



IE9111-O AI Box

User's Manual

Qualcomm QCS605 SoC with Built-in AI Engine • Video Processing and Machine Learning •
Supports VCA Solutions via Installation of S&ST APPs •
Enables Any Type of Network Camera to act as AIoT Device



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	9
Configuration	10
Remote Management.....	15
Peripheral	15
Device Info	16
Privacy Mask	16
Virtual Camera	17
Stream Configuration	17
Device Health	18
User Management.....	18
Network	19
Date & Time.....	19
Firmware	20
Applications - Overview	21
Data Magnet and VAST2.....	21
Applications - Cloud Connection	25
Applications - Legal	30
Technology License Notice.....	31
Electromagnetic Compatibility (EMC).....	32

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 S&ST Android OS
- Supports a variety of VCA solutions through S&ST 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.

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.



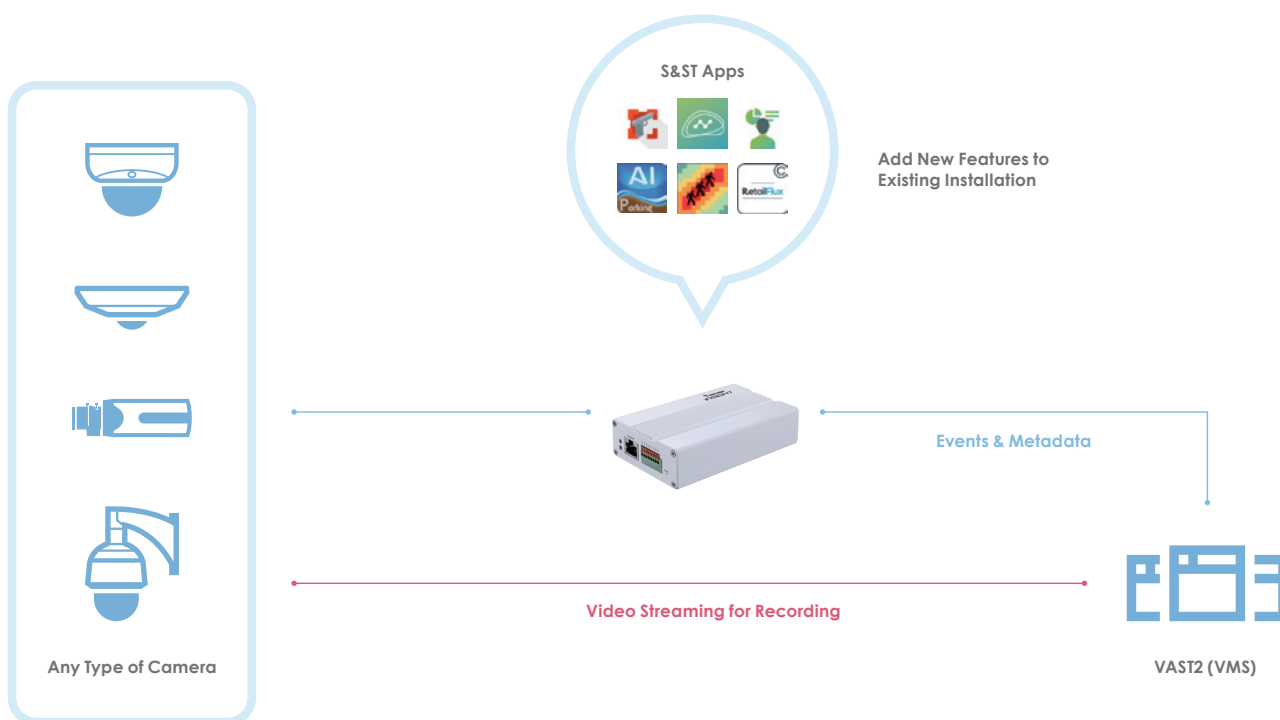
NOTE:

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

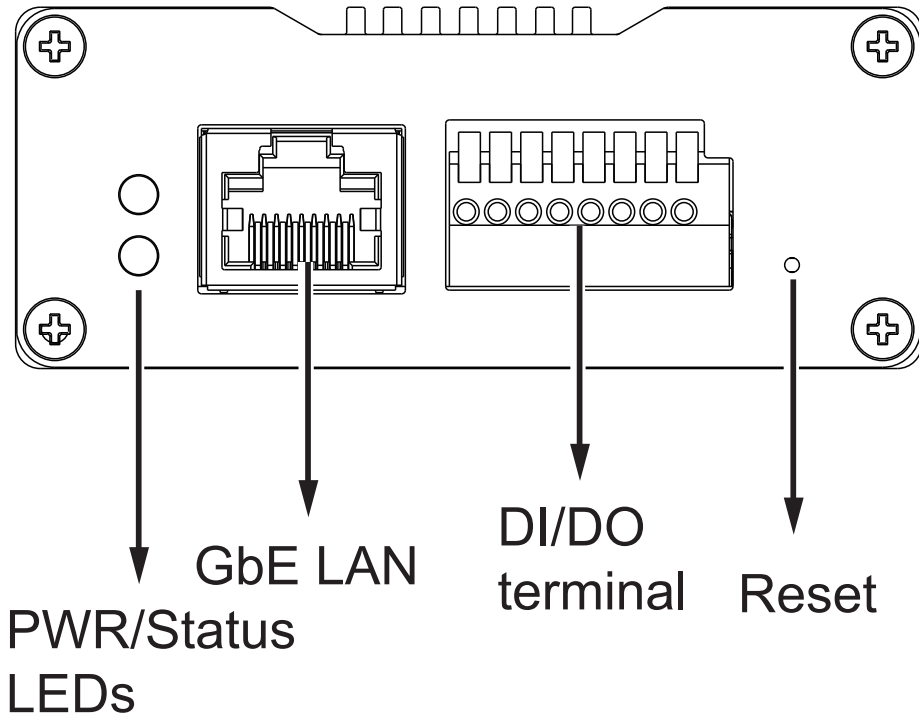
- IE9111-O
- Screw pack.
- Wall- / Panel-mount bracket.
- Quick Installation Guide.

Application

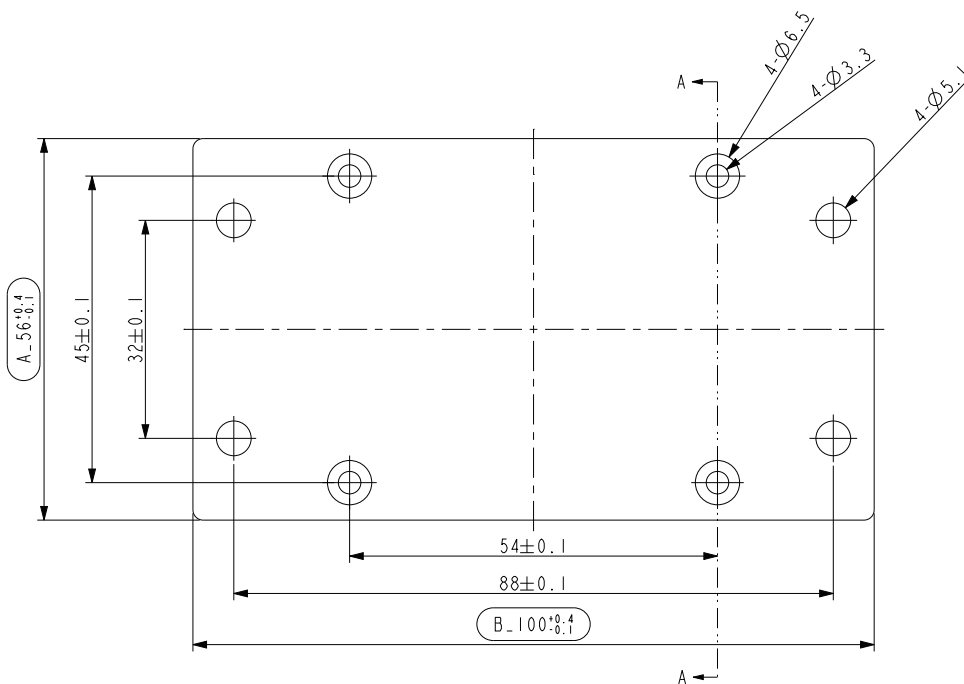


Physical Description

Outer View

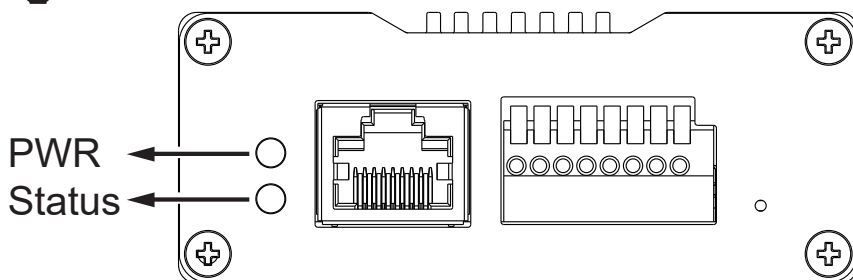
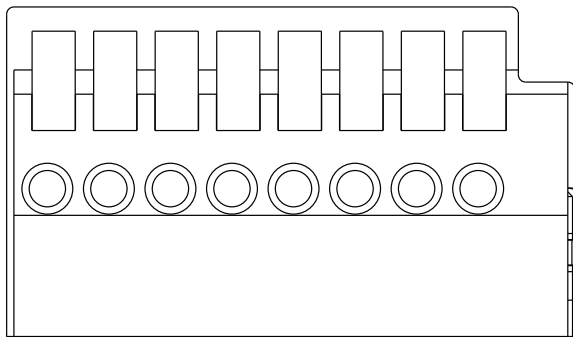


Bracket Dimensions



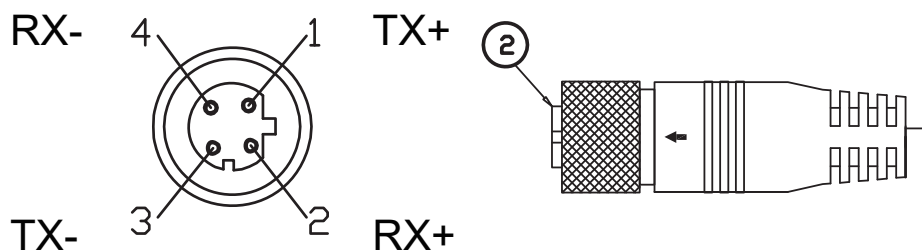
DI/DO Terminal Block Pinouts

D12-
D12+
D11-
D11+
D02-
D02+
D01-
D01+



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.

