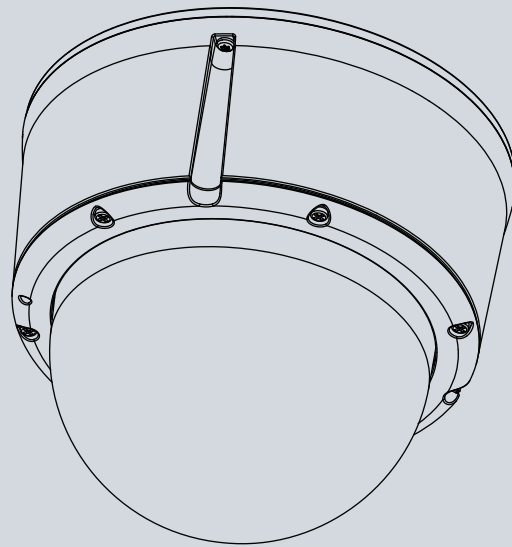




FD9392-EHTV-0 Network Camera User's Manual

Qualcomm QCS603 SoC with Built-in AI Engine • Video Processing and Machine Learning •
Supports VCA Solutions via Installation of S&ST APPs •



Rev. 1.0

Table of Contents

Revision History	4
Read Before Use.....	4
Symbols and Statements in this Document.....	4
Package Contents	5
Physical Description	6
Hardware Installation.....	7
Configuration	16
Preview.....	24
Peripheral	24
Zoom / Focus	25
Device Info	26
Privacy Mask	27
Virtual Camera	28
Video settings	28
Stream Configuration	29
Device Health	30
User Management.....	30
Network	31
Date & Time.....	31
Firmware	32
Applications - Overview	33
Data Magnet and VAST2.....	33
Applications - Cloud Connection	37
Applications - Legal	42
Technology License Notice.....	43
Electromagnetic Compatibility (EMC).....	44

Overview

- Powered by Qualcomm QCS603 SoC with a built-in AI Engine
- Powerful Computing for Video Processing and Machine Learning
- Driven by OSSA, running on S&ST OS
- Supports a variety of VCA solutions through S&ST APPs
- Remote Focus Lens / P-iris
- Built-in IR Illuminators up to 50 meters
- Digital input*1, Digital Output*1
- 8MP

Revision History

- Rev. 1.0: Initial release.

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 facilitate 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

- FD9392-EHTV-O
- T10 stardriver, desiccant bag, screws
- Waterproof Ethernet and I/O wires cable housing
- Quick Installation Guide & alignment sticker
- Side-routing bracket.



WARNING:

1. IR lights emit from this product.
2. Use appropriate shielding or eye protection.



NOTE:

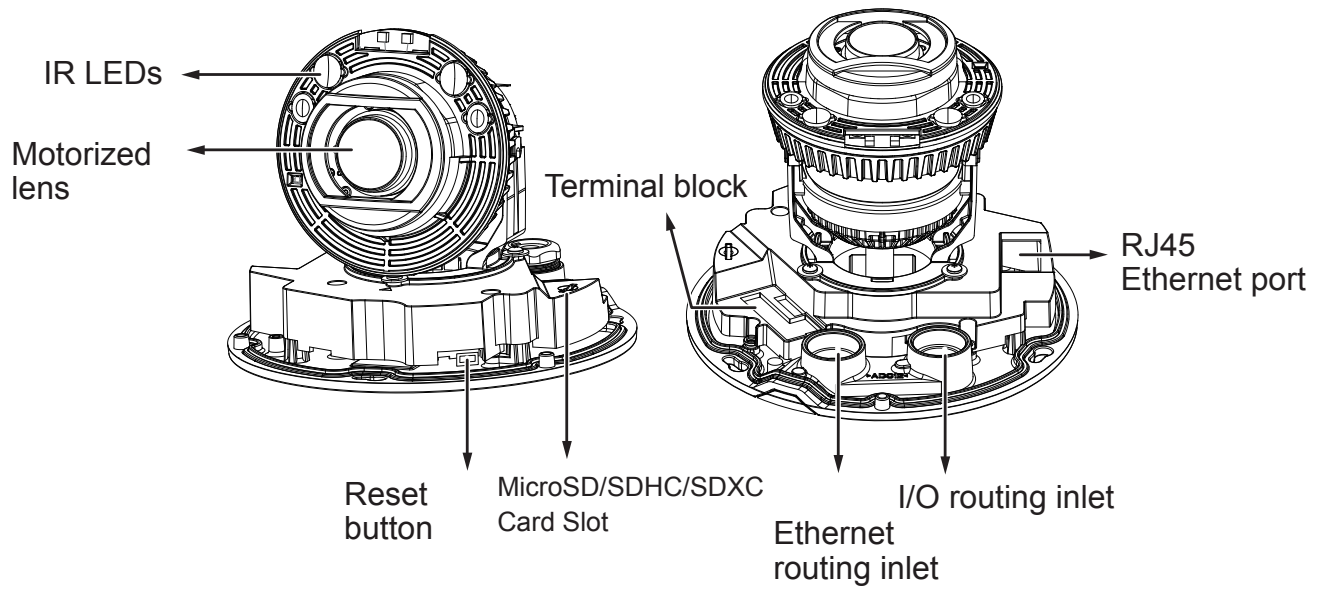
Use the camera only with a DC power supply that is UL listed, and limited power source (LPS) certified. The power supply should bear the UL listed and LPS marks. The power supply should also meet any safety and compliance requirements for the country of use.

REMARQUE :

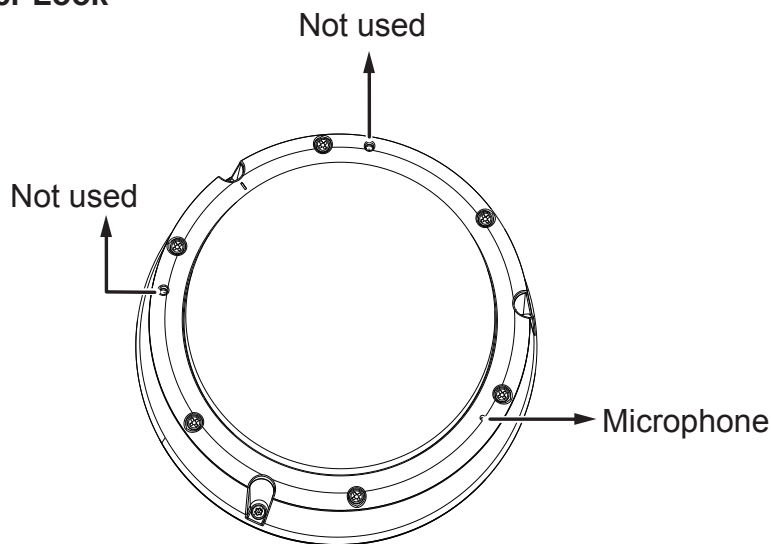
n'utilisez la caméra qu'avec un bloc d'alimentation CC homologué UL, ainsi qu'avec une alimentation limitée (LPS) certifiée. Le bloc d'alimentation doit porter les indications d'homologation UL et LPS. Il doit également répondre aux exigences en matière de sécurité et de conformité relatives au pays d'utilisation.

Physical Description

● Inner View



● Outer Look




 **NOTE:**

Some of the suffix syntax used in model naming are listed below:

E	w/ heater for extreme weather
Fx	Focal length w/ number
T	w/ Remote focus lens
R	w/ PoE repeater
H	w/ High Dynamic Range functionality

 **IMPORTANT:**

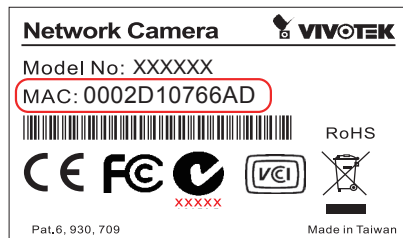
 The camera comes with an embedded heater and requires an 802.3at PoE switch.

Operating Consumption & Power Input Temperature	
≥-50°C	PoE: 24.3W (PoE Plus mid-span or switch, 42.5V-57V - 0.57A-0.43A); AC 24V input: 21.6W [1.76A (PF0.55)]; DC 12V: 21W (1.8A)

Hardware Installation

1. Jot down the camera's MAC address for later reference.

1

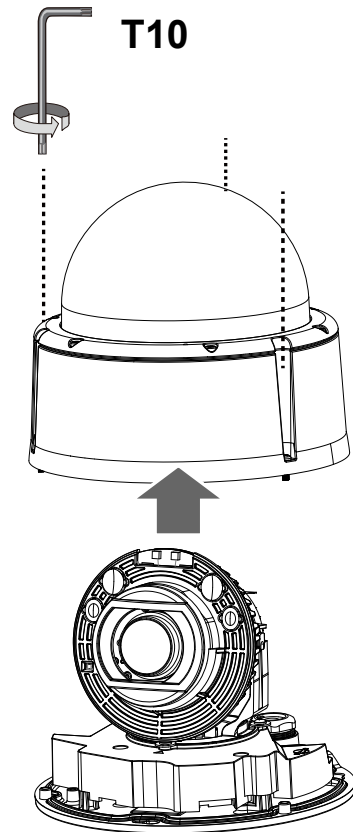
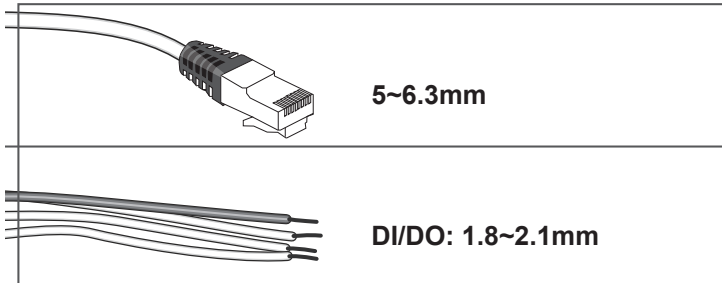


 **IMPORTANT:**

If DC power is preferred, it should comply with: O/P: 12VDC, 1A or 2A min., L.P.S. per IEC 60950-1.

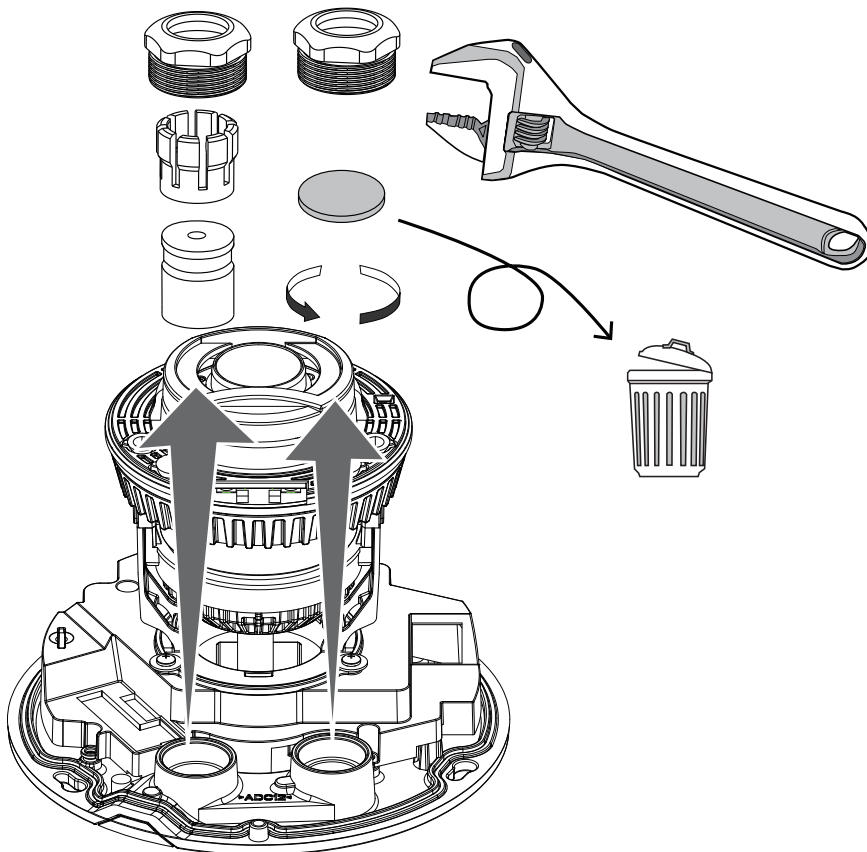
Si l'alimentation CC est préférable, elle devrait être conforme avec ce qui suit : Sortie : 12 VCC, 2 A min., alimentation limitée à conformité CEI 60950-1.

2. Use the included T10 star driver to remove the dome cover.

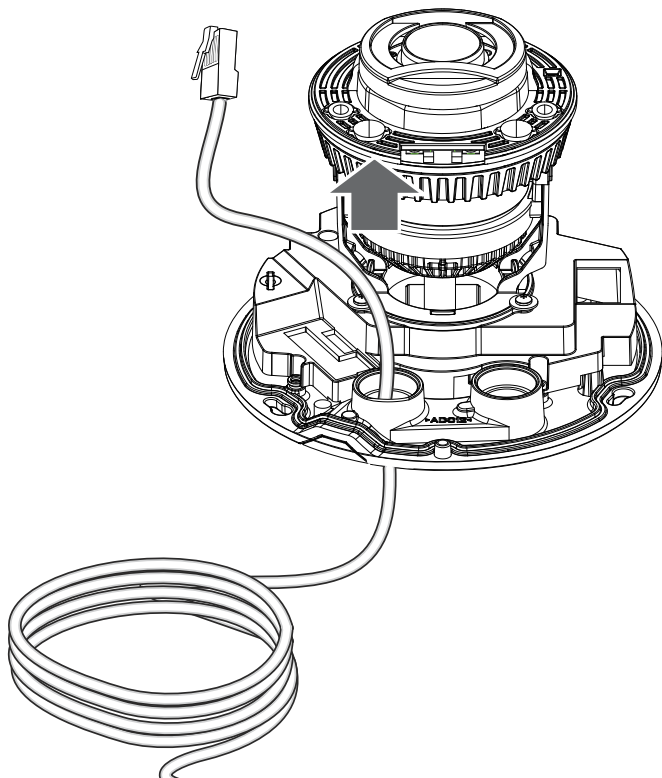


3. Loosen and remove the waterproof connectors.

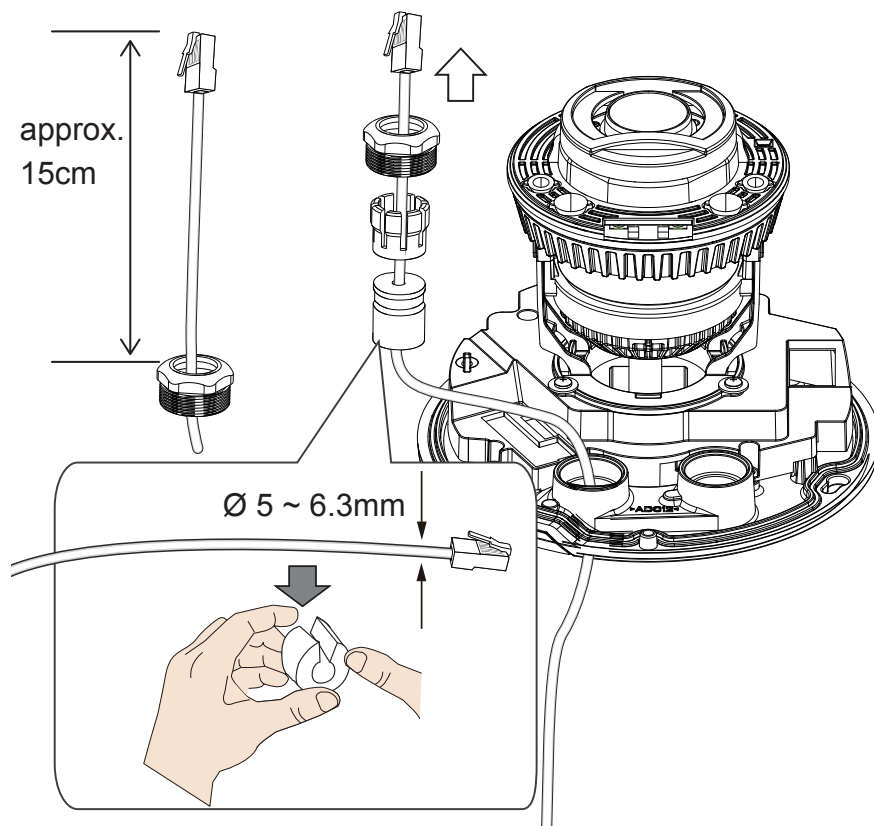
IMPORTANT: You should install the waterproof cable gland to the I/O routing inlet whether you connect the I/O and power wires or not. If you leave it open, water or moisture can destroy the camera.



