VIVOTEK
A Delta Group Company

IE9111-O

AI Box User Manual

Key Features

- Qualcomm QCS605 SoC with built-in AI Engine
- Video processing and machine learning
- Supports VCA solutions through video analytics apps from the Azena Application Store
- Enables any type of network camera to act as a IoT Device

Driven by:

open security & safety alliance

Powered by:

azena

Table of Contents

Overview

- Powered by Qualcomm QCS605 SoC with a built-in AI Engine
- Powerful Computing for Video Processing and Machine Learning
- Designed with OSSA Technology Stack, running on Azena Android OS
- Supports a variety of VCA solutions through Azena APPs
- Enables Any Type of Network Camera to act as AIoT Device
- RJ-45 or M12 Connectors for PoE Connection
- Digital input*2, Digital Output *2
- EN50155 Compliance for Professional Mobile Surveillance

Revision History

- Rev. 1.0: Initial release.
- Rev. 1.1: Updated the initial portal login and other firmware features.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Symbols and Statements in this Document

ⓘ **INFORMATION:** provides important messages or advices that might help prevent inconvenient or problem situations.

✎ **NOTE**: Notices provide guidance or advices that are related to the functional integrity of the machine.

💡 **Tips**: Tips are useful information that helps enhance or facilitae an installation, function, or process.

⚠ **WARNING: or IMPORTANT:**: These statements indicate situations that can be dangerous or hazardous to the machine or you.

⚡ **Electrical Hazard**: This statement appears when high voltage electrical hazards might occur to an operator.

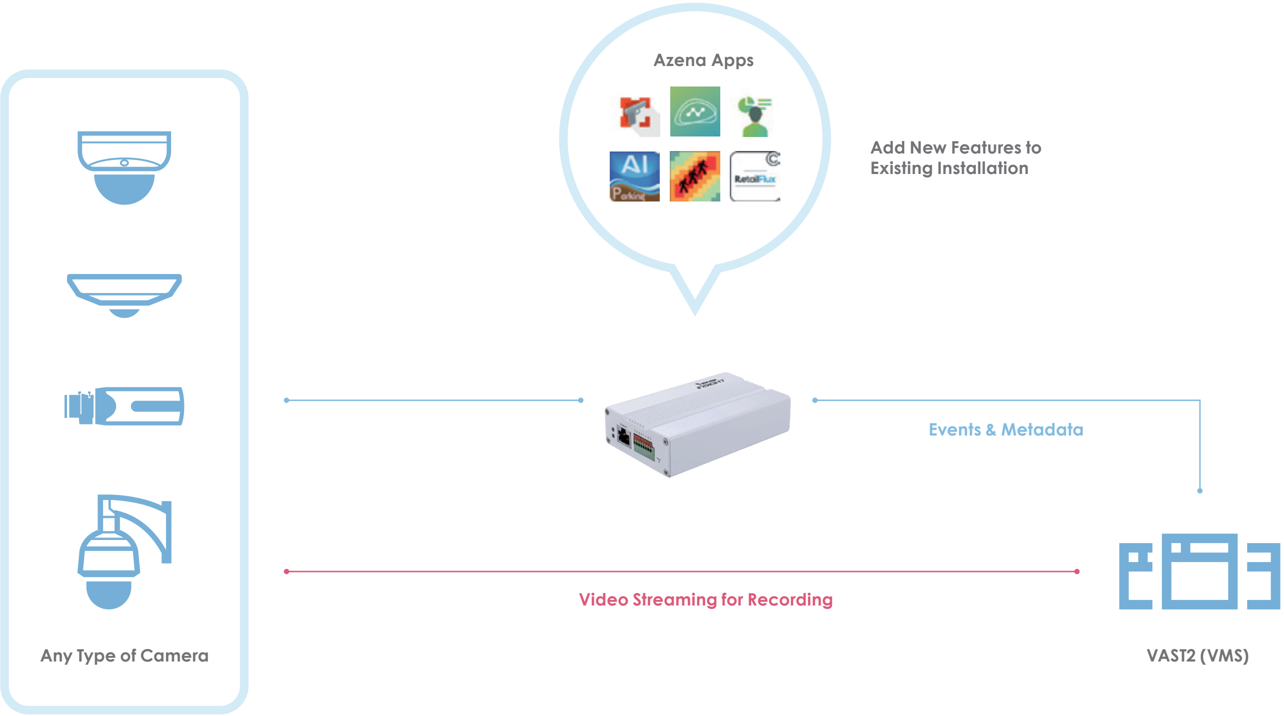
✎ **NOTE:**

1. The camera is only to be connected to PoE networks without routing to outside plants.
2. For PoE connection, use only UL listed I.T.E. with PoE output.

Package Contents

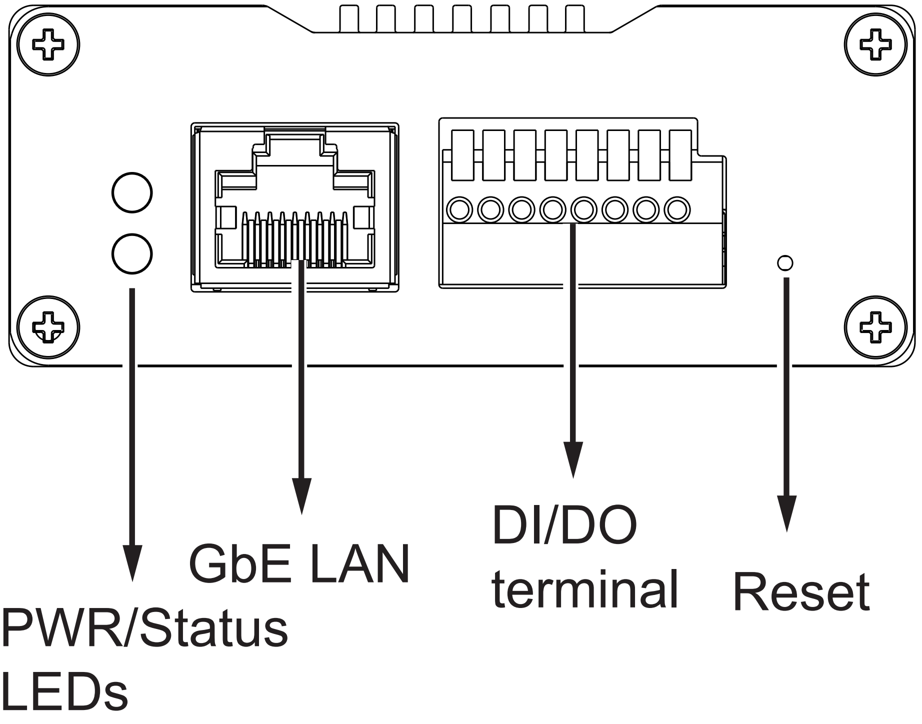
- IE9111-O
- Screw pack.
- Wall- / Panel-mount bracket.
- Quick Installation Guide.

Application

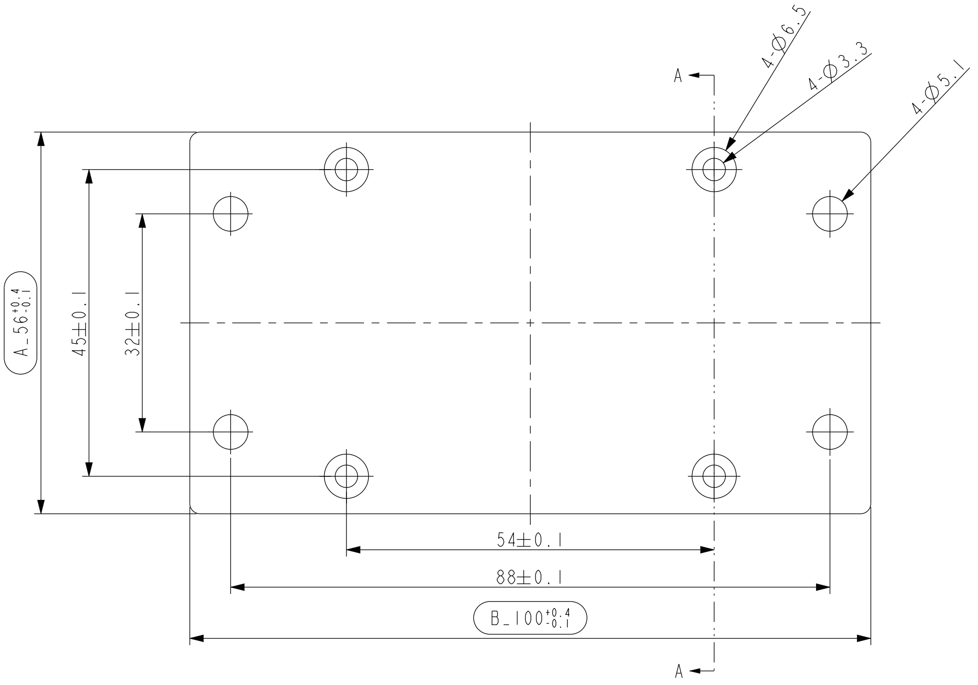


Physical Description

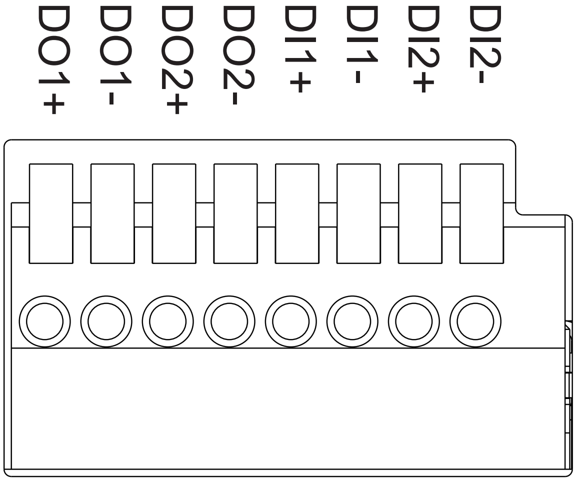
Outer View

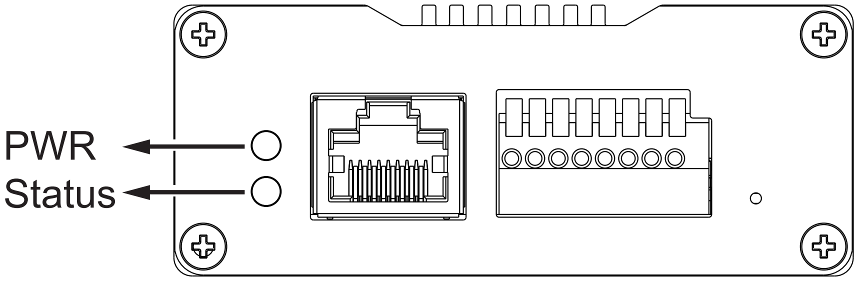


Bracket Dimensions



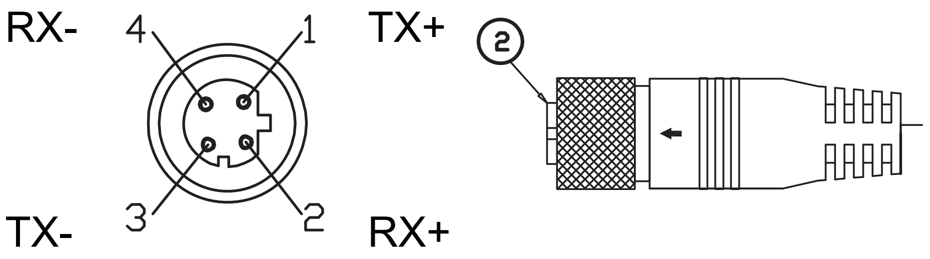
DI/DO Terminal Block Pinouts





LED	Behavior
PWR Red ON	Power is on
PWR Red ON + Status Green blinking	System ready
PWR Red + Status Green blinking	Reset taking place / restoring default

Below is the pinouts for the model that comes with a M12 connector:



M12 D-CODE 4 pin F

Consumption & Power Input
PoE: 802.3af class3

Hardware Reset

The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Use a flatten paper clip to press the button.

Reset: Press the recessed reset button. Wait for the Network Camera to reboot.

Restore: Press and hold the reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

Prerequisites

Hardware:

- Azena Enabled camera.
- A host computer (Windows/Linux/Mac/Ubuntu) with Google Chrome browser.
- Local network (e.g. router and cables) to connect the camera and the host computer.
- POE – Power Over Ethernet (via router, hub or PoE adapter) to power the camera.

Network:

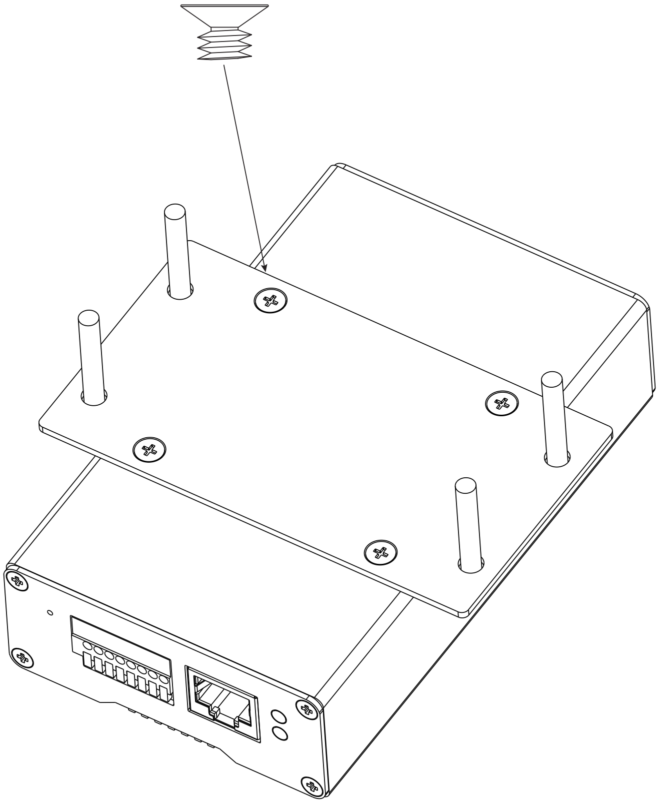
- Network with connectivity to internet (offline camera supported: not described in this document).
- DHCP Network (Using DHCP the camera automatically receives the IP address once connected to a network).

Software:

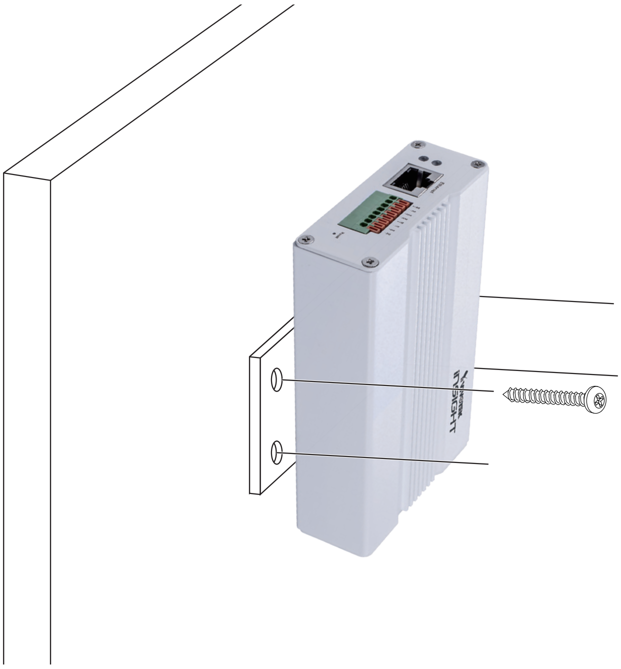
- Ecosystem credentials used across application store and **Device Management Portal**. Additionally you can also invite your colleagues to the account via the User Management.
- Download Azena Device Management tool from the resources section and install on the host computer. The tool can be used for device discovery and installing applications on cameras in offline network.
- Our devices communicate to the external URLs which needs to be allowed in the network firewall – details can be found in the resources section to the left.

Hardware Installation

1.The optional bracket allows you to install the AI box to a wall or panel. Secure the bracket to the box using the included sunk head screws.



2.Secure the assembly to wall/panel using the included tapping screws and anchors.



Purchase apps from the Azena Application Store

Sign up/log in to the Azena platform

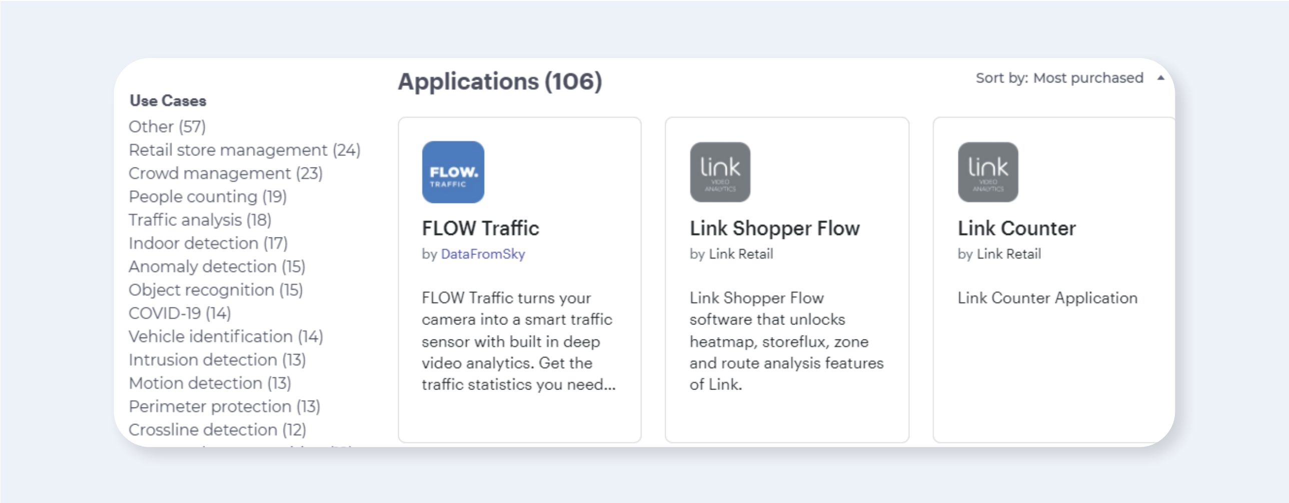
- Visit the Application Store and click "register".
- Choose in which role you want to use the Application Store, system integrator, application developer or both. Depending on which role you choose, the store will be set up for you.

