SM Instruments

Now See Your Sound and Vibration!

BATCAM FX2

제품 매뉴얼 · Product Manual

English

생성 / Generated: 2026-11-11 07:21 UTC

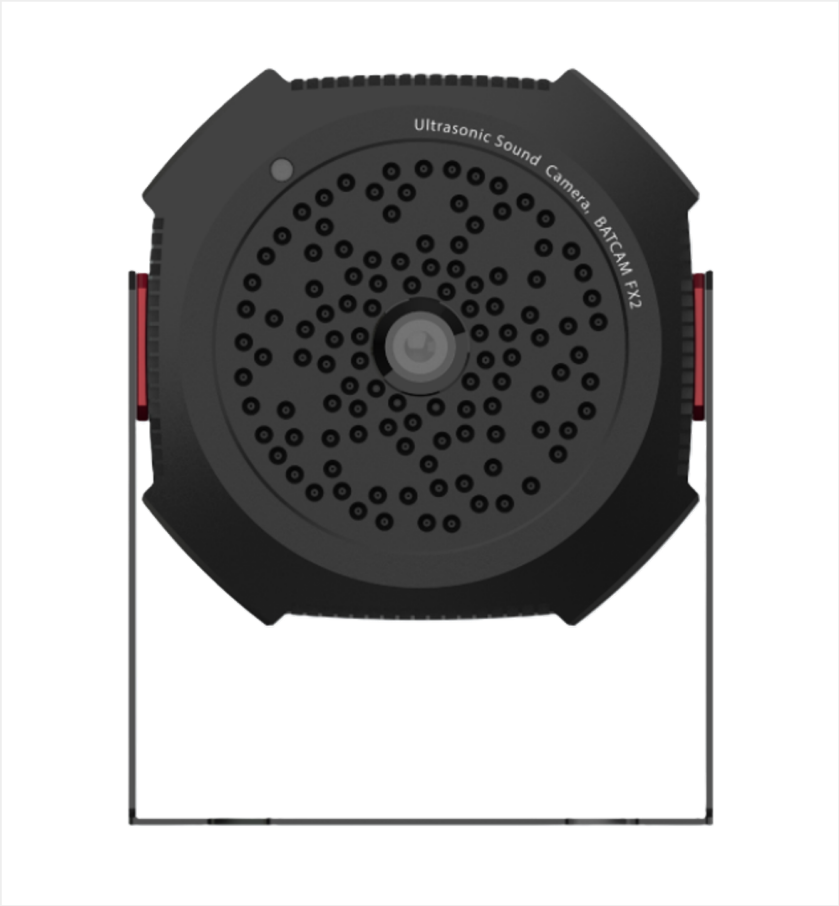
목차 · Contents

Product Overview 3
Safety and Handling Precautions 7
Product Specifications and Package Contents 10
Installation 16
First Connection 20
Device Manager Screen Layout 24
Live Video and Beamforming 29
Camera Settings 35
AI Detection 41
Events 47
Microphone Check 55
User Accounts and Permissions 62
System Settings 68
Firmware Update 79
External System Integration 87
ROS 2 Integration 95
API and Developer Integration 103
FX Viewer Integration 107
Troubleshooting 109
Frequently Asked Questions 118
Firmware Version Information 122
Product Support and Inquiries 125

Product Overview

This page explains the features and operating principles of the BATCAM FX2. First, see what this device can detect.

What Is the BATCAM FX2?



The BATCAM FX2 is a fixed ultrasonic camera that houses a 112-channel MEMS microphone array and a camera in a single enclosure. It measures sounds in frequencies beyond human hearing and displays their locations in color over the camera image. You can locate compressed-air and gas leaks and partial discharges on the screen.

Measurement, analysis, and AI classification are all processed on the device. Settings and results are accessed through Device Manager, the device's built-in web interface. The title of the Device Manager screen is FX2 Device Management Console.



Key Features

- Microphones — 112 digital MEMS microphones receive sound simultaneously.
- Sampling — Each channel is sampled at 200 kHz and 24 bits.
- Beamforming — The FPGA processes signals from 112 microphones to determine the direction and intensity of incoming sound. The result is a 44 × 26-cell map rendered as a heatmap over the image.
- Device Manager — Access it through a web browser. No separate software is required.
- On-device AI — Leak AI and partial-discharge AI run on the device. Classification does not require a server connection.
- Ethernet ports — Two ports are provided: eth0 and eth1.
- Power — Uses PoE+ or DC input.
- Integration — Supports RTSP, ONVIF (some query operations), Modbus TCP, ROS 2, REST API, and WebSocket.

Applications

- Detecting compressed-air and gas leaks in pipes, valves, fittings, and tanks
- Detecting partial discharges in electrical equipment
- Continuous monitoring of equipment sounds

- Recording photos, video, and audio when an abnormal sound occurs

Detection Targets

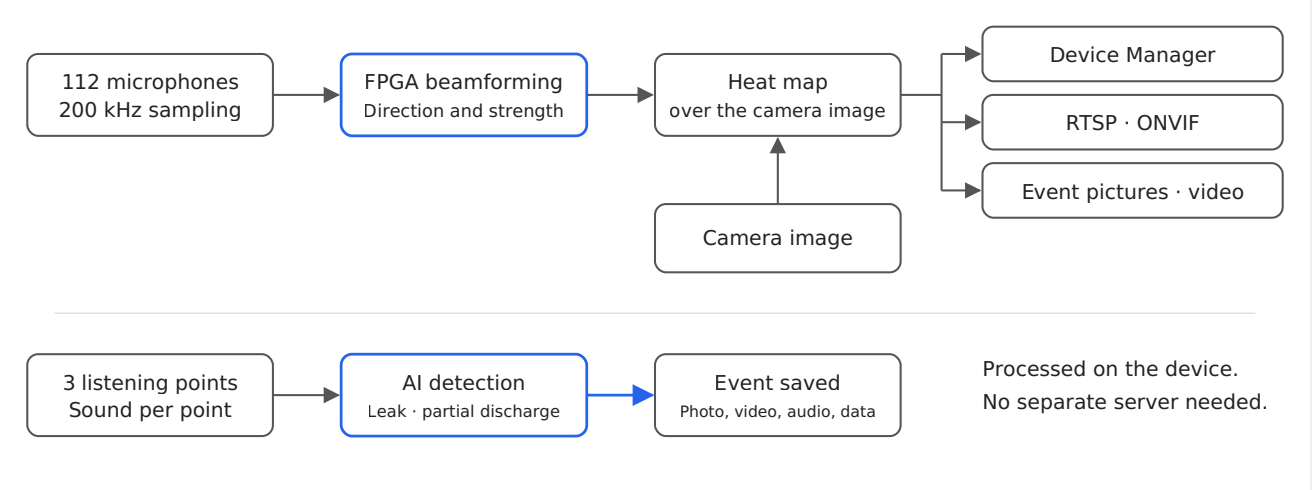
- Leaks — Detects the sound of escaping compressed air and gas.
- Partial discharges — Detects electrical partial discharges and distinguishes their types (Corona, Floating, Surface).

For details, see AI Detection.

How It Works

The 112 microphones receive sound simultaneously. The FPGA calculates the direction and intensity of incoming sound from the differences in arrival time between microphones. The result is overlaid in color on the camera image; redder colors indicate a higher level (dB). The composite image can be viewed in Device Manager and via RTSP.

The device separately captures sound at three listening points on the screen and classifies it using AI. When the conditions are met, it saves the photo, video, audio, and measurement data from that moment as an event.



For details, see Live Video and Beamforming.

Components

- Camera — Depending on the configuration, one of the following two models is installed. Check “Camera Model” on the Device Manager home screen.
  - SMIA462 Wide — No focus adjustment mechanism.
  - SMI3708 Wide — Supports focus adjustment.
- Two Ethernet ports — eth0 and eth1
- One rear function button — Press and hold for at least 3 seconds to start a factory reset.
- Status LED — Located on the front. Green means the device is measuring normally. Red means measurement has stopped for more than 2 seconds or the device is starting up.

- Rear LEDs — PWR LED and ETH LED. The ETH LED is normally off.

Safety and Handling Precautions

These are the safety precautions to follow before installing and using the BATCAM FX2. Read them in full before installation.

Before You Begin

Failure to follow the safety precautions may result in electric shock, product damage, or measurement errors. Installation and electrical work must be performed by qualified personnel.

Power

- Use only a 12 ~ 24 V DC or PoE+ (IEEE 802.3at) power supply. Connecting a power supply outside these specifications may damage the device.
- The device has reverse-polarity protection. Even so, use only the specified cable and power supply.
- Do not handle the power connector with wet hands.
- Do not disconnect or connect cables while power is supplied.
- Do not turn off the power or unplug cables during firmware or FPGA updates. The update may fail, or the FPGA may be damaged.

Installation Environment

- The operating temperature is -20 ~ 50 °C, and the operating humidity is 93 % RH (non-condensing). Measurement performance may decline outside these ranges.
- The water and dust resistance rating is IP68. Avoid prolonged immersion and high-pressure washing.
- For outdoor installation, we recommend adding a waterproof junction box around the mult cable connector junction.
- Avoid locations exposed to prolonged direct sunlight or heat buildup, or continuous strong vibration.
- Do not obstruct the front of the microphone array or the camera lens with water, dust, or foreign matter. Doing so reduces measurement accuracy.

Mounting and Fall Prevention

- The unit weighs approximately 1,245 g, or approximately 1,395 g including the cable. Secure it firmly to a rear VESA 75 or VESA 100 mount or the dedicated bracket.
- Take measures to prevent falls when installing the device at height. Make sure the structure can adequately support the device’s weight.

Measurement Environment

- Near hazardous equipment such as high-pressure piping and rotating machinery, maintain the safety distance specified for that equipment.

- The BATCAM FX2 is not explosion-proof. Do not install it in areas with an explosion hazard (hazardous areas).

Network

- At the factory defaults, the eth0 port uses 192.168.0.80 and the eth1 port uses 192.168.0.81. Before connecting multiple devices to the same network, assign each device a different IP address.
- The factory-default administrator account has the ID `admin` and password `1234`. These values are also displayed on the Device Manager login screen. Change the administrator password after the first login. Delete the factory-default regular user account (user) if it will not be used.
- In firmware v1.1.0, the following connections do not require authentication. Anyone who can access the device can receive video and data.
  - RTSP video and WebRTC video
  - WebSocket
  - ONVIF snapshots, device discovery, and queries
  - Event files
  - Modbus TCP (off by default)
  - ROS 2 topics and actions
- Keep the device on an internal network; do not expose it directly to the internet.
- The device does not support HTTPS. Device Manager is accessed over unencrypted HTTP.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

- A device account is required to receive RTSP video, WebRTC video, WebSocket data, ONVIF snapshots, and event files (stream authentication is on by default). Save the device account in the VMS and viewer.
- Account information is transmitted over unencrypted RTSP and HTTP. Keep the device on an internal network; do not expose it directly to the internet.
- The following connections do not require authentication.
  - ONVIF device discovery and queries
  - Modbus TCP (off by default)
  - ROS 2 topics and actions. Anyone in the same DDS domain can view video through the video topic without an account, even when stream authentication is enabled.
- If an administrator turns off stream authentication, video, WebSocket data, and event files also become accessible without an account. Turn it off only when absolutely necessary.

For more information, see External System Integration.

Test Signal and Factory Reset

- Turn off the 40 kHz reference signal used to test the microphone when testing is complete. If left on, the reference signal may be measured instead of actual sound, causing the level trigger to operate incorrectly. For more information, see Microphone Test.
- Pressing the rear function button for 3 seconds or longer starts a factory reset without confirmation. Settings, accounts, and events are all deleted, so take care not to press it accidentally. For more information, see System Settings.

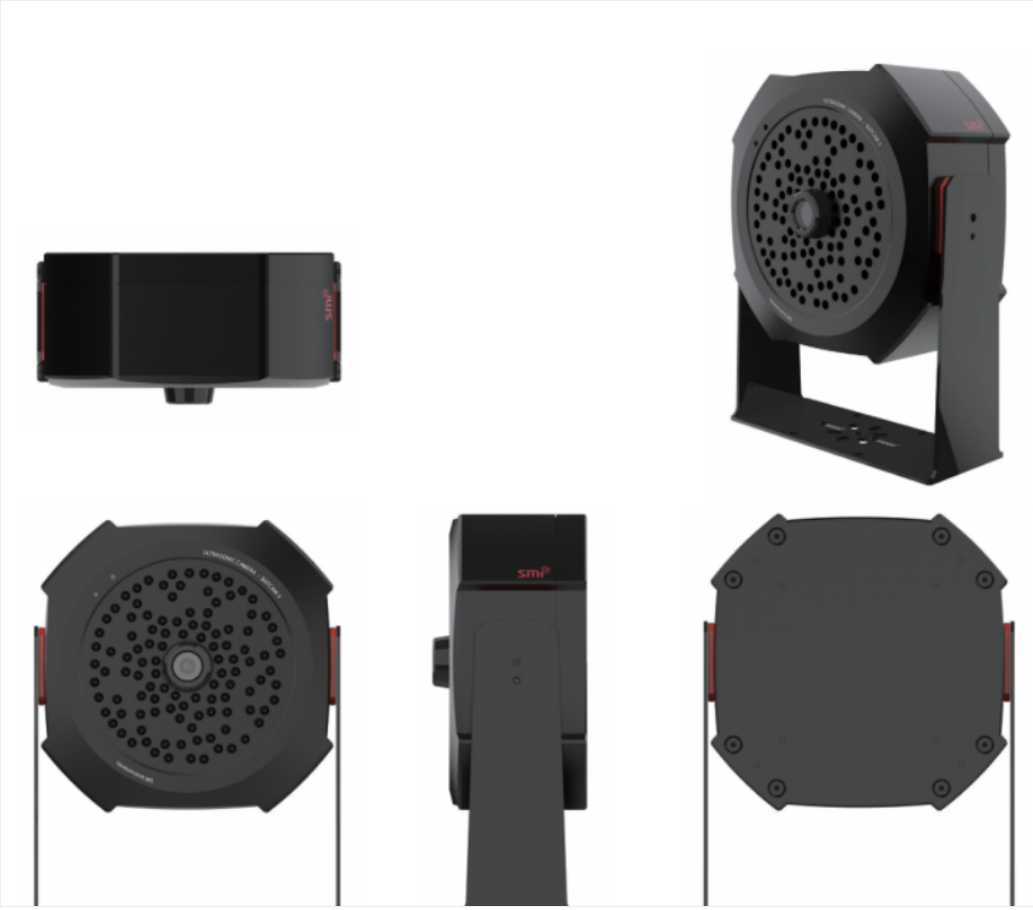
Handling and Maintenance

- Do not disassemble or modify the unit. Doing so voids the warranty and compromises its water resistance.
- Wipe the surface with a dry or soft cloth. Avoid solvents and high-pressure water jets.
- If you notice unusual noise or heat, disconnect the power and contact the seller or manufacturer. For more information, see Product Support and Inquiries.

Product Specifications and Package Contents

This page describes the hardware specifications of the BATCAM FX2, the features of firmware v1.1.0, and the package contents.

Product Specifications



- Product — Fixed ultrasonic camera
- Model — BATCAM FX2
- Primary uses — Gas leak detection, partial discharge detection, industrial acoustic monitoring
- Dimensions (main unit) — Within 148 × 146 × 69 mm (excluding mount and cable gland)
- Dimensions (overall) — Within 152 × 197 × 96 mm (including mount and cable gland)
- Weight — Main unit 1,245 g; including cable 1,395 g
- Color — Black

Acoustics

- Microphones — Digital MEMS microphones
- Number of channels — 112
- Frequency range — 1 kHz ~ 100 kHz

- Sampling rate — 200 kS/s
- Bit resolution — 24 bits
- Measurement range — 5 dB SPL ~ 122 dB SPL (25 kHz ~ 60 kHz, beamforming level)
- Minimum detectable leak flow rate — 50 cc/min (based on a nitrogen gas leak from a circular micro-nozzle)
- Effective measurement distance — 0.5 m ~ 200 m
- Beamforming — FPGA-based real-time processing, 44 × 26 grid map
- Default measurement band — 20 kHz ~ 60 kHz
- Self-diagnostics — Microphone check using a built-in 40 kHz reference signal

※ The lower limit of the measurement range is the minimum detection level after applying the processing gain of the 112-channel beamforming array. It differs from the noise floor of a single microphone.

※ The lower limit of the measurement range is the minimum detection level after applying 112-channel beamforming processing gain and differs from the noise floor of a single microphone.

Camera

Depending on the configuration, the device contains one of the following two cameras. Check “Camera Model” on the Device Manager home page to identify it.

SMIA462 Wide

- Focus adjustment — None
- Firmware file — fx2-cm5-arducam-v<version>.mender
- Sensor capture mode — 1920 × 1080
- Output resolution — 1920 × 1080 (default), 1600 × 900, 1280 × 720, 640 × 360
- Frame rate — 25 fps
- Horizontal field of view at 100 % — 124.07°
- Horizontal field of view at 67 % — 82.71°
- Horizontal field of view at 50 % — 62.03°
- Horizontal field of view at 33 % — 41.36°

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

The default horizontal field-of-view values for SMIA462 Wide devices without device-specific field-of-view calibration have changed as follows.

- Horizontal field of view at 100 % — 123.78°

- Horizontal field of view at 67 % — 82.53°
- Horizontal field of view at 50 % — 61.89°
- Horizontal field of view at 33 % — 41.26°

SMI3708 Wide

- Focus adjustment — Available (0 ~ 35 D, automatic or manual)
- Firmware file — fx2-cm5-imx708-v<version>.mender
- Sensor capture mode — 2304 × 1296 (pixel array 4608 × 2592)
- Output resolution — 1920 × 1080 (default), 1600 × 900, 1280 × 720, 640 × 360
- Frame rate — 25 fps
- Horizontal field of view at 100 % — 101.6°
- Horizontal field of view at 67 % — 67.74°
- Horizontal field of view at 50 % — 50.8°
- Horizontal field of view at 33 % — 33.87°

Common Features

- Image rotation — 0°, 180°
- Field-of-view options — “100%”, “67%”, “50%”, “33%”

The horizontal field-of-view values are firmware defaults. Each device is calibrated before shipment, so actual values may differ slightly.

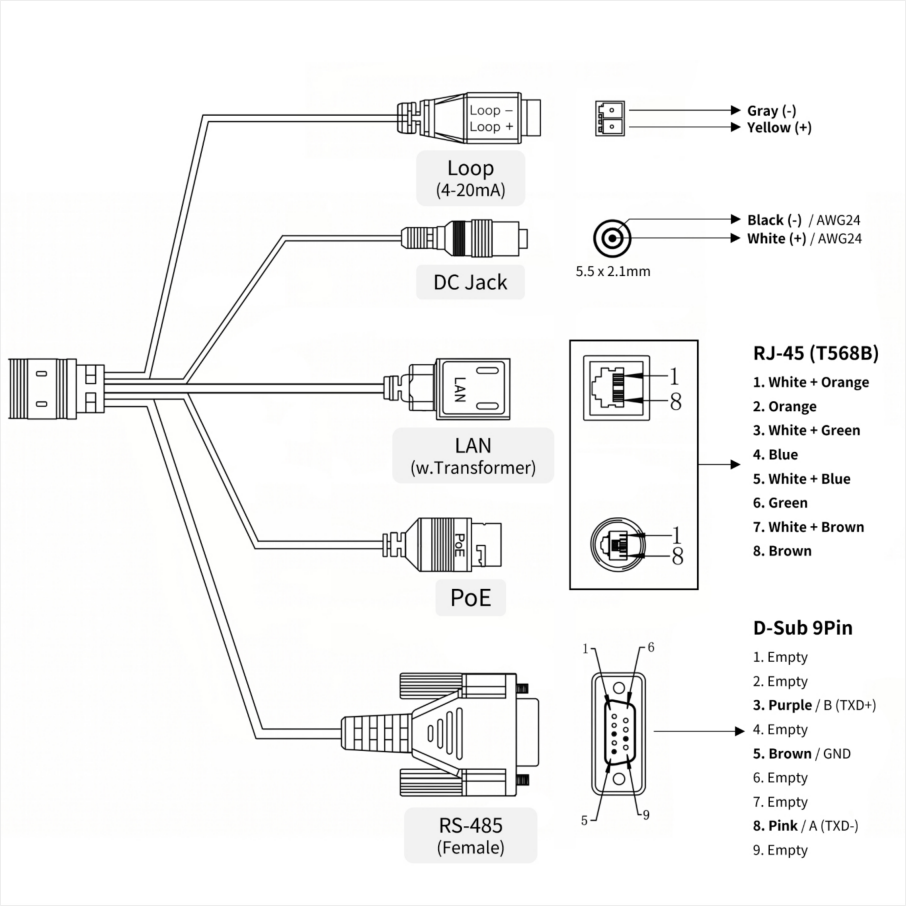
Hardware and Interfaces

- Signal processing — FPGA and embedded controller
- AI acceleration — Onboard NPU
- Power input — 12 ~ 24 V DC or PoE+(IEEE 802.3at)
- Power consumption — 14 W in standard mode, 21 W in maximum mode
- Wired interfaces — Two Gigabit Ethernet ports (10/100/1000 Mbps), 4 ~ 20 mA analog output, RS485
- Mounting — VESA 75, VESA 100, dedicated bracket
- Ingress protection — IP68
- Controls — One rear function button
- Indicator — Status LED
- Power protection — Reverse-polarity protection circuit
- Corrosion resistance — Anti-corrosion surface treatment

※ The interface cable extending from the device is a multi-cable. Connect an Ethernet cable to the LAN connector at the end of the multi-cable. Use a CAT5e or higher UTP Ethernet cable. CAT6 is recommended, as is an installation length of no more than 80 m.

Multi-Cable

The multi-cable is permanently attached to the rear of the product.



- Loop(4-20 mA) — 2-pin terminal. Yellow +, gray –
- DC jack — 5.5 × 2.1 mm. White +, black –, AWG24. Input voltage is 12 ~ 24 V DC.
- LAN — RJ-45(T568B), built-in transformer
- PoE — eth0 port. RJ-45(T568B)
- RS-485 — Female D-Sub 9-pin. Pin 3: purple B(TXD+); pin 5: brown GND; pin 8: pink A(TXD–). The remaining pins are unused.

Software Features

- Real-time sound-source display — Heatmap, peak markers, and level (dB) overlaid on the camera image
- AI detection — Leak AI, partial discharge AI
- Events — Automatic saving and saving based on level trigger, LEAK AI, or partial discharge AI conditions

- Event files — Images (JPG), video (MP4), audio (WAV), measurement data (HDF5)
- Development integration — REST API, WebSocket
- PC software — FX Viewer
- Robot integration — ROS 2

Network and Protocols

- Network interfaces — Two Gigabit Ethernet (RJ-45) ports
- Factory-default addresses — eth0 192.168.0.80, eth1 192.168.0.81
- Device Manager — HTTP port 80
- Video stream — H.264 Baseline, 25 fps, up to 1080p
- RTSP — `rtsp://<device-ip>:8554/overlay`, no authentication, TCP, UDP unicast, UDP multicast
- WebRTC — Used for video in Device Manager, no authentication
- ONVIF — Supports device information, profiles, GetStreamUri, and GetSnapshotUri
- Modbus TCP — Disabled by default, default port 5020
- ROS 2 — Jazzy, five topics
- Data interface — WebSocket (real-time acoustic data and measurement results), no authentication
- Control API — REST API
- Time — NTP

※ The BATCAM FX2 has no RTC (built-in clock). If power is turned off while the device is disconnected from a time server (NTP), it loses the device time. If powered on without NTP, the device time starts at 1970-01-01T00:00:00.

※ The BATCAM FX2 is not officially ONVIF-conformant. ONVIF functionality is only partially implemented. For details, see External System Integration.

※ In firmware v1.1.0, RTSP, WebRTC, WebSocket, ONVIF snapshots, event files, ONVIF device discovery and queries, Modbus TCP, and ROS 2 do not require authentication. For details, see External System Integration.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

- RTSP — Requires a device account (Basic), unicast (TCP, UDP)
- WebRTC — Requires a device account
- ROS 2 — Includes a video topic (JPEG, 25 Hz)
- WebSocket — Requires a device account

※ A device account is required to receive RTSP, WebRTC, WebSocket, ONVIF snapshots, and event files. An administrator can disable authentication for these streams. ONVIF device discovery and queries, Modbus TCP, and ROS 2 (including the video topic) do not require authentication.

Environment

- Operating temperature — -20 ~ 50 °C
- Storage temperature — -40 ~ 70 °C
- Operating humidity — 93 % RH at 30 °C, non-condensing
- Ingress protection — IP68

Package Contents

The standard package contains the following items.

- BATCAM FX2 main unit
- DC to Pigtail cable, 0.5 m
- LAN cable (CAT6, 0.5 m)
- 485 to Pigtail cable (485 to USB converter)
- Waterproof PoE connector
- Standard installation kit (swing mount)
- DC 12 ~ 24 V adapter
- Quick manual, product inspection report

Certifications and Tests

- Product certifications — CE, FCC, KC, RoHS
- Shock test — 15 g, 11 ms (Half-sine), three times in each of six directions (KS C IEC 60068-2-27)
- Vibration test — MIL-STD-810H Method 514.8, Category 4 (vertical 1.08 g rms, lateral 0.21 g rms, longitudinal 0.76 g rms, one hour each)
- Temperature test — -20 ~ 50 °C (KS C IEC 60068-2-1, 60068-2-2)
- Humidity test — 30 °C, 93 % RH, 24 hours (KS C IEC 60068-2-78)

Specifications are subject to change without notice to improve the product.

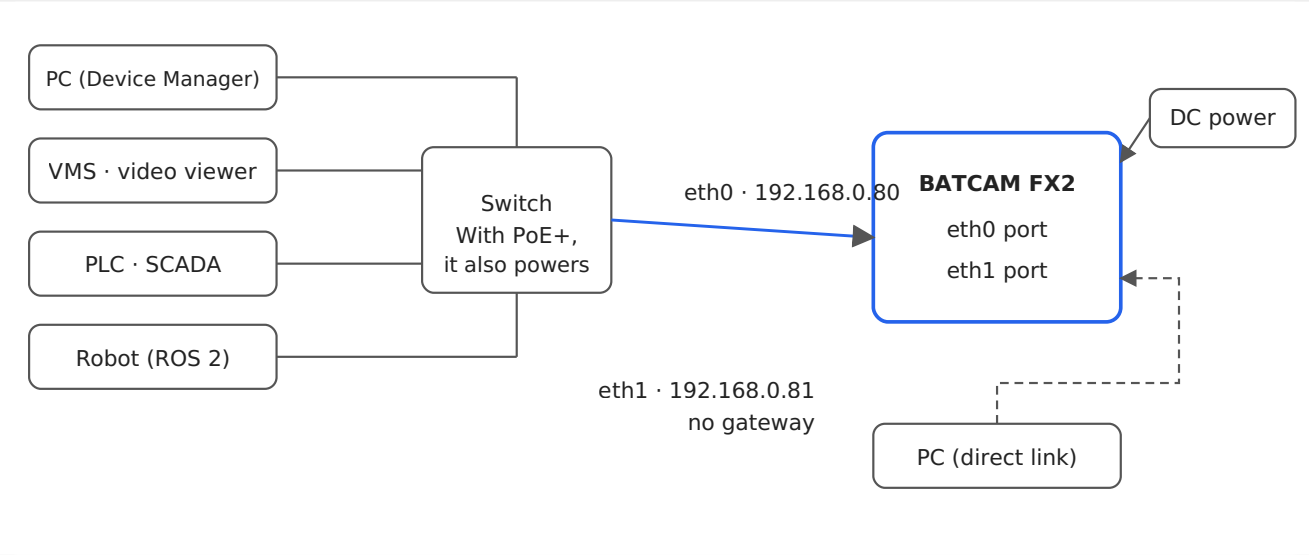
Installation

This guide explains how to connect the BATCAM FX2 to a network and power source, choose an installation location, and mount the device. Read the safety and handling precautions before installation.

System configuration

The BATCAM FX2 is a network device. Connect it to a PC, switch, or server with an Ethernet cable. It has two Ethernet ports: eth0 and eth1.

- eth0 port — Connects to a PC, VMS, PLC, or robot through a switch. Its factory-default address is 192.168.0.80.
- eth1 port — Connects directly to a PC. Its factory-default address is 192.168.0.81, and it has no gateway.



The connector labeled PoE on the multi-cable is the eth0 port. PoE+ power is supplied through this connector.

- Use a CAT5e or higher UTP cable. A length of 80 m or less is recommended.
- A Gigabit Ethernet connection is recommended for video and Device Manager access.
- Fiber-optic cable is recommended for distances over 80 m.

Power supply options

1) Using PoE+

Connecting to a PoE+ (IEEE 802.3at) switch or injector supplies both data and power over a single Ethernet cable. This is suitable for outdoor or elevated locations where separate power wiring is difficult.

2) Using DC power

If DC power is available at the installation location, supply 12–24 V DC. Use only power supplies and cables that meet the specified requirements.

The device boots when power is connected. Measurement begins when the status LED turns green.

Mounting the device

The device can be mounted in two ways.

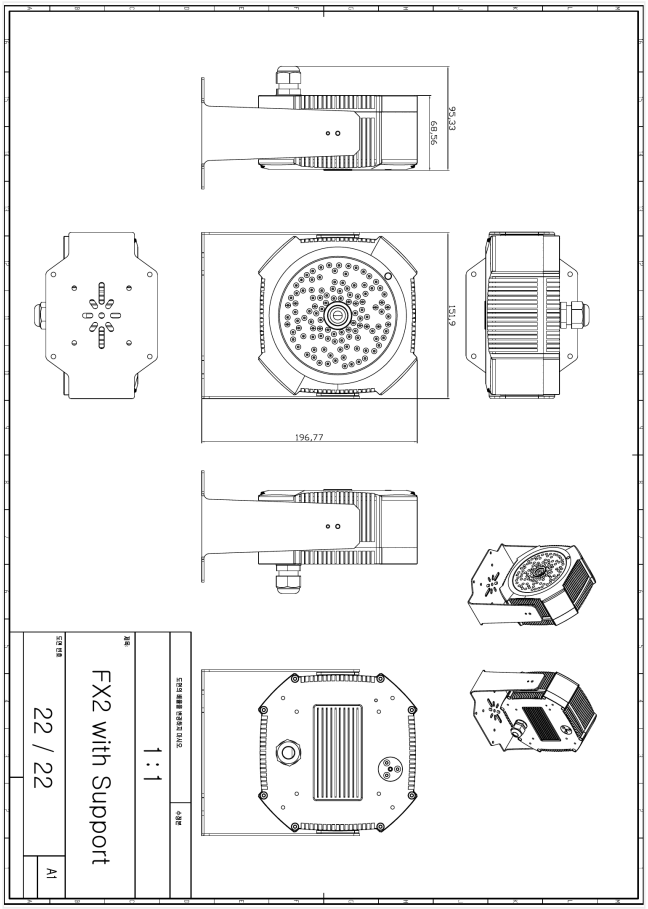
1) VESA 75 / VESA 100

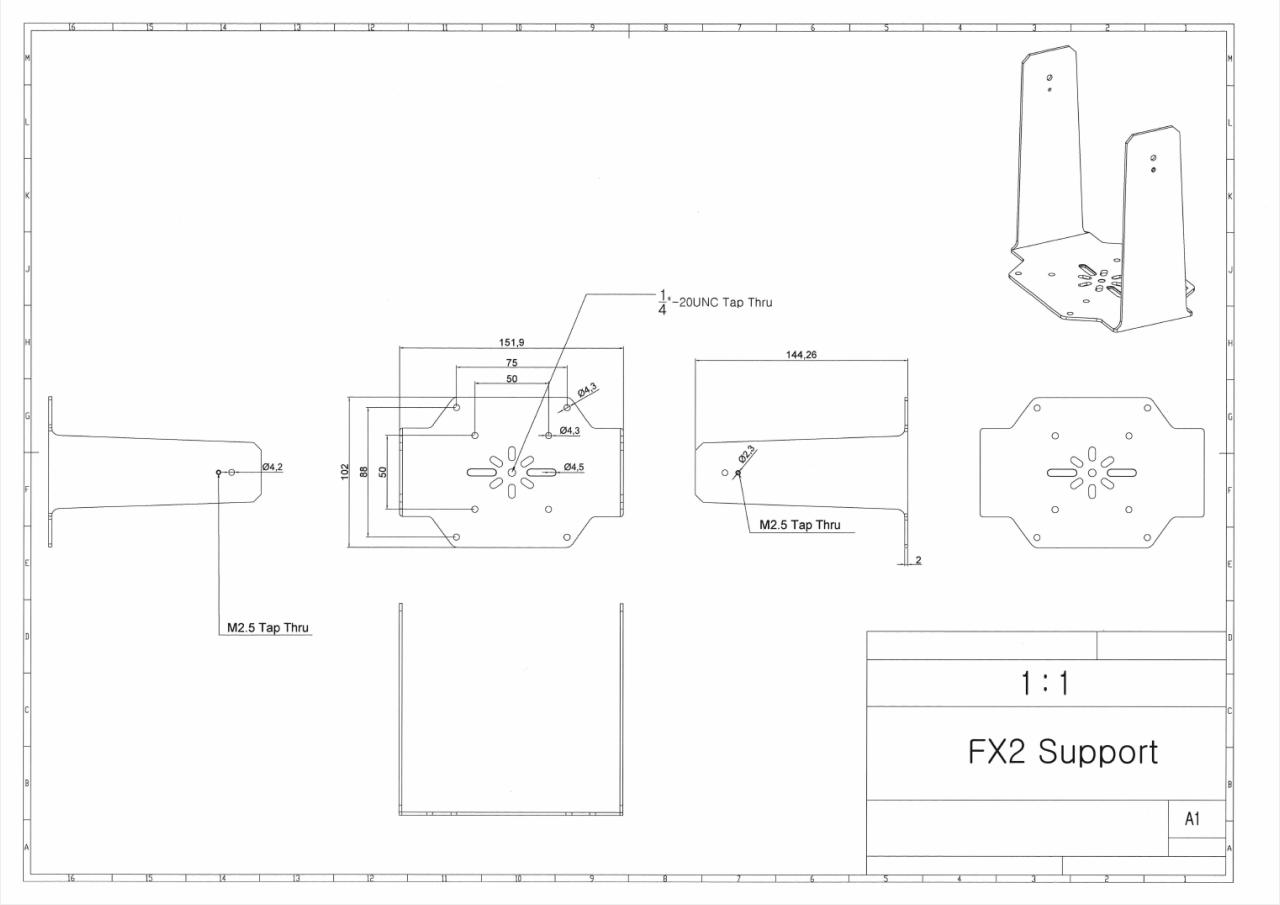
Bolt a commercially available mount to the VESA 75 or VESA 100 threaded holes on the rear. Make sure the mount can adequately support the device's weight (approximately 1,245 g).

2) Dedicated bracket

The standard installation kit (swing mount) allows you to adjust the installation angle. Use only the bracket and bolts included in the kit. Tighten the left and right fixing screws securely.

With the dedicated bracket installed, the overall dimensions are 151.9 mm wide, 196.77 mm high, and 95.33 mm deep.





Installation location and field of view

Position the device and set its distance so that the measurement target is centered on the screen and the area to be monitored falls within the field of view. Areas outside the field of view cannot be seen in the image.

At a 100% field-of-view setting, the default horizontal fields of view for the firmware are as follows.

- SMIA462 Wide — 124.07°
- SMI3708 Wide — 101.6°

Each device is calibrated before shipment, so actual values may vary slightly. See Camera Settings for the values at 67%, 50%, and 33% field-of-view settings.

