Security settings recommendations

4000 series IP cameras

NOVUS®

TABLE OF CONTENTS

PRELIMINARY INFORMATION

1. Preliminary information

The following instructions describe the recommended settings of the Novus 4000 series IP cameras to properly protect access to the device and data processed on it.
Areas:

- initial configuration
- permissions settings / accounts managing
- password policy
- device network configuration
- remote access

2. Initial configuration

2.1 Accounts and access

2.1.1 Recommendations regarding access to the system

- The camera should be located in a safe place preventing unauthorized access. In case it is impossible, cameras in vandal-proof housings should be used.
- The system should be updated on a regular basis for security improvements.
- Each of the system users should have their own personal account, which can be easily linked to a specific person.
- System privileges should be granted based on the consent of the system owner or authorized person.
- Once every six months there should be a verification of active accounts in the system.
- Verification should be carried out by the system owner or authorized persons.
- Administrative access should be granted only to the person responsible for system configuration.
- The built-in administrator account should be properly secured and used in case of emergency.
- The administrator account name should be changed from the default one to another.
- The account password should be written down and properly secured (card, pendrive or other medium located in a safe place, e.g. a safe).

Administrator account password policy. The password should be:

- random
- with the maximum available length
- contain a minimum of 2 special characters
- contain at least one digit and one upper case letter
- do not contain dictionary words
- do not include the username in the password

DETAILED CONFIGURATION

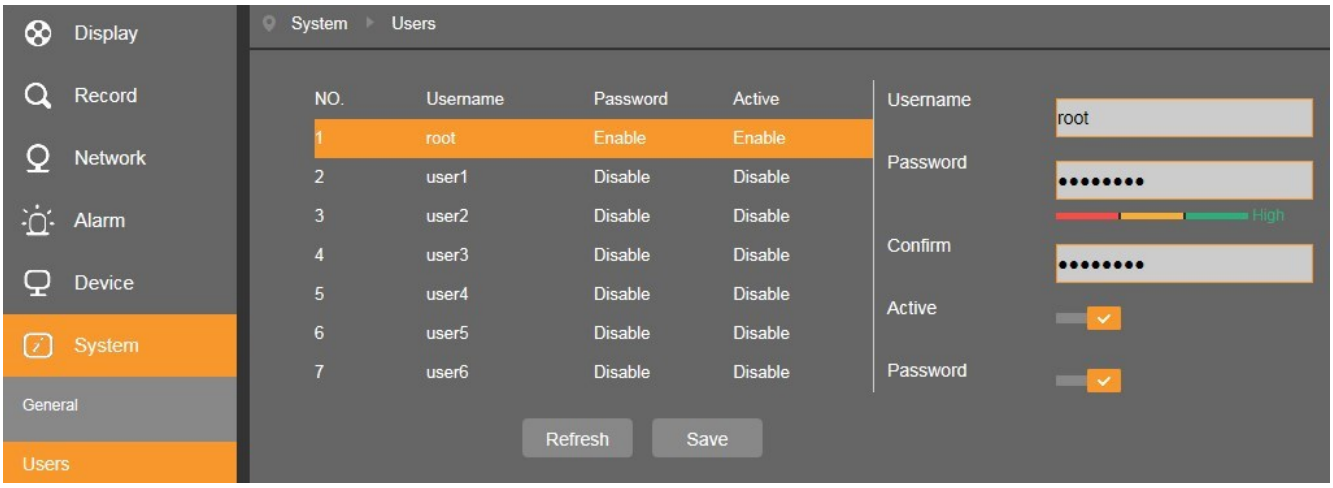
eng

Password policy and recommended password settings for other accounts:
The password for other accounts should be:

- random
- with the maximum available length
- contain a minimum of 2 special characters
- contain at least one digit and one upper case letter
- do not contain dictionary words
- do not include the username in the password