First you'll be asked for information about you and your company as well as contact details. The email you give will be your login name. When everything is completed, we'll send you an email to confirm your identity.

Finally, we check your registration and provide you with your personal link to the shop by e-mail for you to start creating your user profile. In the "Team" section of your profile, you can also invite other users from your team and manage their user rights and permissions.

Browse the Application Store and find apps

To access the Azena Application Store, click on "Application Store" in the navigation bar at the top of the Azena website or visit store.azena.com/shop. There you will get an overview of the available apps, search function and detailed information.



Use Cases
Other (57)
Retail store management (24)
Crowd management (23)
People counting (19)
Traffic analysis (18)
Indoor detection (17)
Anomaly detection (15)
Object recognition (15)
COVID-19 (14)
Vehicle identification (14)
Intrusion detection (13)
Motion detection (13)
Perimeter protection (13)
Crossline detection (12)

Applications (106)

Sort by: Most purchased

FLOW Traffic
by DataFromSky
FLOW Traffic turns your camera into a smart traffic sensor with built in deep video analytics. Get the traffic statistics you need...

Link Shopper Flow
by Link Retail
Link Shopper Flow software that unlocks heatmap, storeflux, zone and route analysis features of Link.

Link Counter
by Link Retail
Link Counter Application

- Search for apps by name, developer and use cases
- Get an idea of each app's functionality, use cases and developer details
- See how other users rate the apps and browse their comments

Purchase the desired apps

Buying apps for your AI Box is as easy as searching and clicking. The Azena Application Store works in the same familiar way as other online shops.

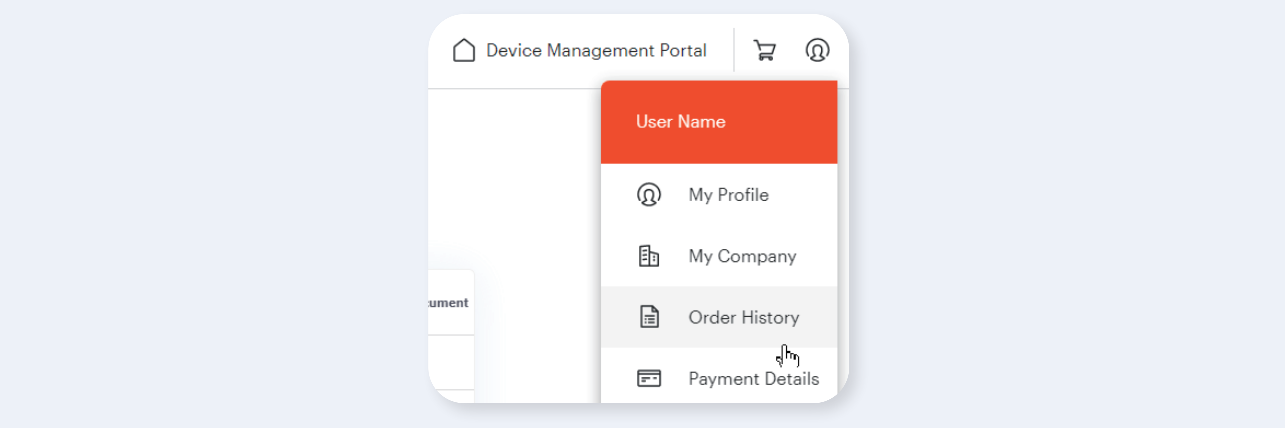
Add an app to the shopping cart with just one click

- Simply select the number of licences you need for your cameras in the app page's "Pricing" section and click "Add to card".
- If a trial version is available, you can install the app for free and test it for 30 days. Each trial licence expires automatically after this period.

Place orders and checkout securely

- After adding an app to your shopping cart, you're taken directly to the order summary. You also get there by clicking the shopping cart symbol at the top of the page.
- When you're ready to buy, just click "Place order". The new app is immediately added to your apps. You get there by clicking "Applications" in the navigation at the top of the page. With every purchase you'll receive a confirmation email.

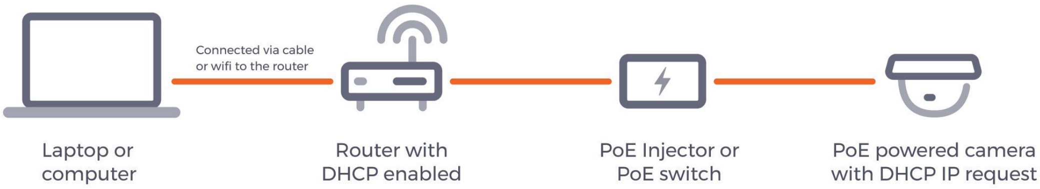
Note: You'll find an overview of all your orders in the "Order history" section, in the profile menu in the upper right corner of the Application Store.



Scan here for the full Azena Application Store guide:

Configuration

1. Download the **Device Management Tool**. The tool can be requested here:
   https://devices.azena.com/tooldownload


Connected via cable or wifi to the router
Laptop or computer
Router with DHCP enabled
PoE Injector or PoE switch
PoE powered camera with DHCP IP request

Make sure DHCP service is available in your local network.

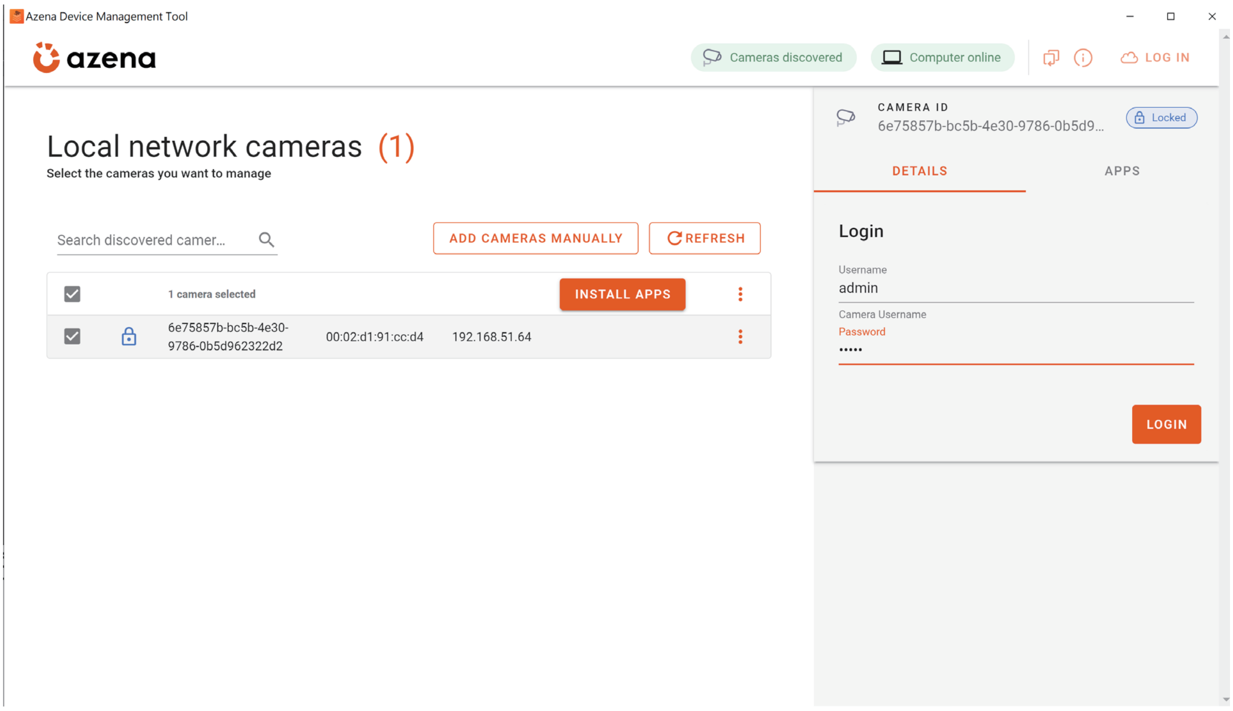
Resources:

1 User Management Guide: https://hubs.ly/H0xV2j40

2 Download Azena Device Management Tool: https://hubs.li/H0xYjtL0

3 Network Firewall Details: https://hubs.li/H0xYhkr0

2. Use the Device Management Tool to locate your device.



Local network cameras (1)

Select the cameras you want to manage

☑		1 camera selected		
☑	🔒	6e75857b-bc5b-4e30-9786-0b5d962322d2	00:02:d1:91:cc:d4	192.168.51.64

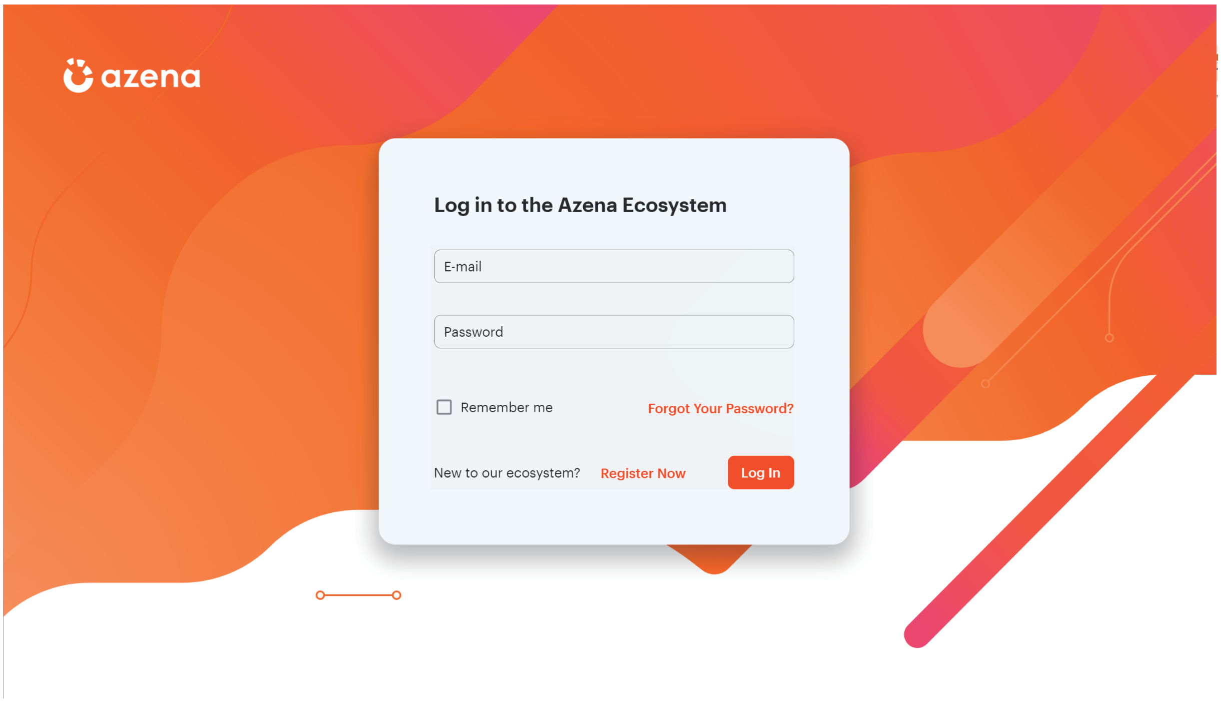
CAMERA ID
6e75857b-bc5b-4e30-9786-0b5d9...

Login

Username
admin

Camera Username
Password
•••••

3. You can click Cloud Login to download Azena apps or visit:
https://store.azena.com/shop/



azena

Log in to the Azena Ecosystem

E-mail

Password

□ Remember me

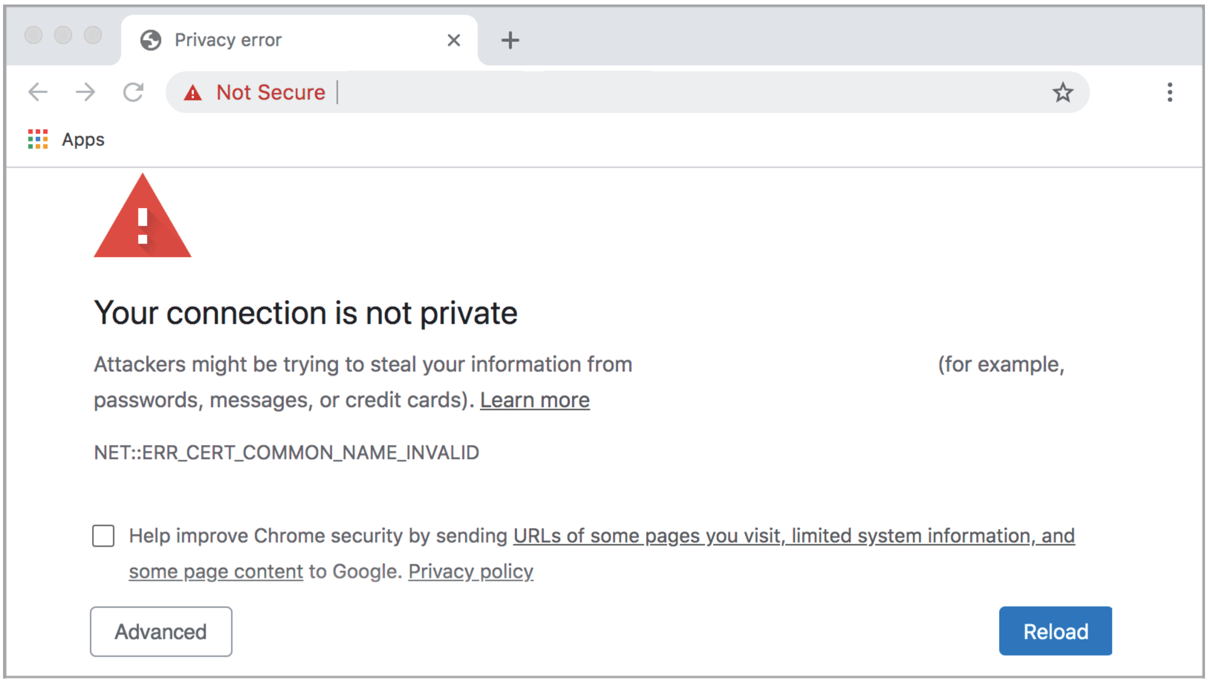
Forgot Your Password?

New to our ecosystem? Register Now

4. Enter URL: https://<ip_address>:8443/

Enter admin/admin as the default credential.

Since the connection is using a self-signed certificate, your connection will not be considered as a secure connection. Click Advanced to proceed.



Your connection is not private

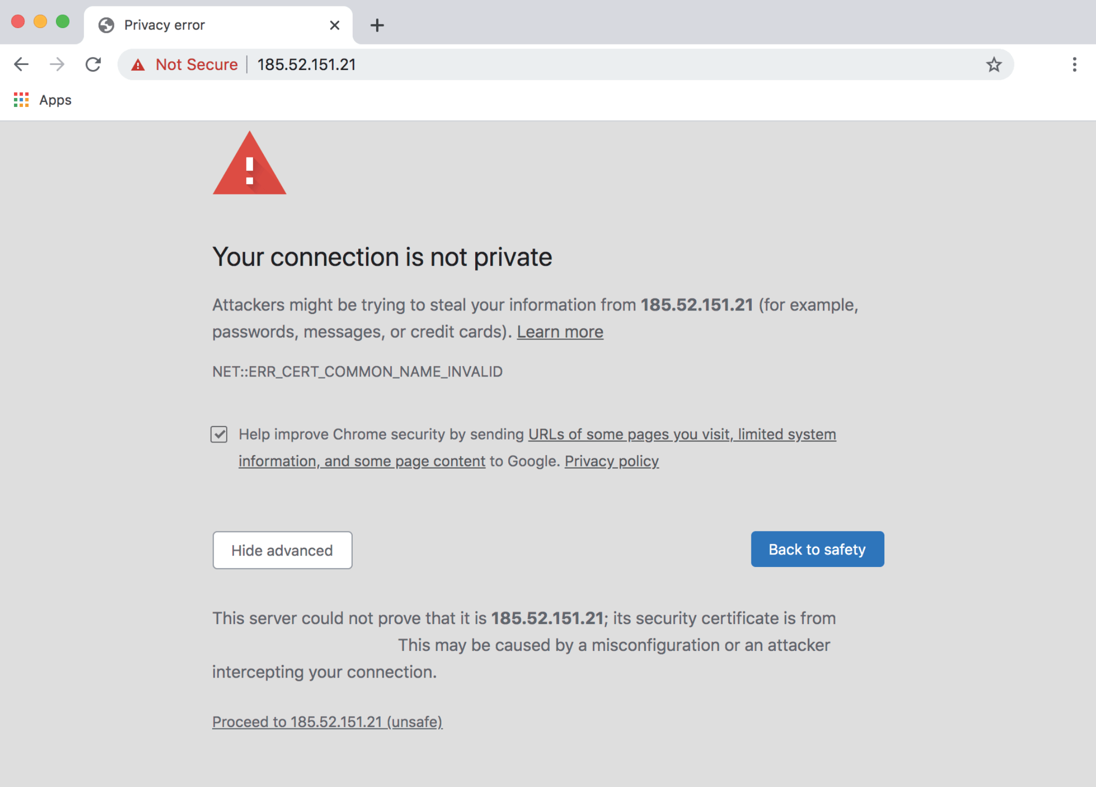
Attackers might be trying to steal your information from (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Click Proceed to xxx.xxx.xxx.xxx (Unsafe) to open the web console.

Note the IP addresses below are for reference only.