Pre-release software (v1.1.1-beta.1)

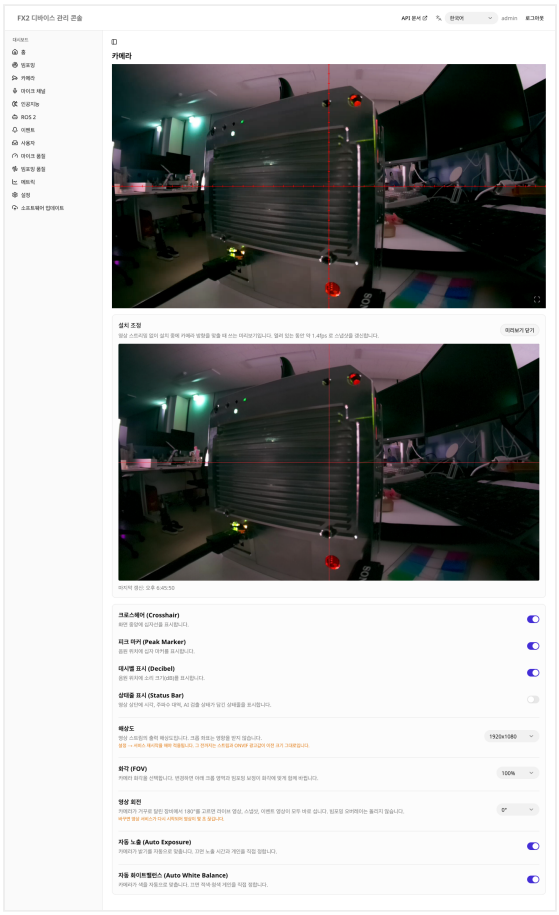
This information is based on firmware v1.1.1-beta.1 and may change in the official release.

For an SMIA462 Wide device without device-specific calibration values, the default horizontal field of view at the 100% setting is 123.78°.

In the camera menu, you can select “100%”, “67%”, “50%”, or “33%” under “Field of View (FOV)”. Lower values magnify a narrower area.

Aligning the device

During installation, turn on “Crosshair” in the camera menu and align the measurement target with the red crosshair at the center of the screen. Select “Open Preview” under “Installation Adjustment” to check the alignment using snapshots that update at approximately 1.4 fps without video streaming.



For details, see Camera Settings.

Cables and waterproofing

- The device has an IP68 water- and dust-resistance rating.
- For outdoor installations, an additional waterproof junction box is recommended around the multi-cable connector joints.
- For outdoor installations, use the included waterproof PoE connector to protect the Ethernet connector from water and dust.

Installation precautions

- Do not disconnect or connect cables while power is supplied.
- Do not obstruct the front of the microphone array or the camera lens.
- Avoid locations exposed to prolonged direct sunlight or continuous strong vibration.
- Before connecting multiple devices to the same network, assign a different IP address to each device. For details, see Connecting for the First Time.

First Connection

You can connect to a factory-default BATCAM FX2 from a PC for the first time, change the password, and complete the initial setup. Install the device and connect power before proceeding.

1. Factory-default network

The factory-default Ethernet port settings are as follows.

- eth0 port — IP 192.168.0.80, subnet mask 255.255.255.0, gateway 192.168.0.1
- eth1 port — IP 192.168.0.81, subnet mask 255.255.255.0, no gateway

The eth1 port is intended for a direct PC connection. Even though both ports are on the same subnet (192.168.0.x), connect using the address of the port to which the cable is plugged in.

2. Set up the PC network

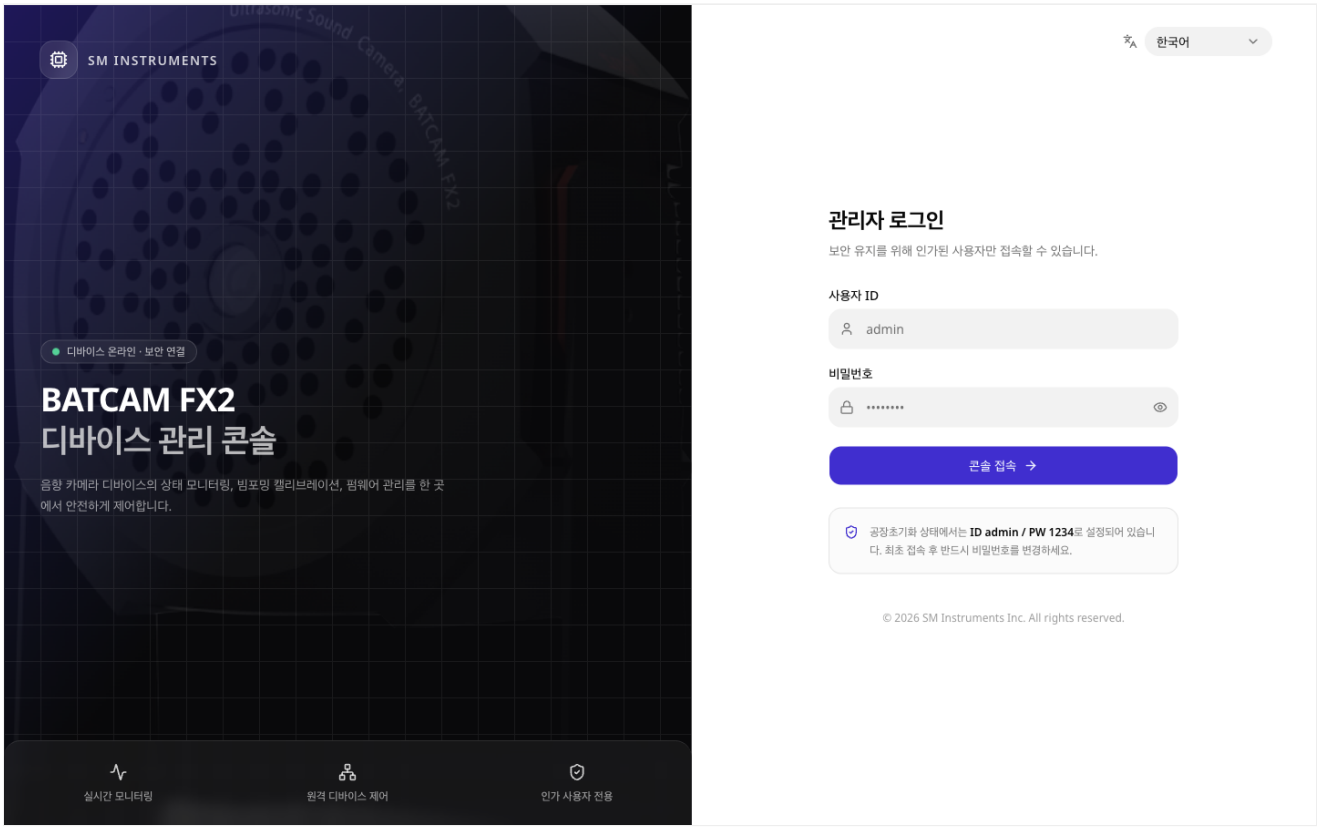
Set the PC's wired network to the same 192.168.0.x subnet as the device. For example:

- IP address — 192.168.0.10
- Subnet mask — 255.255.255.0

Connect the PC and device directly with an Ethernet cable or connect them to the same switch. Choose a PC address that does not conflict with the device addresses (192.168.0.80, 192.168.0.81).

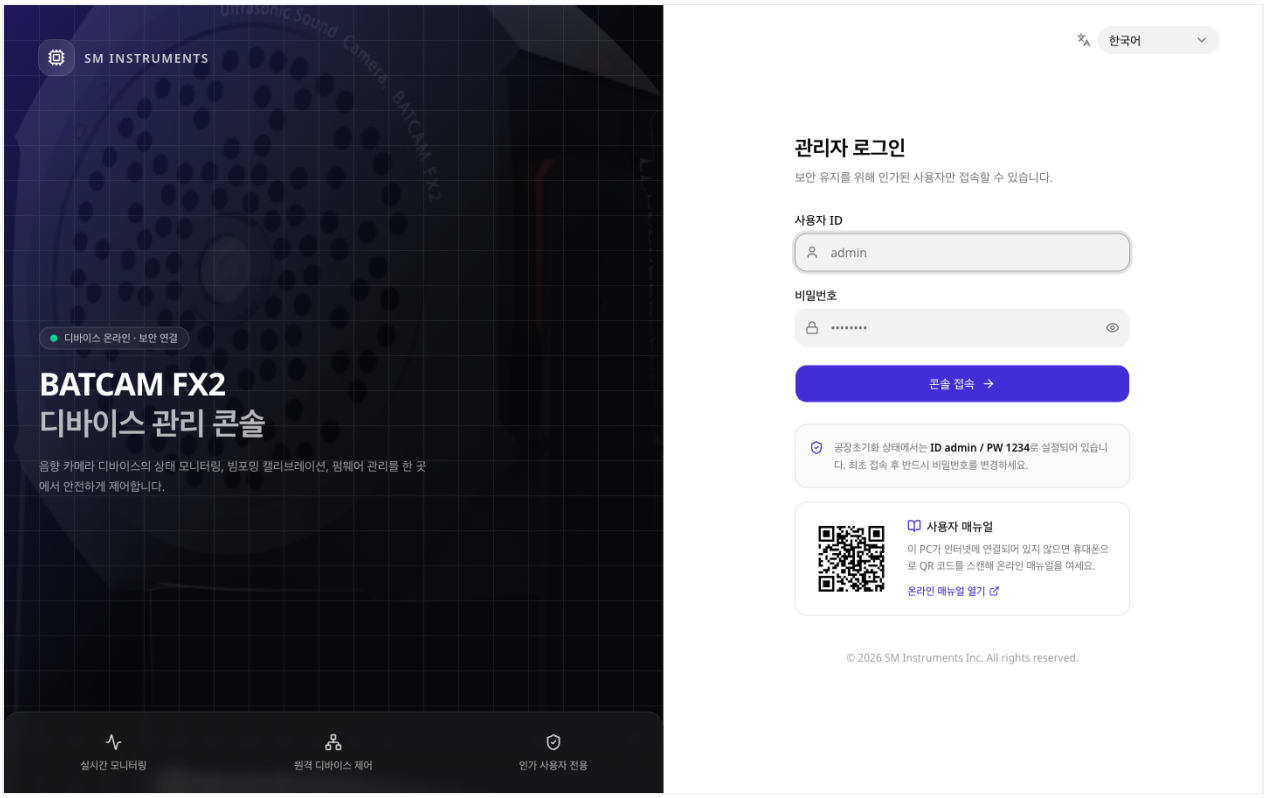
3. Connect

Enter `http://192.168.0.80` in the PC's web browser address bar. The login screen opens.



Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.



The v1.1.1 login screen has a “User Manual” link and QR code. If you cannot open the online manual on a PC connected directly to the device, scan the QR code with a phone that has internet access.

※ The device is accessible only over HTTP. There is no HTTPS address.

4. Log in

The factory-default administrator account has the ID `admin` and password `1234`. The same values appear in the instructions below the login form. Enter them in “User ID” and “Password,” then click “Console Login.”

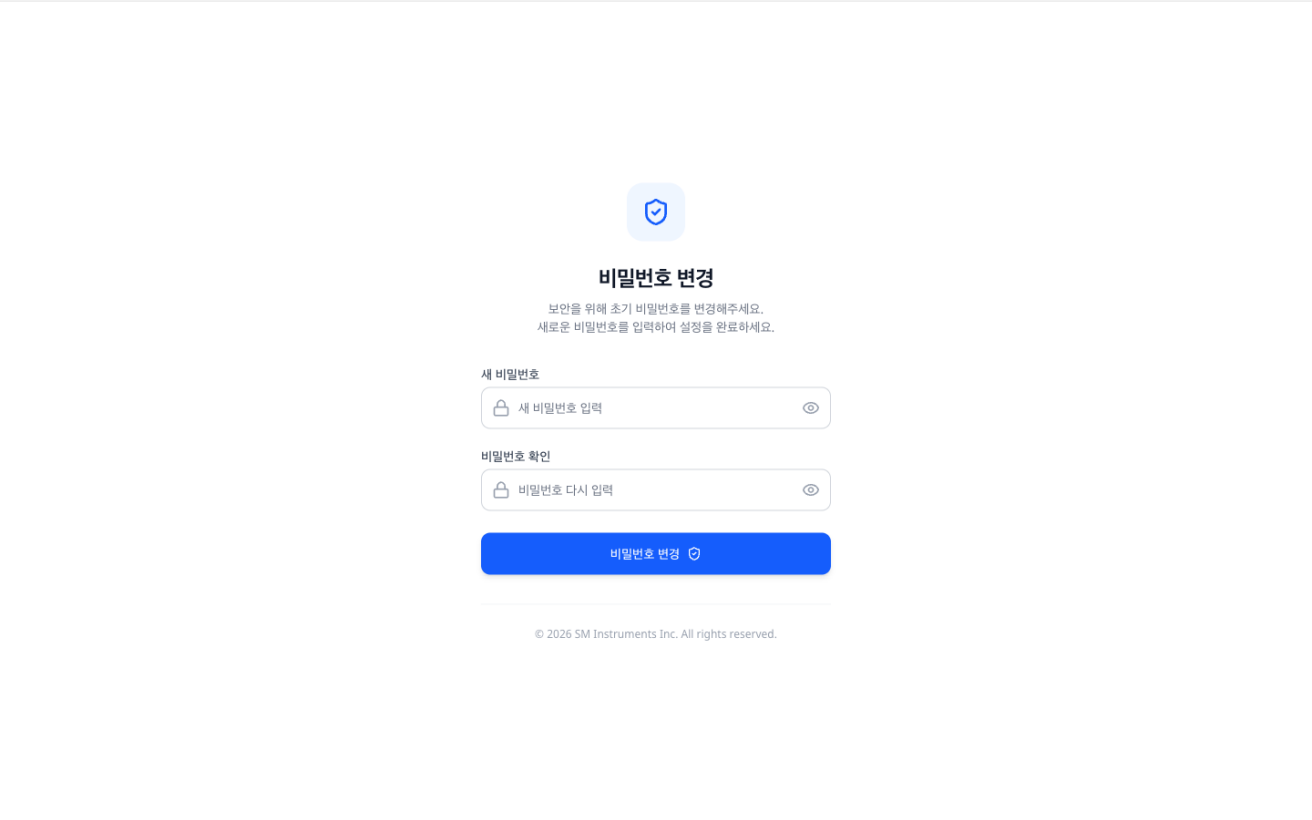
After you log in, Device Manager opens. The screen title is FX2 Device Management Console. The login remains valid for 24 hours.

※ If login fails, an error message may appear in English.

For details, see Device Manager Screen Layout.

5. Change the password

When you log in with the initial password (`1234`), you are automatically taken to the “Change Password” screen. Enter the same value in “New Password” and “Confirm Password,” then click “Change Password.” After the change, you are immediately logged in with the new password and Device Manager opens.



- The password must be at least 4 characters long.
- You cannot reuse the initial password (`1234`).
- Changing a password requires administrator privileges. Standard user accounts cannot change their own passwords. An administrator must change them in the User menu.

※ This screen opens automatically only when you log in with the initial password. You can use Device Manager without changing the password, but you must change it after the first connection.

For details, see User Accounts and Permissions.

6. Initial settings

Configure the following settings in order. You must be logged in with an administrator account.

1) Time

Under Settings → Time Settings, click the gear button to set the time zone and time server (NTP). Event timestamps and AI operating hours are based on the device time.

※ BATCAM FX2 does not have an RTC (built-in clock). If power is turned off while the device is not connected to a time server (NTP), it loses the device time. Without NTP, the device time starts at 1970-01-01T00:00:00 when power is turned on. Specify a time server the device can access. On an isolated network without an external connection, use a local time server.

2) Network and IP address

To install multiple devices on the same network or match the site network, go to Settings → Network Settings and use the gear button at the end of the eth0 or eth1 row to change its address. For “Connection Method,” choose “Automatic (DHCP)” or “Manual Configuration.”

If you change the address you are currently using to connect, a “Connection will be lost” confirmation dialog appears. Clicking “Apply” disconnects this screen from the device. After applying the change, reconnect using the new address. If you switch to “Automatic (DHCP),” check the DHCP server for the device’s new address.

- Enter IP addresses without leading zeros. Example: 192.168.0.10
- Changing a port other than the one you are using to connect does not disconnect you.

For details, see System Settings.

3) Camera field of view and installation check

Check the video in the Camera menu and set the field of view. Adjust the device’s orientation so that the measurement target is centered on the screen. For details, see Camera Settings.

4) Check event triggers

Under Events → Trigger Conditions, check the conditions under which events are saved. For details, see Events.

7. Install multiple devices

All factory-default devices use the same addresses. Before connecting them to the same network, connect each device one at a time and assign it a unique IP address. Address conflicts make connections unstable.

Device Manager Screen Layout

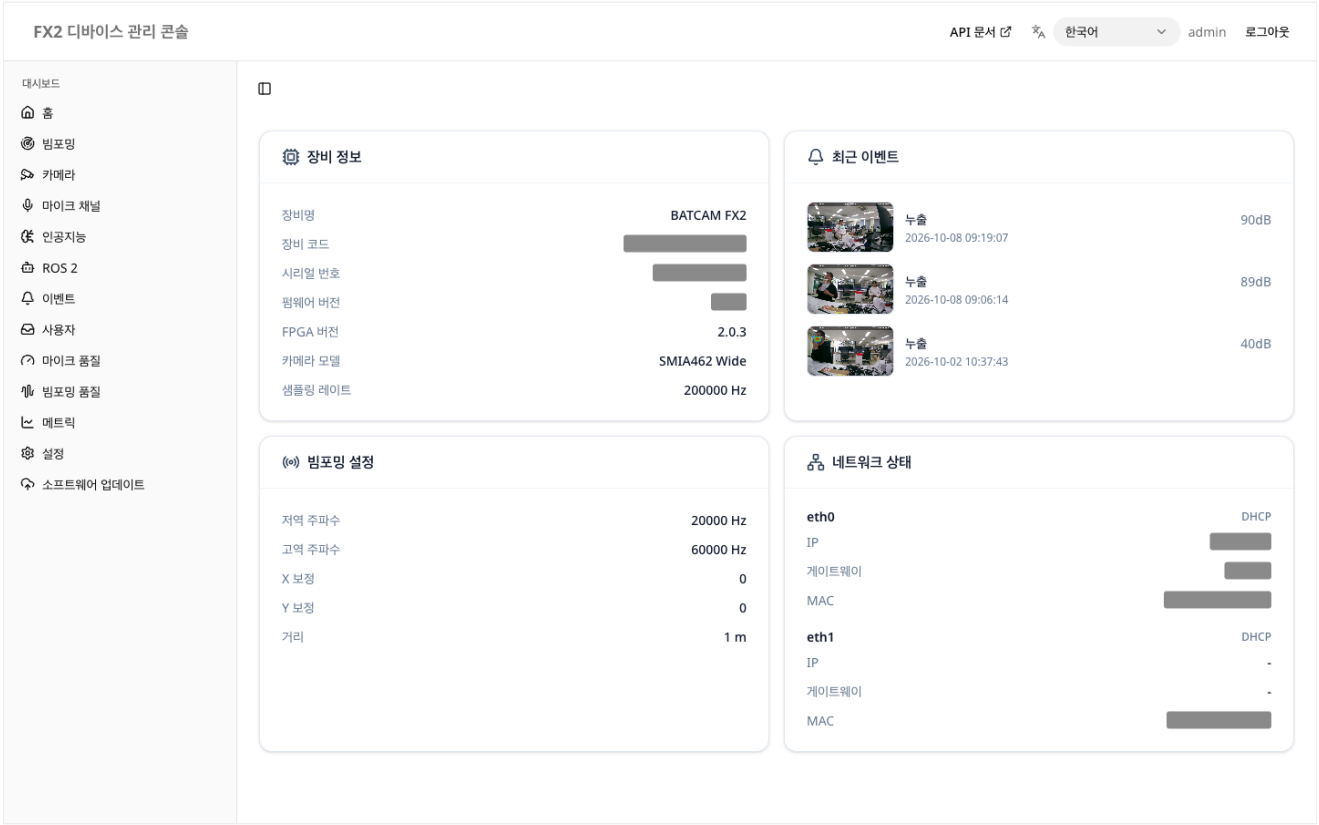
Device Manager is a web-based management interface built into the BATCAM FX2. You can access it in a browser to view video, change settings, review events, and update firmware. This page describes the screen layout and the information shown on the Home screen.

What is Device Manager?

Device Manager is built into the device, so you only need a browser; no separate program is required. The screen title is FX2 Device Management Console. The browser tab has the same title.

- Connection — Enter the device address in a browser (HTTP, port 80)
- Minimum screen width — 768 px
- Browser — Device Manager can be used with Chrome 157 for macOS.

※ For instructions on connecting for the first time, see First Connection.

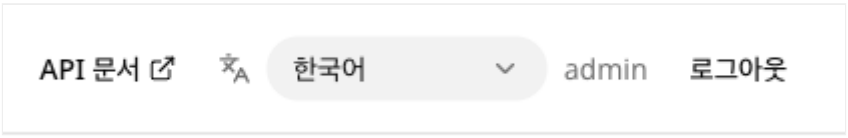


Top bar

The top bar appears at the top of every screen except the login and password change screens. Select the title on the left to go Home. The following items appear on the right, in order.

- API Documentation — Opens the device's REST API documentation in a new tab.
- Language Selection — Changes the interface language.
- Account ID — Shows the account currently logged in.

- Log Out — Returns to the login screen.



For more about the API documentation, see API and Development Integration.

Menu

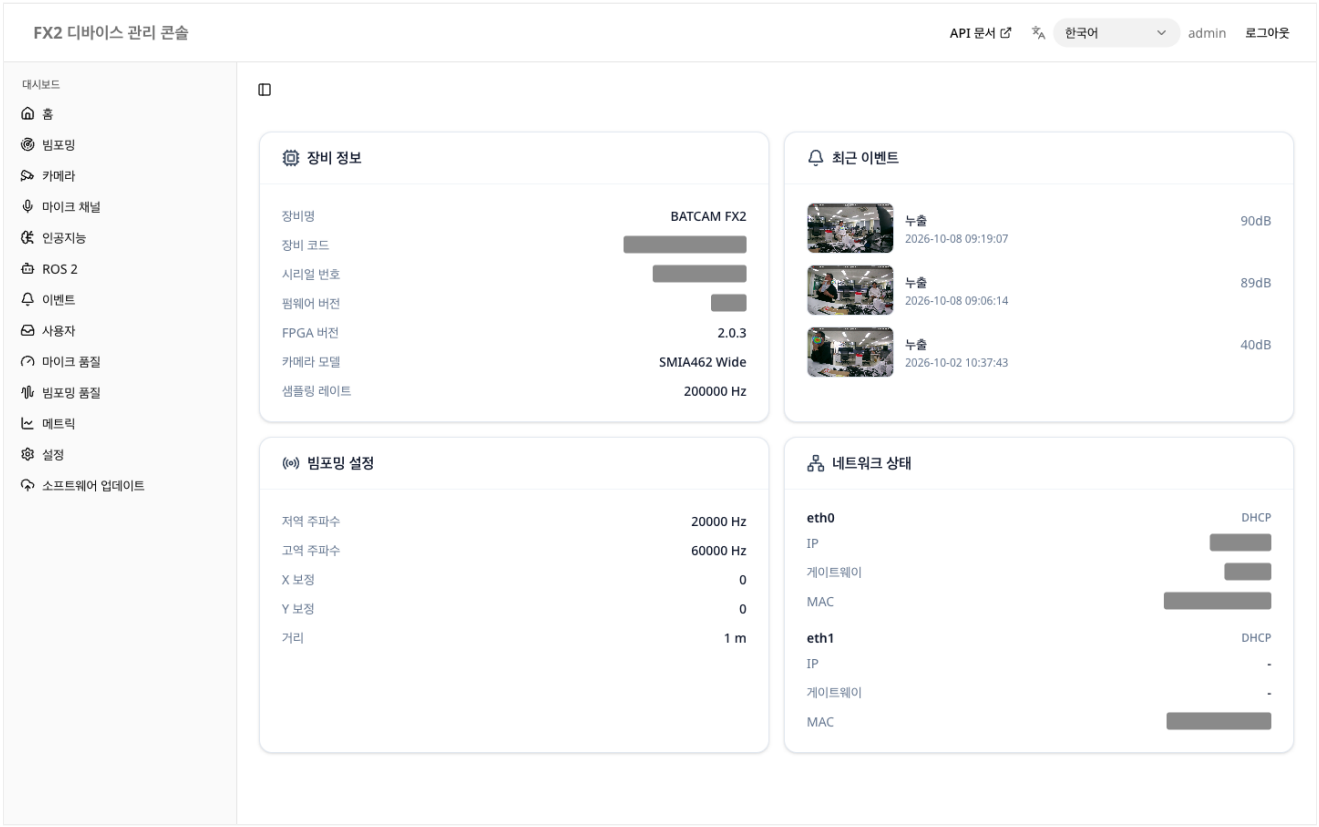
There are 13 menu items on the left side of the screen. Administrator and standard user accounts see the same menu. Use the icon beside the menu to collapse or expand the list.

- Home — Shows device information, recent events, beamforming settings, and network status on one screen. This page describes it.
- Beamforming — Configures live video, measurement band, overlay display, and ROI. For details, see Live Video and Beamforming.
- Camera — Configures field of view, image rotation, resolution, exposure, white balance, and focus. For details, see Camera Settings.
- Microphone Channel — Shows the waveform and spectrum of one microphone channel and turns the 40 kHz reference signal on or off. For details, see Microphone Check.
- AI — Configures leak AI and partial-discharge AI. For details, see AI Detection.
- ROS 2 — Sets the ROS 2 domain ID that the device joins. For details, see ROS 2 Integration.
- Events — Displays saved events and configures triggers. For details, see Events.
- Users — Adds and deletes accounts and changes passwords. For details, see User Accounts and Permissions.
- Microphone Quality — Checks sensitivity variation and noise across 112 microphone channels. For details, see Microphone Check.
- Beamforming Quality — Shows a numerical measure of contrast in the beamforming results. For details, see Microphone Check.
- Metrics — Graphs CPU load, temperature, core frequency, and humidity. For details, see System Settings.
- Settings — Covers network, time, language, service restart, and factory reset. For details, see System Settings.
- Software Update — Uploads firmware and FPGA updates. For details, see Firmware Update.

※ The menu item and screen title differ in two places. The screen title for “Microphone Channel” is “Microphone,” and the screen title for “Metrics” is “System Metrics.”

Home screen

Home consists of four cards. Information is loaded only once when you open the screen. Refresh the browser to see updated values.



1. Device Information

Shows values that identify the device.

- Device name
- Device code
- Serial number
- Firmware version — Shows the version of the currently installed firmware.
- FPGA version — Shows “-” if no value is available.
- Camera model — Shows “SMIA462 Wide” or “SMI3708 Wide,” depending on the device’s camera. If the camera cannot be found, it shows “Not detected.”
- Sampling rate — 200000 Hz

2. Recent Events

Shows the three most recent events. Each event displays a thumbnail, type, level (dB), and creation time.

- Type — Automatic save, level trigger, leak, discharge
- Time — Based on the time zone set on the device
- If there are no events, “No recent events.” is displayed.

For more about events, see Events.

3. Beamforming Settings

Shows the current beamforming values as read-only information. You cannot change them on this card.

- Low frequency, high frequency — The current measurement band
- X correction, Y correction, distance — Values calibrated at the factory for each field of view

※ Changing the field of view also changes the X correction, Y correction, and distance values. Change the measurement band in the Beamforming menu and the field of view in the Camera menu.

※ If the device cannot read the values, X correction, Y correction, and distance are shown as “-”.

4. Network Status

Shows the connection method (Static or DHCP), IP address, gateway, and MAC address for the eth0 and eth1 ports. This card is shown only to administrator accounts. Standard user accounts see “Unable to load information.”

For instructions on changing network settings, see System Settings.

Language

Choose the interface language from 한국어, English, 简体中文, 日本語, and Tiếng Việt.

- Change it using Language Selection in the top bar or Settings → Language Settings.
- The page reloads when you make a selection.
- The selected language is stored in a browser cookie for one year. It applies separately to each browser used to access the device; it is not a device-wide setting.
- On your first visit, the interface follows the browser language. If that language is not supported, the interface is shown in Korean.

Login Duration and Log Out

Your login remains valid for 24 hours. After 24 hours, you must log in again. Selecting “Log Out” in the top bar clears the login information from this browser and returns you to the login screen.

After a factory reset, the browser used to perform the reset is logged out and taken to the login screen. In firmware v1.1.0, logins in other browsers remain valid for up to 24 hours after they were issued.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

After updating the firmware to v1.1.1 or performing a factory reset, all logins end. You must log in again.

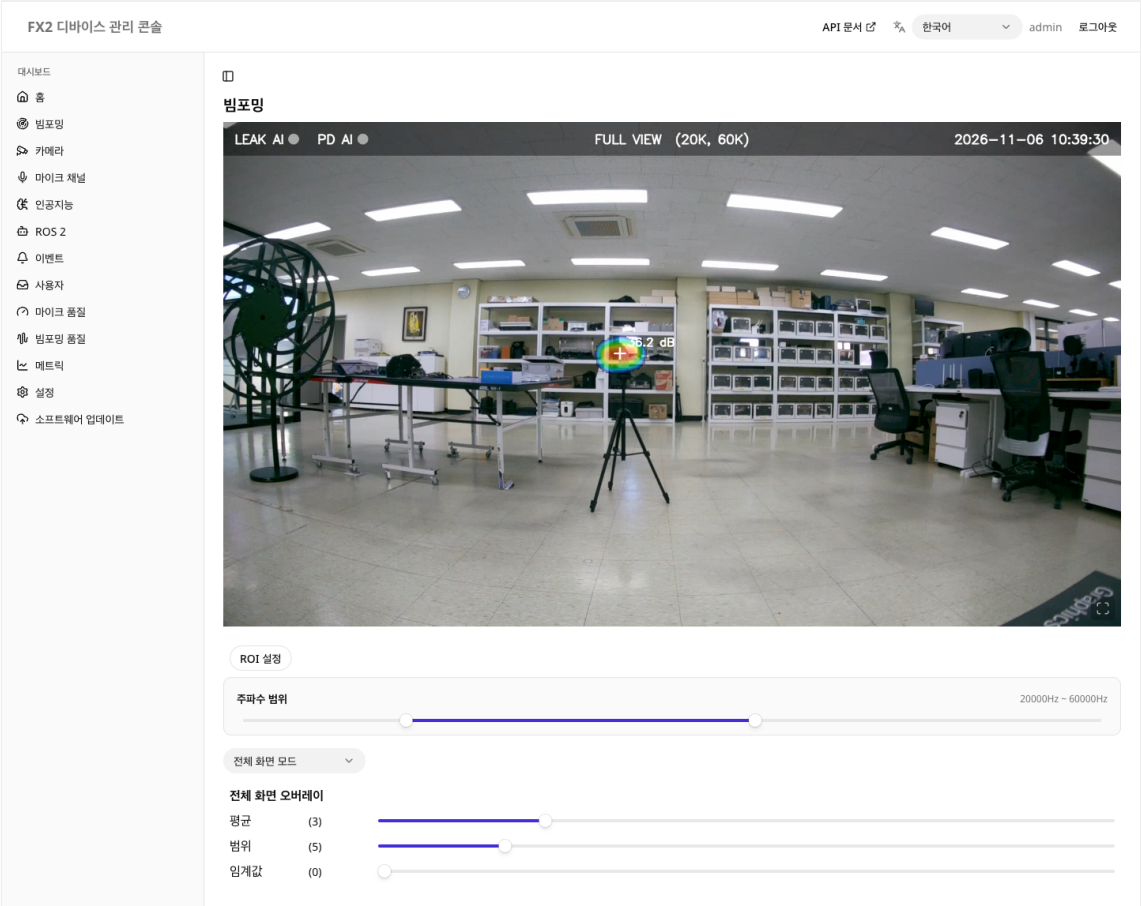
Account Permissions

There are two account types: administrator and standard user. Both accounts see the same menu. Restarting services, performing a factory reset, uploading firmware, and managing accounts require administrator permissions.

For details, see User Accounts and Permissions.

Live Video and Beamforming

In the Beamforming menu, you can view live video from the device and a sound-intensity heatmap. Set the measurement band, overlay display mode, and regions of interest (ROIs) on this screen.



Live video

Video is sent directly from the device to the browser over WebRTC. The device draws the heatmap, peak markers, ROI boxes, and status bar on the video before sending it. The browser does not draw them separately.

- Video address — port 8889 at the device address
- Required connections — TCP port 8889 and a UDP port (8189 by default)
- Simultaneous viewing — up to 10 connections

※ Video will not appear if a firewall or router blocks these ports.

Use the icon at the bottom right of the video to enter or exit full screen.

Before the video appears, one of the following messages is displayed.

- “Connecting to camera...” — A video connection is being attempted.
- “Waiting to receive video...” — The connection is established, and the first video frame is pending.

- “Disconnected. Reconnecting…” — The connection was lost and is being re-established. The retry interval starts at 1 second and increases to a maximum of 15 seconds.

Status bar

This is the strip at the top of the video. It displays the following information on the left, center, and right.

- Left — Colored dots appear next to “LEAK AI” and “PD AI.” Gray means off, green means running with no detection, and red means a detection. During a detection, the type is also shown: “Leak” for leaks, and “Corona,” “Floating,” or “Surface” for partial discharge.
- Center — The display mode (“OVERLAY OFF,” “MULTI SOURCE,” or “FULL VIEW”) and measurement band. The band is shown as a low and high value in parentheses, such as “(20K, 60K).”
- Right — Device time (YYYY-MM-DD HH:MM:SS)

※ Turn the status bar on or off using “Show Status Bar” in the Camera menu. See Camera Settings for details.

Peak markers and levels

A peak marker (white cross) and level (dB) appear at the strongest sound source. Up to three can be displayed. Peak markers and levels can each be turned on or off in the Camera menu.

When AI is on and there is no detection, the heatmap appears gray. Colors appear when there is a detection. If all AI functions are off, the heatmap always appears in color.

In firmware v1.1.0, the heatmap is drawn progressively farther inward than the peak marker toward the edges of the video.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information applies to firmware v1.1.1-beta.1 and may change in the official release.
>
> The heatmap appears at the same position as the peak marker even at the edges of the video. Peak position values do not change.

Measurement band

Use the “Frequency Range” slider to set the frequency band used for beamforming calculations. The current values appear above the slider, for example, “20000Hz ~ 60000Hz.”

- Selectable range — 2 kHz ~ 98.9 kHz
- Adjustment increment — 100 Hz
- Default — 20 kHz ~ 60 kHz
- When saved — Immediately upon releasing a handle. There is no Save button.

The saved band persists after a reboot.

※ Setting the slider to its far right end (99 kHz) does not save the value; it reverts to the previous value. Use no more than 98.9 kHz for the upper value.

※ Setting both handles to the same value does not save either. The lower value must be less than the upper value.



Band lock while AI is running

While AI is running, the slider is disabled and “The frequency range cannot be changed while AI is running.” appears. Turn off AI or wait until its operating period ends before changing the band.

※ The lock state is checked once when the screen opens. If the lock does not appear after AI is turned on, refresh the page.

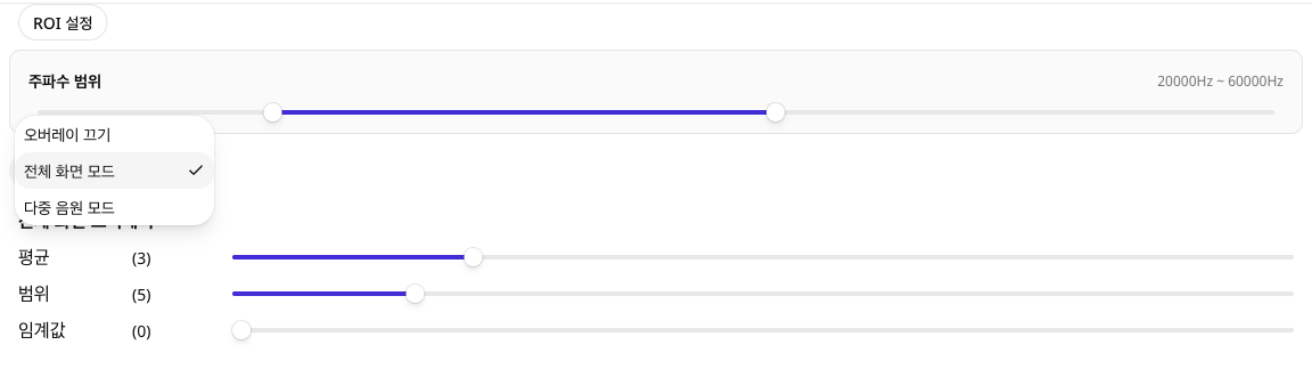
See AI Detection for the relationship between AI and the band.

