

Quick start guide



NVIP-4Q-6101/PIR/W

NoVus

IMPORTANT SAFEGUARDS AND WARNINGS

THE PRODUCT MEETS THE REQUIREMENTS CONTAINED IN THE FOLLOWING DIRECTIVES:



DIRECTIVE 2014/30/EU OF THE EUROPEAN PARLIMENT AND OF THE COUNCIL of 26 February 2014 on the harmonization of the laws of the Member States relating to electromagnetic compatibility (OJ L 96, 29.3.2014, p. 79–106, with changes).



DIRECTIVE 2012/19/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2012 on waste electrical and electronic equipment WEEE) (OJ L 197, 24.7.2012, p. 38–71, with changes).



DIRECTIVE 2011/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (OJ L 174, 1.7.2011, p. 88–110, with changes).

COMMISSION DELEGATED DIRECTIVE (EU) 2015/863 of 31 March 2015 amending Annex II to Directive 2011/65/EU of the European Parliament and of the Council as regards the list of restricted substances.

DIRECTIVE (EU) 2017/2102 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 November 2017 amending Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Exclusion of liability in the event of damage to data contained on disks or other devices or media:

The manufacturer is not liable in the event of damage or loss of data contained on disks or other devices or carriers during the operation of the Product.

Obligation to consult the Manufacturer before performing any action not provided for in the instruction manual or other documents:

Before performing an action that is not provided for a given Product in the user manual, other documents attached to the Product or does not result from the normal purpose of the Product, it is necessary, under pain of exclusion of the Manufacturer's liability for the consequences of such action, to contact the Manufacturer.



Pictures in this publication showing camera views can be simulations. Actual camera images may vary depending on the type, model, settings, observation area, or environmental conditions.

IMPORTANT SAFEGUARDS AND WARNINGS



Before using the device, read the instruction manual in order to ensure proper and safe operation of the device. Failure to comply with the instructions may lead to damage to the device and/or safety violations.



The user may not repair the device himself. Repairs and maintenance of the device may only be performed by qualified service personnel.



The device, which is an element of a professional CCTV system used for supervision and control, is not intended for self-assembly in households by persons without specialist knowledge.

eng

1. Please read this manual carefully before installation and operation;
2. Please keep this manual for the lifespan of the device in case referring to the contents of this manual is necessary;
3. It is necessary to comply with the safety requirements described in the manual, as they have a direct impact on the safety of users and the durability and reliability of the device;
4. All activities performed by installers and users must be carried out as described in the manual;
5. The device should be disconnected from power sources during maintenance procedures;
6. It is not allowed to use any additional devices, components or accessories not provided for and not recommended by the manufacturer;
7. Do not install this device in places where proper ventilation cannot be provided (e.g. closed cabinets, etc.), as this may cause heat build-up and may result in damage;
8. Do not place the device on unstable surfaces. Installation must be carried out by qualified personnel with appropriate permissions in accordance with the recommendations provided in this manual;
9. The device may be powered only from sources with parameters compliant with those indicated by the manufacturer in the technical data;



As the product is constantly improved and optimised, some of its parameters and functions may have changed from those described in this manual. If in doubt, please refer to the user manual at **www.novuscctv.com**

The user manual located at www.novuscctv.com is always the most up-to-date version.

FOREWORD INFORMATION

1. TECHNICAL SPECIFICATION

IMAGE	
Image Sensor	4 MPX CMOS sensor 1/3" SmartSens
Number of Effective Pixels	2568 (H) x 1448 (V)
Min. Illumination	0.01 lx/F2.1 - color mode, 0 lx (IR on) - B/W mode
Electronic Shutter	auto: 1/3 s ~ 1/100000 s
Digital Slow Shutter (DSS)	up to 1/3 s
Wide Dynamic Range (WDR)	yes (double scan sensor), 120dB
Digital Noise Reduction (DNR)	2D, 3D
Highlight Compensation (HLC)	yes
Back Light Compensation (BLC)	yes
Reduction of image flicker (Antiflicker)	yes
LENS	
Lens Type	fixed focal, f=2.1 mm/F2.1
DORI	
DORI (Detection, Observation, Recognition, Identification)	for f = 2.1mm - D: 36m, O: 14m, R: 7m, I: 4m
DAY/NIGHT	
Mode	day/night switching: mechanical IR cut filter
Switching Mode	auto, manual, time, external
Switching Level Adjustment	yes
Switching Delay	2 ~ 6000 s
Visible Light Sensor	yes
NETWORK	
Stream Resolution	2560 x 1440 (QHD), 2304 x 1296, 1920 x 1080 (Full HD), 1280 x 720 (HD), 704 x 576, 352 x 288 (CIF), 480 x 240
Frame Rate	30 fps for each resolution
Multistreaming Mode	number of streams: 2 (main stream, sub stream)
Video/Audio Compression	H.264, H.265, MJPEG/G.711
Number of Simultaneous Connections	max. 2
Bitrate	for H.264 : 64 kbps - 6144 kbps for H.265 : 64 kbps - 6144 kbps
Network Protocols Support	HTTP, IPv4/v6, UDP, HTTPS, FTP, DHCP, DDNS, NTP, RTSP, UPnP, QoS, IEEE 802.1X, PPPoE, SMTP, P2P, HTML5, RTMP
ONVIF Protocol Support	Profile G/S/T
Camera Configuration	from Edge, Firefox, Chrome, Opera browser languages: Polish, English, and others
Compatible Software	NOVUS MANAGEMENT SYSTEM VSS, NOVUS MANAGEMENT SYSTEM AC
Mobile applications	ipGO 6 (iPhone, Android)
WIFI	
Network standard	IEEE802.11b, g, n
Band	2.4GHz
Security	WEP, WPA-PSK/WPA2-PSK
Transmission range	up to 50 m
Antenna	built-in, omnidirectional

FOREWORD INFORMATION

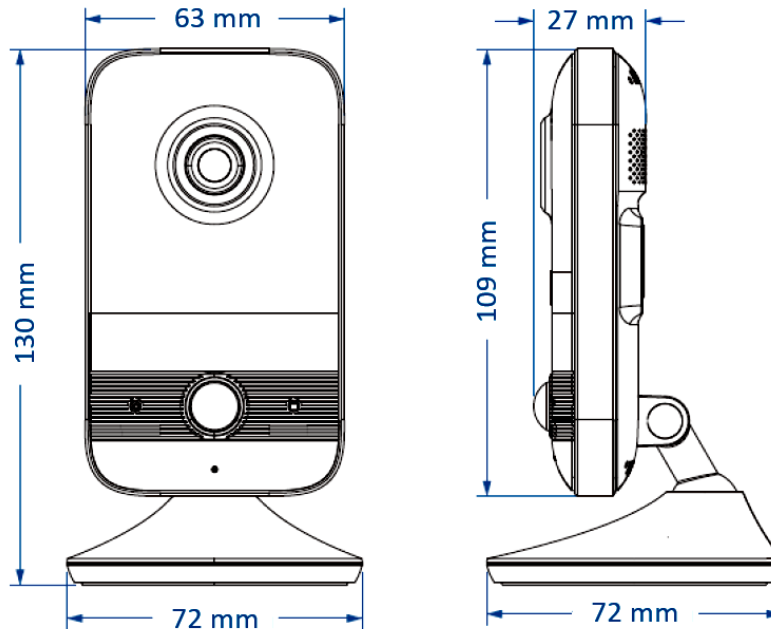
VIDEO ANALYTICS	
Functions	tamper, line cross, pedestrian detection, intrusion detection, smart motion detection with objects distinguishing
OTHER FUNCTIONS	
Security	IEEE 802.1X support, HTTPS support, MAC/IP address filtering, force change of default password, compliance with the EN18031 standard defining cybersecurity standards for radio and IoT devices
Privacy Zones	4 video mask type: single color
Motion Detection	yes
PIR detector	range up to 5 m
Region of interest (ROI)	8
Image Processing	sharpening, mirror effect, vertical flip
Prealarm/Postalarm	up to 6 s/up to 120 s
System Reaction to Alarm Events	e-mail with attachment, saving file on FTP server, saving file on SD card, alarm output activation, playback of the audio message
Restoring default settings	via web browser, using reset button, via NMS IPTool software
IR LED	
LED Number	1
Range	10 m
Smart IR	yes (hardware support)
INTERFACES	
Audio Input/Output	built-in microphone/speaker
Alarm Input/Output	1 (NO/NC)/1 relay type (max. 12VDC/300mA)
Network Interface	1 x Ethernet - RJ-45 interface, 10/100 Mbit/s 1 x Wireless (Wi-Fi)
Memory Card Slot	microSD - capacity up to 128GB
INSTALLATION PARAMETERS	
Dimensions (mm)	63 (W) x 109 (H) x 27 (L) with bracket: 72 (W) x 130 (H) x 72 (L)
Weight	0.2 kg
Enclosure	plastic, black and white, wall mount/base in-set included Enclosure type: 4Q
Power Supply	12 VDC, PoE (IEEE 802.3af, Class 3)
Power Consumption	3 W, 4 W (IR illuminator on)
Operating Temperature	-20°C ~ 50°C
Humidity	max. 95%, relative (non-condensing)



The declared range of the Wi-Fi network is based on laboratory research and relates to open spaces. It should be noted, that the materials used for the construction of houses and flats, wall thickness and electromagnetic field conditions in the immediate surroundings may affect the range of the network.

START-UP AND INITIAL CONFIGURATION

1.1. Camera dimensions



1.2. Package contents

After you open the package make sure that the following elements are inside:

- IP camera
- Accessories bag
- Quick start guide

If any of this elements has been damaged during transport, pack all the elements back into the original box and contact your supplier for further assistance.