Your connection is not private

Attackers might be trying to steal your information from **185.52.151.21** (for example, passwords, messages, or credit cards). Learn more

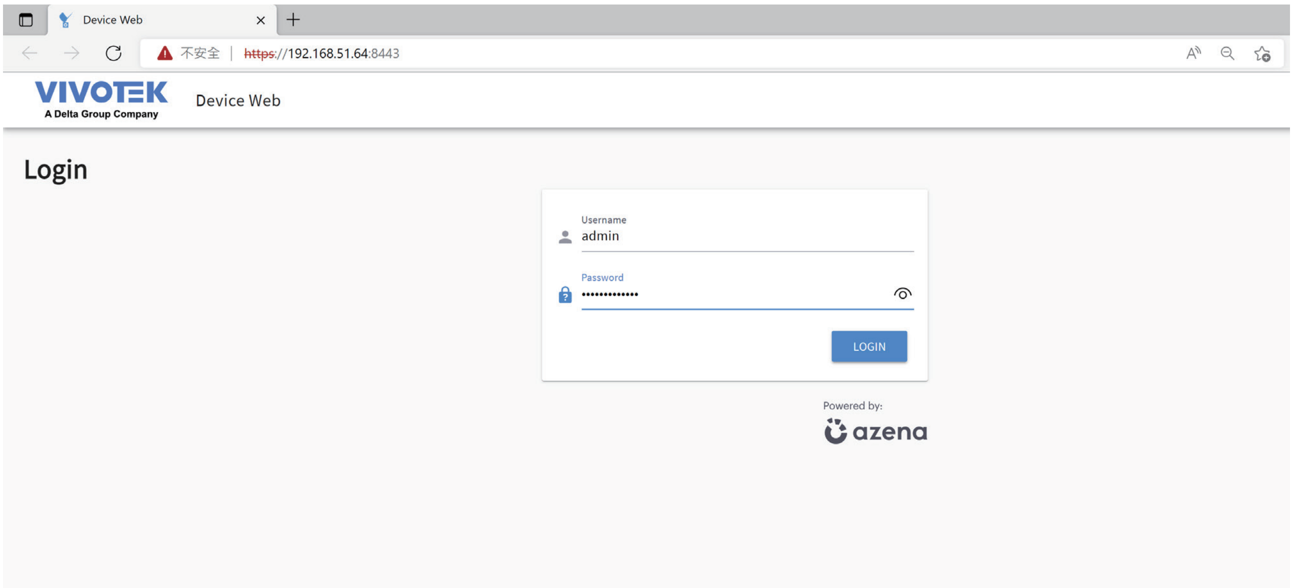
NET::ERR_CERT_COMMON_NAME_INVALID

☑ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is **185.52.151.21**; its security certificate is from This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 185.52.151.21 (unsafe)

Enter **admin/admin** as the default credential.



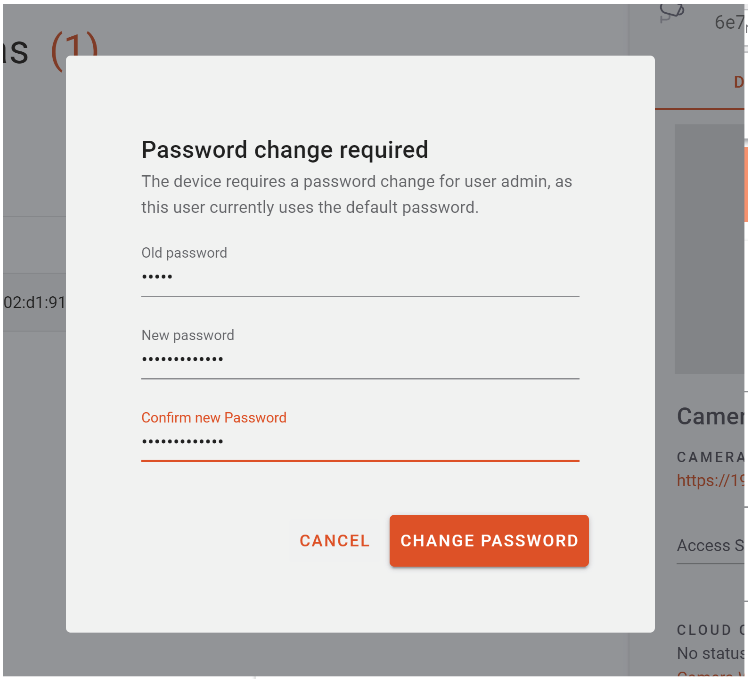
Login

Username
admin

Password
•••••••••••••

You will be requested to create a new password for security concern. Enter a combination of alphabetic, numeric, and special characters that is strong enough for protection.

The new password must comprise of at least 10 characters, containing uppercase, lowercase, digits or special characters.



Password change required

The device requires a password change for user admin, as this user currently uses the default password.

Old password
•••••

New password
•••••••••••••

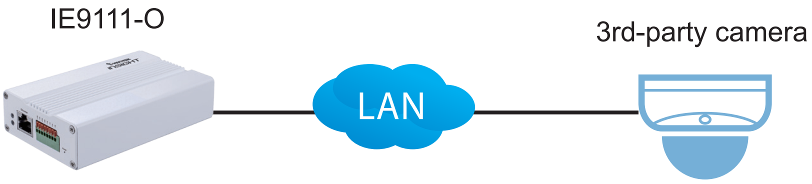
Confirm new Password
•••••••••••••

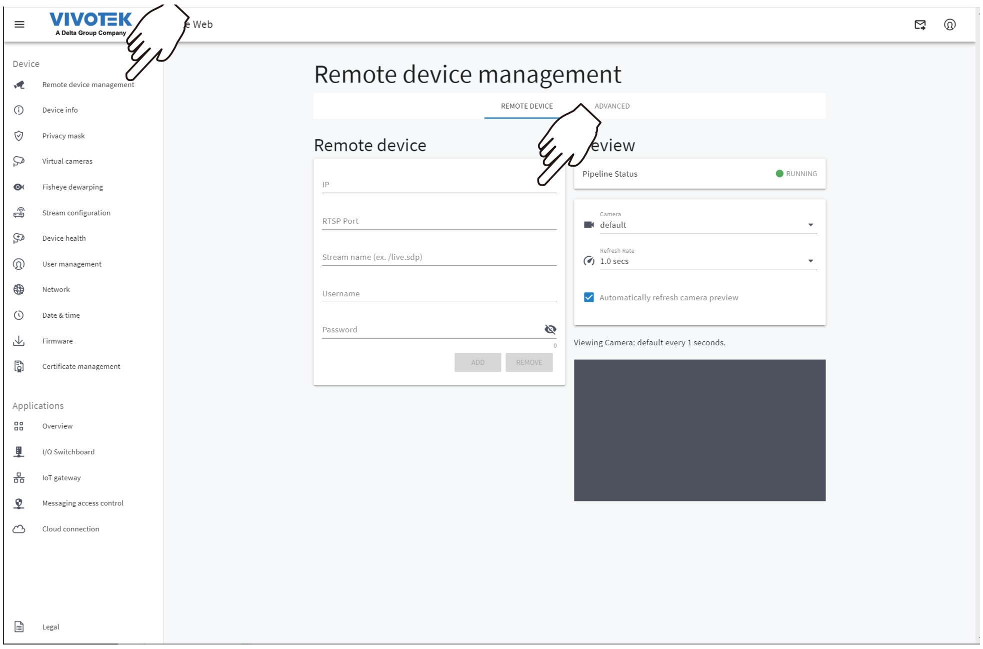
You can also use 3rd party tools like Onvif Device Manager to discover the Azena enabled cameras.

NOTE:

If installing or testing Insight devices on a network with different VMS, there will be a chance that a software like Nx Witness will scan and try to add the devices automatically. If this happens, the user will be timed out from our devices due to login failures. It is highly recommended that users change their login name from "admin" to something else, or add a second login account.

5. From the Remote device management page, you can enter the address, and credentials for connecting to the 3rd-party IP camera.





Remote device management

Remote device

IP

RTSP Port

Stream name (ex. /live.sdp)

Username

Password

0

eview

Pipeline Status ● RUNNING

Camera: default

Refresh Rate: 1.0 secs

☑ Automatically refresh camera preview

Viewing Camera: default every 1 seconds.

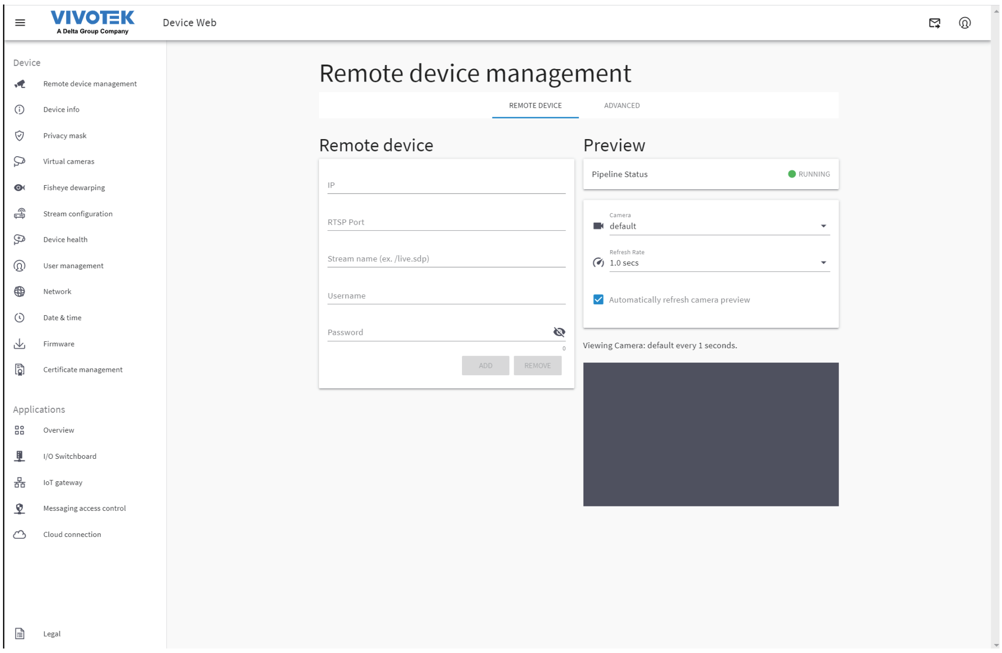
Enter 8554 as the RTSP port.

Enter /live.sdp as the stream name. /live1s1.sdp can also be used.

For some older models, the RTSP port can be 554.

Remote Management

This page is used mainly to connect a 3rd-party network camera.



Remote device management

Remote device

Preview

Pipeline Status ● RUNNING

Camera: default

Refresh Rate: 1.0 secs

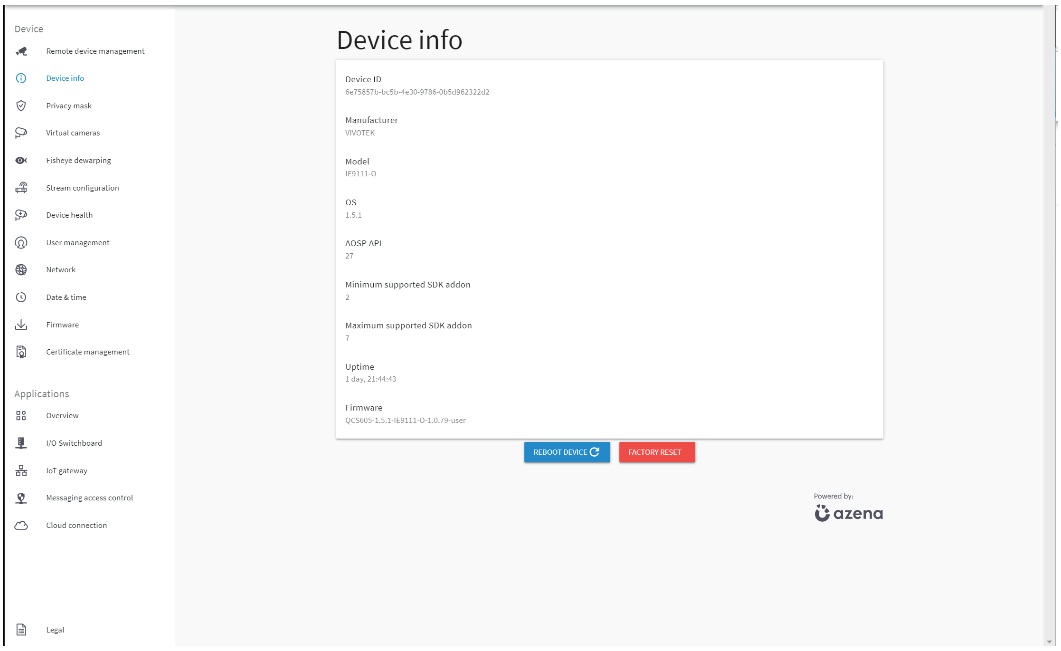
☑ Automatically refresh camera preview

Viewing Camera: default every 1 seconds.

Device Info

Important information about this device is displayed on this page: including Device ID, OS version, AOSP API, SDK addon, firmware version, etc.
The Device ID is a unique ID for each camera and will be displayed in the Device Management Portal.

Here, you can also reboot the device or perform a Factory reset.



Device info

Device ID
6e75857b-bc5b-4e30-9786-0b5d962322d2

Manufacturer
VIVOTEK

Model
IE9111-O

OS
1.5.1

AOSP API
27

Minimum supported SDK addon
2

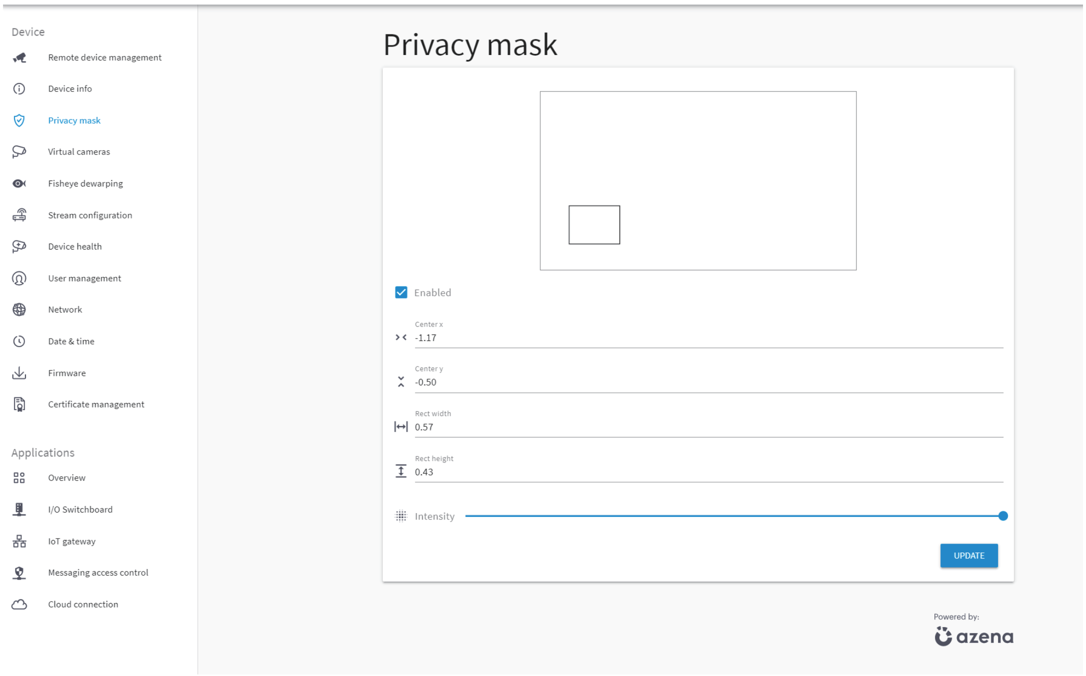
Maximum supported SDK addon
7

Uptime
1 day, 21:44:43

Firmware
QCS605-1.5.1-IE9111-O-1.0.79-user

Privacy Mask

Click and drag on the screen to block out sensitive areas in your field of view. The size the orientation will display on screen. Use the Intensity slide bar to determine how much image within the privacy mask is blurred. Currently 1 privacy mask is supported.



Privacy mask

☑ Enabled

Center x
-1.17

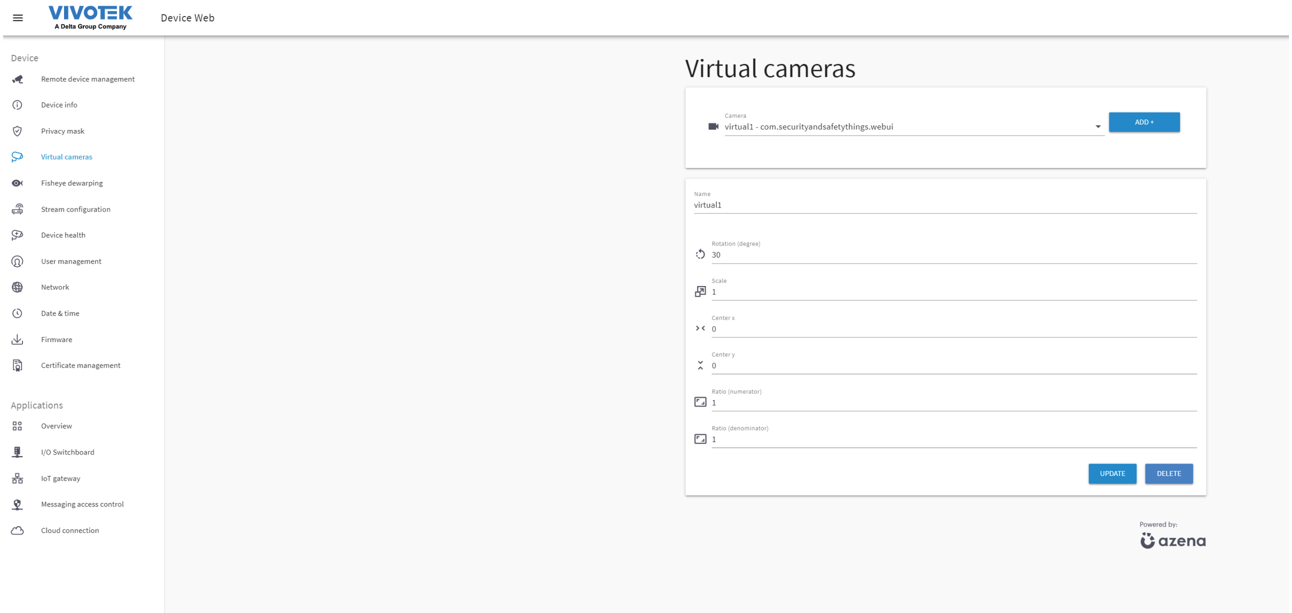
Center y
-0.50

Rect width
0.57

Rect height
0.43

Virtual Camera

Allows the creation of additional sub-stream(s) which can cover a certain zone of interest in the camera's field of view. The sub-streams are used for video analytics on apps.