Overlay display

A list lets you choose the overlay display mode. Your selection is saved immediately and applied to the video at once.

- Overlay Off — Does not draw the heatmap.
- Full View Mode — Draws the heatmap across the entire video. This is the default.
- Multi-Source Mode — Draws the heatmap only around the strongest sound sources.

※ The overlay setting changes only what is drawn on the screen. Peak search, level triggers, AI decisions, and event recording continue to operate even when the overlay is off.



Full View Mode

There are three sliders under “Full View Overlay.” Changes are saved when you release a handle.

- Average — 1 ~ 10, default 3. Higher values make the display steadier but slower to respond.
- Range — 0 ~ 30, default 5. Sets the upper end of the heatmap color scale this amount below the highest level (dB). At 0, only the threshold is applied.
- Threshold — 0 ~ 50, default 0. Levels at or below this value are not colored on the heatmap.

Multi-Source Mode

Under “Multi-Source Overlay,” there is a source-count list and two sliders. This mode displays up to three sound sources, starting with the strongest, each as a separate patch.

- Source Count — Choose 1, 2, or 3. The default is 3. Your selection is saved, but it does not limit the number of sources shown in the video. If there are multiple sources, up to three may appear even when you select 1.
- Average — 1 ~ 10, default 3
- Threshold — 0 ~ 50, default 0

This mode has no “Range” slider.

Threshold and peaks

※ The threshold does more than control heatmap coloring. Sound sources weaker than the threshold are not shown as peak markers or used in level-trigger comparisons.

※ If you set the threshold higher than the level-trigger value, the level trigger will not activate.

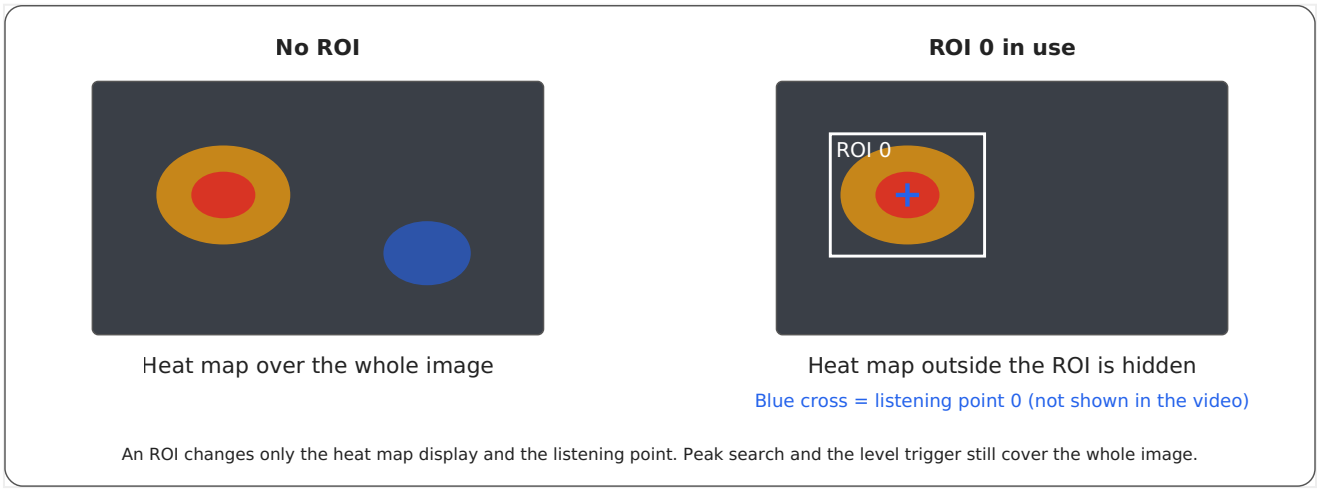
See Events for level triggers.

ROI settings

An ROI is a rectangular region defined on the video. You can define up to three (ROI 0, ROI 1, and ROI 2).

Using ROIs has the following effects.

- ROIs appear as white boxes on the video.
- If at least one ROI is enabled, the heatmap outside the boxes is cleared.
- Listening point n points toward the center of ROI n. Listening points are used for AI decisions and event audio (WAV).

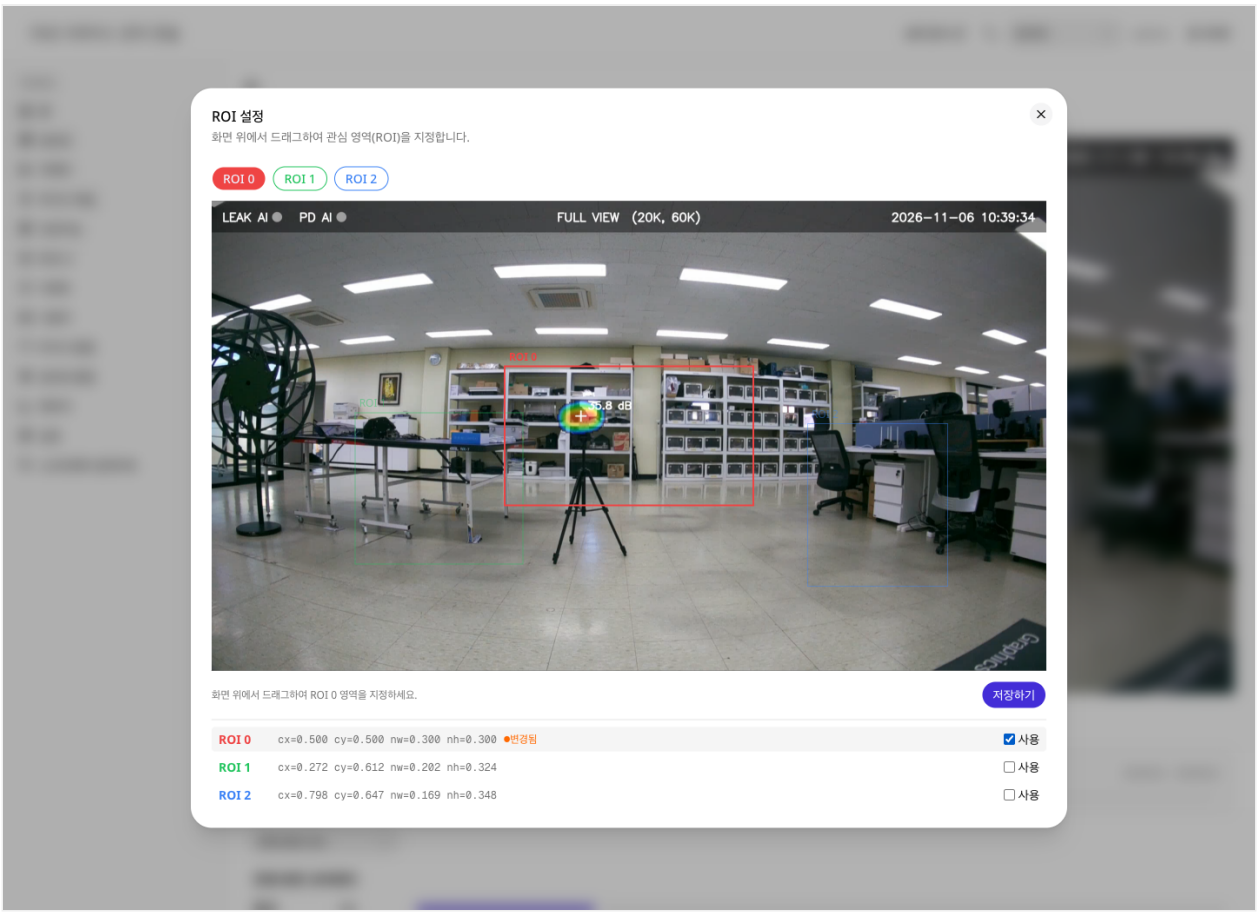


※ ROIs do not limit the area used for peak search or level triggers. The strongest sound source anywhere in the video is identified as a peak and used for event decisions.

1. Open the ROI settings dialog

Click the “ROI Settings” button beside the video. A still frame captured when you click the button appears for defining the regions.

- If the still frame cannot be captured, “Unable to capture screenshot (check video connection)” appears and you cannot define a region. Check that the video is playing, then open the dialog again.



2. Choose an ROI number

Choose “ROI 0,” “ROI 1,” or “ROI 2.” In the dialog, they are distinguished by red, green, and blue, respectively.

※ These colors appear only in the settings dialog. On the video, all ROIs appear as white boxes.

3. Define a region

Drag on the still frame to draw a rectangle. Dragging again moves the selected ROI to the new region. Drags smaller than 3 px do not define a region.

- The list below shows each ROI’s center (cx, cy) and size (nw, nh) as values between 0 and 1.
- Unsaved changes are marked “●Changed.”

4. Turn on “Use”

Select “Use” in the list for each ROI you want to enable. An ROI is not applied to the video unless “Use” is selected, even if you have drawn its region.

5. Save

Click “Save” to save only the ROIs you changed.

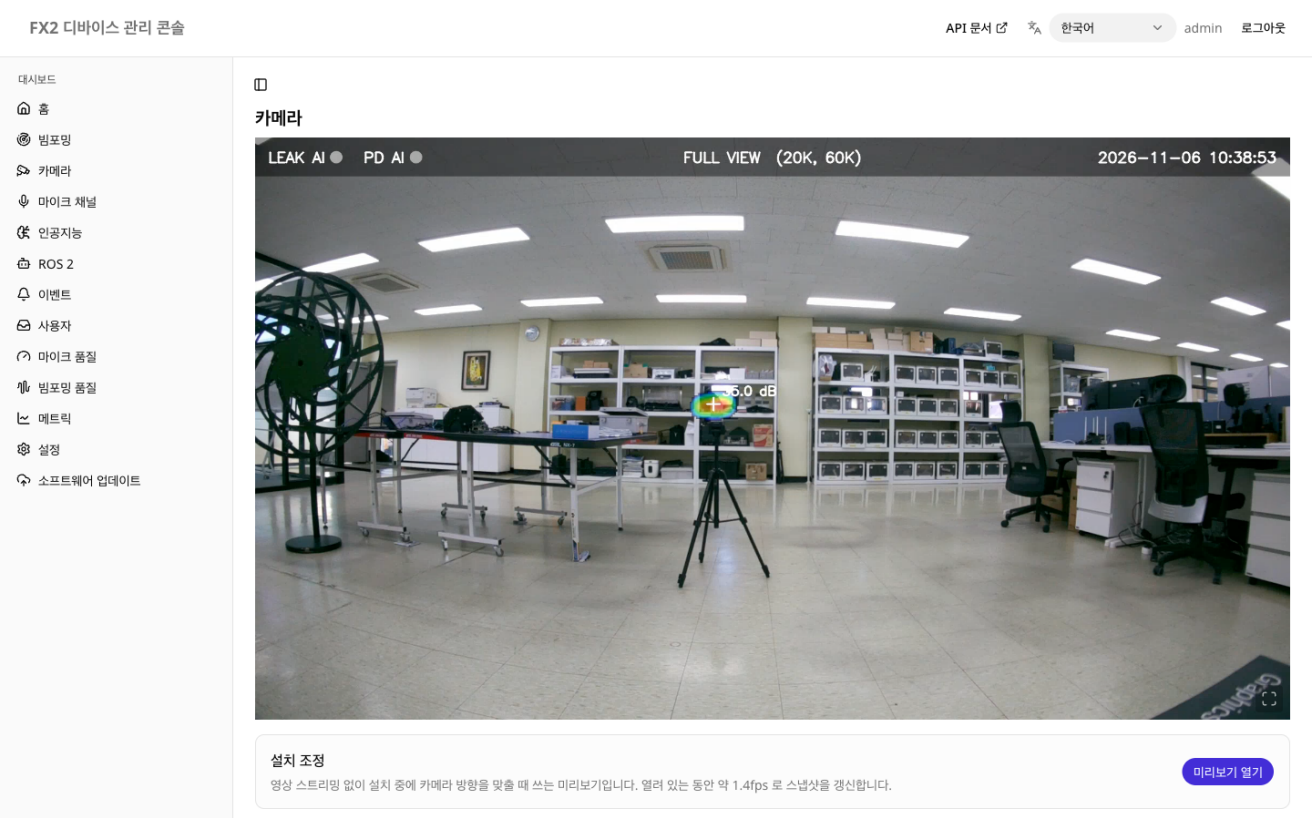
- The result appears with the ROI number, such as “ROI 0 saved.”
- If nothing changed, “No changes.” appears.
- If only some ROIs are saved, “Partial failure - Succeeded: … / Failed: …” appears.

※ Closing the dialog without saving discards your changes.

Camera Settings

In the Camera menu, configure what appears in the video, field of view, image rotation, resolution, brightness and color, and focus. During installation, you can use the installation alignment preview to aim the device.

From top to bottom, the screen shows live video, the “Installation Alignment” panel, and the settings.



How settings are saved

There is no Save button in the Camera menu. Switches, selection lists, and sliders save changes automatically.

- Switches and selection lists — saved as soon as you choose a value
- Sliders — saved when you release the handle. While dragging, a value is applied 0.5 seconds after you stop moving it (exposure time, gain, red and blue gain, and focus distance)

Display options

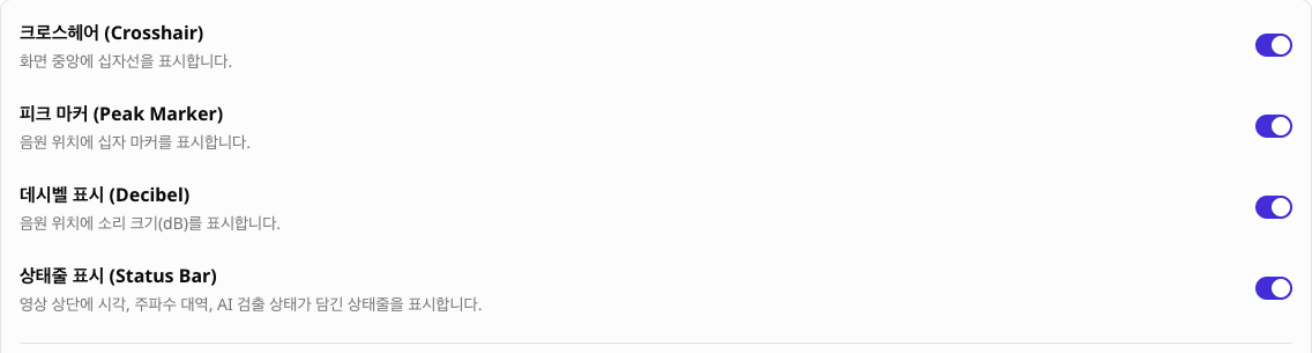
Turn items overlaid on the video on or off. The device draws the three items other than the crosshair directly onto the video. They therefore remain visible in RTSP video, web video, event photos, and event video.

- Crosshair — displays a red cross at the center of the screen. Off by default.
- Peak marker — displays a white cross at the sound source location. On by default.

- Decibel display — displays the level (dB) at the sound source location to one decimal place. On by default.
- Status bar display — displays the time, measurement band, and AI detection status at the top of the video. On by default.

※ The browser draws the crosshair only on the screen. It is not saved on the device and returns to off when you reopen this screen. It is not included in video streams or event video.

※ Turning off the peak marker does not hide the level (dB). Turn off both to hide both.



For details about the status bar and peak marker, see Live Video and Beamforming.

Field of view

Choose the area captured by the device under “Field of View (FOV).” The options are 100 %, 67 %, 50 %, and 33 %; the default is 100 %.

- Smaller values magnify a narrower area.
- Changing the field of view adjusts both the video area and beamforming calibration to match.
- Beamforming uses the calibration set at the factory for each field of view. The X Offset, Y Offset, and Distance values on the Home screen change accordingly.
- Changes are saved immediately.

※ If the device cannot apply the beamforming calibration, the field-of-view change is not saved.

The horizontal fields of view based on firmware defaults are listed below. Actual values may differ slightly because each device is calibrated at the factory.

- SMIA462 Wide — 100 % 124.07°, 67 % 82.71°, 50 % 62.03°, 33 % 41.36°
- SMI3708 Wide — 100 % 101.6°, 67 % 67.74°, 50 % 50.8°, 33 % 33.87°

If device-specific calibration values are unavailable, the default calibration values for that camera model are used.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

The default values have changed for SMIA462 Wide devices without device-specific calibration values. This improves heatmap positioning on those devices.

- SMIA462 Wide — 100 % 123.78°, 67 % 82.53°, 50 % 61.89°, 33 % 41.26°

If device-specific calibration values cannot be used, the Camera screen displays a warning and the reason. The default calibration values for that camera model are then used for the current field of view.

For the relationship between field of view and installation distance, see Installation.



Image rotation

Under “Image Rotation,” choose 0° or 180°. If the device is installed upside down, choose 180° to make the video upright.

- Live video, snapshots, and event video are all rotated.
- Overlays such as the heatmap, peak marker, and status bar are not rotated.
- Changing this setting restarts the video service, interrupting the video for a few seconds.

※ While the video is interrupted after a change, a message may briefly appear in the Installation Alignment panel. It clears automatically after a few seconds.

Resolution

Under “Resolution,” choose the video stream’s output size.

- 1920x1080 — default
- 1600x900
- 1280x720
- 640x360

※ After choosing a resolution, go to Settings → Restart Services to apply it. Until the services restart, the video stream and ONVIF continue to report the previous size.

※ Restarting services requires administrator privileges. For details, see System Settings.

Brightness and color

Exposure, white balance, and focus change the image captured by the camera itself. The changes also appear in event photos and video. They take effect immediately without restarting services.

Exposure

Turn on “Auto Exposure” to let the device adjust brightness automatically. Turn it off to show two sliders.

- Exposure time — displays both a shutter value in “1/N s” format and a value in microseconds (µs).
- Gain — displayed as a multiplier in “×N.N” format.

Both sliders provide finer control at lower values. Their adjustment ranges follow the values reported by the device’s camera.

※ Auto Exposure cannot be turned off on SMI3708 Wide devices running firmware v1.1.0.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information is based on firmware v1.1.1-beta.1 and may change in the official release.
>
> Auto Exposure can also be turned off on SMI3708 Wide devices. If saving fails, a message appears and the screen returns to the device’s actual value.

White balance

Turn on “Auto White Balance” to let the device adjust color automatically. Turn it off to show the “Red Gain” and “Blue Gain” sliders. Values are displayed in “×N.NN” format.

Focus

Turn on “Auto Focus” to let the device adjust focus continuously. Turn it off to show the “Focus Distance” slider. Distances are displayed as “∞,” “50 cm,” or “1.5 m,” with the diopter (D) value in parentheses.

※ Focus settings appear only for camera modules that support focus adjustment. They are available on the SMI3708 Wide camera but not the SMIA462 Wide camera.



When the adjustment range is unavailable

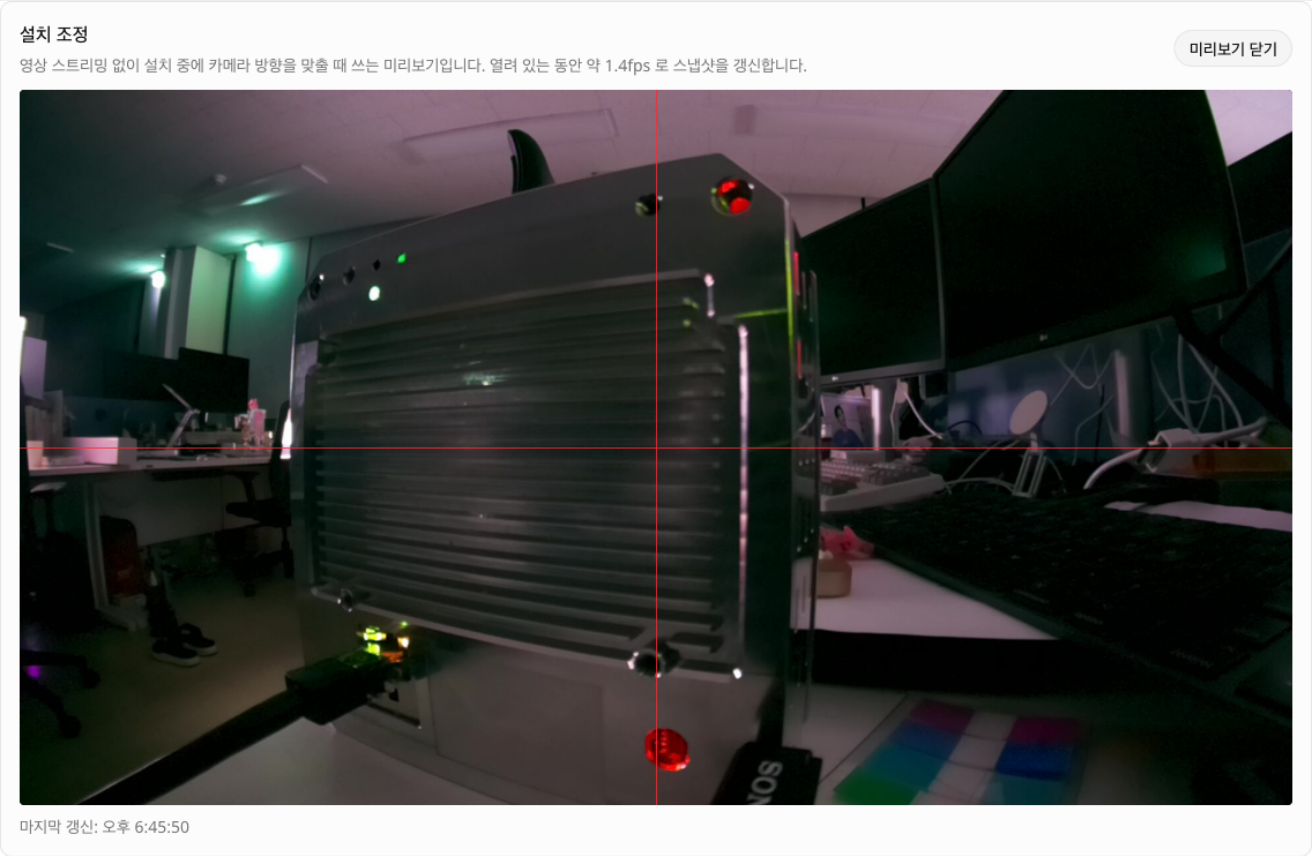
If the device has not yet reported the adjustment range, the slider is replaced with “The adjustment range has not yet been received from the device. You can adjust it when the video service is running.” This can happen just after the device is turned on or while the video service is stopped. Refresh the page once video appears.

Installation alignment preview

The “Installation Alignment” panel helps you aim the device during installation. It displays a sequence of snapshots without video streaming. You can open it even where video streaming is unavailable.

1. Open the preview

Click “Open Preview.” While it is open, snapshots refresh at approximately 1.4 fps. Before the first image arrives, “Loading snapshot…” is displayed.



2. Aim the device

The snapshot is the final image, including the heatmap, peak marker, status bar, and ROI box. Image rotation is also applied. If you turn on the crosshair, two red lines appear at the center of the snapshot. Move the device until the target is centered on the screen.

3. Close the preview

Click “Close Preview.” Refreshing stops when you navigate to another screen. It also stops while the browser tab is hidden and resumes when the tab becomes visible again.

※ The device captures only one image every 0.5 seconds in total. If an image is being captured elsewhere at the same time, the last image remains visible until refreshing resumes.

Status messages

If a problem occurs, a red message appears and the preview automatically retries.

- “The video service is not running. Attempting to reconnect.” — The video service has not started yet or is restarting.
- “No video has been received yet. Retrying.” — The first video frame has not arrived yet.
- “Unable to retrieve a snapshot. Retrying.”
- “Unable to connect to the device. Retrying.” — Check communication between the browser and the device.
- “Authentication has expired. Please log in again.” — Refreshing stops when this message appears. Log in again, then open the preview.

AI Detection

BATCAM FX2 runs AI models on the device to detect compressed-air and gas leaks and electrical partial discharge. This page explains how to turn on the models, change the detection criteria, and set when AI runs.

The settings are in the AI menu. The same settings are also at the bottom of the Events → Trigger Conditions tab. Changes made in either location save the same values.

AI Models

The device has two AI models. Both run on the device.

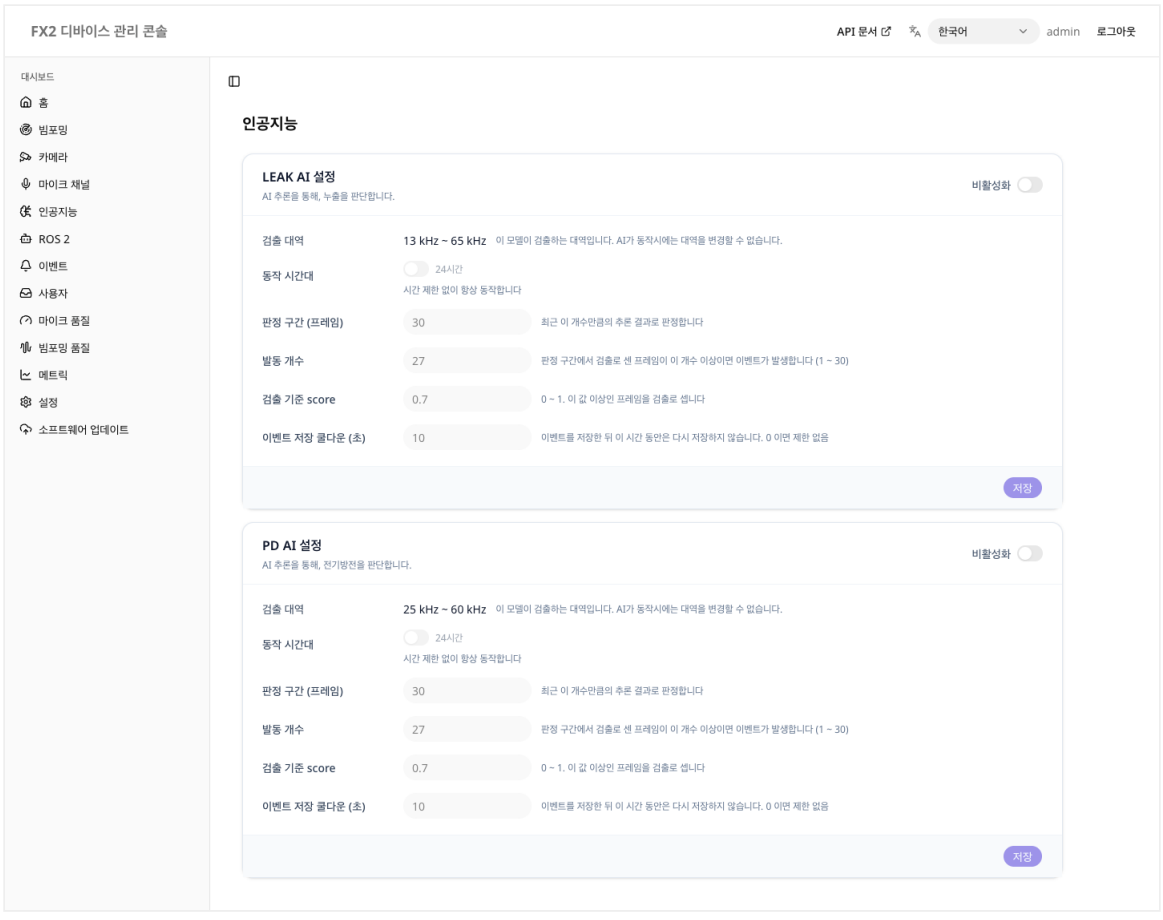
- Leak AI (LEAK AI) — detects compressed-air and gas leaks. Its screen is called “LEAK AI Settings.”
- Partial Discharge AI (PD AI) — detects electrical partial discharge and classifies it as Corona, Floating, or Surface. Its screen is called “PD AI Settings.”

Both models make detections using sound received from three listening points.

Turning Models On and Off

Each model card has an “Enable” switch in the upper right. Turning it on saves the change immediately. You do not need to press “Save.”

Both models are off by default when shipped.



Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

“PD AI Settings” appears as “Partial Discharge AI Settings.” The model-switching dialog says, for example, “Turn off LEAK AI and turn on Partial Discharge AI?” The save-failure message is “Failed to save Partial Discharge AI settings.”

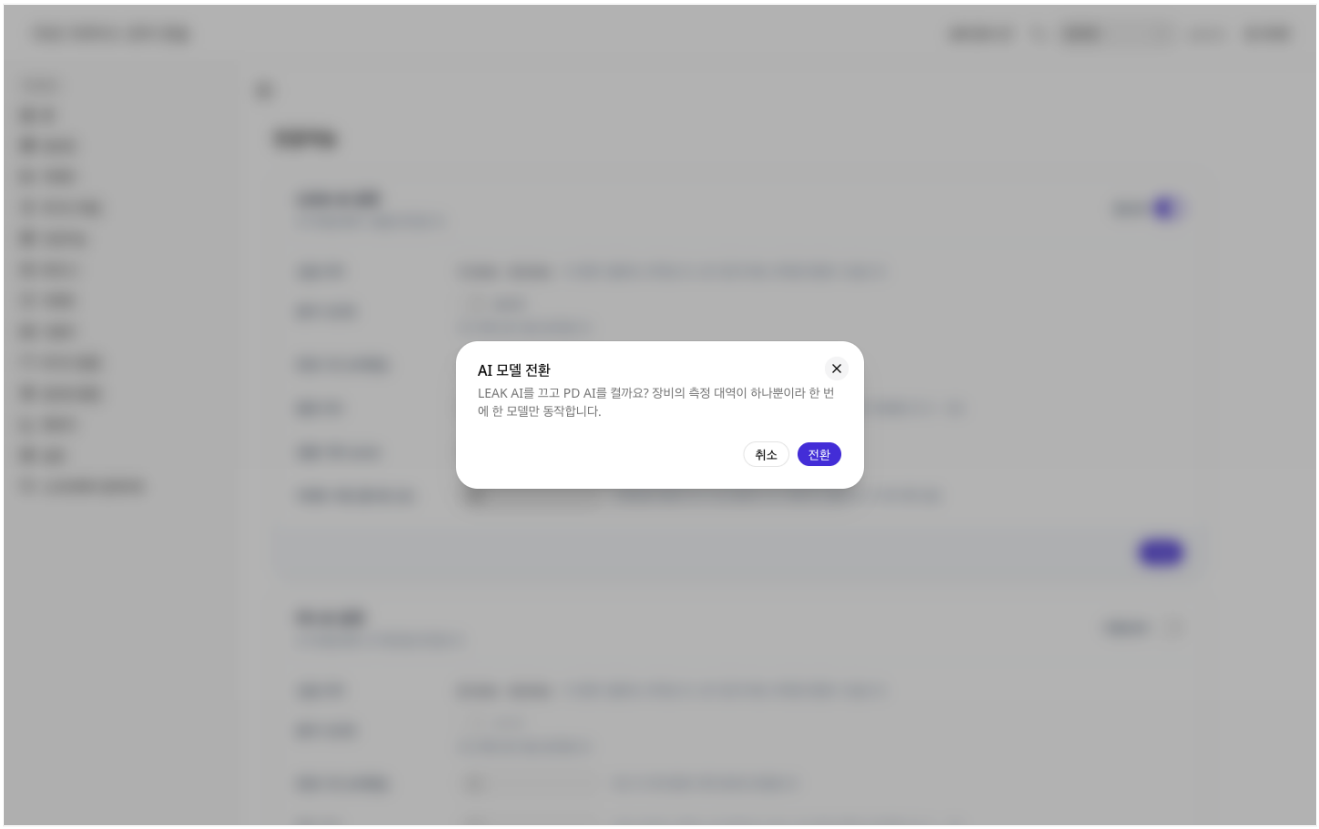
Only One Model Can Be On at a Time

The device has only one measurement band, so Leak AI and Partial Discharge AI cannot be on at the same time.

If you turn on one model while the other is on, an “Switch AI Model” dialog opens. It describes the change, for example, “Turn off LEAK AI and turn on PD AI?”

- “Switch” — turns off the current model and turns on the selected model.
- “Cancel” — makes no changes.

No confirmation dialog appears when you turn a model off.



The Measurement Band Is Fixed

While AI is running, the measurement band is set to the model’s detection band. When AI stops, it returns to the measurement band you selected manually.

- Partial Discharge AI — 25 kHz ~ 60 kHz
- Leak AI — 13 kHz ~ 65 kHz

While AI is running, you cannot change the following:

- The “Frequency Range” slider in the Beamforming menu
- The microphone check in the Microphone Quality menu

A message such as “The frequency range cannot be changed while AI is running” appears. To change the measurement band, turn off AI first.

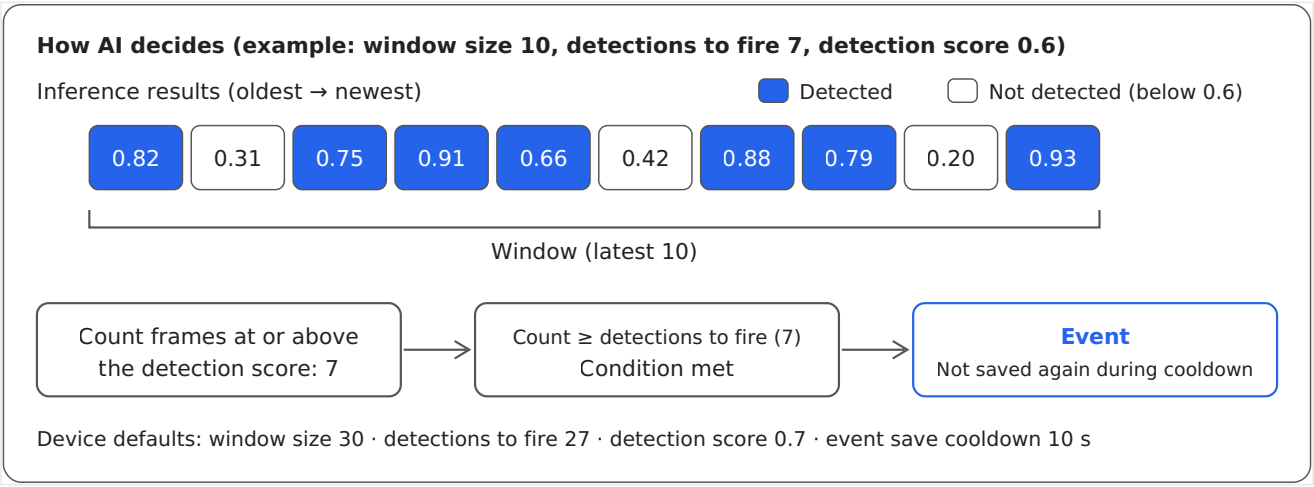
The “Detection Band” on the model card is read-only. It shows the band the model detects.

How Detection Works

The device runs AI inference on sound about 10 times per second. Each inference result is called a frame.

Detection follows these steps:

- Each frame receives a score. A frame is counted as a detection if its score is at least the “Detection Threshold Score.”
- The device counts detected frames within the most recent “Decision Window.”
- An event occurs when the detection count reaches the “Trigger Count.”
- After saving an event, the device does not save another event from the same model during the “Event Save Cooldown.”



Detection Parameters

You can set four parameters for each model. Both models have the same defaults.