Caution:

If the device was brought from a location with lower temperature, please wait until it reaches the temperature of location it is currently in. Turning the device on immediately after bringing it from a location with lower ambient temperature is forbidden, as the condensing water vapour may cause short-circuits and damage the device as a result.

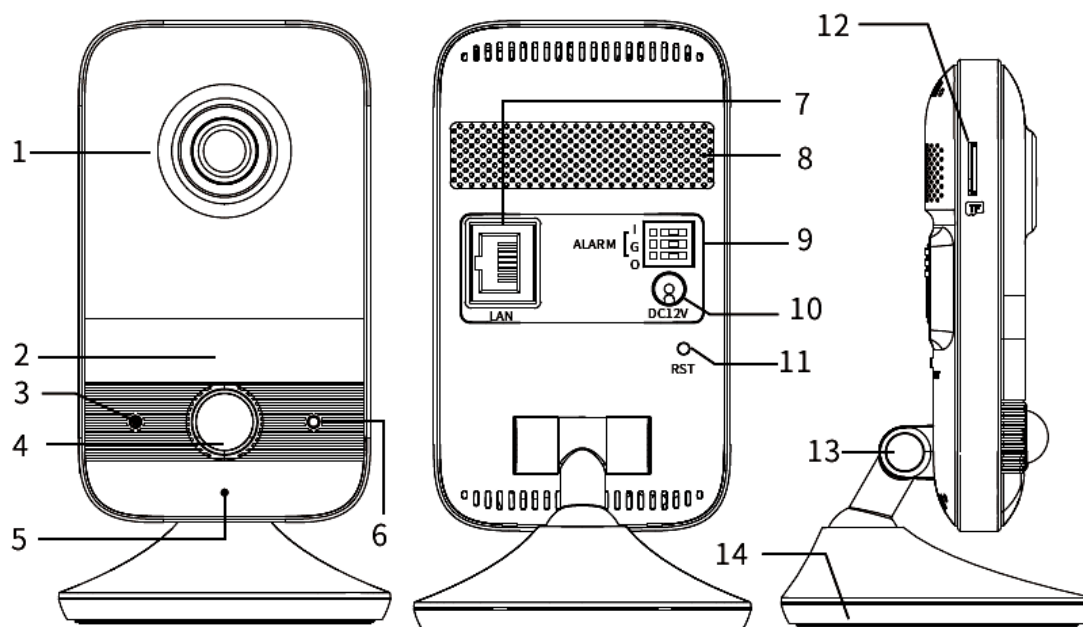
Caution:

Before starting the device familiarize yourself with the description and the role of particular inputs, outputs and adjusting elements that the device is equipped with.

START-UP AND INITIAL CONFIGURATION

2. START-UP AND INITIAL CONFIGURATION

2.1. Description of camera components and connectors



1	Lens	8	Speaker
2	IR LED (infrared illuminator)	9	Alarm input/output connectors
3	Microphone	10	12VDC power socket
4	PIR detector	11	RESET button
5	Status light	12	Memory card slot
6	Light sensor	13	Camera position adjustment
7	LAN socket	14	Base

Status Light Options

Red, solid	Starting	Red, flashing	Network disconnected
Blue, solid	Setting up WiFi connection	Blue, flashing	Camera not activated, Activation in progress, Alarm
Green, solid	Working	Green, flashing	Firmware update

START-UP AND INITIAL CONFIGURATION

2.2. Power supply connection

The camera can be powered from AC or DC power supplies available on the market, provided that it meets the technical requirements of the camera. The power supply must provide a stabilized DC voltage of 24V, must allow for the consumption of at least 10W of power, and must have a DC 2.5/5.5 cylindrical power plug with the correct polarity of the contacts:



It is also possible to power the camera via the RJ45 network socket, using PoE technology (IEEE 802.3af, Class 3).

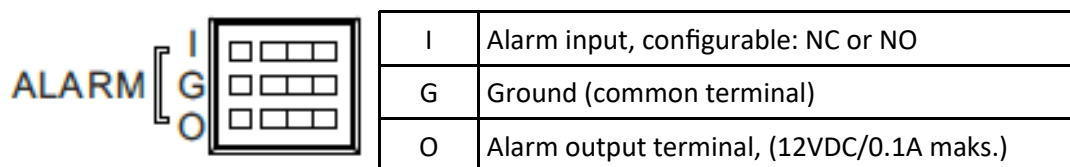
Caution!

Do not use power supplies and POE adapters that do not comply with the IEEE 802.3af standard, the so-called "passive POE" power supplies. Damage resulting from the use of an unsuitable adapter is not covered by the warranty!

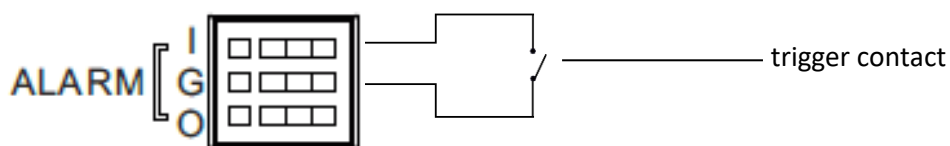
2.3. Connection of alarm input/output

The camera has one alarm input and output. The alarm input is used to connect a device such as a motion detector, button, reed switch or photocell. Violation of the input will trigger the alarm and activate the previously programmed action.

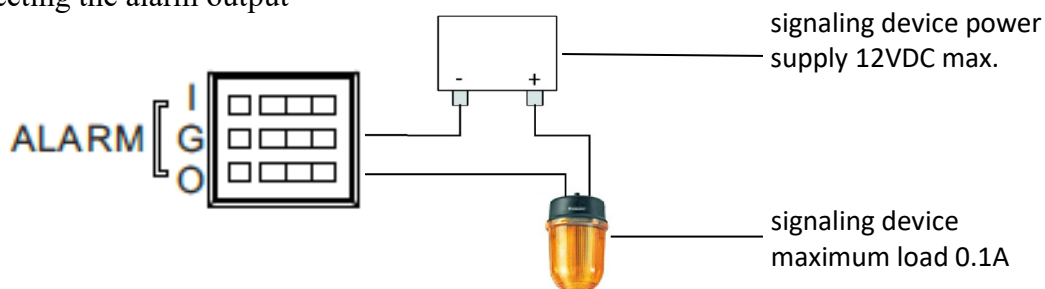
The alarm output enables connection of an external siren and implementation of automatic control functions, such as switching on light.



Connecting the alarm input



Connecting the alarm output



START-UP AND INITIAL CONFIGURATION

2.4. Camera mounting

The camera design allows flexible selection of the place of attachment / installation. The camera can work when placed on any flat surface or be hung using mounting holes in the foot.

To mount the camera in a hanging position, we recommend you follow the following guidelines:

- Place the template where you want to install the camera. Then drill the holes according to the template.
- Insert the dowels into the holes and tighten the screws. The screws should protrude a few millimeters above the wall surface.
- Route and connect the cables to the camera.
- Hang the camera by the mounting base on the screws and make sure it is securely fastened. Then adjust the camera position.

eng

**Caution:**

The camera is designed for indoor use in living quarters. Using it outdoors, or in rooms with high humidity such as swimming pools, bathrooms, laundries, etc. may cause the camera to malfunction or damage.

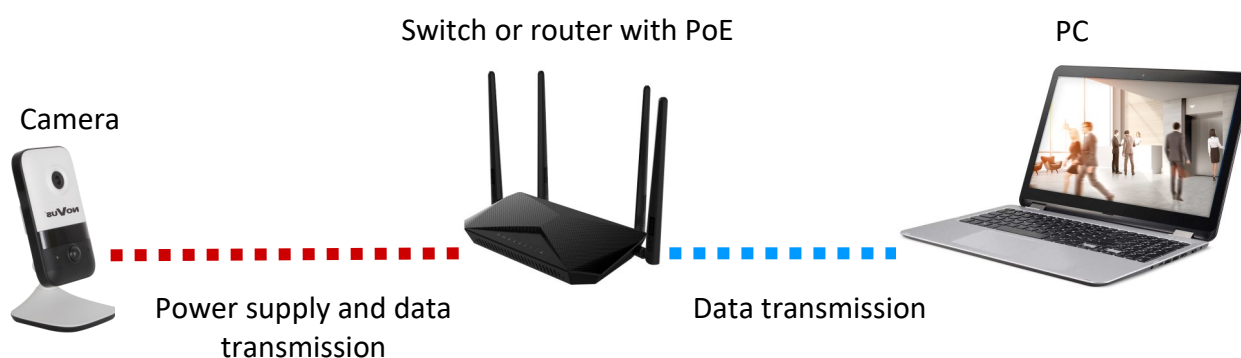
START-UP AND INITIAL CONFIGURATION

2.5. Starting the camera

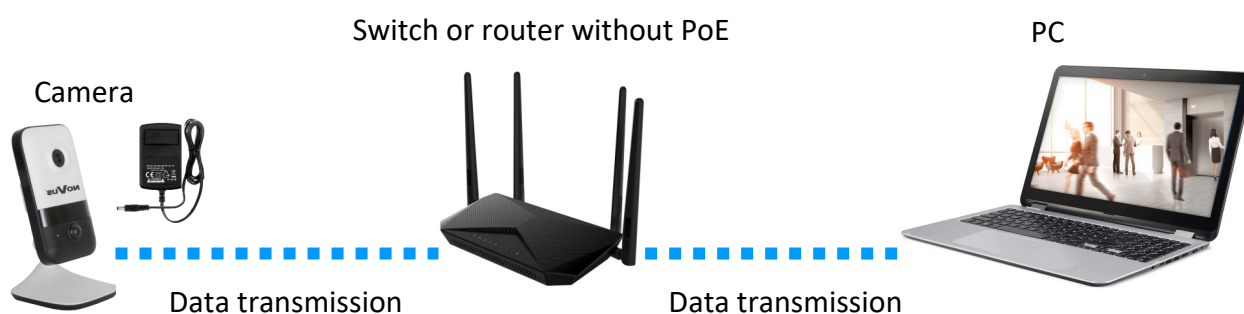
2.5.1 Starting with connecting the camera to a wired LAN network