Virtual cameras

Camera: virtual1 - com.securityandsafetythings.webui

Name: virtual1

Rotation (degree): 30

Scale: 1

Center x: 0

Center y: 0

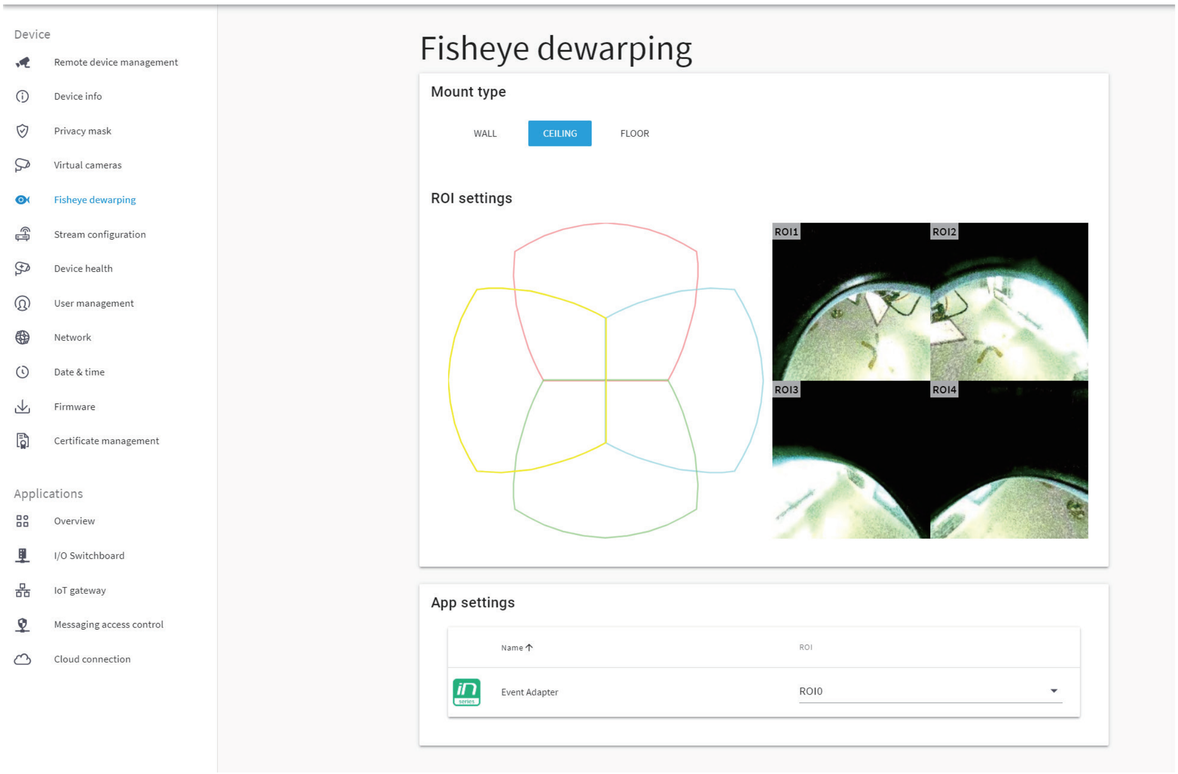
Ratio (numerator): 1

Ratio (denominator): 1

Fisheye dewarping

On this page, there are four pre-configured Region of Interest for the dewarped views for a fisheye camera.

Streams are defined as Full High Definition and Ultra High Definition streams.



Fisheye dewarping

Mount type: CEILING

ROI settings

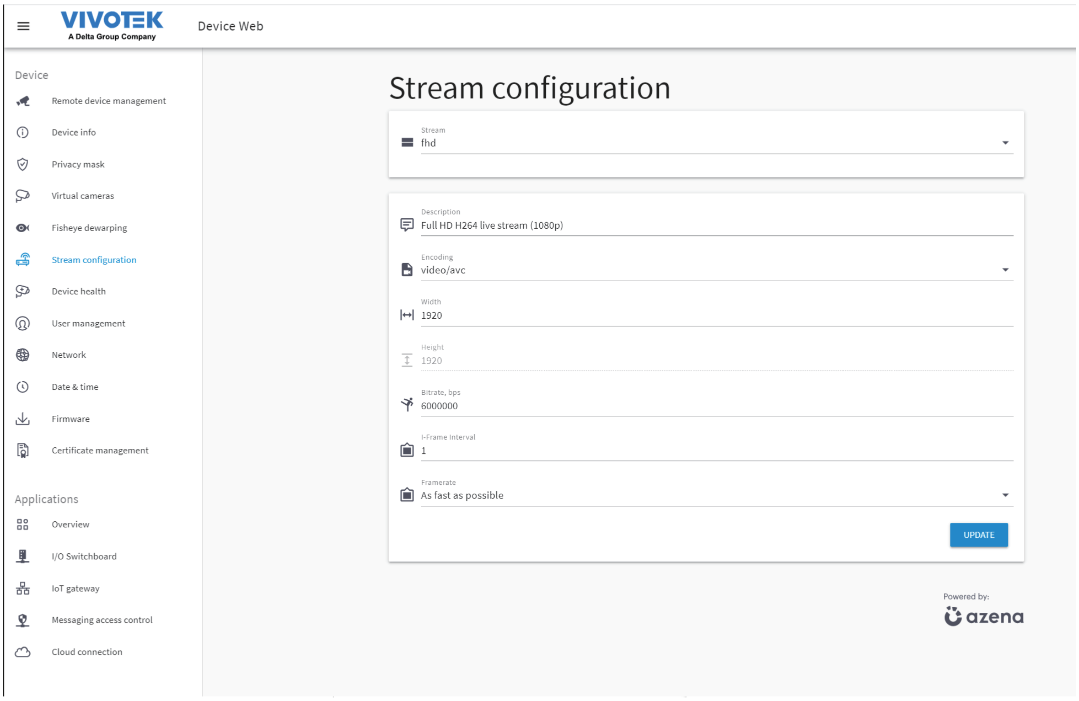
App settings

Name ↑	ROI
Event Adapter	ROI0

Stream Configuration

On this page, there are four pre-configured video streams which can be additionally modified with regards to encoding, size, bitrate and I-frame interval.

Streams are defined as Full High Definition and Ultra High Definition streams.



Stream configuration

Stream: fhd

Description: Full HD H264 live stream (1080p)

Encoding: video/avc

Width: 1920

Height: 1920

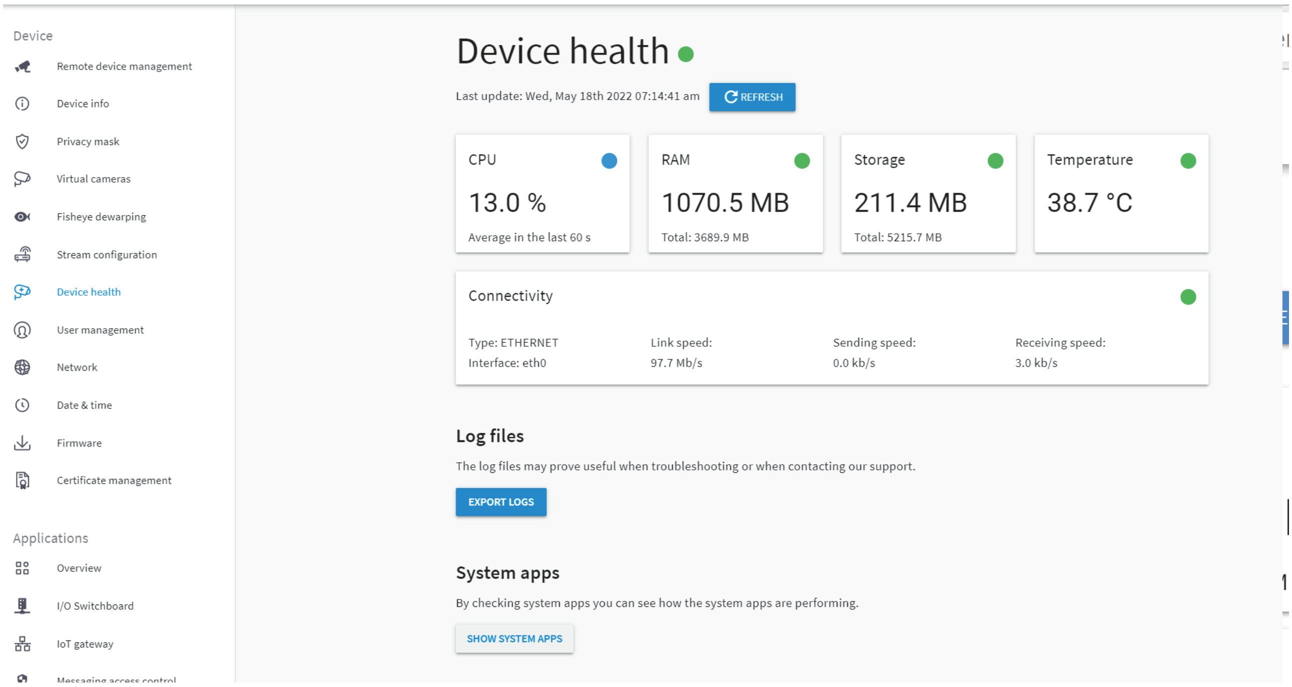
Bitrate, bps: 6000000

I-Frame Interval: 1

Framerate: As fast as possible

Device Health

This page displays various device health information: CPU/Memory/Storage usage, Connectivity, Temperature and App status. You can also export a system log for troubleshooting.



Device health ●

Last update: Wed, May 18th 2022 07:14:41 am

CPU ●
13.0 %
Average in the last 60 s

RAM ●
1070.5 MB
Total: 3689.9 MB

Storage ●
211.4 MB
Total: 5215.7 MB

Temperature ●
38.7 °C

Connectivity ●

Type: ETHERNET
Interface: eth0

Link speed:
97.7 Mb/s

Sending speed:
0.0 kb/s

Receiving speed:
3.0 kb/s

Log files

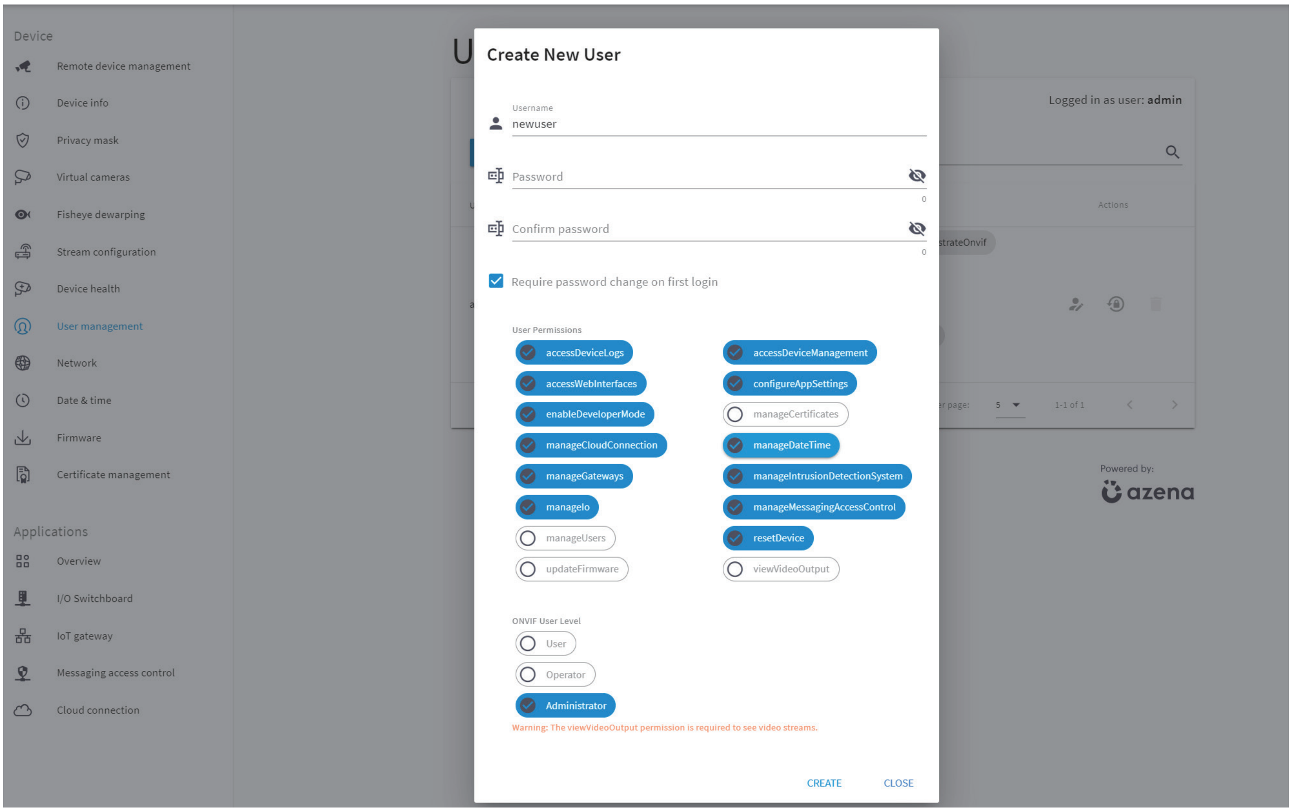
The log files may prove useful when troubleshooting or when contacting our support.

System apps

By checking system apps you can see how the system apps are performing.

User Management

On this page, you can add/remove users and set user's rights and permissions. Select the management rights from the checkboxes.



Logged in as user: **admin**

Create New User

Username
newuser

Password
0

Confirm password
0

☑ Require password change on first login

User Permissions

✓ accessDeviceLogs
✓ accessDeviceManagement
✓ accessWebInterfaces
✓ configureAppSettings
✓ enableDeveloperMode
○ manageCertificates
✓ manageCloudConnection
✓ manageDateTime
✓ manageGateways
✓ manageIntrusionDetectionSystem
✓ manageIo
✓ manageMessagingAccessControl
○ manageUsers
✓ resetDevice
○ updateFirmware
○ viewVideoOutput

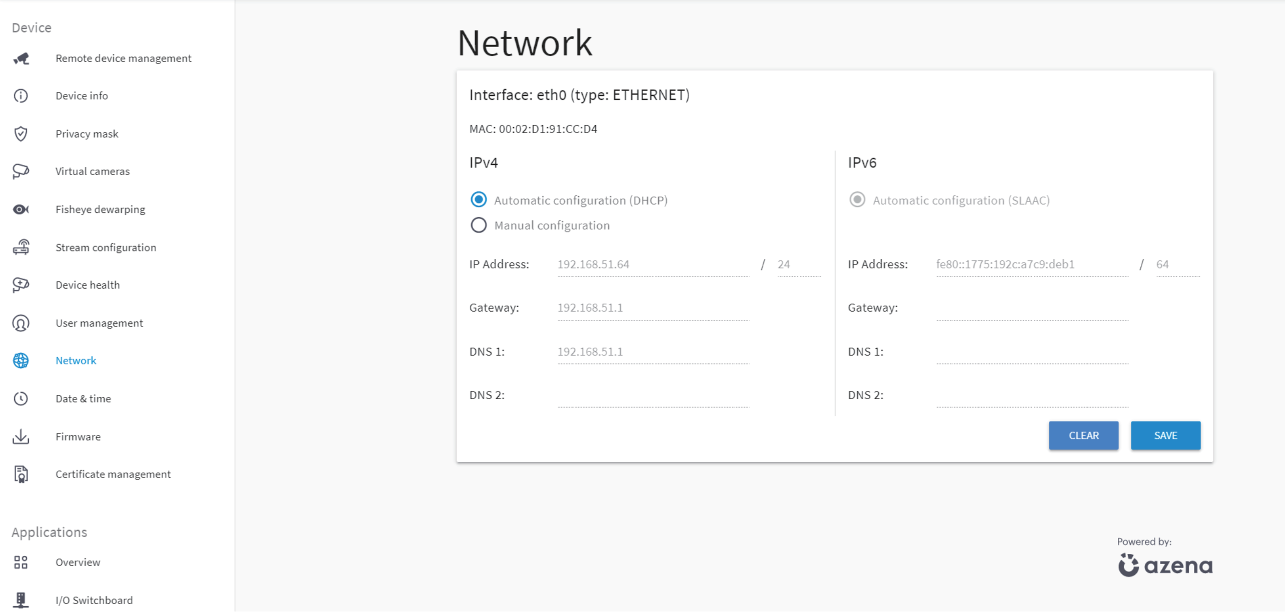
ONVIF User Level

○ User
○ Operator
✓ Administrator

Warning: The viewVideoOutput permission is required to see video streams.

Network

By default, the AI box has the network setup to receive the IP address via DHCP. On this page you can change different network parameters, disable the DHCP and set a specific IP.