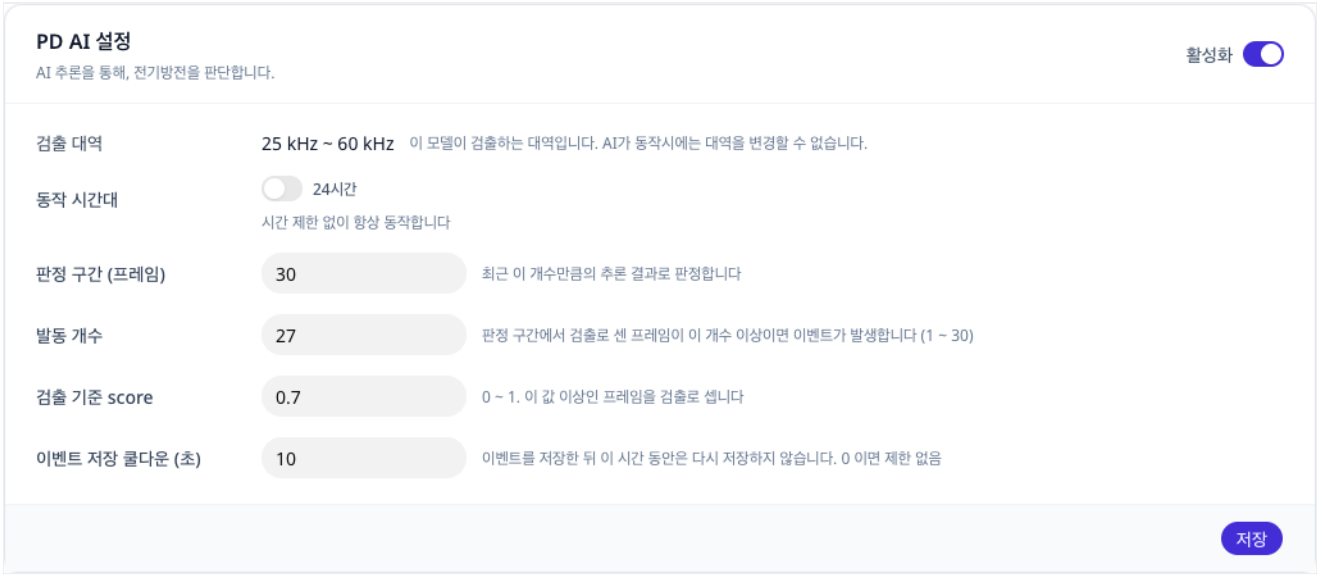
- Decision Window (frames) — default: 30. An integer of at least 1. Detection uses this many recent inference results. Thirty frames is about 3 seconds.
- Trigger Count — default: 27. An integer from 1 to the Decision Window value. An event occurs when at least this many frames in the decision window count as detections.
- Detection Threshold Score — default: 0.7. A value from 0 to 1. Frames with a score at least this high count as detections.

- Event Save Cooldown (seconds) — default: 10. An integer of at least 0. A value of 0 means no restriction.

※ If you reduce the Decision Window, the Trigger Count is also reduced to fit. Out-of-range values are corrected to the allowed range when saved.

After changing values, press “Save” at the bottom of the card. “Saved” appears briefly when the settings are saved. If saving fails, “Failed to save LEAK AI settings” or “Failed to save PD AI settings” appears.

When a model’s switch is off, its parameter fields, operating-hours switch, and “Save” button are disabled. Turn on the model before changing its values.



Operating Hours

You can set the hours when AI runs. The default is “24 hours.”

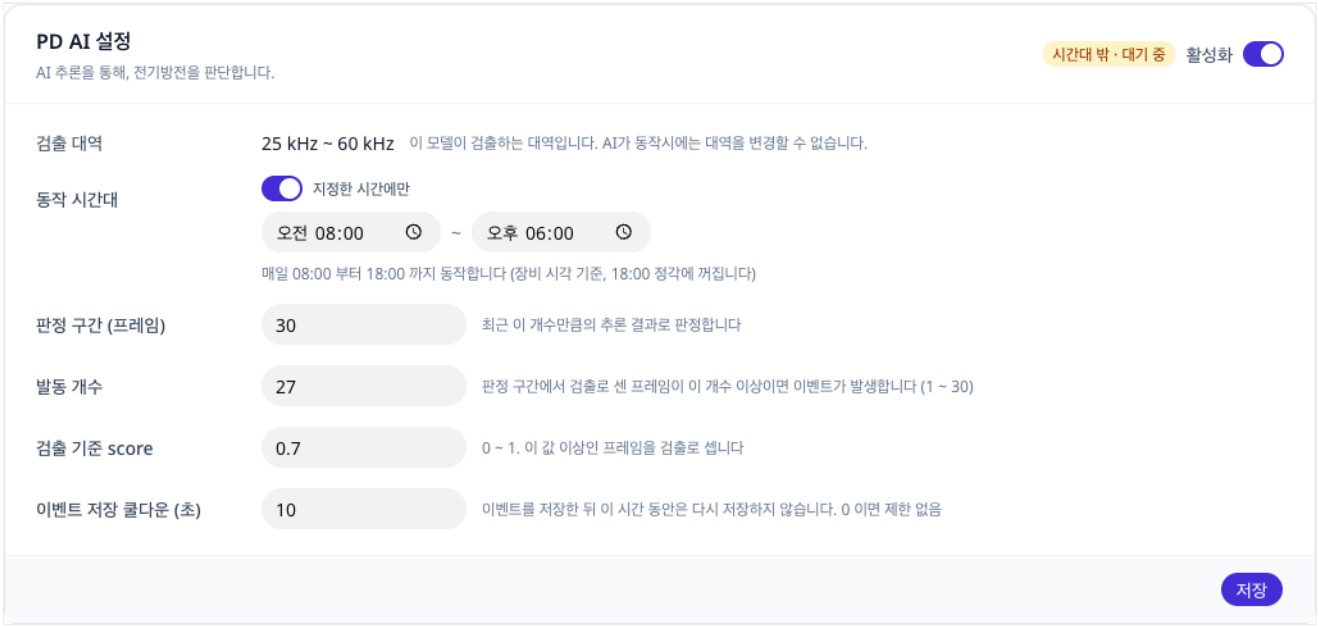
Turning on the “Operating Hours” switch changes the setting to “Only during specified hours” and reveals start and end time fields. When first turned on, they are set to 08:00 ~ 18:00.

- Times are based on the device clock, not the browser clock or UTC. Set the device clock under Settings → Time Settings.
- The start time is included; the end time is excluded. The model stops at the exact end time.
- If the start time is later than the end time, the period spans midnight. For example, 22:00 ~ 06:00 runs from 10 p.m. until 6 a.m. the next day.
- The start and end times cannot be the same. In that case, “The start and end times are the same. Turn off the schedule to run 24 hours a day” appears, and “Save” is disabled.
- Time changes take effect only after you press “Save.” The “Enable” switch takes effect immediately.
- Turning off the operating-hours switch clears the entered times. The device does not remember the previous schedule.
- The device checks the schedule about once a minute. Saved changes take effect immediately.

The “Enable” switch must be on for the schedule to matter. If it is off, the model does not run even during the scheduled hours.

Outside the scheduled hours, the model stops and the measurement band returns to its previous setting. “Outside operating hours · Standby” appears beside the switch on the model card. This indicator shows the state when the screen was opened or the settings were saved; it does not update in real time. Reload the screen to see the current state.

※ If the device cannot access a time server (NTP), its clock starts at 1970-01-01T00:00:00 when powered on and will not match the actual time. See System Settings for details.



On-Screen Indicators

AI status appears on the video overlay.

Heatmap Colors

- When both models are off, the heatmap is always in color.
- While AI is running, the heatmap is gray when nothing is detected.
- The heatmap changes to color when a detection occurs.

Status Bar

“LEAK AI” and “PD AI” appear with dots on the left side of the status bar.

- Gray dot — off
- Green dot — on, no detection
- Red dot — detecting

The detection type appears beside the dot only while detection is in progress. Leak AI shows Leak; Partial Discharge AI shows Corona, Floating, or Surface.

The status bar is visible only when “Show Status Bar (Status Bar)” is on in the Camera menu. See Camera Settings for details.

AI Events

An event is saved when the detection criteria are met. In the event list, the type is shown as “Leak” for Leak AI and “Discharge” for Partial Discharge AI.

The “Confidence” column has a value only for AI events. It is the proportion of frames counted as detections within the decision window at the moment the event occurs. It is different from the “Detection Threshold Score.” See Events for information on event files and viewing the list.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

In the event list, Partial Discharge AI events have the type “Partial Discharge.” The “Confidence” column is named “Detection Ratio.”

For an AI event to occur, the current video must contain a peak. A peak is the strongest sound source among sounds at or above the overlay “Threshold.”

Events

An event is a record the device saves when a condition is met. This page explains how to view, download, and delete saved events, and how to configure the conditions that create them.

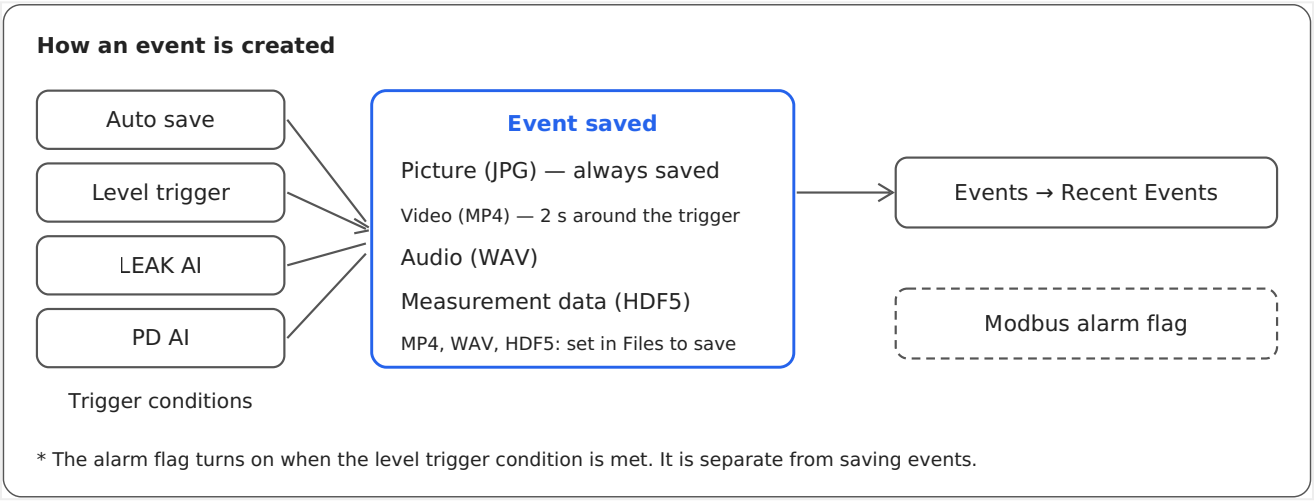
The Events menu has two tabs: “Recent Events” and “Trigger Conditions.”

What Is an Event?

When an event occurs, the device saves a record of that moment as files.

- Photo (JPG) — An image with the heatmap overlaid. Always saved.
- Video (MP4) — A 2-second clip spanning the moment before and after the trigger.
- Audio (WAV) — Sound from the event period.
- Measurement data (HDF5) — Raw beamforming data.

You can choose whether to save video, audio, and measurement data. See “Event Storage Items” below for details.



Events occur through one of the following four triggers. The same names appear under “Type” in the event list.

- Auto Save — Saves an event if no event occurs for a set period.
- Level Trigger — Saves an event when the level meets or exceeds a threshold.
- Leak — Saves an event when the leak AI detects a leak.
- Discharge — Saves an event when the partial discharge AI detects a discharge.

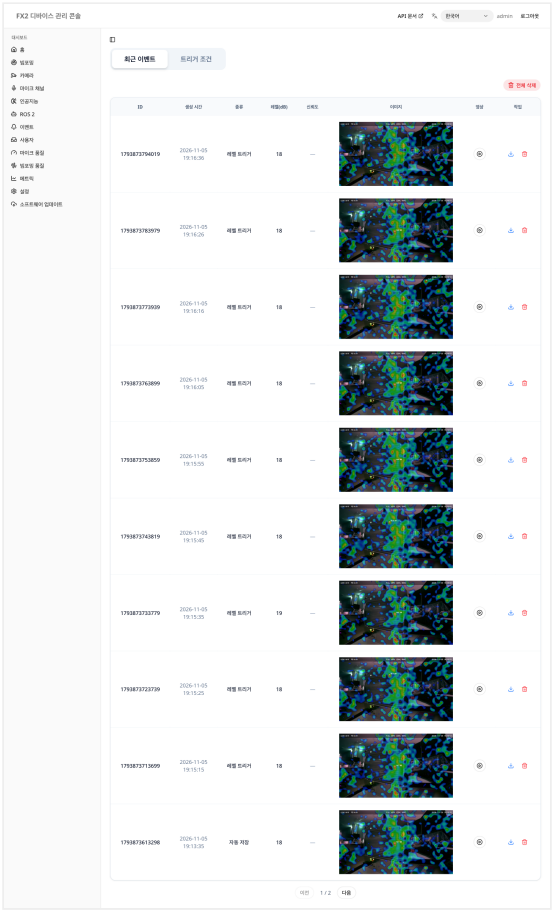
Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

The type of a partial discharge AI event is shown as “Partial Discharge” instead of “Discharge.” The “PD AI Settings” card on the Trigger Conditions tab is shown as “Partial Discharge AI Settings.”

Recent Events

Saved events are shown newest first. Each page shows 10 events. If there are 11 or more, “Previous” and “Next” buttons and page numbers appear below the list. If there are no events, “No events” is displayed.



List Columns

- ID — The event number.
- Creation Time — The date and time the event occurred, shown in the browser’s time zone.
- Type — Auto Save, Level Trigger, Leak, or Discharge.
- Level (dB) — The level of the strongest peak at the moment of the event, displayed as an integer with decimal places truncated.
- Confidence — Shown only for AI events. Other events show “—.”
- Image — The saved photo.
- Video — A play button. Shows “—” if there is no video.
- Actions — Download and delete buttons.

※ Recent events on the home screen are shown in the device’s time zone. If the browser and device use different time zones, the times shown on the two screens will differ.

Confidence

Confidence is the percentage of frames counted as detections during the AI's evaluation interval when it classified the event. If 8 of 10 frames in the interval are detections, confidence is 80 %.

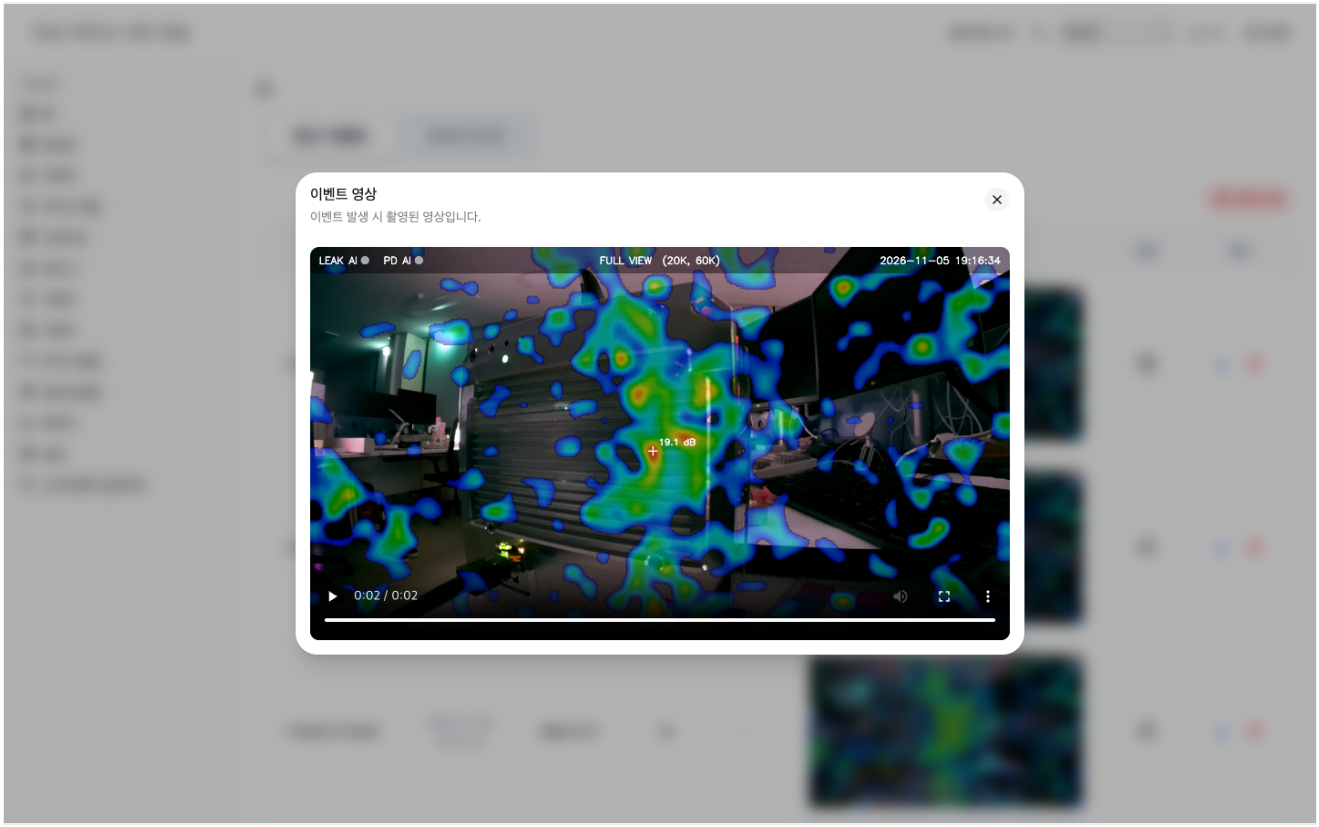
Hover over the confidence value to see the original count, such as "8 / 10."

Confidence is different from the "detection threshold score." The detection threshold score determines whether an individual frame counts as a detection. See AI Detection for how classification works.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information is based on firmware v1.1.1-beta.1 and may change in the official release.
>
> The "Confidence" column has been renamed "Detection Rate." Its meaning and calculation are unchanged.

View Video

Click the play button in the "Video" column to open the "Event Video" window. The video plays automatically.



Download

Click the download button in the "Actions" column to download the event files as a single ZIP file. The filename is `fx2-event-<ID>.zip`.

The ZIP contains only files actually saved for that event. Any photo, video, audio, or measurement data that was not saved is excluded.

※ In firmware v1.1.0, event files can be downloaded without an account.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

If even one file cannot be downloaded, no ZIP is created and “Failed to download event” is displayed.

※ A device account is required to download event photos, videos, and files (stream authentication, enabled by default). Device Manager uses your existing login credentials. If the login has expired and the download fails, you are taken to the login screen. Opening an event file URL directly in a browser brings up a login prompt. Enter the device account credentials.

Delete

Administrator privileges are required to delete events.

- Delete one event — Click the delete button in the “Actions” column and confirm at “Delete this event?”
- Delete all events — Click “Delete All” at the top right. Confirm “Delete all events?” and then “This action cannot be undone. Are you sure you want to delete all events?”

Deleted events cannot be restored, so download any events you need first. Deleting all events does not change the trigger condition settings.

The delete button is also visible to standard user accounts. If you attempt to delete an event with a standard user account, “Failed to delete event” appears and the event remains. See User Accounts and Permissions for account permissions.

Automatic Cleanup

When 10 % or less of the device’s storage space remains, the device automatically deletes events, starting with the oldest. This threshold cannot be changed in Device Manager.

Download any events you need before storage space runs low.

Trigger Conditions

Configure the conditions that create events and the files to save. The following cards appear from top to bottom:

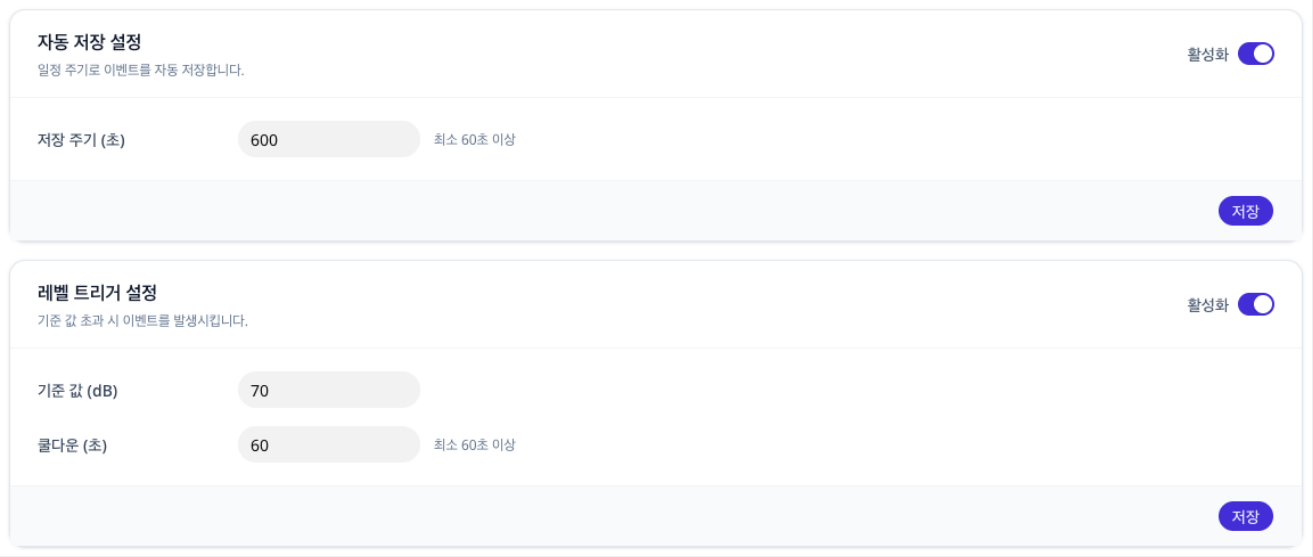
- Event Storage Items
- Modbus TCP
- Auto Save Settings
- Level Trigger Settings
- LEAK AI Settings, PD AI Settings

Each card’s “Enable” switch is saved immediately. Numeric values are saved only when you click “Save” on the card. When the switch is off, the numeric fields and “Save” button are disabled. In firmware v1.1.0, standard user accounts can also change Auto Save Settings and Level Trigger Settings.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Administrator privileges are required to change Auto Save Settings and Level Trigger Settings. Standard user accounts can only view the values, and the cards display “Only administrators can make changes.”



Auto Save

Saves an event if no event of any type occurs for a set period. Enable this to keep a periodic record of site conditions.

- Enable — Off by default.
- Save Interval (seconds) — 600 seconds by default. The minimum is 60 seconds; smaller values are raised to 60 seconds when saved.

Auto Save occurs when the save interval has elapsed since the last event, regardless of its type. Any new event restarts the interval.

※ If there is no peak in the video, an Auto Save event is not saved either.

Level Trigger

Saves an event when the level meets or exceeds a threshold.

- Enable — On by default.
- Threshold (dB) — 70 dB by default.
- Cooldown (seconds) — 60 seconds by default. The minimum is 60 seconds; smaller values are raised to 60 seconds when saved.

The cooldown starts from the last event, even if that event was an Auto Save or AI event. If another event occurs during the cooldown, the Level Trigger cannot occur until the cooldown ends.

※ If the overlay “Threshold” in the Beamforming menu is higher than the Level Trigger threshold, the Level Trigger will not occur. Sounds below the overlay threshold are not identified as peaks.

AI Triggers

The “LEAK AI Settings” and “PD AI Settings” cards are the same as those in the AI menu. Their switches and parameters are linked. See AI Detection for details.

Event Storage Items

Choose which files to keep when an event occurs. The selections apply equally to all triggers.

- Video (MP4) — Selected by default. Has the highest processing cost.
- Audio (WAV) — Selected by default. Sound from the event period.
- Measurement data (HDF5) — Selected by default. Raw data, usually the largest file.

There is no option to select photos. Called “Screenshot” on the screen, they are always saved. If you turn off all three optional items, “If all are turned off, only a screenshot will remain for the event” is displayed.

Changes take effect from the next event after you click “Save.” Files for previously saved events remain unchanged.



Video Encoding Mode

Choose how videos are created under “Video Encoding Mode.”

- Encode on Event (default) — Keeps CPU usage low during normal operation. Creates a video when an event occurs.
- Continuous Encoding — Avoids a processing spike when an event occurs. Video encoding runs continuously.

With “Encode on Event,” up to two videos can be created at the same time. If a third event occurs while they are being created, only a photo is saved for that event.

Modbus TCP

This tab also includes a Modbus TCP card. It lets PLC and SCADA systems read levels and alarms from the device. See External System Integration for setup instructions.

Custom Triggers

In firmware v1.1.0, an administrator can add triggers through REST, but added triggers are only saved; they do not create events. Only Auto Save, Level Trigger, and AI triggers create events.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Custom triggers record events when their conditions are met. Triggers registered and enabled before an update may start working immediately after the update, so check their thresholds and enabled status beforehand.

You can register additional level triggers with thresholds different from the main Level Trigger. Device Manager has no controls to add or delete them; an administrator registers them through REST. Each registered trigger has its own threshold and fires when the level meets or exceeds it.

- Add — `POST /event/trigger` (multipart). Put the threshold (dB) in the `value` field. Administrator privileges are required.
- Number — New trigger IDs start at 101.
- Initial state — Created enabled. If no cooldown is set, it operates with a 60-second cooldown. In that case, the `cooldown` value in the list is empty.
- Set cooldown — Specify `cooldown` with `PATCH /event/trigger`. Administrator privileges are required.
- List — View registered triggers with `GET /event/trigger`.
- Delete — Put the trigger number in the `id` field of `DELETE /event/trigger`. Administrator privileges are required. Default triggers with IDs of 100 or less cannot be deleted.

This example adds a trigger with an 85 dB threshold and sets its cooldown to 60 seconds. For `id` in the second command, use the number returned by the first command.

```
curl -u <ID>:<password> -F value=85 http://<device-ip>/event/trigger
curl -u <ID>:<password> -X PATCH -F id=<trigger-id> -F cooldown=60 http://
<device-ip>/event/trigger
```

See API and Developer Integration for how to make REST calls.

Operating Tips

- Start with a low Level Trigger threshold. After checking the site’s normal level, raise the threshold to reduce unnecessary events.
- Check the normal level using the number next to the peak marker on the Beamforming screen.
- Download events regularly. When storage space runs low, the oldest events are deleted automatically.

Microphone Check

Use the Microphone Channel, Microphone Quality, and Beamforming Quality menus to check the device's microphones and beamforming results. Use them immediately after installation or when measurements seem questionable.

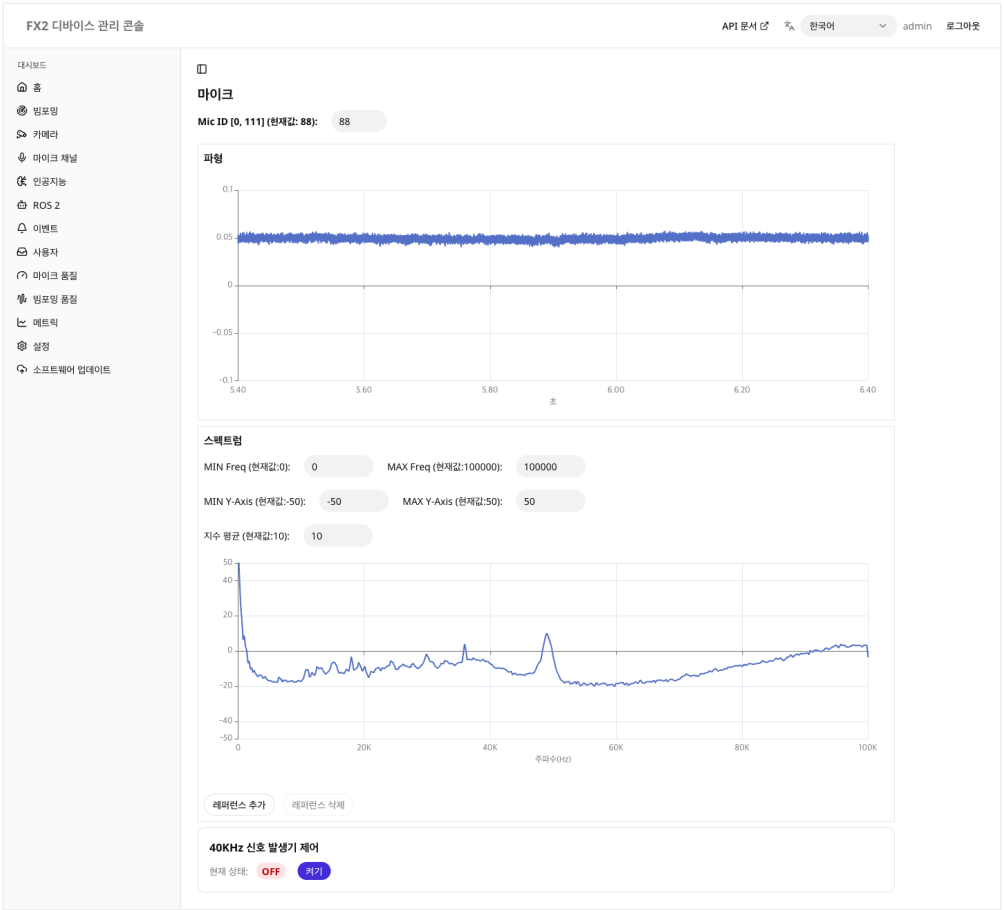
The three menus serve these purposes:

- Microphone Channel — View the waveform and spectrum of one microphone channel. You can also turn the 40 kHz reference signal on and off here.
- Microphone Quality — Measure all 112 channels at once to check sensitivity differences and noise across channels.
- Beamforming Quality — Collect beamforming results over a set period and check the difference between the maximum and minimum values.

※ Check results are not saved on the device. Both administrator and regular user accounts can perform these checks.

Microphone Channel

The Microphone Channel menu (titled "Microphone" on the screen) shows the signal from one selected microphone channel.



Mic ID

Enter the microphone number you want to check in the “Mic ID [0, 111]” field. There are 112 microphones, numbered 0–111. The factory default is 88.

- Entering a value within the range changes the selection immediately and displays a result such as “Mic ID=88”.
- Entering a value outside the range displays “id must be in the [0, 111] range” and does not send it to the device.
- The selected number is saved on the device and persists after a reboot.

※ Mic ID only determines which channel is shown on this screen. It does not affect beamforming results.

Waveform

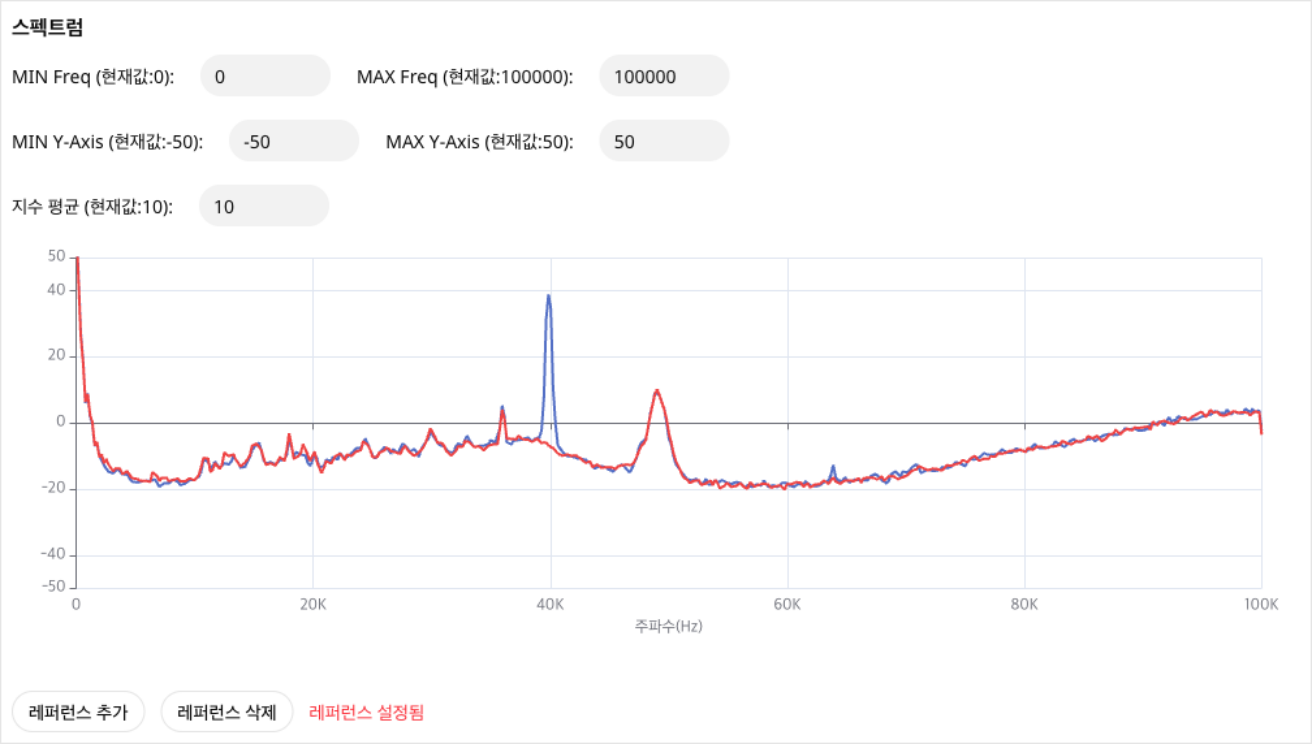
Shows the selected channel’s signal over time. The horizontal axis shows seconds, and the vertical axis shows signal amplitude. The most recent one-second interval is displayed. The vertical axis adjusts automatically to the signal amplitude.

Spectrum

Shows the selected channel’s level (dB) by frequency. The browser calculates the values by analyzing approximately 0.3 seconds of signal at a time, then smooths them with exponential averaging.

Spectrum options apply only to the browser screen. They are not saved on the device and return to their defaults when you reopen the screen.

- MIN Freq, MAX Freq — Integers from 0 to 100000 Hz. Defaults: 0 and 100000. MIN must be less than MAX.
- MIN Y-Axis, MAX Y-Axis — Integers. Defaults: -50 and 50. MIN must be less than MAX.
- Exponential averaging — Positive integer. Default: 10. A value of 1 shows only the most recent values without averaging; larger values make the curve smoother.



Reference

Click “Add Reference” to fix the current spectrum curve as a red line for comparison with subsequent curves. Click “Delete Reference” to remove it.

- While it is fixed, “Reference Set” appears in red.
- If there is no spectrum to display yet, “No spectrum data to capture” appears.

※ The reference is retained only on this screen. It disappears if you refresh the page or move to another menu.

40 kHz Reference Signal

The device can generate a 40 kHz signal for testing. Turn it on and off under “40KHz Signal Generator Control” in the Microphone Channel menu. Use it to check whether the microphone detects 40 kHz sound.

“Current Status” shows one of the following:

- ON — The signal is on. The button says “Turn Off”.
- OFF — The signal is off. The button says “Turn On”.
- UNKNOWN — The status has not yet been read. The button cannot be pressed.

The status is read once when you open the screen. If it is changed elsewhere, refresh the page to see the new status. If UNKNOWN persists, check communication with the device and refresh the page.