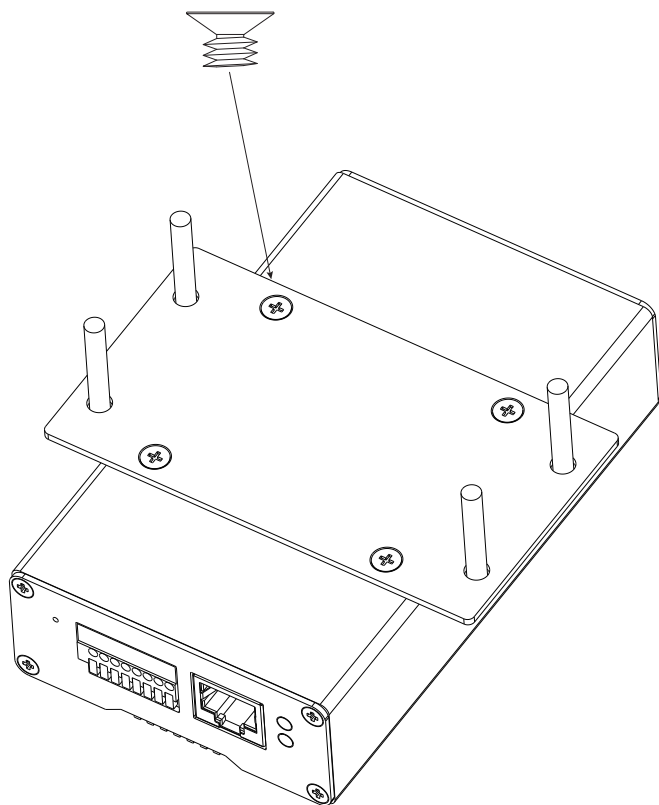
Use a flattened paper clip to press the button.

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

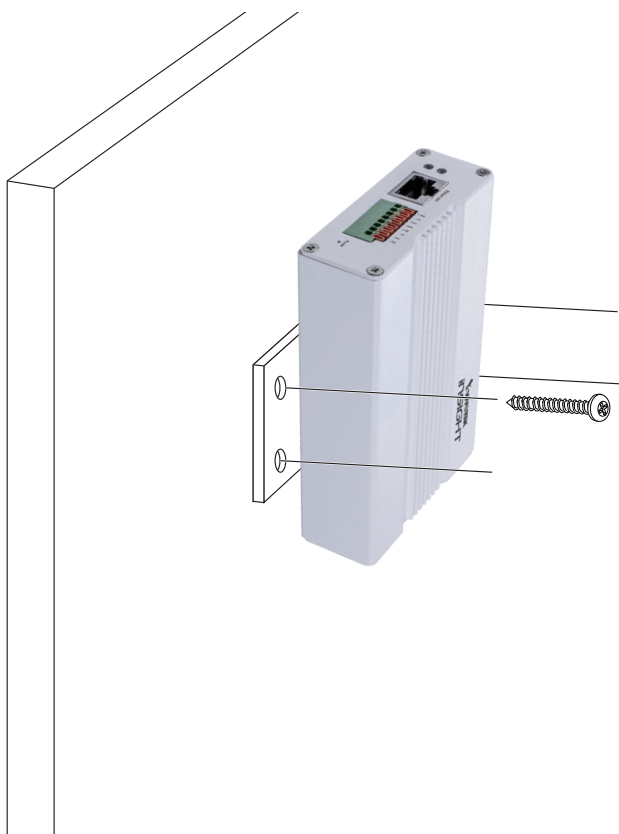
Restore: Press and hold the reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

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.



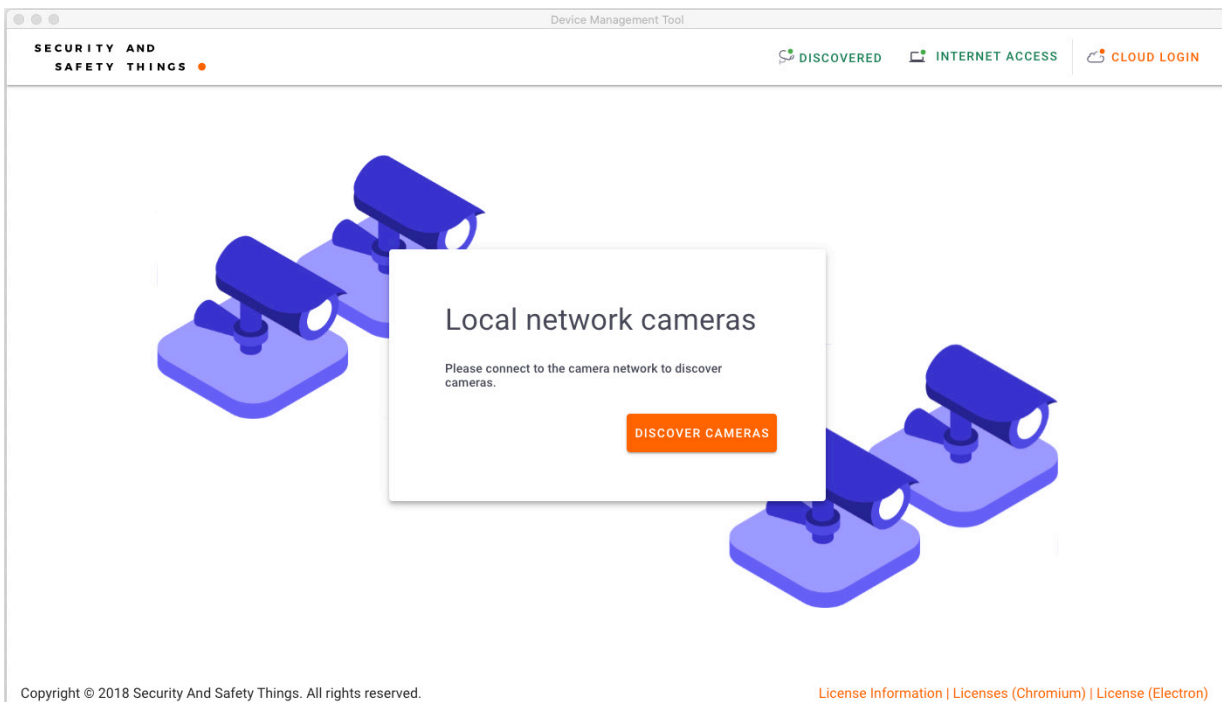
Configuration

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

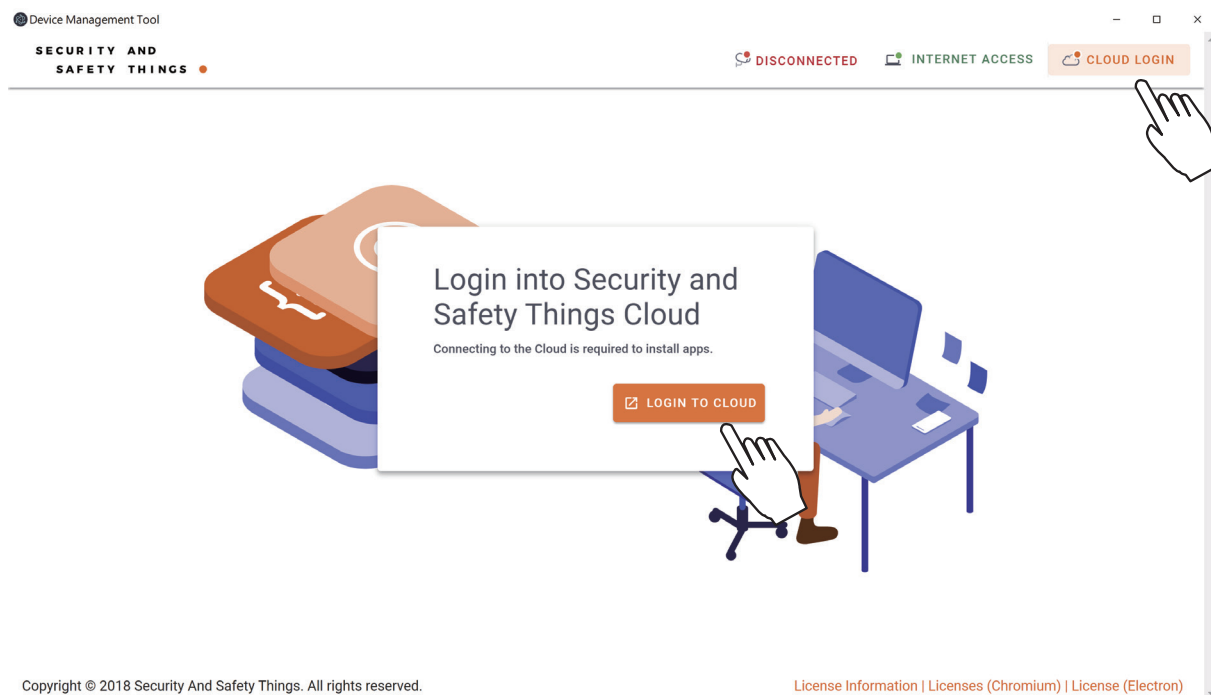


Make sure DHCP service is available in your local network.

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



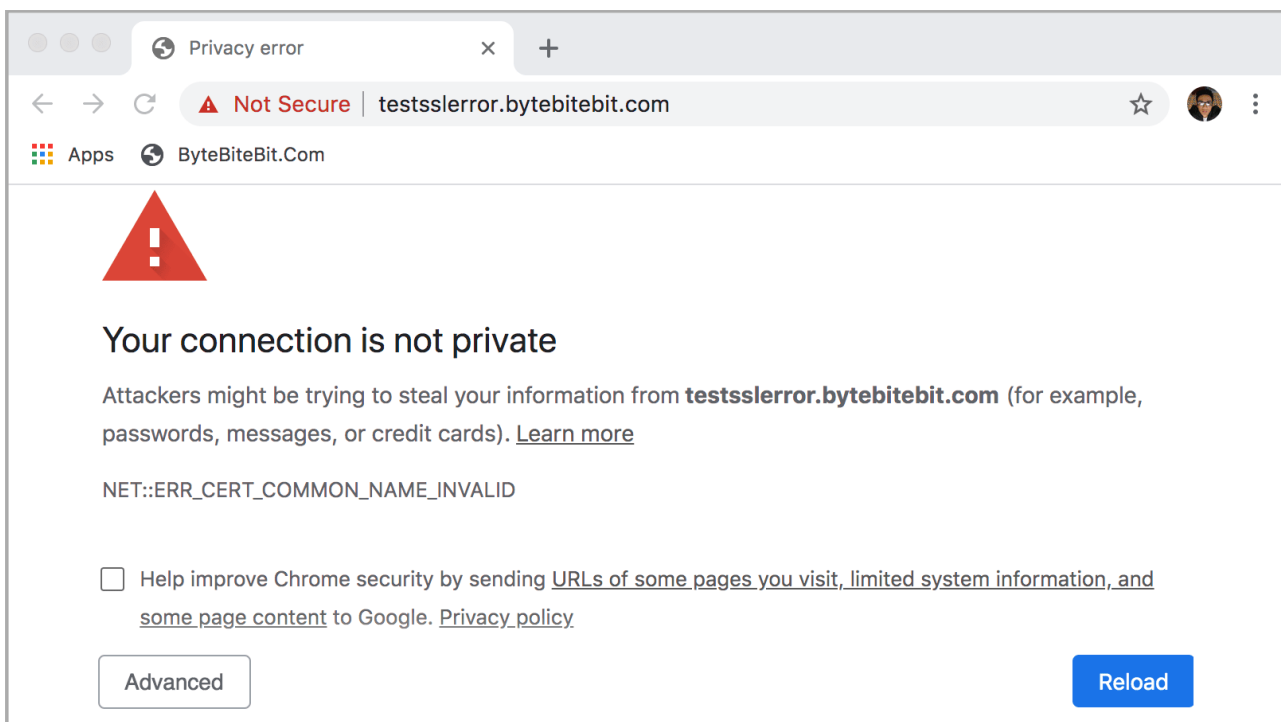
3. You can click Cloud Login to download S&ST apps or visit:
<https://store.securityandsafetythings.com/shop/catalog/c/main>