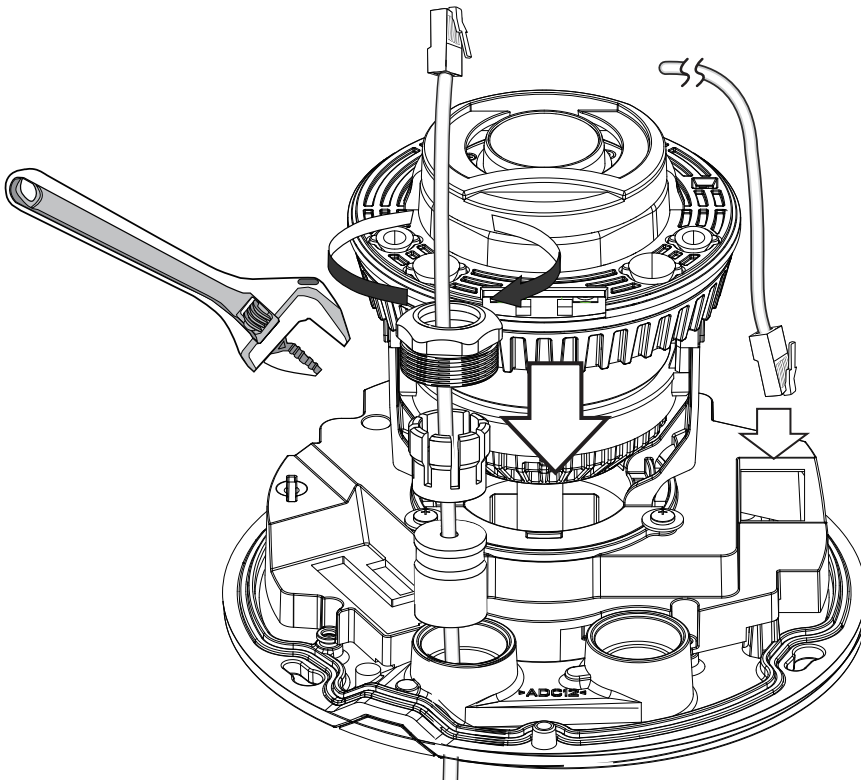
4. Insert an Ethernet cable through the cable gland, and the rubber seal.



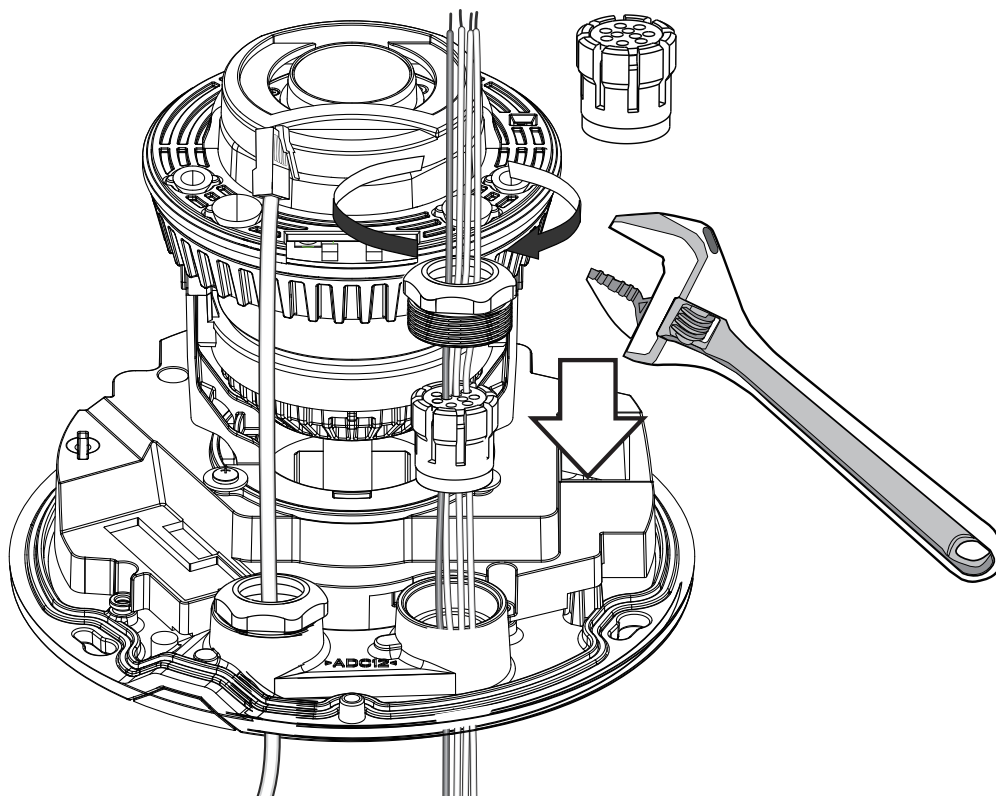
5. Insert the Ethernet cable through the components of the waterproof connector, e.g., the rubber seal. Leave 15cm of cable length inside, counting from the edge of the aluminum hex nut.



6. Use a crescent wrench to tighten the components of the waterproof connector. Connect the cable to the RJ45 connector.

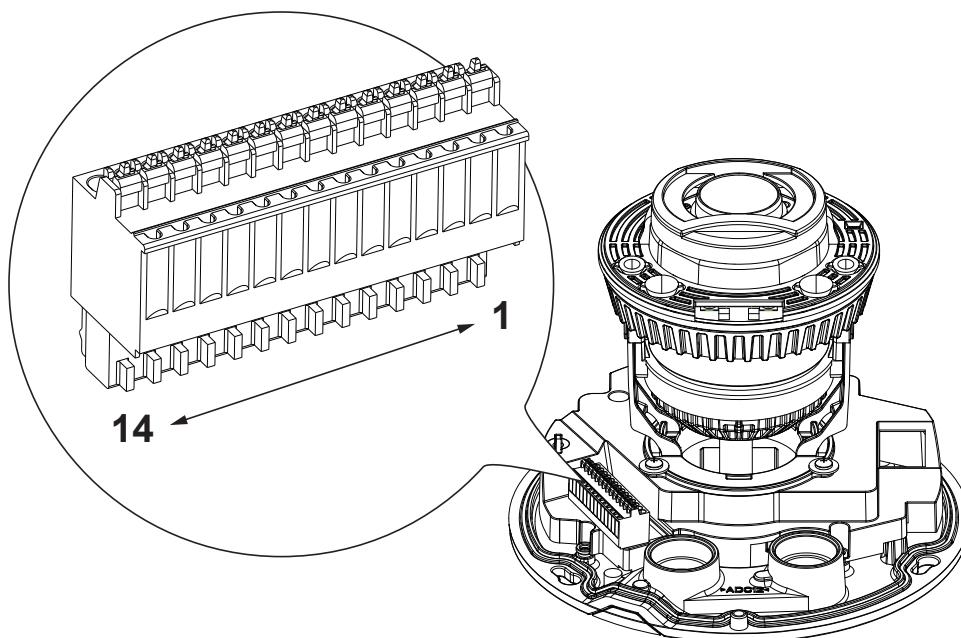


7. If preferred, pass power or I/O wires through the rubber seal and waterproof components of another connector. Install and tighten the components.



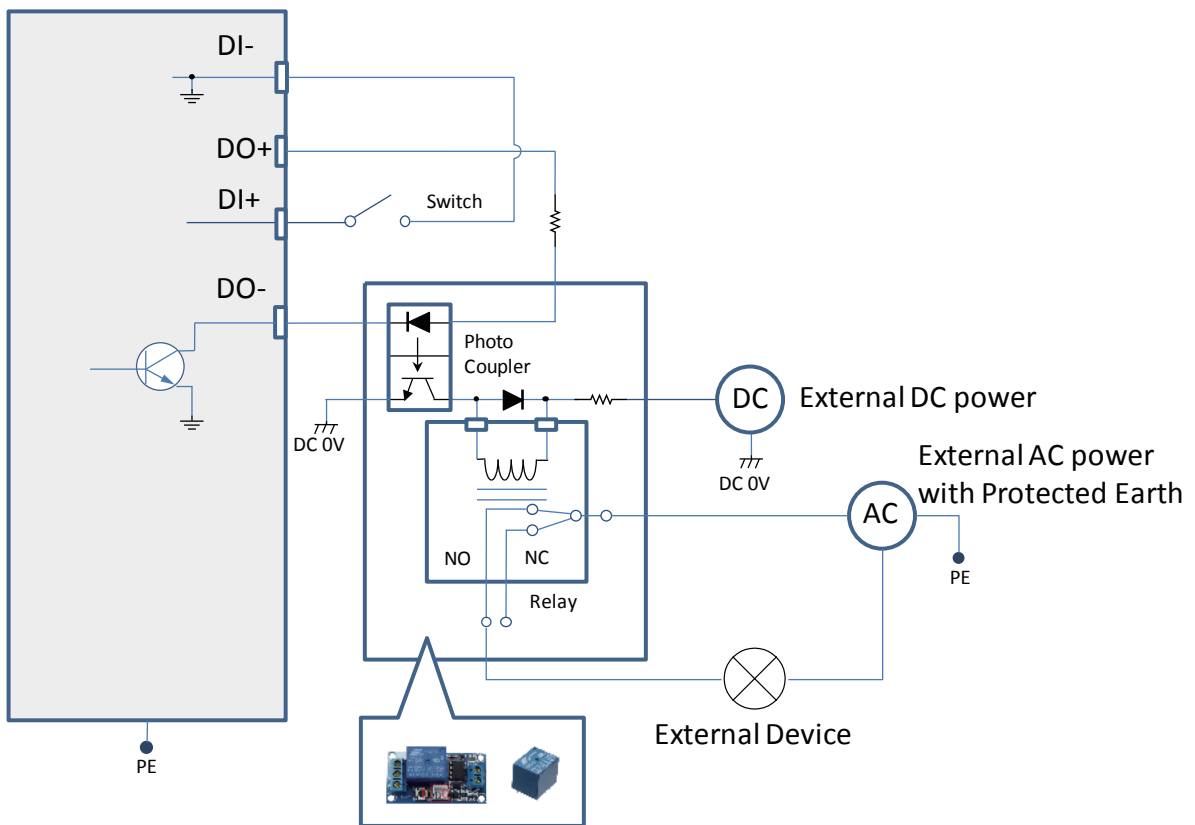
8. If applied, connect DI/DO wires, 12/24V DC power, or audio wires to the terminal block.

#	Name
1	AC 24V
2	AC 24V
3	DC 12V IN-
4	DC 12V IN+
5	DI- (GND)
6	GND
7	DI+ _0
8	GND
9	DO- _0
10	DO+ (5V)
11	MIC-IN_N (GND)
12	MIC-IN_P
13	AUDIO-OUT_N (GND)
14	AUDIO-OUT_P

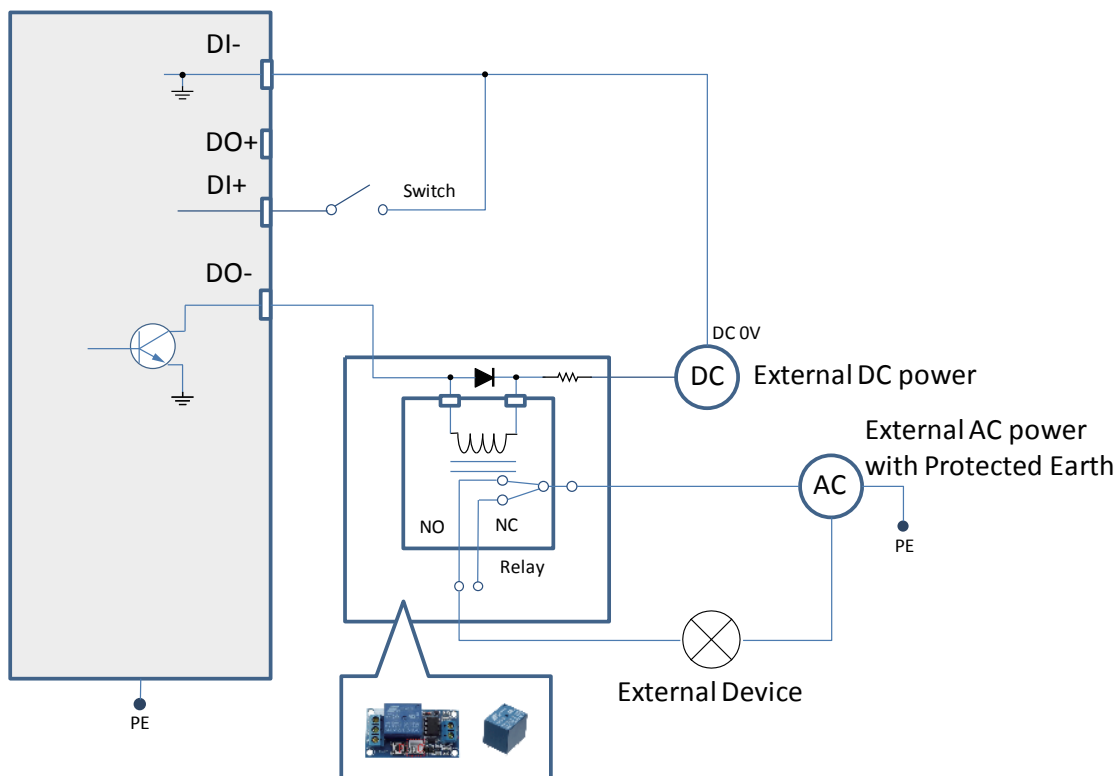


1. The DO+ pin provides a 12V output, and the max. load is 50mA.
2. The max. voltage for DO- pins is 30VDC (External power).
 In order to control AC devices, the following diagram can be taken into consideration. This diagram uses a relay to control the ON/OFF condition of the AC device.
3. An external relay can be triggered by using the DO+ or by an external power source, depending on the type of relay you use.
4. In case of using an individual relay (instead of using a relay module), for protection against voltage or current spikes, a transient voltage suppression diode must be connected in parallel with the inductive load.