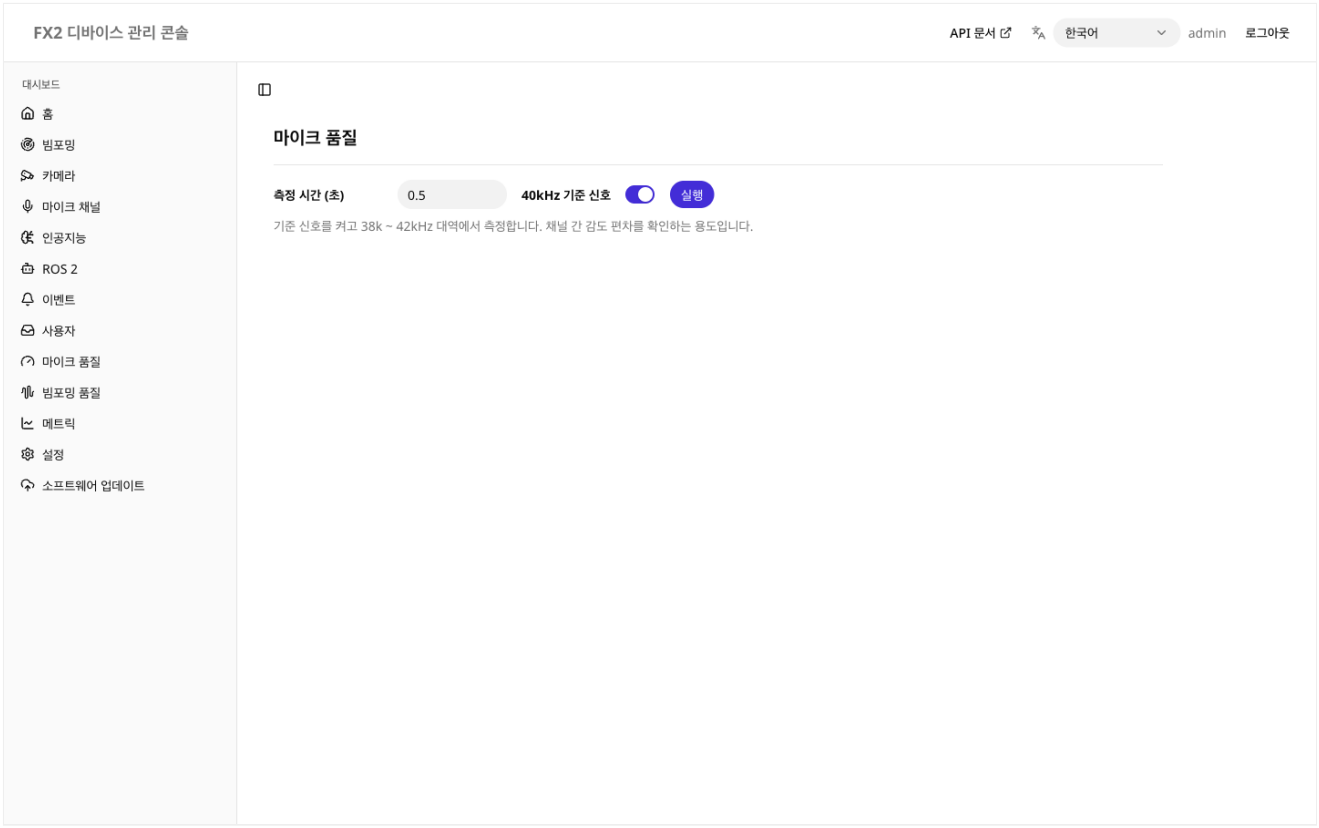


When the signal is on, the device measures this 40 kHz signal instead of actual sound. The measurement band must include 40 kHz for the microphone to detect the signal.

Turn the signal off as soon as the check is complete. If left on, this signal will be measured instead of actual sound, affecting beamforming results and the level trigger.

Microphone Quality

The Microphone Quality menu measures the signal amplitude (RMS) of all 112 channels at once. Use it to find channels with different sensitivity or high noise.



1. Set the Measurement Conditions

- Measurement Duration (seconds) — 0.1–0.5; default: 0.5. An out-of-range value displays “Measurement duration: 0.1–0.5”.
- 40kHz Reference Signal — Off by default

The measurement method depends on the switch setting.

- On — Turns on the reference signal and measures in the 38 kHz–42 kHz band. Use this to check sensitivity differences across channels.
- Off — Turns off the reference signal and measures using the current measurement band. Use this to check the noise floor of each channel.

※ When measuring with the switch on, the device changes the measurement band to 38 kHz–42 kHz, waits one second, then measures. Afterward, it restores the original band and reference signal state.

※ Changes to the measurement band made elsewhere while a measurement is in progress wait until the measurement is complete.

2. Run

Click “Run”. The button displays “Measuring...” while the measurement is in progress.

You cannot run it while AI is operating. The screen displays “Microphone calibration cannot run while AI is operating.” and disables the button. Turn off AI or run it outside its operating hours.

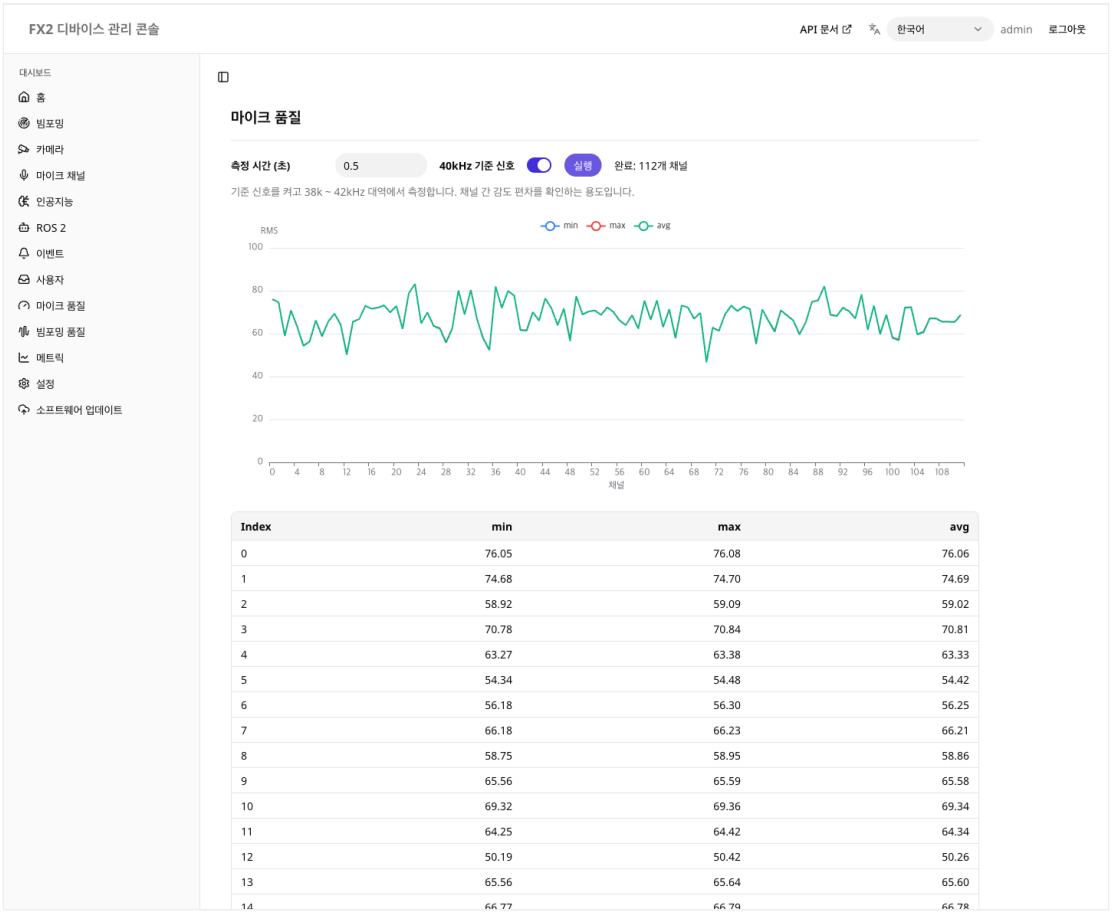
※ AI status is checked once when you open the screen. If AI starts after you open it, refresh the page.

3. Check the Results

When the measurement is complete, “Complete: 112 channels” appears, followed by a graph and table.

- Graph — The horizontal axis shows channels, and the vertical axis shows RMS. Three lines show min, max, and avg.
- Table — Contains Index, min, max, and avg columns. Values are displayed to two decimal places.
- If the measurement fails, “Failed: ...” or “Error: ...” appears.

A channel that receives no signal is marked “No signal” in the table and appears as a gap in the graph. If no channel receives a signal, “No signal detected on any channel.” appears above the graph.



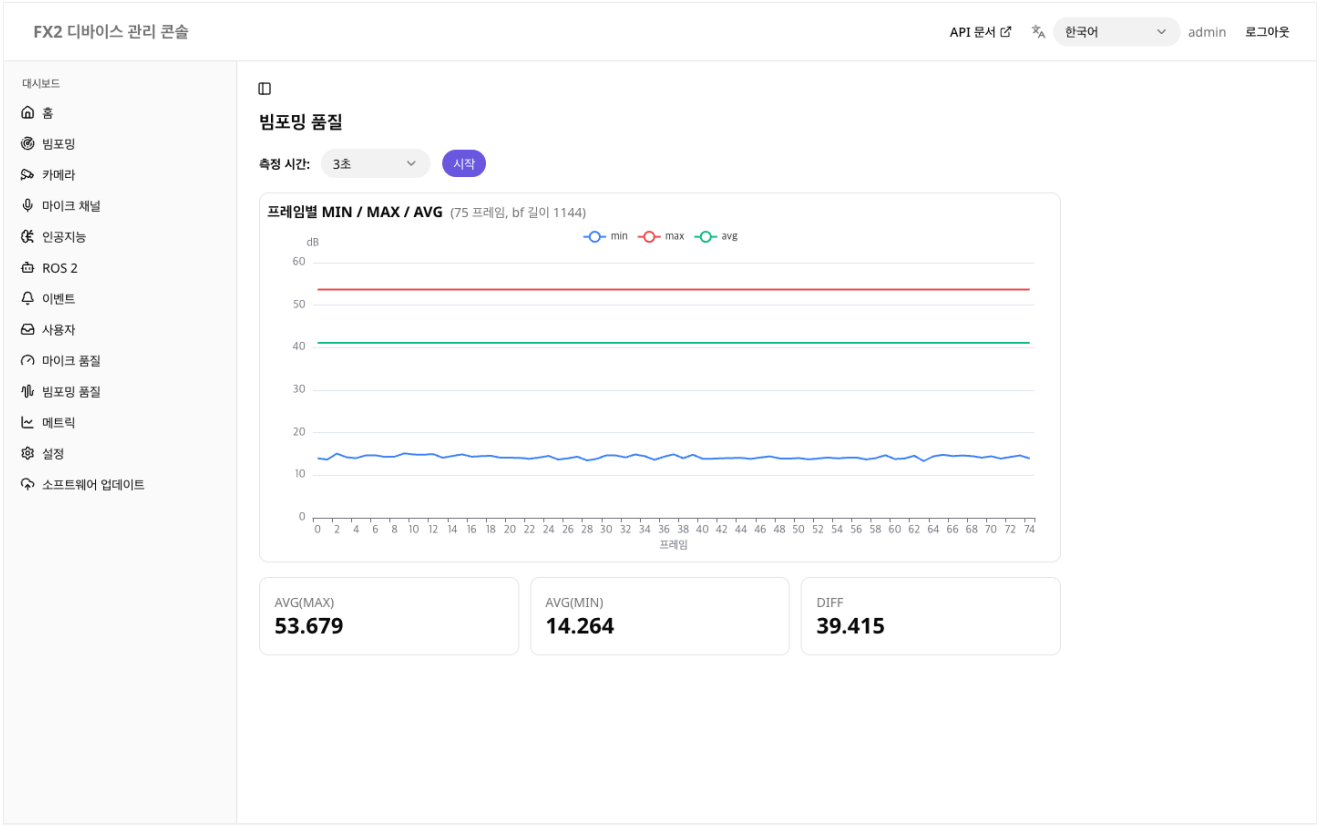
Index	min	max	avg
0	76.05	76.08	76.06
1	74.68	74.70	74.69
2	58.92	59.09	59.02
3	70.78	70.84	70.81
4	63.27	63.38	63.33
5	54.34	54.48	54.42
6	56.18	56.30	56.25
7	66.18	66.23	66.21
8	58.75	58.95	58.86
9	65.56	65.59	65.58
10	69.32	69.36	69.34
11	64.25	64.42	64.34
12	50.19	50.42	50.26
13	65.56	65.64	65.60
14	66.77	66.79	66.78

How to Read the Results

- With the reference signal on, an avg value noticeably lower or higher than those of nearby channels may indicate a sensitivity issue in that channel.
- With the reference signal off, a channel with a higher avg value than nearby channels has more noise.
- A “No signal” channel may indicate a microphone or connection problem.
- Save the results from immediately after installation as a baseline for comparison with later checks.

Beamforming Quality

The Beamforming Quality menu collects beamforming results over a specified period and calculates statistics. Use it to check the difference between the maximum and minimum beamforming results numerically.



1. Choose the Measurement Duration

Under “Measurement Duration”, choose 1–5 seconds. The default is 3 seconds.

2. Start

Click “Start”. During collection, the button displays “Collecting...” and the measurement duration selector is locked.

3. Check the Results

When collection is complete, a graph and three cards appear. The graph title shows the number of frames collected.

- Graph — Plots MIN (blue), MAX (red), and AVG (green) for each frame. The values are calculated from the 1,144 cells of the beamforming result.
- AVG(MAX) — Average of the per-frame maximum values
- AVG(MIN) — Average of the per-frame minimum values
- DIFF — AVG(MAX) minus AVG(MIN)

Values are in dB and displayed to three decimal places.

※ Compare these values only when the measurement band, ambient sound, and device position are the same. Values can differ even for the same device if conditions change.

※ This check can run regardless of whether AI is operating.

User Accounts and Permissions

There are two types of accounts for logging in to Device Manager: administrators and regular users. This page compares what each role can do and explains how to add, change, and delete accounts in the User menu.

Permissions

- Administrator — Can use all features. Only administrators can manage accounts, configure the network and time, restart services, perform a factory reset, and update firmware.
- Regular user — Can use measurement and event settings. Cannot perform high-risk operations.

Regular users are not read-only. They can change settings such as beamforming, camera, and AI. In firmware v1.1.0, regular users can also change auto-save and level trigger settings.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Only administrators can change auto-save and level trigger settings. Only administrator accounts can call REST `PATCH /event/trigger`.

In the factory-default state, there is an administrator account with the ID admin and a regular user account with the ID user. After a factory reset, the administrator account has the ID `admin` and password `1234`. The same values appear in the notice below the login screen. You must change the password after your first login.

※ If you do not use the factory-default regular user account (user), delete it. If you do use it, change its password using an administrator account.

Logging in issues authentication valid for 24 hours. After 24 hours, you must log in again. A browser used to perform a factory reset is logged out and must log in again.

In firmware v1.1.0, no account is required for RTSP video, WebRTC video, WebSocket, ONVIF snapshots, or event files.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

After updating the firmware to v1.1.1 or performing a factory reset, you must log in again in every browser and program.

Both administrators and regular users can use the same account to receive RTSP video, WebSocket data, and event files in a VMS, viewer, or script. See External System Integration for details.

Permissions comparison

Feature	Administrator	Regular user
View video; configure beamforming, camera, and microphone	Yes	Yes
Enable AI and set detection criteria	Yes	Yes
View events; play and download video	Yes	Yes
Delete events	Yes	No
Configure auto-save and level triggers	Yes	Yes
Configure items to save	Yes	Yes
Add and delete custom triggers (see REST and Events)	Yes	No
Configure Modbus TCP	Yes	Alarm hold time only
Change the ROS 2 domain ID	Yes	Yes
View and change network settings	Yes	No
Change time settings	Yes	No (view only)
View the user list; add and delete accounts; change passwords	Yes	No
Restart services and perform a factory reset	Yes	No
Update firmware and FPGA	Yes	No

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

The differences from the table above are as follows.

Feature	Administrator	Regular user
Receive RTSP video, WebSocket data, ONVIF snapshots, and event files	Yes	Yes
Configure auto-save and level triggers	Yes	No (view only)
Add, change, and delete custom triggers (see REST and Events)	Yes	No
Turn stream authentication on or off	Yes	No (item is not shown)

What regular users see

Regular user accounts can see all menus. Items that require administrator permissions are empty or display a failure message.

- “Network Status” on Home — “Unable to load information.”
- Network settings under Settings — The table is empty.
- Time settings under Settings — The table is visible, but there is no change button (gear icon).
- Users — The list is empty. Clicking “Add User” displays “Failed to add user.”
- Delete under Events — “Failed to delete event” is displayed.
- Software Update — Uploading displays “Upload failed (HTTP 403).”
- Restart Service under Settings — The service does not restart. “Restarting service” remains displayed without a completion message.
- Factory Reset under Settings — No reset occurs and no data is erased, but the user is logged out and taken to the login screen.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

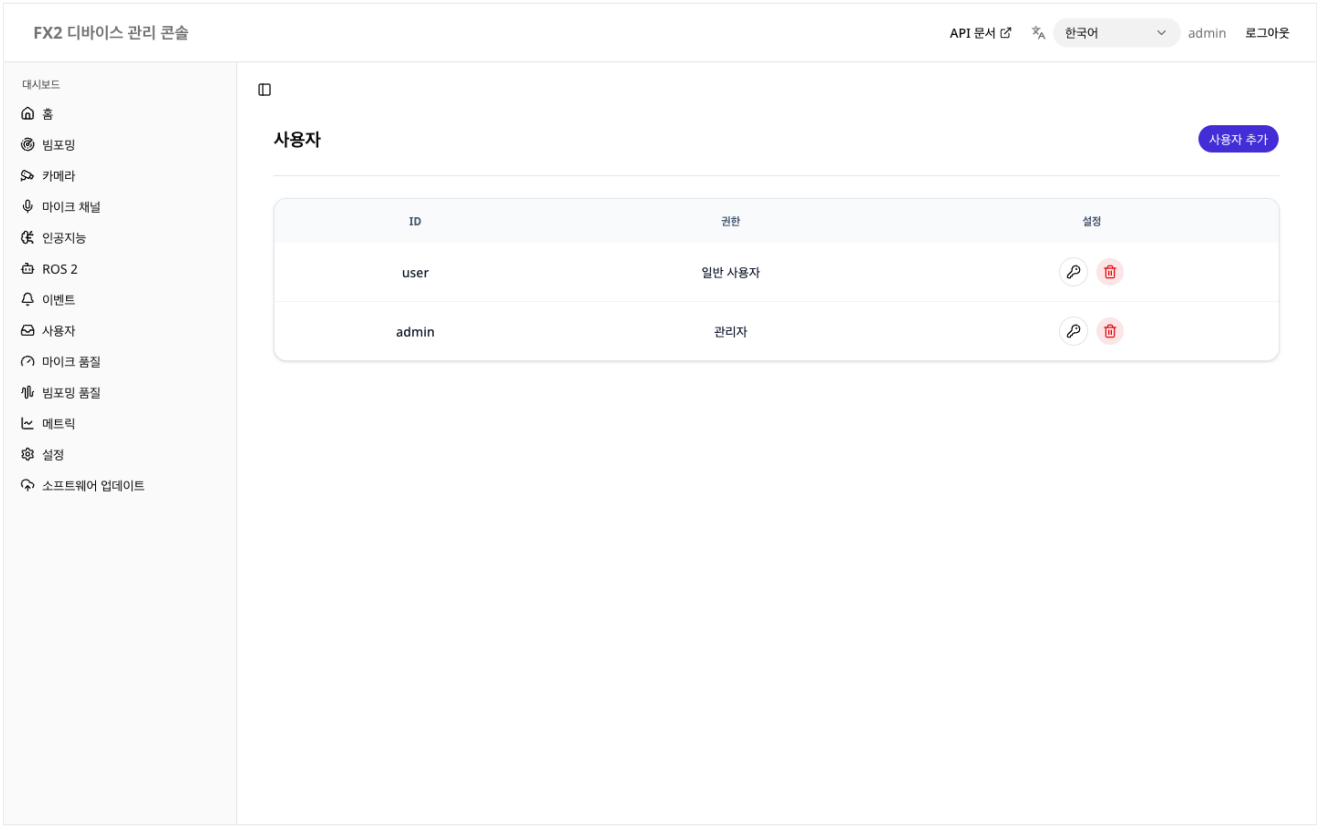
Under Trigger Conditions in Events, the auto-save and level trigger settings cards show their values but cannot be changed. The cards display “Only administrators can make changes.”

User menu

Manage accounts in the User menu. You must log in with an administrator account to see the list.

The list shows ID, permissions, and settings. The Settings column has buttons to change the password (key icon) and delete the user (trash can icon).

Only the 10 most recently created accounts appear in the list. Older accounts do not appear, so they cannot be changed or deleted from this screen.

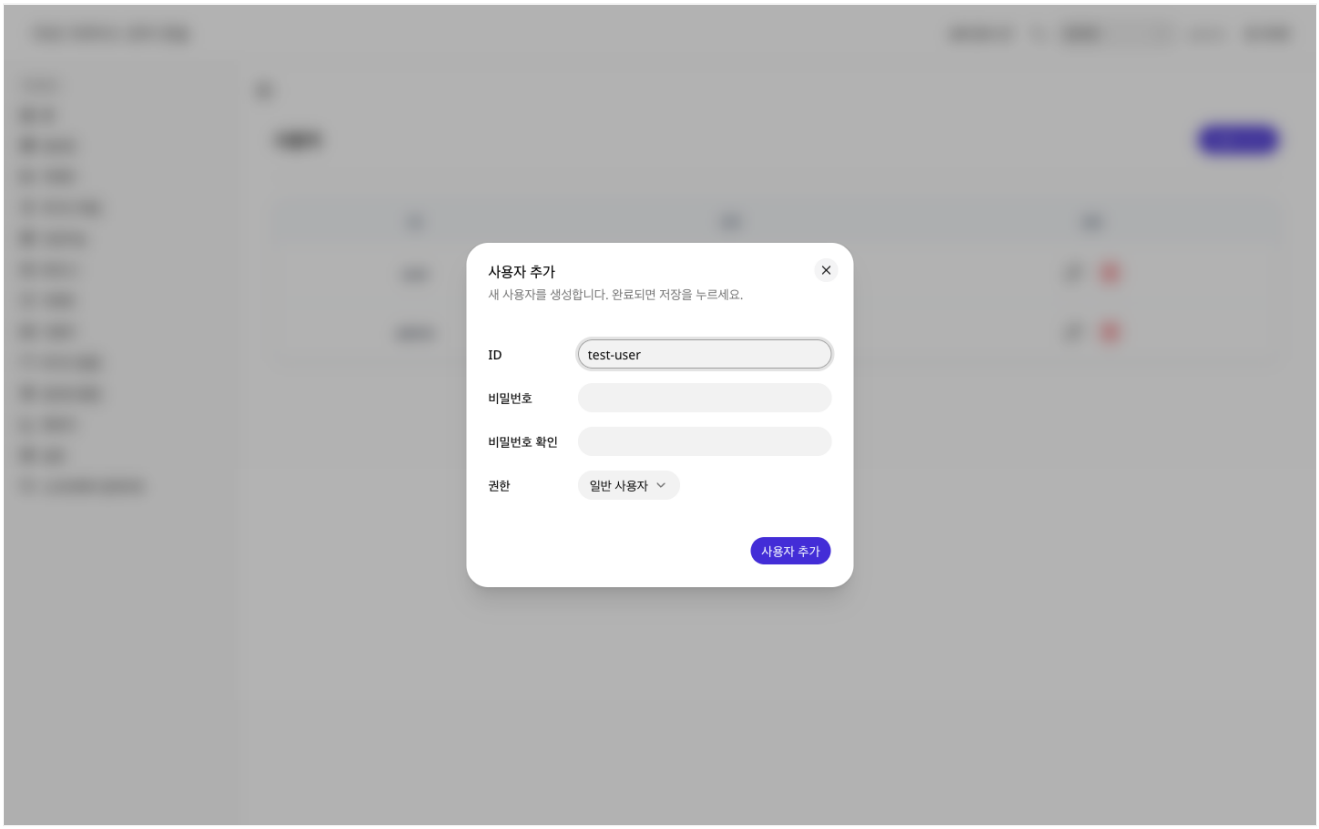


1. Add a user

Click “Add User” in the upper right of the User menu and enter the following:

- ID — At least 4 characters
- Password — At least 4 characters
- Confirm Password — The same value as the password
- Permissions — “Administrator” or “Regular User.” The default is “Regular User.”

Click the “Add User” button in the dialog to create the account.



If the two passwords differ, “Passwords do not match” is displayed. All other failures display only “Failed to add user,” without a reason. Check the following:

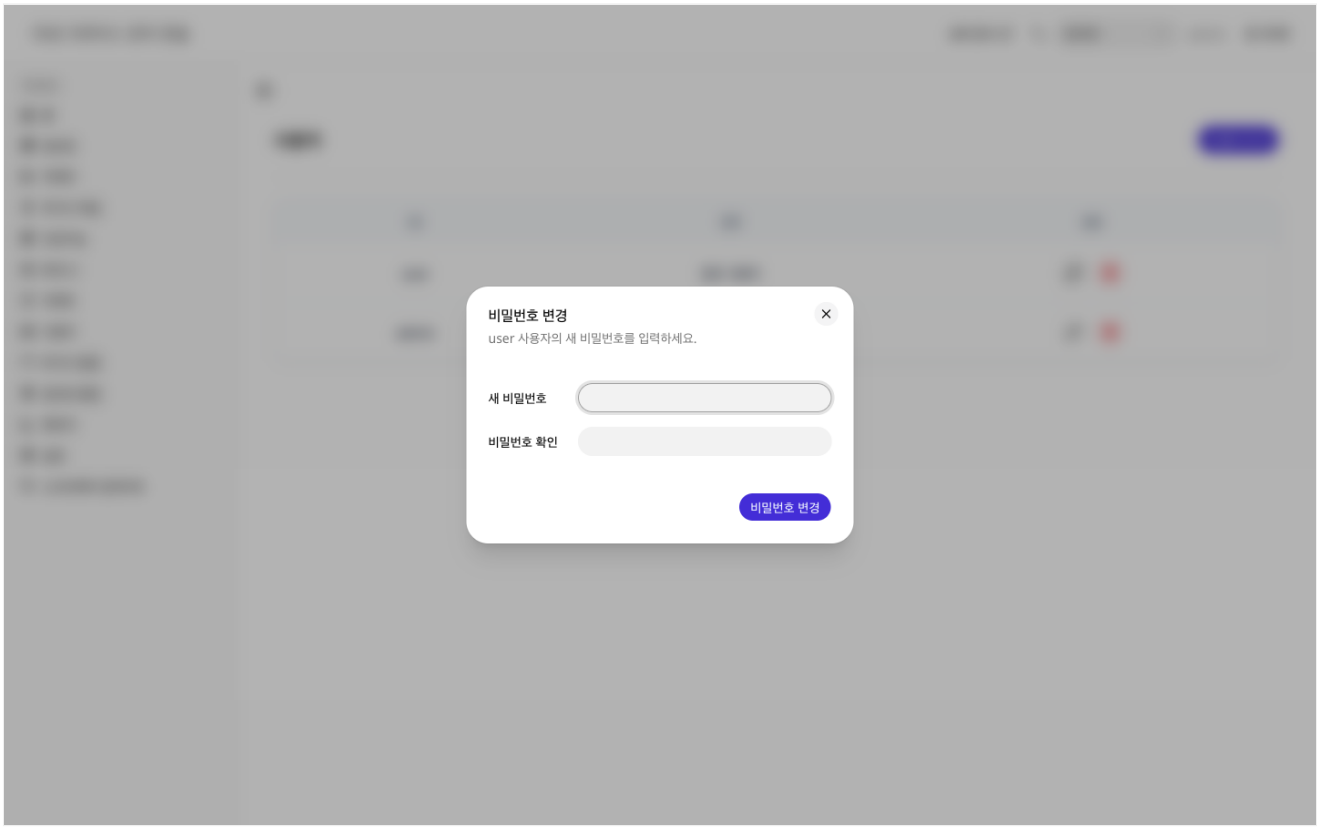
- Whether the ID and password are each at least 4 characters long
- Whether an account with the same ID already exists
- Whether you are logged in with an administrator account

※ An account’s permissions cannot be changed after it is created. To change them, delete the account and create a new one.

2. Change a password

Click the key icon for the account in the list and enter the new password twice. When complete, “Password changed” is displayed.

- Administrators can change the password of any account. The current password is not required.
- The new password must be at least 4 characters long.
- Regular users cannot change their own passwords. An administrator must change them.



3. Delete a user

Click the trash can icon for the account in the list and confirm at “Delete this user?” Deleted accounts cannot be recovered, so check the account again before deleting it.

- The account with the ID admin cannot be deleted. If you try, it remains in the list without any message.
- Other administrator accounts can be deleted. You can also delete the account currently logged in.
- Nothing is displayed if deletion fails. Check whether the account has disappeared from the list.

Existing sessions

Changing a password or deleting an account does not immediately invalidate authentication that has already been issued. It remains usable for up to 24 hours after issuance.

If you forget your password

There are two options, depending on the situation.

- If another administrator account exists, log in with that account and change the password.
- If you cannot log in to an administrator account, you must perform a factory reset. Press the button on the back of the device for 3 seconds to start a factory reset without logging in.

A factory reset deletes the accounts, all settings, and events, and restores the device to its factory-default state. It cannot be undone, so use it only when there is no other option. See System Settings for the items that are deleted.

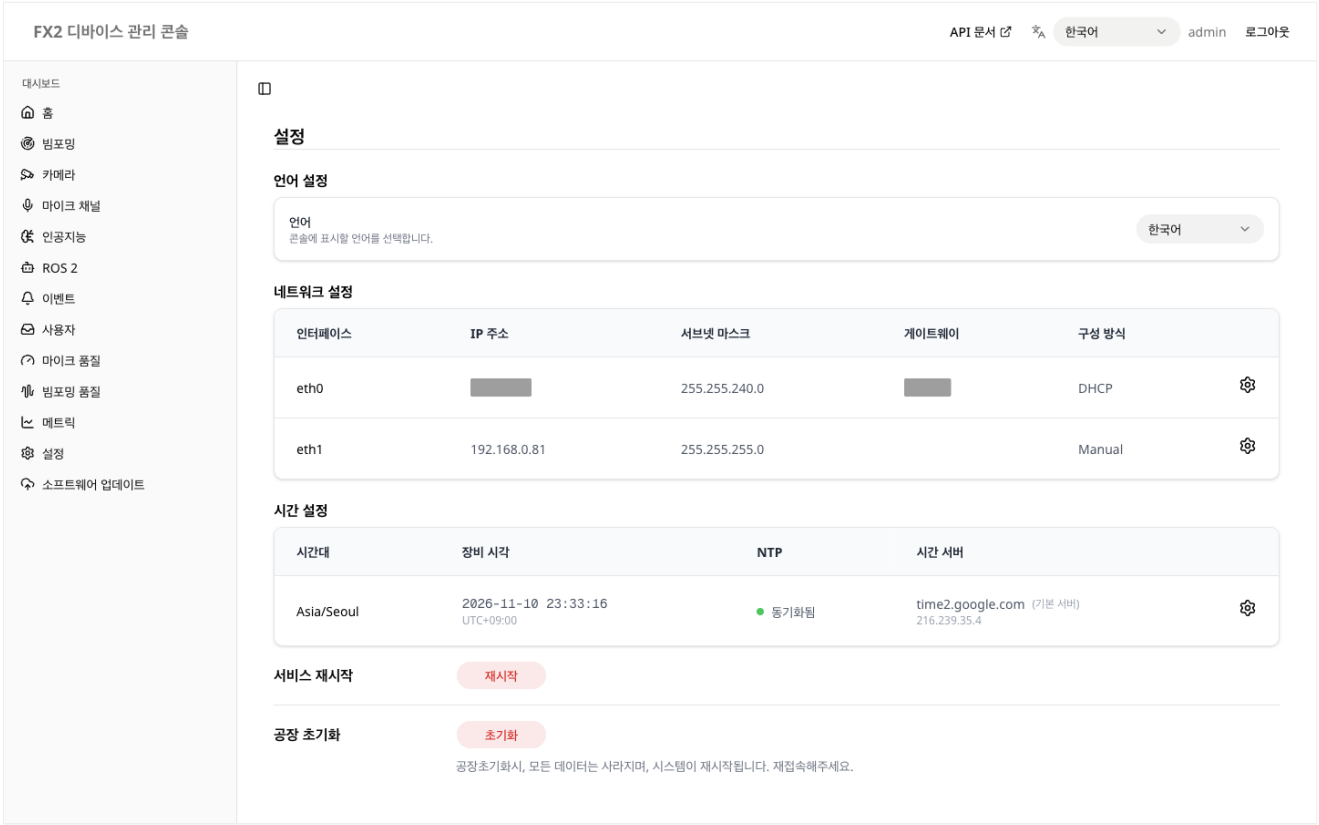
System Settings

In the Settings menu, you can set the language, network, and time, restart services, and perform a factory reset. This page explains each item in the Settings menu and how to use the Metrics menu.

The Settings screen shows the following items from top to bottom.

- Language Settings
- Network Settings
- Time Settings
- Service Restart
- Factory Reset

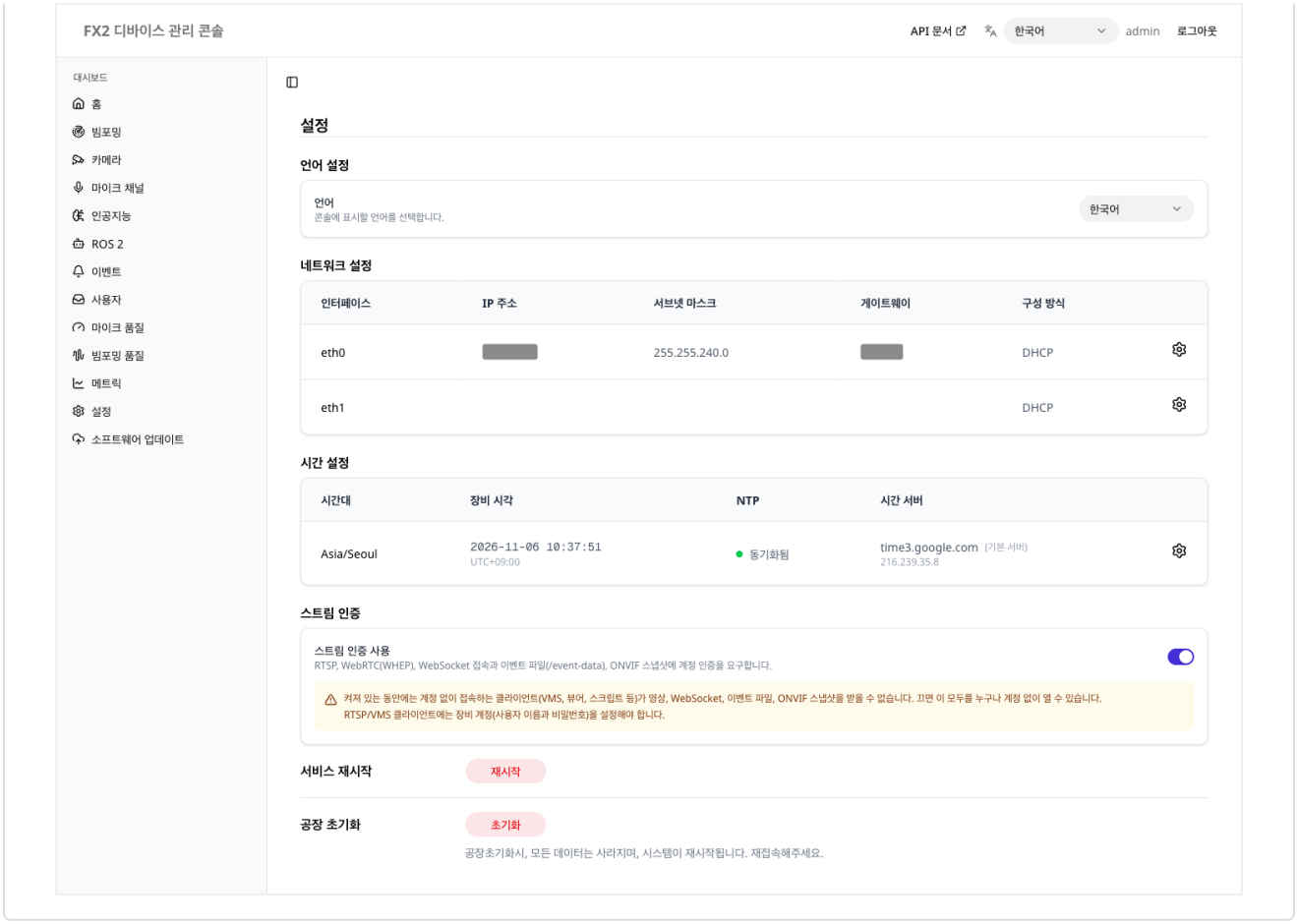
Network Settings, Time Settings, Service Restart, and Factory Reset require administrator privileges. For what appears under a regular user account, see User Accounts and Permissions.



Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Stream Authentication appears between Time Settings and Service Restart. It is visible only to administrator accounts and requires administrator privileges.



Language Settings

Choose the language displayed in Device Manager. Select from 한국어, English, 简体中文, 日本語, and Tiếng Việt. The screen reloads when you make a selection.

