
- Black wire: Negative DC pole (-)

Connection

1. Connect your computer to the LAN port (green cable), which is used as a service port by default. A detailed description follows in the section TrafficXRoads Initial Setup.
2. Connect the POE+1 port (blue cable) to your camera network.

For setups involving multiple IP cameras, it is recommended to use an external PoE switch to ensure stable performance and adequate power distribution.

TrafficXRoads Initial Setup

TrafficXRoads is designed for professional use and must only be operated by qualified personnel. Qualified personnel are individuals who have completed training directly with the manufacturer, an authorized distributor, or an authorized reseller of this product.

TrafficXRoads product deployments with special editions of FLOW video analytics software may result in variations in setting up and usage of the device.

Pre-installation Requirements

Before installation, ensure the following checks are performed:

1. **Compliance Verification**: Verify that the product complies with all applicable local, provincial, federal, and municipal laws, regulations, standards, and codes relevant to the application or installation site.
2. **Permits and Approvals**: The buyer is responsible for obtaining all necessary permits, licenses, exemptions, consents, and approvals required for the import, integration, installation, and operation of the product.
3. **Site Assessment**: Confirm that the installation site is prepared and meets all necessary requirements for safe and efficient operation.

By adhering to these guidelines, you can ensure the safe and compliant installation of the TrafficXRoads system.

IP Address Assignment

This section explains the methodology used for assigning IP addresses to TrafficXRoads devices. These are equipped with multiple Ethernet ports, each having its own MAC address. This design enables independent IP assignment for each port, allowing flexibility for specific network configurations and redundancy.

Below is the IP assignment approach for each product model. Manual configurations are possible using the System Web Interface described in the next section.

TrafficXRoads 30N Model

The 30N model features these ports:

- **PoE port 1 (eth0):** DHCP enabled only.
- **PoE port 2 (eth1):** Default static IP `192.168.50.10`, DHCP enabled.

  Note: We recommend keeping the default IP or at least one static IP for recovery.

TrafficXRoads OV008 Model

The OV008 model features these ports:

- **10 Gb Ethernet (eth1):** DHCP enabled.
- **9-Port Switch:**
  - 1 Gb Ethernet **(eth0)**: Default static IP `192.168.50.10`, DHCP enabled.
  - 8 PoE ports (100 Mbps): For connecting peripheral devices.

  Note: We recommend keeping the default IP or at least one static IP for recovery.

TrafficXRoads I132 Model

The I132 model features these ports:

- **LAN port:** Default static IP `192.168.50.10`, DHCP enabled.
- **POE+1 and POE+2 ports:** internally bridged (switch mode), operating as a single interface; IP address obtained via DHCP.
- **Note:** We recommend keeping the default IP or at least one static IP for recovery.

Common Setup Instructions

To set up your TrafficXRoads device, follow the steps outlined below. These instructions will help you connect to your device through available interfaces.

1. Connect the power source. The device should start automatically.
    - Depending on your order, some products are delivered without the power source included.
    - Some devices contain a Power LED indicator, which indicates the status.
2. Find the Device's IP Address:
    - Default IP: `192.168.50.10`
    - If a DHCP server is used, find the IP via the device's MAC address (on the top side of the device).
3. Access the Web-Admin Console:
    - Open: `https://deviceIP:8000` (e.g.,`https://192.168.50.10:8000`).
    - Default Login:
        - Username: `admin`
        - 1.18 - dokumentace -Password: `admin01`
4. Configure the Device:
    - Launch **FLOW Insights** and click **Quick Connect to FLOW Device**.
    - Connect via the device's IP address:
    - Default Login:
        - Username: `admin`
        - Password: `admin`
    - Add cameras, interfaces, and configure analytics.

Additional Notes

- Ensure the power supply meets the recommended specifications for stable performance.
- Change default passwords during initial setup to enhance security.

System Web Interface and Network Settings

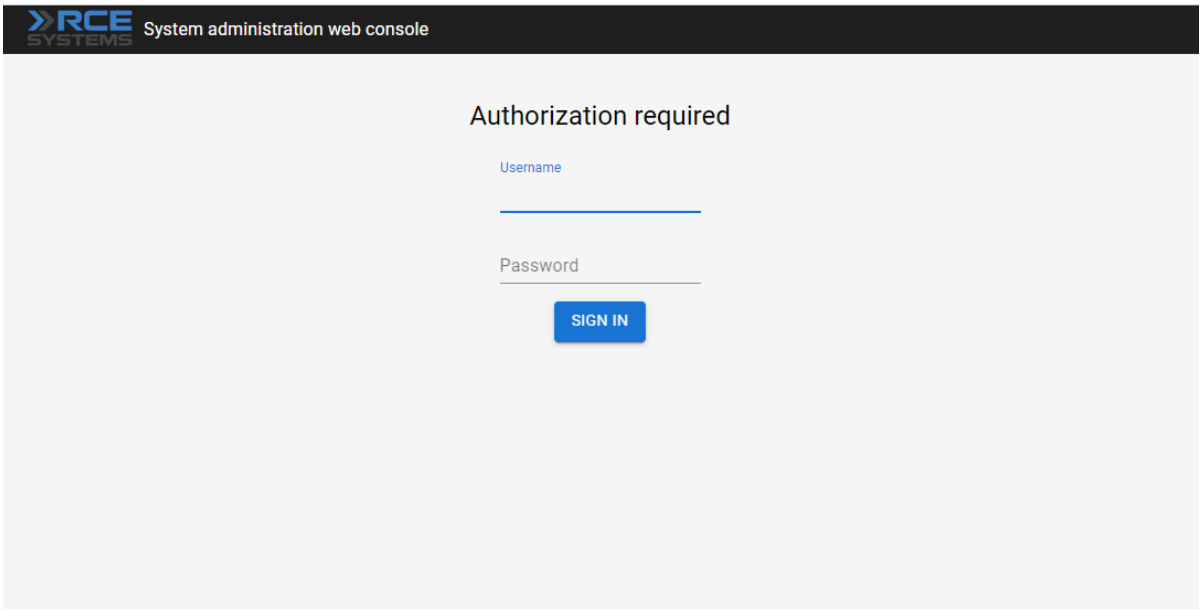
The TrafficXRoads unit is adaptable to various deployment scenarios and network setups. This section provides an overview of how to configure and manage the system via the web interface.

Accessing the Web Administration Interface

The web administration interface allows you to configure network settings, manage VPNs, and perform system maintenance tasks such as rebooting or resetting the unit to factory settings.

To access the interface, your computer must be on the same network. Configure an appropriate IP address and subnet mask for your computer, such as `192.168.50.2/24` (subnet mask: `255.255.255.0`).

- **Default IP Address**: `192.168.50.10`
- **Access URL**: `https://192.168.50.10:8000`
- **Default Login Credentials**:
  - **Username**: `admin`
  - **Password**: `admin01`

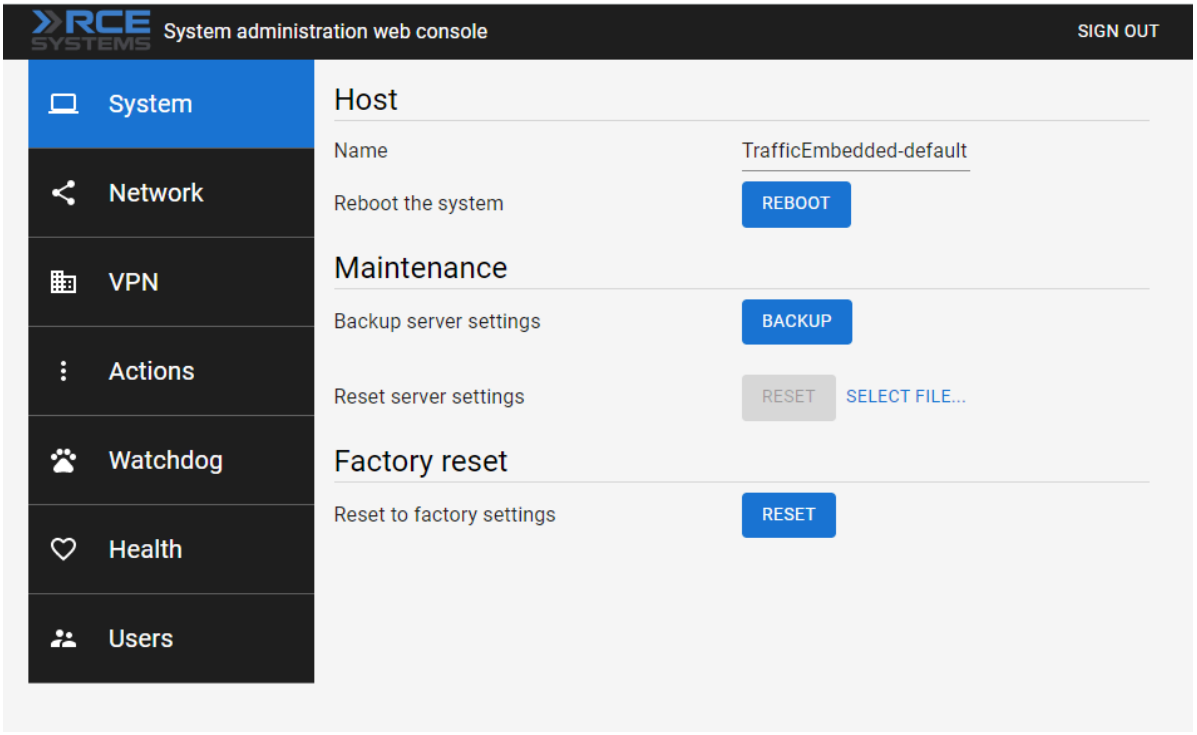


All advanced configurations for the video analytics system are handled via the **FLOW Insights** desktop application. To connect to the system through FLOW Insights, you will need the server's IP address.

System Settings

Upon logging into the web console, the **System** tab appears as the default view. This tab allows you to:

- Change the unit's name.
- Reboot the system.
- Backup or restore the console's settings.
- Perform a factory reset to restore default settings, including IP addresses, names, and passwords.



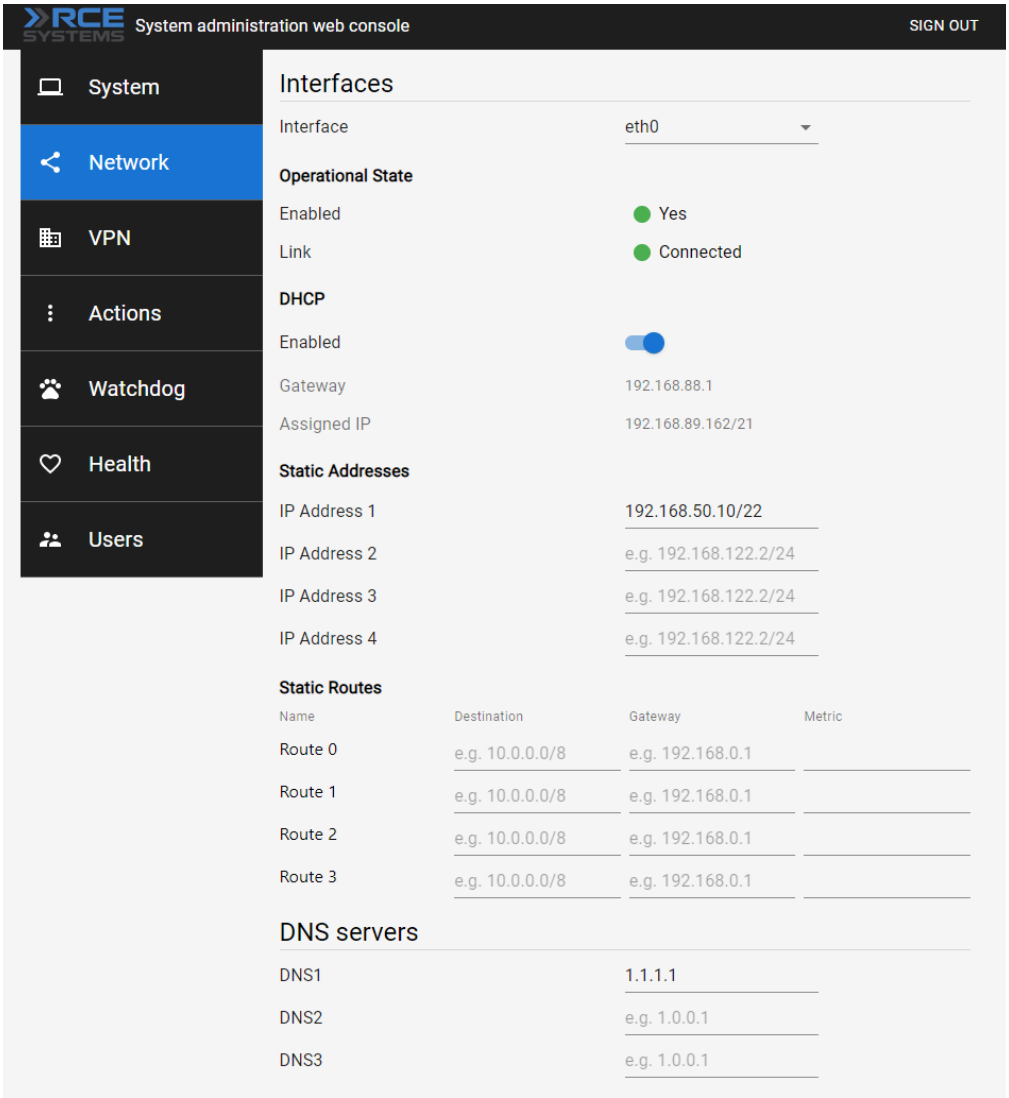
Network Settings

Network configurations are managed in the **Network** tab. This tab includes information about the current state of the interface and configuration options for connectivity.