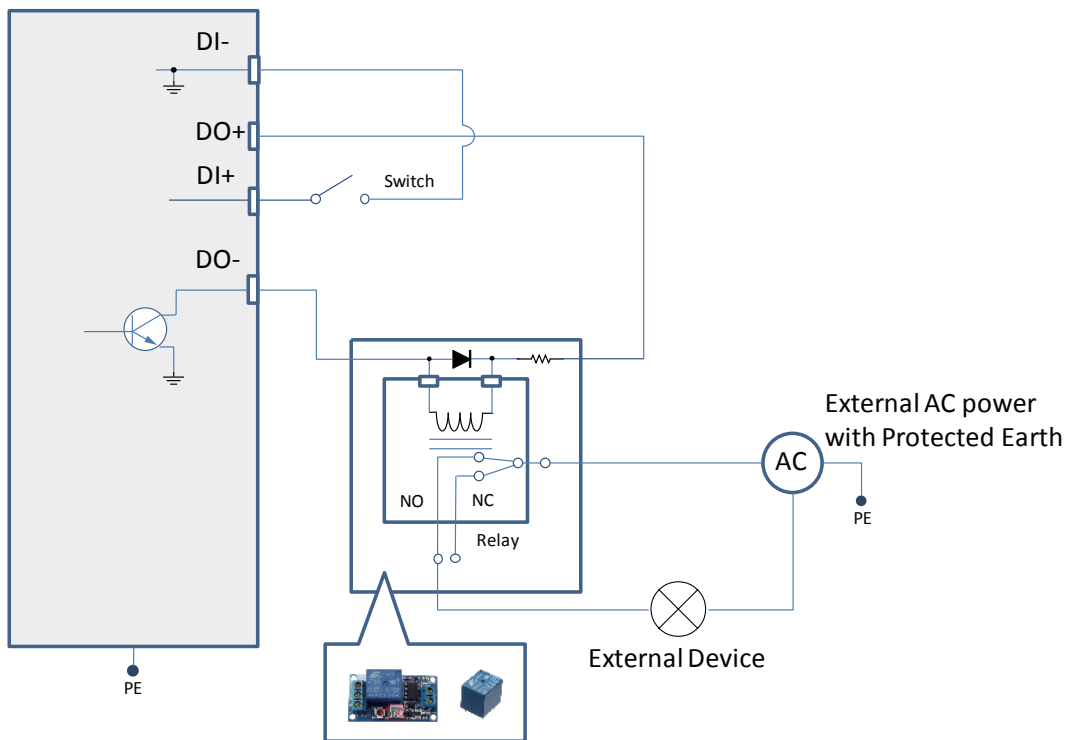
Dry contact with external DC power source to supply a relay. Dry contact is the safest connection to protect devices.



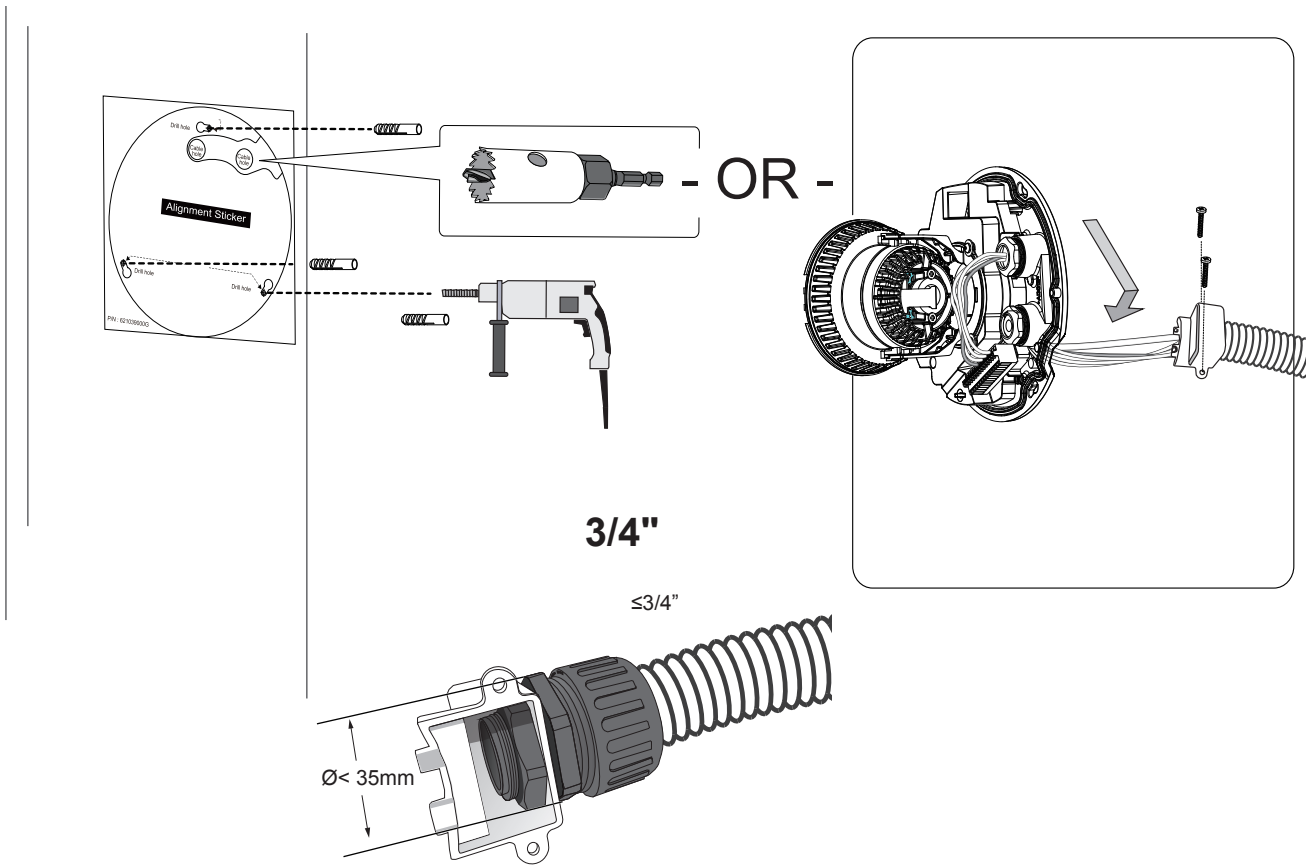
Wet contact with external DC power source to supply a relay.



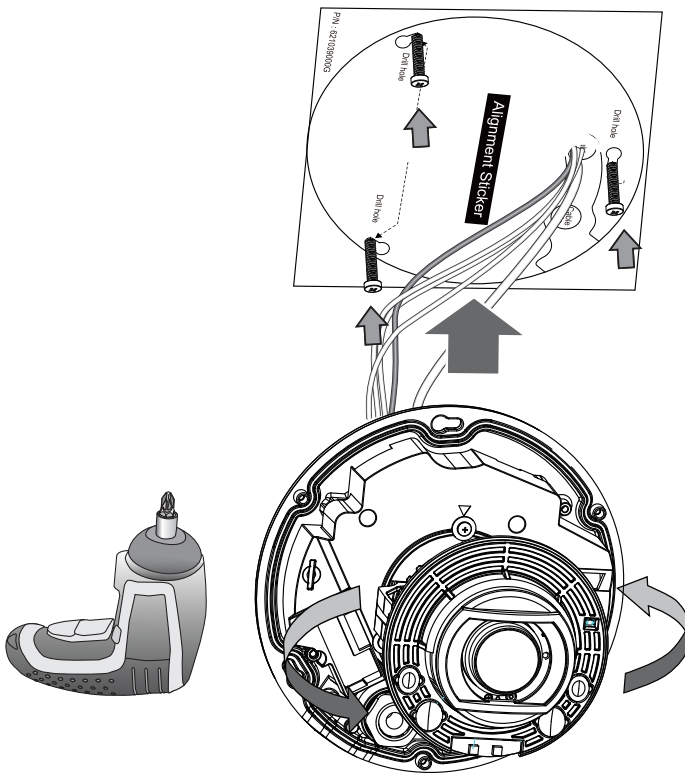
Dry contact and using camera's DO+ to supply a relay.



9. You can either route cables through a routing hole on the ceiling or wall, or you can route cables through the side of the camera. You can use the side-routing bracket to install a 3/4" conduit. Please note that the conduit hex nut should not be larger than 35mm.



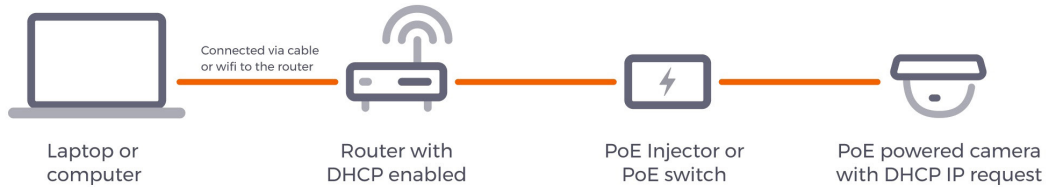
10. Attach the included alignment sticker to a preferred location. Drill holes for mounting screws and if preferred, drill one or two routing holes.



When fastening the screws, do not completely tighten the screws. Pass cables through the routing holes, and then mount the camera by passing the screw heads through the keyhole slots. Turn the camera counter-clock wise, and then fasten the screws.

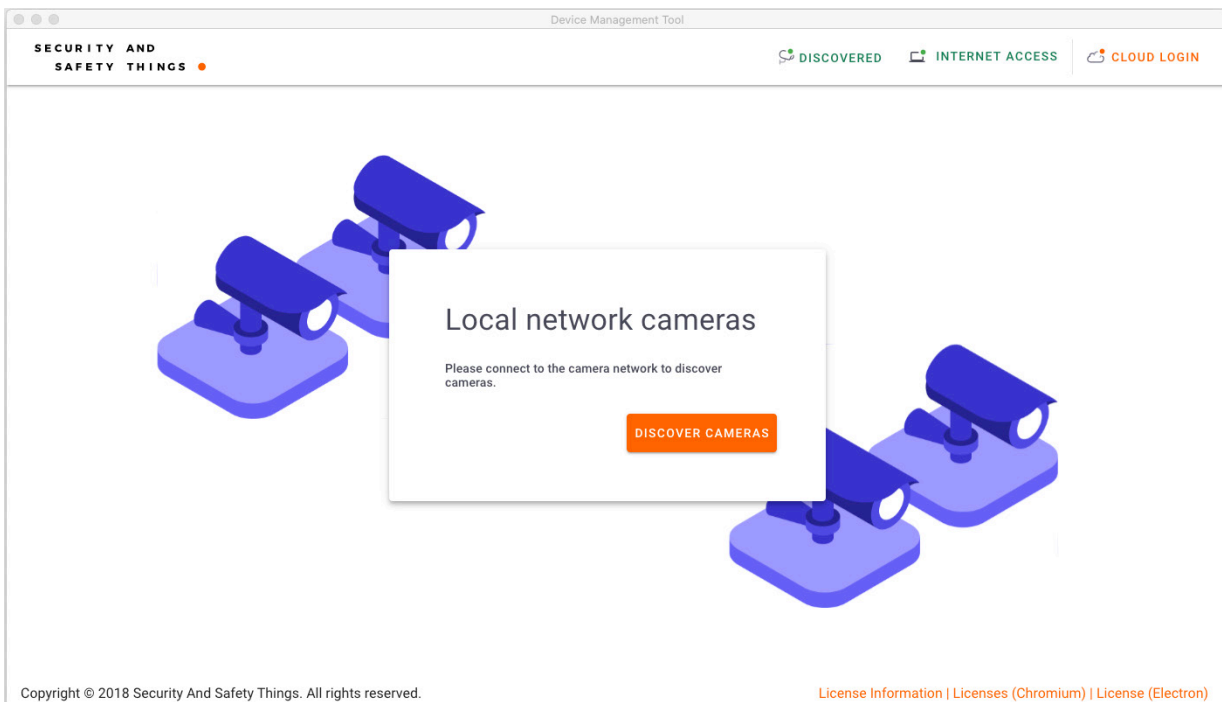
Configuration

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

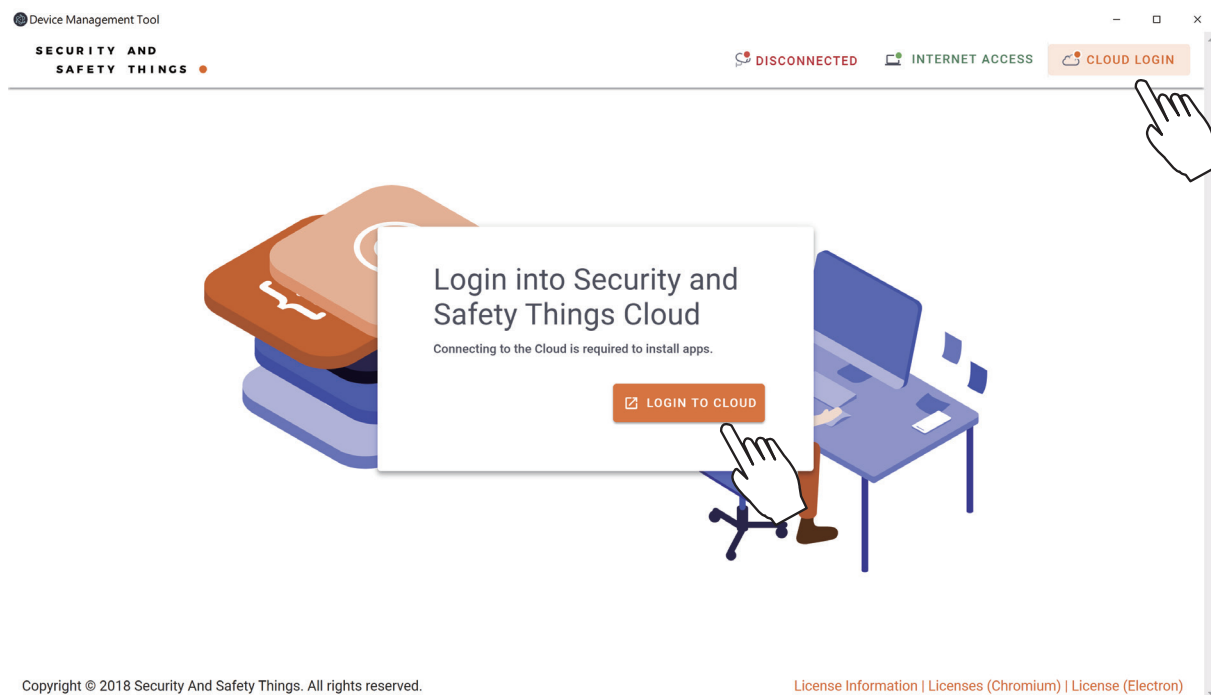


Make sure DHCP service is available in your local network.