The language selection is saved in the browser for one year. It is not saved on the device, so you must choose it separately in each browser.

Network Settings

Set the IP addresses of the device's two Ethernet ports, eth0 and eth1. Administrator privileges are required.

The table shows the interface, IP address, subnet mask, gateway, and configuration method. The configuration method is “DHCP” or “Manual”. Use the gear button at the end of each row to open its settings dialog.



Factory settings

- eth0 port — 192.168.0.80, subnet mask 255.255.255.0, gateway 192.168.0.1
- eth1 port — 192.168.0.81, subnet mask 255.255.255.0, no gateway

The eth1 port is intended for a direct connection to a PC. On a newly installed device, eth1 comes without a gateway. A device whose firmware has been updated retains its previously saved network settings.

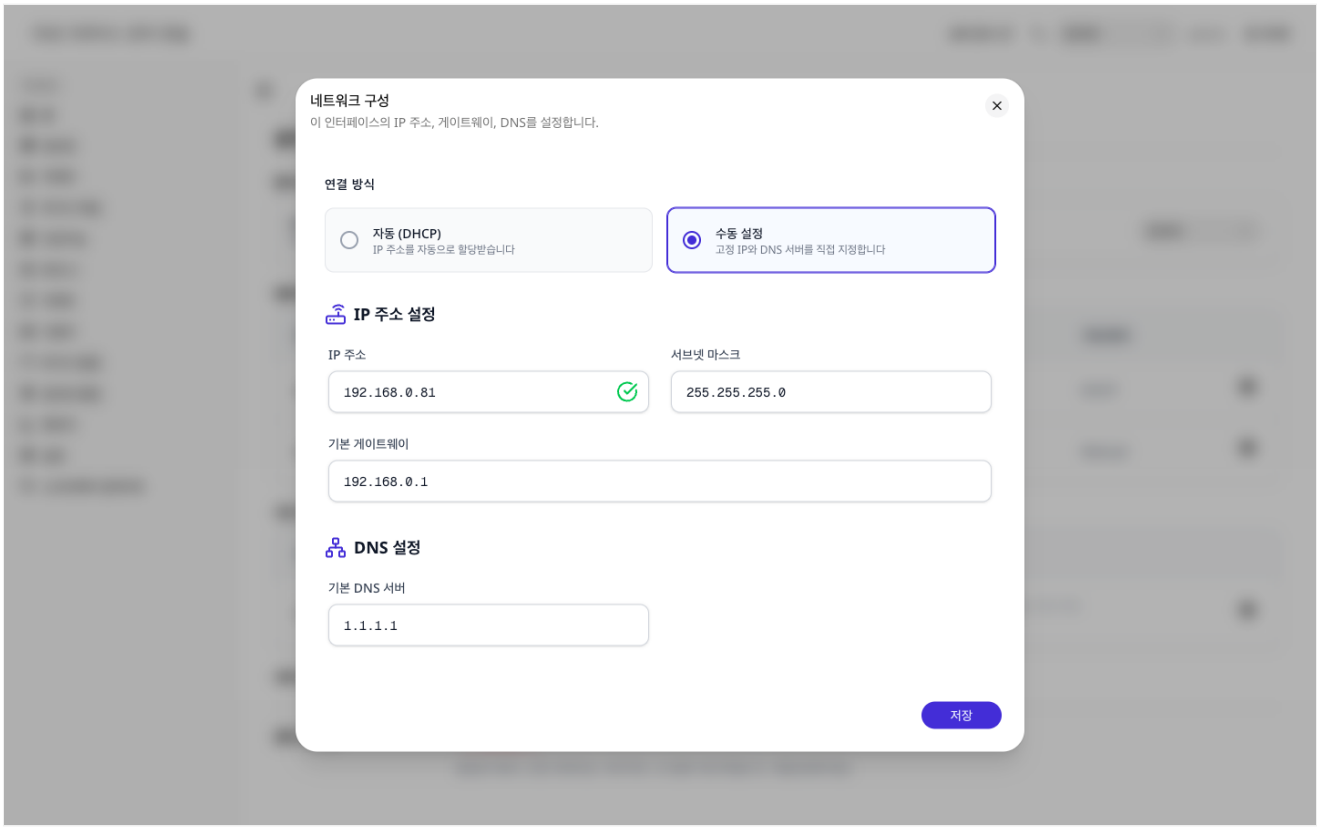
Port settings dialog

Set the following in the “Network Configuration” dialog.

- Connection method — “Automatic (DHCP)” or “Manual Configuration”
- IP address, subnet mask — Required for manual configuration.
- Default gateway — May be left blank.
- Default DNS server — May be left blank.

If you choose “Automatic (DHCP)”, the IP address, subnet mask, default gateway, and default DNS server fields turn gray and cannot be edited.

The default DNS server field is prefilled with 1.1.1.1 every time you open the dialog. This is not a value loaded from the device. To use another DNS server, enter it yourself.



Input rules

Enter an IP address as four numbers separated by periods. Each number must be from 0 to 255. Numbers with two or more digits cannot start with 0. For example, enter 10 instead of 010. This is because the browser interprets 010 as an octal number.

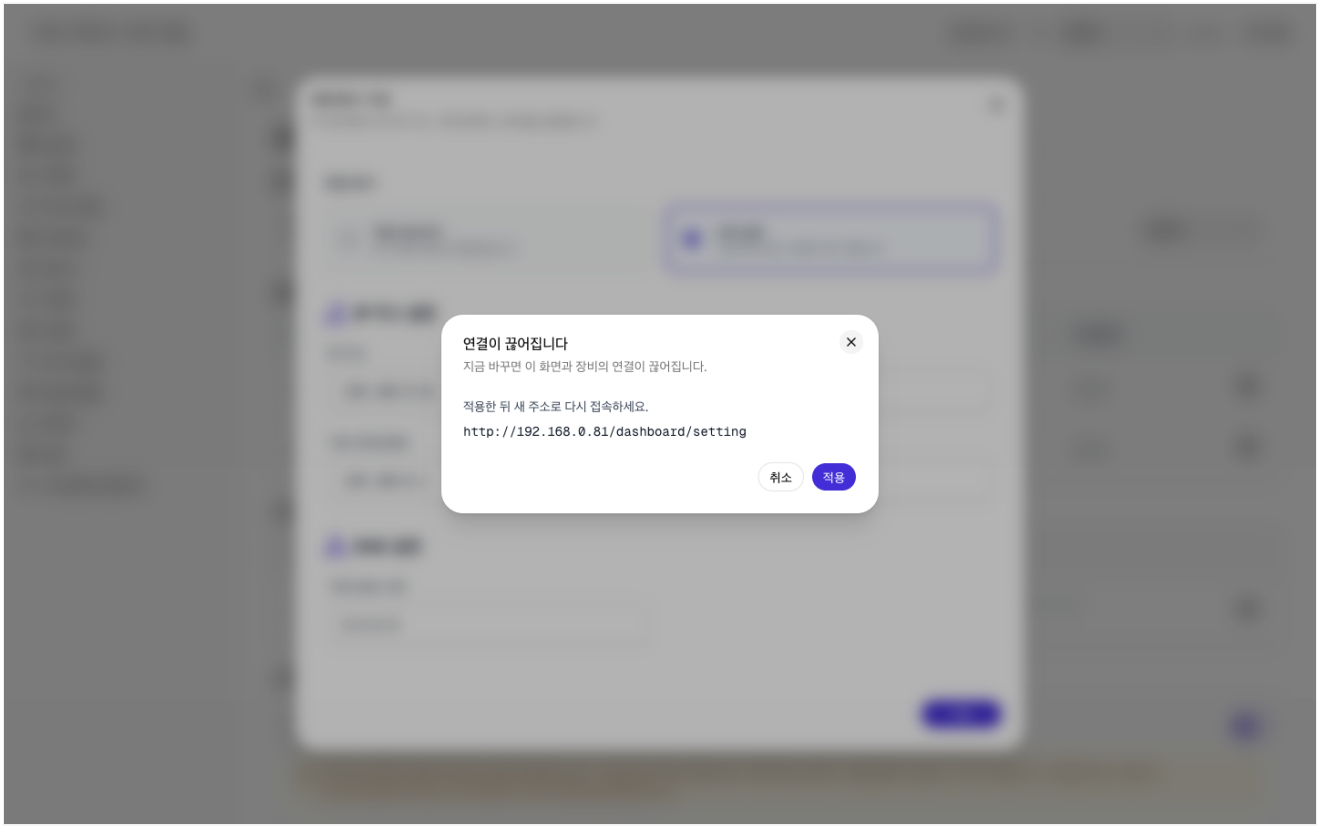
If the format is invalid, “Invalid IP address format. (Example: 192.168.0.10)” appears. If any field has an invalid format, pressing “Save” displays “Check your input” and identifies the field.

Changes that disconnect you

If you change the address of the port you are currently using to connect, this screen will lose its connection to the device. In this case, a “You will be disconnected” dialog appears before the change is applied.

- Changing one static IP address to another — The new address is shown. After applying the change, reconnect using the new address.
- Changing a static IP address to DHCP — The new address is assigned by the DHCP server (such as a router), so it cannot be shown on the screen. Check the address assigned to the device by the DHCP server, then connect to it.

Press “Cancel” to leave everything unchanged. Press “Apply” to start the change.



The following changes are applied immediately without a confirmation dialog.

- Changing DHCP to DHCP
- Leaving the IP address unchanged
- Changing a port other than the one used for the current connection

After applying the change, the screen waits up to 8 seconds for a response from the device. The result appears in the settings dialog.

- “Settings sent. Reconnect using the new address:” and a link to the new address — The device confirmed the change.
- “No response received, so it is not known whether the settings were applied. Try connecting to the new address. If that fails, save again:” — The result could not be confirmed. Try connecting to the new address; if you cannot connect, save again.

If you changed to DHCP, the messages above are replaced with “Settings sent. Check the new address assigned to the device by the DHCP server, then reconnect.” or “No response received, so it is not known whether the settings were applied. Check the device address on the DHCP server and try connecting. If that fails, save again.”

For a change that does not disconnect you, the settings dialog closes and the screen reloads when saving is complete.

DHCP and gateway behavior

- If you change from a static IP address to DHCP and the DHCP server does not assign an address, the DHCP setting remains in effect. The device continues trying to obtain an address and accepts one when it becomes available. It does not revert to the previous static IP address.
- If both ports have a gateway, eth0 is used for the default route.
- Even if both ports are on the same subnet, each port responds through itself to requests sent to its own address. Connect using the address of the port with the cable attached.

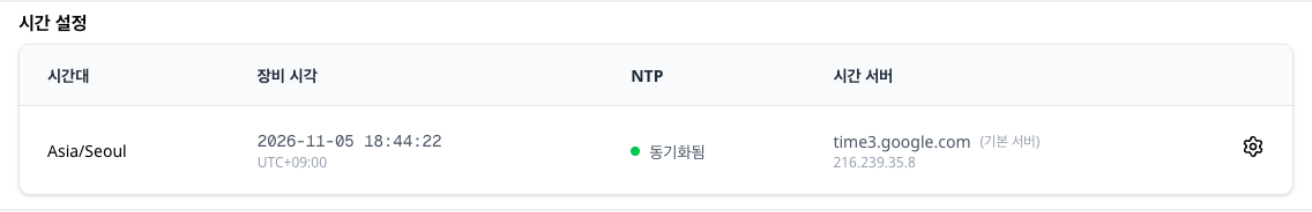
Time Settings

Set the device's time zone and time servers (NTP). Only an administrator can change the time settings. Regular user accounts can see the table but not the gear button.

The table shows the following items.

- Time zone — The device's time zone.
- Device time — The device's current time. The offset from UTC is also shown.
- NTP — The synchronization status: “Disabled”, “Synchronizing”, or “Synchronized”.
- Time server — The time server currently in use. If no server has been specified, “Default server” is shown.

The NTP and time server information is refreshed every 30 seconds.



Time Settings dialog

Press the gear button to open the “Time Settings” dialog.

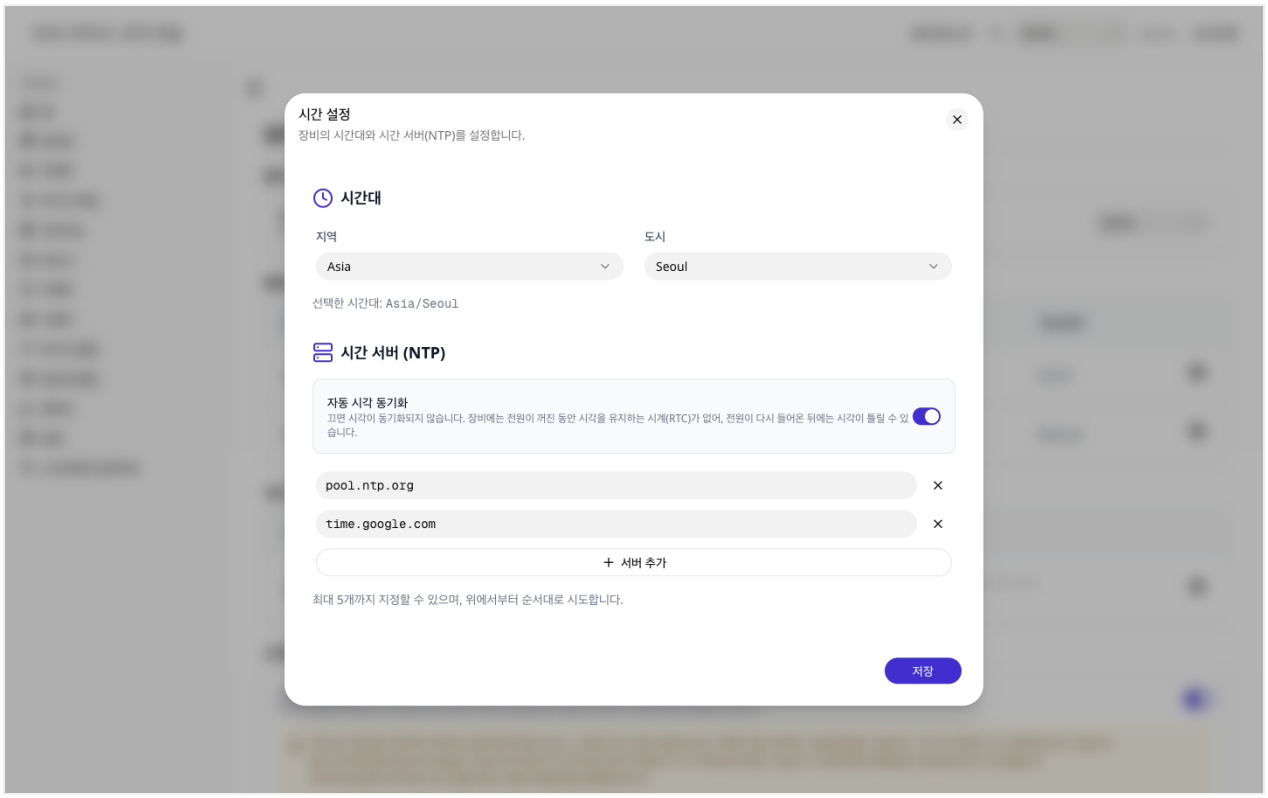
- Time zone — Choose a “Region”, then a “City”. The selected time zone name appears in the dialog.
- Automatic time synchronization — Turn NTP on or off. When it is off, the time is not synchronized and the time server list is disabled. The device has no RTC to maintain the time while power is off, so its time may be incorrect after it is powered on again with synchronization off.
- Time servers — Specify up to five. The servers are tried in order from top to bottom. Use “Add Server” to add a row and the “X” at the end of a row to remove it.

In firmware v1.1.0, the Time Settings dialog says that, when automatic time synchronization is off, time continues based on the device's RTC. This description is incorrect because the device has no RTC.

Pre-release software (v1.1.1-beta.1)

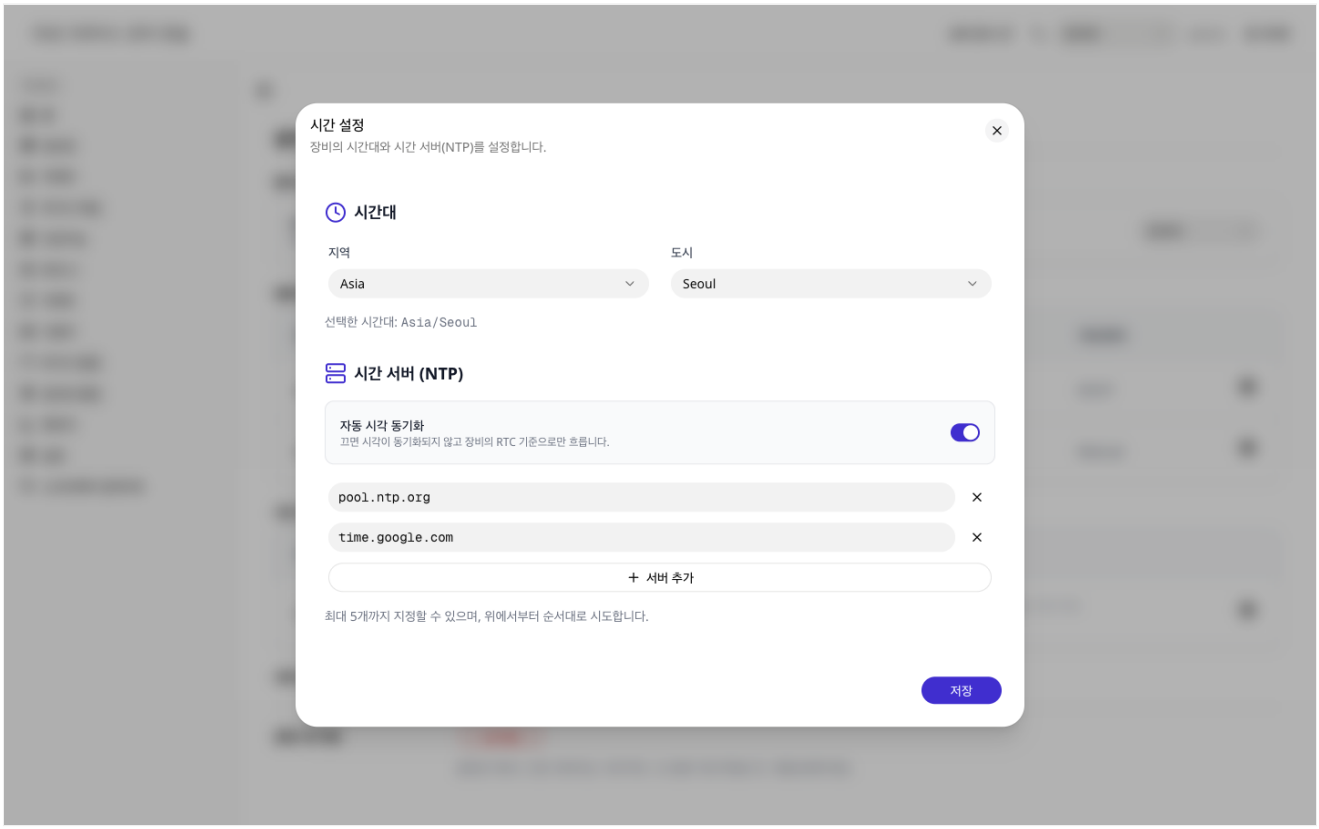
This information is based on firmware v1.1.1-beta.1 and may change in the official release.

The description of automatic time synchronization in the Time Settings dialog has changed. It now says that the device has no RTC to maintain the time while power is off, so its time may be incorrect after it is powered on again if automatic time synchronization is disabled.



Enter servers as hostnames or IP addresses. If a format is invalid, “One or more server addresses are invalid. Enter a hostname or IP address.” appears, and you cannot save.

If you enter no time servers, the default servers time1.google.com, time2.google.com, time3.google.com, and time4.google.com are used. Check the Time Settings table to see which server is currently used for synchronization.



Press “Save” to apply the settings immediately. A service restart or reboot is not required. If you change the time servers, “Synchronizing” may appear briefly, and the time may jump significantly all at once.

Where time has an effect

- AI operating time periods — Based on device time.
- Recent events on Home and the time in the video status bar — Displayed in the device's time zone.
- Creation time in the Events menu — Displayed in the browser's time zone.

Changing the time zone does not change the records of previously saved events. Only the displayed times change.

※ BATCAM FX2 has no RTC (built-in clock). If power is turned off while it is not connected to a time server (NTP), the device loses its time. When powered on without NTP, the device time starts at 1970-01-01T00:00:00. Specify a time server the device can reach. On an isolated network without an external connection, you can use a time server on-site. After powering on, check that the device time is correct under Settings → Time Settings.

Stream Authentication

This feature is available starting with firmware v1.1.1. In firmware v1.1.0, an account is not required for RTSP video, WebRTC video, WebSocket, ONVIF snapshots, or event files.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Stream Authentication requires a device account for RTSP video, WebRTC video, WebSocket, ONVIF snapshots, and event files. It is on by default and can be changed only by an administrator. Regular user accounts do not see this item.

- “Use Stream Authentication” switch — A change is saved and applied immediately. No reboot or service restart is required.
- On — Enter a device account in the VMS, viewer, or script to receive video and data. Both administrator and regular user accounts work.
- Off — Anyone can receive them without an account. Turn this off only when you must use an older VMS or viewer that cannot provide an account.

※ If you turn it back on after it has been off, video and WebSocket connections established without an account are disconnected. Video in Device Manager continues to play.

※ The Stream Authentication item also displays this notice: “ROS 2 topics (including camera video topics) are not subject to stream authentication, so anyone on the same DDS domain can receive them without an account. To protect them, we recommend placing the device on a separate network.” For details, see ROS 2 Integration.

※ The same setting can be changed through REST `PATCH /setting/stream` (`{"auth": false}` or `{"auth": true}`). An administrator account is required.



For details, see Security and Accounts under External System Integration.

Metrics

Use the Metrics menu to view graphs of the device's CPU load, temperature, core frequency, and humidity. The menu is named “Metrics”, and the screen title is “System Metrics”. Both administrators and regular users can view it.

There are four graphs.

- CPU load — Measured in %.
- Temperature — Shows CPU and board temperatures in °C.
- Core frequency — Measured in MHz.
- Humidity — Measured in %.

Values update every 5 seconds, and the most recent hour is shown. The horizontal axis shows time in the browser's time zone. Hover over a graph to see values.



Use these graphs to check how temperature and humidity change in the installation environment. Compare the values at the installation site with the operating temperature and humidity ranges in Product Specifications and Configuration. If a sensor cannot read a value, its graph is empty.

Service Restart

Restart the measurement and video programs without turning off the device. Administrator privileges are required.

Pressing “Restart” starts the process immediately, without a confirmation dialog. Check any work in progress before pressing it.

- Video and measurements pause briefly. AI and ROS 2 also restart.
- Device Manager may briefly stop responding.
- After the request is sent, “Restarting services” appears. If the request succeeds, it changes to “Services restarted”. Video and measurements may resume shortly afterward.
- The device does not reboot.

Video and measurement data usually resume within a few seconds after a service restart. Check the live screen to confirm that the video and measurements are updating.

A service restart is required after changing the resolution in the Camera menu. The resolution is saved to the settings immediately, but the change takes effect in the video only after the services restart.



Reboot

Device Manager has no reboot button. To restart the entire device, turn its power off and then on again. Developers can request a reboot through REST. For details, see API and Developer Integration.

Factory Reset

Delete settings, accounts, and events, and return the device to its factory state. Administrator privileges are required.

Pressing “Reset” starts the process immediately, without a confirmation dialog. Before pressing it, download any events you need and record your settings. A factory reset cannot be undone once it starts.

What is deleted

- All accounts — Restored to the factory-default accounts.
- All settings — Network, camera, AI, ROS 2, Modbus TCP, and event settings return to their factory defaults.
- The entire event list and all event files
- System logs

What remains

- Camera calibration values — Camera center and field-of-view calibration values.
- Installed firmware and FPGA

※ Reinstalling the device image deletes the device-specific camera calibration values. Contact your service representative before reinstalling it.

After the reset

“Factory reset in progress” appears, and you are immediately logged out and taken to the login screen. The device stops all services and then reboots.

- Network — eth0 returns to 192.168.0.80 and eth1 to 192.168.0.81. Set your PC's network to this address range, then reconnect.
- Login — Log in with the factory-default administrator account (ID `admin`, password `1234`). The same credentials are shown in a notice below the login screen. You must change the password after your first login.

In firmware v1.1.0, other browsers and programs can continue using login credentials (tokens) obtained before the factory reset for up to 24 hours after they were issued.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

- Other browsers and programs — All login credentials (tokens) obtained before the factory reset become invalid. You must log in again.
- Stream Authentication — Returns to On.

If you perform a factory reset remotely, the device address may change and prevent you from reconnecting.

Firmware Update

You can update the device firmware to a new version from the Software Update menu. This page explains what to prepare before updating, the update sequence, how an update is confirmed or rolled back to the previous firmware, and automatic FPGA version matching.

Settings, accounts, and events remain unchanged after the update. You do not need to download events separately beforehand.

Before you begin

- Log in with an administrator account. If you upload using a regular user account, “Upload failed (HTTP 403)” appears.
- Prepare the file that matches the device’s camera model.
- Do not turn off the power or disconnect the Ethernet cable until the update is complete.
- Perform the update over an Ethernet connection.

File for your camera model

Firmware files differ by camera model. Their extension is `.mender`.

- SMIA462 Wide — `fx2-cm5-arducam-v<version>.mender`
- SMI3708 Wide — `fx2-cm5-imx708-v<version>.mender`

Check the camera model under Home → Device Information → “Camera Model.”

If you upload a file for the wrong device type, such as firmware for a different camera, the screen still displays “Upload successful.” The device reboots without an installation failure notice, and the firmware version remains unchanged. Video and measurements stop, so check the filename before uploading.

Where to get the file

Request the firmware file through Product Support and Inquiries.

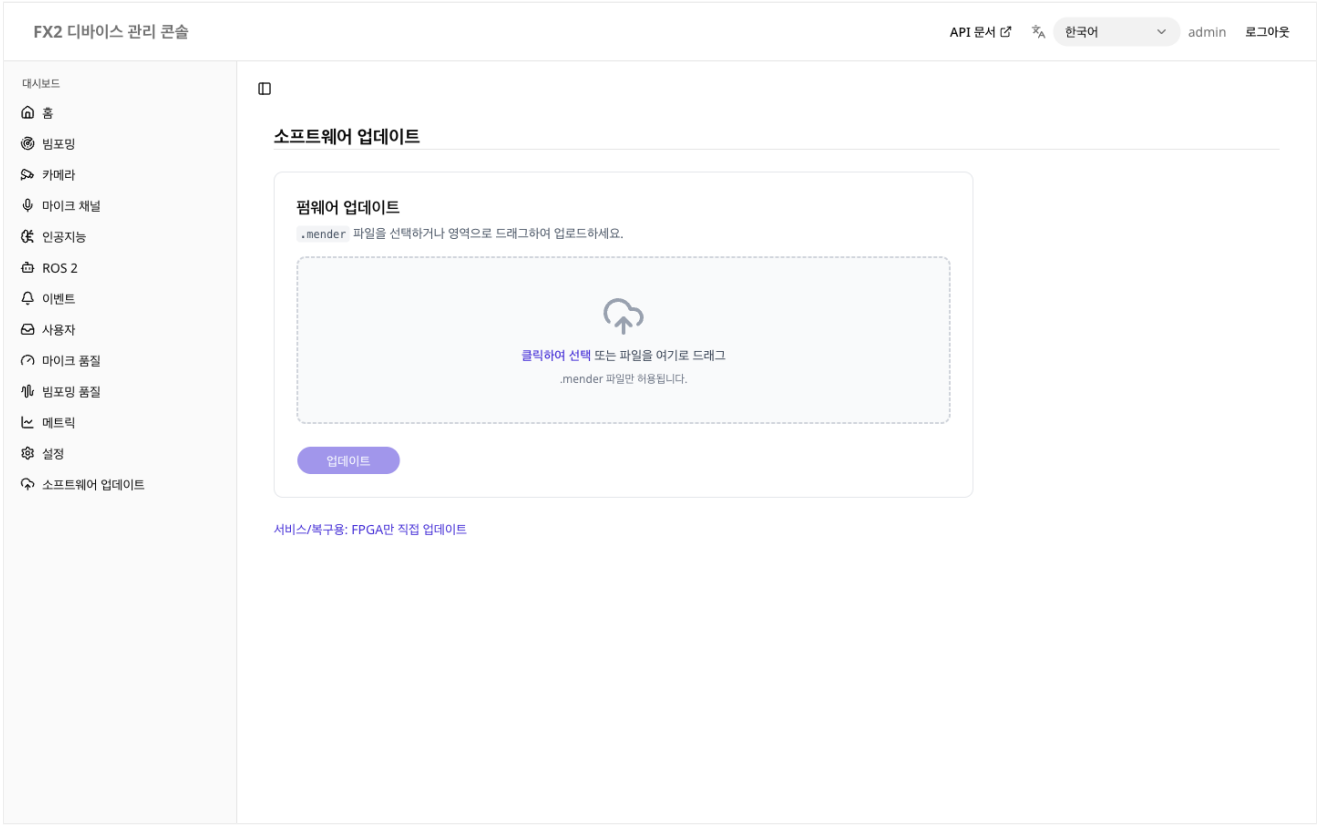
Update sequence

The full sequence is as follows.

- Upload the file
- Install (about 2 minutes)
- Reboot
- Check the trial boot
- Confirm

1. Open the update screen

Open the Software Update menu. The “Firmware Update” card appears.



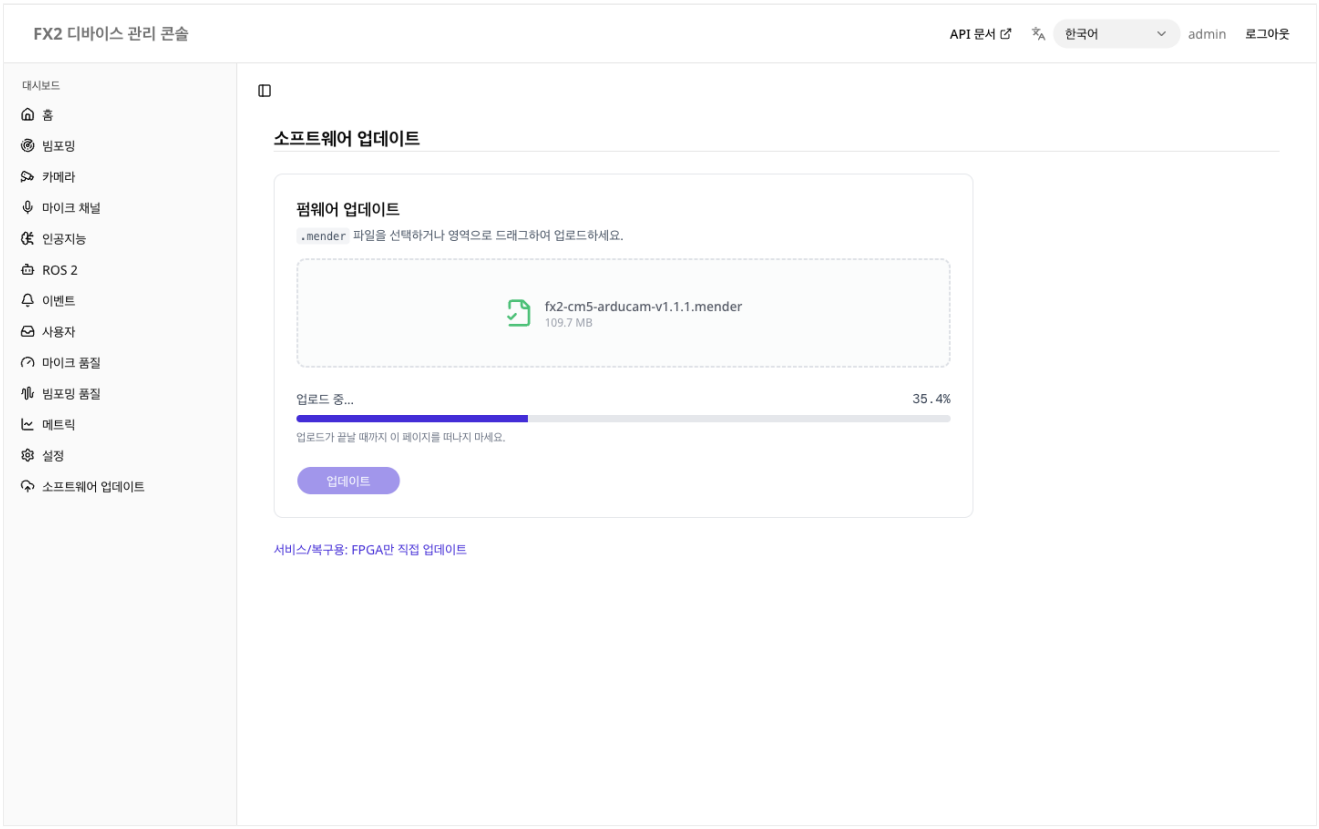
2. Upload the file

Click the area in the card to choose a file, or drag and drop a file into it. Once selected, the filename and size appear.

- For a file other than `.mender`, “Only .mender files can be uploaded.” appears, and the file is not selected.
- The maximum upload size is 1 GB.

Click “Update” to start the upload. Progress is shown as a percentage.

Do not leave this page until the upload finishes. The browser warns you if you try to close or leave the page during the upload.



If the upload fails, one of the following appears in the card.

- “Upload failed (HTTP 403)” — You are not using an administrator account.
- “Upload failed due to a network error.” — Check the network connection and upload again.
- “Upload canceled.”
- “Authentication information is missing. Please log in again.” — Log in again.

3. Installation and reboot

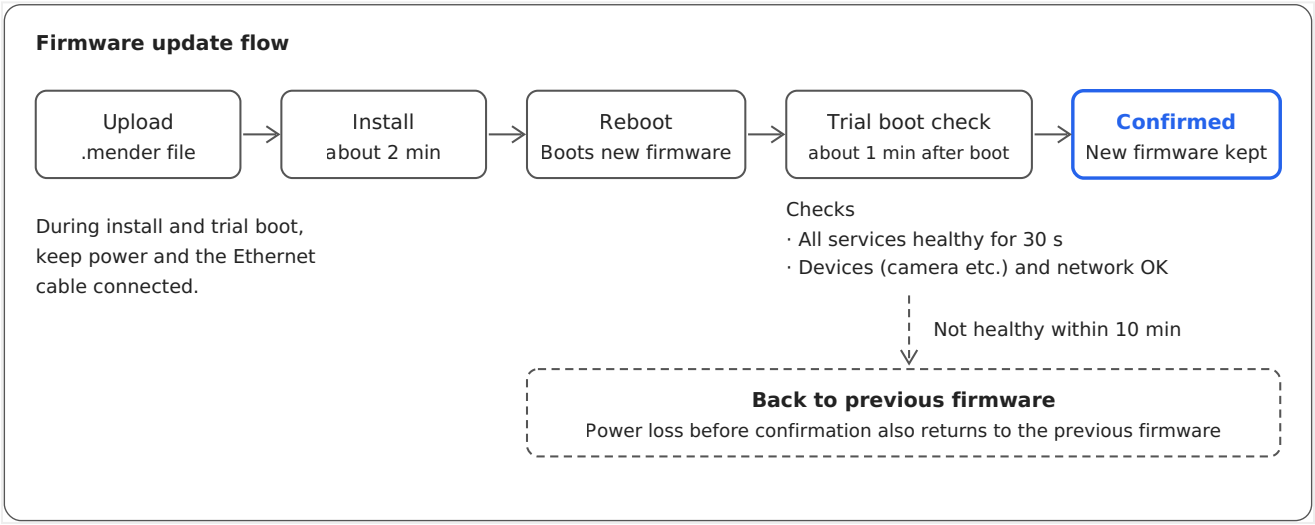
When the upload finishes, “Upload successful. Installation will take a few minutes (about 2 minutes). The device will restart after installation is complete.” appears.

- Video and measurements stop during installation.
- The device reboots automatically when installation finishes.
- Do not turn off the power before the reboot finishes.

While installation is in progress, you cannot run an FPGA update, factory reset, or service restart at the same time.