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

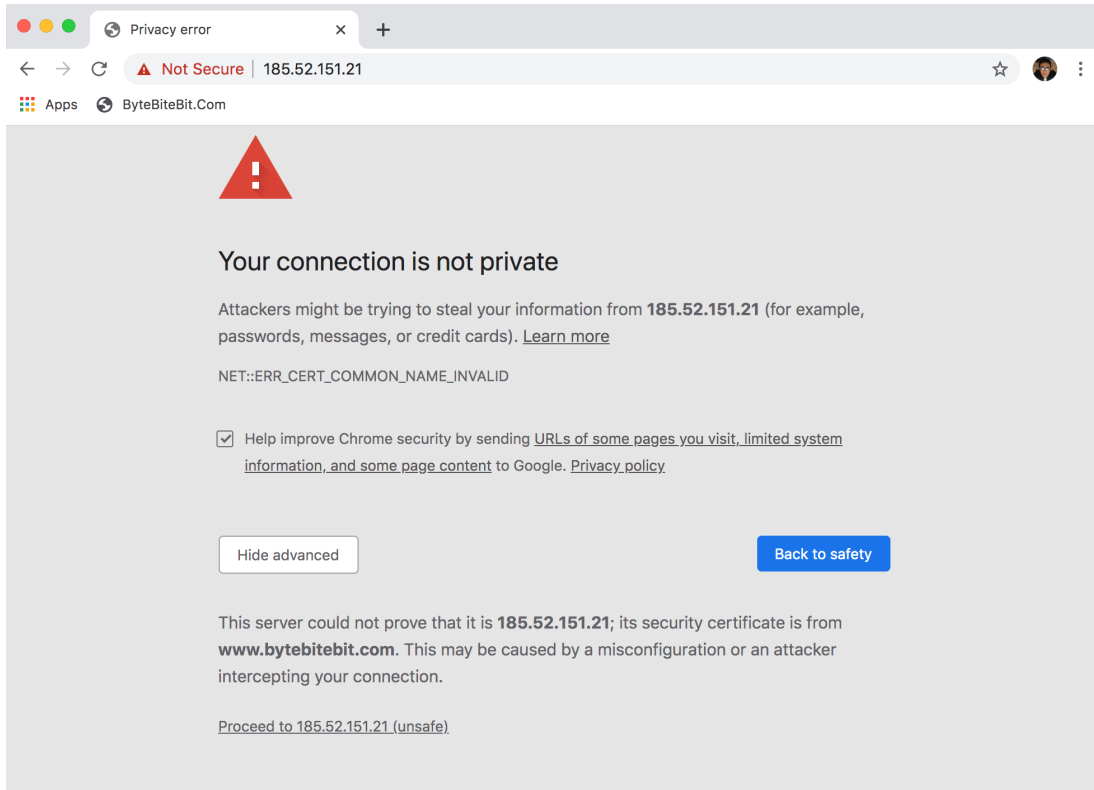
Enter [admin/admin](#) as the default credential.

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

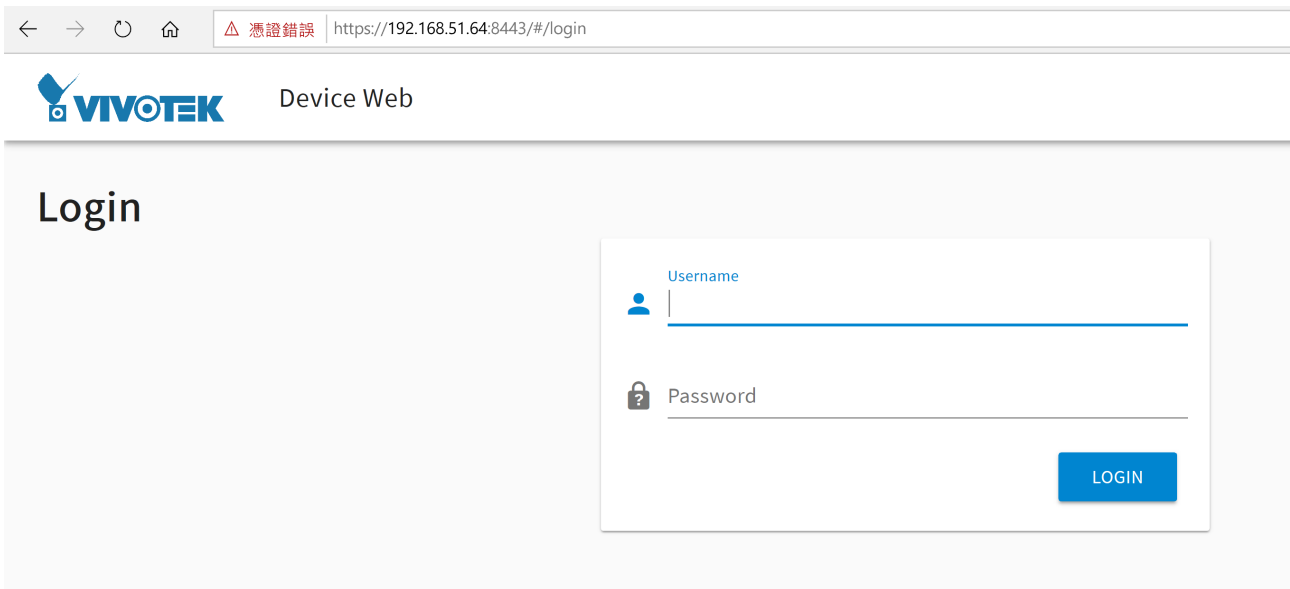


Click Proceed to [xxx.xxx.xxx.xxx \(Unsafe\)](#) to open the web console.

Note the IP addresses below are for reference only.

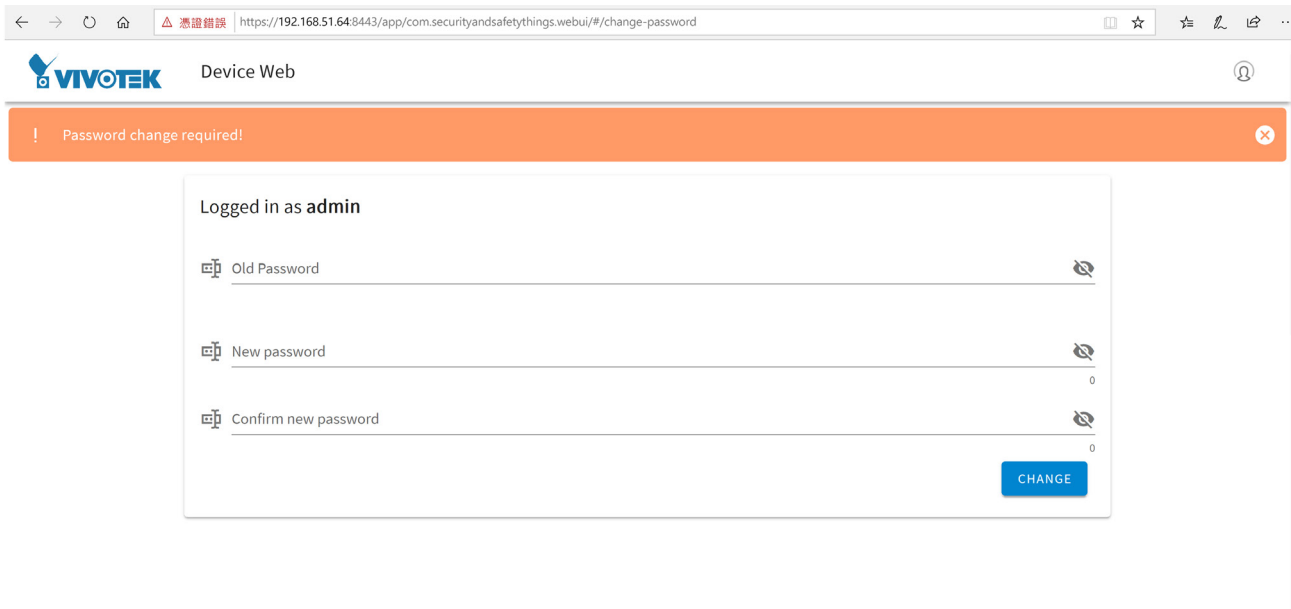


Enter **admin/admin** as the default credential.



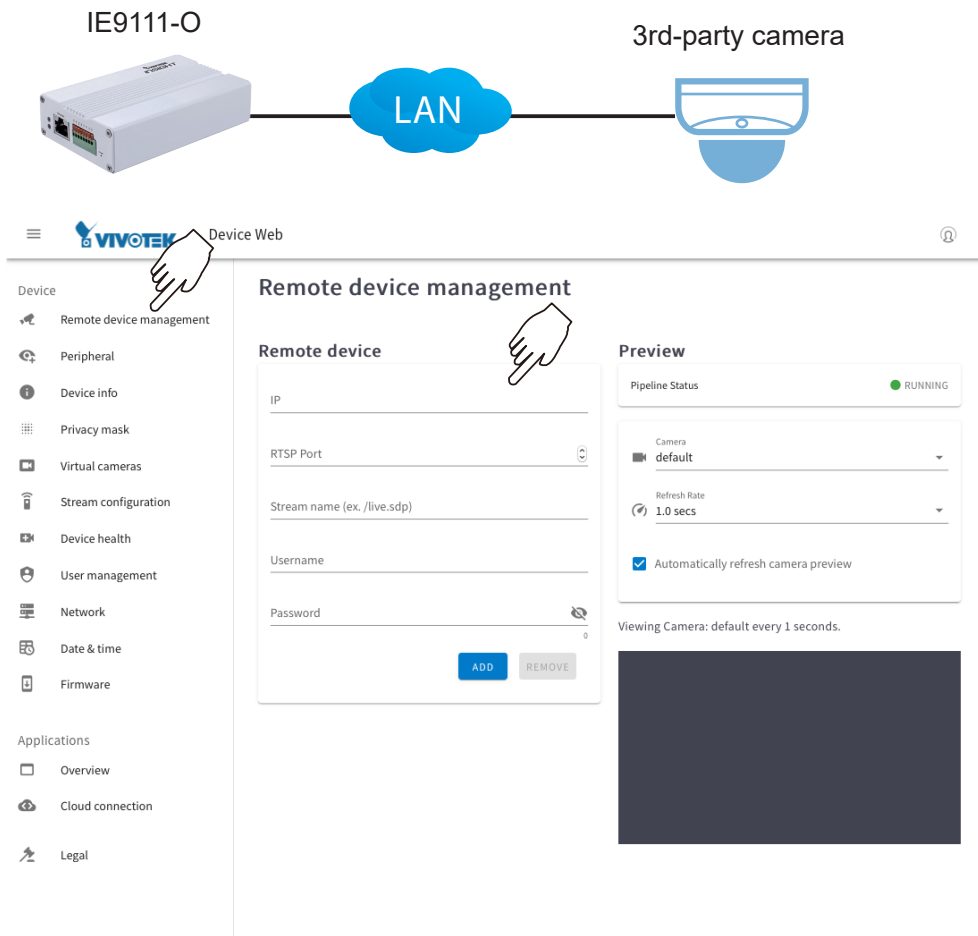
You will be requested to create a new password for security concern. Enter a combination of alphabetic, numeric, and special characters that is strong enough for protection.