Configuration options include:

- Enabling/disabling DHCP.
- Setting up static IP addresses (up to 4).
- Static routes (up to 4).
- DNS servers (up to 3).

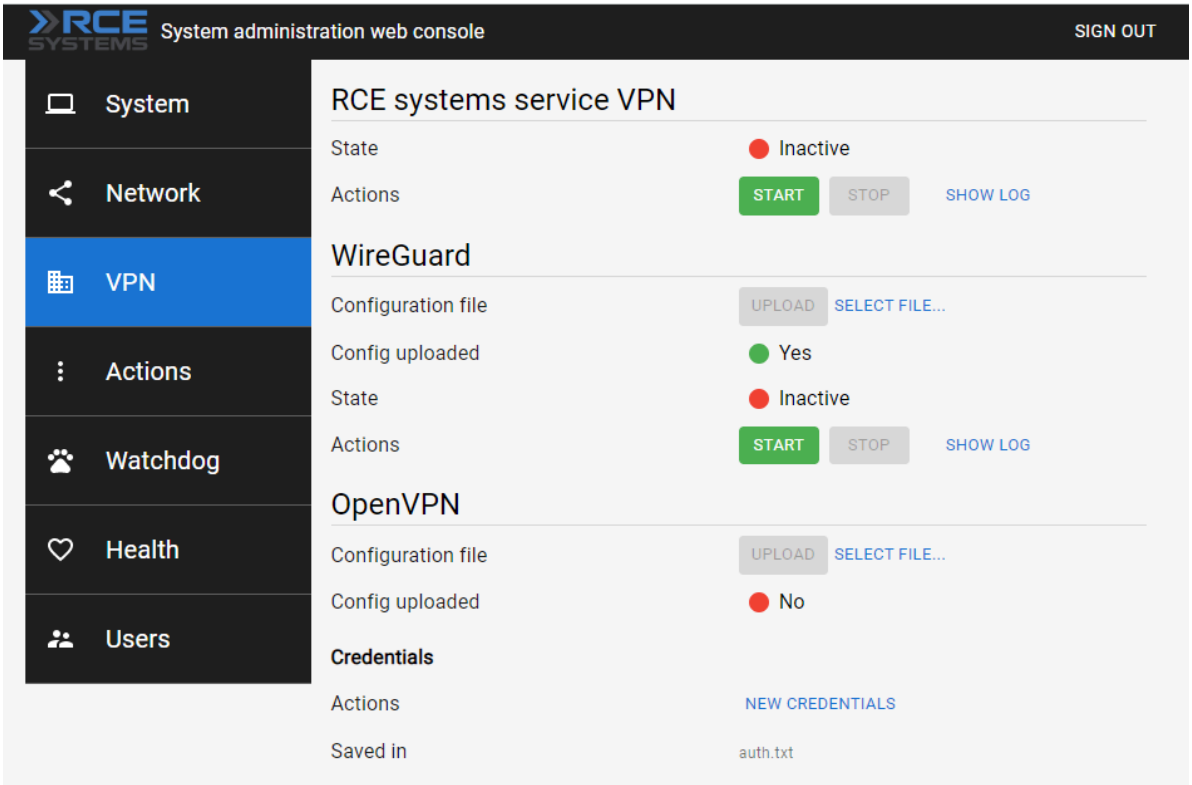
Recommendation: Use static IP addresses for deployments.



Virtual Private Networks (VPNs)

The unit supports multiple VPN configurations for secure connectivity.

1. **System Service VPN**:
   - Preconfigured for remote manufacturer access.
   - Requires an active internet connection, allowed outgoing connection to IP `172.105.65.31` and UDP port `31228` enabled.
   - Can be deactivated if necessary.
2. **User-Configurable VPNs**:
   - Supports **WireGuard** and **OpenVPN**.
   - Configured by uploading a text configuration file tailored to the specific VPN requirements.


RCE SYSTEMS
System administration web console
SIGN OUT
System
Network
VPN
Actions
Watchdog
Health
Users
RCE systems service VPN
State
Inactive
Actions
START
STOP
SHOW LOG
WireGuard
Configuration file
UPLOAD
SELECT FILE...
Config uploaded
Yes
State
Inactive
Actions
START
STOP
SHOW LOG
OpenVPN
Configuration file
UPLOAD
SELECT FILE...
Config uploaded
No
Credentials
Actions
NEW CREDENTIALS
Saved in
auth.txt

FLOW Framework

FLOW framework is an AI-powered video analytics engine running on the TrafficXRoads unit. To configure traffic tasks, you need the **FLOW Insights** application, available for download here: https://datafromsky.com/flow-versions/. Ensure the version matches the **FLOW** version installed on your TrafficXRoads unit.

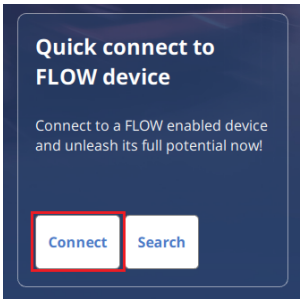
For the latest **FLOW Insights** version, download **FLOW Demokit** here: http://www.datafromsky.com/download/flow/demokit/FLOW_Demokit.exe

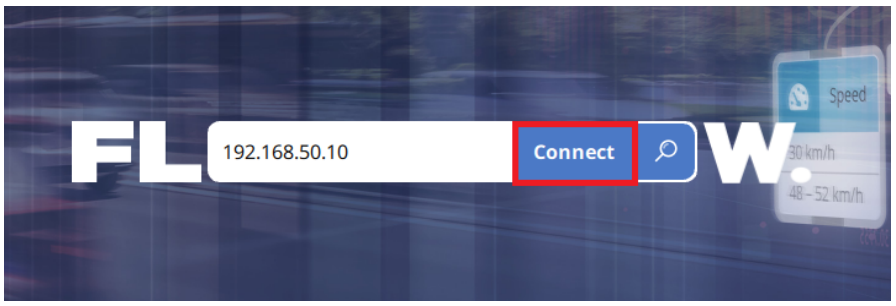
Connecting to the Unit with FLOW Insights

1. Download and Install FLOW Insights:
   Compatible with 64-bit Windows or Linux systems (contact support for the Linux version).

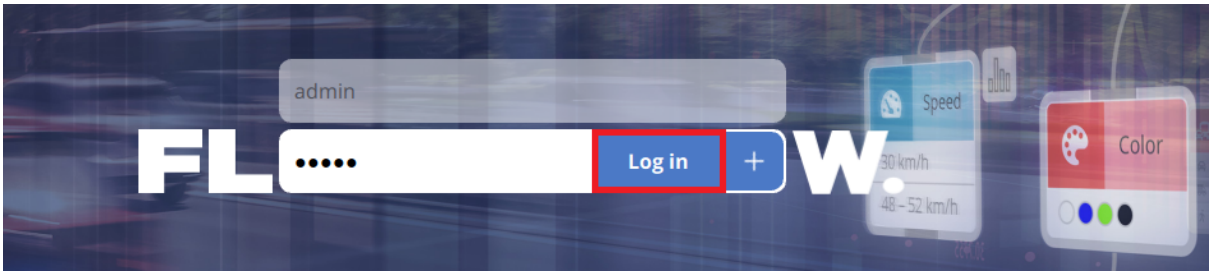
2. Network Configuration:
   Ensure the unit is network-accessible and you know its IP address (see Network Settings).

3. Launch FLOW Insights:
   - Open the app and click **Connect** in the bottom-right tile **Quick connect to FLOW device**.
   - Enter the unit's IP address (e.g., `192.168.50.10`) and click **Connect**.





4. Log In:
   Use the default credentials:
   - **Username**: admin
   - **Password**: admin



Important: You should change the default password in the user settings section after logging in.

Adding Camera Streams and Configuring Analytics

To add a camera stream, follow these steps:

1. Add a Camera Stream:

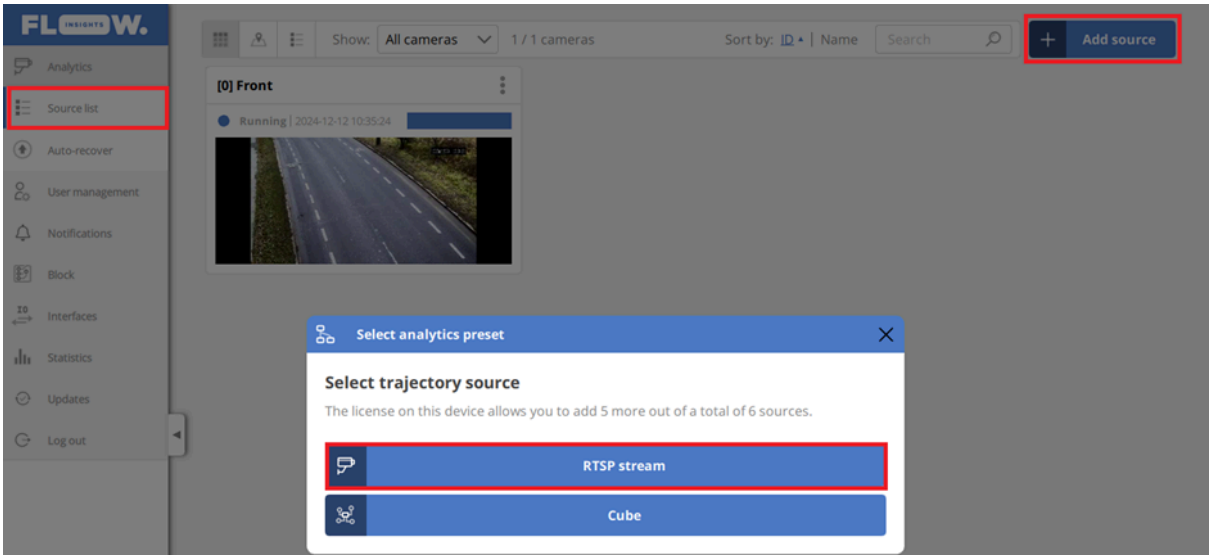
   Enter the RTSP video source stream and optional OnVIF source address in the following formats.

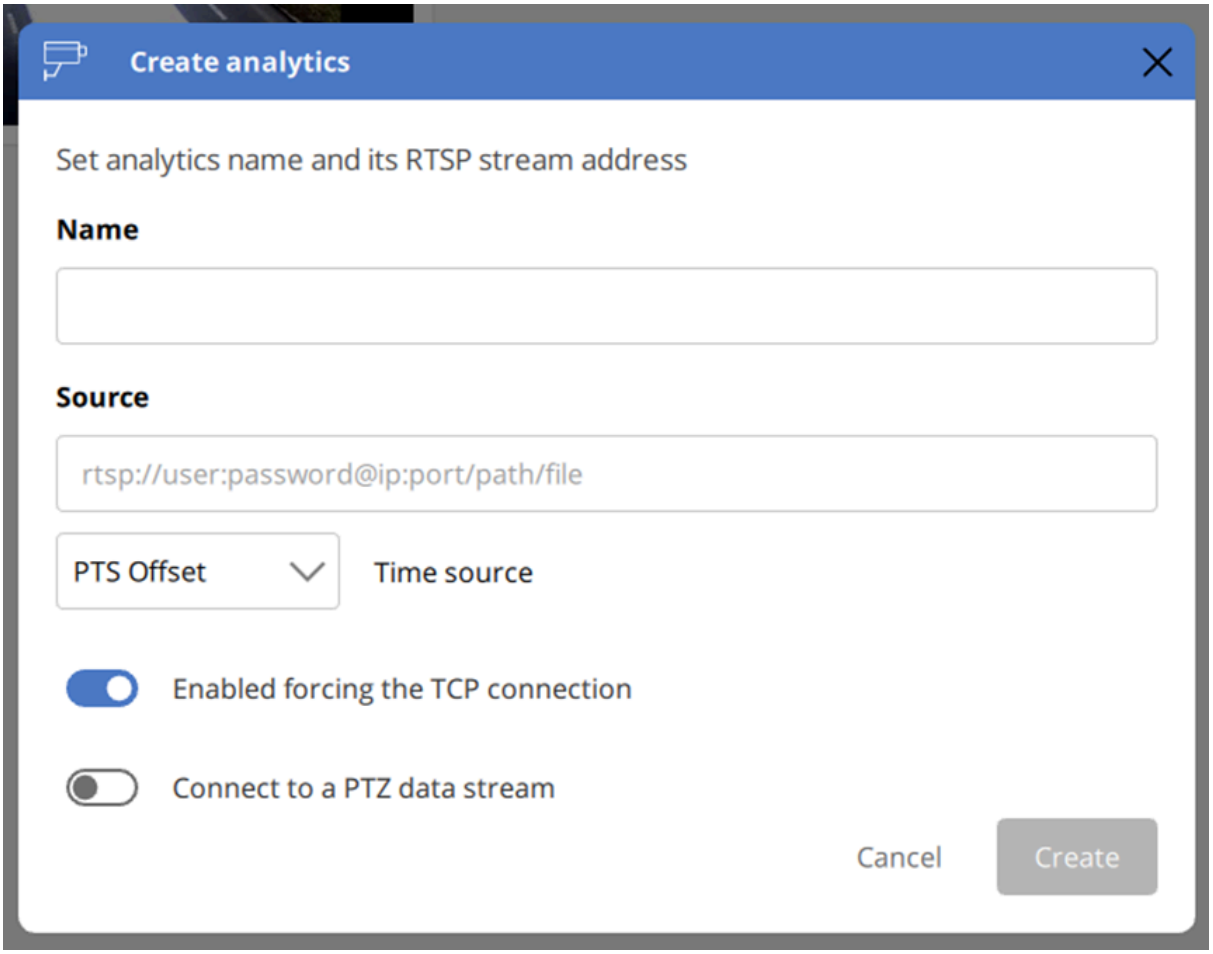
   - **Video source**: `rtsp://user:password@ip:port/path/file`
   - **OnVIF source**: `user:password@ip`
     Refer to the camera's manual or web interface for specific details. Ensure the camera is network-accessible from the unit.