4. Trial boot and confirmation

After booting with the new firmware, the device checks it in a trial boot state instead of confirming it immediately.



The device checks the following.

- All device services operate normally for 30 seconds without restarting.
- Devices such as the network port and camera are all detected.
- The device or gateway recorded during installation responds.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

If there is no peer to check for network connectivity, or only the current gateway is a response target, a record of packets sent and received through an Ethernet port with an IPv4 address also passes the check.

If everything is normal, the update is confirmed about 1 minute after booting. Once confirmed, the device continues using the new firmware.

In the following cases, the update is not confirmed and the device returns to the previous firmware.

- The conditions above are not met within 10 minutes of booting.
- Power is lost or the device reboots before confirmation.

When returning to the previous firmware, the device reboots once more. The rollback may take more than 10 minutes. You can update a device again after it returns to the previous firmware. If the device freezes during the trial boot, you must turn it off and back on for it to return to the previous firmware.

※ Events saved by the new firmware during the trial boot are not visible after returning to the previous firmware.

If the PC and device are connected directly, keep the cable connected and the PC powered on until the trial boot finishes. The device may return to the previous firmware if the cable is disconnected between installation and reboot, or if the uploading PC is turned off and there is no gateway. With firmware v1.1.0, a device with only its eth0 port connected directly to a PC may return to the previous firmware if the gateway does not respond.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

The issue where a device with only its eth0 port connected directly to a PC returned to the previous firmware when the gateway did not respond has been fixed. The issue where the device restarted after the update had already been confirmed has also been fixed. However, if a PC as well as the gateway was recorded as a peer during installation and neither responds, the device may return to the previous firmware even if packets are being exchanged. If the cable is disconnected, the device returns to the previous firmware as before.

5. Verify the update

When the reboot finishes, reconnect to Device Manager.

- Check that “Firmware Version” under Home → Device Information shows the new version.
- Check “FPGA Version” as well.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

After updating to v1.1.1, the login screen appears, so log in again. API clients must also obtain new tokens.

※ After updating to v1.1.1, RTSP video, WebRTC video, WebSocket, ONVIF snapshots, and event files require a device account (stream authentication, enabled by default). Before updating, add the device account to your VMS, viewer, and scripts. For details, see Security and Accounts under External System Integration.

※ Robot programs integrated through ROS 2 must be rebuilt with message package fx2_stream_msgs 2.0.0. Prepare the robot side before updating. For details, see ROS 2 Integration.

Automatic FPGA version matching

Firmware v1.1.0 includes FPGA 2.0.2. After the firmware update is confirmed, the device acts as follows based on the FPGA version it reads.

- If it is the official 2.0.2 release, or a version higher than 2.0.2 and no higher than 2.0.3, the device keeps it.
- If it is lower than 2.0.2, higher than 2.0.3, or a development build of 2.0.2, the device changes it to 2.0.2.
- If the version cannot be read, the device does not flash the FPGA automatically.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Firmware for v1.1.1 includes the official FPGA 2.0.3 release. After the firmware update is confirmed, the device acts as follows based on the FPGA version it reads.

- If it is the official 2.0.3 release, the device keeps it.
- If it is a lower or higher version, or a development build of 2.0.3, the device changes it to the official 2.0.3 release.
- If the version cannot be read, the device does not flash the FPGA automatically.

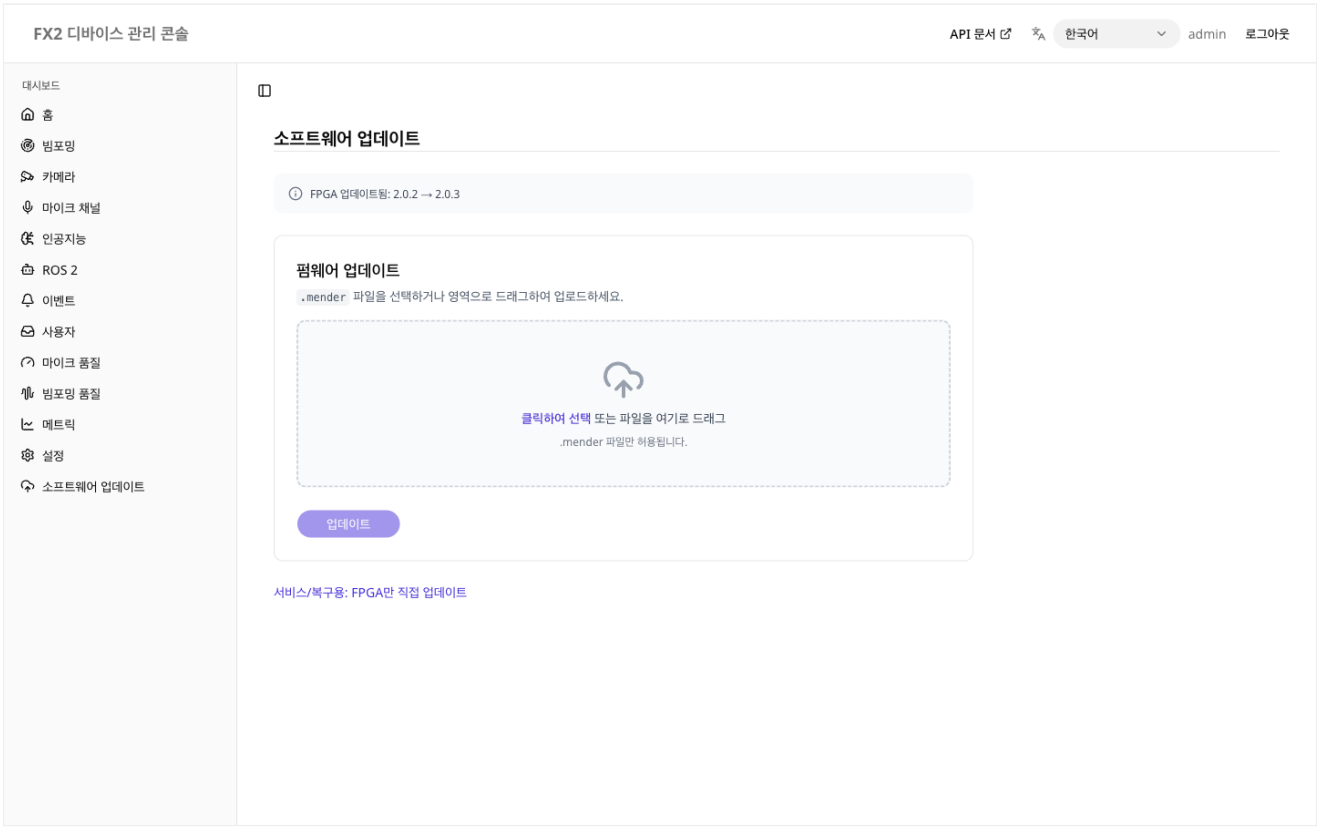
Do not turn off the power while the FPGA is being changed. The device may restart afterward.

If the FPGA change fails, the device does not retry automatically. It continues operating with the FPGA it was using.

Messages on the update screen

FPGA status appears at the top of the Software Update menu. Nothing is displayed if the version already matches or is left unchanged.

- “Updating FPGA. Do not turn off the power. The device may restart when complete.” — The FPGA is being changed. Wait.
- “FPGA updated: {previous version} → {new version}” — The FPGA was updated.
- “FPGA downgraded: {previous version} → {new version}. The FPGA included with this firmware is an earlier version.” — The FPGA included with the firmware was lower than the current version, so it was downgraded.
- “Failed to update FPGA after firmware installation.” — This is a red notice. The device continues operating with the current FPGA and does not retry automatically. Contact the support address shown on the screen.
- “Could not read the FPGA version, so no update was attempted.” — The FPGA was not changed. Contact information is also shown.
- “FPGA check is waiting for firmware update confirmation. If this continues after rebooting, contact support.” — This is normal for about 1 minute immediately after the update. Contact support if the message remains for more than 15 minutes.



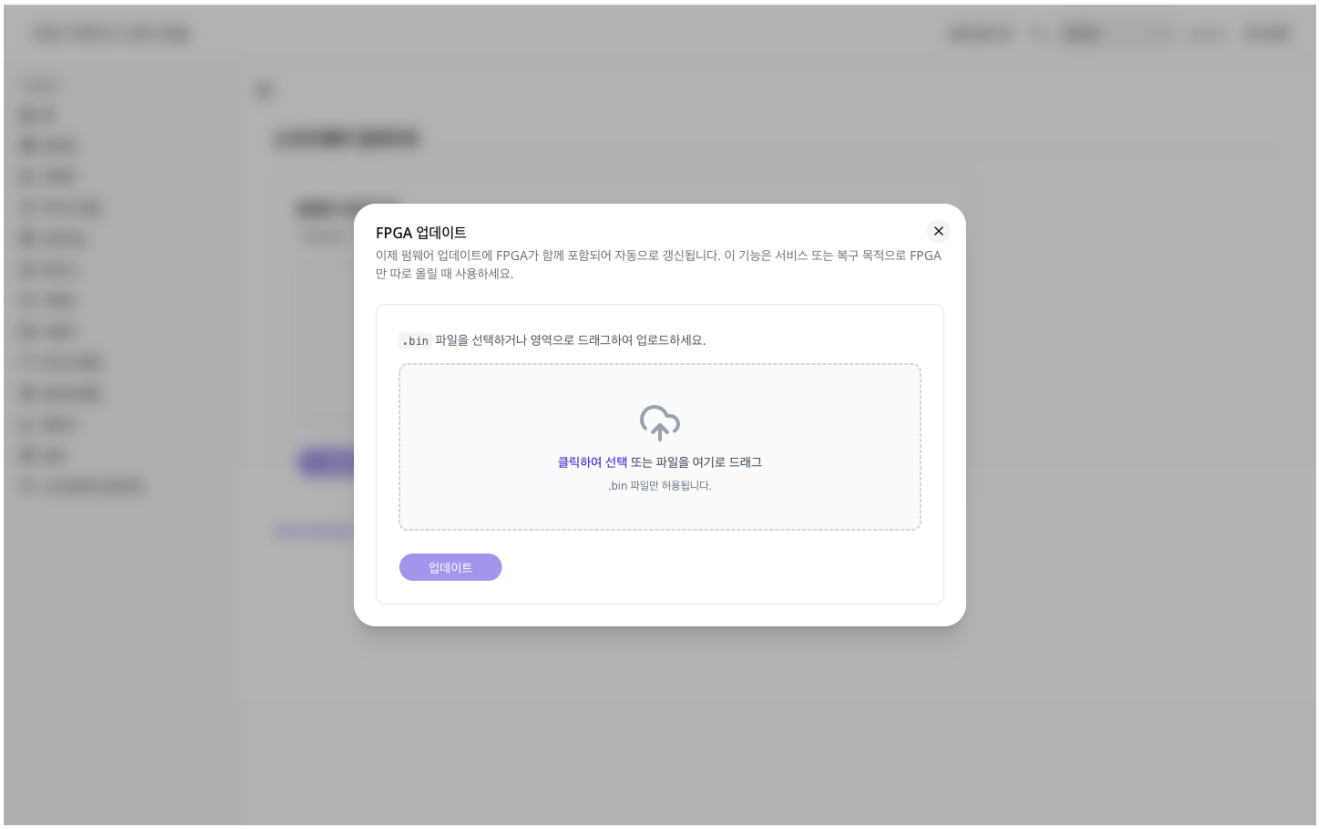
Manually update only the FPGA

If the device cannot read the FPGA version, it does not flash the FPGA automatically. An administrator can upload an FPGA file manually when service or recovery is needed.

Click the “For service/recovery: Update only the FPGA manually” link below the Software Update menu to open the “FPGA Update” window. Upload an FPGA file with the `.bin` extension. Administrator privileges are required. Request a recovery FPGA file through Product Support and Inquiries.

- You cannot close the window during the upload.
- Changing the FPGA takes a few minutes, and the device reboots when it finishes. Do not turn off the power during this time.
- If the version in the filename is lower than the current FPGA version, “The selected file appears to be an earlier version than the currently running FPGA ({version}). If you continue, the FPGA will be changed to the earlier version.” appears.

※ An FPGA uploaded manually also follows the automatic version-matching rules above on the next boot.



Older firmware cannot be installed

You cannot install firmware older than v1.1.0 through an update. The installation is rejected.

If you need older firmware, the device’s firmware image must be reinstalled. Request firmware image reinstallation through Product Support and Inquiries.

※ This restriction applies only to installation through an update. It does not prevent a device from returning to the previous firmware when an update is not confirmed.

External System Integration

BATCAM FX2 can send video, measurements, and events to other systems such as VMSs, PLCs, and robots. This page helps you choose a method for each type of system and explains the connection details.

Choose an integration method

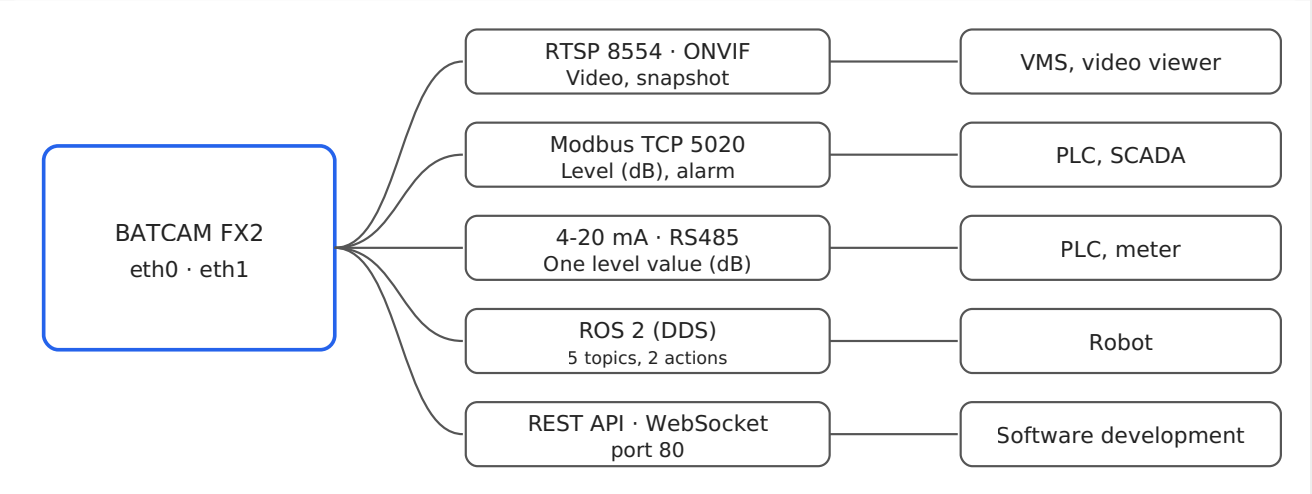
Choose a method that matches the system you want to connect.

System to connect	Method	Data received
VMS, video viewer	RTSP, ONVIF	Video with a heatmap overlay
PLC, SCADA	Modbus TCP	Level (dB), alarm
PLC, measuring instrument (analog input)	4-20 mA, RS485	One level (dB) value
Robot	ROS 2	Beamforming results, audio, AI assessments
Software development	REST API, WebSocket	Settings, events, real-time data

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Robots can also receive camera video through ROS 2, along with beamforming results, audio, and AI assessments.



For REST API and WebSocket, see API and Development Integration. For ROS 2, see ROS 2 Integration.

Security and accounts

In firmware v1.1.0, no account is required for RTSP or WebRTC video, WebSocket real-time data, ONVIF snapshots, or event files (photos, video, audio, and measurement data). Anyone who can access the device can receive them.

The following connections also do not require authentication.

- ONVIF services (device discovery and queries) — no authentication
- Modbus TCP — no authentication. It is off by default and should be enabled only when needed.
- ROS 2 topics and actions — no authentication. For details, see ROS 2 Integration.

※ The device must be used only on an internal network that cannot be accessed from outside.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

A device account is required to receive RTSP or WebRTC video and WebSocket real-time data. This is called stream authentication and is enabled by default starting with firmware v1.1.1. Use the same account you use to log in to Device Manager; both administrator and regular user accounts work.

- RTSP video — account required
- WebRTC (Device Manager video) — account required. Device Manager uses your existing login information.
- WebSocket — account required
- ONVIF snapshots — account required
- Event files (photos, video, audio, and measurement data) — account required
- ONVIF services (device discovery and queries) — no authentication
- Modbus TCP — no authentication. It is off by default and should be enabled only when needed.

- ROS 2 topics and actions — no authentication. Anyone in the same DDS domain can view video through the video topic without an account, even when stream authentication is enabled. For details, see ROS 2 Integration.

※ Account information is transmitted over unencrypted RTSP and HTTP. The device must be used only on an internal network that cannot be accessed from outside.

1. Turn off stream authentication

This feature is available starting with firmware v1.1.1.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

If you need to use an older VMS or viewer that cannot accept account credentials, an administrator can turn off stream authentication. Turn it off under Settings → Stream Authentication, or send `{"auth": false}` to REST `PATCH /setting/stream`. No reboot is required. Once it is off, anyone can receive the items listed above as requiring an account without one. For details, see System Settings.

2. Repeated invalid account attempts

This feature is available starting with firmware v1.1.1.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

If account verification fails 10 times within one minute from an address, video, WebSocket, and event file connections from that address are blocked for 60 seconds. During this period, Device Manager login information and recently successful accounts can still be used. A newly entered account may have to wait up to 60 seconds. This limit does not apply to the Device Manager login screen.

RTSP

VMSs and video viewers receive video from an RTSP address.

```
rtsp://<device-ip>:8554/overlay
```

- Path — /overlay only. The video includes a heatmap and status bar overlay. There is no raw video path (/raw).
- Port — 8554
- Authentication — none in firmware v1.1.0. Video can be received without an account.
- Transport — TCP is recommended. UDP unicast and UDP multicast are also available.

- Codec — H.264 Baseline
- Frame rate — 25 fps
- GOP — 2 seconds (50 frames)
- Resolution — the resolution set in the Camera menu. A resolution change is reflected in the stream after the service restarts.
- Audio — none

※ The encoder stops when no clients are viewing the video and starts again when a client reconnects.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

You must save a device account in the VMS or viewer. You can also include the account in the address.

```
rtsp://<ID>:<password>@<device-ip>:8554/overlay
```

- Authentication — device account. Only Basic authentication is supported; Digest authentication is not supported. Requests with missing or incorrect account credentials are rejected with 401.
- Transport — TCP is recommended. UDP unicast is also available. Multicast is rejected (461) when stream authentication is enabled. If multicast is essential, you must turn off stream authentication.

※ To play video in VLC, enter the device username and password as the RTSP credentials. Video playback with account credentials has been verified in VLC. Other VMSs and viewers may use different methods for entering credentials and were not verified when this document was written.

For instructions on changing the resolution, see Camera Settings.

WebRTC

Device Manager receives video through WebRTC. Video will not appear if a firewall or router blocks this communication.

- Address — http://<device-ip>:8889/overlay/whep
- Ports — TCP 8889, UDP 8189
- Authentication — none in firmware v1.1.0.
- Simultaneous viewing — up to 10 connections

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

A device account is also required for WebRTC video. Device Manager uses your existing login information, so you do not need to enter credentials separately.

If video does not appear, see Troubleshooting for checks to perform.

ONVIF

A VMS that supports ONVIF can automatically discover the device and obtain its video address.

- Device discovery — WS-Discovery (UDP 3702). The device responds only to discovery requests.
- Service addresses — http://<device-ip>/onvif/device_service, http://<device-ip>/onvif/media_service
- Video address — GetStreamUri returns rtsp://<device-ip>:8554/overlay. The address does not include account credentials.
- Snapshot address — GetSnapshotUri returns http://<device-ip>/onvif/snapshot/overlay. It provides the current screen as a JPEG image with a heatmap overlay.
- Profile — overlay only
- Authentication — in firmware v1.1.0, device discovery, service queries, video (RTSP), and snapshots all require no authentication

※ BATCAM FX2 is not an officially ONVIF-conformant certified product. Its ONVIF implementation supports six device information operations and seven media operations, including queries for device information, profiles, GetStreamUri, and GetSnapshotUri. Events, setting changes, and user management are not available through ONVIF.

※ Registering and using the device in an actual VMS had not been verified when this document was written. Registration methods may vary by VMS.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

To receive video and snapshots, you must save a device account in the VMS. Without saved account credentials, the VMS can discover the device and obtain the video address but cannot receive video or snapshots.

- Authentication — none for device discovery and service queries. A device account (Basic) is required for video (RTSP) and snapshots.

※ The video and snapshot addresses obtained through ONVIF have been verified to work when device account credentials are provided. The method for setting credentials may vary by VMS.

Modbus TCP

PLCs and SCADA systems read the level (dB) and alarm through Modbus TCP. The device acts as a Modbus server (slave).



1. Settings

Configure it in the “Modbus TCP” card on the Events → Trigger Conditions tab. Modbus TCP is off by default.

- Enable — off by default
- Port — 5020 by default. The standard port is 502. Choose a port from 1 to 65535; ports used by the device (22, 80, 1935, 3000, 3001, 3002, 8554, 8888, 8889) cannot be used.
- Unit ID — 1 by default (1 to 247)
- Device number — 1 by default (1 to 255). The value of register 40001 is 0x4600 plus the device number.
- Allow writes — off by default. When enabled, the PLC can change the threshold, alarm hold time, and measurement band.
- Alarm hold time — 5.0 seconds by default (1.0 to 3276.7 seconds, in 0.1-second increments)

Only an administrator can change these settings, except for “Alarm hold time.” Settings take effect immediately without restarting the service. Turning Modbus TCP off closes all open connections.

2. Connection rules

- Supported functions — read (0x03), write (0x06, 0x10). Write requests are rejected when “Allow writes” is off.
- Addresses — 0 to 16 or 40001 to 40017
- Simultaneous connections — 10. An 11th connection is closed immediately.
- Idle connections — closed after 60 seconds without a request.
- A request using a different unit ID receives an exception response (0x0B).

3. Register map

There are 17 registers. The map is the same as the FX1 map.

Address	Name	Format	Read/ write	Value
40001	DEVICE_ID	U16	Read	0x4600 + device number (default 0x4601)
40002	DEVICE_CONNECTED	0/1	Read	1 if a beamforming result was received within the last 3 seconds
40003 ~ 40008	Year, month, day, hour, minute, second	U16	Read	Device time (UTC)
40009	MAX_DBx10	S16	Read	Level (dB) of the strongest peak × 10. 0 if there is no peak
40010	ALARM_FLAG	0/1	Read	1 for alarm, 0 for cleared
40011	THRESH_DBx10	S16	Read/ write	Level trigger threshold (dB) × 10. Writable range: 0 to 1200 (0 to 120 dB)
40012	THRESH_HOLDx10	U16	Read/ write	Alarm hold time (seconds) × 10. Writable range: 10 to 32767 (1.0 to 3276.7 seconds)
40013 ~ 40014	FREQ_LOW_HZ	U32	Read/ write	Measurement band lower limit (Hz). The high word comes first
40015 ~ 40016	FREQ_HIGH_HZ	U32	Read/ write	Measurement band upper limit (Hz)
40017	WATCH_ID	U16	Read/ write	Fixed at 100. Other values cannot be written

- Time — the time registers use UTC. They may differ from the device time shown in Device Manager, which applies the time zone.
- MAX_DBx10 — this is the same value the level trigger compares. Sounds below the overlay threshold are not detected as peaks, so they are read as 0.

- ALARM_FLAG — when the level trigger is enabled, this becomes 1 when the level reaches or exceeds the threshold. It returns to 0 after the level falls below the threshold and the alarm hold time elapses. This value is independent of the event cooldown.
- Writing the measurement band — requests are rejected while AI is running. Write the lower and upper limits together within the range of 100 to 98999 Hz.

4-20 mA and RS485

The device has a connector for 4-20 mA and RS485 outputs. For wiring, see the Multicable section of Product Specifications.

ROS 2 Integration

BATCAM FX2 publishes beamforming results, microphone audio, listening-point audio, and AI detection results as ROS 2 topics. A robot can receive this data and use ROS 2 actions to change the measurement band and overlay settings. This page explains how to connect the robot and device.

Available Features

- Topics — beamforming results, microphone audio, listening-point audio, partial discharge AI detection, leak AI detection
- Actions — change measurement band, change overlay
- Video — firmware v1.1.0 has no video topic. Receive video via the RTSP `/overlay` path.
- Level trigger — level trigger results are not published as a topic.

For the message fields of the five topics and two actions, see the Developer Center.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Starting with firmware v1.1.1, camera video can be received as a ROS 2 video topic, bringing the total to six topics. See Video Topic below for details. VMS and video viewers continue to receive video via the RTSP `/overlay` path.

Prerequisites

- Network — the robot and device must be on the same network.
- Domain ID — the robot and device must have the same ROS 2 domain ID.
- ROS 2 distribution — the steps below are based on Jazzy.
- QoS — the device publishes all topics with BEST_EFFORT. Subscribers must also use BEST_EFFORT. A RELIABLE subscriber will not receive data.

Pre-release software (v1.1.1-beta.1)

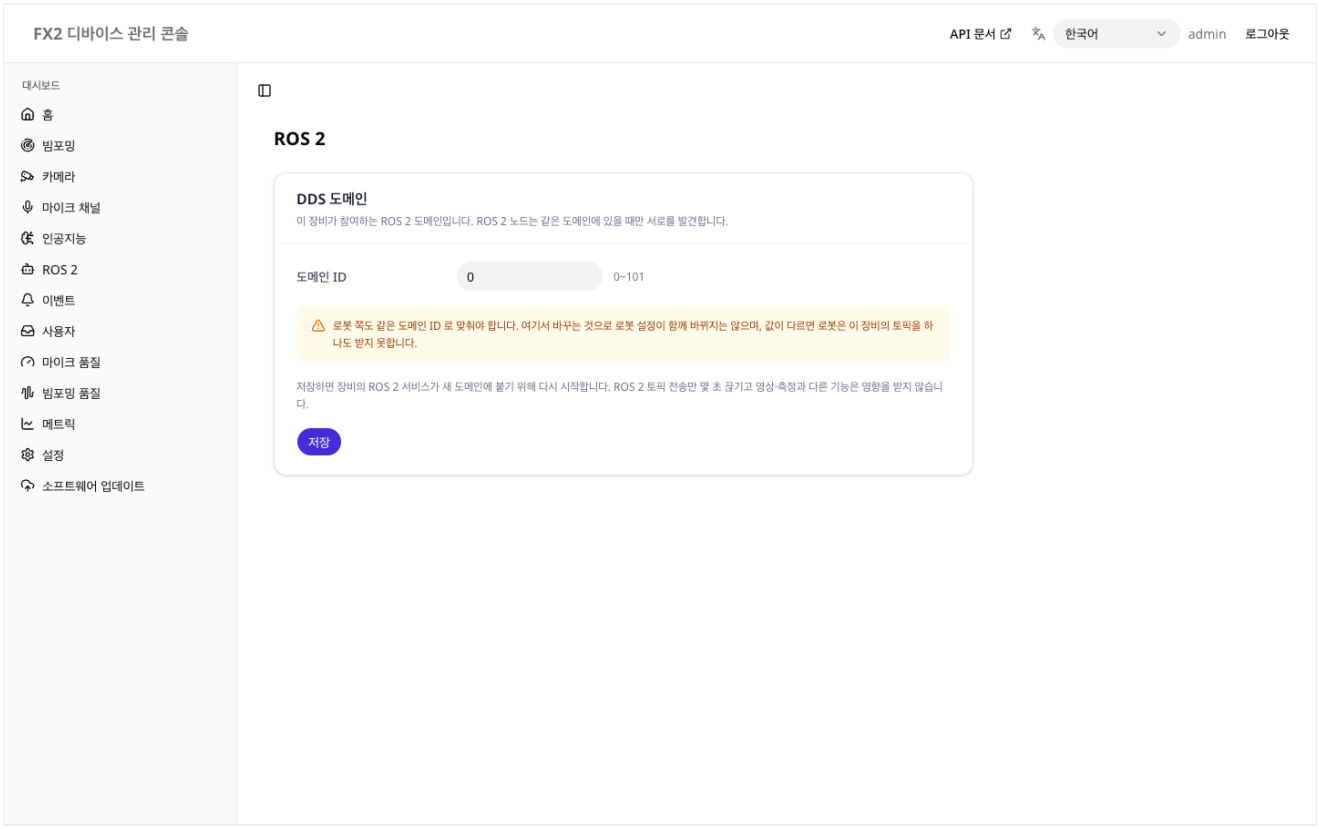
This information is based on firmware v1.1.1-beta.1 and may change in the official release.

- ROS 2 distribution — we confirmed that fx2_stream_msgs 2.0.0 builds on Humble and Jazzy and that the device's beamforming results, microphone audio, and listening-point audio topics can be received. The tested environment used Fast DDS (rmw_fastrtps_cpp) and domain ID 0. On Humble, the "sequence size exceeds remaining buffer" warning may appear a few times when subscription starts; in testing, it did not affect data reception.
- QoS — the five topics other than the video topic are published with BEST_EFFORT. The video topic can be received with the default QoS.

Connection Steps

1. Domain ID

Set the domain ID in the Device Manager's ROS 2 menu.



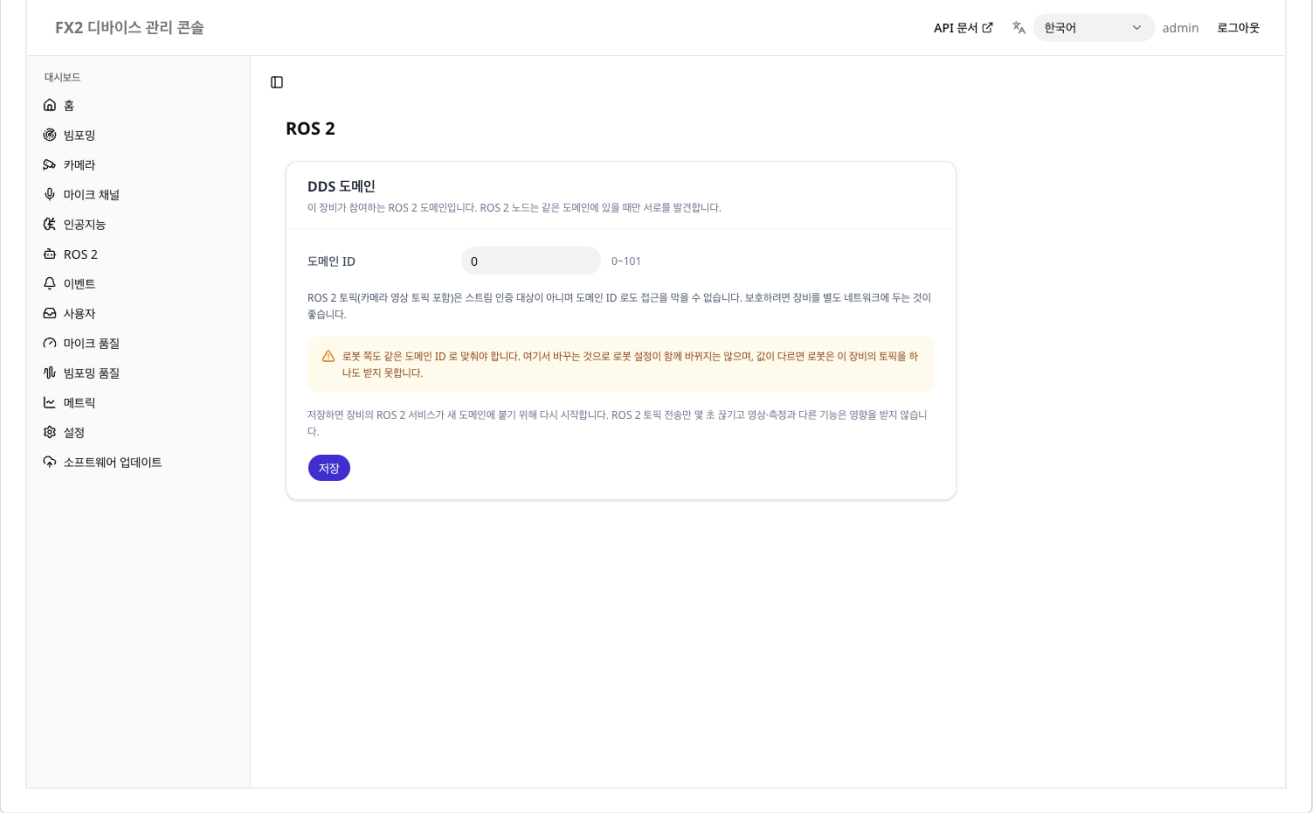
- Domain ID — 0–101. The default is 0.
- Saving restarts only the device's ROS 2 service. Topic transmission stops for a few seconds. RTSP video, measurement, and other functions are unaffected.
- Saving the current value does not cause a restart.
- You must set the robot's domain ID separately. Changing it on the device does not change the robot's settings. If the values differ, the robot will not receive any of this device's topics.

※ Changing the device's IP address also restarts the ROS 2 service.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

The ROS 2 menu also displays this notice: "ROS 2 topics (including the camera video topic) are not subject to stream authentication, and access cannot be blocked with a domain ID. To protect them, we recommend placing the device on a separate network."



2. Message Package

Install the fx2_stream_msgs message package on the robot. For firmware v1.1.0, use the following package.

- Package — fx2_stream_msgs 1.2.0
- License — MIT
- Repository — FX2 ROS 2 message repository

Download and build the message package on a PC with ROS 2 and colcon installed. The commands are for Bash and Jazzy.

```
source /opt/ros/jazzy/setup.bash
mkdir -p ~/fx2_ws/src
cd ~/fx2_ws
git clone https://github.com/SM-Instruments-Inc/sw2-fx2-ros-stream-msgs src/
fx2_stream_msgs
colcon build --packages-select fx2_stream_msgs
source install/setup.bash
ros2 interface show fx2_stream_msgs/msg/Beamforming
```

The last command displays the locally installed message definition. In the next step, check communication with the device.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

- Package — fx2_stream_msgs 2.0.0
- License — MIT
- Repository — public fx-stream-msgs repository on gitlab.com (master branch)

Firmware v1.1.1 requires fx2_stream_msgs 2.0.0. Robot programs built with an earlier version (1.x) must be rebuilt with 2.0.0. Otherwise, they may fail to receive or may misinterpret the beamforming results, microphone audio, and listening-point audio topics.

Download and build the message package on a PC with ROS 2 and colcon installed. The repository also contains fx_stream_msgs, a package for BATCAM FX, so select only fx2_stream_msgs for the build. The commands are for Bash and Jazzy.

```
source /opt/ros/jazzy/setup.bash
mkdir -p ~/fx2_ws/src
cd ~/fx2_ws/src
git clone https://gitlab.com/smins-oss/sound-camera/framework/protocol/fx-stream-msgs.git
cd ~/fx2_ws
colcon build --packages-select fx2_stream_msgs
source install/setup.bash
ros2 interface show fx2_stream_msgs/msg/Beamforming
```

The last command displays the locally installed message definition. If the output contains the line `builtin_interfaces/Time stamp`, it is version 2.0.0.

3. Check Topics

Check the topic list on the robot.

```
ros2 topic list
```

The device's topic names begin with `/fx2/<serial-token>/`. The serial token is derived from the serial number under Home → Device Information by replacing every character other than letters, digits, and `_` with `_`. For example, the serial number BFX2-xxxx becomes BFX2_xxxx.

```
/fx2/BFX2_xxxx/beamforming
/fx2/BFX2_xxxx/leak_detection
/fx2/BFX2_xxxx/lpoint_audio
/fx2/BFX2_xxxx/pd_detection
/fx2/BFX2_xxxx/ws_audio
/parameter_events
/rosout
```



Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

In firmware v1.1.1, the video topic `/fx2/BFX2_xxxx/image/compressed` also appears in the list. It is not shown in the image above.