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



The screenshot shows a web browser window with the URL `https://192.168.51.64:8443/app/com.securityandsafetythings.webui/#/change-password`. The page title is "Device Web" and the VIVOTEK logo is visible in the top left. An orange notification bar at the top reads "Password change required!". The main content area is titled "Logged in as admin" and contains three password input fields: "Old Password", "New password", and "Confirm new password". Each field has a strength indicator on the right, with the "New password" and "Confirm new password" fields showing a "0" below the indicator. A blue "CHANGE" button is located at the bottom right of the form.

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

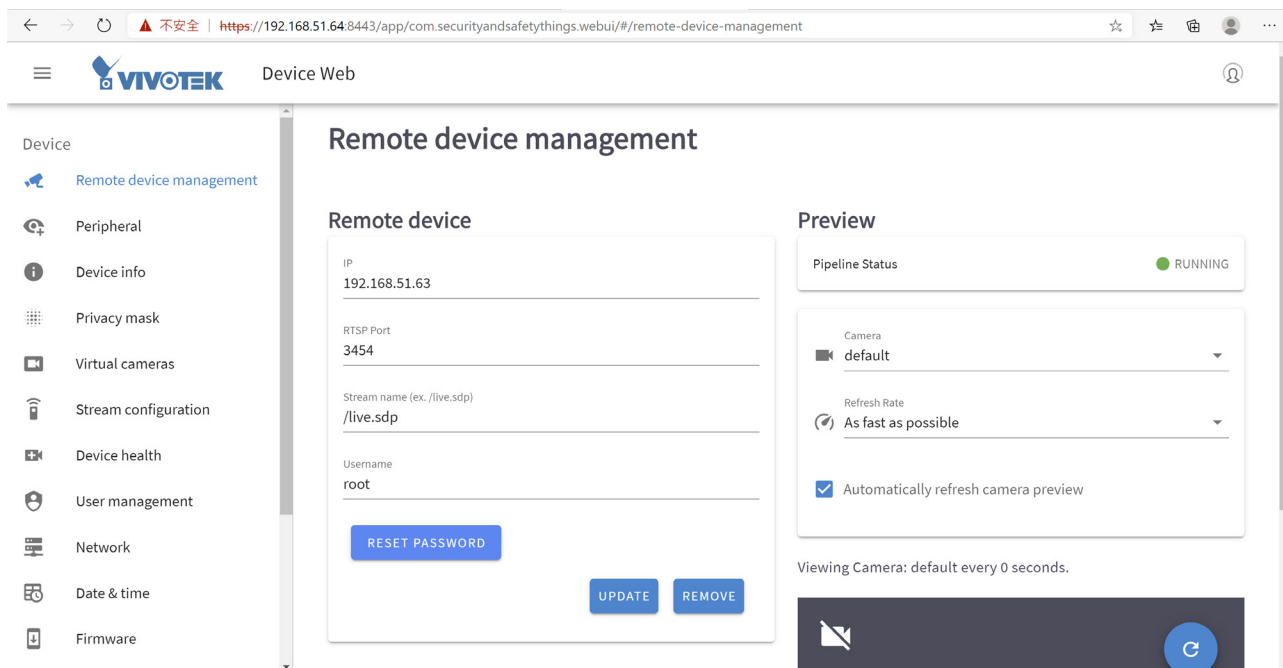


Enter **8554** as the RTSP port.

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

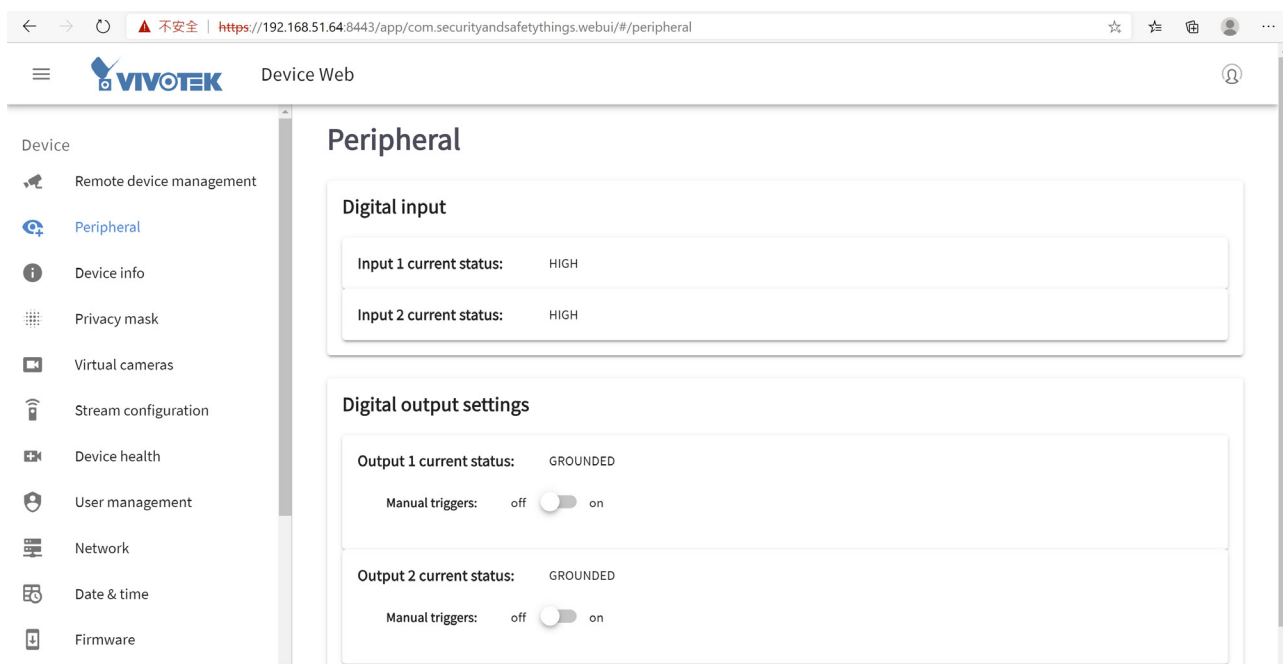
Remote Management

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



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.

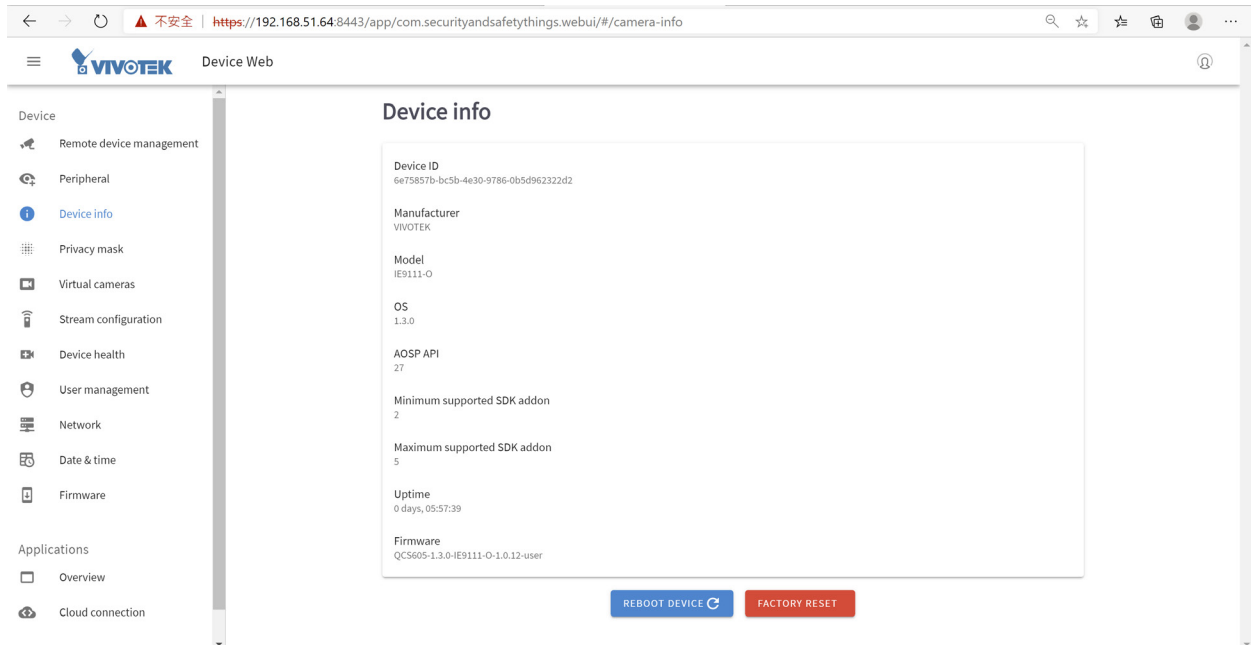


Device Info

Important information about this device is displayed on this page: including Device ID, OS version, AOSP API, SDK addon, firmware version, etc.

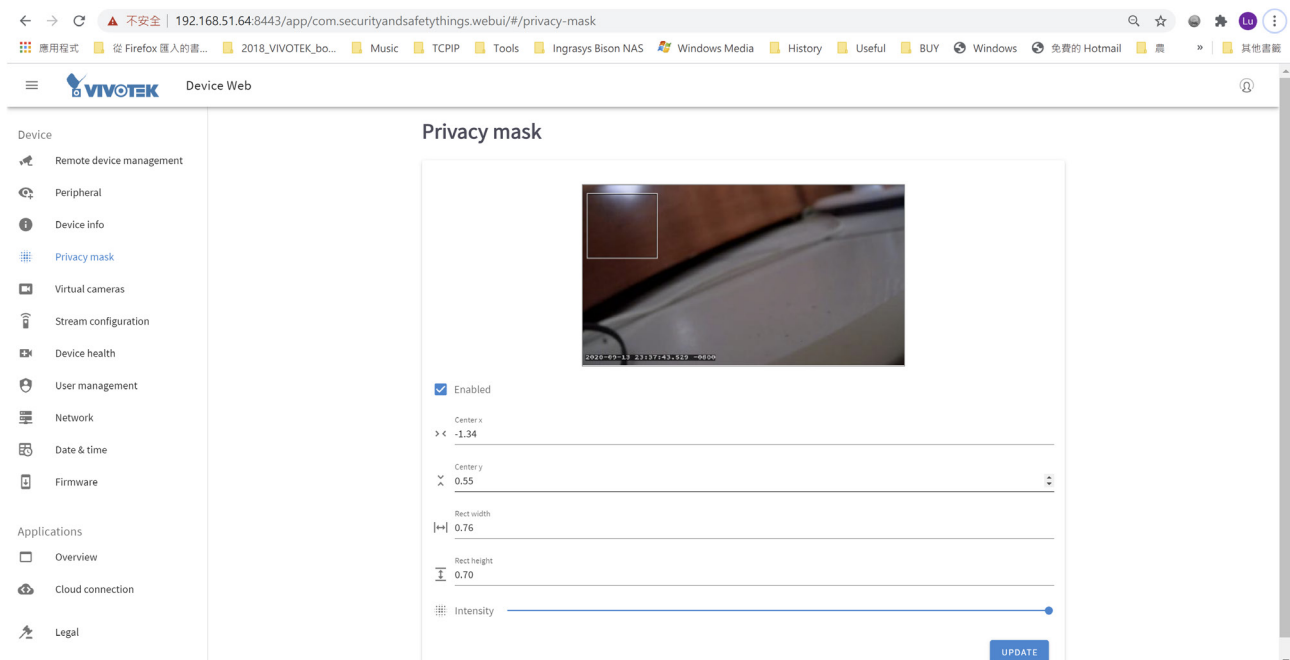
The Device ID is a unique ID for each camera and will be displayed in the Device Management Portal.