   Manufacturer-Specific Notes:
   Many manufacturers have unique RTSP configurations. The RSTP definition is common for all: `rtsp://user:password@ip:port`, suffix differs as follows - below are common examples:

   - Hikvision: `/Streaming/channels/101`
   - AXIS: `/axis-media/media.amp`
   - Dahua: `/dahua/cam/realmonitor?channel=1`
   - Wisenet(Hanwha): `/profile2/media.smp`
   - DataFromSky Linux OS with Movidius cameras: `/LiveH264_0`
   - Azena OS DataFromSky cameras (including port): `8554/fhd`

   For detailed instructions, consult the respective camera's manual or support documentation.





2. Register the Stream:
   - Click **Create** to add the camera stream. The unit will attempt to connect.
   - If successful, a live preview will appear, and the status will change to **Running**.
   - If unsuccessful, verify the camera's network accessibility and RTSP address.
3. Adding Additional Camera Streams:
   Repeat the process for each camera.

The number of streams is limited by the unit's license.

FLOW Insights

Expected Maximum Number of Supported Streams

The following table provides an illustrative breakdown of the expected maximum number of supported streams based on hardware configurations and type of running analytics. These figures are derived from typical setups and are intended for guidance only, reflecting potential performance under specific analytics loads. Actual device capabilities may differ per use case. The overview below may be incomplete and may include configurations that are not part of the current product offerings.

HW Chipset	RAM Memory	Analytics Complexity	Expected Max Streams
NVIDIA Orin Nano	4 GB	standard analytics	Max 1 stream
NVIDIA Orin Nano	8 GB	standard analytics	Max 3 streams
NVIDIA Orin NX	8 GB	standard analytics or thermal imaging	Max 6 streams
NVIDIA Orin NX	8 GB	360° camera analytics	Max 1 stream
NVIDIA Orin NX	16 GB	standard analytics or thermal imaging	Max 8 streams
NVIDIA Orin AGX	32 GB	standard analytics	Max 14 streams

Processing Capacity and FPS Management

The unit processes a configurable number of frames per second (FPS). If the total FPS exceeds the unit's capacity, some image frames may be dropped. This usually doesn't impact traffic statistics if the evaluation FPS is sufficient for the monitored scene.

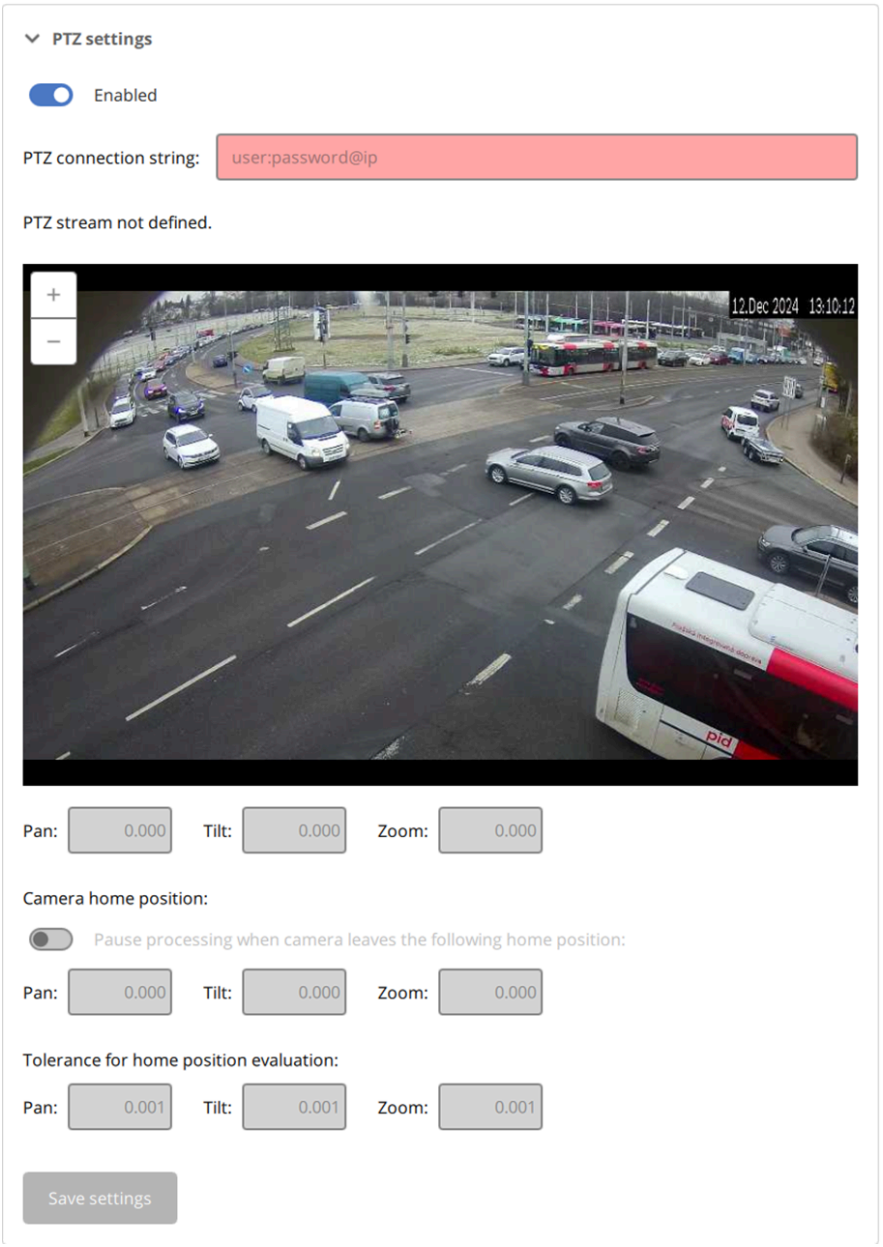
Recommended Minimum Detection FPS

- Pedestrian movements (up to 7 km/h): 5 FPS
- Cyclists (up to 50 km/h): 10 FPS
- City traffic (up to 75 km/h): 15 FPS
- District-level roads (up to 150 km/h): 20 FPS
- Highways (up to 200 km/h): 25 FPS

PTZ Cameras with ONVIF Protocol Support

FLOW supports PTZ cameras using the ONVIF S protocol, enabling scenario-based analytics tied to specific camera positions:

1. Define the **ONVIF address** in the Analytics setup dialog.
2. In **Settings**, set the camera's home position and movement tolerance in the **PTZ settings** section.
3. When the camera is in its defined position, the analytics runs. If it leaves this position, no new trajectories are processed, but the analytical engine remains active.



Note: FLOW acts as a passive receiver of camera position and zoom data, activating analytics based on this information. FLOW is not used to control the camera's movement.

Detection of Traffic Events

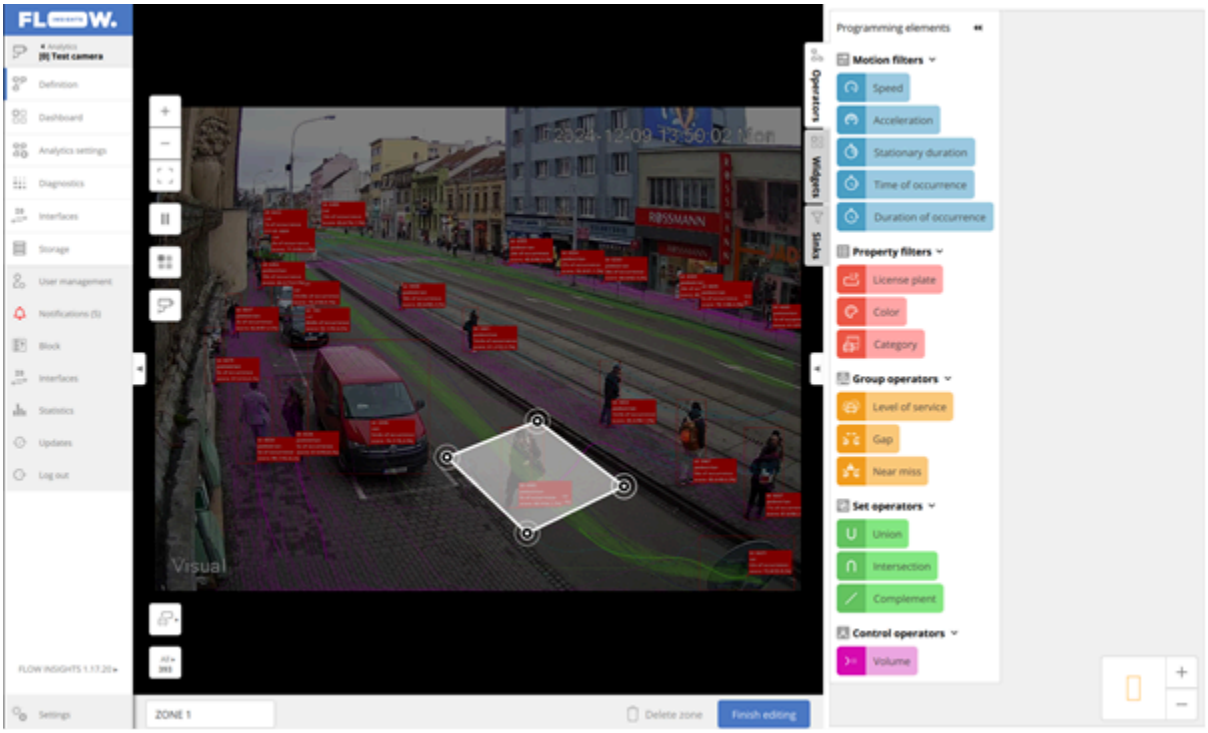
The FLOW framework enables defining complex traffic events, including interactions between objects. A comprehensive guide to the FLOW and tutorials can be found here. This document focuses on selected basic tasks for traffic detection systems. All configurations for detecting traffic events are made in the **Definition** tab.

Basic Object Presence Detection

Real-time detection of object presence is achieved using a Zone spatial filter in the NOW time mode. The Category filter can also be applied to detect specific object types. The system allows an unlimited number of detectors.

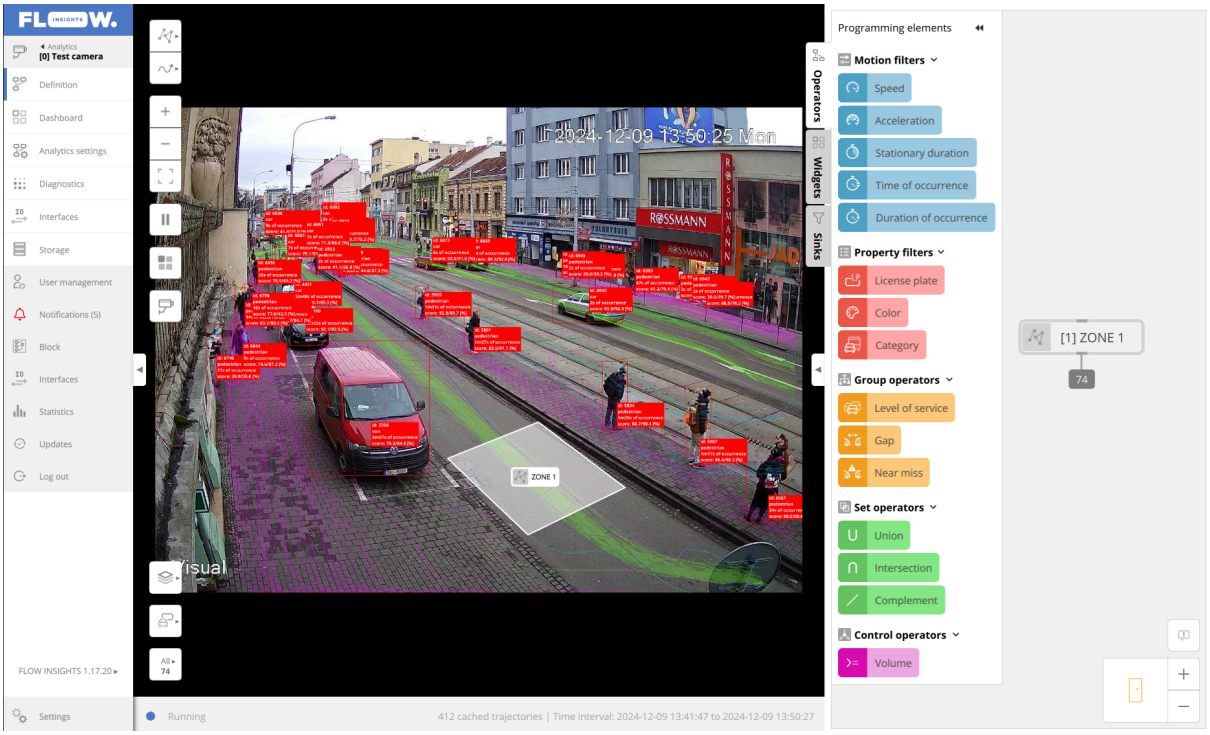
Step 1: Create a Zone or Gate

- Use the **Create zones/gates** tool from the left panel to draw a detection zone in the desired area.
- The system will automatically determine whether the shape is the gate or the zone.