Try receiving data with BEST_EFFORT.

```
ros2 topic echo /fx2/BFX2_xxxx/beamforming --qos-reliability best_effort
```

Topics

Topic	Message Type	Frequency	Content
beamforming	fx2_stream_msgs/msg/Beamforming	25 Hz	Raw beamforming map values (1,144), peak level (dB), and location
ws_audio	fx2_stream_msgs/msg/WsAudio	25 Hz	Audio from the channel selected in the Microphone Channel menu
lpoint_audio	fx2_stream_msgs/msg/LPointAudio	25 Hz	Audio from three listening points
pd_detection	fx2_stream_msgs/msg/PdDetection	Approx. 10 Hz	Partial discharge AI detection. Only when PD AI is enabled
leak_detection	fx2_stream_msgs/msg/LeakDetection	Approx. 10 Hz	Leak AI detection. Only when LEAK AI is enabled

Topic names are prefixed with `/fx2/<serial-token>/`.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Firmware v1.1.1 adds the following topic.

Topic	Message Type	Frequency	Content
image/compressed	sensor_msgs/msg/CompressedImage	25 Hz	Camera video (JPEG). Only when a robot subscribes

Measurement Timestamp

In firmware v1.1.0 (fx2_stream_msgs 1.2.0), beamforming, ws_audio, and lpoint_audio messages do not have a measurement timestamp field.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Starting with firmware v1.1.1, beamforming, ws_audio, and lpoint_audio messages include the measurement timestamp `stamp`.

- Value — the time the device received that frame (40 ms). It uses the same device clock as the video topic's capture timestamp (`header.stamp`).
- Same frame — the three topics for the same frame usually have the same `stamp`. You can use this value to align beamforming results, audio, and video by time.
- Clock changes — because the timestamp follows the device clock, it jumps forward or backward on the frame when the clock changes through a time server (NTP) or manual setting. BATCAM FX2 does not have an RTC (built-in clock).
- AI detection — the `stamp` in pd_detection and leak_detection is the time the detection message was created, not the measurement time.

Video Topic

Firmware v1.1.0 has no video topic. Receive video via the RTSP `/overlay` path.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Starting with firmware v1.1.1, the device also publishes camera video as a ROS 2 topic.

- Topic — `/fx2/<serial-token>/image/compressed`
- Message type — sensor_msgs/msg/CompressedImage. Because this is a standard ROS 2 message, it can be received without fx2_stream_msgs.
- Video — the topic publishes the same view shown in Device Manager and via RTSP `/overlay`. If overlay display is enabled in the Beamforming menu, the view includes the heatmap and any peak marker and level (dB) enabled under display options in the Camera menu. If overlay display is disabled, only the camera video appears. The unprocessed video without an overlay is not published separately.
- Format — JPEG. The video dimensions follow the camera's resolution setting.
- Frequency — 25 Hz
- Transmission condition — the device generates and sends video only while a robot is subscribed. Without a subscriber, the device does not read video or encode it as JPEG for the video topic.
- QoS — it can be received with the default QoS or with BEST_EFFORT.

Check whether video is arriving on the robot.

```
ros2 topic hz /fx2/BFX2_xxxx/image/compressed
```

If approximately 25 Hz is displayed, video is arriving. In testing, we subscribed to this topic and received 60 JPEG frames at 1920 × 1080 and 25 Hz; all decoded correctly. To view the video, select this topic in rqt_image_view.

The video topic has no authentication. Anyone in the same DDS domain (with the same domain ID) can view the video without a device account. This is true even when stream authentication is enabled. A domain ID cannot block access either. To protect the video, we recommend placing the device on a separate network.

Actions

- setting_beamforming — changes the measurement band. It uses the same values as the settings in Device Manager's Beamforming menu.
- setting_overlay — changes the overlay settings.

Action results contain the values actually applied. The measurement band cannot be changed while AI is running.

API and Developer Integration

You can use the REST API to read and change BATCAM FX2 settings and events, and receive real-time measurement data through WebSocket. This page explains where to find the API documentation, how to authenticate, and which addresses to use.

REST API

The device provides a REST API over HTTP port 80. Most settings available in Device Manager are also available through the API.

1. API documentation

You can open the API documentation in a browser without authentication.

```
http://<device-ip>/api-docs
```

- Format — Swagger UI
- Languages — English, Korean, Japanese, Simplified Chinese, and Vietnamese. Select a language from the list at the top of the page.
- Test requests — Use “Try it out” for an operation to send a request directly to the device.



※ The “API Documentation” link in the top bar of Device Manager opens the same address in a new tab.

2. Authentication

The REST API supports two authentication methods. The operations that do not require authentication are `/ping`, `/auth/login`, and the API documentation.

- Basic — Send the account ID and password with each request.
- Bearer token — Log in through `/auth/login` to obtain a token, then include it in requests. Tokens are valid for 24 hours; you must log in again when they expire. Tokens are specific to each device.

Some operations can be called only by an administrator account. Calling them with a regular user account returns a `no permission` error. The API documentation identifies administrator-only operations.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Updating the firmware to v1.1.1 invalidates previously issued tokens. A factory reset does the same. Log in again to obtain a new token. The same may happen with later updates. Basic authentication is unaffected.

※ If a page on another site calls the device REST API from a browser using Basic authentication, the request is rejected (403). Browser apps should use a login token (Bearer). Non-browser programs are unaffected.

3. Example requests

Check whether the device responds. No authentication is required.

```
curl http://<device-ip>/ping
```

Example response:

```
{"error":0,"result":{"text":"pong"}}
```

Log in to obtain a token. Send the login request as multipart/form-data, not JSON.

```
curl -X POST http://<device-ip>/auth/login -F username=<ID> -F password=<password>
```

Example response:

```
{"error":0,"result":{"tokenType":"Bearer","accessToken":"<token>","expiresIn":
86400}}
```

Use the token to read device information.

```
curl http://<device-ip>/setting/status -H "Authorization: Bearer <token>"
```

With Basic authentication, send the ID and password directly.

```
curl http://<device-ip>/setting/status -u <ID>:<password>
```

- Successful response — `{"error":0,"result":...}`
- Failed response — `{"error":1,"result":{"message":"..."}}`
- Exception — A successful camera snapshot request (`/camera/snapshot`) returns a JPEG image.

WebSocket

Receive real-time measurement data through WebSocket.

```
ws://<device-ip>/ws
```

- Authentication — In firmware v1.1.0, WebSocket does not require an account.
- Encryption — None (ws, plaintext).
- Subscription — After connecting, you must subscribe to the data you want to receive. No data is sent before you subscribe.
- Data types — 0 Beamforming, 1 WsAudio, 2 LPointAudio, 3 PdDetection, 4 LeakDetection

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

- Authentication — A device account. Both administrator and regular user accounts work. If stream authentication is disabled, you can connect without an account.
- Encryption — None (ws, plaintext). Basic account credentials are also unencrypted.
- Non-browser programs — Include an `Authorization: Basic …` or `Authorization: Bearer <token>` header in the connection request. Request the `subscribe` subprotocol.
- Browsers — Because browsers cannot add the header, request both the `fx2-ws` and `fx2-token.<token>` subprotocols. Do not put the token in the address. A page on another site that connects using Basic authentication is rejected (403).
- If account verification fails repeatedly, that address is blocked for 60 seconds. For details, see Security and Accounts in External System Integration.

Example subscription request:

```
{"type":"subscribe","id":1}
```

※ The device sends data in binary frames. See the Developer Center for the message structure.

Other integration methods

- Video, Modbus TCP, ONVIF — See External System Integration.
- Robots — See ROS 2 Integration.

In firmware v1.1.0, custom triggers added through REST `POST /event/trigger` are saved but do not record events.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information is based on firmware v1.1.1-beta.1 and may change in the official release.
>
> In firmware v1.1.1, custom triggers added through REST `POST /event/trigger` also record events when their conditions are met. For registration instructions, see Custom Triggers under Events.

See the Developer Center for request and response fields. Example code is available in the SM Instruments public repositories.

FX Viewer Integration

FX Viewer is PC software for viewing, recording, and analyzing video from multiple BATCAM cameras on one screen. This page covers what you need to know when using the BATCAM FX2 with FX Viewer.

What is FX Viewer?

FX Viewer is dedicated software installed on a PC. It is separate from the device's Device Manager. The following features belong to FX Viewer and are not available on the device.

- Monitor video from multiple cameras on one screen
- Manual, trigger, and interval recording
- Play back recordings and analyze signals (Analysis mode)
- Generate gas leak and partial discharge reports

The device stores events. When specified conditions are met, an event saves approximately two seconds of photos, video, audio, and measurement data. The device does not record continuously. For continuous recording, use FX Viewer's recording feature. See Events for more information about events.

Registering the FX2

To register the device, the PC and device must be able to communicate with each other. The device's factory IP addresses are 192.168.0.80 for the eth0 port and 192.168.0.81 for the eth1 port. See Initial Connection for the PC network settings.

The device's video path is `/overlay`. There is no `/raw` path.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

In FX Viewer 1.1.1 for Windows, open "Camera List" in camera settings and click the Add button. Under "Camera Information," enter the device's "IP Address," port, "RTSP Port," and "Device Name." Enter the device account under "Username" and "Password," then click "Add."

If stream authentication is enabled on the device (the default), you must also enter the device account in FX Viewer to receive video and measurement data.

Viewing video

You can also view video from the device without FX Viewer using either of these methods.

- Device Manager — Open the device address in a browser.
- RTSP — Receive the stream in a VMS or video viewer at `rtsp://<device-ip>:8554/overlay`.

With firmware v1.1.0, no account is required to view RTSP video.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

If stream authentication is enabled (the default), a device account is required to receive RTSP video.

See External System Integration for the RTSP address and other integration methods.

Troubleshooting

This page organizes common BATCAM FX2 problems and checks by symptom. Find the symptom that matches yours and go through the checks in order.

Connection and login

1. Cannot access Device Manager

Symptoms

- Nothing appears when you open the device address in a browser

Checks

- The factory IP addresses are 192.168.0.80 for the eth0 port and 192.168.0.81 for the eth1 port.
- The PC must be on the same subnet as the device (192.168.0.xxx).
- The address is `http://<device-ip>`. HTTPS is not supported.
- After changing the device IP address, connect using the new address. If you switched to DHCP, check the DHCP server for the address assigned to the device.

Cause — If you change the device IP address, you must put the PC on the same subnet.

For initial setup, see Getting started.

2. Keep returning to the login screen

Symptoms

- Returned to the login screen after logging in
- The login screen suddenly appears during use

Checks

- Login credentials remain valid for 24 hours. Log in again when they expire.
- Login credentials are stored in browser cookies. If you clear the cookies, you must log in again.
- A browser is logged out after a factory reset, so you must log in again.
- After a factory reset, the administrator account has the ID `admin` and password `1234`. The same values appear in the notice below the login form. You must change the password after your first login.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

After updating the firmware to v1.1.1 or performing a factory reset, you must log in again once in every browser and application.

3. Cannot change password

Symptoms

- Unable to change the password

Checks

- Standard user accounts cannot change passwords. An administrator account is required.
- You cannot use the initial password (`1234`) again.
- The password must be at least four characters long.
- “New password” and “Confirm password” must match.

For account management, see User accounts and permissions.

4. “Unable to load information” appears or a list is empty

Symptoms

- “Unable to load information” appears on the Network Status card on Home
- The network table or user list in Settings is empty
- There is no Edit button in Time Settings

Checks

- Network, user, and time settings require administrator privileges.
- When you log in with a standard user account, the menus appear but this information is empty.
- Log in again with an administrator account.

5. Only an “...in progress” message remains after pressing a button

Symptoms

- After pressing “Restart” under Settings → Restart Service, “Restarting service” remains on the screen

Checks

- Only an administrator account can restart the service or perform a factory reset.
- Requests from standard user accounts are denied, but the in-progress message remains on the screen.
- Log in again with an administrator account and retry.

6. Deletion fails

Symptoms

- Deleting an event displays “Failed to delete event: no permission”

Checks

- Only an administrator account can delete events or delete all events.

Video and display

7. No video

Symptoms

- “Connecting to camera...” or “Disconnected. Reconnecting...” remains on the screen

Checks

- Device Manager receives video through WebRTC. The browser must support WebRTC.
- Video will not appear if a firewall or router between the PC and device blocks TCP 8889 or UDP 8189 (the defaults).
- If the video disconnects, it automatically tries to reconnect. It disconnects for a few seconds immediately after a service restart or a change to video rotation.
- WebRTC supports up to 10 simultaneous connections.
- RTSP video is available at `rtsp://<device-ip>:8554/overlay`. There is no `/raw` path.

7-1. No video in a VMS or viewer

This section applies to stream authentication in firmware v1.1.1. In firmware v1.1.0, no account is required for RTSP video, WebRTC video, WebSocket, ONVIF snapshots, or event files.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

Symptoms

- A VMS, video viewer, or script cannot retrieve RTSP video, ONVIF snapshots, WebSocket data, or event files
- A login prompt appears when you open a video or event-file address in a browser

Checks

- When stream authentication is enabled, a device account is required. Save the device account (ID and password) in the VMS or viewer, or include it in the address, as in `rtsp://<ID>:<password>@<device-ip>:8554/overlay`. A VMS that registers the device through ONVIF must also save the account.
- RTSP supports Basic authentication only. Clients that use only Digest authentication cannot connect.
- When stream authentication is enabled, RTSP multicast is rejected (461). Switch to TCP or UDP unicast.
- If an incorrect account fails 10 times within one minute, that PC address is blocked for 60 seconds. Correct the account and wait up to 60 seconds.
- A web page on another site is rejected (403) if it connects using Basic authentication.

- If you must use a client that cannot provide an account, an administrator can turn off Settings → Stream Authentication. For details, see System settings.

8. Resolution does not change

Symptoms

- The video size stays the same after changing the resolution in the Camera menu

Checks

- The resolution takes effect after you use Settings → Restart Service.
- Until the restart, the RTSP stream and ONVIF retain the previous size.
- Only an administrator account can restart the service.

9. Cannot change the measurement band

Symptoms

- The “Frequency Range” slider in the Beamforming menu does not move
- “The frequency range cannot be changed while AI is running” appears

Checks

- While AI is running, the measurement band is fixed to the model's band. PD AI uses 25 kHz ~ 60 kHz, and LEAK AI uses 13 kHz ~ 65 kHz.
- Turning off AI restores the previously selected measurement band.
- If you set an AI operating schedule, the band is fixed only during that period.
- If you move the upper limit to the end of the slider (99 kHz), the setting is not saved. Set the upper limit to 98.9 kHz or lower.

10. Heatmap covers the screen or is not visible

Symptoms

- Color covers the entire video
- The heatmap is not visible

Checks

- “Threshold” in the Beamforming menu is the lower limit for drawing the heatmap. A low value colors even faint sounds; a high value can make the heatmap disappear.
- “Range” and “Average” also affect the heatmap's appearance.
- If the overlay mode is “Overlay Off,” the heatmap is not drawn. Measurement and event storage continue to work.
- When a region of interest (ROI) is enabled, the heatmap outside the ROI box is not visible.

- While AI is running, the heatmap appears gray when nothing is detected. Color appears when a detection occurs.

11. Heatmap position does not match the sound source

Symptoms

- The peak marker and heatmap positions do not match
- The heatmap does not match the actual location of the sound

Checks

- Changing “Field of View (FOV)” in the Camera menu also changes the beamforming calibration. Check that the field of view matches the installation.
- Video rotation applies only to the video. The beamforming overlay does not rotate.
- In firmware v1.1.0, the heatmap is drawn farther inward than the peak marker near the edges of the screen.
- If a sound source lies on a grid-cell boundary, the peak marker may alternate between the two neighboring cells.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

- The heatmap appears at the same position as the peak marker.
- If a field-of-view warning appears on the Camera screen, the model default is being used instead of the device calibration value. Check the reason shown below the warning, and contact the seller or manufacturer if the positions do not match.

For how to change the field of view, see Camera settings.

Events and time

12. No level-trigger event is created

Symptoms

- No event is saved even when there is a loud sound

Checks

- On the Events → Trigger Conditions tab, check that the level trigger is enabled. It is enabled by default, with a threshold of 70 dB.
- If “Threshold” in the Beamforming menu is higher than the level trigger's “Threshold (dB),” no event is created. Sounds below the beamforming threshold are not identified as peaks.
- The level trigger compares the peak value after averaging. If there is no peak above the threshold, no event is created.

- Cooldown is measured from the last event, regardless of event type. If an automatic-save or AI event was just saved, no level-trigger event is created until the cooldown ends.
- In firmware v1.1.0, triggers added through REST are saved but do not record events.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

Triggers added through REST also record events when their conditions are met. Under Custom Triggers in Events, check whether the trigger is enabled, its threshold, and its cooldown.

Note — For a few seconds immediately after an event occurs, the device collects data for that event, so no new event can occur.

13. Too many events are created

Symptoms

- The event list fills up in a short time

Checks

- Raise the level trigger's “Threshold (dB)” or increase “Cooldown (sec).”
- Check whether “Automatic Save Settings” is enabled. It is off by default.
- For AI events, raise “Detection Threshold Score” or “Trigger Count,” or increase “Event Save Cooldown (sec).”
- Check whether the 40 kHz signal generator is on.
- When free storage falls below 10%, the oldest events are deleted automatically.

14. Event times are incorrect

Symptoms

- The times in the event list differ from the actual time

Checks

- Under Settings → Time Settings, check “Time Zone” and the NTP status. If the NTP status is “Synchronized,” the device clock is synchronized with the time server.
- “Creation Time” in the event list is displayed in the PC browser's time zone. Recent events on Home are displayed in the device's time zone. If the two time zones differ, the times on the two screens differ.
- The time in the status bar over the video is the device time.
- BATCAM FX2 has no RTC (built-in clock). If the power is turned off while it is disconnected from a time server (NTP), the device loses its time. When powered on without NTP, the device time starts at 1970-01-01T00:00:00. Use an accessible NTP server. On an isolated network, use an on-site NTP server and check the time under Settings → Time Settings after powering on.

- The Modbus TCP time registers use UTC.

For time settings, see System settings.

Checks and measurements

15. Cannot run Microphone Quality

Symptoms

- Running Microphone Quality displays “Microphone calibration cannot run while AI is running”

Checks

- Microphone Quality cannot run while AI is running.
- Turn off AI in the Artificial Intelligence menu, then run it.

16. The 40 kHz signal generator shows UNKNOWN or measurements are abnormal

Symptoms

- The current status in the Microphone Channels menu is UNKNOWN, and the button cannot be pressed
- The measured level is high even though there is no sound

Checks

- UNKNOWN means the status could not be read or is still being read. Try reopening the screen.
- If the 40 kHz signal generator is left on, the reference signal is measured instead of the actual sound. This can cause the level trigger to operate incorrectly.
- The signal generator starts in the off state when the device is powered on again. It does not turn off automatically during operation.

Note — When the check is complete, press “Off” in the Microphone Channels menu to turn off the signal generator.

For the procedure, see Microphone check.

Firmware

17. Update fails or reverts to the previous version

Symptoms

- The uploaded firmware is not installed, and the device restarts with the same version
- The device returns to the previous version after updating

Checks

- Firmware files differ by camera. If the camera model on Home is “SMIA462 Wide,” upload a file whose name starts with fx2-cm5-arducam. If it is “SMI3708 Wide,” upload a file whose name starts with fx2-cm5-imx708.
- A file for a different camera is rejected, and the device restarts.
- When the device reboots after an update, the new firmware performs a trial boot. If it operates normally, it is confirmed after about one minute.
- If the service does not become healthy within 10 minutes, the device automatically reverts to the previous firmware.
- During trial boot, the device list and Ethernet connection are checked. A device or gateway recorded during installation must respond. The device may revert to the previous firmware if a cable is unplugged between installation and reboot, or if the PC used to upload the firmware is turned off and there is no gateway. In firmware v1.1.0, a device connected directly to a PC through only the eth0 port may also revert if the gateway does not respond. For detailed conditions, see Trial boot and confirmation under Firmware update.
- Rebooting or losing power before confirmation also causes a return to the previous firmware. Events saved by the new firmware will then not be visible in the previous firmware.
- A device that reverted before confirmation can be updated again.
- Only an administrator account can update the firmware.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

If there is no response target during trial boot, or the only target is the current gateway, the check can pass based on a record of packets sent and received through an IPv4 port. The issue in which a device connected directly to a PC through only the eth0 port reverted because the gateway did not respond has been fixed. If the PC was recorded alongside the gateway as a connection target during installation and neither responds, the device may still revert to the previous firmware.

Note — You cannot use an update to install firmware older than v1.1.0. If you need older firmware, see Product support and inquiries to get in touch.

For the update procedure, see Firmware update.

18. An FPGA notification appears

Symptoms

- An FPGA notification appears on the Software Update screen

Checks

- “Updating FPGA. Do not turn off the power.” — A new FPGA version is being written. The device may restart when this finishes.

- “FPGA update failed after firmware installation.” — The device continues operating with its current FPGA. It will not retry automatically.
- “FPGA version could not be read, so no update was attempted.” — If the version cannot be read, it is not written automatically.
- “FPGA verification is waiting for firmware update confirmation.” — If this persists after a reboot, contact support.

If the update fails or the version cannot be read, you can upload an FPGA file through the “Service/ Recovery: Update FPGA Only Manually” link on the Software Update screen. Only an administrator account can upload it.

Note — Do not turn off the power while uploading the FPGA. In firmware v1.1.0, if the version read at the next boot is outside the 2.0.2 ~ 2.0.3 range or is a development build of 2.0.2, the device restores FPGA 2.0.2 included with the firmware.

Pre-release software (v1.1.1-beta.1)

This information applies to firmware v1.1.1-beta.1 and may change in the official release.

If the version read at the next boot differs from the official 2.0.3 release, the device restores the official FPGA 2.0.3 release included with the firmware.

Accounts

19. Forgot password

Symptoms

- Cannot log in

Checks

- If another administrator account exists, log in with it. Set a new password using “Change Password” for the account in the Users menu.
- If there is no administrator account, press the rear button for at least three seconds to perform a factory reset.
- After a factory reset, the administrator account has the ID `admin` and password `1234`. The same values appear in the notice below the login form. You must change the password after your first login.

Note — A factory reset deletes all accounts, settings, and events. This cannot be undone.

Further assistance

20. Further assistance

If these steps do not resolve the issue, check the values under Home → Device Information before contacting support. Provide the device name, device code, serial number, firmware version, FPGA version, and camera model. For contact information, see Product support and inquiries.

Frequently Asked Questions

Frequently asked questions and answers about BATCAM FX2 are grouped by category. For solutions by symptom, see Troubleshooting.

Product

Q. What is BATCAM FX2?

It is a fixed ultrasonic camera equipped with a 112-channel MEMS microphone array and a camera. It displays the location of a sound as a heatmap over the video.

Q. What camera models are available?

There are two: SMIA462 Wide and SMI3708 Wide. To check which one is installed, see Camera Model under Home → Device Information. Both cameras provide video at 1920 × 1080 (default), 1600 × 900, 1280 × 720, or 640 × 360 resolution at 25 fps.

Q. What does the AI detect?

There is Leak AI (LEAK AI), which identifies compressed-air and gas leaks, and Partial Discharge AI (PD AI), which identifies partial discharge. Both models run on the device.

Q. Can both AI models be enabled at the same time?

No. Only one model can be enabled at a time.

Q. Does the device record video continuously?

The device saves events when the specified conditions are met. It does not record continuously.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information is based on firmware v1.1.1-beta.1 and may change in the official release.
>
> To record continuously on a PC, use FX Viewer 1.1.1 for Windows.

Q. What is the water and dust resistance rating?

It is rated IP68.

Installation and Power

Q. How is power supplied?

Power can be supplied via PoE+ or DC 12 ~ 24 V.

Q. What are the cable requirements for installation?

Use a CAT5e or higher UTP cable; CAT6 is recommended. The installation distance must be within 80 m.

Q. What are the factory-default IP addresses?

The eth0 port uses 192.168.0.80, and the eth1 port uses 192.168.0.81.

Device Manager

Q. What are the default login credentials?

After a factory reset, the administrator account has the ID `admin` and password `1234`. The same values are shown in the notice below the login screen. Change the password after your first login.

Q. Can a regular user account change settings?

It can change measurement settings such as beamforming, camera, and AI settings. Only an administrator account can manage accounts, network settings, time, firmware updates, service restarts, factory resets, and event deletion. In firmware v1.1.0, a regular user account can also change auto-save and level-trigger settings.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information is based on firmware v1.1.1-beta.1 and may change in the official release.
>
> Only an administrator account can change auto-save and level-trigger settings.

Q. What does an event ZIP file contain?

It contains the photos (JPG), videos (MP4), audio (WAV), and measurement data (H5) actually saved for that event. Files that were not saved are not included.

Q. How long are events stored?

Each event covers approximately 2 seconds. When free storage space falls below 10 %, the oldest events are automatically deleted first.

Integration

Q. What is the RTSP stream address?

It is `rtsp://<device-ip>:8554/overlay`. There is no raw video path (/raw). In firmware v1.1.0, an account is not required to view RTSP video.

> **Pre-release software (v1.1.1-beta.1)**
>
> This information is based on firmware v1.1.1-beta.1 and may change in the official release.
>
> If stream authentication is enabled (the default), a device account is required. Save the credentials in the VMS or viewer, or include them in the address as `rtsp://<ID>:<password>@<device-ip>:8554/overlay`. RTSP supports Basic authentication only.

Q. What are the `rtsp://…:8554/raw` address and `/fx_…/image` video topic mentioned in other documentation?

They apply to BATCAM FX and not to BATCAM FX2. Receive BATCAM FX2 video from `rtsp://<device-ip>:8554/overlay`. Firmware v1.1.0 does not have a ROS 2 video topic.

> **Pre-release software (v1.1.1-beta.1)**

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Starting with firmware v1.1.1, video can also be received through the ROS 2 video topic `/fx2/<serial-token>/image/compressed`. For details, see ROS 2 Integration.

Q. How does the API work?

It uses a REST API and WebSocket. API documentation is available at `http://<device-ip>/api-docs`.

Q. Is Modbus TCP enabled by default?

No. An administrator enables it in the “Modbus TCP” card on the Events → Trigger Conditions tab.

Q. Does it support ROS 2?

Yes. It supports the Jazzy distribution of ROS 2 and provides five topics and two actions.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

A camera video topic has been added, bringing the total to six topics and two actions.

Q. Do the integration methods require authentication?

The REST API requires a device account. In firmware v1.1.0, RTSP, WebRTC, WebSocket, ONVIF, event files, Modbus TCP, and ROS 2 do not require an account. The device should be used only on an internal network.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

A device account is required to access RTSP, WebRTC, WebSocket, ONVIF snapshots, and event files. An administrator can disable this under Settings → Stream Authentication. ONVIF device discovery and queries, Modbus TCP, and ROS 2 do not require authentication. Anyone in the same DDS domain can view video through the ROS 2 video topic without an account, even when stream authentication is enabled.

Q. Does it support HTTPS?

No. Device Manager and the REST API are accessed over HTTP on port 80.

Firmware

Q. Where can I check the firmware version?

In Device Manager, check “Firmware Version” under Home → Device Information.

Q. Are settings retained after a firmware update?

Settings, accounts, and events are retained.

Q. Can I turn off the power during an update?

No. If power is interrupted before the update is finalized, the device reverts to the previous firmware.

Q. Where can I get the firmware file?

Request the firmware file through Product Support and Inquiries.

Firmware Version Information

This page summarizes the current BATCAM FX2 firmware version, firmware files for each camera, FPGA compatibility, and known issues. Check the file for your device before uploading firmware.

Current Version

The current BATCAM FX2 firmware is v1.1.0 (2026.11.03). This page covers the firmware files, FPGA compatibility, and known issues for v1.1.0.

- Installed firmware version — In Device Manager, check “Firmware Version” under Home → Device Information.
- How to install firmware — See Firmware Update.

Changes in v1.1.1

The following changes are planned for the next version, v1.1.1.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

- Stream authentication — RTSP video, WebRTC video, WebSocket, ONVIF snapshots, and event files require a device account. Authentication is enabled by default, and an administrator can turn it off under Settings → Stream Authentication. Before updating, add a device account to your VMS, viewers, and scripts. For details, see Security and Accounts in External System Integration.
- Sign in again — After updating, sign in again once in both Device Manager and API clients.
- Trigger condition changes — Only administrator accounts can call REST `PATCH /event/trigger`.
- Custom triggers — Triggers added by an administrator through REST also record events when their conditions are met. Before updating, check the threshold values of triggers you have already enabled.
- Camera — If a device-specific field-of-view calibration value is unavailable, the reason is shown on the camera screen.
- ROS 2 video topic — Camera video is available through the ROS 2 topic `image/compressed` (JPEG, 25 Hz). It is sent only when a robot subscribes. This topic has no authentication, so anyone in the same DDS domain can view the video without an account. For details, see ROS 2 Integration.
- ROS 2 messages 2.0.0 — The beamforming, ws_audio, and lpoint_audio messages now include a measurement timestamp, `stamp`. Robot programs must be rebuilt with message package fx2_stream_msgs 2.0.0. Prepare the robot side before updating. For details, see ROS 2 Integration.

- ROS 2 notice — The ROS 2 menu and Settings → Stream Authentication display a notice recommending that the device be placed on a separate network because ROS 2 topics have no authentication.
- WebSocket measurement timestamp — The timestamp in beamforming results, microphone audio, and listening-point audio messages is when the device received the frame, not when it sent the message. The three messages for the same frame have the same timestamp. AI decision messages continue to use the time they were sent.
- SMIA462 Wide default field of view — The default used when a device has no device-specific field-of-view calibration value has been updated. Heatmap positions on these devices will be more accurate. The default horizontal field of view at 100% field of view is 123.78°.
- Login screen — The Device Manager login screen displays a link and QR code for the online user manual. You can scan the QR code with a phone to open the manual even if the device is not connected to the internet.
- Heatmap position — The heatmap is drawn at the same position as the peak crosshair. Previously, the heatmap was drawn farther inward than the crosshair toward the edges of the screen. Peak position values do not change.
- Update confirmation — Fixed an issue that caused the device to restart after an update had already been confirmed. Also fixed an issue that caused devices with only eth0 connected directly to a PC, where the gateway did not respond, to revert to the previous firmware. If the cable is disconnected, the device still reverts to the previous firmware.
- Auto exposure — Fixed an issue that prevented auto exposure from being turned off on the camera screen of SMI3708 Wide devices. If saving fails, a message appears and the screen returns to the device's actual setting.
- Time synchronization notice — Corrected the description of automatic time synchronization in Time Settings. The device has no RTC to maintain the time while powered off, so if automatic time synchronization is turned off, the time may be incorrect after the device is powered on again.

※ The release date for v1.1.1 will be posted on this page after release.

Firmware Files by Camera

Firmware files differ by camera. Check "Camera Model" under Home → Device Information and upload the matching file. A file for a different camera will be rejected, and the device will restart.

Camera Model on Home	Firmware File
SMIA462 Wide	fx2-cm5-arducam-v<version>.mender
SMI3708 Wide	fx2-cm5-imx708-v<version>.mender

FPGA Compatibility

Firmware v1.1.0 includes FPGA 2.0.2. After the update is confirmed, FPGA 2.0.2 is reflashed if the device's FPGA version is lower than 2.0.2, higher than 2.0.3, or a development build of 2.0.2. The official 2.0.2 release and versions higher than 2.0.2 but no higher than 2.0.3 are left unchanged.

FPGA Version	Status
2.0.2	Verified
2.0.3b	Verified

- 2.0.2 — The version included in the firmware.
- 2.0.3b — Within the 2.0.2–2.0.3 range, so it remains unchanged after the update.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

Firmware v1.1.1 includes the official FPGA 2.0.3 release. After the update is confirmed, if the FPGA version read by the device differs from the official 2.0.3 release, it is updated to 2.0.3. If it is already the official release, it is left unchanged.

Known Issues

- A factory reset does not erase the camera principal point or field-of-view calibration values. Reflashing the device image does erase them, so back them up first.
- If the FPGA version cannot be read, it is not flashed automatically. An administrator can upload an FPGA recovery file from the Software Update menu.

Pre-release software (v1.1.1-beta.1)

This information is based on firmware v1.1.1-beta.1 and may change in the official release.

- X Calibration, Y Calibration — In FPGA 2.0.3, X Calibration and Y Calibration shift the entire screen by the same amount. Values set in FPGA 2.0.2 remain after the update, so the heatmap position may be misaligned. If it is misaligned, readjust X Calibration and Y Calibration on the Home screen. If you cannot align it or need help, contact the manufacturer.
- FX Viewer — A build of FX Viewer 1.1.1 that supports stream authentication and the RTSP path `/overlay` is required. Earlier builds may not receive video.

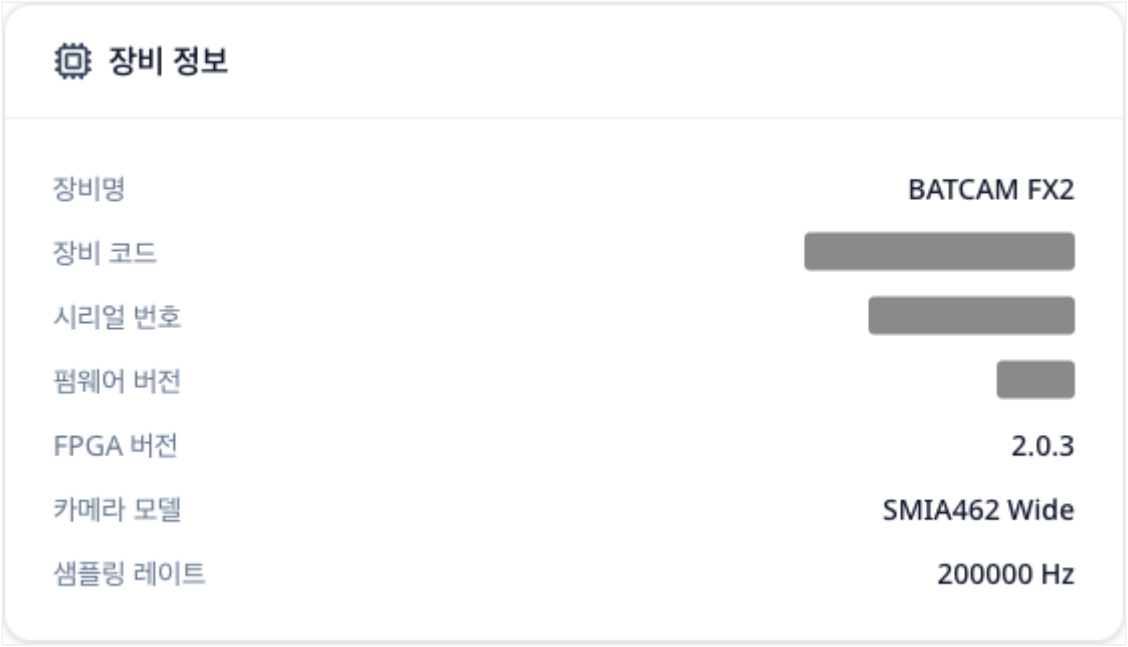
For automatic FPGA version matching, FPGA notifications, and uploading FPGA files, see Firmware Update.

Product Support and Inquiries

This page provides information about BATCAM FX2 firmware files, development resources, and contact details. It also explains what device information to check before making an inquiry.

What to Prepare Before Contacting Us

You will need your device information when making an inquiry. In Device Manager, go to Home → Device Information and check the following values.



- Device name
- Device code
- Serial number
- Firmware version
- FPGA version
- Camera model

If you encounter a problem, also tell us when it happened, which screen you were on, and what you were doing. For possible solutions, consult Troubleshooting first.

Firmware Files

Request firmware and FPGA files through Product Support and Inquiries.

- Firmware files vary by camera. Obtain the file that matches the camera model shown on the Home screen.
- For installation instructions, see Firmware Update.
- For camera-specific file names and FPGA compatibility, see Firmware Version Information.

Development Resources

API documentation and integration details are available in the Developer Center. Example code is available on GitHub.

- Developer Center — API and integration documentation
- GitHub — SM Instruments public repositories
- API documentation built into the device — `http://<device-ip>/api-docs`

For information on using the API, see API and Developer Integration.

Open-Source Code Availability

BATCAM FX2 firmware includes open-source software. The source code is available in the open-source category on the FX2 download page. For inquiries, see Contact Information.

Contact Information

- Company — SM Instruments Co., Ltd.
- Phone — 042-861-7004
- Email — sales@smins.co.kr
- Website — SM Instruments website