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



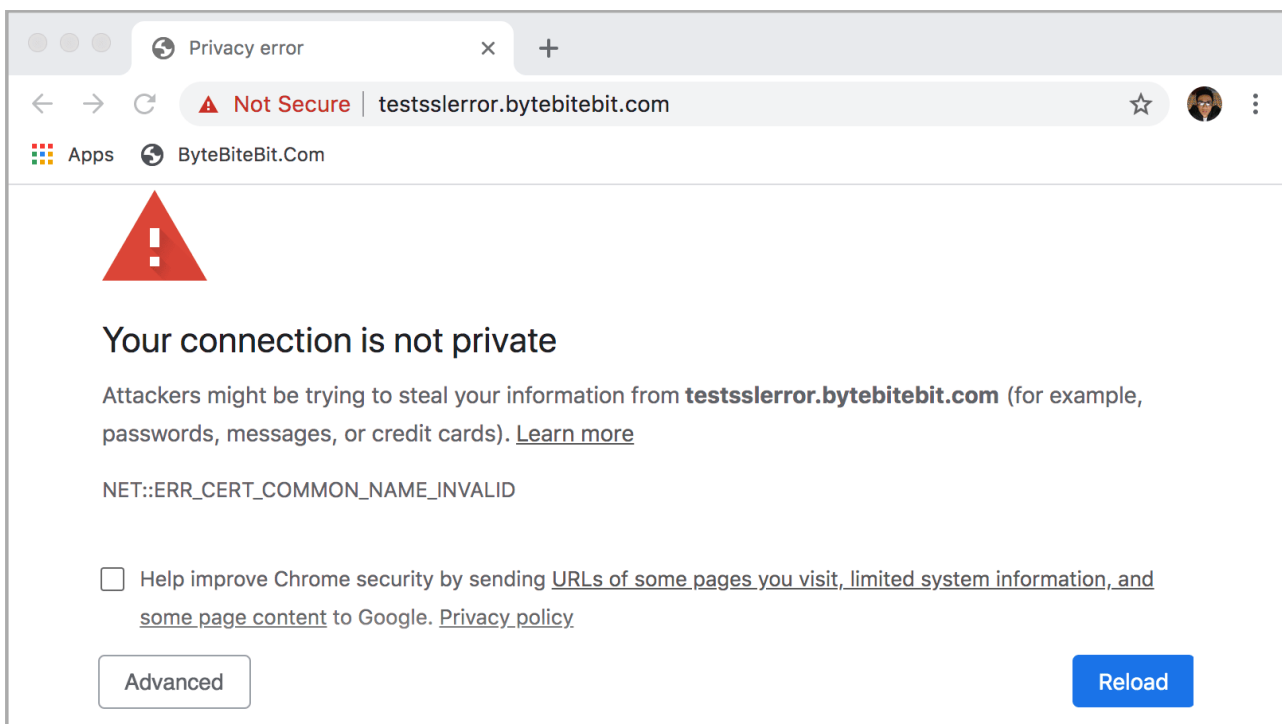
3. You can click Cloud Login to download S&ST apps or visit:
<https://store.securityandsafetythings.com/shop/catalog/c/main>



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

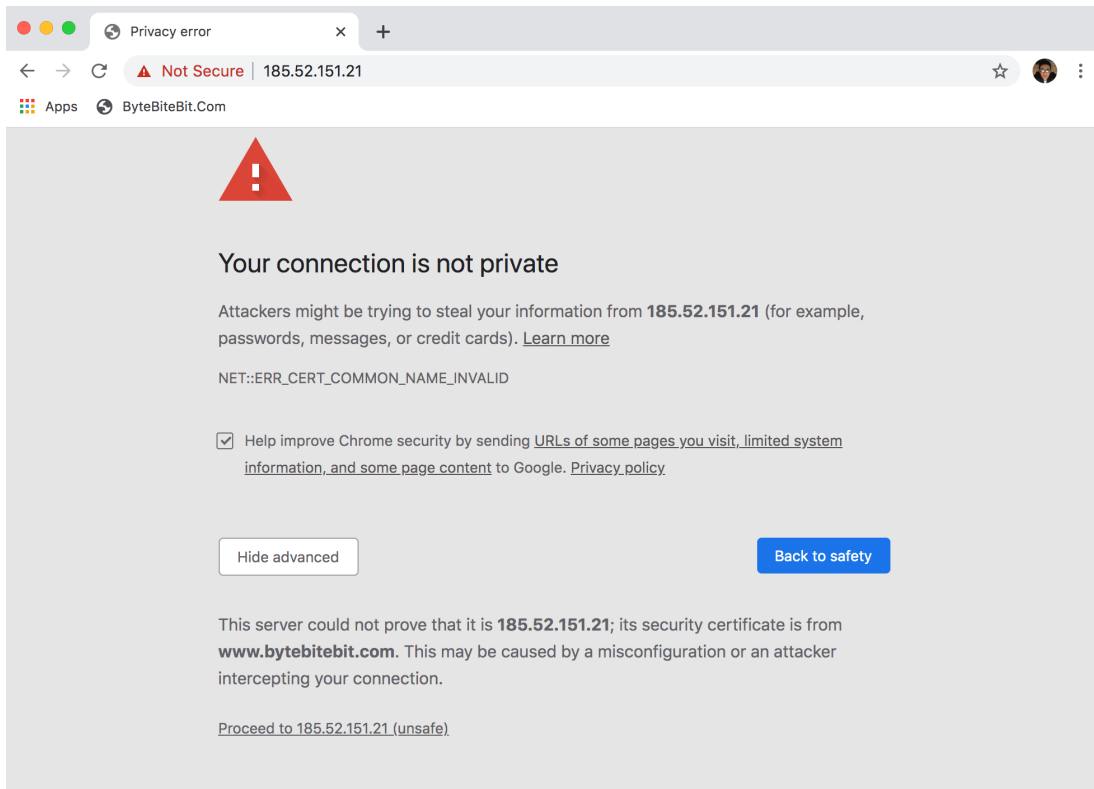
Enter [admin/admin](#) as the default credential.

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

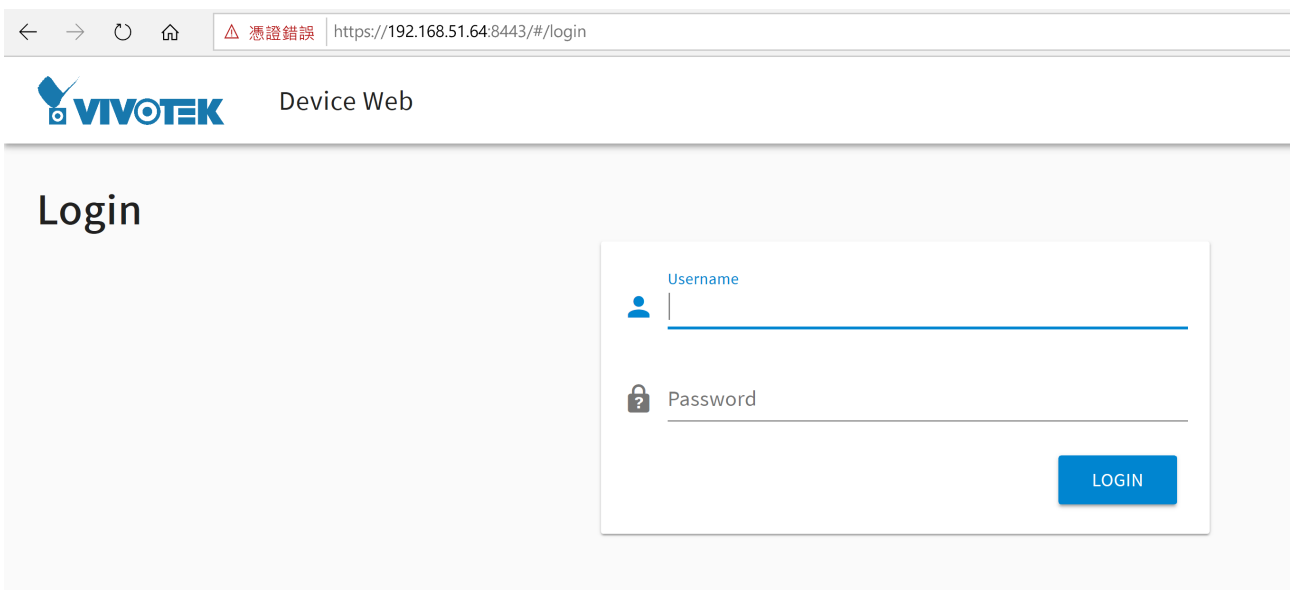


Click Proceed to [xxx.xxx.xxx.xxx \(Unsafe\)](#) to open the web console.

Note the IP addresses below are for reference only.

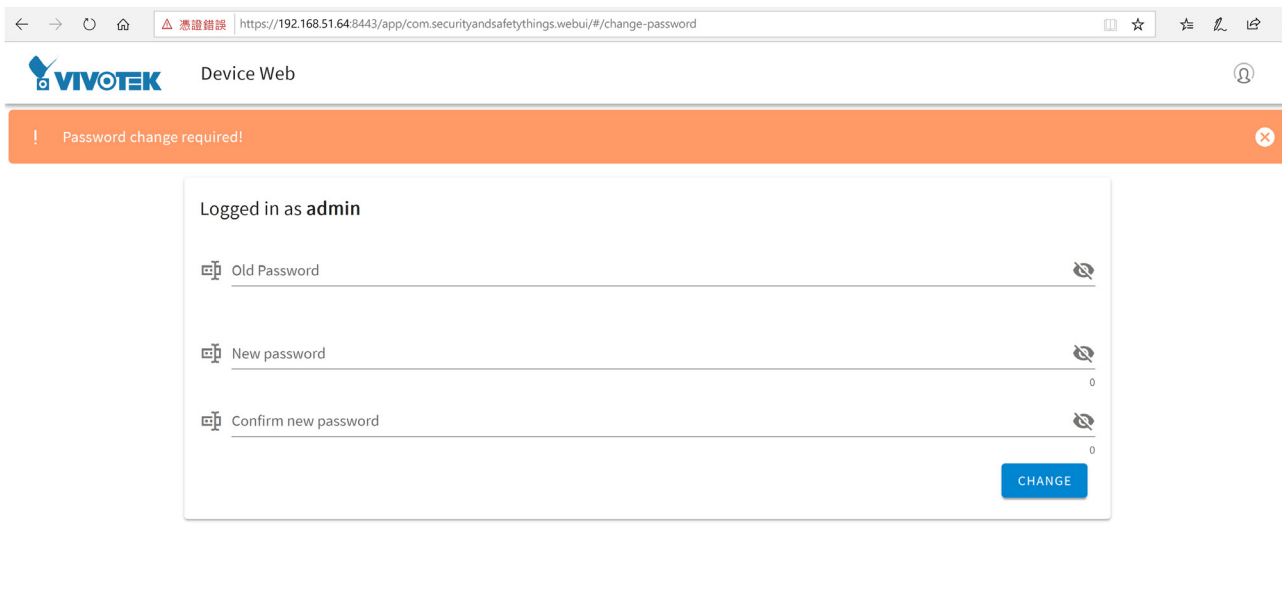


Enter **admin/admin** as the default credential.



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.

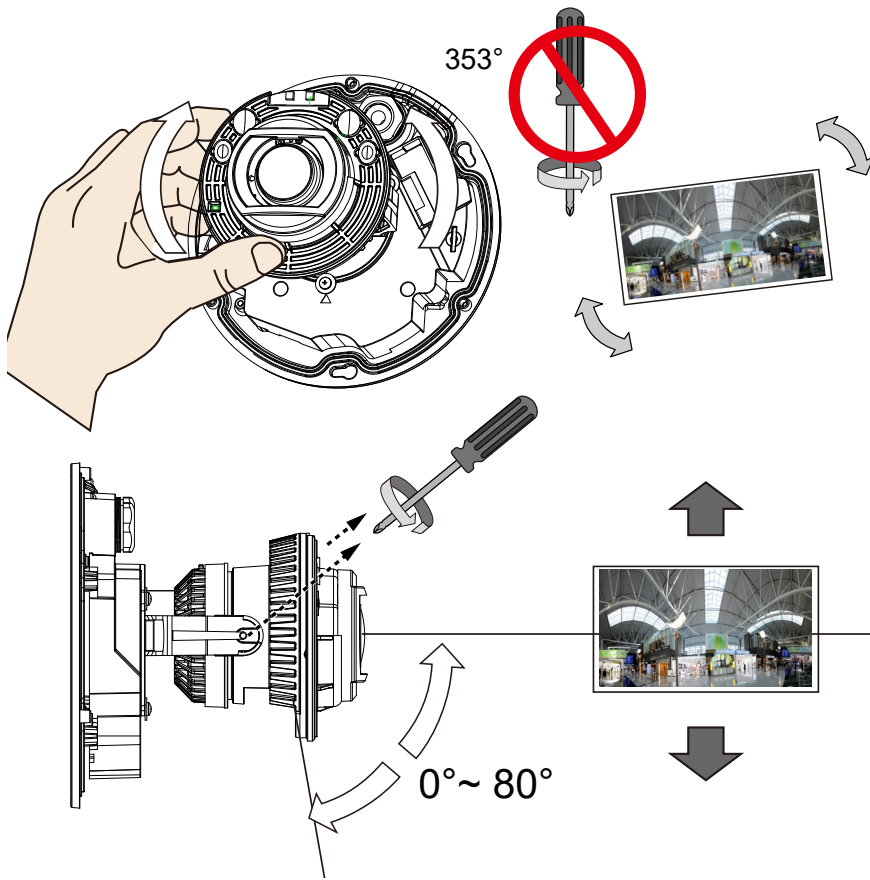


- On the device web console, click Zoom/Focus. If necessary, zoom in on the scene, and use the Auto Focus function to find the best imaging result.