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



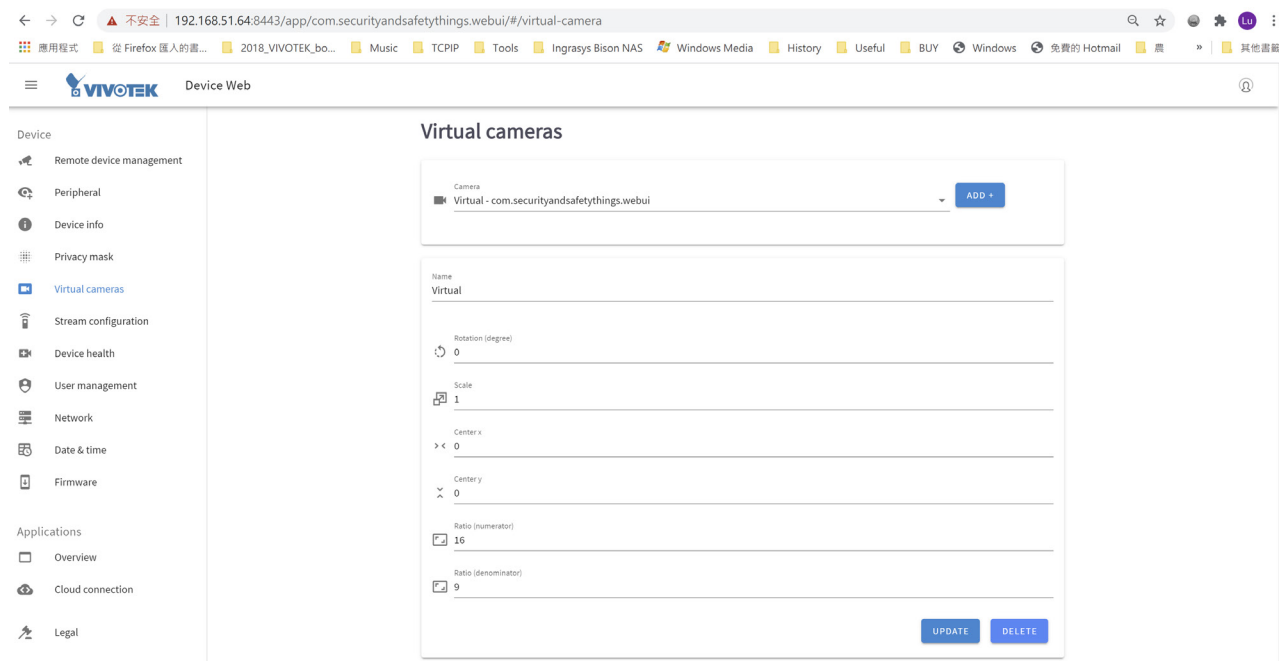
Privacy Mask

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.



Virtual Camera

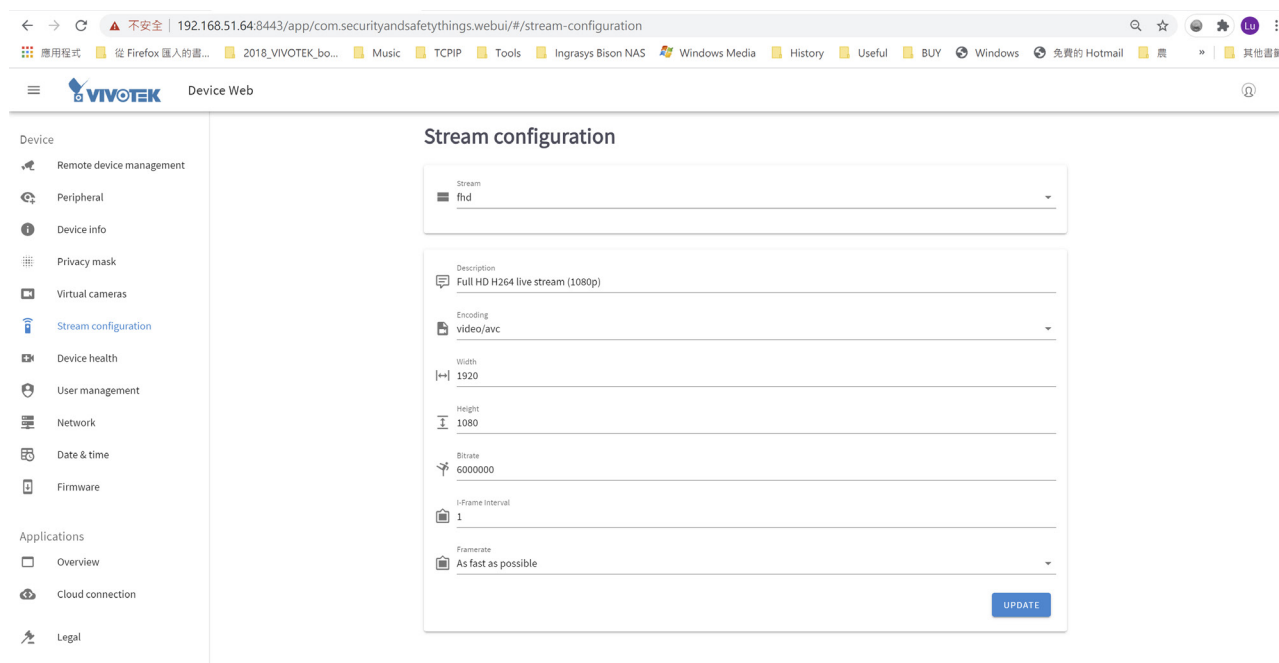
Allows the creation of additional sub-stream(s) which can cover a certain zone of interest in the camera's field of view. The sub-streams are used for video analytics on apps.



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.



Device Health

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

The screenshot shows the VIVOTEK Device Web interface. The main content area is titled "Device health" and includes a "REFRESH" button. The metrics are as follows:

Metric	Value	Total
CPU	13.9 %	Average in the last 60 s
RAM	926.4 MB	3689.9 MB
Storage	98.0 MB	5215.7 MB
Temperature	Unknown	

Connectivity information:

Type	Link speed	Sending speed	Receiving speed
ETHERNET	97.7 Mb/s	1.0 kb/s	0.0 kb/s

A "SHOW SYSTEM APPS" button is located below the connectivity section.

User Management

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

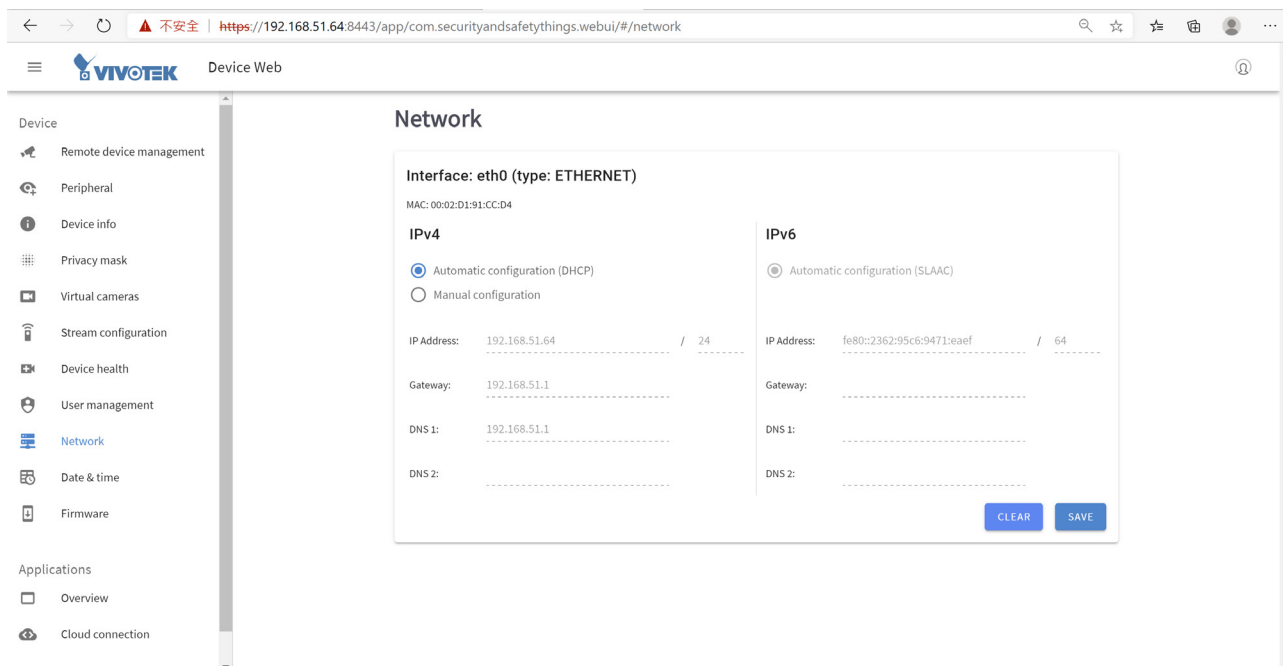
The screenshot shows the VIVOTEK Device Web interface with the "User management" page. A "Create New User" dialog box is open, showing the following details:

- Username:** power_user
- Password:** [Redacted]
- Confirm password:** [Redacted]
- Require password change on first login
- User Permissions:**
 - web
 - streaming
 - onvifUser
 - onvifAdmin
 - userManagement
 - factoryReset
 - developerMode

Buttons for "CREATE" and "CLOSE" are visible at the bottom of the dialog box.