To start the camera, connect the Ethernet cable to the camera's network socket, and the other end to the switch or router. If your switch or router is not a PoE device, you should also connect a 12VDC power supply to the camera. The following schemes may help:

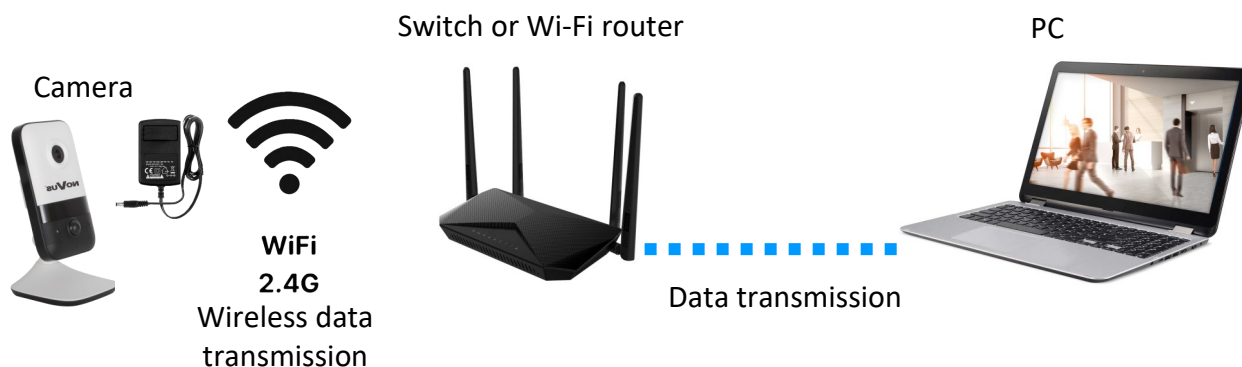
- Wired connection using a PoE switch or router:



- Wired connection using a switch or router without PoE and 12VDC power supply:



2.5.2 Connecting the camera to a Wi-Fi wireless network



After making connections and starting the camera (which takes a few minutes) it is possible to connect to the camera.

START-UP AND INITIAL CONFIGURATION

2.6. Security recommendations for network architecture and configuration

WARNING!

Below are shown security recommendations for network architecture and configuration of CCTV systems that are connected to the Internet to reduce the risk of unauthorized interference with the system by a third party.

1. Absolutely change the default passwords and user names (if the device gives this possibility) of all applied network devices (recorders, cameras, routers, network switches, etc.) to the severely complexity password. Use lowercase and uppercase letters, numbers, and special characters if there is such possibility.

2. Depending on the available functionality in the order to restrict access to the used network devices at the administrator account level, it is recommended to configure the users accounts accordingly.

3. Do not use DMZ function (Demilitarized zone) in your router. Using that function you open the access to recorder system from the Internet on all ports, which gives possibility for an unauthorized interference with the system.

Instead of DMZ use port forwarding redirect only the ports which are necessary for the performance of the connection (detailed information about ports of communication in different models of recorders, cameras, etc. can be found in the operating instructions).

4. Use routers with firewall function and make sure it is enabled and properly configured.

5. It is recommended to change the default network communication port numbers of used devices if there is such possibility.

6. If used network devices has a UPnP feature and it is not used, turn it off.

7. If used network devices has a P2P feature and it is not used, turn it off.

8. If used network devices support HTTPS protocol for connection, it is recommended to use it.

9. If used network devices support IP filtering for authorized connections function, it is recommended to use it.

eng

NETWORK CONNECTIONS TO THE CAMERA

3. NETWORK CONNECTIONS TO THE CAMERA

3.1. Connecting to the camera for the first time using Wi-Fi and a mobile device with the ipGO6 app



To activate the camera with a Wi-Fi connection, you must have a mobile device (smartphone, tablet) with the ipGO6 app installed. Before starting the operation, ensure that the camera and mobile device are within range of the same Wi-Fi network. Make sure the mobile device connects to the Wi-Fi network in the 2.4GHz band, as the camera only operates in this band.

eng

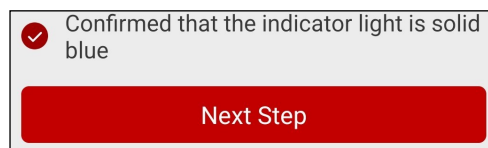


When starting the camera with a Wi-Fi connection, the camera can be powered from a 12V power supply or from a PoE switch/router.

First, download the ipGO6 app to your mobile device (from the Play Store for Android devices or the Apple Store for iOS devices). After installing the app, log in (or create an account).

Then go to the "Device List" tab and tap the "Options" button  in the upper right corner of the screen, then the "Add Device" option. A QR code scanning window will open. Use it to scan the code located on the camera's base. After a successful scan, the device adding window will open, displaying an image of the camera and its P2P code. Then, tap the "Add" button to proceed.

Next, make sure the camera's status light is flashing blue. Confirm this on your mobile device and tap "Next Step."

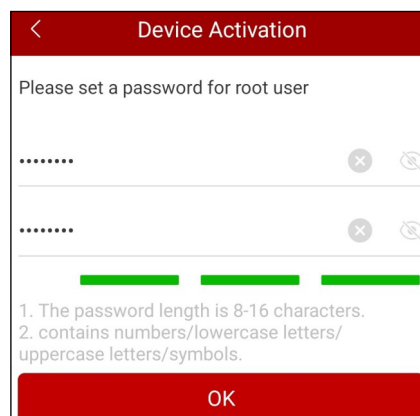


In the next window, enter your Wi-Fi network password and tap "Next Step." Another window will open, allowing you to connect to the camera you're adding.



At this stage, the camera is activated. The mobile device connects to the hotspot enabled by the camera to set the user's password.

After connecting to the camera's hotspot, enter and confirm the camera's login password for the administrator (**root**) account in the next window.

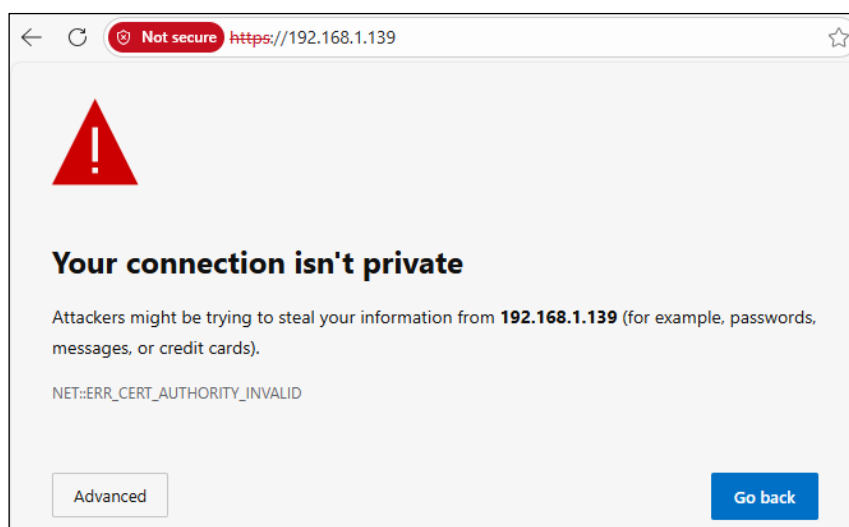


After entering the password, the camera will be activated and will appear in the ipGO6 app devices list.

NETWORK CONNECTIONS TO THE CAMERA

3.2. Connecting to the camera for the first time using a wired LAN or wireless Wi-Fi network and a computer with a web browser

Because the camera meets the EN 18031 standard, which defines basic cybersecurity and quality requirements for wireless and IoT devices, including Wi-Fi cameras, it connects to a web browser using the HTTPS protocol. Therefore, when entering the camera's IP address in the browser's address bar, precede it with "https://." Once connected, the browser will display a security alert, similar to the one below, indicating the connection is not secure:



eng



The alert is displayed because the camera has a private, untrusted security certificate installed, which the browser can't verify. Don't worry - at this stage, this is normal behavior, and the camera's certificate is sufficient to ensure the confidentiality of the connection.



If necessary, user can install a trusted security certificate themselves, which will not trigger browser alerts. The certificate can be installed in the "Settings -> Network -> HTTPS" menu.

In the alert window, click the "Advanced" button or the "Help me understand" link or similar. Additional security information will be displayed:

This server couldn't prove that it's **192.168.1.139**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Continue to 192.168.1.139 \(unsafe\)](#)

Click the "Continue to (IP address here) (unsafe)" link to connect to the camera.