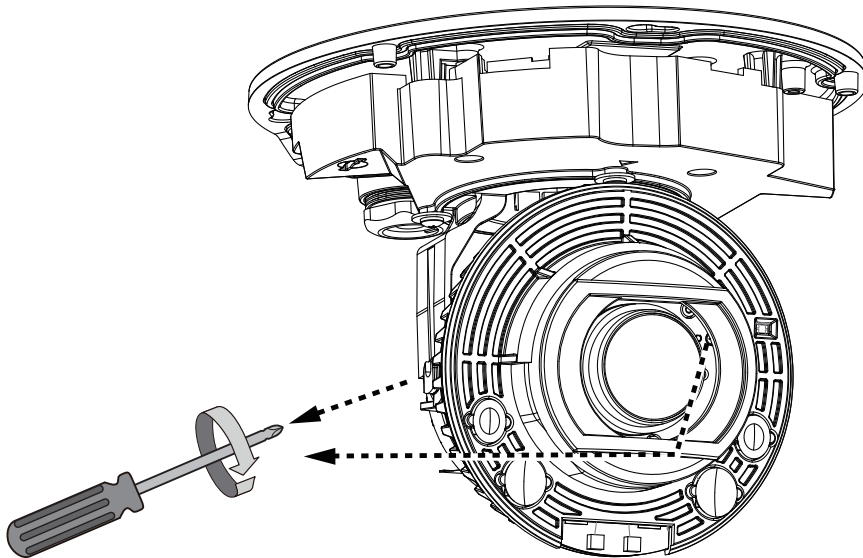
Zoom / Focus



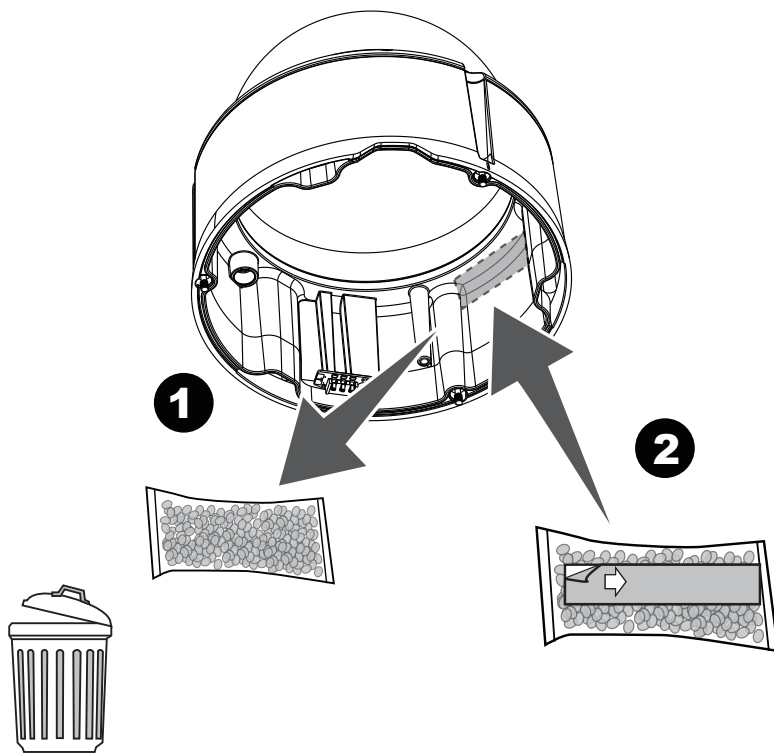
- With a live view displayed on your laptop, adjust the pan and tilt angles to obtain an optimal image. Check the live view to ensure the shooting direction and image coverage.



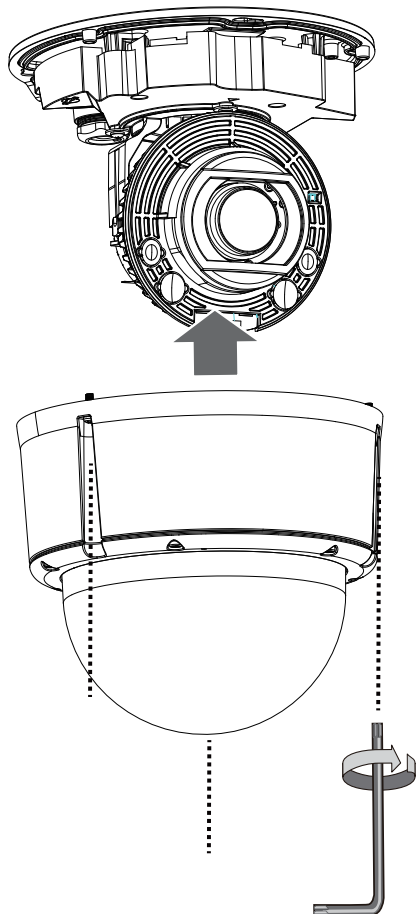
- Carefully tighten the retention screws on the side of the camera lens.



15. Replace the desiccant bag on the inside the camera dome cover.

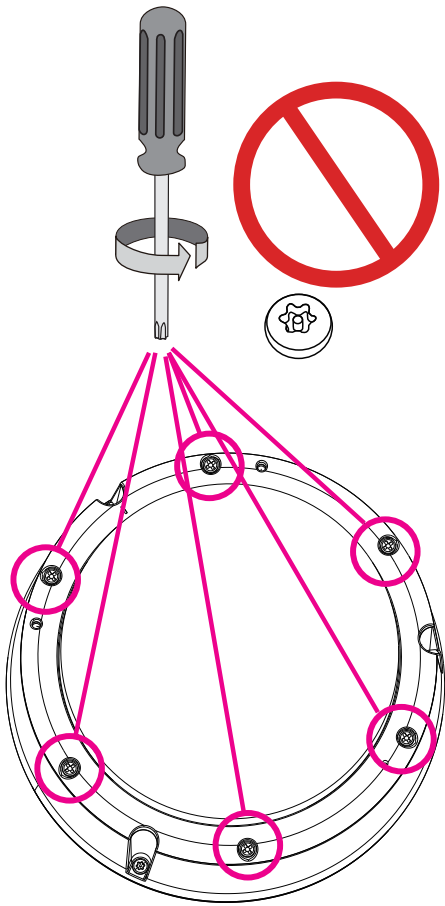


16. Align and install the dome cover.





Note that you should not remove the 6 anti-tamper screws on the dome cover.



LED Definitions

	Item	LED status	Description
LED Definition	1	Steady Red	Powered and system booting, or network failed
		Red LED off	Power off
		Green LED off	Network is disconnected
	2	Steady Red and Green LED blinks every 1 sec.	Connected to network
	3	Green LED blinks every 1 sec. and RED LED blinks consecutively every 0.15 sec.	Upgrading firmware
	4	Green and RED blink every 0.15 sec, Green and RED light on, then blink again.	Restoring defaults
	5	RED LED is on, Green LED blinks and RED LED is constantly on.	Status after a reset (network connected)
		Green and RED LEDs are constantly on.	Status after a reset (network disconnected)

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.

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.

Preview

This page displays the camera stream preview window. You can select which virtual camera's stream to preview and at which refresh rate.

The screenshot shows the VIVOTEK web interface. The top navigation bar includes 'Developer Mode' and 'Device Web'. The left sidebar lists various settings categories. The main 'Preview' section displays the following information:

- Pipeline Status:** RUNNING
- Camera:** default
- Refresh Rate:** 1.0 secs
- Automatically refresh camera preview

Below the settings, it indicates 'Viewing Camera: default every 1 seconds.' and shows a live video feed of a room with a timestamp '2020-09-24 11:17:01.726'.

Peripheral

On this page you can see the current connection statuses of digital inputs. If your digital inputs are connected to sensor devices, its statuses will be automatically detected as being pulled high or pulled low. You can also manually trigger a digital output. Digital outputs can also be triggered via the Alarm settings.

The screenshot shows the VIVOTEK web interface for the 'Peripheral' settings. The main content area displays the following settings:

- Digital input:** Input 1 current status: LOW
- Digital output settings:** Output 1 current status: GROUNDED, Manual triggers: off
- Day/Night settings:** IR cut filter: Night mode, Light sensor sensitivity: Normal

An 'UPDATE' button is located at the bottom right of the settings panel.

The Day and Night setting is also available on this page. You can change the IR cut filter and the light sensor sensitivity settings. Normally the default setting suffices ordinary uses.

The IR cut filter is turned on or off depending on the lighting level detected by the onboard light sensor.

Zoom / Focus

The camera comes with a zoom module lens. If an area of your interest is a distance away, you can zoom in on the scene.

If you find your image is out of focus, use the AUTO FOCUS function to let the camera find the optimal image focus.

You can use the << or >> buttons to fine-tune the imaging results. Normally the AUTO FOCUS function can deliver the best results.

The screenshot shows the VIVOTEK web interface in Developer Mode. The top navigation bar includes the VIVOTEK logo, 'Developer Mode', and 'Device Web'. The sidebar menu on the left lists various settings categories: Camera (Preview, Peripheral, Zoom / Focus, Device info, Privacy mask, Virtual camera, Video settings, Stream configuration, Device health, User management, Network, Date & time, Firmware), Applications (Overview, Cloud connection), and Legal (Logout). The main content area is titled 'Zoom / Focus' and features a camera preview window. Above the preview are radio buttons for 'Auto' (selected) and '100%'. The preview shows a timestamp '2020-09-24 11:38:51.097'. Below the preview are three sliders: 'Zoom', 'Focus', and 'Iris', each with left and right arrow buttons for fine-tuning. An 'AUTO FOCUS' button is positioned at the bottom right of the settings panel.

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.

The screenshot displays the VIVOTEK Developer Mode interface. The top navigation bar includes the VIVOTEK logo, 'Developer Mode', and 'Device Web'. A left sidebar lists various camera settings under 'Camera' and 'Applications' categories. The main content area is titled 'Device info' and contains a table of device specifications. Below the table are two buttons: 'REBOOT DEVICE' and 'FACTORY RESET'. Underneath is a 'Developer Options' section with explanatory text and an 'ENABLE DEVELOPER MODE' button.

Device info	
Device ID	Deviceid
Manufacturer	VIVOTEK
Model	FD9392-EHTV-O
OS	1.2.2
AOSP API	27
Minimum supported SDK addon	2
Maximum supported SDK addon	4
Security patch level	2018-09-05
Uptime	0 days, 02:43:29
Firmware	QC5603-1.2.2-camera-FD9392-EHTV-O-1.0.157-user

Developer Options

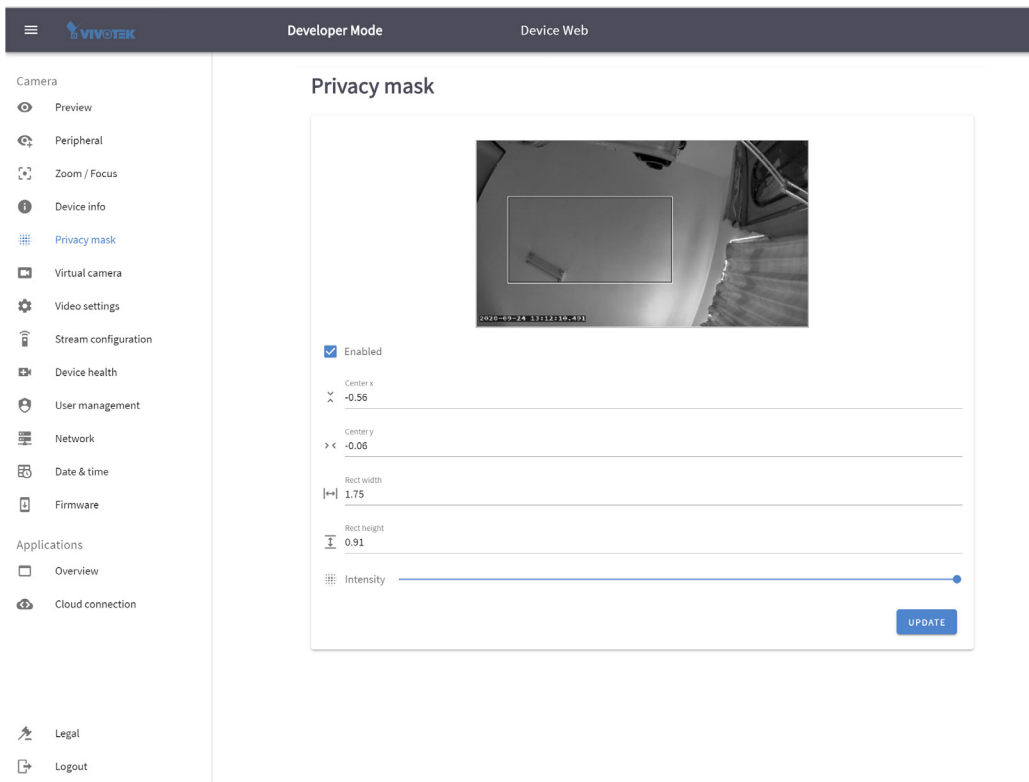
Developer mode allows to develop and debug apps on the device. In developer mode it is not possible to install apps via the Device Management Portal or through a compatible ONVIF client. Additional terms and conditions apply when running a device in developer mode.

By enabling developer mode **all applications and licenses will be removed**.

To disable the developer mode, perform a factory reset.

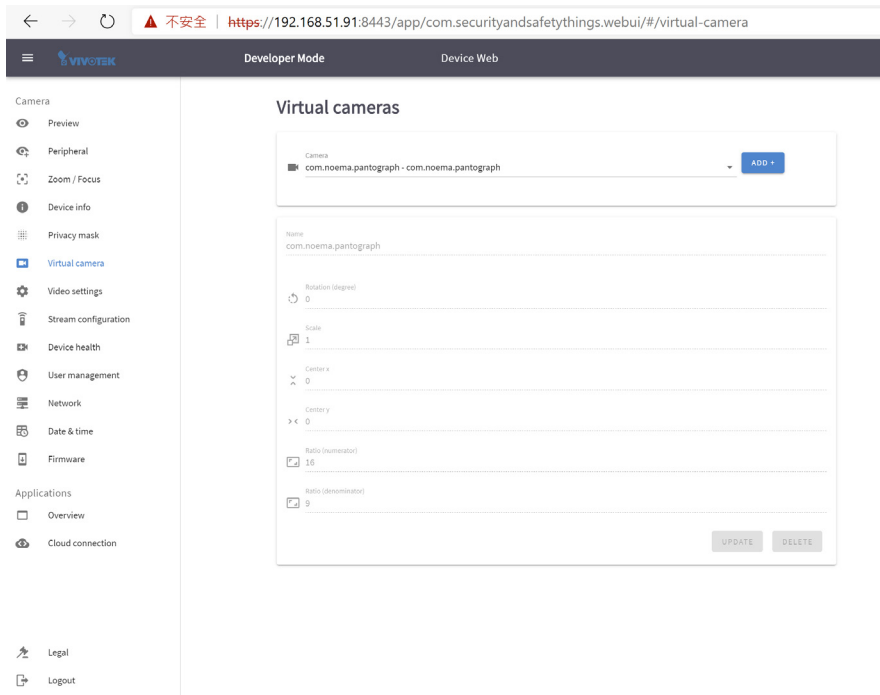
Privacy Mask

Click and drag on the screen to block out sensitive areas in your field of view. The size and 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.