Network

Interface: eth0 (type: ETHERNET)

MAC: 00:02:D1:91:CC:D4

IPv4

● Automatic configuration (DHCP)
○ Manual configuration

IP Address: 192.168.51.64 / 24

Gateway: 192.168.51.1

DNS 1: 192.168.51.1

DNS 2:

IPv6

● Automatic configuration (SLAAC)

IP Address: fe80::1775:192c:a7c9:deb1 / 64

Gateway:

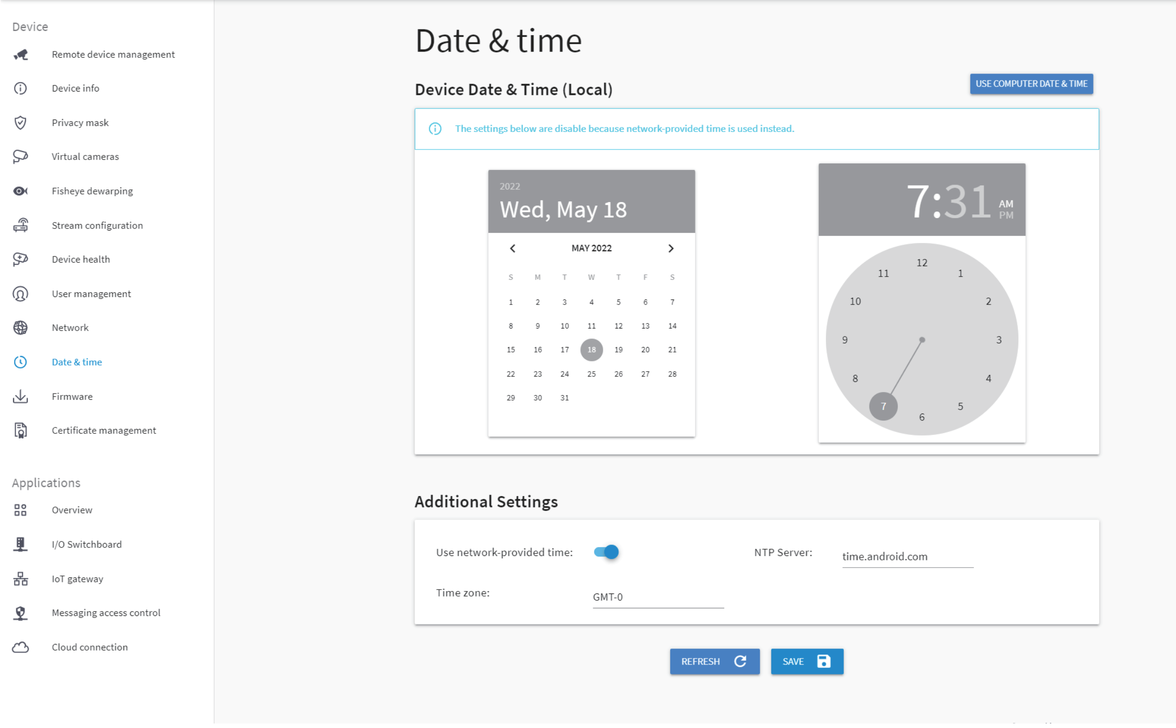
DNS 1:

DNS 2:

Date & Time

This page allows the user to configure the current date/time on the device, synchronize with computer time and also to enable network time synchronization via an NTP server.

The network time setting is necessary when you "**claim**" the camera for downloading apps.



Date & time

Device Date & Time (Local)

The settings below are disable because network-provided time is used instead.

Additional Settings

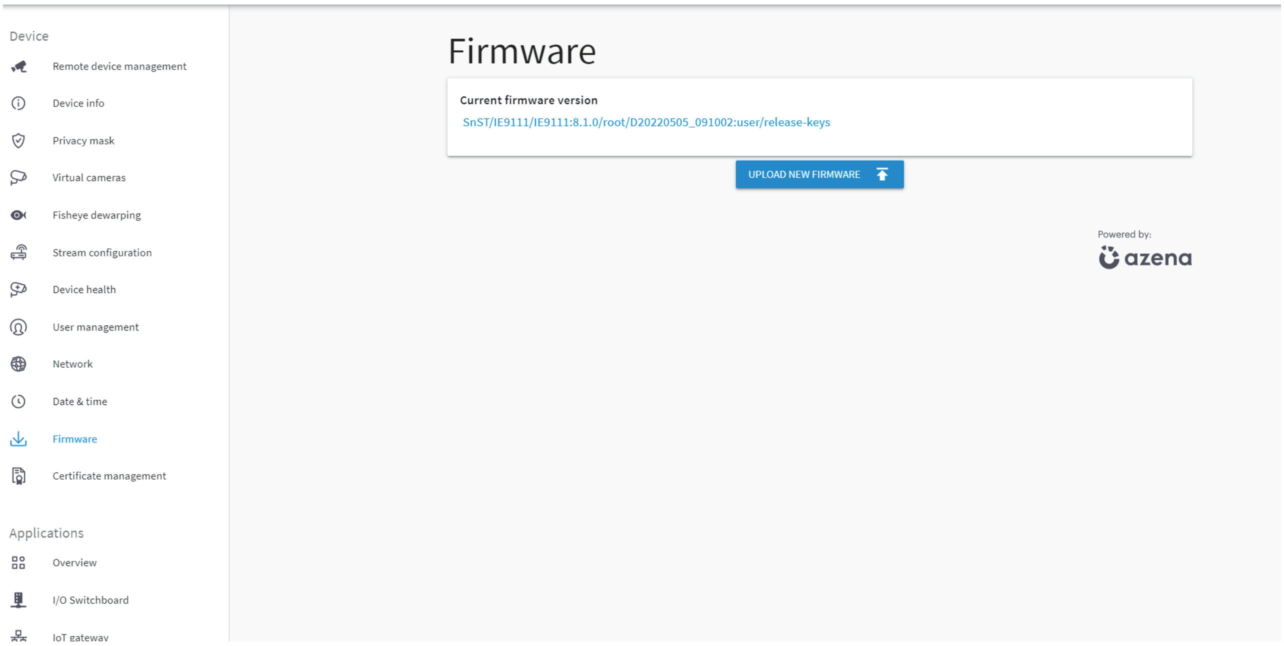
Use network-provided time: on

NTP Server: time.android.com

Time zone: GMT-0

Firmware

On this page you can perform a Firmware (OS version) OTA upgrade.

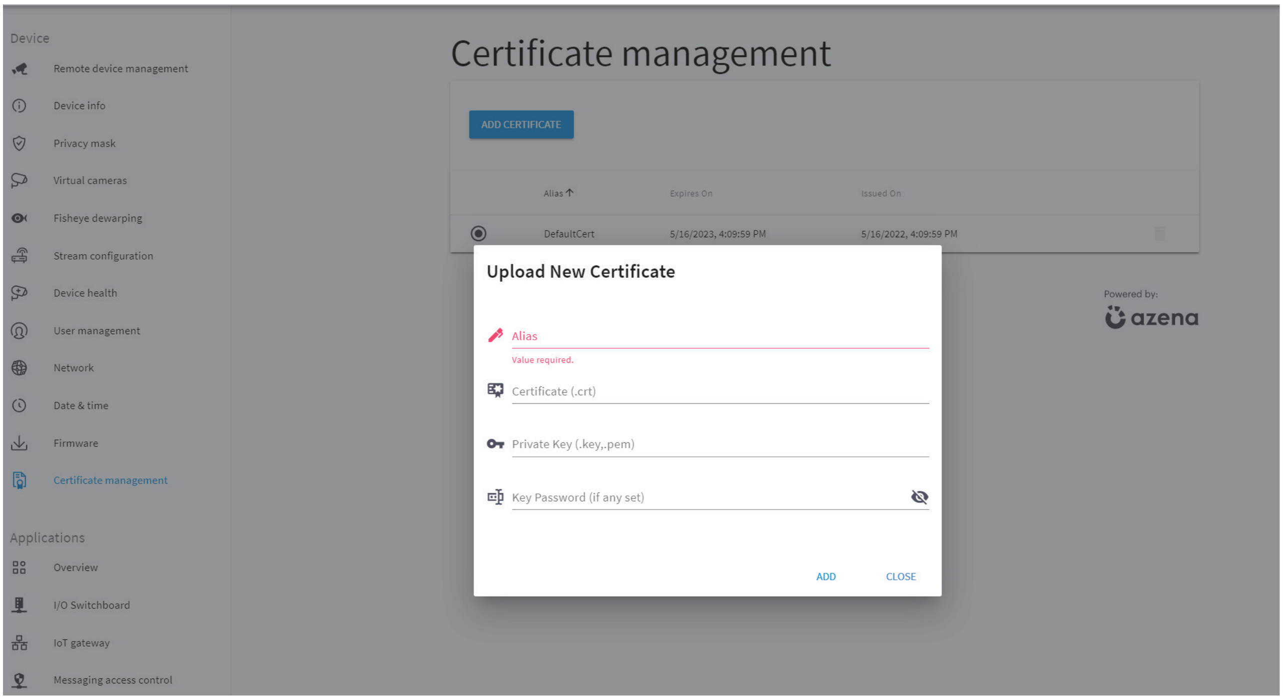


Firmware

Current firmware version
SnST/IE9111/IE9111:8.1.0/root/D20220505_091002:user/release-keys

Certificate management

Use this page to upload a certificate for secure connection.



Certificate management

	Alias ↑	Expires On	Issued On
●	DefaultCert	5/16/2023, 4:09:59 PM	5/16/2022, 4:09:59 PM

Upload New Certificate

Alias
Value required.

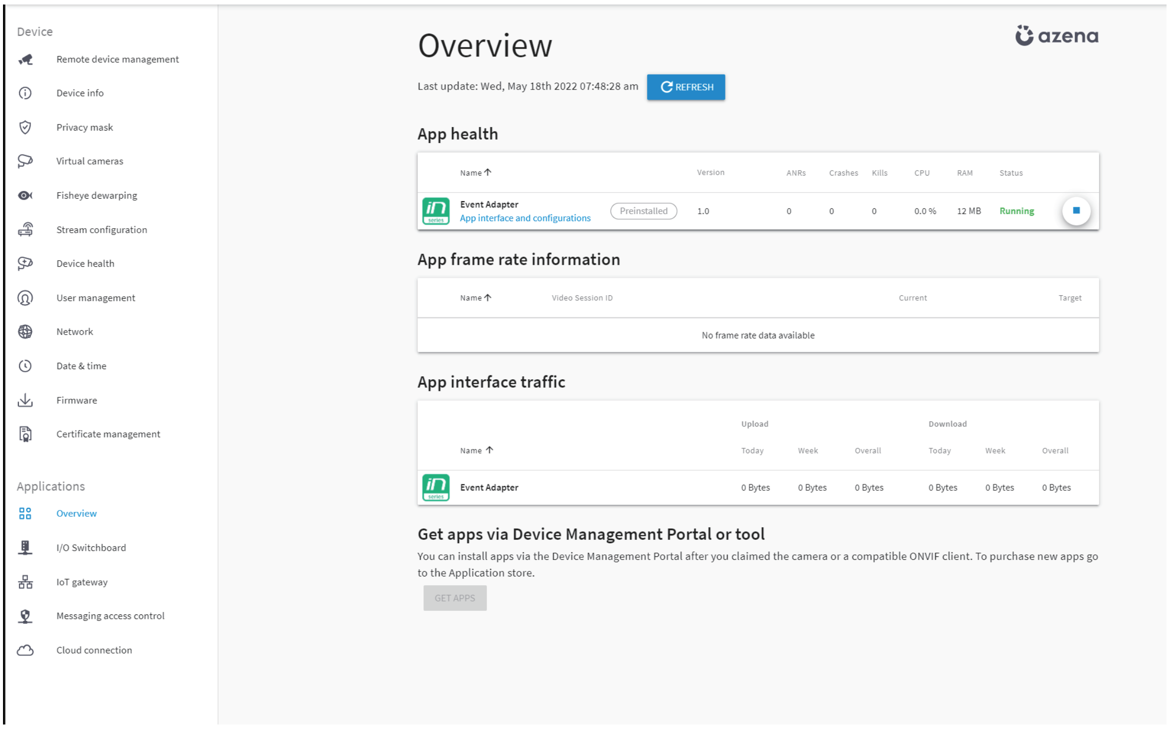
Certificate (.crt)

Private Key (.key,.pem)

Key Password (if any set)

Applications - Overview

On this page, users can see all the installed applications, their status, version and they can also start/stop or uninstall an application using the vertical 3-dot menu:



Overview

Last update: Wed, May 18th 2022 07:48:28 am

App health

Name ↑		Version	ANRs	Crashes	Kills	CPU	RAM	Status
Event Adapter App interface and configurations	Preinstalled	1.0	0	0	0	0.0 %	12 MB	Running

App frame rate information

Name ↑	Video Session ID	Current	Target
No frame rate data available			

App interface traffic

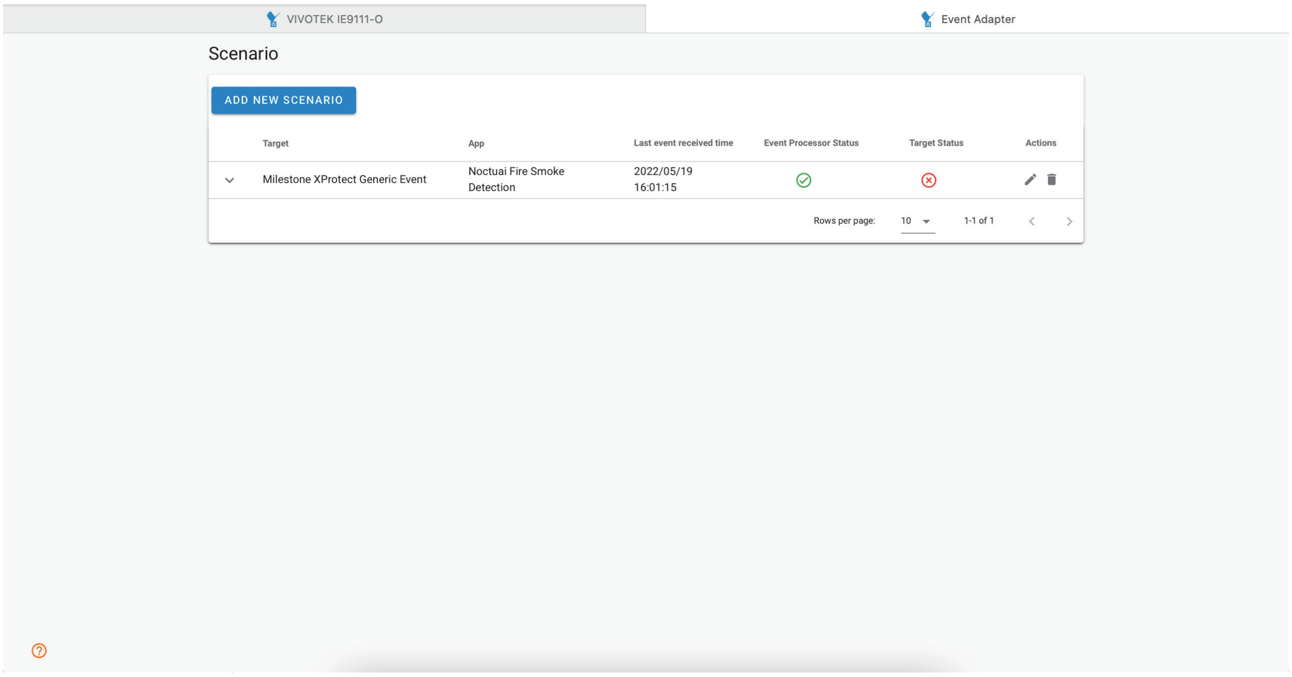
	Upload			Download		
Name ↑	Today	Week	Overall	Today	Week	Overall
Event Adapter	0 Bytes	0 Bytes	0 Bytes	0 Bytes	0 Bytes	0 Bytes

Get apps via Device Management Portal or tool

You can install apps via the Device Management Portal after you claimed the camera or a compatible ONVIF client. To purchase new apps go to the Application store.

Data Magnet and VAST2

To enable the display of video analytics from apps on the VAST2, click on the **App interface and configurations**. Please note that **NOT ALL** Azena apps can be integrated through the Data Magnet interface.



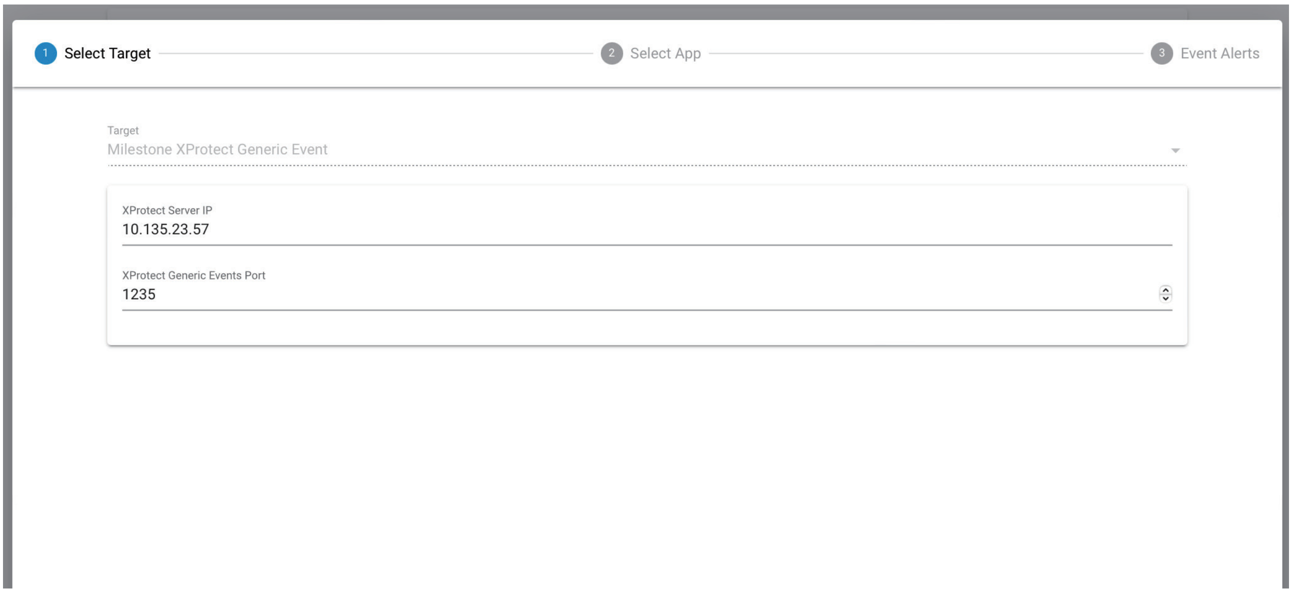
Scenario

	Target	App	Last event received time	Event Processor Status	Target Status	Actions
⌄	Milestone XProtect Generic Event	Noctuai Fire Smoke Detection	2022/05/19 16:01:15	✓	⊗	✎ 🗑

Rows per page: 10 ▾ 1-1 of 1 ‹ ›

Enter the following to enable the connection through Data Magnet:

1. Your VAST2 server IP.
2. Data Magnet port: usually 3443.
3. Data Source Name: Note that this name **must be identical** to that on the VAST2 Data Magnet setting page.
4. VAST2 user name and password.
5. Select the app installed on your device. Click the Update button.