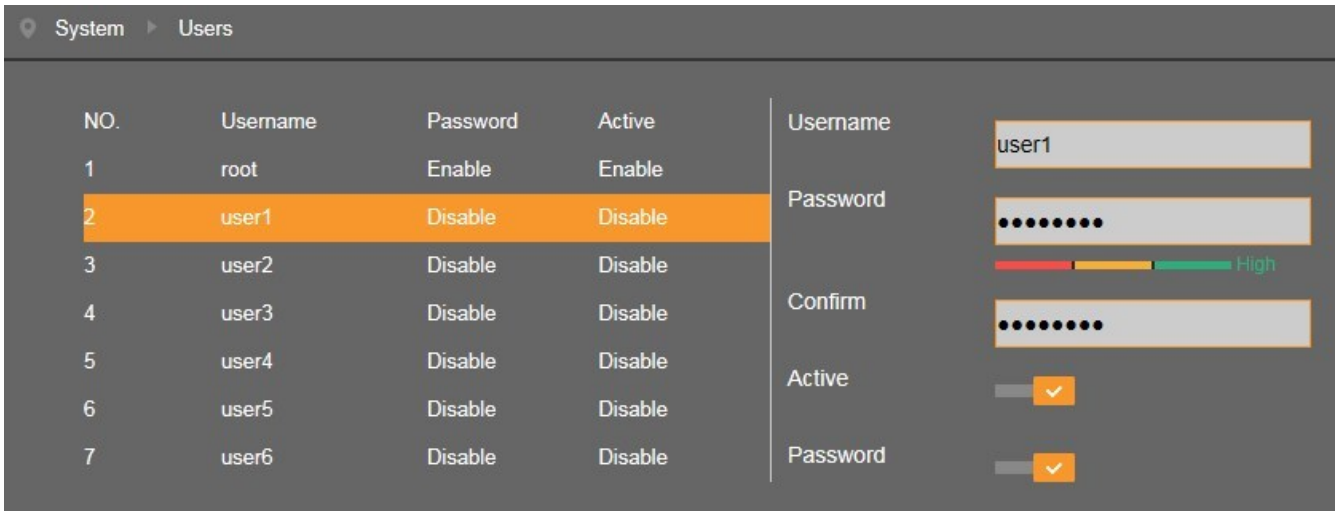
2.1.2 Detailed configuration

In the *"System"* camera menu, select the *"Users"* submenu.



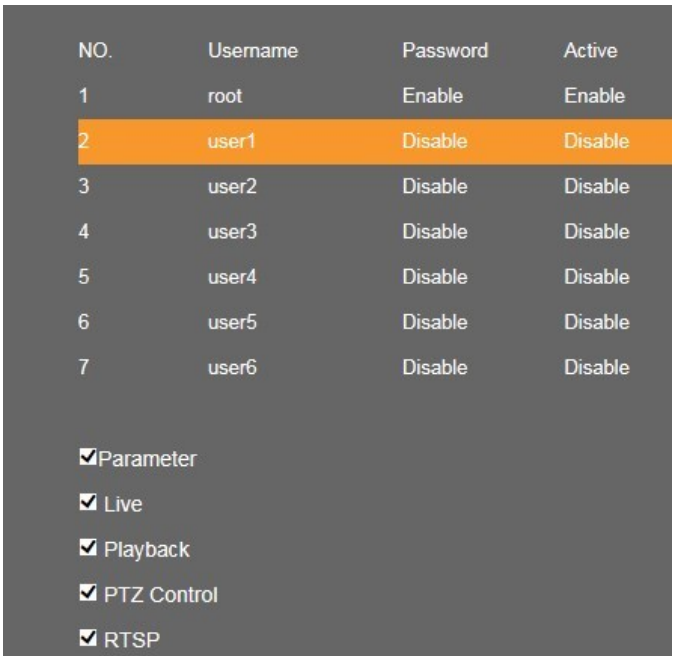
Activation and giving appropriate privileges to a new user are started by selecting the appropriate line on the list of users.