Virtual Camera

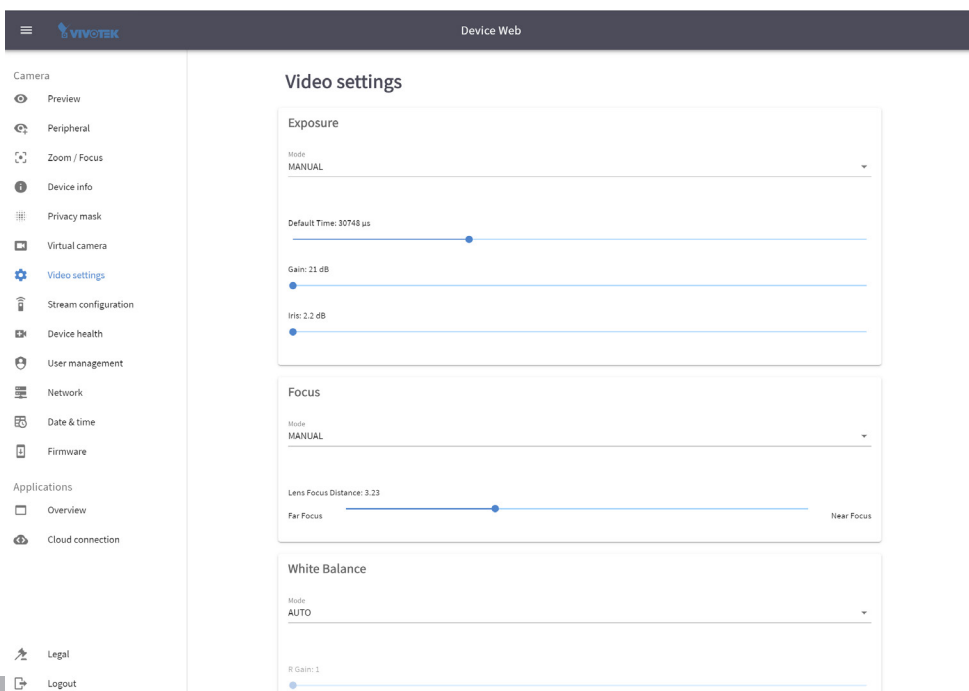
Allows the creation of additional sub-stream(s) which can cover a certain zone of interest in the camera's field of view. The sub-streams are used for video analytics on apps.



Video settings

On this page some additional video stream settings can be set like Exposure, Focus and White Balance, etc.

Normally the Auto settings can deliver satisfactory results. If the need should arise, you can manually change the parameters, such as prolonging the exposure time for a place with less lighting, change the electronic gain level, and iris size. You can also modify the Focus and White Balance if your surveillance scene needs special adaptation.



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.

The screenshot displays the 'Stream configuration' page in a web interface. The top navigation bar includes the VIVOTEK logo, 'Developer Mode', and 'Device Web'. A sidebar on the left lists various system settings under 'Camera' and 'Applications'. The main configuration area is titled 'Stream configuration' and contains the following fields:

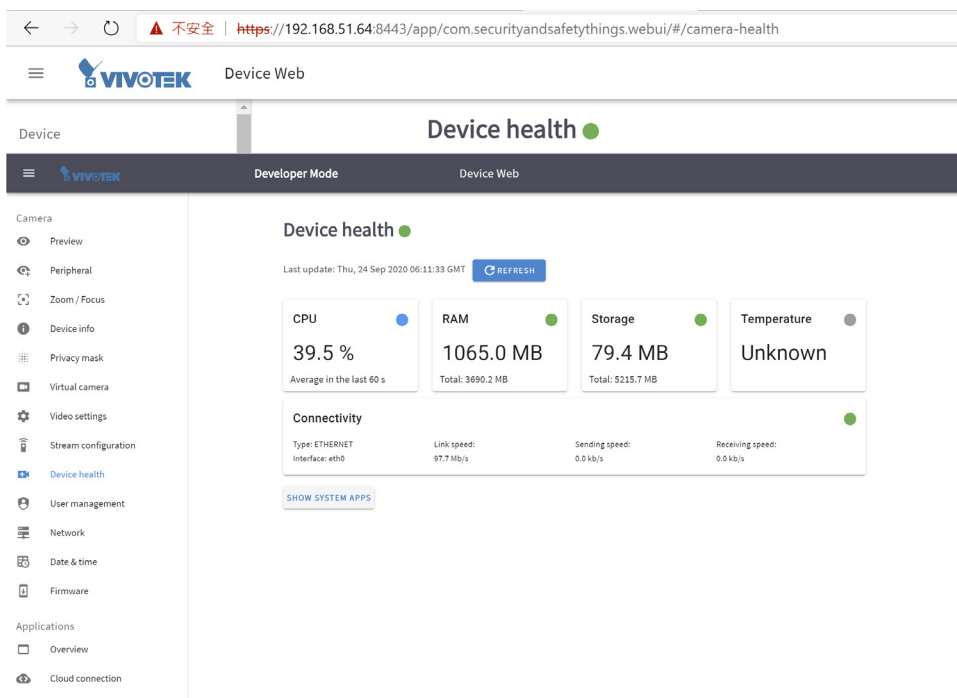
- Stream:** uhd265
- Description:** 4K Ultra HD H265 live stream (2160p)
- Encoding:** video/avc
- Width:** 3840
- Height:** 2160
- Bitrate:** 20000000
- I-Frame Interval:** 1

An 'UPDATE' button is positioned at the bottom right of the configuration form.

The bit rate is represented in bits. Streams are defined as Full High Definition and Ultra High Definition streams. The default 20000000 bits is approximately 244kb or 1.9megabits.

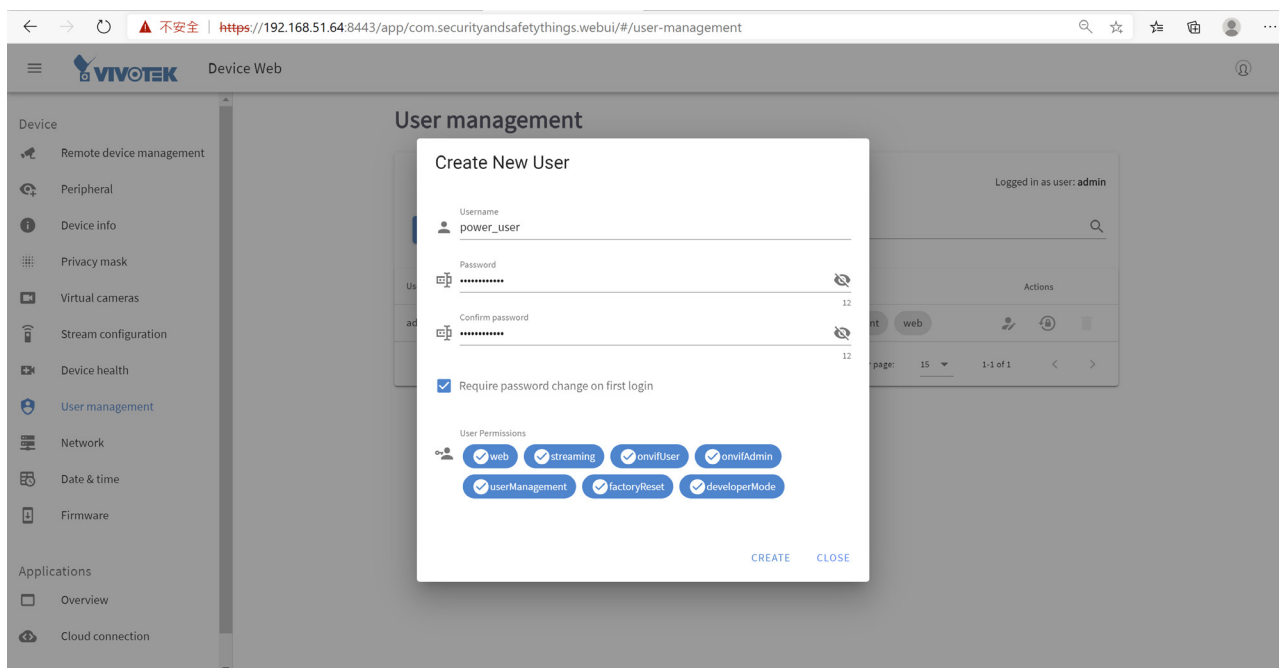
Device Health

This page displays various device health information: CPU/Memory/Storage usage, Connectivity, Temperature and App status.



User Management

On this page, you can add/remove users and set user's rights and permissions.



Network

By default, the device 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.

The screenshot shows the 'Network' configuration page in Developer Mode. The interface includes a sidebar with navigation options like Camera, Peripheral, Zoom/Focus, Device info, Privacy mask, Virtual camera, Video settings, Stream configuration, Device health, User management, Network (selected), Date & time, Firmware, Applications, Overview, and Cloud connection. The main content area is titled 'Network' and shows settings for the 'ETH0' interface. The 'Automatic configuration (DHCP)' toggle is turned off. Below this, there are input fields for IPv4 and IPv6 addresses, gateways, and DNS servers. The IPv4 address is 192.168.51.91/24, the IPv6 address is fe80::2830:795d:192:deac/64, and the gateway is 192.168.51.1. There are 'SAVE', 'REFRESH', and 'SAVE ALL' buttons at the bottom.

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.

Enabling network time setting is a necessary step when you "claim" the camera for downloading apps.

The screenshot shows the 'Date & Time' configuration page in Developer Mode. The interface includes a sidebar with navigation options like Camera, Peripheral, Zoom/Focus, Device info, Privacy mask, Virtual camera, Video settings, Stream configuration, Device health, User management, Network, Date & time (selected), Firmware, Applications, Overview, and Cloud connection. The main content area is titled 'Date & Time' and shows 'Device Date & Time (Local)' with a 'USE COMPUTER DATE & TIME' button. Below this, there is a calendar showing 'Thu, Sep 24' and a digital clock showing '2:51 PM'. Under 'Additional Settings', there is a 'Use network-provided time' toggle which is turned on, and a 'Time zone' dropdown set to 'GMT+08:00'. There are 'REFRESH' and 'SAVE' buttons at the bottom.

Firmware

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

The screenshot shows the Vivotek Developer Mode interface. At the top, there is a dark header with the Vivotek logo, 'Developer Mode', and 'Device Web'. On the left, a sidebar menu lists various settings categories: Camera (Preview, Peripheral, Zoom / Focus, Device info, Privacy mask, Virtual camera, Video settings, Stream configuration, Device health, User management), Applications (Overview, Cloud connection), and other options like Legal and Logout. The main content area is titled 'Firmware' and displays the 'Current firmware version' as 'OS_ADSP/qcs605/qcs605-8.1.0/root/D20200519_155639/user/test-keys'. Below this, there is a blue button labeled 'UPLOAD NEW FIRMWARE' with a downward arrow icon.

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:

The screenshot shows the VIVOTEK Developer Mode interface. On the left is a navigation menu with categories like Camera, Applications, and Legal. The main content area is titled 'Overview' and shows the last update time and a 'REFRESH' button. Below this is a table of installed applications:

Name	Version	ANRs	Crashes	Kills	CPU	RAM	Status
Pantograph Tracker Go to application website	Expires	1.0.0	0	1	0	3.6 % 57 MB	Running 0 day(s) left

Below the application table is the 'App frame rate information' section, which contains another table:

Name	Video Session ID	Current	Target
Pantograph Tracker	1016995067554033500	N/A	30

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** S&ST apps can be integrated through the Data Magnet interface.

This screenshot shows the VIVOTEK Developer Mode interface with a browser address bar at the top. The main content area is titled 'Overview' and shows the last update time and a 'REFRESH' button. Below this is a table of installed applications:

Name	Version	ANRs	Crashes	Kills	CPU	RAM	Status
FaceBiometrics Pro App interface and configurations	1.0	0	0	0	35.6 %	130 MB	Running 28 day(s) left
VAST2 Data Magnet App interface and configurations	8.1.0	0	0	0	0.0 %	10 MB	Running

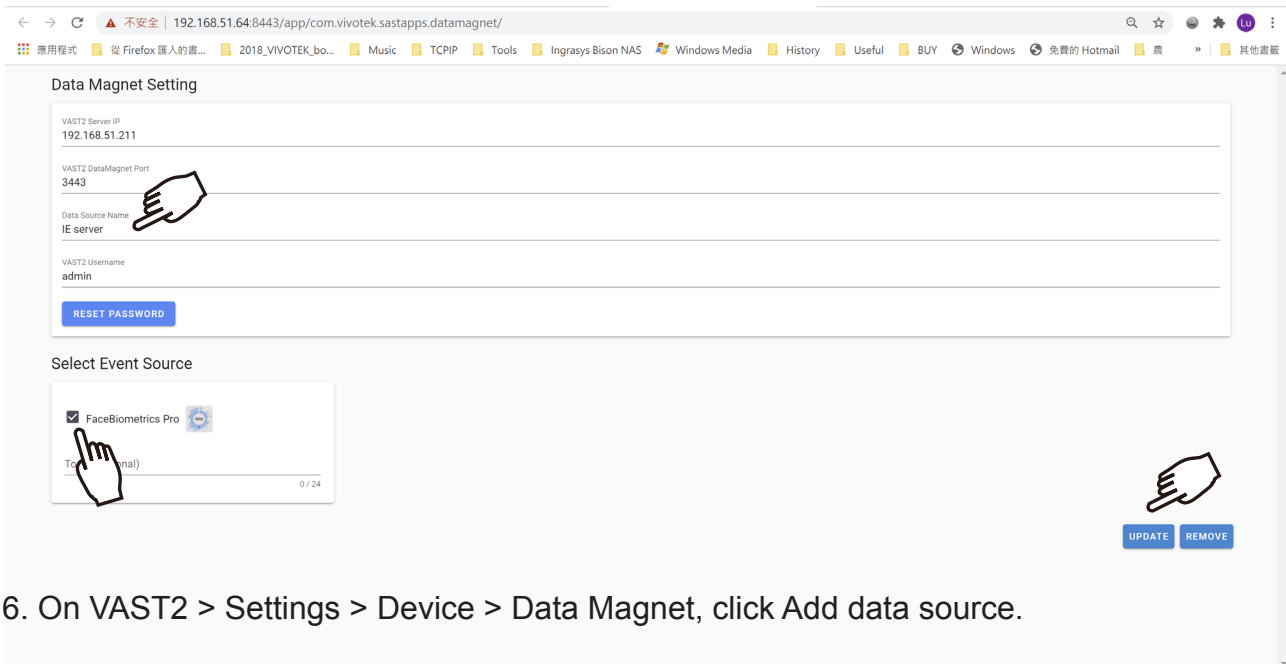
A hand icon points to the 'App interface and configurations' link for the VAST2 Data Magnet app. Below the application table is the 'App frame rate information' section, which contains another table:

Name	Video Session ID	Current	Target
FaceBiometrics Pro	6495160242591344000	N/A	15.151516

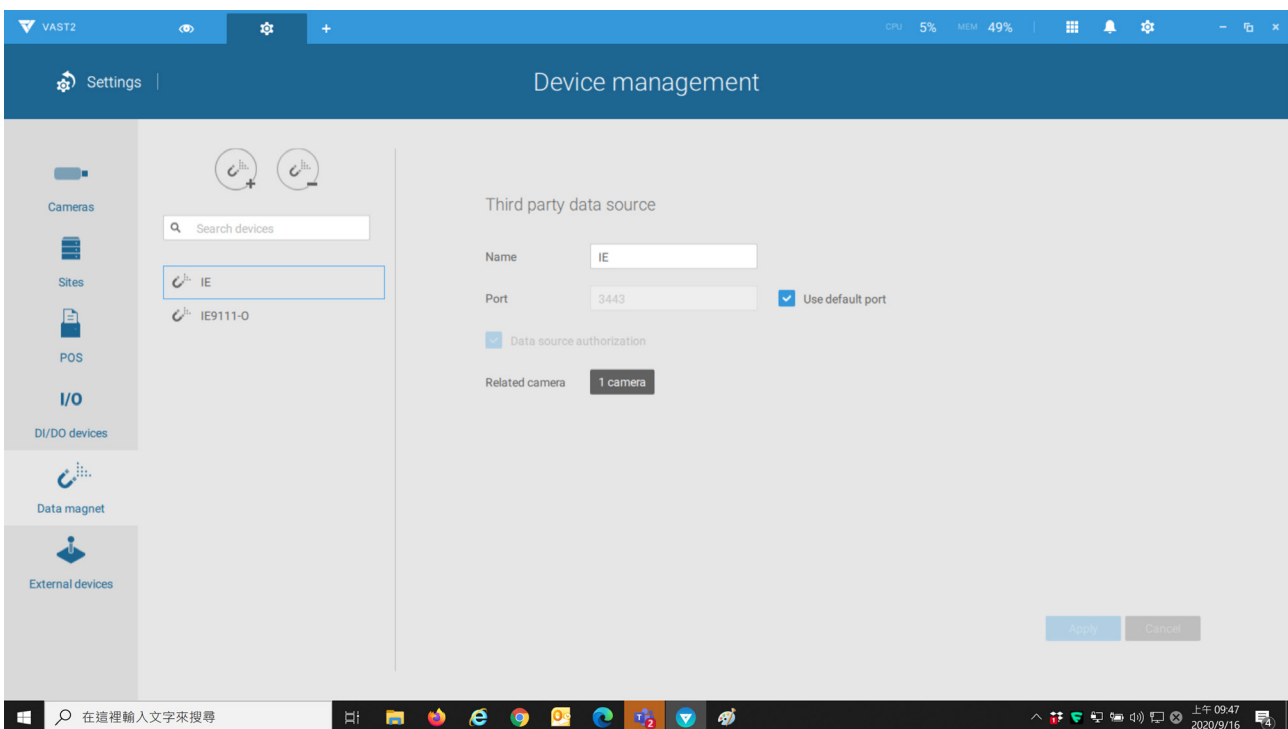
At the bottom of the page, there is a section titled 'Get apps via Device Management Portal or tool' with a 'GET APPS' button.