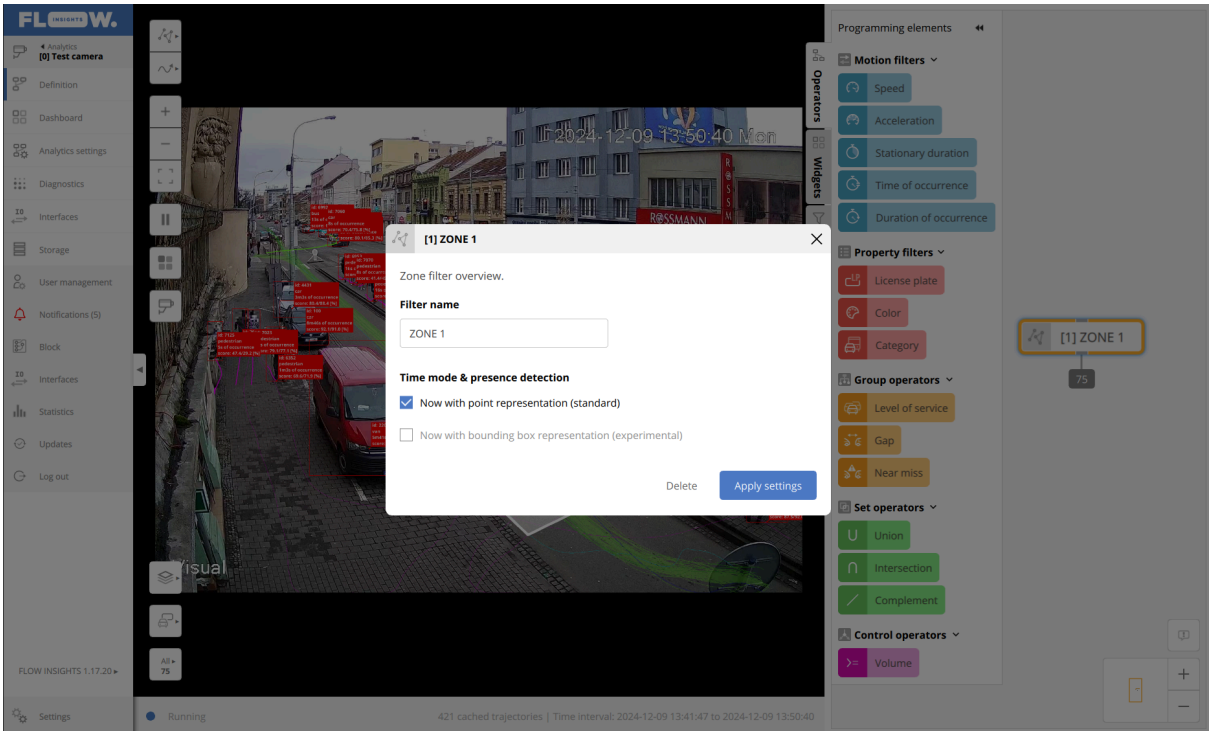
Step 2: Add the Zone to the Workspace

- Drag and drop the zone into the right-side canvas.
- This action instantiates the zone, enabling it to filter trajectories from the FLOW device cache.



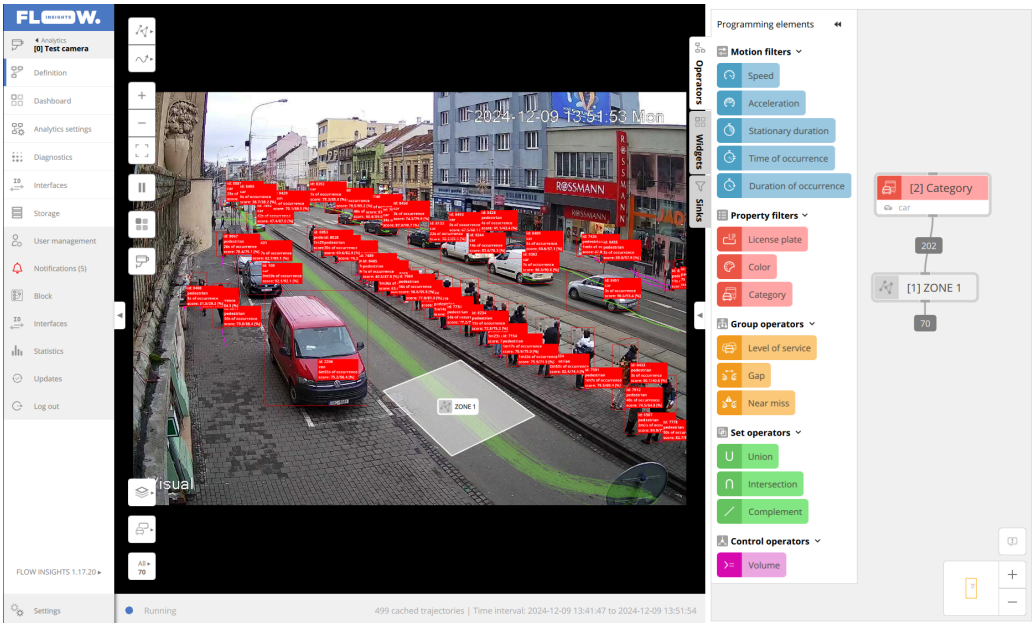
Step 3: Activate NOW Mode

- To detect objects currently inside the zone, activate **NOW mode**:
  - Double-click the zone in the workspace panel.
  - In the dialog window, enable the **Now with point representation (standard)**.
- Once activated, the zone displays the current number of objects detected within it.



Step 4: Apply a Category and other Filters (Optional)

- To filter specific object types (e.g., vehicles, pedestrians), use the **Category** filter:
  - Locate it in **Programming Elements > Property Filters**.
  - Drag and drop the filter into the workspace, connecting its output to the zone input to create a sequence filter.
  - Double-click the filter to specify object categories to pass through.

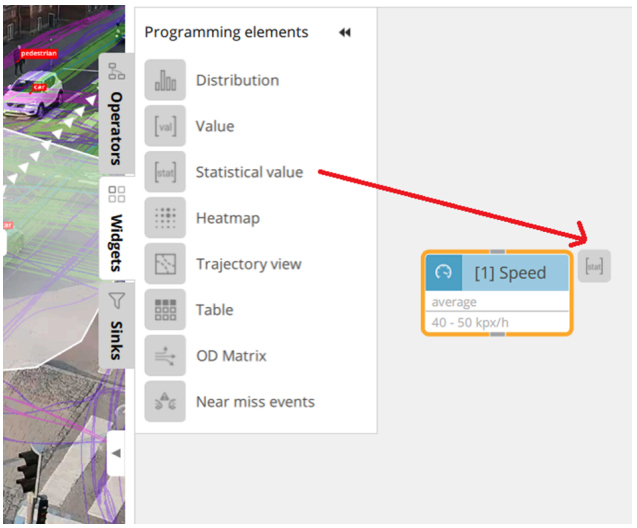


Step 5: Publishing Data

Data from detection zones can be published using **Widgets**. These are used to:

- Display data on dashboards.
- Use expressions to control relays or SDLC interfaces.

Furthermore, widgets may be used for traffic control, enabling communication with external devices, such as smart city platforms and data systems.

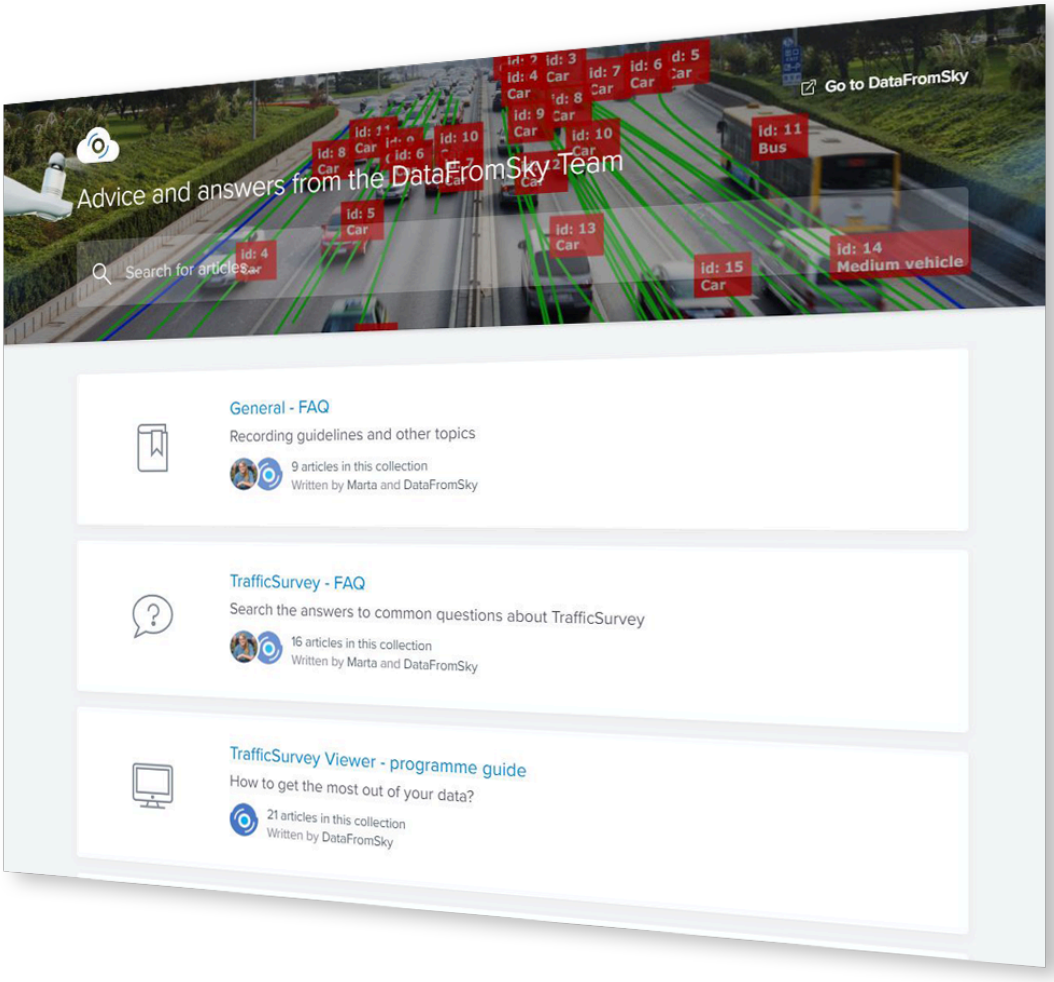


More About the FLOW Framework

The FLOW framework is a versatile and comprehensive system designed to support a wide range of hardware devices. Apart from **TrafficXRoads**, these include **TrafficCamera**, **TrafficEmbedded**, **TrafficEnterprise**, and the mobile processing unit **TrafficDrone**. Regardless of hardware requirements or specific use cases, all devices operate within the same unified system. To explore the complete documentation for the FLOW framework, visit the online manual at:

https://intercom.help/datafromsky/en/collections/2019942-flow-and-flow-insights.

This resource contains a wealth of articles covering the framework's functionality, system architecture, and step-by-step guides for configuring analytics for various scenarios. The manual is regularly updated to reflect new features and best practices. Use the search bar at the top of the page to quickly find the topics most relevant to your needs.



Communication with Traffic Controller

The TrafficXRoads unit allows detected traffic events to be communicated to traffic controllers via various interfaces, including data interfaces (REST API, WEBHOOKs, UDP) and physical interfaces (relay interface). This chapter focuses on the most widely used communication methods: UDP, SDLC, and the relay interface.

Before setting up communication, ensure the traffic controller supports the required interface. For documentation on FLOW data interfaces, refer to FLOW Insights Public API: https://intercom.help/datafromsky/en/articles/3773368-introduction-to-data-sinks-and-flow-insights-public-api.

For additional integration support, contact: support@datafromsky.com.