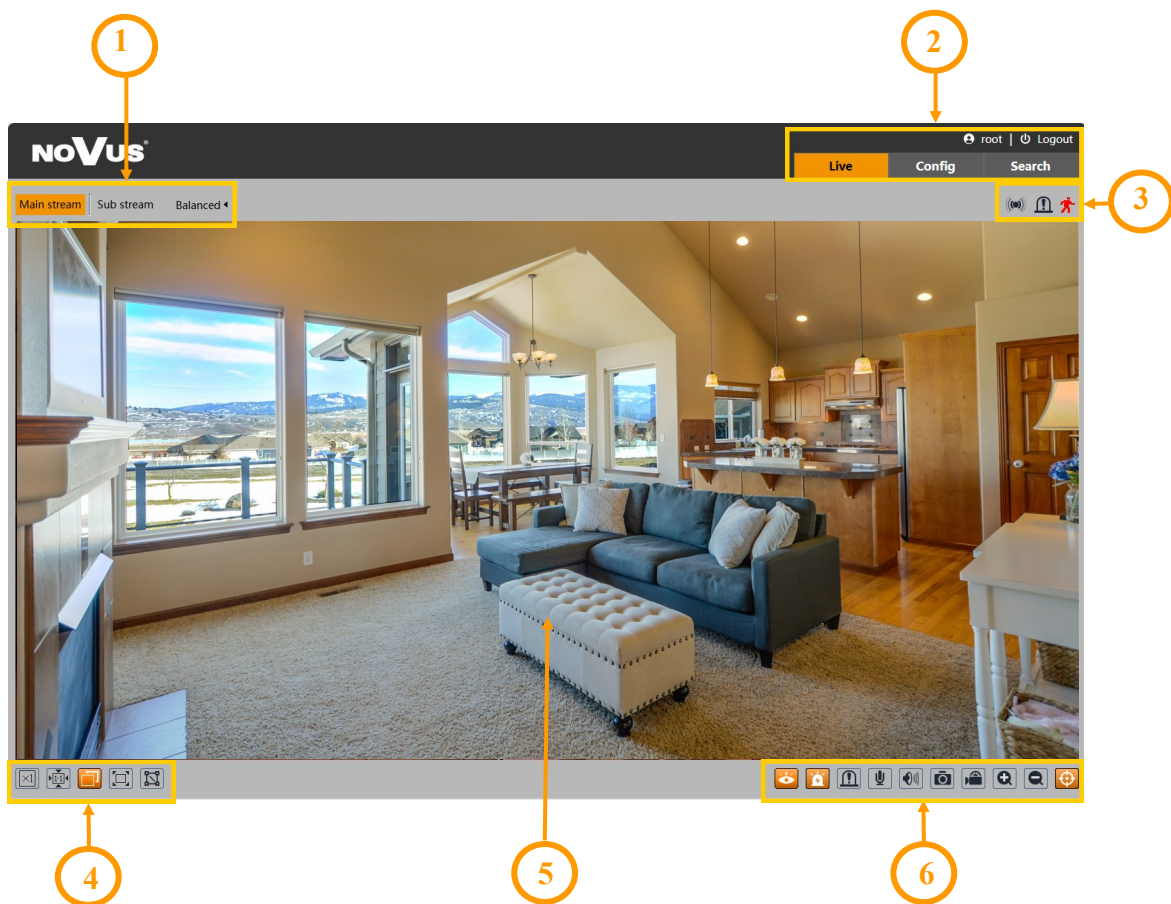
After clicking on the link, the browser will remember the user's decision and will automatically insert the "https://" protocol before the IP address when connecting to the camera in the future and will not display an alert, although the "Not Secure" warning will still be visible in the address bar.

NETWORK CONNECTIONS TO THE CAMERA

Once connected, a privacy policy window will appear, which you must accept by checking the box and pressing "Read." The camera will then display a time zone configuration window, followed by a security question selection window, which allows you to regain access to the camera if you forget the administrator password without having to reset the device. Next, an activation window will appear, where you can define the administrator password (and the password for ONVIF account). After completing these steps, the camera will display a login screen, where you must enter the administrator account name (root by default) and the configured password.

4. USING AND CONFIGURING

4.1. Remote view window



1. Selection of the stream to be displayed in the preview window and set the buffer size of the camera.

2. Camera operation mode selection and configuration buttons:

- | | |
|--------|---|
| Live | - enables the live stream preview |
| Config | - displays the camera configuration panel |
| Search | - displays the panel for searching and playing back recordings from the memory card |
| root | - information about the logged in user |
| Logout | - logs out of the camera |

RESTORE FACTORY SETTINGS

3. Alarm event icons display panel:



From left to right: alarm output activation, memory card recording, color change, sabotage, scene change, people detection, PIR detection, alarm input alarm, motion detection alarm. The occurrence of a given event is signaled by a flashing red color.

4. Image adjusting buttons:



From left to right: original size, original aspect ratio, automatic window fit, full screen, displays pixel counter

5. Live view window.

Double-clicking the left mouse button on the preview window turns the display of the image on and off in full screen.

6. Buttons for controlling camera functions:



From left to right: enables/disables live view, enables and disables the display of alarm event icons, enables and disables the alarm output, turns on two-way audio, turns on audio monitoring, takes a photo, enables/disables recording, digital zoom buttons, enables/disables the display of image analysis lines

5. RESTORE FACTORY SETTINGS

5.1 Software restore of factory settings

The restore of factory settings function is located in the "Config -> Maintenance -> Backup and Restore" menu. You can choose the "Restore default parameters" option, where selecting the "Keep" option allows you to keep the network settings, security configuration or image configuration unchanged. This option does not reset user passwords. The "Restore factory settings" option completely resets all camera settings.

5.2 Hardware restore of factory settings

To restore the camera's factory settings using the hardware, use the RESET button located on the rear panel. To restore the default settings using the RESET button, press and hold it for about 5 seconds.



AAT SYSTEMY BEZPIECZEŃSTWA Sp. z o.o.

431 Pulawska St., 02-801 Warsaw, Poland

tel.: +4822 546 0 546, kontakt@aat.pl

www.novuscctv.com

Skrócona instrukcja obsługi



NVIP-4Q-6101/PIR/W

NoVus

UWAGI I OSTRZEŻENIA

PRODUKT SPEŁNIA WYMAGANIA ZAWARTE W DYREKTYWACH:



DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2014/30/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (Dz.U. L 096 z 29.3.2014, s. 79-106, z późniejszymi zmianami) – zwana Dyrektywą EMC.



DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2012/19/UE z dnia 4 lipca 2012 r. w sprawie zużytego sprzętu elektrycznego i elektronicznego WEEE (Dz.U. L 96 z 29.3.2014, str. 79-106, z późniejszymi zmianami) – zwana Dyrektywą WEEE.



DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2011/65/UE z dnia 8 czerwca 2011 r. w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (Dz.U. L 174 z 1.7.2011, str. 88-110, z późniejszymi zmianami) - zwana Dyrektywą RoHS.

DYREKTYWA DELEGOWANA KOMISJI (UE) 2015/863 z dnia 31 marca 2015 r. zmieniająca załącznik II do dyrektywy Parlamentu Europejskiego i Rady 011/65/UE w odniesieniu do wykazu substancji objętych ograniczeniem (Dz. U. z 3 stycznia 2017).

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2017/2102 z dnia 15 listopada 2017 r. zmieniająca dyrektywę 2011/65/UE w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (Dz. U. z 10 lipca 2019).

Wyłączenie odpowiedzialności w przypadku uszkodzenia danych zawartych na dyskach lub innych urządzeniach lub nośnikach:

Producent nie ponosi odpowiedzialności w razie uszkodzenia lub utraty w trakcie eksploatacji Produktu danych zawartych na dyskach lub innych urządzeniach lub nośnikach.

Obowiązek konsultowania się z Producentem przed wykonaniem czynności nieprzewidzianej instrukcją obsługi albo innymi dokumentami:

Przed wykonaniem czynności, która nie jest przewidziana dla danego Produktu w instrukcji obsługi, innych dokumentach dołączonych do Produktu lub nie wynika ze zwykłego przeznaczenia Produktu, należy, pod rygorem wyłączenia odpowiedzialności Producenta za następstwa takiej czynności, skontaktować się z Producentem.



Zamieszczone w niniejszej publikacji zdjęcia przedstawiające obrazy z kamer mogą być symulacjami. Rzeczywiste obrazy z kamer mogą się różnić, w zależności od typu, modelu, ustawień, obszaru obserwacji lub warunków zewnętrznych.

WARUNKI BEZPIECZEŃSTWA



Przed rozpoczęciem użytkowania urządzenia, należy zapoznać się z instrukcją obsługi w celu zapewnienia właściwej i bezpiecznej pracy urządzenia. Nieprzestrzeganie instrukcji może prowadzić do uszkodzenia urządzenia i/lub naruszenia bezpieczeństwa użytkownika.



Użytkownik nie może dokonywać samodzielnych napraw urządzenia. Naprawy i konserwację urządzenia mogą być wykonywane wyłącznie przez wykwalifikowanych pracowników serwisu.



Urządzenie będące elementem profesjonalnego systemu telewizji dozorowej służącego do nadzoru i kontroli, nie jest przeznaczone do samodzielnego montażu w gospodarstwach domowych, przez osoby nie posiadające specjalistycznej wiedzy.

pl

1. Przed zainstalowaniem i rozpoczęciem eksploatacji należy dokładnie zapoznać się z niniejszą instrukcją obsługi;
2. Instrukcję należy przechowywać przez czas eksploatacji urządzenia na wypadek konieczności odniesienia się do zawartych w niej treści;
3. Należy przestrzegać wymogów bezpieczeństwa opisanych w instrukcji, gdyż mają one bezpośredni wpływ na bezpieczeństwo użytkowników i trwałość oraz niezawodność urządzenia;
4. Wszystkie czynności wykonywane przez instalatorów i użytkowników muszą być realizowane zgodnie z opisem zawartym w instrukcji;
5. Podczas przeprowadzania czynności konserwatorskich urządzenie musi być odłączone od zasilania;
6. Nie wolno stosować żadnych dodatkowych urządzeń, podzespołów lub akcesoriów nie przewidzianych i nie zalecanych przez producenta;
7. Nie należy instalować tego urządzenia w miejscach, gdzie nie można zapewnić właściwej wentylacji (np. zamknięte szafki, itp.), gdyż może to powodować kumulowanie się ciepła i w konsekwencji może doprowadzić do uszkodzenia;
8. Nie wolno umieszczać urządzenia na niestabilnych powierzchniach. Instalacja musi być przeprowadzona przez wykwalifikowany personel o odpowiednich uprawnieniach według zaleceń podanych w niniejszej instrukcji;
9. Urządzenie może być zasilane jedynie ze źródeł o parametrach zgodnych ze wskazanymi przez producenta w danych technicznych;



Ponieważ produkt jest stale ulepszany i optymalizowany, niektóre jego parametry i funkcje mogły ulec zmianie w stosunku do opisanych w niniejszej instrukcji. W razie wątpliwości prosimy o zapoznanie się z instrukcją obsługi znajdującą się na stronie **www.novuscctv.com**

Instrukcja obsługi znajdującą się na stronie www.novuscctv.com jest zawsze najbardziej aktualną wersją.