Enter the following to enable the connection through Data Magnet:

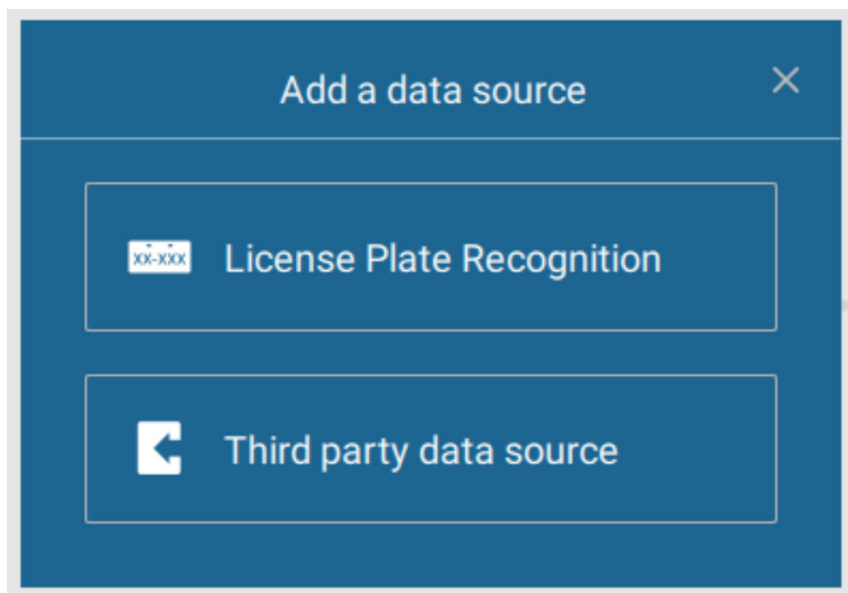
1. Your VAST2 server IP.
2. Data Magnet port: usually 3443.
3. Data Source Name: Note that this name **must be identical** to that on the VAST2 Data Magnet setting page.
4. VAST2 user name and password.
5. Select the app installed on your device. Click the Update button.



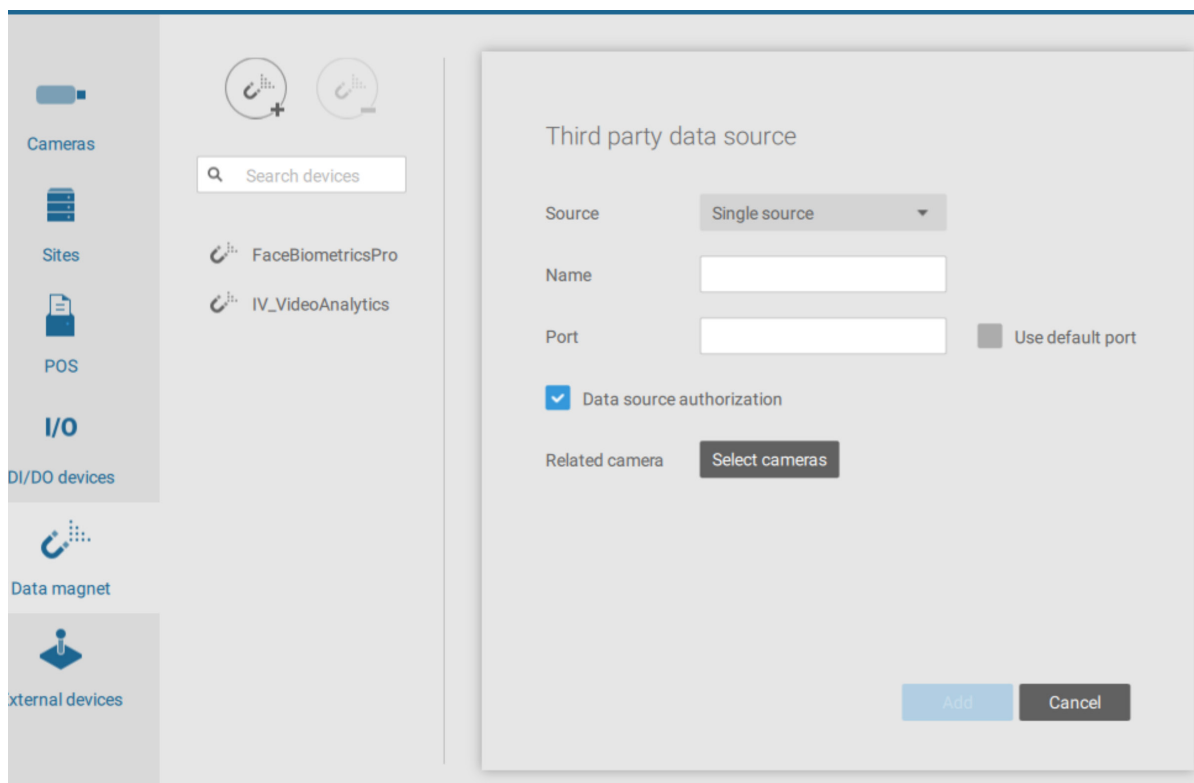
6. On VAST2 > Settings > Device > Data Magnet, click Add data source.



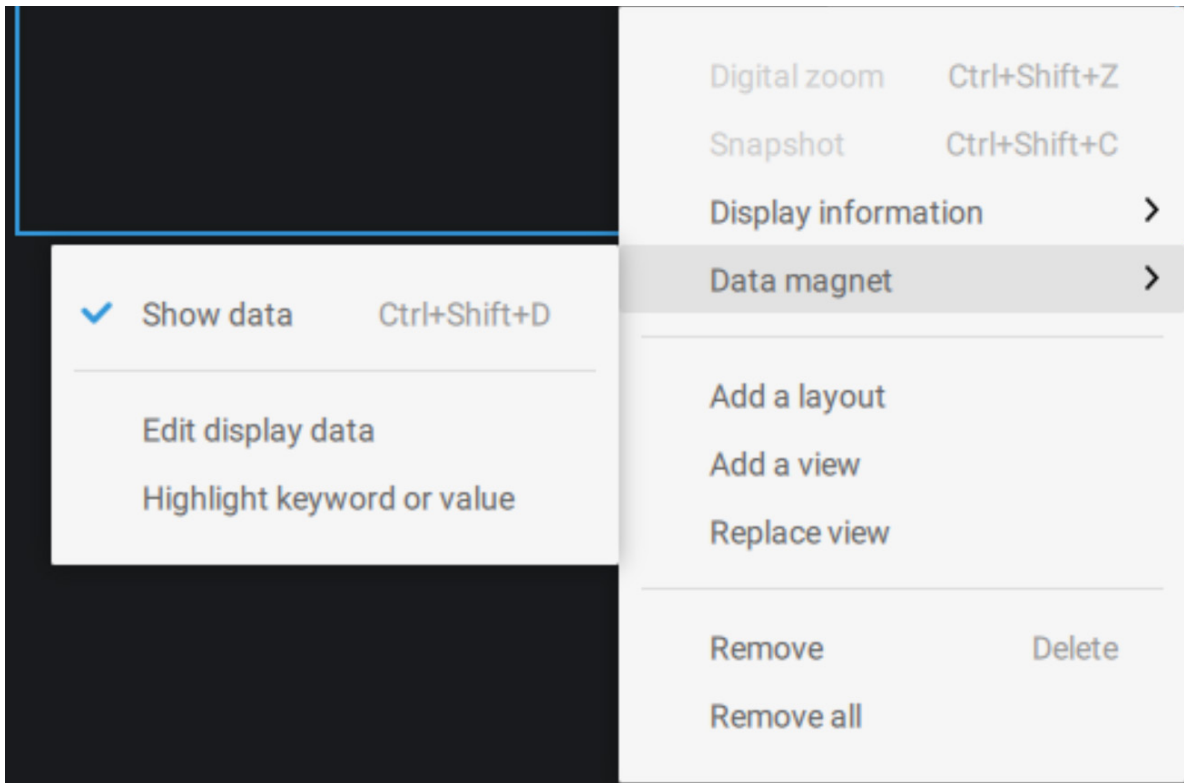
7. Select Third party data source.



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

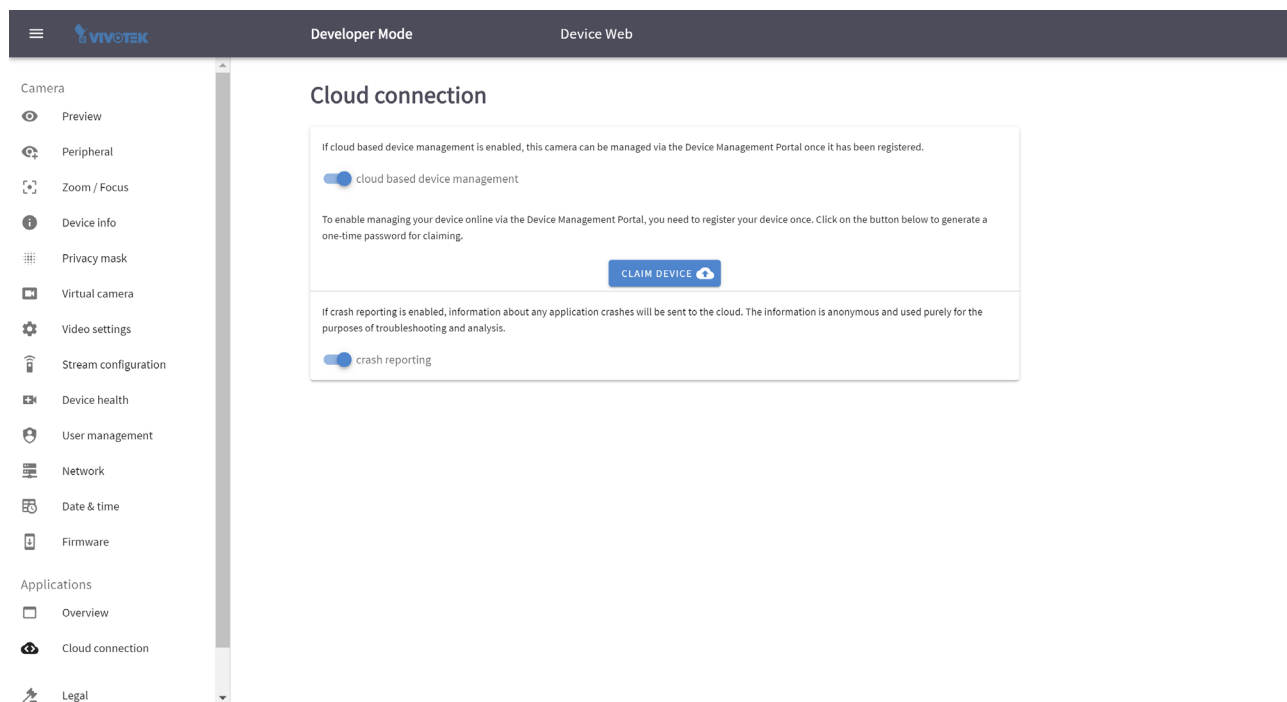


9. You can then right-click on a VAST2 view cell to display the Data magnet data. The analytics detection results can display along with the live video.



Applications - Cloud Connection

You can connect your device to Security and Safety Things 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.