UDP Data Interface

The UDP interface operates on a subscribe model, where the traffic controller connects to the FLOW device to receive data from defined UDP sinks.

Supported UDP Sinks:

1. **ZONE Sink**: Sends object presence data (object IDs) for a specific zone. Data is transmitted upon subscription or when values change.
2. **CATEGORY COUNT Sink**: Transmits data only when requested by the controller.

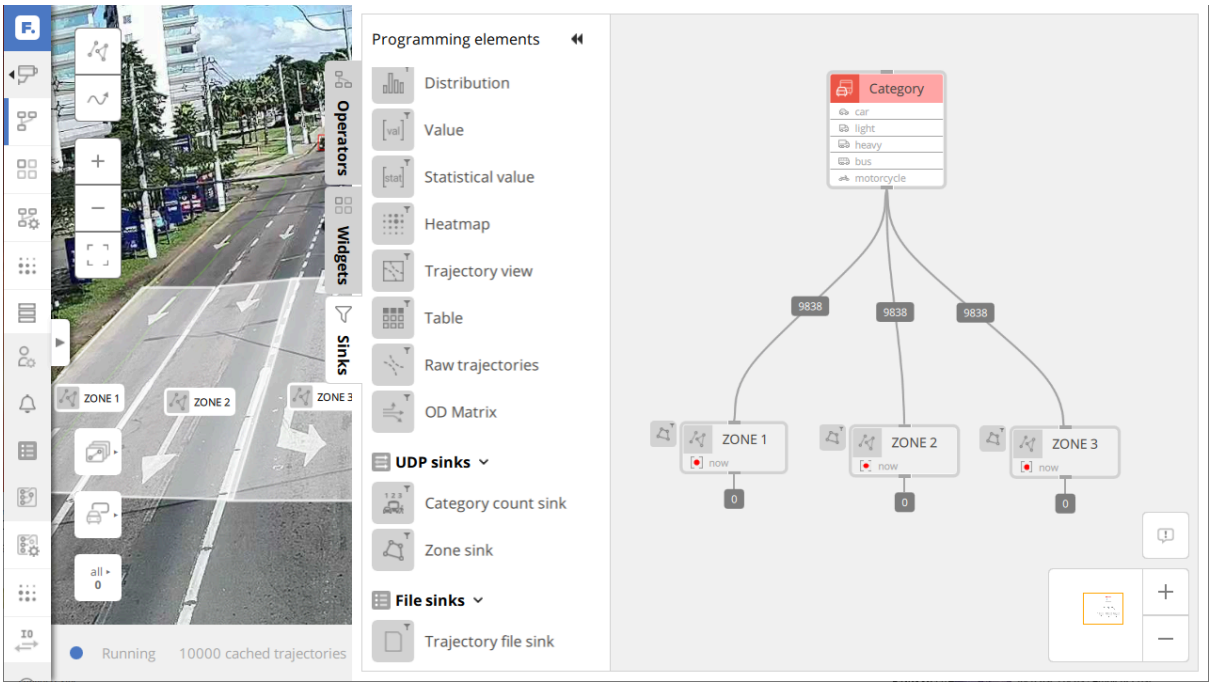
Configuration Steps:

3. Define a traffic detection task in FLOW.
4. Add a UDP sink with a unique name (e.g., `CAM[X]-ZONE[Y]`) to the final ZONE operators in NOW mode.

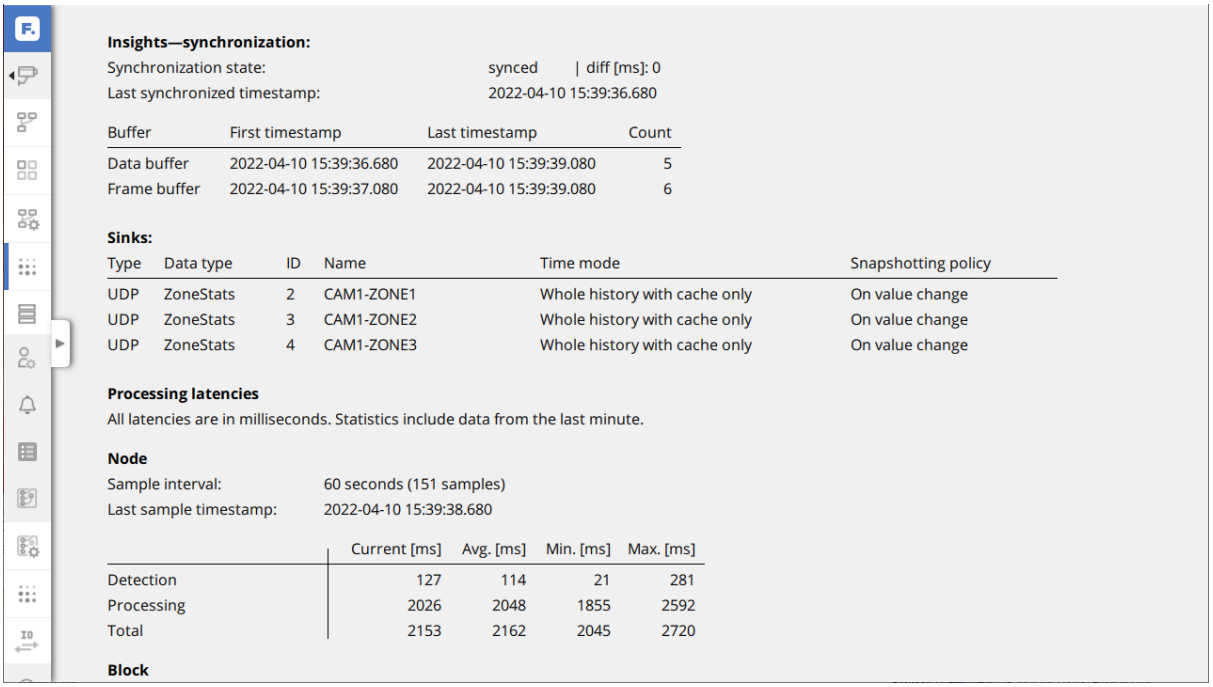
The “sink name” is used as an ID in payloads for communication with the controller. Please make sure it is unique.

Example Setup:

- Add UDP ZONE sinks to detectors for `CAM1-ZONE1`, `CAM1-ZONE2`, and `CAM3-ZONE3`.
- The controller receives vehicle presence/absence information for each zone.



The list of the created UDP sinks can be found on the **Diagnostics** page in FLOW. The status of the zone is communicated to the controller under the names listed in the **Name** row in the table.



Insights—synchronization:

Synchronization state: synced | diff [ms]: 0
Last synchronized timestamp: 2022-04-10 15:39:36.680

Buffer	First timestamp	Last timestamp	Count
Data buffer	2022-04-10 15:39:36.680	2022-04-10 15:39:39.080	5
Frame buffer	2022-04-10 15:39:37.080	2022-04-10 15:39:39.080	6

Sinks:

Type	Data type	ID	Name	Time mode	Snapshotting policy
UDP	ZoneStats	2	CAM1-ZONE1	Whole history with cache only	On value change
UDP	ZoneStats	3	CAM1-ZONE2	Whole history with cache only	On value change
UDP	ZoneStats	4	CAM1-ZONE3	Whole history with cache only	On value change

Processing latencies

All latencies are in milliseconds. Statistics include data from the last minute.

Node

Sample interval: 60 seconds (151 samples)
Last sample timestamp: 2022-04-10 15:39:38.680

	Current [ms]	Avg. [ms]	Min. [ms]	Max. [ms]
Detection	127	114	21	281
Processing	2026	2048	1855	2592
Total	2153	2162	2045	2720

Block

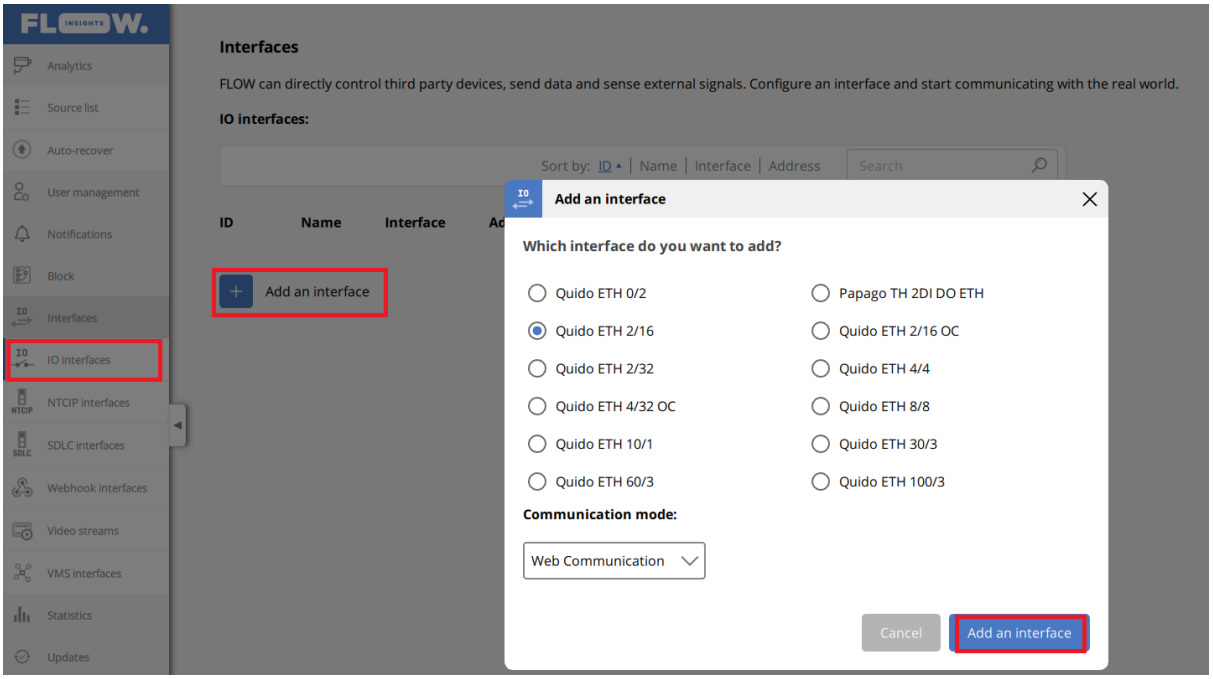
I/O Interfaces

Communication with I/O interfaces (modules) is managed in FLOW via the **I/O interfaces** tab. Configuring interfaces lets you manage supported I/O modules, available in various combinations. A FLOW device can manage multiple I/O modules, and each I/O module can be managed by multiple FLOW devices.