Network

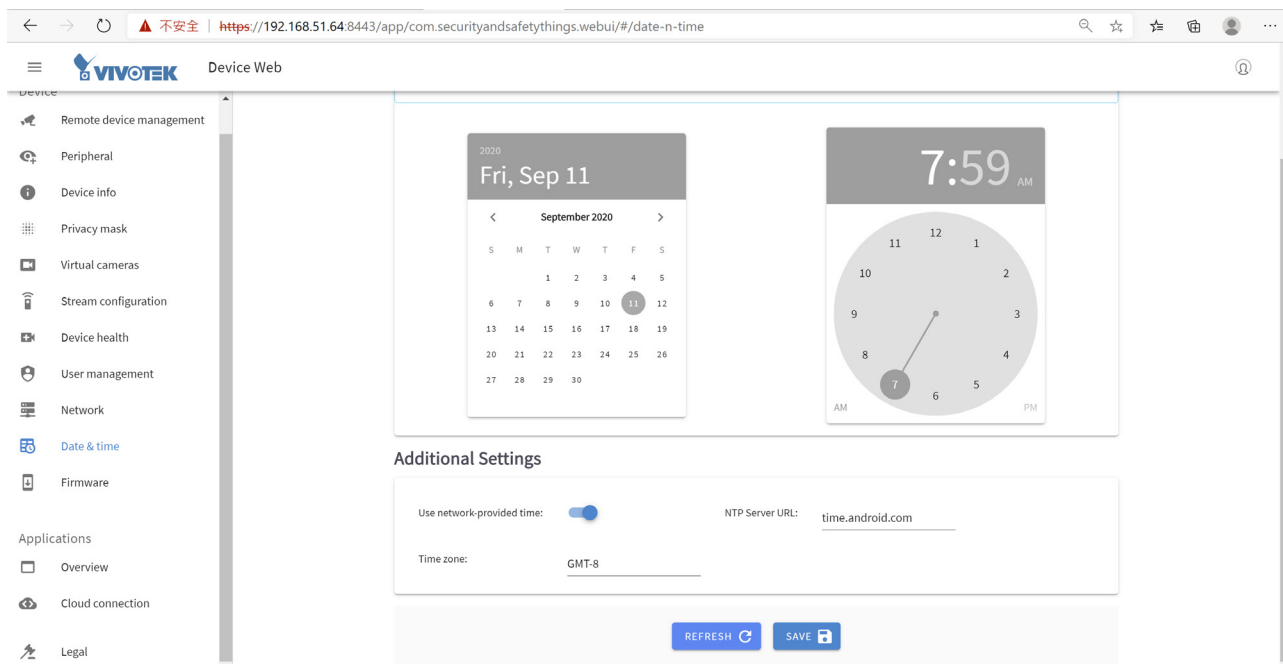
By default, the AI box has the network setup to receive the IP address via DHCP. On this page you can change different network parameters, disable the DHCP and set a specific IP.



Date & Time

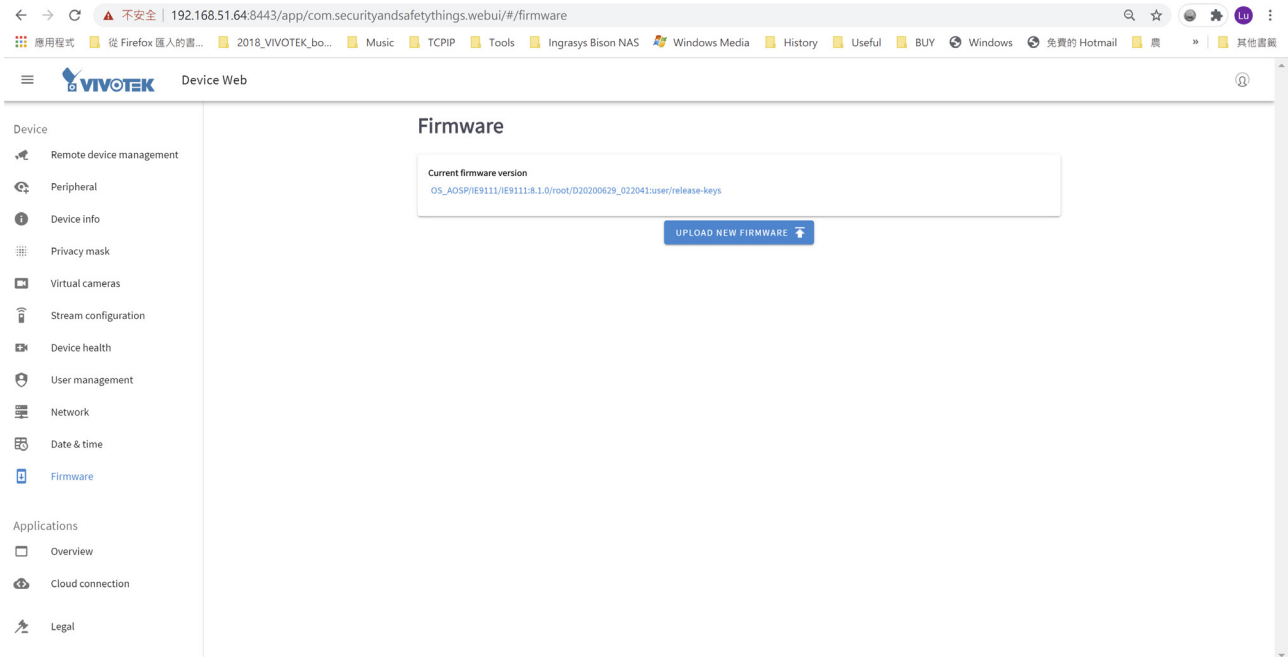
This page allows the user to configure the current date/time on the device, synchronize with computer time and also to enable network time synchronization via an NTP server.

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



Firmware

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



The screenshot shows a web browser window displaying the VIVOTEK Device Web interface. The browser's address bar shows the URL: `192.168.51.64:8443/app/com.securityandsafetythings.webui/#/firmware`. The page title is "Firmware".

On the left side, there is a navigation menu with the following items:

- Device
 - Remote device management
 - Peripheral
 - Device info
 - Privacy mask
 - Virtual cameras
 - Stream configuration
 - Device health
 - User management
 - Network
 - Date & time
 - Firmware
- Applications
 - Overview
 - Cloud connection
 - Legal

The main content area displays the "Firmware" section. It shows the "Current firmware version" as `OS_AOSP|E9111|E9111:8.1.0/root/D20200629_022041:user/release-keys`. Below this information is a blue button labeled "UPLOAD NEW FIRMWARE" with an upward-pointing 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 Device Web interface. The left sidebar contains navigation options: Device (Remote device management, Peripheral, Device info, Privacy mask, Virtual cameras, Stream configuration, Device health, User management, Network, Date & time, Firmware), Applications (Overview, Cloud connection, Legal), and a 'GET APPS' button. The main content area is titled 'Overview' and shows a table of installed applications:

Name	Version	ANRs	Crashes	Kills	CPU	RAM	Status
FaceBiometrics Pro App interface and configurations	Expires 1.0	0	0	0	35.6 %	79 MB	Running 29 day(s) left
VAST2 Data Magnet App interface and configurations	8.1.0	0	0	0	0.0 %	10 MB	Running

Below the table is the 'App frame rate information' section:

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

A 'GET APPS' button is located at the bottom of the main content area.

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 is similar to the previous one but includes a hand icon pointing to the 'App interface and configurations' link for the VAST2 Data Magnet application in the table. The table data is as follows:

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

The 'App frame rate information' table and 'GET APPS' button are also visible.

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.

Data Magnet Setting

VAST2 Server IP
192.168.51.211

VAST2 DataMagnet Port
3443

Data Source Name
IE server

VAST2 Username
admin

[RESET PASSWORD](#)

Select Event Source

FaceBiometrics Pro

To: (name) 0 / 24

[UPDATE](#) [REMOVE](#)

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

Device management

Settings | **Device management**

Cameras

Sites

POS

I/O

DI/DO devices

Data magnet

External devices

Search devices

IE

IE9111-O

Third party data source

Name: IE

Port: 3443 Use default port

Data source authorization

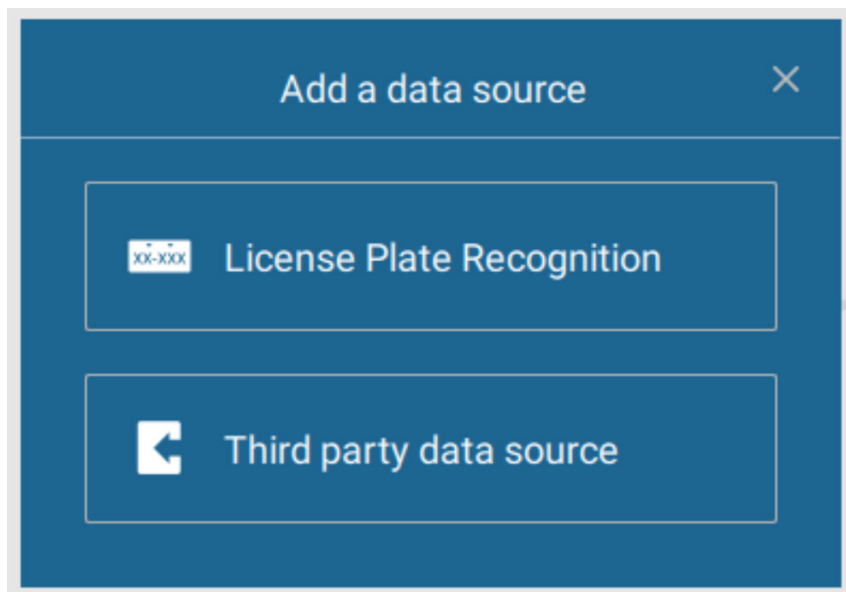
Related camera: 1 camera

[Apply](#) [Cancel](#)