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

The prerequisites for connecting the camera to the cloud are:

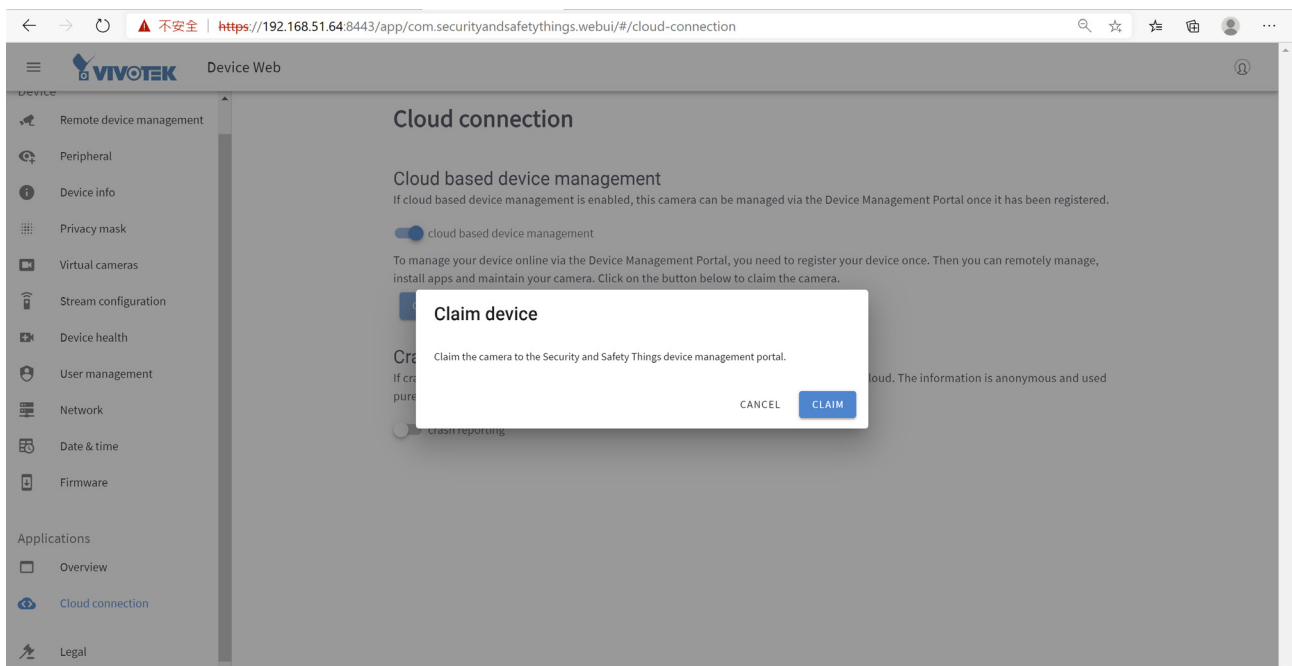
- You have an account on the S&ST Device Management Portal.
- Cameras have a non-restricted access to the Internet.
- Your camera has a valid certificate. Please verify this by accessing the camera using a web browser and go to the Device info page. Then check if a Device ID is present:



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

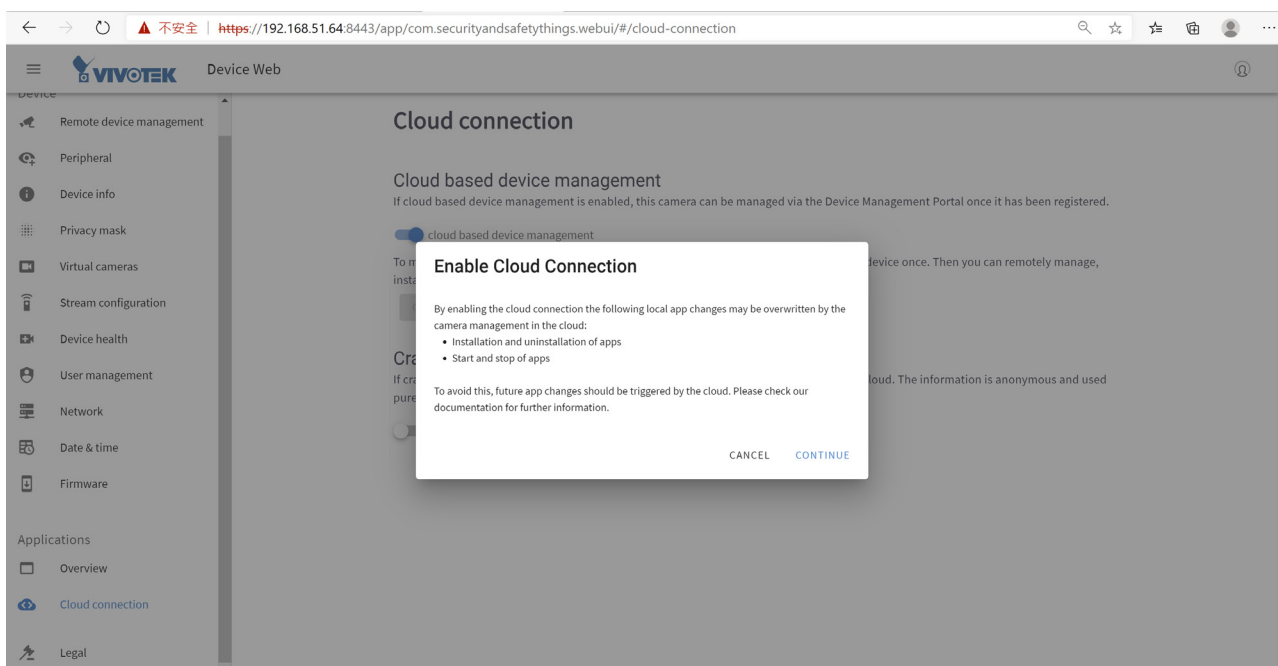
Proceed with the following for connecting the camera to the Device Management Portal:

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."



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

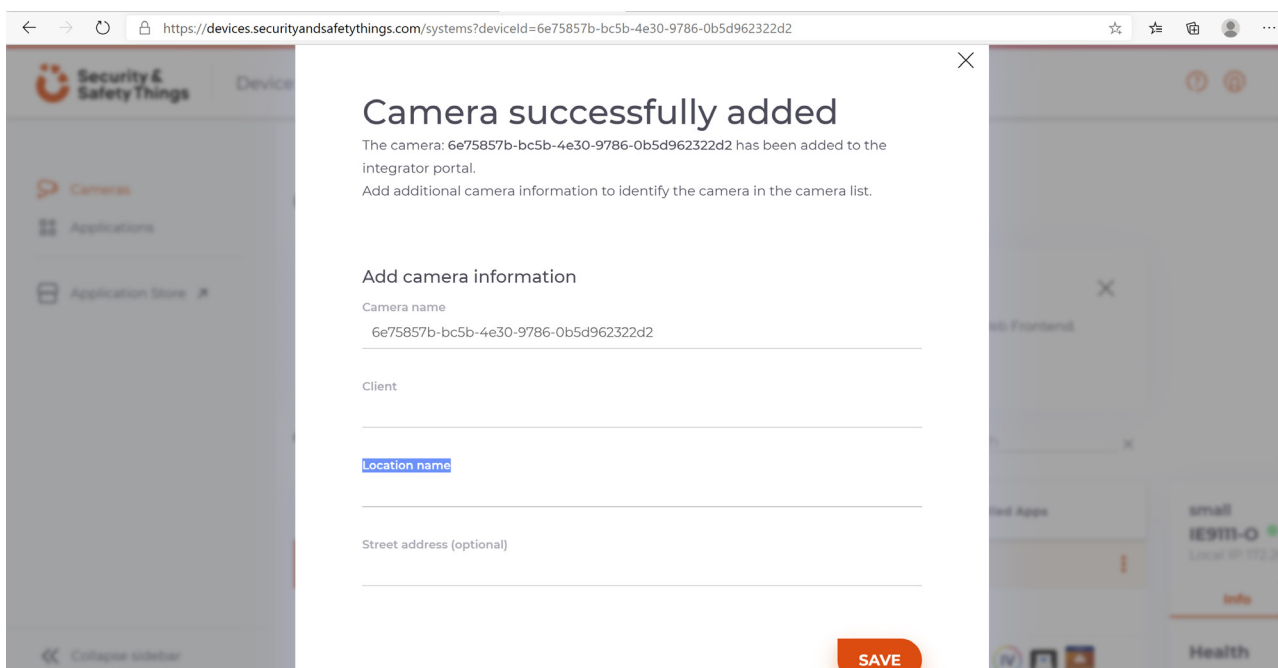
Click CONTINUE.



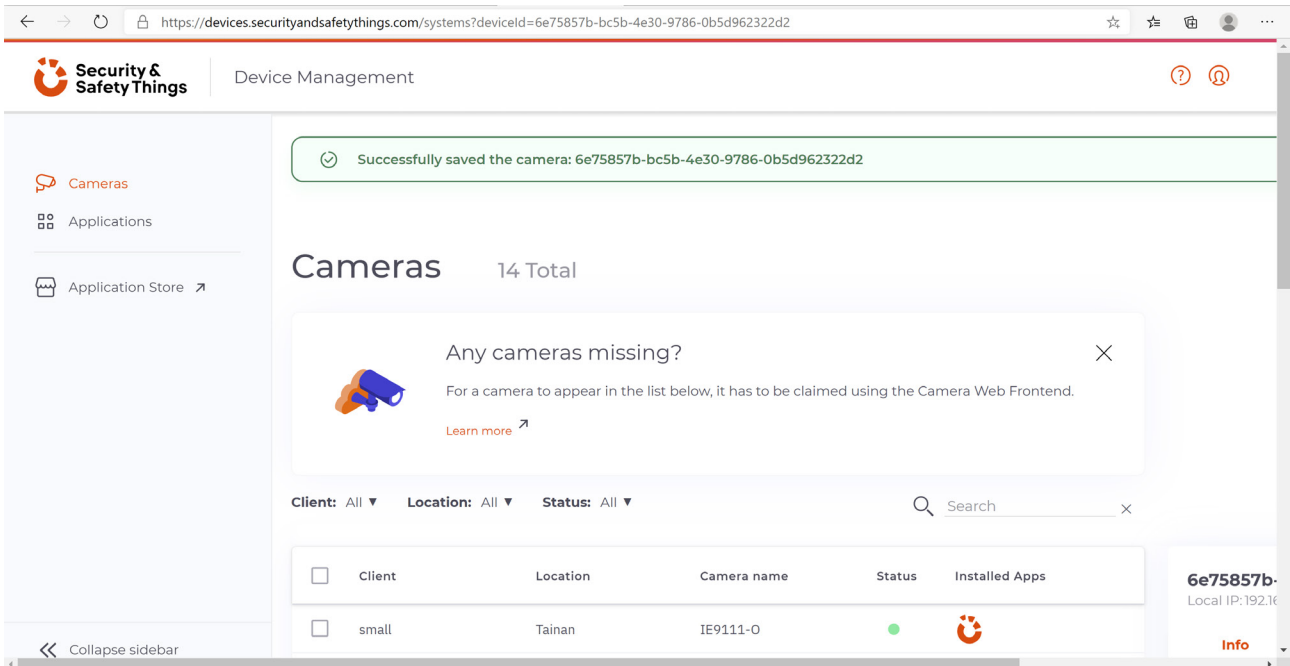
On the Device Management Portal page, you can enter some additional information regarding the device:

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

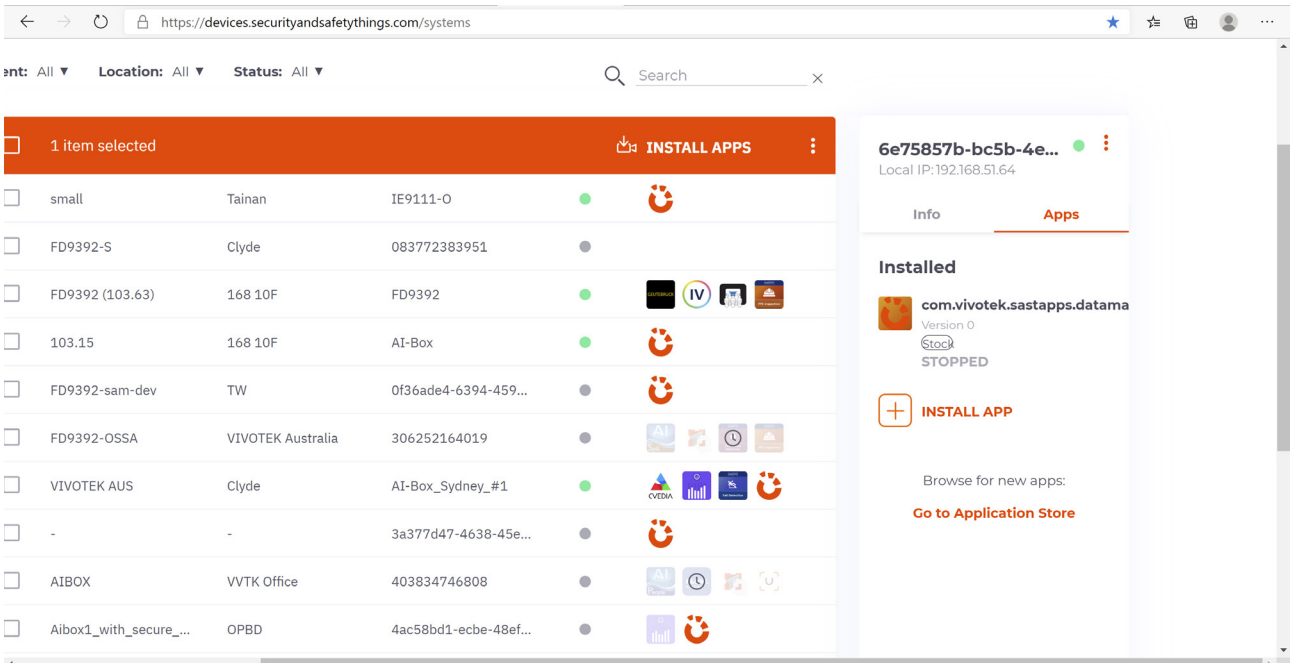
Click the SAVE button in order to save the changes and your camera will appear in the list of cameras on the Device Management Portal.



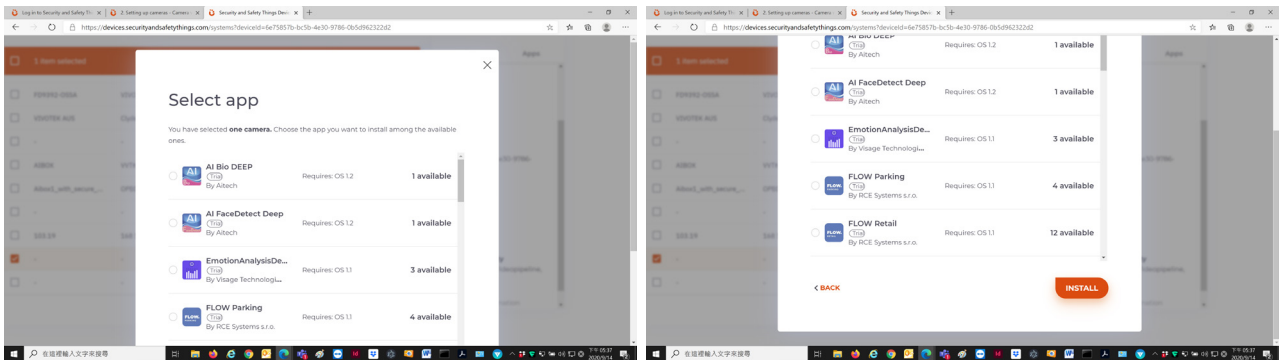
On the Device Management Portal page, you can see all connected devices/cameras.



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



Scroll to select an app. Select and click INSTALL.



Applications - Legal

This page provides legal information for the OS.

← → 🔍 不安全 | 192.168.51.64:8443/licenses/aosp_notice

應用程式 從 Firefox 匯入的書... 2018_VIVOTEK_bo... Music TCP/IP Tools Ingrasys Bison NAS Windows Media History Useful BUY Windows 免費的 Hotmail 農 其他書籤

Licenses

WRITTEN OFFER

This product may contain software under a license 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 the GNU General 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 software contained in 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, es 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-lifetime](#)
- [kernel](#)
- [recovery/root/letv-make2fs.conf](#)
- [recovery/root/hongnial_file_contexts](#)
- [recovery/root/hongnial_recovery_contexts](#)
- [recovery/root/kial_file_contexts](#)
- [recovery/root/kial_recovery_contexts](#)
- [recovery/root/kip/recovery](#)
- [recovery/root/letpolicy](#)
- [root/init](#)
- [system/sep/AdbAuthorization/AdbAuthorization.apk](#)
- [system/sep/Power/Power.apk](#)

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](http://www.voiceage.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](http://www.mpegla.com)

Electromagnetic Compatibility (EMC)

FCC Statement

This device complies 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）の基準に基づくクラス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.