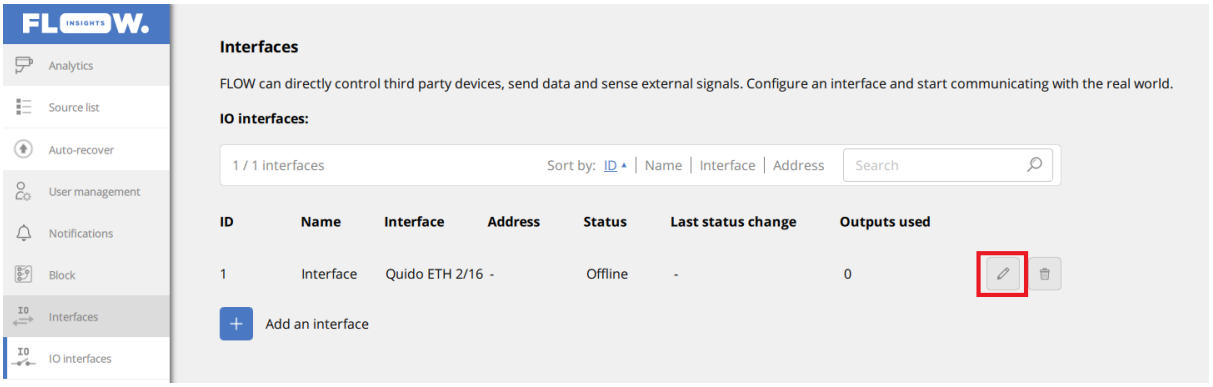
Setup Steps

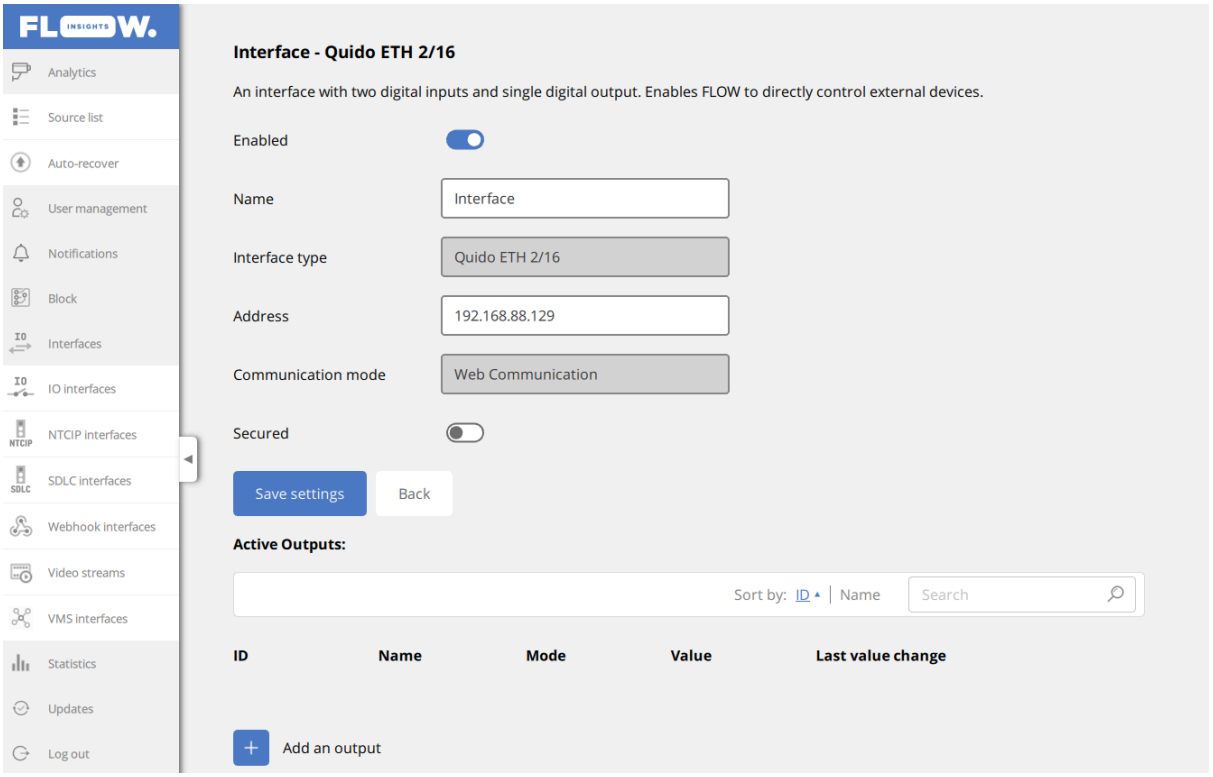
1. Register the I/O Interface:
    - Navigate to **Interfaces->IO interfaces**.
    - Click **Add an interface** and select the module type.
    - From the pop-up list of supported modules, select the appropriate module type (e.g., Quido ETH 2/16 for 2 inputs and 16 outputs).
    - Confirm your selection by clicking **Add an interface**.

      Tip: Ensure the selected module matches your hardware model to avoid compatibility issues.

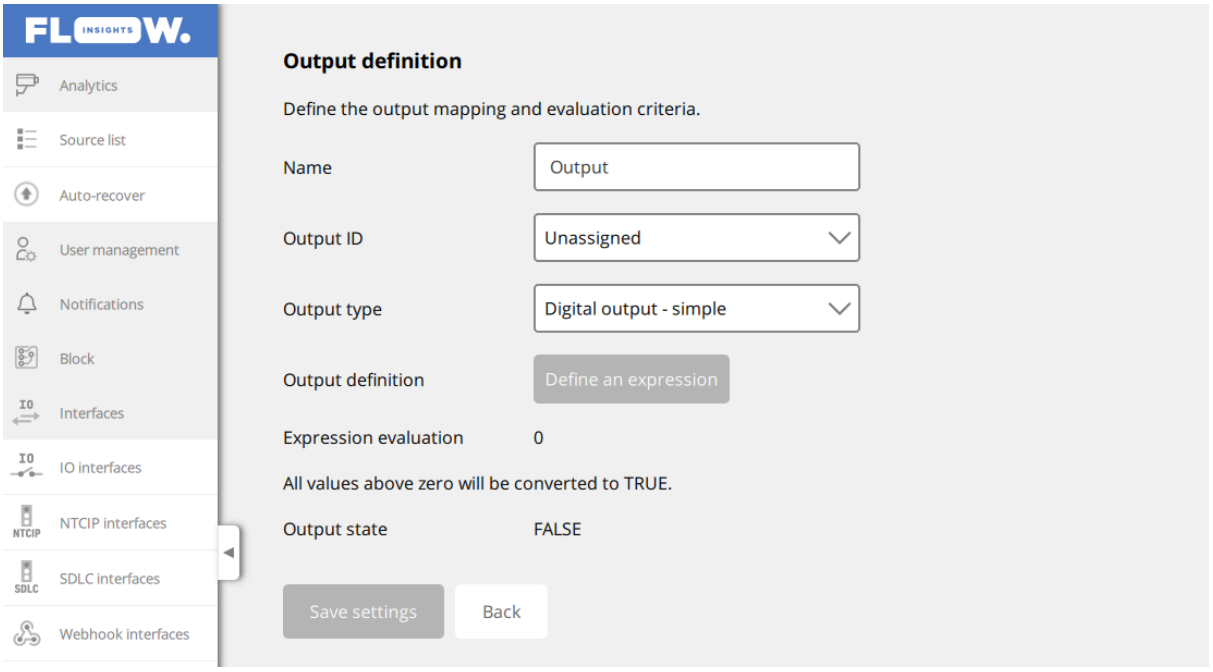


2. Configure the Interface:
   - Open the IO module settings using the **Edit** icon.
   - Assign a name and the IP address.
   - Save settings to establish communication.
   - Click **Save settings**.





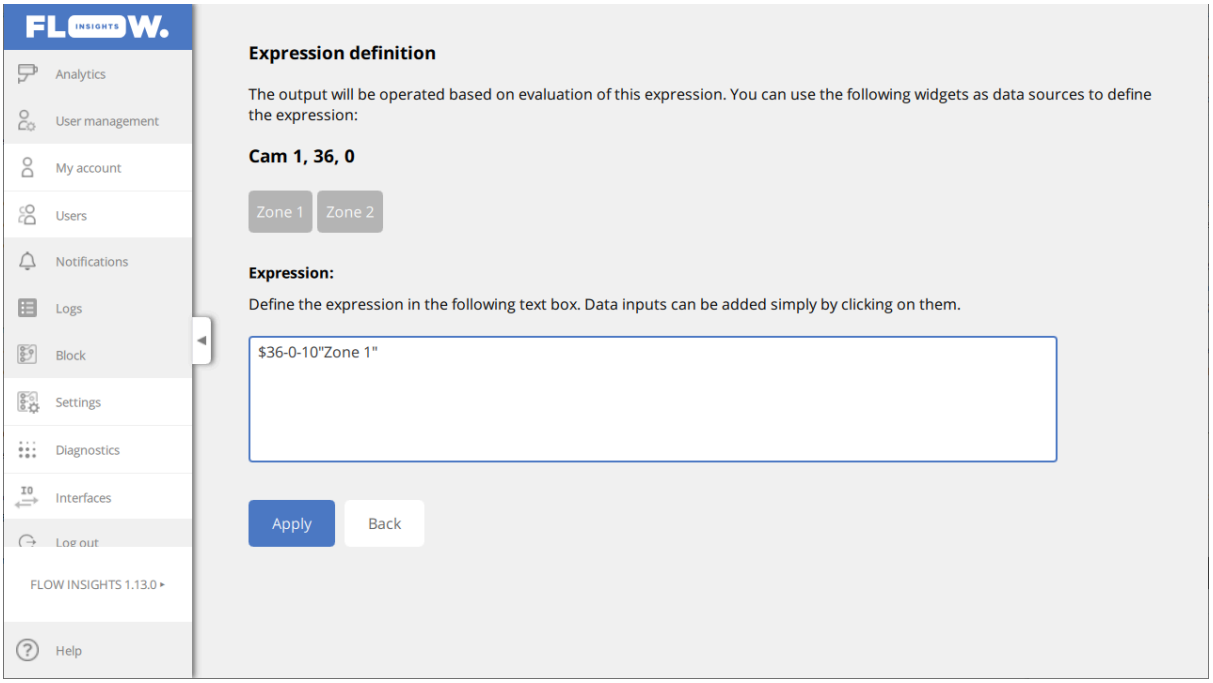
3. Define the Outputs:
    - Click **Add an output** and the pencil icon to open its settings.
    - Define the **Output Name**, **Output ID,** and **Output Type** to assign a physical interface to it.



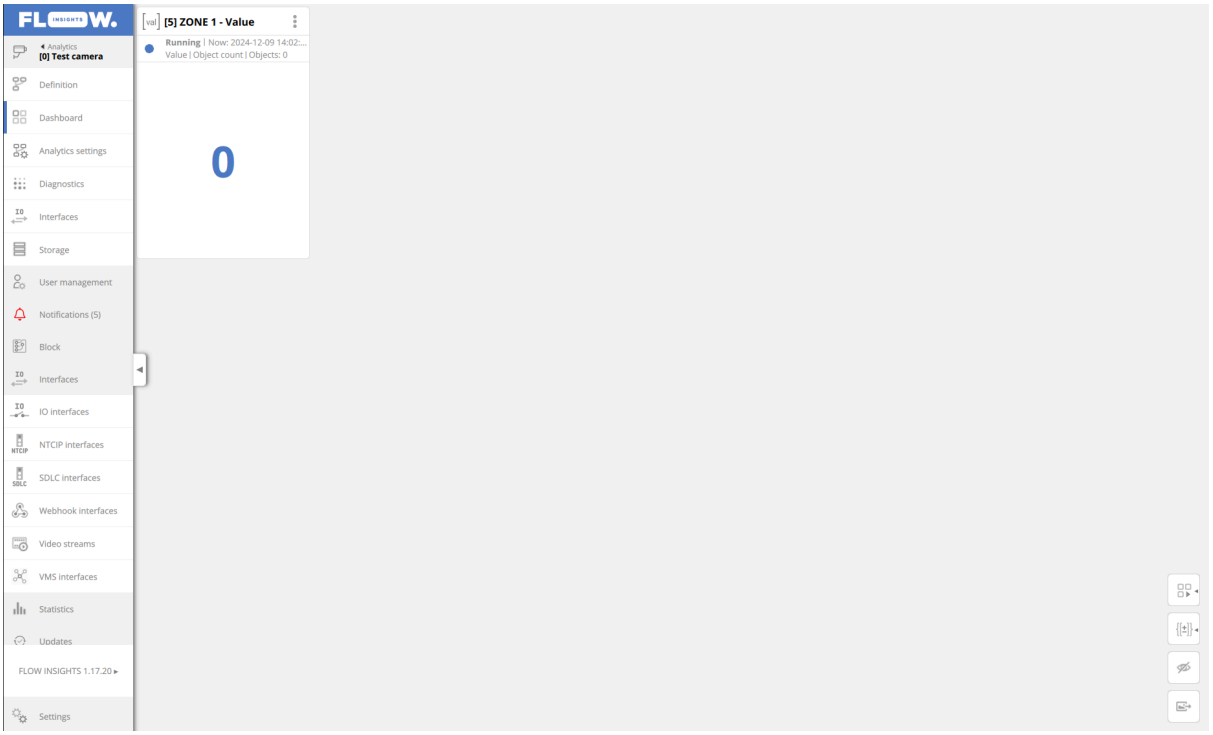
4. Define Output Expression Rules:

   To define the rule for ON/OFF behavior of the interface output:

   - Click **Define an expression** next to the **Output Definition** field. The expression editor opens.



   - Use Dashboard Widgets:
     - Widgets must be **Simple Value** or **Statistical Value** types.
     - To trigger a relay (e.g., based on object presence in a zone), propagate analytic data into a dashboard widget (e.g., Simple Value Widget).
     - Use widget values as variables in the expression.



- Expression Syntax:
  - Widgets from analytics are automatically available for use.
  - Use the Expression Editor with full JavaScript support, enabling:
    - Numerical operators: `+`, `-`, `*`, `/`.
    - Comparison operators: `>`, `<`, `==`.
    - Logic: `if-else`, Boolean conditions, and functions.