在 這裡輸入文字來搜尋

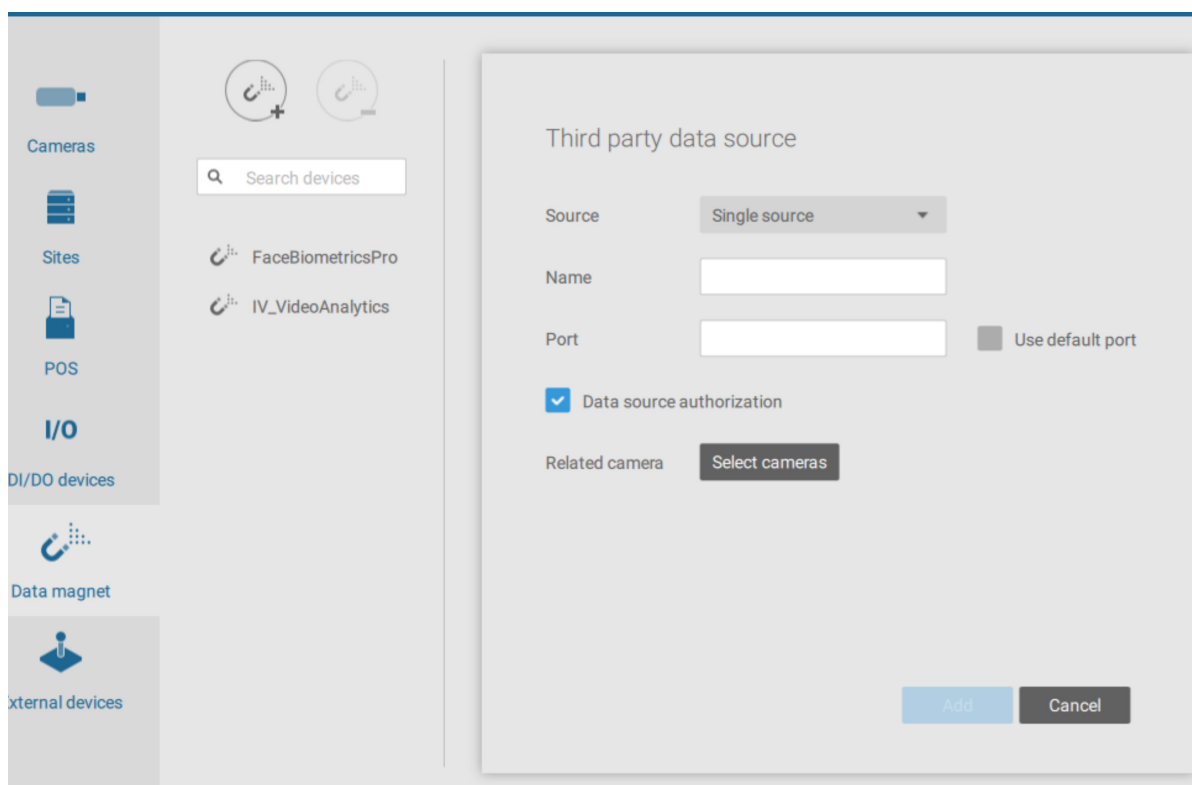
上午 09:47
2020/9/16

7. Select Third party data source.

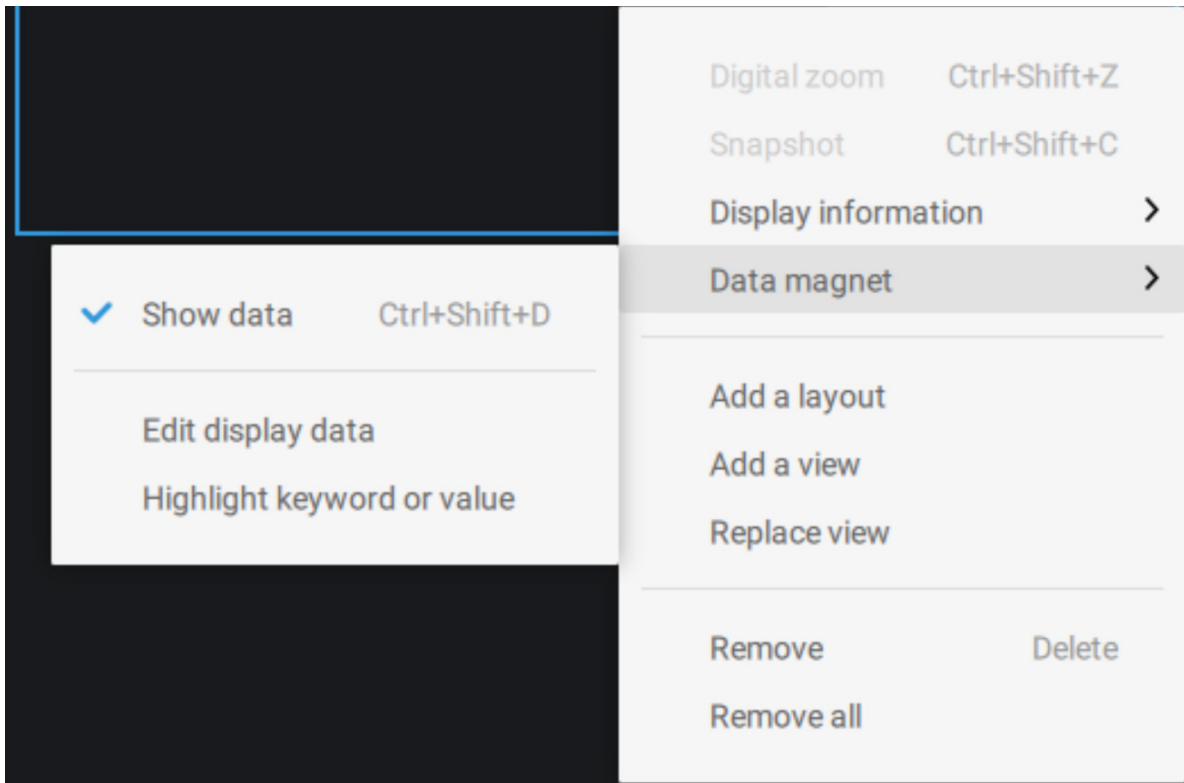


8. Enter the Data Source Name, port (usually 3443), select the associated camera, and click Add.

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

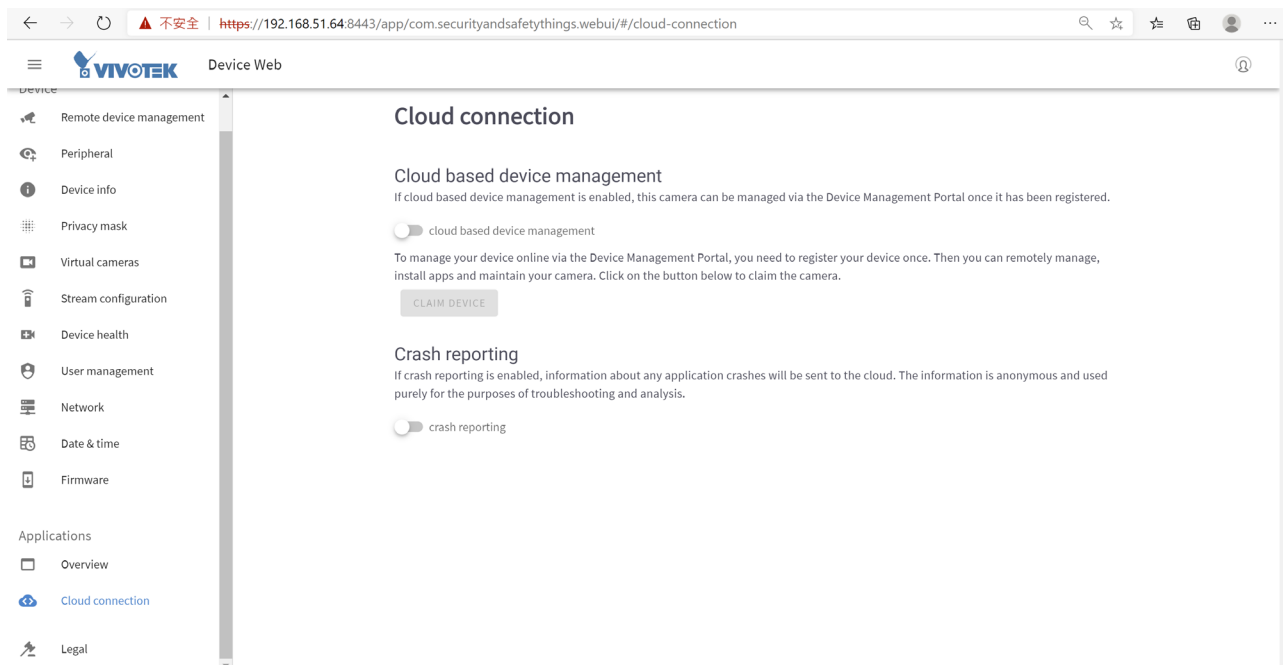


9. You can then right-click on a VAST2 view cell to display the Data magnet data. The analytics detection results can display along with the live video.



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:

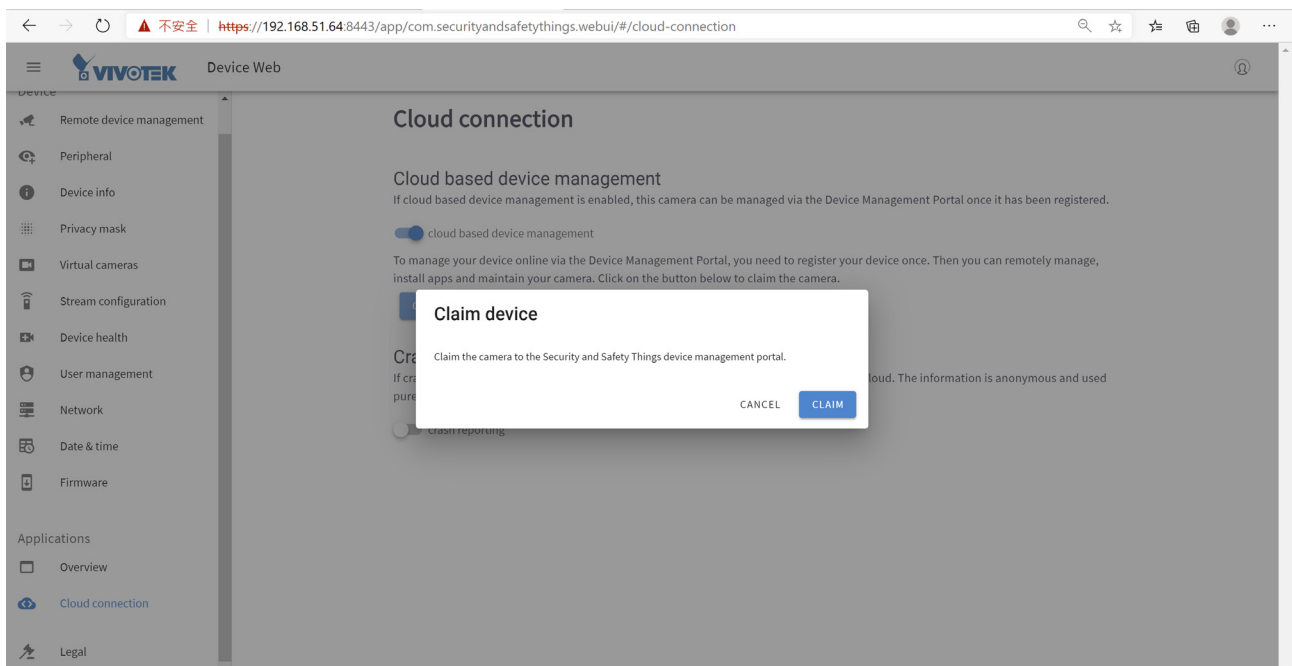
- You have an account on the S&ST Device Management Portal.
- Cameras have a non-restricted access to the Internet.
- Your camera has a valid certificate. Please verify this by accessing the camera using a web browser and go to the Device info page. Then check if a Device ID is present:



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

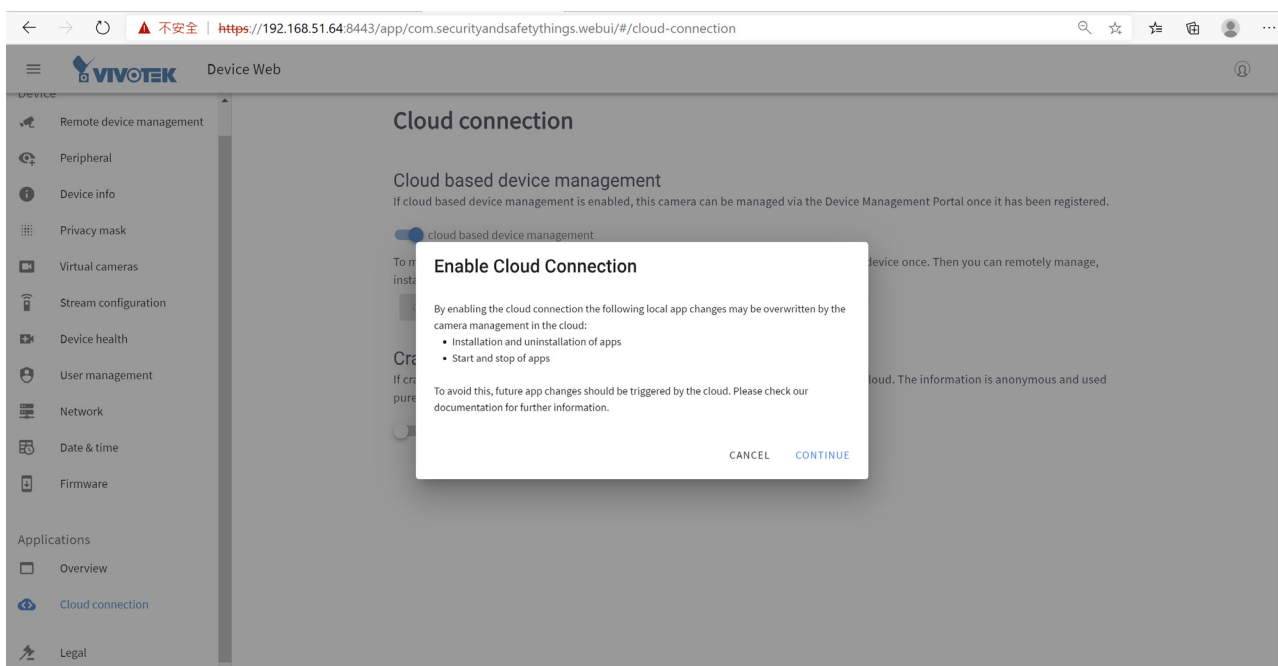
Proceed with the following for connecting the camera to the Device Management Portal:

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.”