INFORMACJE WSTĘPNE

1. DANE TECHNICZNE

OBRAZ	
Przetwornik obrazu	4 MPX, matryca CMOS, 1/3", SmartSens
Liczba efektywnych pikseli	2568 (H) x 1448 (V)
Czułość	0.01 lx/F2.1 - tryb kolorowy, 0 lx (IR wł.) - tryb czarno-biały
Elektroniczna migawka	automatyczna: 1/3 s ~ 1/100000 s
Wydłużona migawka (DSS)	do 1/3 s
Szeroki zakres dynamiki (WDR)	tak (podwójne skanowanie przetwornika), 120dB
Cyfrowa redukcja szumu (DNR)	2D, 3D
Redukcja efektu oślepienia kamery (HLC)	tak
Kompensacja tylnego światła (BLC)	tak
Redukcja migotania obrazu (Antiflicker)	tak
OBIEKTYW	
Typ obiektywu	stałoogniskowy, f=2.1 mm/F2.1
DORI	
DORI (Detekcja, Obserwacja, Rozpoznanie, Identyfikacja)	dla f = 2.1mm - D: 36m, O: 14m, R: 7m, I: 4m
DZIEŃ/NOC	
Tryb pracy	przełączanie dzień/noc: mechaniczny filtr podczerwieni
Tryb przełączania	automatyczny, manualny, czasowy, wyzwalany zewnątrz
Regulacja poziomu przełączania	tak
Opóźnienie przełączania	2 ~ 6000 s
Czujnik światła widzialnego	tak
SIEĆ	
Rozdzielczość strumienia wideo	2560 x 1440 (QHD), 2304 x 1296, 1920 x 1080 (Full HD), 1280 x 720 (HD), 704 x 576, 352 x 288 (CIF), 480 x 240
Prędkość przetwarzania	30 kl/s dla wszystkich rozdzielczości
Tryb wielostrumieniowy	2 strumienie (główny, pomocniczy)
Kompresja wideo/audio	H.264, H.265, MJPEG / G.711
Liczba jednoczesnych połączeń	maks. 2
Przepływność (Bitrate)	dla H.264 : 64 kbps - 6144 kbps dla H.265 : 64 kbps - 6144 kbps
Obsługiwane protokoły sieciowe	HTTP, IPv4/v6, UDP, HTTPS, FTP, DHCP, DDNS, NTP, RTSP, UPnP, QoS, IEEE 802.1X, PPPoE, SMTP, P2P, HTML5, RTMP
Wsparcie protokołu ONVIF	Profile G/S/T
Konfiguracja kamery	z poziomu przeglądarki Edge, Firefox, Chrome, Opera języki: polski, angielski i inne
Kompatybilne oprogramowanie	NOVUS MANAGEMENT SYSTEM VSS, NOVUS MANAGEMENT SYSTEM AC
Aplikacje mobilne	ipGO 6 (iPhone, Android)
WIFI	
Standard sieci	IEEE802.11b, g, n
Pasmo	2.4GHz
Zabezpieczenia	WEP, WPA-PSK/WPA2-PSK
Zasięg transmisji	do 50 m
Antena	wbudowana, dookólna

INFORMACJE WSTĘPNE

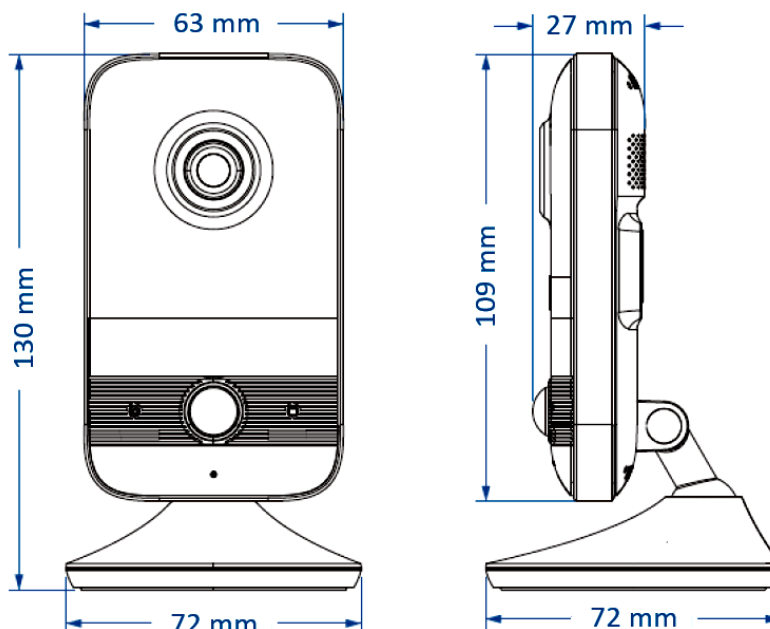
ANALIZA OBRAZU	
Funkcje	sabotaż, przekroczenie linii, detekcja osób, wtargnięcie, detekcja ruchu SMART
POZOSTAŁE FUNKCJE	
Zabezpieczenia	obsługa IEEE 802.1X, obsługa HTTPS, filtrowanie adresów MAC/IP, wymuszenie zmiany hasła domyślnego, zgodność z normą EN18031 definiującą standardy cyberbezpieczeństwa dla urządzeń radiowych i IoT
Strefy prywatności	4 typu kolor
Detekcja ruchu	tak
Detektor PIR	zasięg do 5 m
Obszar obserwacji (ROI)	8
Obróbka obrazu	wyostrzanie, odbicie lustrzane, przerzucenie obrazu w pionie
Prealarm/postalarm	do 6 s/do 120 s
Reakcja na zdarzenia alarmowe	e-mail z załącznikiem, zapis na FTP, zapis na kartę SD, aktywacja wyjścia alarmowego, odtworzenie komunikatu audio
Odstraszenie	wbudowany głośnik (predefiniowane komunikaty głosowe)
Przywracanie ustawień fabrycznych	z poziomu przeglądarki internetowej, za pomocą przycisku reset, za pomocą oprogramowania NMS IPTool
OŚWIETLACZ IR	
Liczba LED	1
Zasięg	10 m
Smart IR	tak (wsparcie sprzętowe)
INTERFEJSY	
Wejścia/wyjścia audio	wbudowany mikrofon/głośnik
Wejścia/wyjścia alarmowe	1 (NO/NC) / 1 typu przekaźnik (maks. 12VDC/300mA)
Interfejs sieciowy	1 x Ethernet - złącze RJ-45, 10/100 Mbit/s 1 x Bezprzewodowy (WiFi)
Gniazdo kart pamięci	microSD - pojemność do 128GB
PARAMETRY INSTALACYJNE	
Wymiary (mm)	63 (szer.) x 109 (wys.) x 27 (dł.) z uchwytem: 72 (szer.) x 130 (wys.) x 72 (dł.)
Masa	0.2 kg
Obudowa	plastikowa, w kolorze czarno-białym, uchwyt ścienny/podstawa w zestawie Typ obudowy: 4Q
Zasilanie	12 VDC, PoE (IEEE 802.3af, Klasa 3)
Pobór mocy	3 W, 4 W (oświetlacz IR wł.)
Temperatura pracy	-20°C ~ 50°C
Wilgotność	maksymalnie 95%, względna (bez kondensacji)



Deklarowany zasięg działania sieci WiFi jest oparty na badaniach laboratoryjnych i dotyczy otwartych przestrzeni. Należy mieć na uwadze, że materiały wykorzystywane do budowy domów i mieszkań, grubość ścian i warunki pola elektromagnetycznego w najbliższym otoczeniu mogą mieć wpływ na ograniczenie zasięgu sieci.

INFORMACJE WSTĘPNE

1.1. Wymiary kamery



1.2. Zawartość opakowania

Po otwarciu należy upewnić się czy w opakowaniu znajdują się następujące elementy:

- Kamera IP
- Torebka z akcesoriami montażowymi
- Skrócona instrukcja obsługi.

Jeżeli którykolwiek z elementów został uszkodzony w transporcie, należy spakować zawartość z powrotem do oryginalnego opakowania i skontaktować się z dostawcą.

Uwaga:

Jeżeli urządzenie przyniesione zostało z pomieszczenia o niższej temperaturze należy odczekać aż osiągnie temperaturę pomieszczenia, w którym ma pracować. Nie wolno włączać urządzenia bezpośrednio po przyniesieniu z chłodniejszego miejsca. Kondensacja zawartej w powietrzu pary wodnej może spowodować zwarcia i w konsekwencji uszkodzenie urządzenia.