- Expression Examples:
  Basic Trigger: `Zone1_Presence > 0`

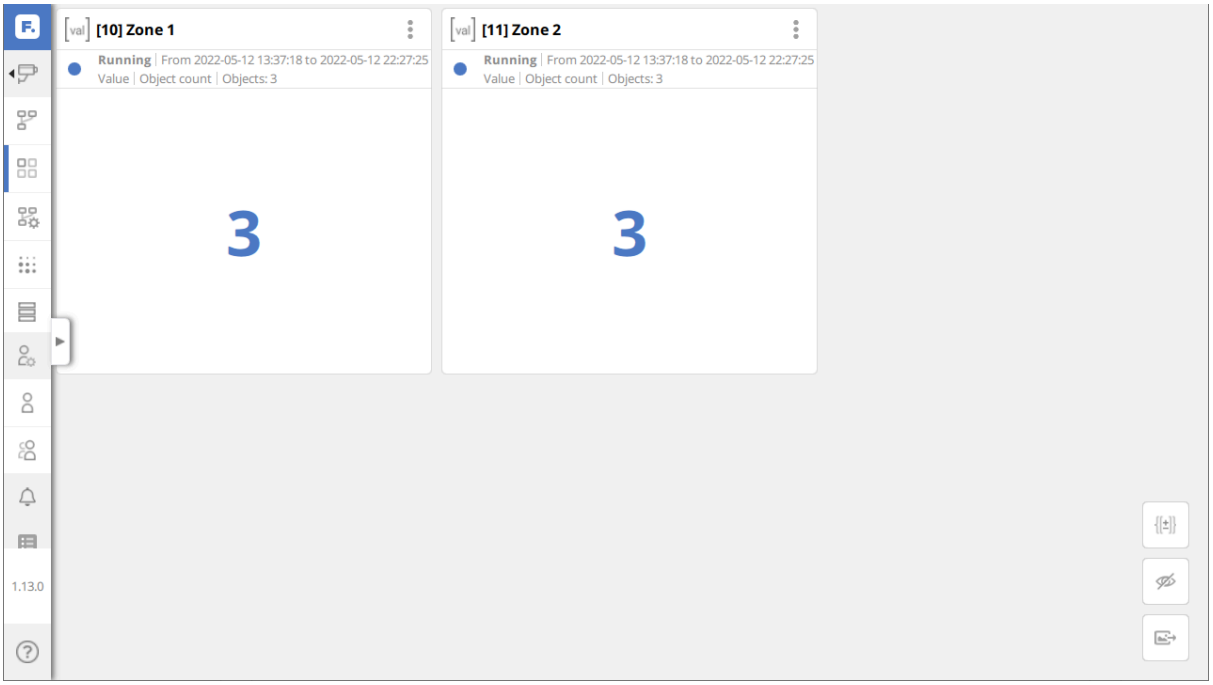
  Conditional Logic:

```
if (object_count_widget > 0) {
    1; // Trigger relay
} else {
    0; // Untrigger relay
}
```

  Complex Logic:

  - Comparison: `Zone1_Presence > 0`

- Boolean Logic: `(Zone1_Presence > 0) && (Zone2_Presence == 0)`
- Math Operations: `(Zone1_Presence + Zone2_Presence) > 5`

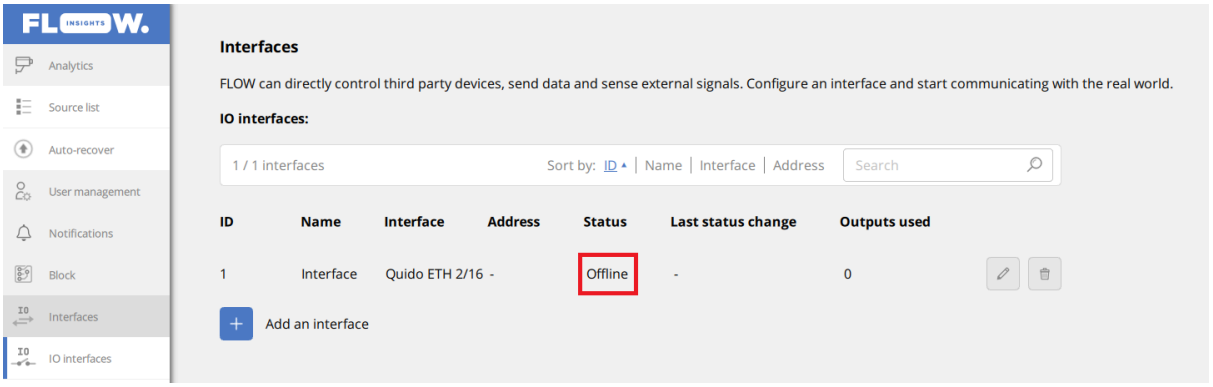


5. Test the Interface:
   - Enter **0** or **1** into the expression definition and save.
   - Confirm the output turns OFF (0) or ON (1).
   - Use physical tools (e.g., multimeter, LED lights) to verify functionality.

6. Check the Interface Status:

   In the Interfaces overview, check the Status field for connection status. Note that the I/O interface status only changes when a real change has been detected. In Analytics, first, create a widget that triggers this status change.

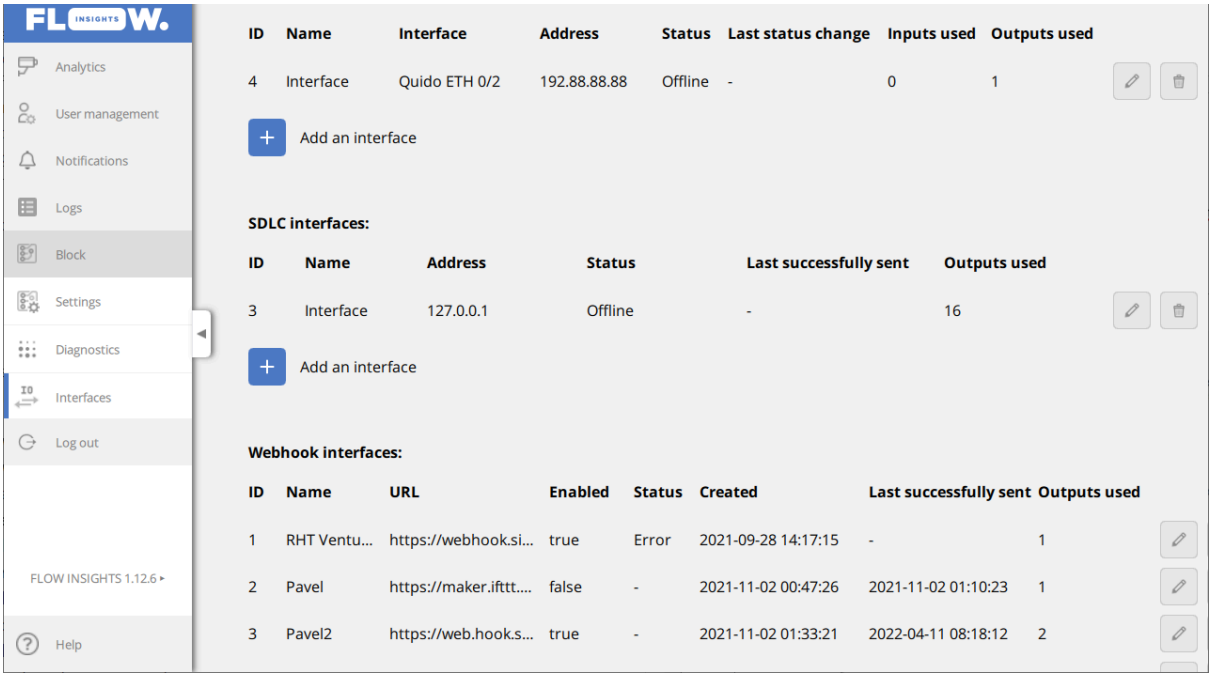
   - **Online**: The module is successfully connected.
   - **Offline**: Verify that the module is powered on, connected to the network, and has the correct IP address.



Troubleshooting Offline Status: Ensure the network cable is securely connected, the module's firmware is updated, and no IP conflicts exist in the network. Also, try opening the module's web interface.

SDLC Data Interface

The **Synchronous Data Link Control (SDLC)** protocol enables reliable communication between the TrafficXRoads unit and traffic controllers. This is achieved through an SDLC converter, such as the Luxcom EM-HDLC, which translates UDP messages from the FLOW device into SDLC protocol responses.



Please note that the number of added convertors is not limited by the FLOW device. A single FLOW device can communicate with multiple convertors at once.

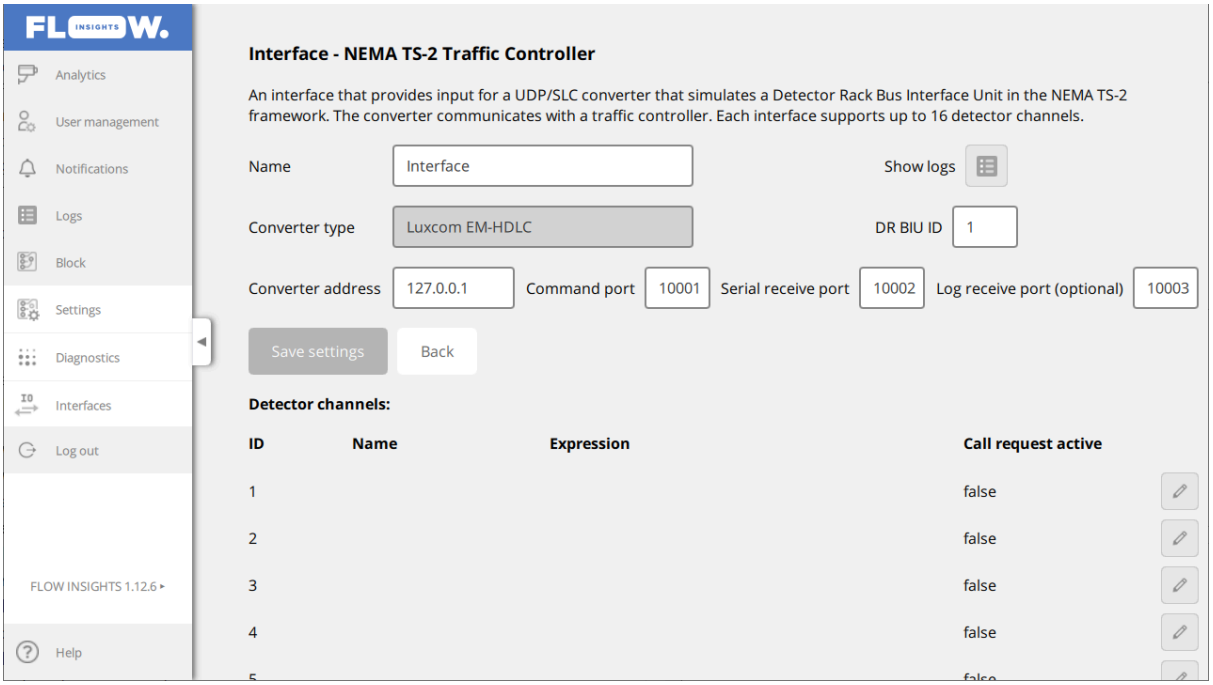
Setup Steps

1. Register the SDLC Converter:
   - Navigate to **Block > Interfaces** and click **Add an Interface** in the **SDLC Interfaces** section.
   - Select **Luxcom EM-HDLC** from the list and confirm the addition.

2. Configure the Converter:

   Access the converter's web management interface and configure the following settings:

   - **Serial Forward IP Address**: Enter the IP address of the embedded unit (TrafficXRoads device).
   - **Serial Forward UDP Port**: Specify the UDP port to be used for SDLC communication.
   - **Syslog IP Address**: Set the IP address where system log messages will be sent (typically the TrafficXRoads device).
   - **Syslog Port**: Define the port for log message communication.
   - **Command IP Address**: Enter the IP address of the TrafficXRoads device to ensure secure communication. The converter will ignore commands from other IPs.
   - **Command UDP Port**: Specify the port for sending and receiving commands to/from the converter.



Tips:

- Avoid ports in the range 0–1023 to prevent requiring administrative privileges for binding.
- Ensure all configured IPs and ports match those set in the TrafficXRoads unit.

3. Verify Communication:

   After configuration, navigate to the **Interfaces** page in FLOW and check the **Status** field under SDLC interfaces:

   - **Online**: The TrafficXRoads device is successfully communicating with the converter.
   - **Offline**: Recheck power, network connections, and IP/port settings.

4. Define Data Handling Rules:
   - Set up the converter to respond to **Call Data** and **Diagnostic Requests** from the controller. Use UDP packets in the required format to dynamically update responses.
   - Example: The TrafficXRoads device sends vehicle presence data, which the converter translates into SDLC-compatible messages.

Monitoring and Diagnostics

The **Diagnostics** page in the SDLC Interfaces section allows you to monitor the performance of the converter and communication link. Key metrics include:

- **Message Counts**: Sent and received message statistics to verify active data exchange.
- **Command Count**: Tracks the number of valid commands processed by the converter, ensuring the setup is functioning correctly.
- **Latency**: Provides real-time insights into communication delays and response times.

Reducing Latency

In many traffic control scenarios, low latency is critical to ensure that traffic events are communicated to the controller as quickly as possible. Achieving minimal latency requires optimizing multiple factors while balancing tradeoffs. This chapter outlines key areas where reducing latency is possible.

Reducing Latency in Cameras

Latency on the camera side is caused by image processing and encoding. To minimize this latency, consider the following optimizations:

- **Resolution**: Use the lowest resolution that meets your requirements. Higher resolutions increase data processing time.
- **Enhancements**: Rotation, scaling, deinterlacing, noise reduction, and more can also
- add latency. Reduce the image enhancements as much as possible, but be aware
- of the effect on image quality, especially in night conditions.
- **Encoding**: Choose H.265 over H.264 for lower latency.
- **Number of Streams**: Limit to only essential streams. Each stream requires separate encoding, increasing the camera's processing load.
- **Frame Rate**: Higher frame rates reduce buffer delays. For example, at 30 FPS, latency per frame is approximately 33 ms.
- **Audio**: Disable audio to eliminate unnecessary latency.
- **Bitrate**: Optimize to reduce data transfer size while maintaining sufficient image quality for automatic processing.

Note: Camera-side processing and encoding typically takes under 50 ms per frame to cover exposure, image enhancement, compressing, and packing.