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

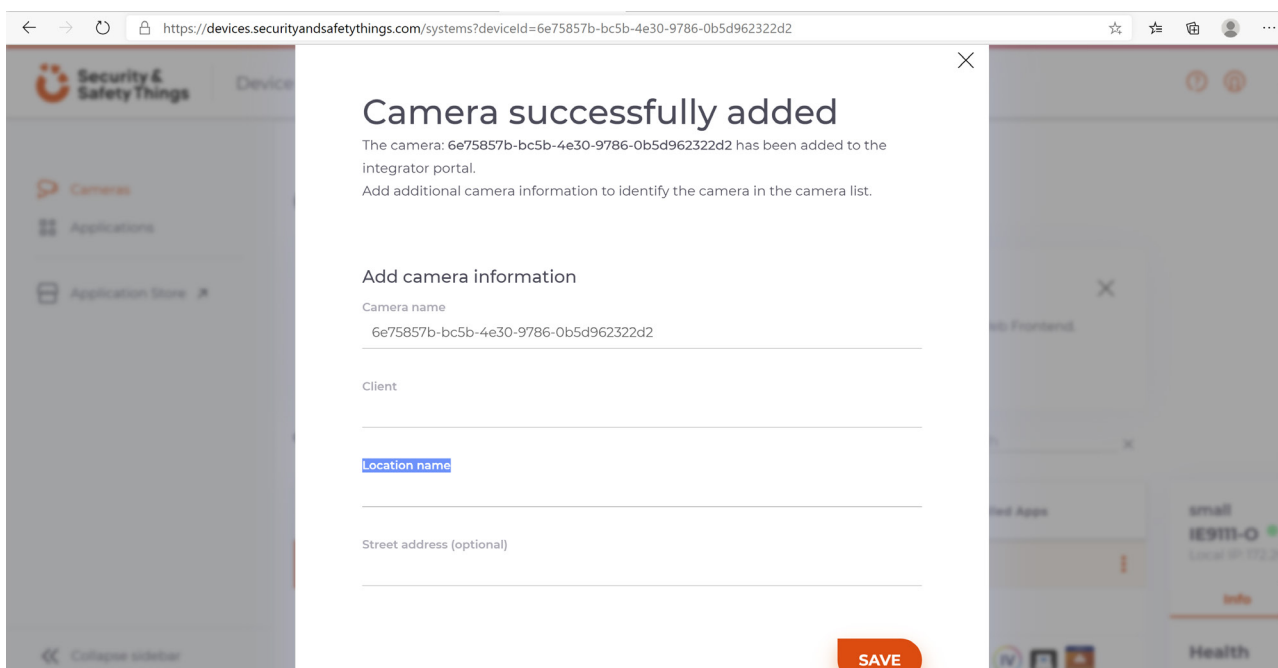
Click Continue.



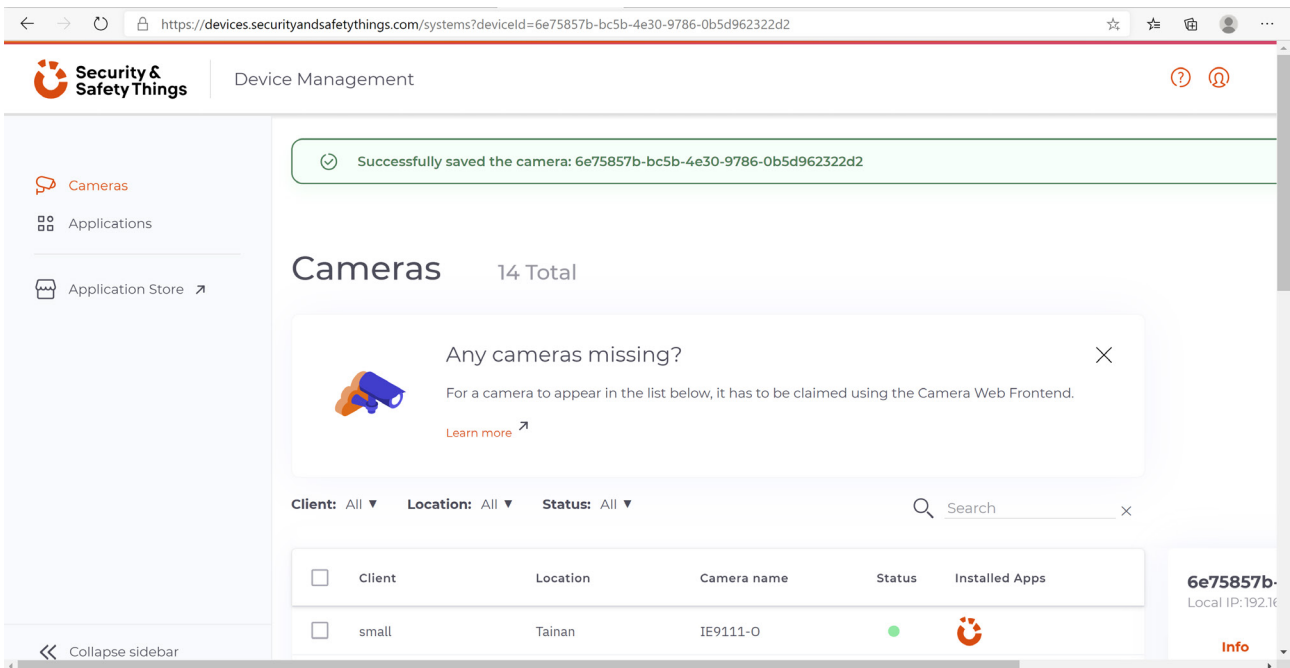
On the Device Management Portal page, you can enter some additional information regarding the device:

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

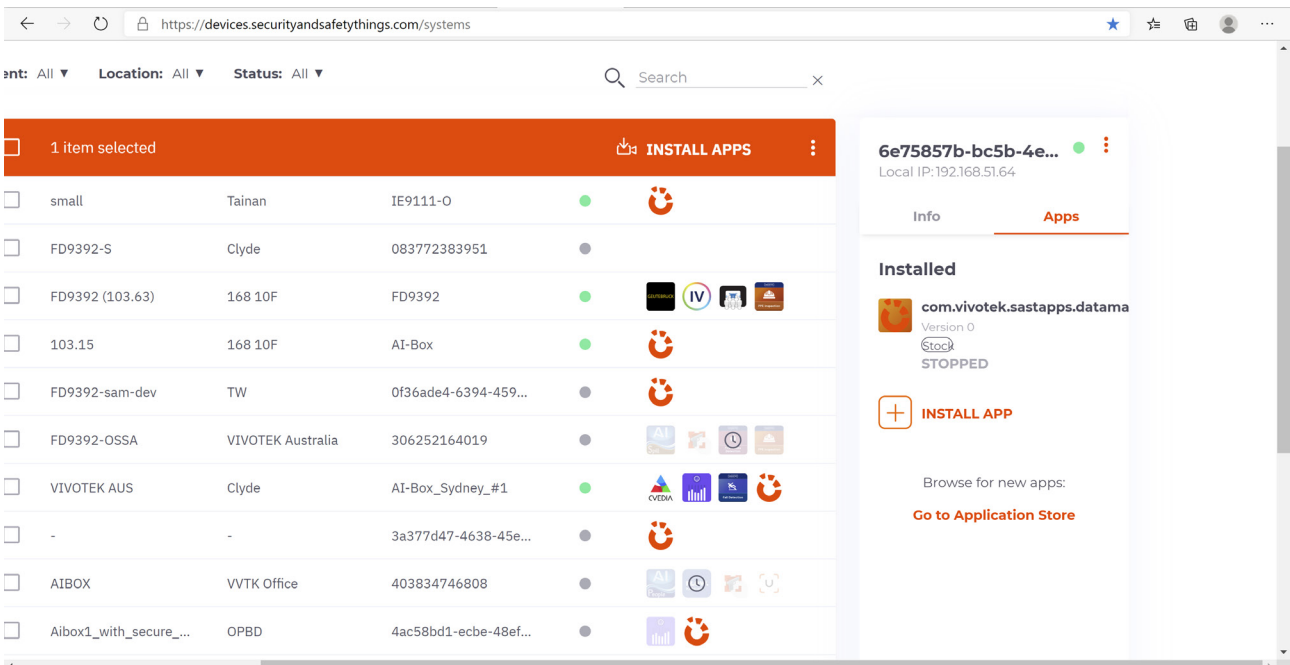
Click the SAVE button in order to save the changes and your camera will appear in the list of cameras on the Device Management Portal.



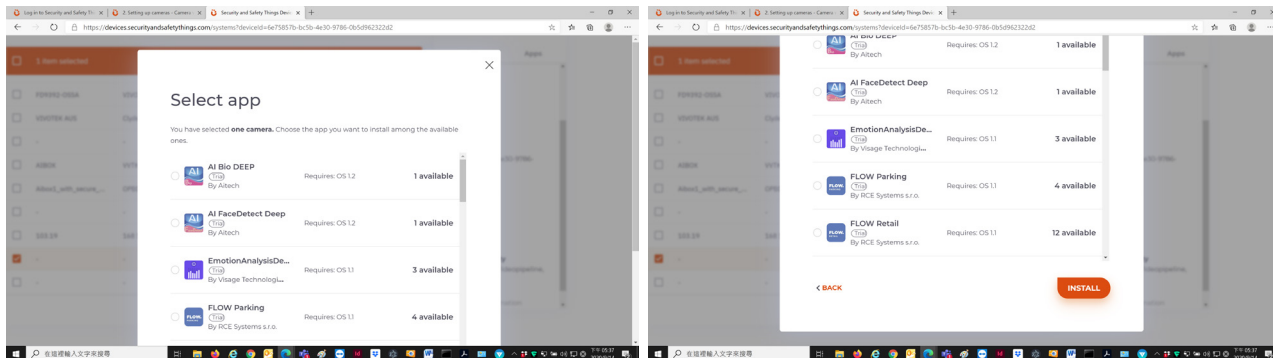
On the Device Management Portal page, you can see all connected devices/cameras.



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/let/make2fs.conf](#)
- [/recovery/root/bin/lsblk_file_contexts](#)
- [/recovery/root/bin/lsblk_recovery_contexts](#)
- [/recovery/root/bin/lsblk_file_contexts](#)
- [/recovery/root/bin/lsblk_recovery_contexts](#)
- [/recovery/root/bin/recovery](#)
- [/recovery/root/sepolicy](#)
- [root.img](#)
- [system/sepolicy/AdbAuthorization/AdbAuthorization.apk](#)
- [system/sepolicy/AdbAuthorization/AdbAuthorization.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.