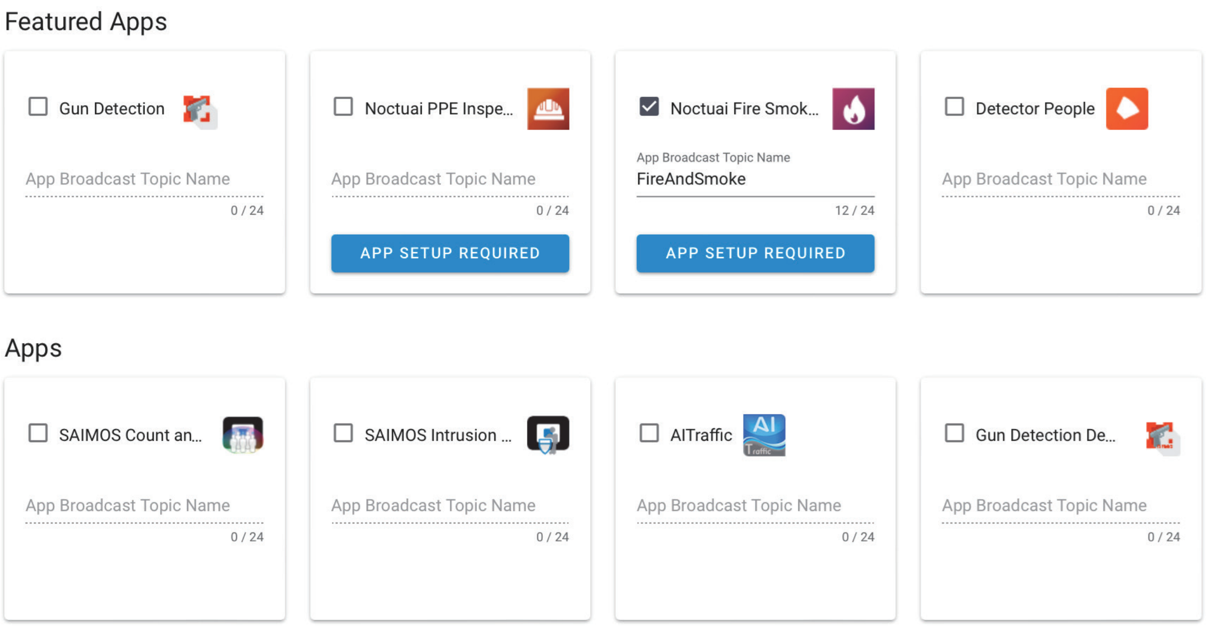


1 Select Target — 2 Select App — 3 Event Alerts

Target: Milestone XProtect Generic Event

XProtect Server IP: 10.135.23.57

XProtect Generic Events Port: 1235



Featured Apps

□ Gun Detection — App Broadcast Topic Name — 0 / 24

□ Noctuai PPE Inspe... — App Broadcast Topic Name — 0 / 24 — APP SETUP REQUIRED

☑ Noctuai Fire Smok... — App Broadcast Topic Name: FireAndSmoke — 12 / 24 — APP SETUP REQUIRED

□ Detector People — App Broadcast Topic Name — 0 / 24

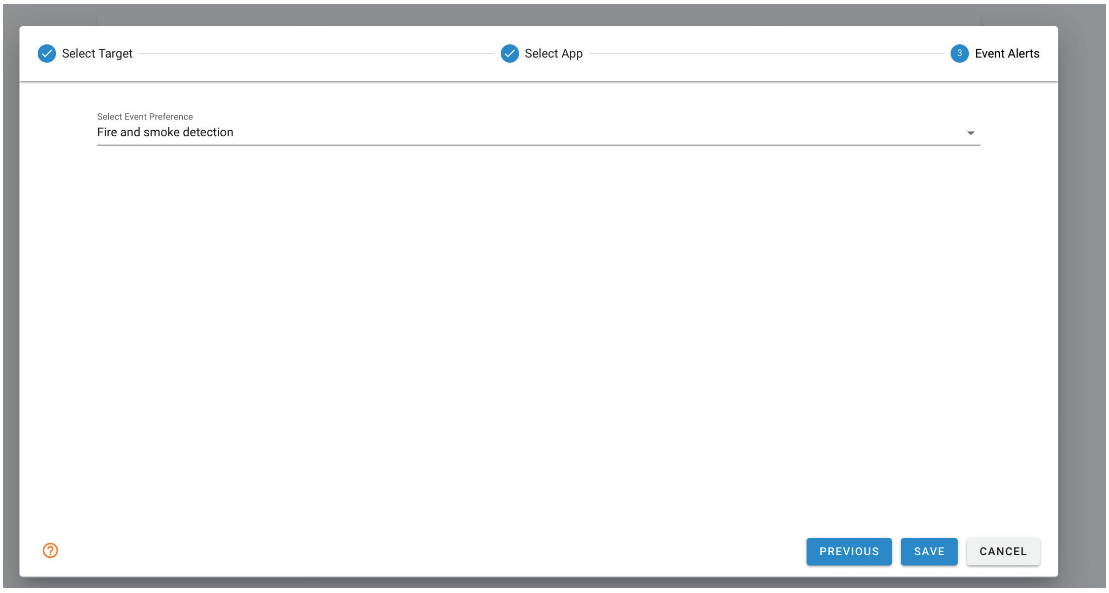
Apps

□ SAIMOS Count an... — App Broadcast Topic Name — 0 / 24

□ SAIMOS Intrusion ... — App Broadcast Topic Name — 0 / 24

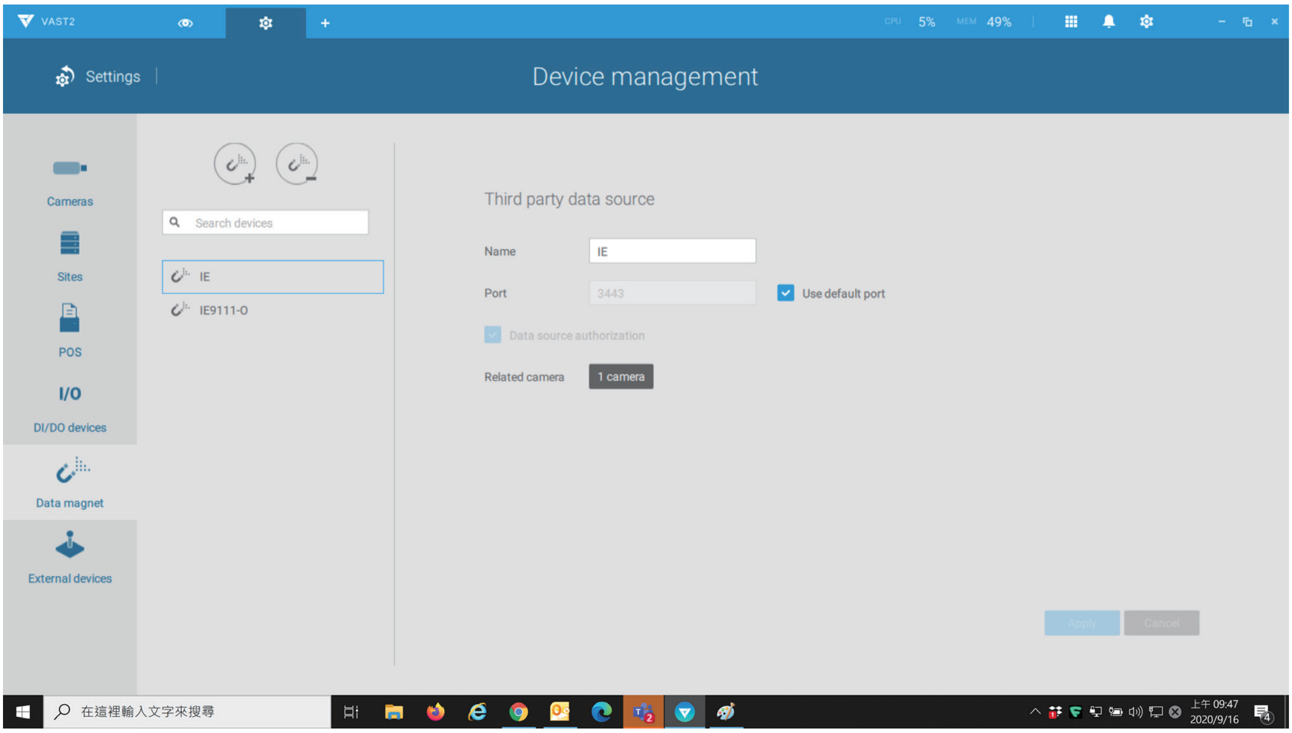
□ AITraffic — App Broadcast Topic Name — 0 / 24

□ Gun Detection De... — App Broadcast Topic Name — 0 / 24



Select Event Preference: Fire and smoke detection

6. On VAST2 > Settings > Device > Data Magnet, click Add data source.



Third party data source

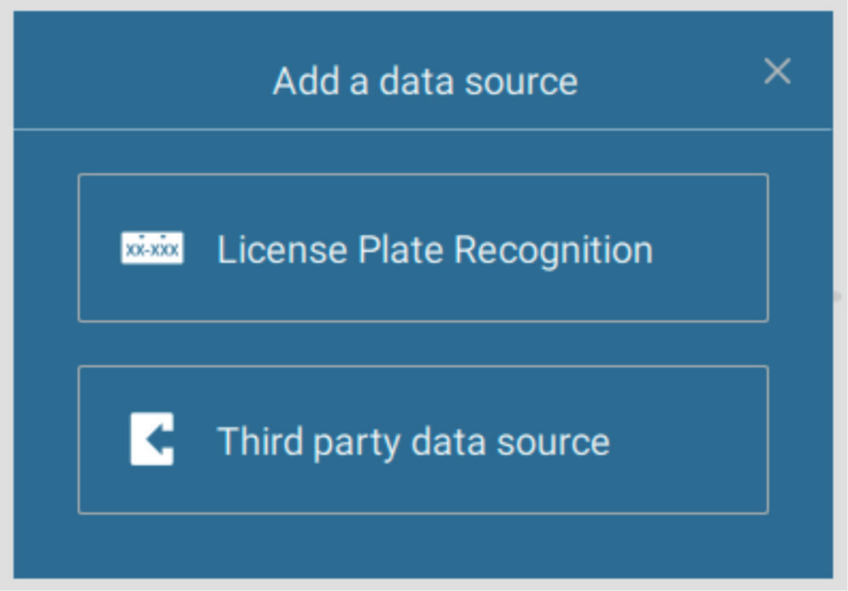
Name: IE

Port: 3443 ☑ Use default port

☑ Data source authorization

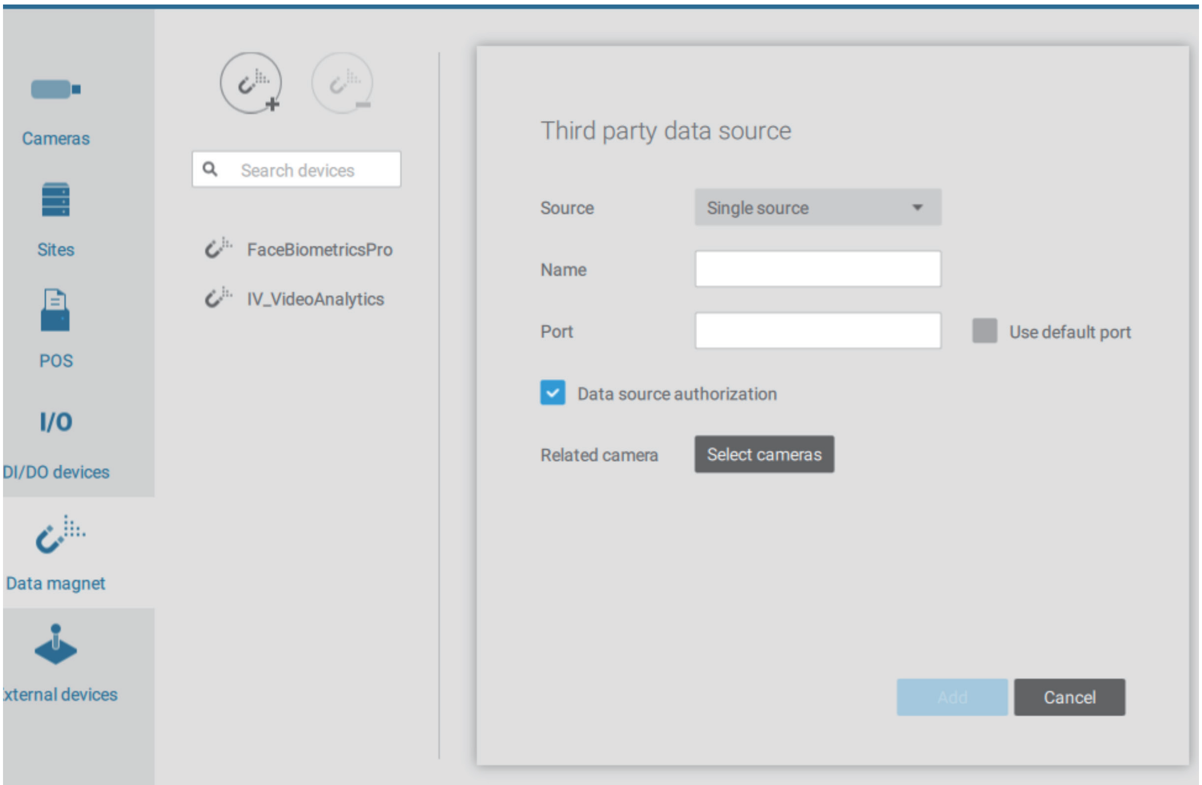
Related camera: 1 camera

7. Select Third party data source.



8. Enter the Data Source Name, port (usually 3443), select the associated camera, and click Add.

   Note that the camera should be the one that the IE9111-O is connected to. The camera should be manually added to VAST2.



Third party data source

Source: Single source

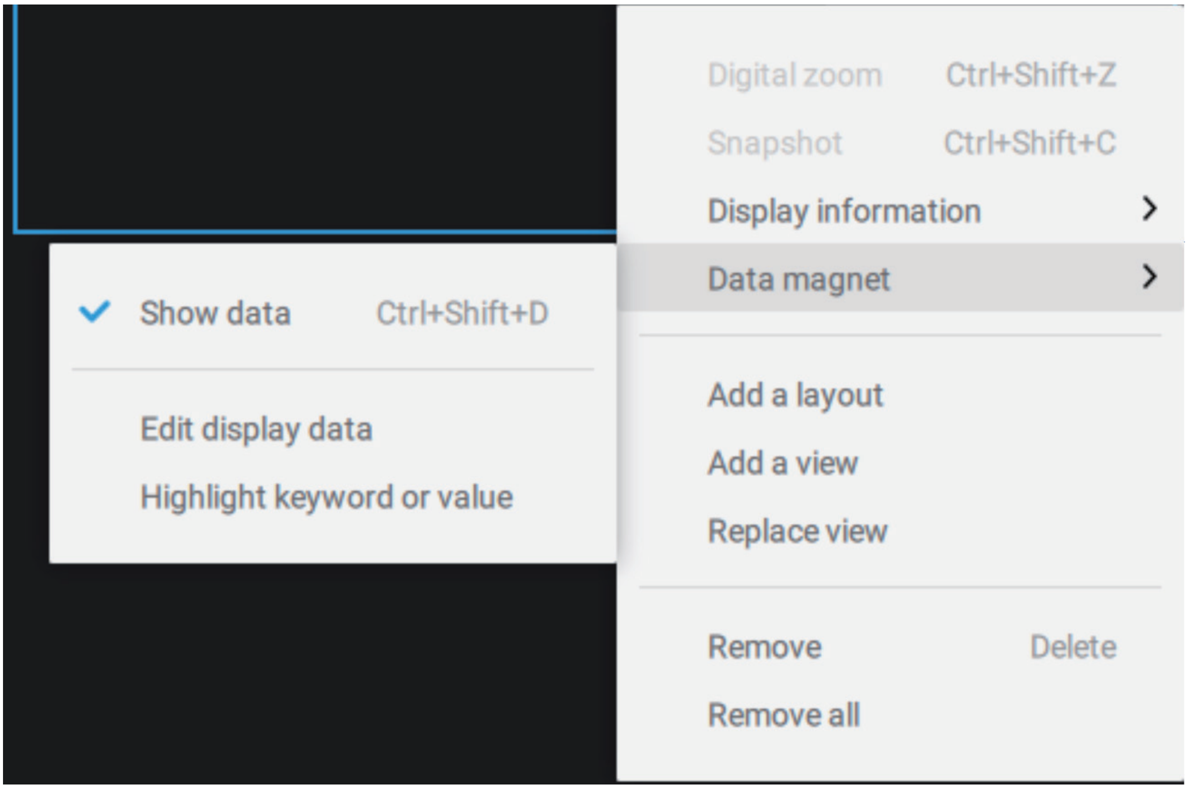
Name:

Port: □ Use default port

☑ Data source authorization

Related camera: Select cameras

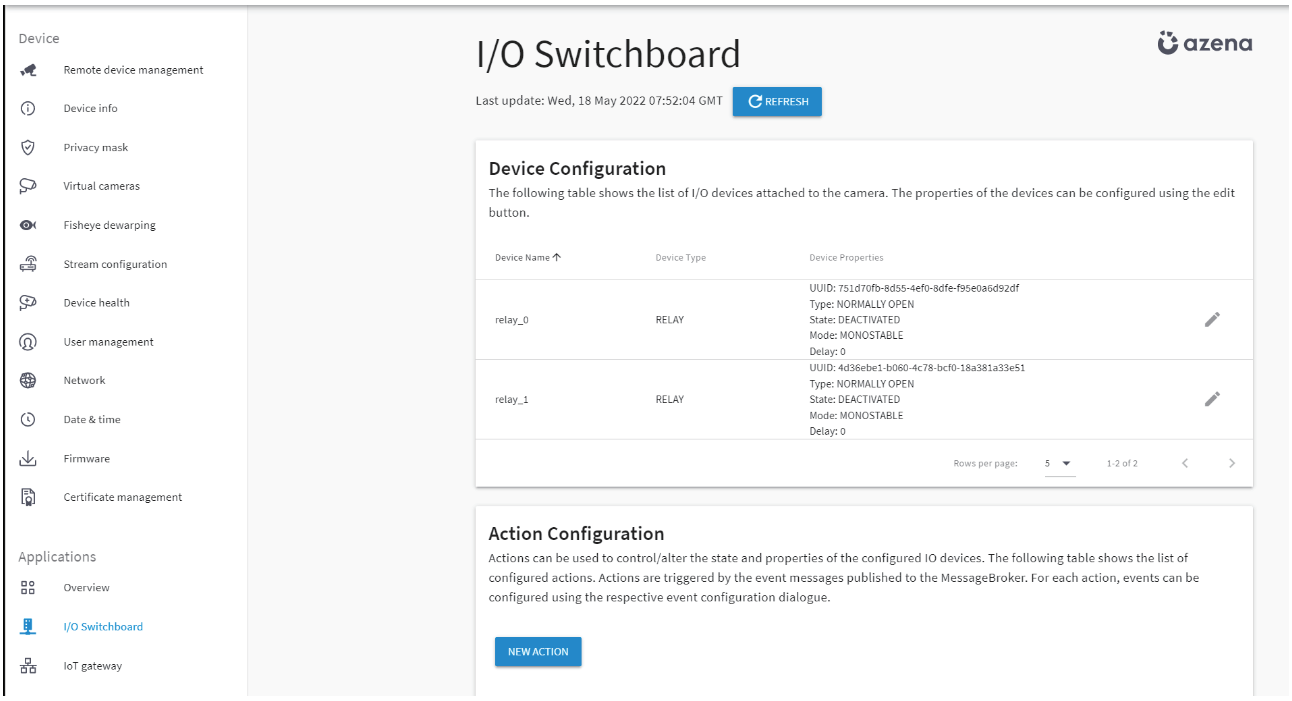
9. You can then right-click on a VAST2 view cell to display the Data magnet data. The analytics detection results can display along with the live video.