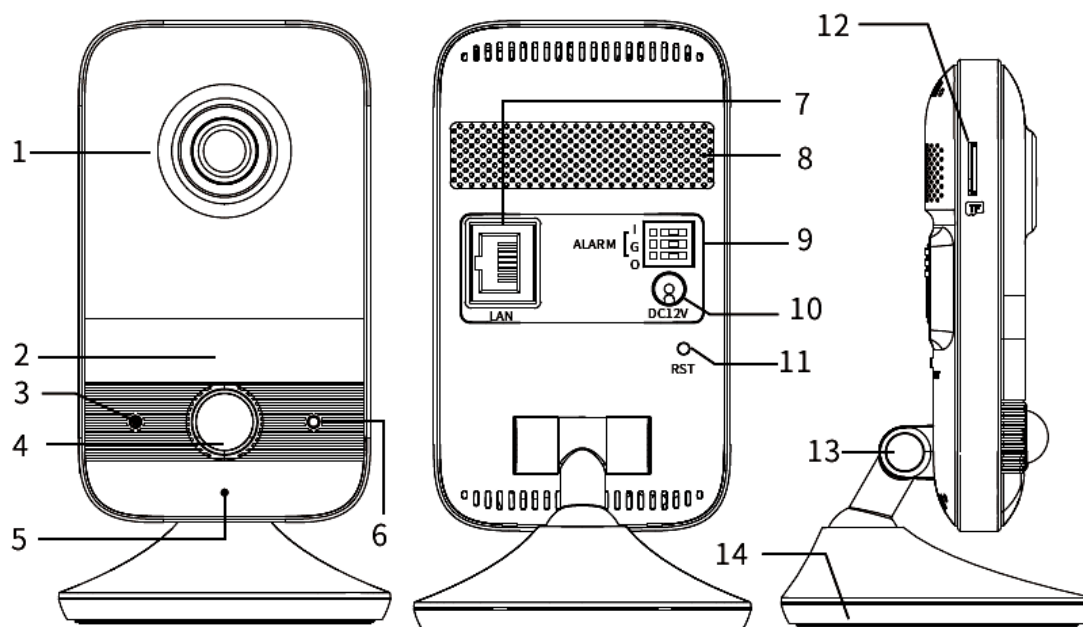
Uwaga:

Przed uruchomieniem urządzenia należy zapoznać się z opisem i rolą poszczególnych wejść, wyjść oraz elementów regulacyjnych, w które wyposażone jest kamera.

URUCHAMIANIE I WSTĘPNA KONFIGURACJA

2. URUCHAMIANIE I WSTĘPNA KONFIGURACJA

2.1. Opis elementów i złącz kamery



1	Obiektyw	8	Głośnik
2	Dioda IR LED (oświetlacz podczerwieni)	9	Blok złącz wejść/wyjść alarmowych
3	Mikrofon	10	Gniazdo zasilania 12VDC
4	Detektor PIR	11	Przycisk RESET
5	Kontrolka stanu	12	Gniazdo karty pamięci
6	Czujnik światła	13	Regulacja położenia kamery
7	Gniazdo sieci LAN	14	Podstawa

Opcje kontrolki stanu

Czerwona, ciągła	Uruchamianie kamery	Czerwona, migająca	Sieć rozłączona
Niebieska, ciągła	Uruchamianie Wi-Fi	Niebieska, migająca	Kamera nieaktywowana, Aktywacja w trakcie, Alarm
Zielona, ciągła	Praca	Zielona, migająca	Aktualizacja firmware

URUCHAMIANIE I WSTĘPNA KONFIGURACJA

2.2. Podłączenie zasilania

Kamerę można zasilic z dostępnego na rynku zasilacza prądu stałego, pod warunkiem spełnienia przez niego wymogów technicznych kamery. Zasilacz musi dostarczać stabilizowanego napięcia stałego o wartości 12V, musi pozwalać na pobór co najmniej 10W mocy, oraz posiadać wtyk zasilający walcowy DC 2.5/5.5 o właściwej polaryzacji styków:



Możliwe jest także zasilanie kamery przez gniazdo sieciowe RJ45, przy wykorzystaniu technologii PoE (IEEE 802.3af, Klasa 3).

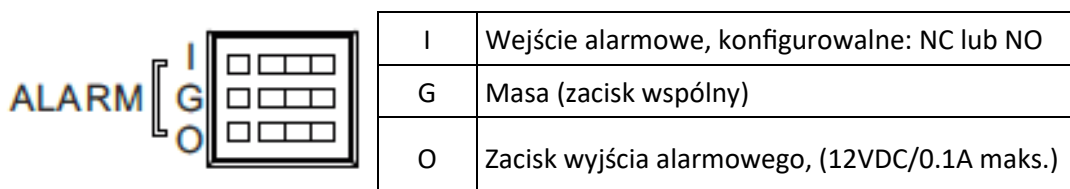
Uwaga!

Zabronione jest stosowanie jako źródło zasilania kamery urządzeń (zasilacze, adaptory itp.) PoE niezgodnych ze standardem IEEE 802.3af, potocznie nazywanych „pasywne zasilacze PoE”. Uszkodzenia wynikłe ze stosowania nieodpowiednich źródeł zasilania nie podlegają gwarancji.

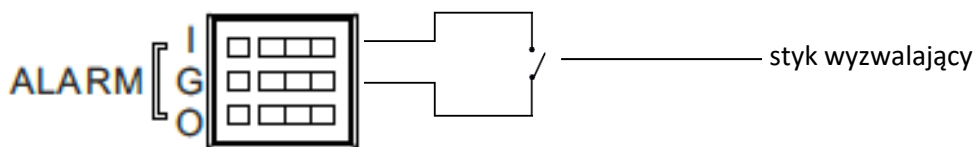
2.3. Podłączenie wejść / alarmowych

Kamera posiada jedno wejście i wyjście alarmowe. Wejście alarmowe służy do podłączenia takiego urządzenia jak czujka ruchu, przycisk, kontaktron lub fotokomórka. Naruszenie wejścia powoduje wyzwolenie alarmu i aktywuje wcześniej zaprogramowaną akcję.

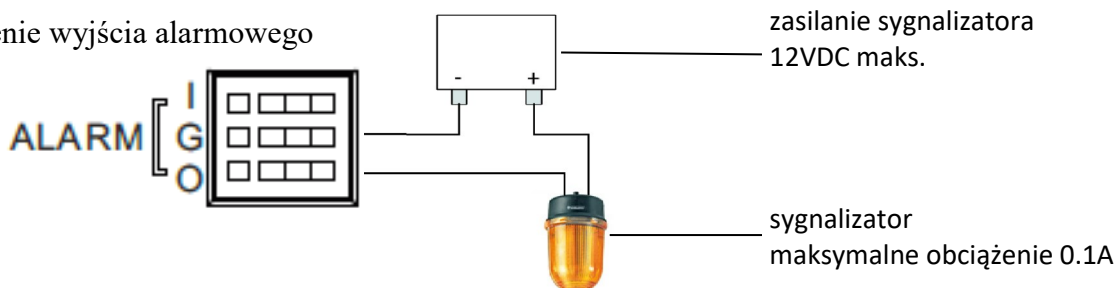
Wyjście alarmowe umożliwia podłączenie zewnętrznego sygnalizatora i realizacji funkcji automatycznego sterowania, takiej jak np. załączanie oświetlenia.



Podłączenie wejścia alarmowego



Podłączenie wyjścia alarmowego



URUCHAMIANIE I WSTĘPNA KONFIGURACJA

2.4. Montaż kamery

Konstrukcja kamery umożliwia elastyczny wybór miejsca zamocowania/postawienia. Kamera może pracować postawiona na dowolnej płaskiej powierzchni lub być zawieszona z wykorzystaniem otworów montażowych w stopie.

Aby zamontować kamerę w pozycji wiszącej, zalecamy postępować wg poniższych wskazówek:

- Przyłóż szablon w miejscu, w którym chcesz zainstalować kamerę. Następnie wywierć otwory na śruby w ścianie zgodnie z szablonem.
- Włóż kołki w otwory i wkręć wkręty. Wkręty powinny wystawać ponad powierzchnię ściany na kilka milimetrów.
- Doprowadź i podłącz przewody do kamery.
- Zawieś kamerę za podstawę montażową na wkrętach i upewnij się, że jest pewnie zamocowana. Następnie wyreguluj położenie kamery.



Kamera jest przeznaczona do pracy wewnątrz pomieszczeń mieszkalnych. Użytkowanie jej na zewnątrz, bądź w pomieszczeniach o dużej wilgotności jak baseny, łazienki, pralnie itp. może być przyczyną nieprawidłowego działania kamery lub jej uszkodzenia.

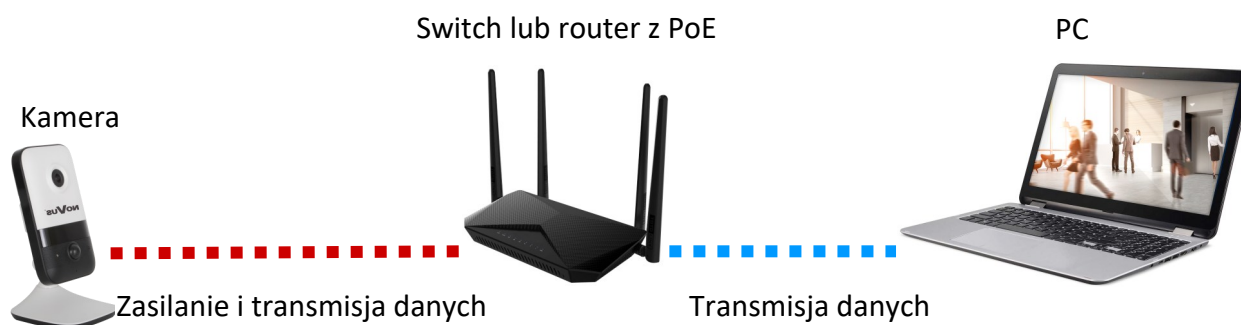
URUCHAMIANIE I WSTĘPNA KONFIGURACJA

2.5. Uruchomienie kamery

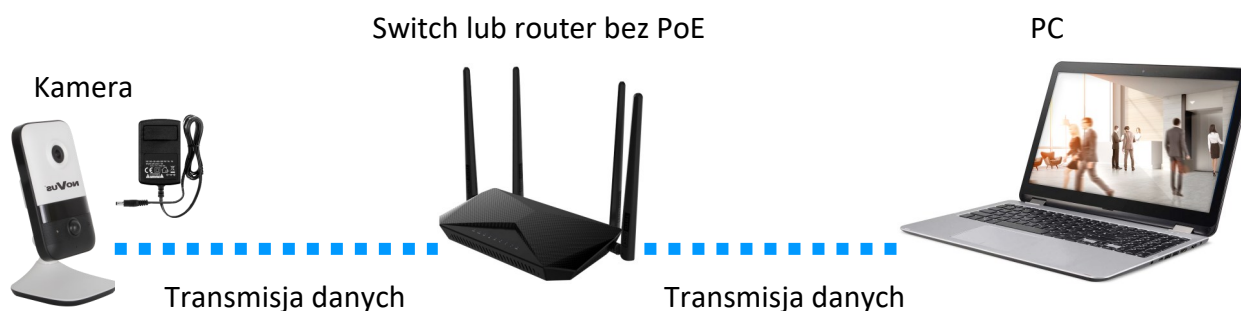
2.5.1 Podłączenie kamery do sieci przewodowej LAN