Reducing Latency in the Network

To minimize latency in the network:

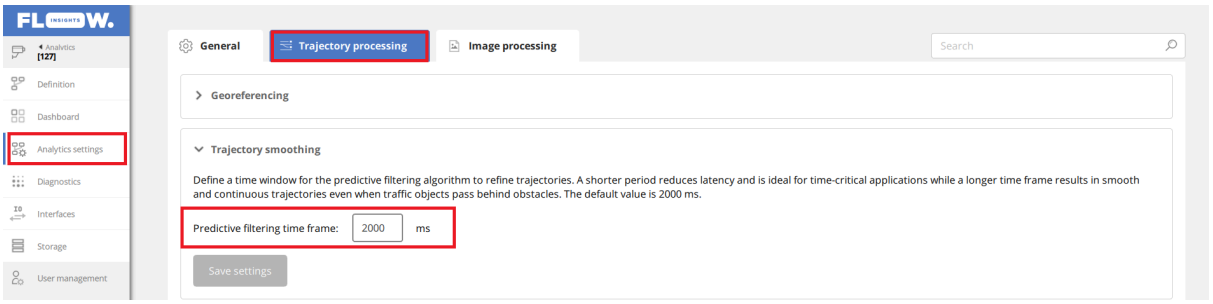
- Limit the total data volume being transmitted.
- Ensure good network quality of service and optimize all network hops for video traffic.
- Connect cameras directly to the TrafficXRoads unit where possible to eliminate intermediate delays.

Reducing Processing Latency in TrafficXRoads

The FLOW framework allows configurable settings to significantly reduce processing latency. Key parameters include:

Trajectory Smoothing Parameter

Trajectory smoothing (configurable under Analytics settings) allows you to define the predictive filtering time window to refine trajectories. This defines the tracker buffer size in milliseconds. A smaller buffer decreases latency but may result in trajectory interruptions in busy scenes.

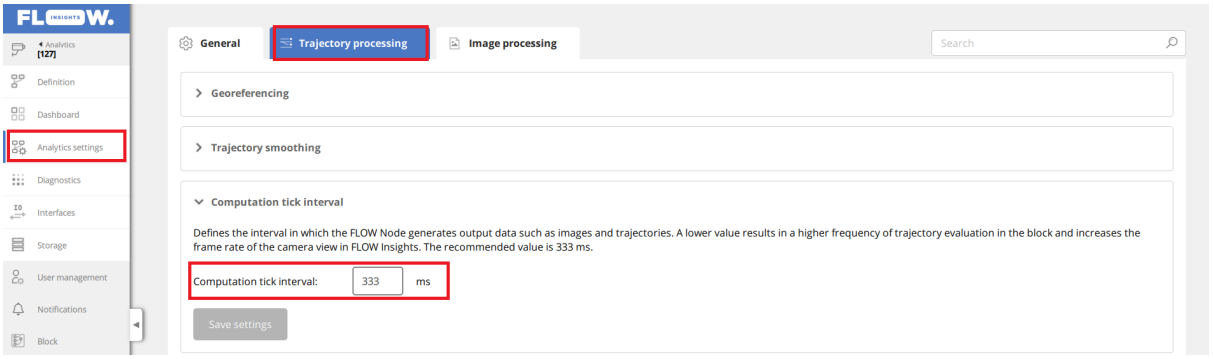


Recommendations:

- **<200 ms**: Maximum responsiveness for tasks like object presence detection.
- **200 ms**: Balanced response time and trajectory continuity (ideal for systems with 10+ FPS).
- **2000 ms**: For applications where continuity is prioritized over speed, such as traffic statistics collection.

Computation Tick Interval

This parameter determines how often the FLOW engine evaluates trajectories and generates results. Lower intervals reduce reaction time but increase the processing load.



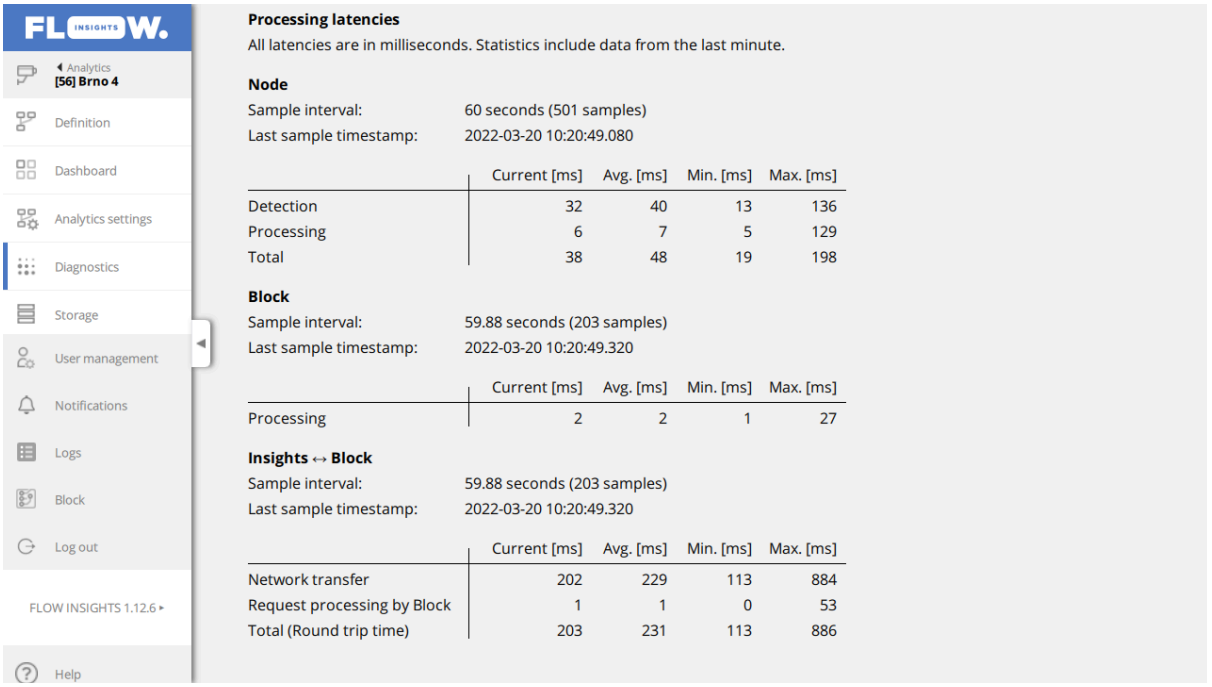
Recommendations:

- **333 ms**: Default.
- **100 ms**: Traffic control tasks for faster system response.

Processing Latencies - Diagnostics

The Processing Latencies section provides an overview of latency metrics for the TrafficXRoads unit, accessible on the **Diagnostics** page. It monitors three key areas:

- **Node**: Displays the latency of the video-analytical component (**FLOW Node**). The **Total** value is critical for evaluating video analytics performance.
- **Block**: Reflects the latency of trajectory evaluation (**FLOW Block**), specifically the time taken for image processing and trajectory calculations, including tracker buffering. The **Processing** metric is key for controller communication.
- **Insights -> Block**: Relates to data transfer into the **FLOW Insights** configuration application. These values, while not essential for controller communication, measure network transfer and request processing efficiency.



Node – Detection Time: Should be 20% shorter than the minimum detection FPS for the scene type. Includes the tracker's configurable time buffer.

Block – Processing Time: Must be at least 50% shorter than the computational tick interval. If not, reduce the number of analytics or data outputs to prevent system overload.

Reducing Latency on Outputs

Output latency refers to the time required to send traffic event data from the FLOW device to the controller. The recommended communication methods, ordered by speed, are:

1. **UDP Sinks**: < 1 ms.
2. **SDLC Interface**: ~1 ms (varies by converter).
3. **Quido I/O Modules (Relay Interface)**: ~11 ms.

Recommendation: Use UDP sinks for minimal latency when supported by the traffic controller.

Achievable Latencies

With optimized settings, overall system latency can be reduced to ~200–350 ms:

- **Camera Processing**: ~50–150 ms.
- **Image Transfer**: <10 ms (local network).
- **TrafficXRoads Processing**: ~100 ms.
- **Controller Communication**: <1 ms (UDP, local network).

Lower latencies, as low as 50 ms, are possible with industrial cameras. Contact us for guidance on implementing ultra-low-latency solutions.

Additional Resources

This manual has provided an overview of the basic configuration and setup of the TrafficXRoads unit.

This manual has provided a comprehensive guide to configuring and using the TrafficXRoads unit in its available core models 30N, OV008, and I131. It has covered essential topics, including device setup using available interfaces, field installation, power, and wiring configurations, and detailed network and camera integration. Additionally, the manual introduced the FLOW framework for advanced analytics, communication with traffic controllers, and methods for optimizing system latency to achieve real-time performance.

Product Datasheets

For more detailed product specifications, refer to the datasheets available online: https://intercom.help/datafromsky/en/articles/5559259-manuals-and-datasheets-trafficcamera-trafficembedded-trafficxroads-trafficdrone

Software Updates

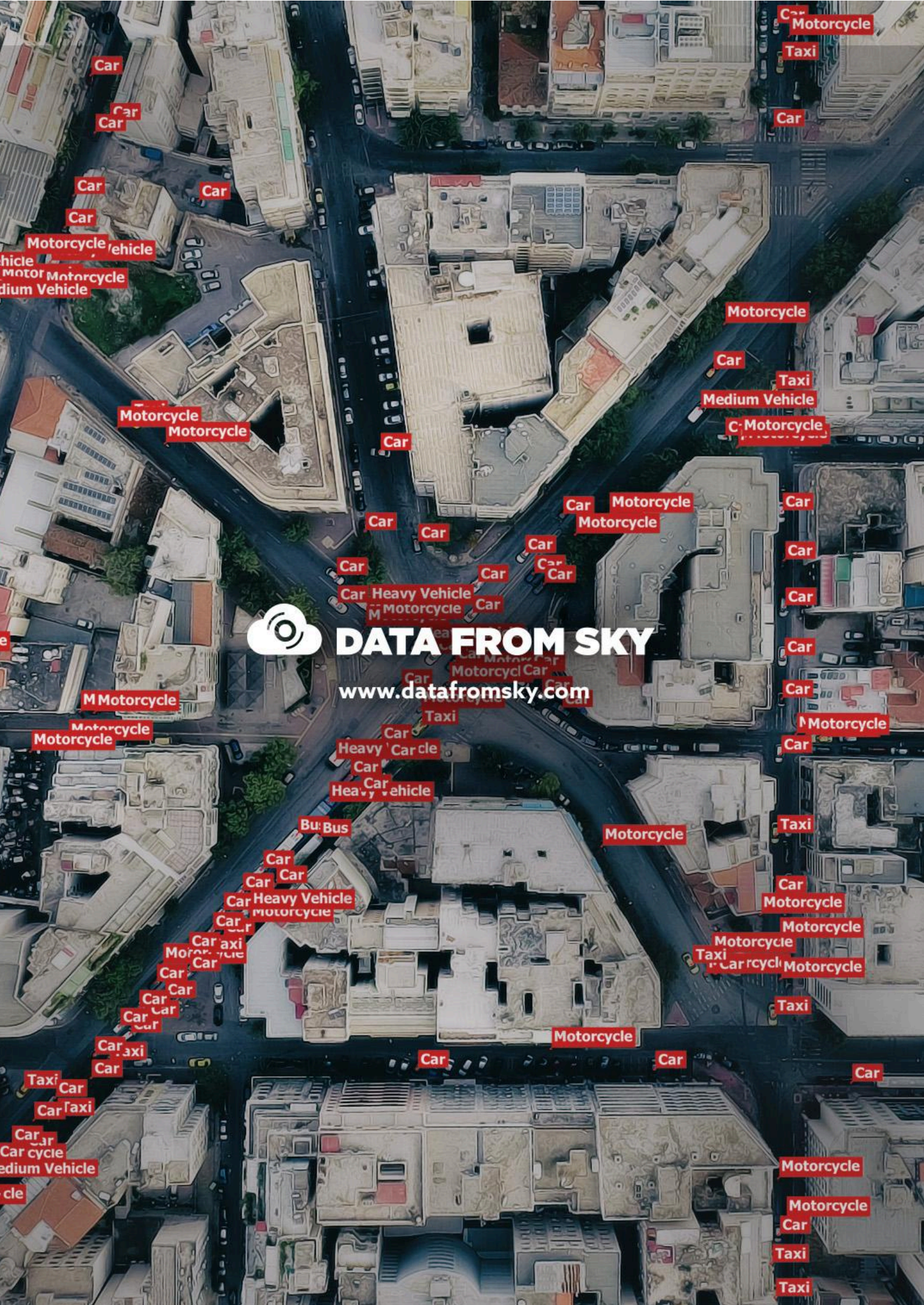
The FLOW platform receives regular updates with new features, performance enhancements, and bug fixes. The FLOW Insights application notifies you about new versions available. To maintain compatibility, always update your TrafficXRoads unit before updating FLOW Insights. For assistance with updates or any related queries, contact us at support@datafromsky.com.

Customer Support

We are committed to providing excellent support for your TrafficXRoads device. If you have questions, encounter issues, or would like to provide feedback, please reach out to us:

- **Support**: support@datafromsky.com
- **General Feedback**: info@datafromsky.com

Thank you for choosing TrafficXRoads. We look forward to supporting your journey toward smarter and safer traffic management.


DATA FROM SKY
www.datafromsky.com