I/O Switchboard

From this page, you can detect the connected statuses of external relay devices. where it can be easily retrieved. Check the statuses and see if the connected devices are working properly.

You can then configure the action to activate those devices.



I/O Switchboard

Last update: Wed, 18 May 2022 07:52:04 GMT

Device Configuration

The following table shows the list of I/O devices attached to the camera. The properties of the devices can be configured using the edit button.

Device Name ↑	Device Type	Device Properties
relay_0	RELAY	UUID: 751d70fb-8d55-4ef0-8dfe-f95e0a6d92df Type: NORMALLY OPEN State: DEACTIVATED Mode: MONOSTABLE Delay: 0
relay_1	RELAY	UUID: 4d36ebe1-b060-4c78-bcf0-18a381a33e51 Type: NORMALLY OPEN State: DEACTIVATED Mode: MONOSTABLE Delay: 0

Rows per page: 5 1-2 of 2

Action Configuration

Actions can be used to control/alter the state and properties of the configured IO devices. The following table shows the list of configured actions. Actions are triggered by the event messages published to the MessageBroker. For each action, events can be configured using the respective event configuration dialogue.

IoT gateway

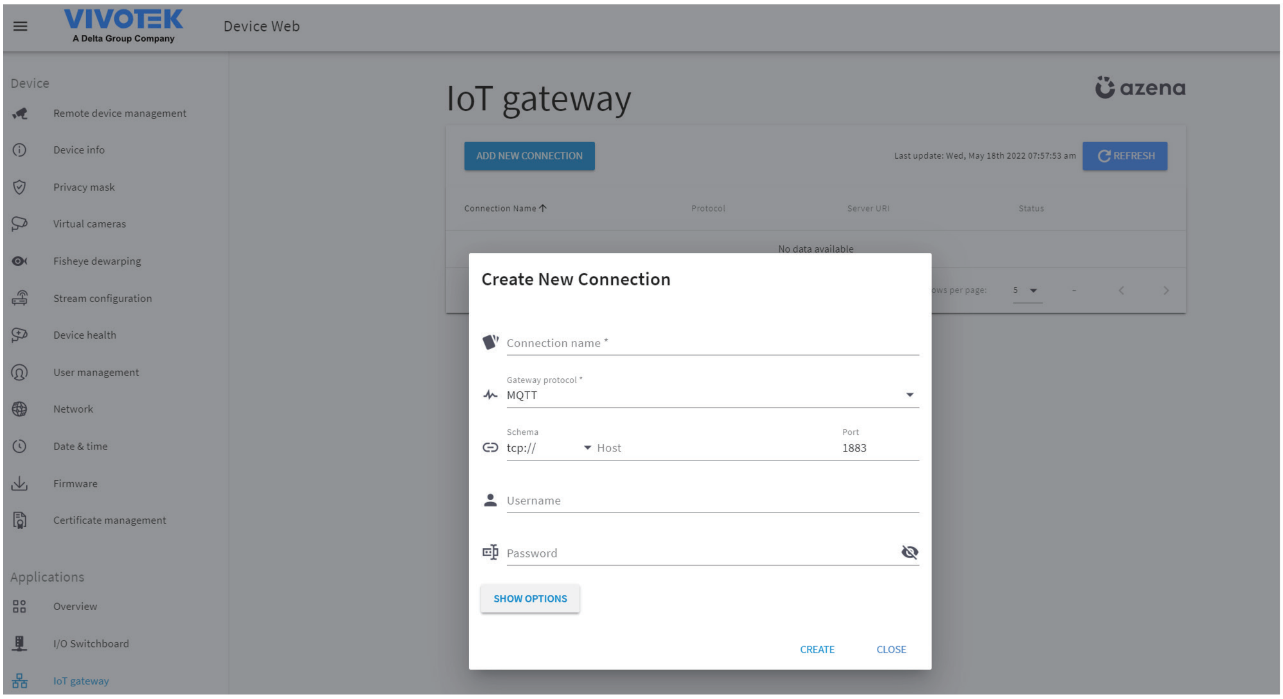
This page is used for connecting to a specific MQTT broker through a TCP connection.

MQTT allows for messaging between a deevvice to cloud and cloud to device. The connection can also be with an external MQTT client.

Type a Connection Name, choose MQTT as the gateway protocol, choose a schema (TCP or SSL), input the server URL and a port number.

If you set the schema to SSL, then you must upload the CA certi cate of the MQTT broker to the camera Ashttps://docs.azena.com/developer/core_topics/os_components/iot_gateway/mqttsoon as you select 'ssl' an extra option will appear in the window with which the camera. As soon as you select 'ssl', an extra option will appear in the window with which you can do this.

Next, set a user name and password if your MQTT broker requires one, otherwise leave it blank.



IoT gateway

Last update: Wed, May 18th 2022 07:57:53 am

Connection Name ↑	Protocol	Server URI	Status
No data available			

ows per page: 5 –

Create New Connection

Connection name *

Gateway protocol *
MQTT

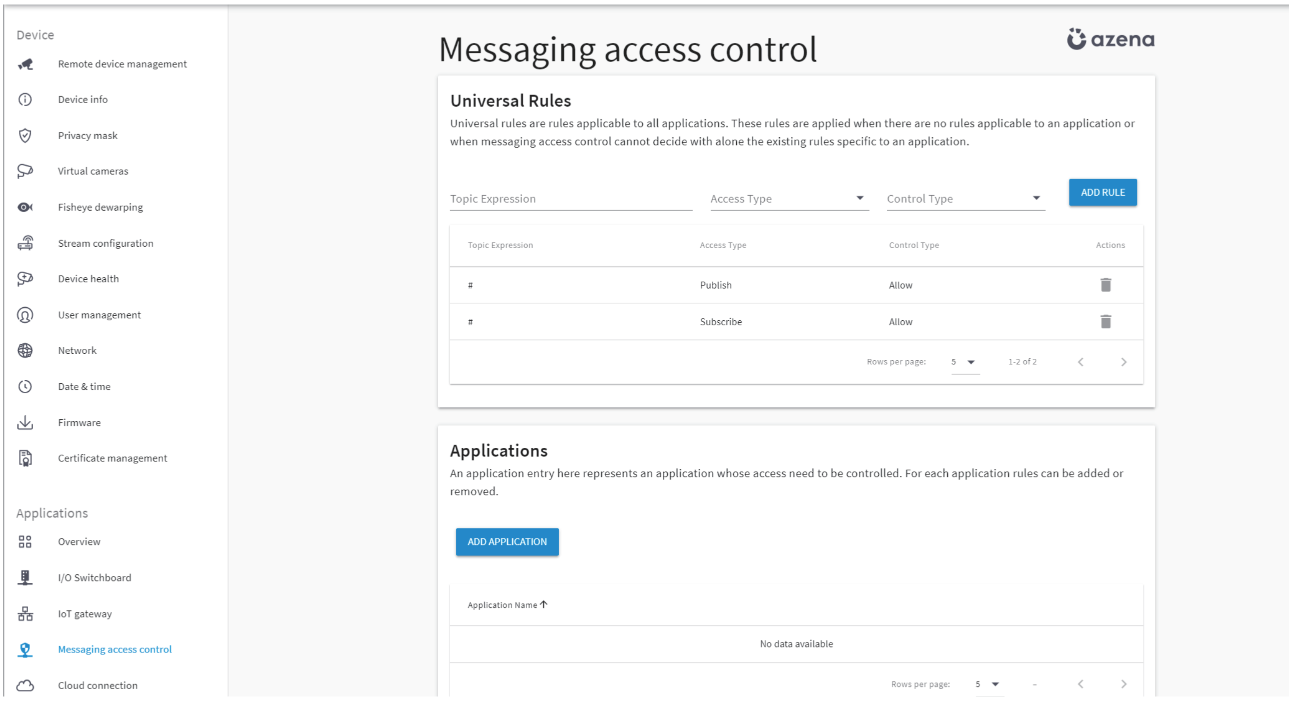
Schema: tcp:// Host Port: 1883

Username

Password

Messaging access control

From this page, you can create messaging rules for applications that do not have applicable rules.



Messaging access control

Universal Rules

Universal rules are rules applicable to all applications. These rules are applied when there are no rules applicable to an application or when messaging access control cannot decide with alone the existing rules specific to an application.

Topic Expression	Access Type	Control Type	Actions
#	Publish	Allow	🗑
#	Subscribe	Allow	🗑

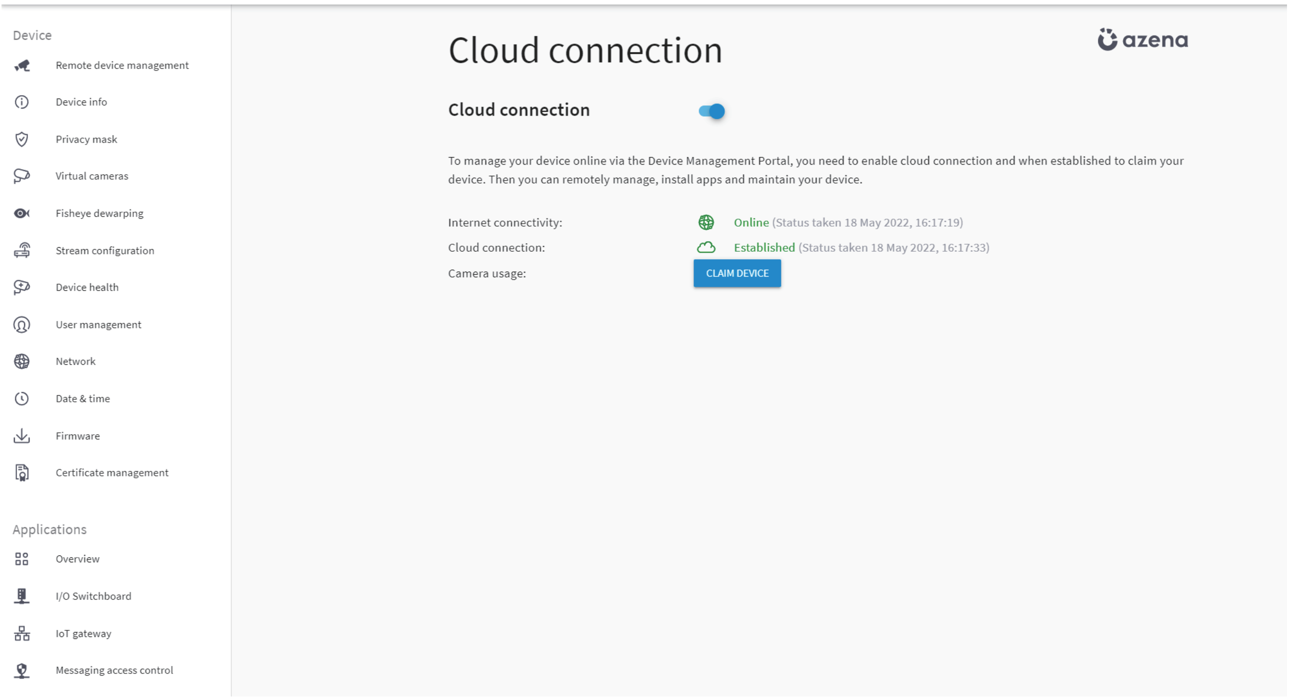
Applications

An application entry here represents an application whose access need to be controlled. For each application rules can be added or removed.

Application Name ↑
No data available

Applications - Cloud Connection

You can connect your device to the Azena cloud where you can install and manage the applications, buy additional licenses and monitor your camera's health. Also, if crash reporting is enabled, all the information about application crashes is sent to the cloud where it can be easily retrieved.



Cloud connection

Cloud connection

To manage your device online via the Device Management Portal, you need to enable cloud connection and when established to claim your device. Then you can remotely manage, install apps and maintain your device.

Internet connectivity: Online (Status taken 18 May 2022, 16:17:19)

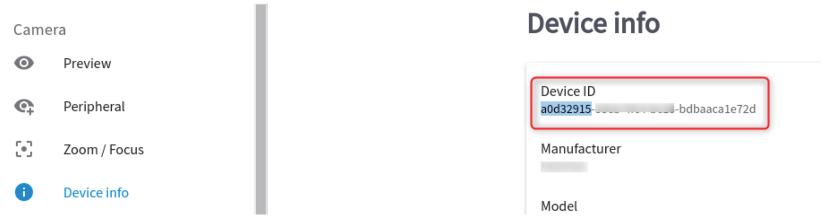
Cloud connection: Established (Status taken 18 May 2022, 16:17:33)

Camera usage:

In order to be able to install applications through the Device Management Portal, the camera has to be connected to the Azena cloud. That process is called claiming.

The prerequisites for connecting the camera to the cloud are:

- You have an account on the Azena Device Management Portal.
- Cameras have a non-restricted access to the Internet.
- Your camera has a valid certificate. Please verify this by accessing the camera using a web browser and go to the Device info page. Then check if a Device ID is present:



Device info

Device ID
a0d32915-[redacted]-bdbaaca1e72d

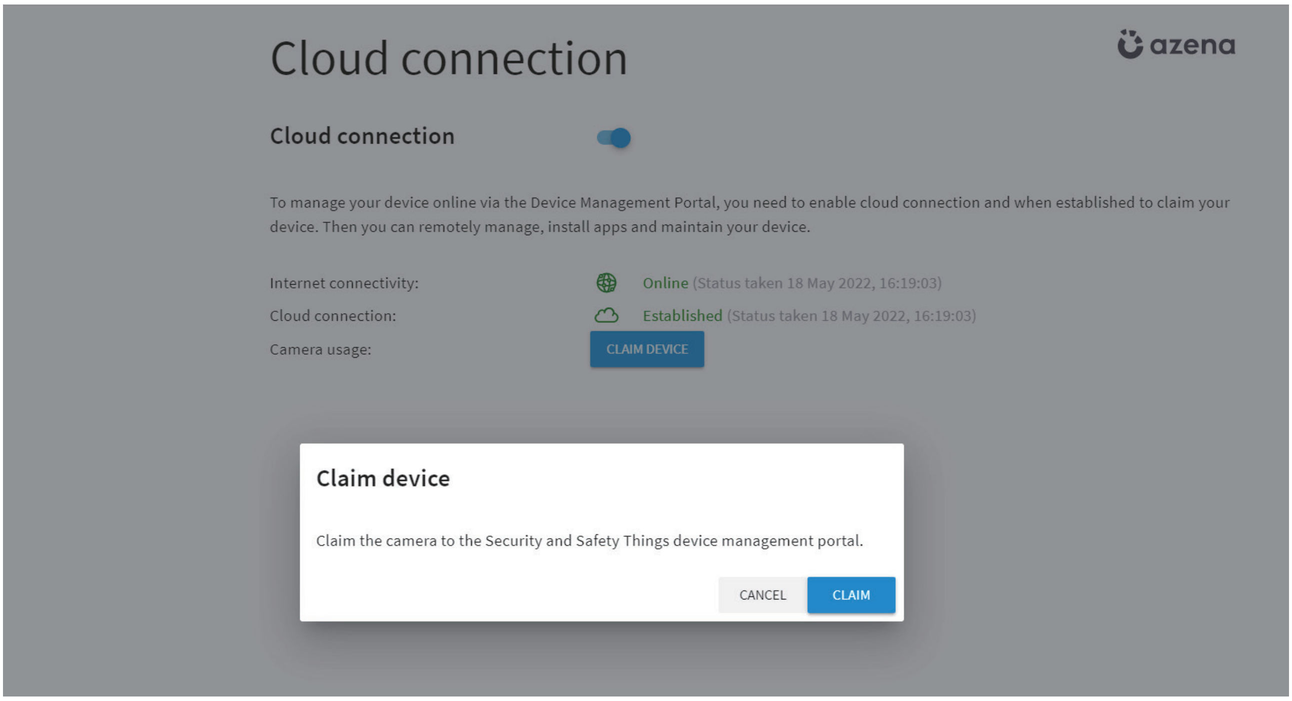
Manufacturer
[redacted]

Model

- Your device has a proper date/time set. This can be verified and set on the Date & time page on the camera's front end.

Proceed with the following for connecting the camera to the Device Management Portal:

1. Go to the Date & time option on camera's web console and enable "Use network-provided time". If necessary, please configure your own NTP server
2. Go to Cloud connection option and enable "cloud based device management". A pop-up will appear with a message. Click Continue.
3. Click on "CLAIM DEVICE."



Cloud connection

Cloud connection

To manage your device online via the Device Management Portal, you need to enable cloud connection and when established to claim your device. Then you can remotely manage, install apps and maintain your device.