W celu uruchomienia kamery należy podłączyć kabel ethernetowy do gniazda sieciowego kamery, a drugi koniec do switcha lub routera. Jeżeli posiadany switch lub router nie jest urządzeniem PoE, do kamery należy także podłączyć zasilanie 12VDC. Pomocne mogą być poniższe schematy:

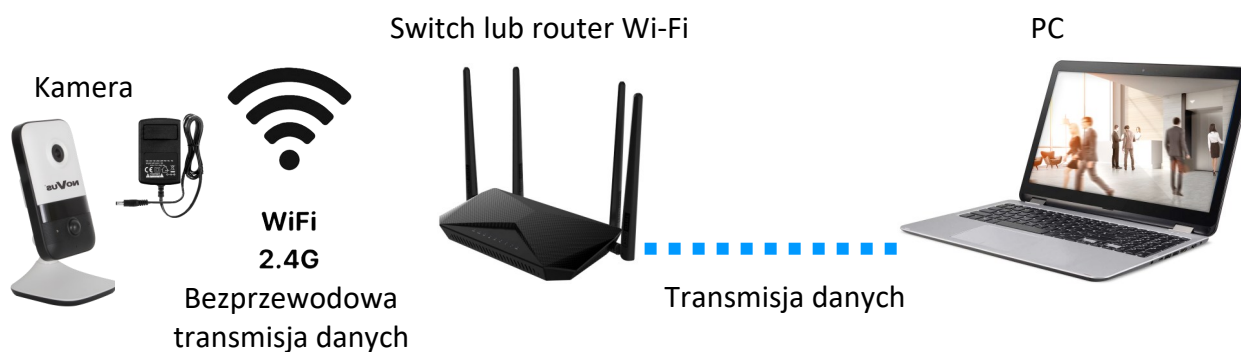
- Połączenie przewodowe wykorzystujące switch lub router PoE:



- Połączenie przewodowe wykorzystujące switch lub router bez PoE i zasilanie kamery 12VDC:



2.5.2 Podłączenie kamery do sieci bezprzewodowej Wi-Fi



Po wykonaniu połączeń i uruchomieniu się kamery (co trwa kilka minut) możliwe jest połączenie się z kamerą.

URUCHAMIANIE I WSTĘPNA KONFIGURACJA

2.6. Zalecenia dotyczące bezpieczeństwa sieci

UWAGA!

Poniżej zostały przedstawione podstawowe zalecenia dotyczące budowy oraz konfiguracji systemów monitoringu podłączonych do sieci Internet, pozwalające ograniczyć ryzyko nieautoryzowanej ingerencji w system przez osoby trzecie.

1. Bezwzględnie należy zmienić domyślne hasła dostępu oraz nazwy użytkowników (jeśli dane urządzenia dają taką możliwość) wszystkich zastosowanych urządzeń sieciowych (tzn. kamery, routerów, przełączników sieciowych itp.) na hasła o znacznym stopniu skomplikowania. W zależności od możliwości konfiguracji danego urządzenia zaleca się, aby hasło zawierało: małe litery, wielkie litery, cyfry oraz znaki specjalne.

2. W zależności od dostępnej funkcjonalności w celu ograniczenia dostępu do zastosowanych urządzeń sieciowych na poziomie konta administratora zaleca się odpowiednią konfigurację kont użytkowników.

3. Bezwzględnie zabronione jest wykorzystywanie funkcji DMZ (Demilitarized zone - strefa zdemilitaryzowana). Zastosowanie tej funkcji otwiera dostęp do systemu od strony sieci Internet na wszystkich możliwych portach, co w znacznym stopniu ułatwia ewentualną nieautoryzowaną ingerencję w system.

Zamiast wykorzystywania funkcji DMZ należy zastosować przekierowanie portów. Przekierowane powinny zostać jedynie porty niezbędne do realizacji połączenia (szczegółowych informacji na temat portów komunikacji w poszczególnych modelach rejestratorów, kamer itp. należy szukać w instrukcjach obsługi urządzeń).

4. Należy stosować routery wyposażone w funkcję zapory sieciowej (Firewall) oraz upewnić się że funkcja jest włączona oraz odpowiednio skonfigurowana.

5. Jeśli urządzenia sieciowe posiadają taką funkcjonalność, zalecana jest zmiana domyślnych numerów portów wykorzystywanych do komunikacji sieciowej.

6. Jeśli urządzenia sieciowe posiadają funkcję UPnP i nie jest ona wykorzystywana, należy ją bezwzględnie wyłączyć.

7. Jeśli urządzenia sieciowe posiadają funkcję P2P i nie jest ona wykorzystywana, należy ją wyłączyć.

8. Jeśli urządzenia sieciowe obsługują protokół HTTPS do realizacji połączeń zaleca się jego stosowanie.

9. Jeśli urządzenia sieciowe obsługują funkcję filtracji adresów IP uprawnionych do nawiązywania połączenia zaleca się jej wykorzystywanie.

POŁĄCZENIA SIECIOWE Z KAMERĄ

3. POŁĄCZENIA SIECIOWE Z KAMERĄ

3.1. Pierwsze łączenie z kamerą z użyciem sieci Wi-Fi i urządzenia mobilnego z aplikacją ipGO6



Do uruchomienia kamery z podłączeniem do sieci Wi-Fi niezbędne jest posiadanie urządzenia mobilnego (smartfon, tablet) z zainstalowaną aplikacją ipGO6. Przed rozpoczęciem operacji należy upewnić się, że kamera i urządzenie mobilne znajdują się w zasięgu tej samej sieci Wi-Fi. Należy zwrócić uwagę, by urządzenie mobilne łączyło się z siecią Wi-Fi w paśmie 2,4GHz gdyż kamera pracuje tylko w tym paśmie.

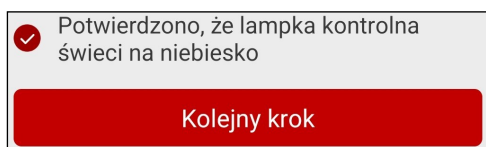


Podczas uruchamiania kamery z podłączeniem do sieci Wi-Fi, kamera może być zasilana z zasilacza 12V lub ze switcha/routera PoE.

W pierwszej kolejności należy pobrać na urządzenie mobilne (ze sklepu Play dla urządzeń z systemem Android lub ze sklepu Apple Store dla urządzeń z systemem iOS) aplikację **ipGO6**. Po zainstalowaniu aplikacji należy zalogować się (lub założyć konto).

Następnie należy przejść do zakładki „Urządzenia” i dotknąć przycisku „Opcje”  w prawym górnym rogu ekranu, a następnie opcję „Dodawanie”. Otworzy się okno skanowania kodu QR, którym należy zeskanować kod umieszczony na podstawie kamery. Po pomyślnym zeskanowaniu otworzy się okno dodawania urządzenia, w którym wyświetli się rysunek kamery i jej kod P2P. Następnie należy dotknąć przycisku „Dodaj” aby przejść dalej.

Następnie należy upewnić się, że kontrolka stanu na kamerze miga niebieskim światłem i na urządzeniu mobilnym należy potwierdzić ten fakt a następnie dotknąć przycisku „Kolejny krok”.

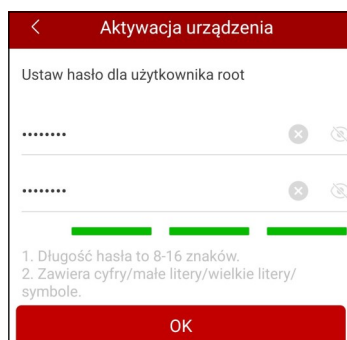


W następnym oknie należy podać hasło do sieci Wi-Fi i dotknąć przycisku „Kolejny krok”. Otworzy się kolejne okno, w którym nastąpi połączenie z dodawaną kamerą.



Na tym etapie odbywa się aktywacja kamery. Urządzenie mobilne łączy się z hot-spotem uruchomionym przez kamerę, by było możliwe ustawienie hasła użytkownika.

Po połączeniu z hot-spotem kamery, w następnym oknie należy wpisać i potwierdzić hasło logowania do kamery dla konta administratora (**root**).



Po wpisaniu hasła nastąpi aktywacja kamery i po chwili kamera pojawi się na liście urządzeń aplikacji ipGO6.