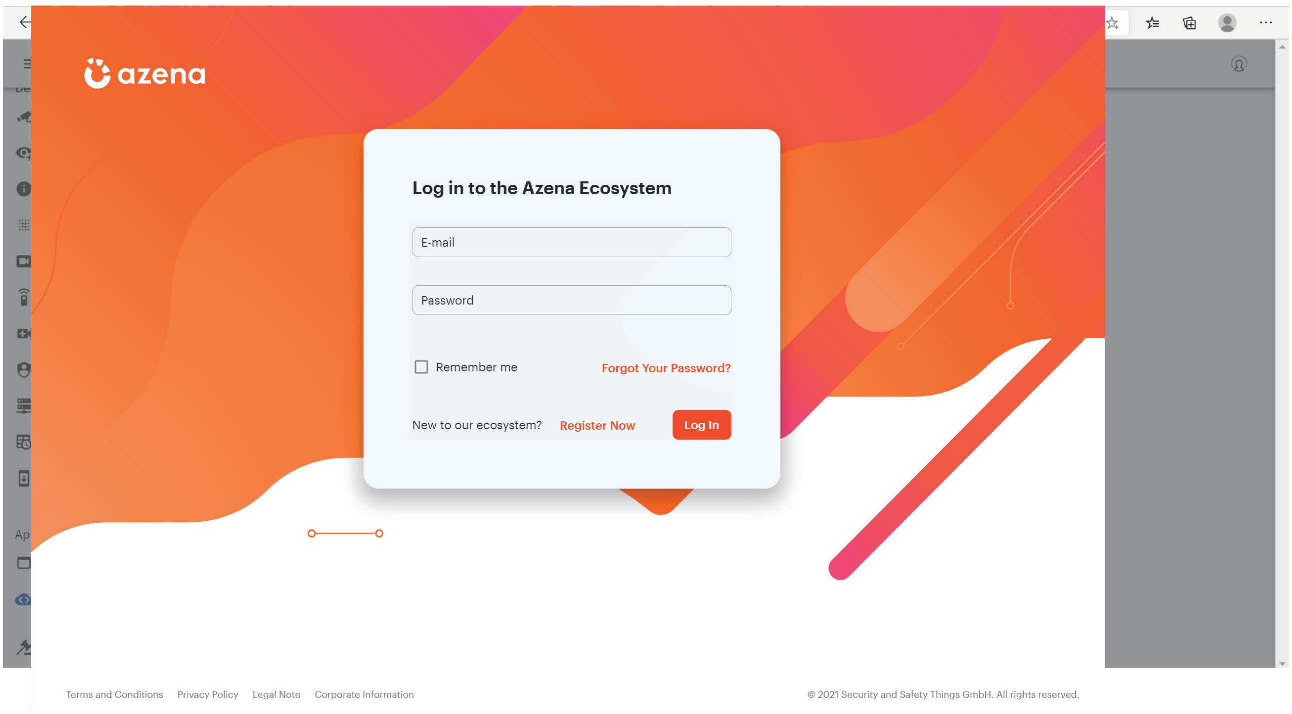
Internet connectivity: Online (Status taken 18 May 2022, 16:19:03)
Cloud connection: Established (Status taken 18 May 2022, 16:19:03)
Camera usage: CLAIM DEVICE

Claim device

Claim the camera to the Security and Safety Things device management portal.

Clicking the CLAIM button will redirect you to the Device Management Portal page where you can enter some additional information regarding this camera:

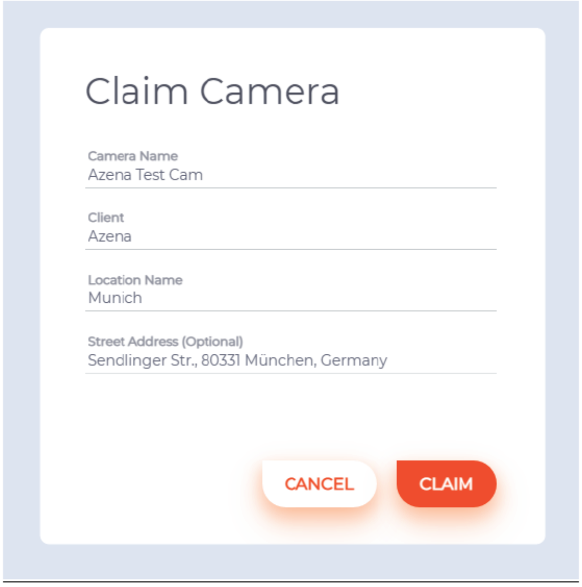
Click Continue.



On the Device Management Portal page, you can enter some additional information regarding the device:

- Camera name
- Client
- Location name
- Street address (optional)

Click the SAVE button in order to save the changes and your camera will appear in the list of cameras on the Device Management Portal.



Claim Camera

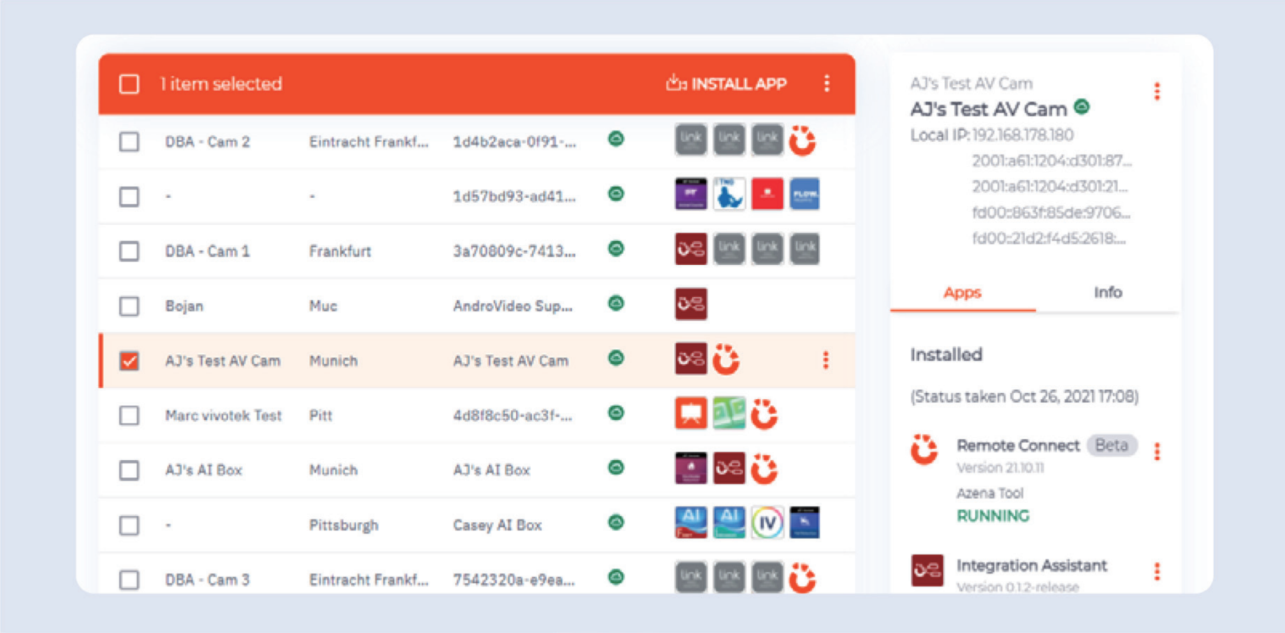
Camera Name
Azena Test Cam

Client
Azena

Location Name
Munich

Street Address (Optional)
Sendlinger Str., 80331 München, Germany

On the Device Management Portal page, you can see all connected devices/cameras.



☐ 1 item selected — INSTALL APP ⋮

☐	DBA - Cam 2	Eintracht Frankf...	1d4b2aca-0f91-...	●
☐	-	-	1d57bd93-ad41...	●
☐	DBA - Cam 1	Frankfurt	3a70809c-7413...	●
☐	Bojan	Muc	AndroVideo Sup...	●
☑	AJ's Test AV Cam	Munich	AJ's Test AV Cam	●
☐	Marc vivotek Test	Pitt	4d8f8c50-ac3f-...	●
☐	AJ's AI Box	Munich	AJ's AI Box	●
☐	-	Pittsburgh	Casey AI Box	●
☐	DBA - Cam 3	Eintracht Frankf...	7542320a-e9ea...	●

AJ's Test AV Cam
AJ's Test AV Cam ●
Local IP: 192.168.178.180
2001:a61:1204:d301:87...
2001:a61:1204:d301:21...
fd00::863f:85de:9706...
fd00::21d2:f4d5:2618:...

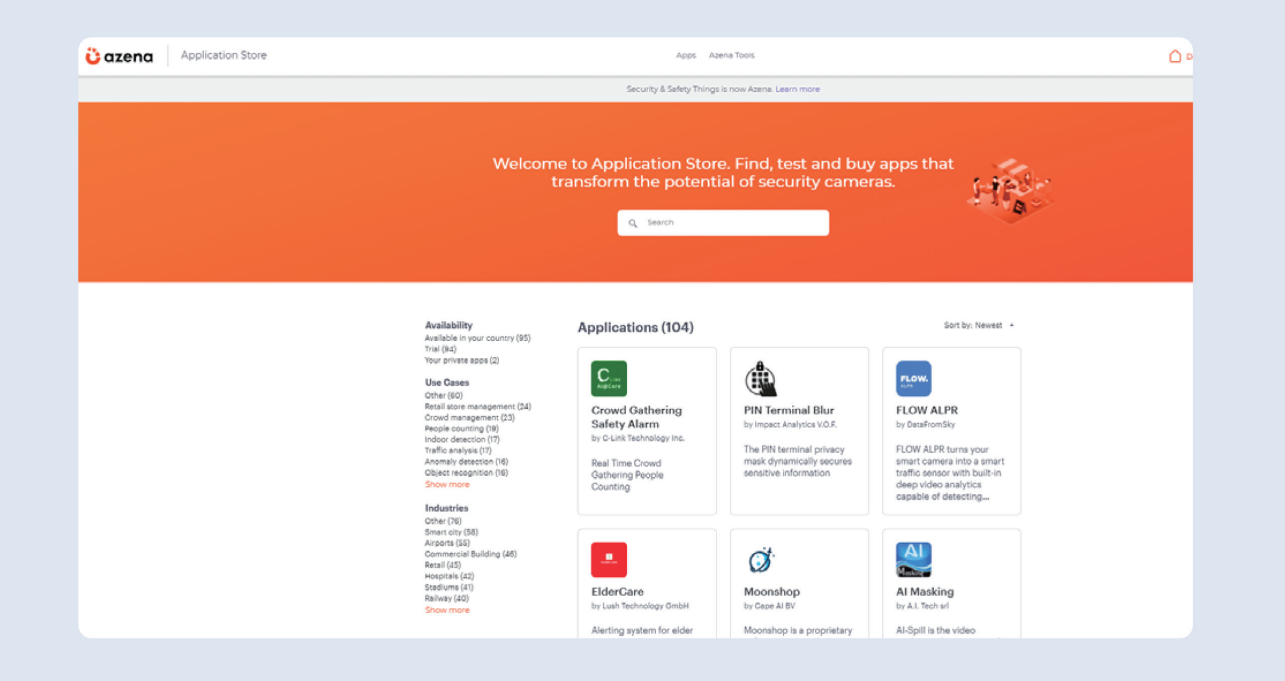
Installed

(Status taken Oct 26, 2021 17:08)

Remote Connect Beta
Version 21.10.11
Azena Tool
RUNNING

Integration Assistant
Version 0.1.2-release

Click to select your device. On the right pane, click INSTALL APP.



Security & Safety Things is now Azena. Learn more

Welcome to Application Store. Find, test and buy apps that transform the potential of security cameras.

Availability
Available in your country (95)
Trial (94)
Your private apps (2)

Use Cases
Other (60)
Retail store management (24)
Crowd management (23)
People counting (19)
Indoor detection (17)
Traffic analysis (17)
Anomaly detection (16)
Object recognition (16)
Show more

Industries
Other (76)
Smart city (58)
Airports (55)
Commercial Building (46)
Retail (45)
Hospitals (42)
Stadiums (41)
Railway (40)
Show more

Applications (104)

Sort by: Newest

Crowd Gathering Safety Alarm
by C-Link Technology Inc.
Real Time Crowd Gathering People Counting

PIN Terminal Blur
by Impact Analytics V.O.F.
The PIN terminal privacy mask dynamically secures sensitive information

FLOW ALPR
by DataFromSky
FLOW ALPR turns your smart camera into a smart traffic sensor with built-in deep video analytics capable of detecting...

ElderCare
by Lush Technology GmbH
Alerting system for elder

Moonshop
by Cape AI BV
Moonshop is a proprietary

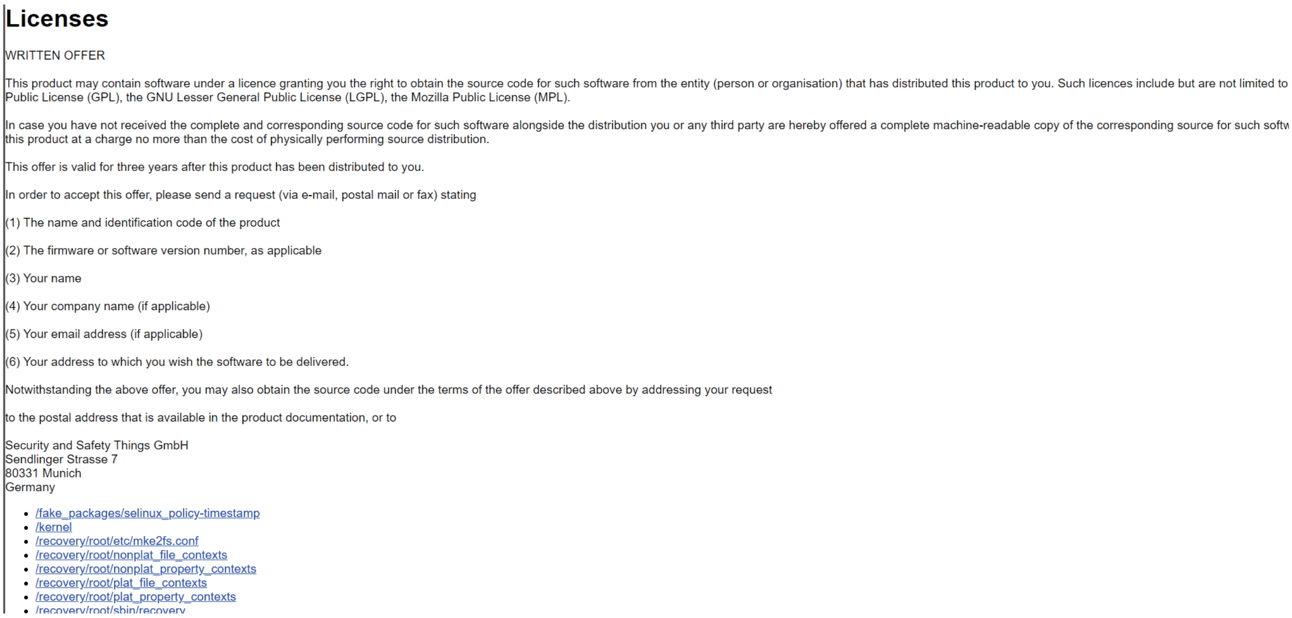
AI Masking
by A.I. Tech srl
AI-Spill is the video

Scroll to select an app. Select and click INSTALL.

You can find apps by either typing into the search bar or navigating on the left side panel. There you will find tailored solutions divided by use cases, such as retail store management, crowd management and COVID-19.

Applications - Legal

This page provides legal information for the OS.



Licenses

WRITTEN OFFER

This product may contain software under a licence granting you the right to obtain the source code for such software from the entity (person or organisation) that has distributed this product to you. Such licences include but are not limited to
Public License (GPL), the GNU Lesser General Public License (LGPL), the Mozilla Public License (MPL).

In case you have not received the complete and corresponding source code for such software alongside the distribution you or any third party are hereby offered a complete machine-readable copy of the corresponding source for such softw
this product at a charge no more than the cost of physically performing source distribution.

This offer is valid for three years after this product has been distributed to you.

In order to accept this offer, please send a request (via e-mail, postal mail or fax) stating

(1) The name and identification code of the product

(2) The firmware or software version number, as applicable

(3) Your name

(4) Your company name (if applicable)

(5) Your email address (if applicable)

(6) Your address to which you wish the software to be delivered.

Notwithstanding the above offer, you may also obtain the source code under the terms of the offer described above by addressing your request

to the postal address that is available in the product documentation, or to

Security and Safety Things GmbH
Sendlinger Strasse 7
80331 Munich
Germany

- /fake_packages/selinux_policy-timestamp
- /kernel
- /recovery/root/etc/mke2fs.conf
- /recovery/root/nonplat_file_contexts
- /recovery/root/nonplat_property_contexts
- /recovery/root/plat_file_contexts
- /recovery/root/plat_property_contexts
- /recovery/root/sbin/recovery

Technology License Notice

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

HEVCAdvance™
Covered by Patents at patentlist.hevcadvance.com

Notices from HEVC Advance:

THIS PRODUCT IS SOLD WITH A LIMITED LICENSE AND IS AUTHORIZED TO BE USED ONLY IN CONNECTION WITH HEVC CONTENT THAT MEETS EACH OF THE THREE FOLLOWING QUALIFICATIONS: (1) HEVC CONTENT ONLY FOR PERSONAL USE; (2) HEVC CONTENT THAT IS NOT OFFERED FOR SALE; AND (3) HEVC CONTENT THAT IS CREATED BY THE OWNER OF THE PRODUCT. THIS PRODUCT MAY NOT BE USED IN CONNECTION WITH HEVC ENCODED CONTENT CREATED BY A THIRD PARTY, WHICH THE USER HAS ORDERED OR PURCHASED FROM A THIRD PARTY, UNLESS THE USER IS SEPARATELY GRANTED RIGHTS TO USE THE PRODUCT WITH SUCH CONTENT BY A LICENSED SELLER OF THE CONTENT. YOUR USE OF THIS PRODUCT IN CONNECTION WITH HEVC ENCODED CONTENT IS DEEMED ACCEPTANCE OF THE LIMITED AUTHORITY TO USE AS NOTED ABOVE.

H.264

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

■ Reorient or relocate the receiving antenna.

■ Increase the separation between the equipment and receiver.

■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

■ Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準にづくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.