POŁĄCZENIA SIECIOWE Z KAMERĄ

3.2. Pierwsze łączenie z kamerą z użyciem sieci przewodowej LAN lub bezprzewodowej Wi-Fi i komputera z przeglądarką internetową

Ponieważ kamera spełnia wymogi norm EN 18031, definiujących podstawowe wymagania dotyczące cyberbezpieczeństwa i jakości dla urządzeń bezprzewodowych i IoT, w tym kamer Wi-Fi, to jej łączenie się z przeglądarką internetową przebiega z użyciem protokołu HTTPS. Dlatego wpisując w pasku adresu przeglądarki WWW adres IP kamery, należy poprzedzić go podaniem protokołu „https://”. Po połączeniu przeglądarka wyświetli alert zabezpieczeń informujący o braku poufności połączenia, podobny do poniższego:



Wyświetlenie alertu jest spowodowane tym, że kamera ma zainstalowany prywatny, niezaufany certyfikat zabezpieczeń, który nie może być zweryfikowany przez przeglądarkę. Nie należy się obawiać - na tym etapie jest to prawidłowe zachowanie, a certyfikat kamery jest wystarczający dla zapewnienia poufności połączenia.



W razie potrzeby użytkownik może we własnym zakresie zainstalować zaufany certyfikat bezpieczeństwa, który nie będzie wywoływał alertów przeglądarki. Certyfikat może być zainstalowany w menu "Ustawienia -> Sieć -> HTTPS"

W oknie alertu należy kliknąć przycisk „Zaawansowane”, lub link „Help me understand” lub podobny. Wyświetli się dodatkowa informacja o zabezpieczeniach:

Ten serwer nie może udowodnić, że jest to **192.168.1.139**; jego certyfikat zabezpieczeń nie jest zaufany przez system operacyjny komputera. Może to być spowodowane błędną konfiguracją lub przechwyceniem połączenia przez atakującego.

[Przejdź do witryny 192.168.1.139 \(niebezpieczna\)](#)

Należy kliknąć na łącze „Przejdź do witryny (tu adres IP) (niebezpieczna)” by połączyć się z kamerą.



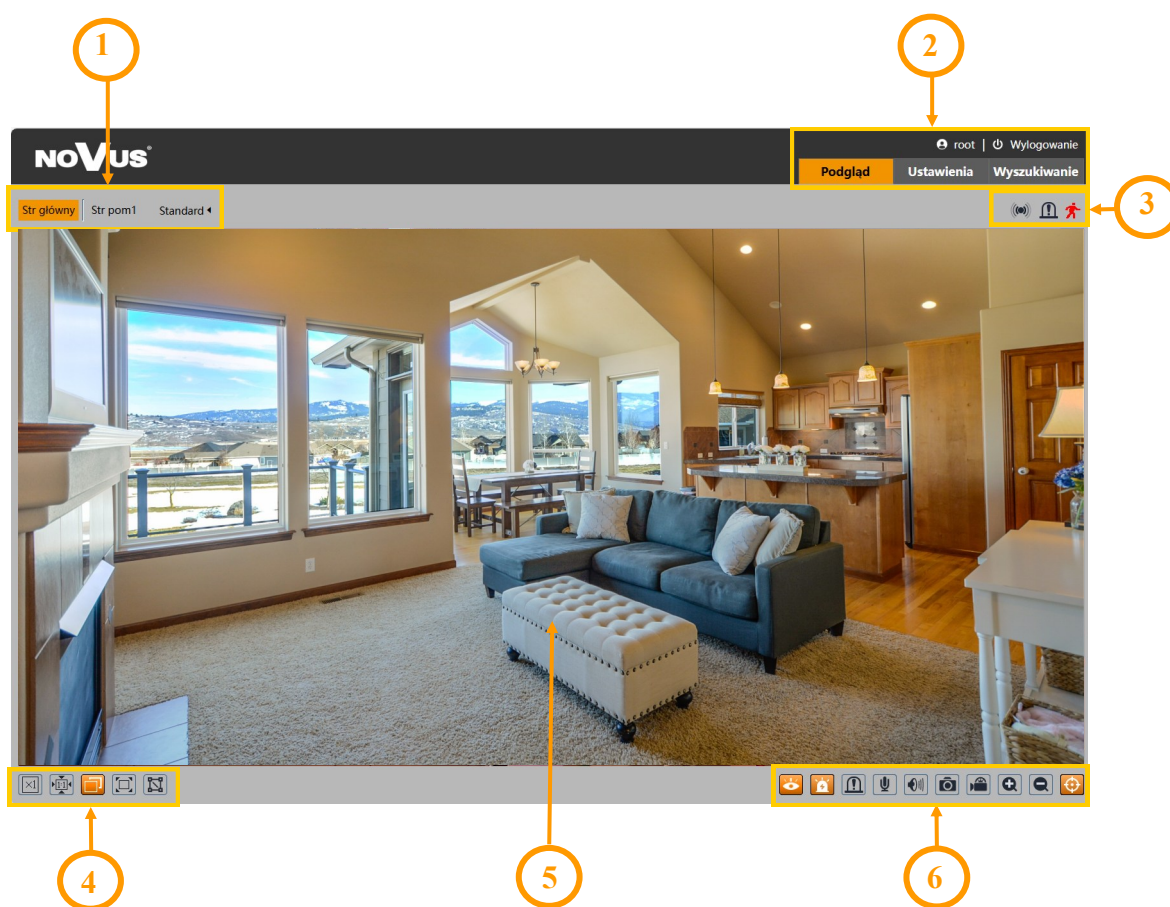
Po kliknięciu na łącze przeglądarka zapamięta decyzję użytkownika i przy kolejnych łączeniach się z kamerą będzie sama wstawiała protokół „https://” przed adresem IP oraz nie będzie wyświetlała alertu, chociaż nadal będzie widoczne ostrzeżenie „Niebezpieczona” na pasku adresu.

INTERFEJS WWW - PRACA Z KAMERĄ

Po połączeniu wyświetli się okno z oświadczeniem o ochronie prywatności, które należy zaakceptować przez zaznaczenie pola wyboru i naciśnięcie przycisku „Odczytane”. Następnie kamera wyświetli okna konfiguracji strefy czasowej, a potem okno wyboru pytań bezpieczeństwa, pozwalających odzyskać dostęp do kamery w przypadku zapomnienia hasła administratora, bez konieczności resetowania urządzenia. Następnie wyświetli się okno aktywacji, w którym definiuje się hasło administratora (oraz hasło do konta ONVIF). Po przejściu tych kroków kamera wyświetli ekran logowania, w którym należy podać nazwę konta administratora (domyślnie root) oraz ustawione hasło.

4. INTERFEJS WWW - PRACA Z KAMERĄ

4.1 Wyświetlanie obrazu na żywo



1. Wybór strumienia do wyświetlania w oknie podglądu oraz ustawienie rozmiaru bufora kamery.

2. Przyciski wyboru trybu pracy i konfiguracji kamery:

Podgląd	- włącza podgląd strumienia na żywo
Ustawienia	- wyświetla panel konfiguracyjny kamery
Wyszukiwanie	- wyświetla okno odtwarzania nagrań zapisanych na karcie pamięci
root	- informacja o zalogowanym użytkowniku
Wylogowanie	- wyloguje aktualnie zalogowanego użytkownika

PRZYWRACANIE USTAWIEŃ FABRYCZNYCH

3. Panel wyświetlania ikon zdarzeń alarmowych:



Od lewej: aktywacja wyjścia alarmowego, sygnalizacja nagrywania na kartę pamięci, zmiana kolorystyki, sabotaż, zmiana sceny, detekcja osób, detekcja PIR, alarm wejścia alarmowego, detekcja ruchu. Wystąpienie danego zdarzenia jest sygnalizowane migającym czerwonym kolorem.

4. Przyciski ustawiania obrazu:



Od lewej: rozmiar oryginalny, proporcje oryginalne, automatyczne dopasowanie do okna, pełny ekran, wyświetla licznik pikseli

5. Okno podglądu na żywo.

Dwukrotne kliknięcie lewym przyciskiem myszy na oknie podglądu włącza i wyłącza wyświetlanie obrazu na całym ekranie.

6. Przyciski sterujące funkcjami kamery:



Od lewej: włącza/wyłącza podgląd na żywo, włącza i wyłącza wyświetlanie ikon zdarzeń alarmowych, włącza i wyłącza wyjście alarmowe, włącza dwukierunkowe audio, włącza odsłuch audio, wykonuje zdjęcie, włącza/wyłącza nagrywanie wideo na dysku komputera, przyciski cyfrowego zoomu, włącza/wyłącza wyświetlanie linii analizy obrazu

5. PRZYWRACANIE USTAWIEŃ FABRYCZNYCH

5.1 Programowe przywracanie ustawień fabrycznych

Funkcja przywracania ustawień fabrycznych znajdują się w menu „Ustawienia -> Konserwacja -> Kopia zapasowa”. Do wyboru jest opcja „Przywróć parametry domyślne”, gdzie zaznaczenie wybranej opcji „Zatrzymaj” pozwala na zachowanie ustawień sieci, konfiguracji zabezpieczeń lub konfiguracji obrazu bez zmian. Ta opcja nie resetuje haseł użytkowników. Opcja „Przywróć ustawienia fabryczne” całkowicie resetuje wszystkie ustawienia kamery.

5.2 Sprzętowe przywracanie ustawień fabrycznych

Do sprzętowego przywracania ustawień fabrycznych kamery służy przycisk RESET umiejscowiony na tylnej ścianie. Aby przywrócić ustawienia domyślne za pomocą przycisku RESET, należy wcisnąć go i przytrzymać przez około 5 sekund.



AAT SYSTEMY BEZPIECZEŃSTWA Sp. z o.o.

ul. Puławska 431, 02-801 Warszawa, Polska

tel.: 22 546 0 546, kontakt@aat.pl

www.novuscctv.com/pl