Activating a new account



After selecting the line with the user account, activate it with the *"Active"* switch and enable password protection with the *"Password"* switch. Next, set the account name and password in accordance with the recommendations provided in chapter 2.1.1

User permission settings



In the next stage, we set the rights granted to the user by checking the appropriate option. After completing the configuration, save the changes with the "Save" button.

2.2 Network configuration

2.2.1 LAN configuration

It is recommended to set the camera's static IP address.

In order to provide adequate protection against unauthorized access, it is recommended to prepare a separate LAN subnet dedicated only to the monitoring system.

Remote access to devices located in a dedicated subnet (such as a recorder, cameras) should be secured by a firewall filtering traffic at the L3 and L4 level:

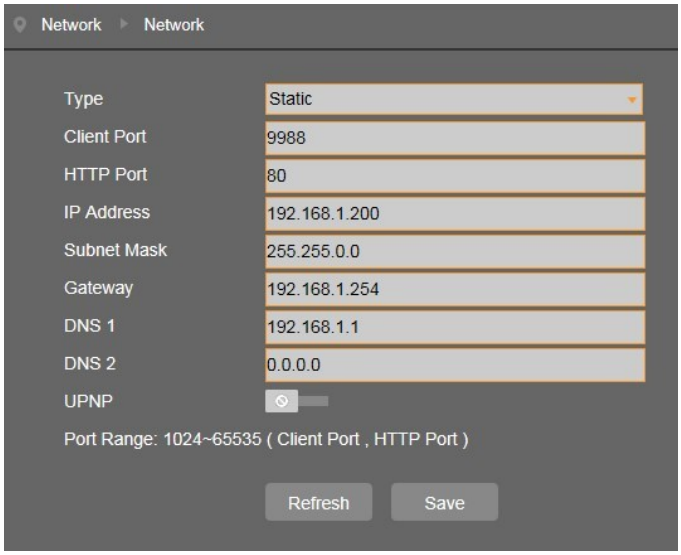
- remote access to the camera is possible only from a dedicated device
- open network ports:
  - HTTP - TCP port 80
  - HTTPS - TCP port 443 (recommended communication port with the recorder)
  - Server port - TCP 9988
  - RTSP - TCP port 554

In case of required access to the device from another location or directly from the Internet, it is recommended to use an encrypted VPN tunnel.

WI-FI CONFIGURATION

Detailed network configuration

In the *„Network”* camera menu, select the *„Network”* submenu. This tab contains TCP/IP settings.



eng

2.2.2 Wi-Fi configuration

In the case of cameras with the possibility of working in wireless networks, it is necessary to properly configure the Wi-Fi network.

In order to provide adequate protection against unauthorized access, it is recommended to prepare a separate Wi-Fi subnet, dedicated only to the monitoring system. For security reasons, you should modify your router's settings to prevent or at least significantly impede unauthorized access to the Wi -Fi network. The basic recommendations are:

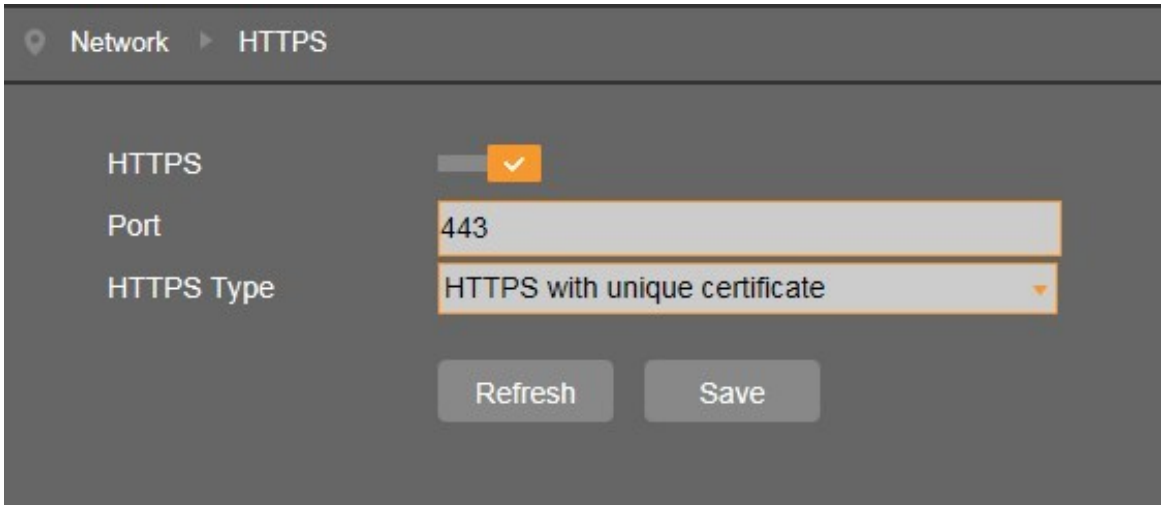
- change of data needed to log in to the router in accordance with the instructions provided in chapter 2.1.1
- WPA or WPA2 encryption must be enabled in the security configuration
- you should change the wireless network name (SSID) from the default to another, not associating with CCTV system, and the best solution is to hide the network name
- limit the number of connections allowed. Enable the option to define a list of devices that can connect to the network ("white list" or "allow list"), and add the MAC addresses of CCTV devices there
- disable Wifi Protected Setup (WPS) support
- disable remote access to the router - "Remote access"
- disable the DHCP server on the router and set permanent IP addresses for all devices on the network

For security reasons, it is not recommended to set the public IP address on the device and share it directly from the Internet.

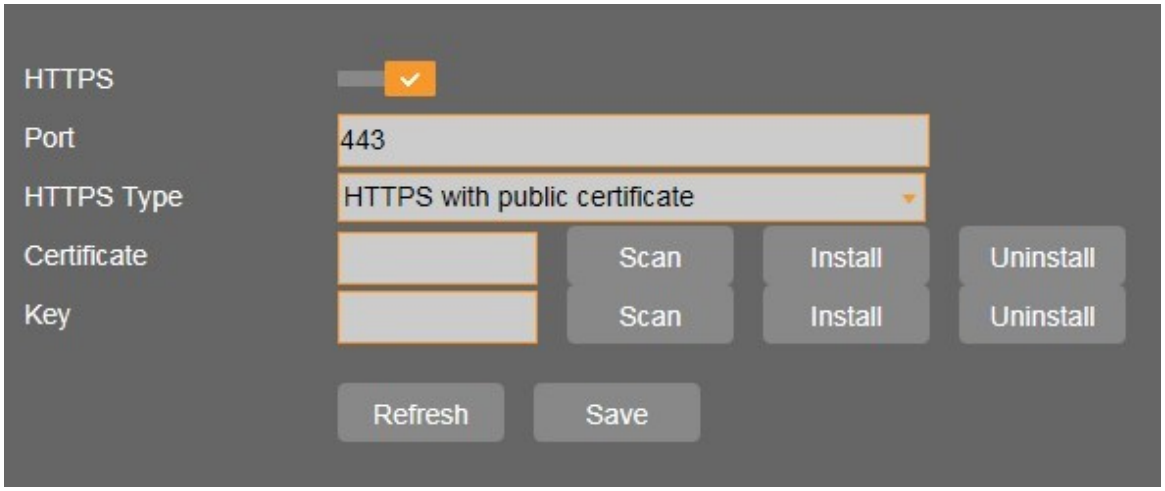
eng

2.2.3 HTTPS connection configuration

To enable logging into the administration panel after HTTPS, log in to the camera via the browser, enter the *"Remote settings"* tab and select *"HTTPS"* in the *"Network"* section.



In the next step, enable HTTPS encryption. Further options allow you to change the HTTPS port (it is recommended to leave the default port 443) and choose the type of certificate. You can use the certificate stored in the camera (*"HTTPS with unique certificate"* option), or select the *"HTTPS with public certificate"* option and upload your own certificate and key.

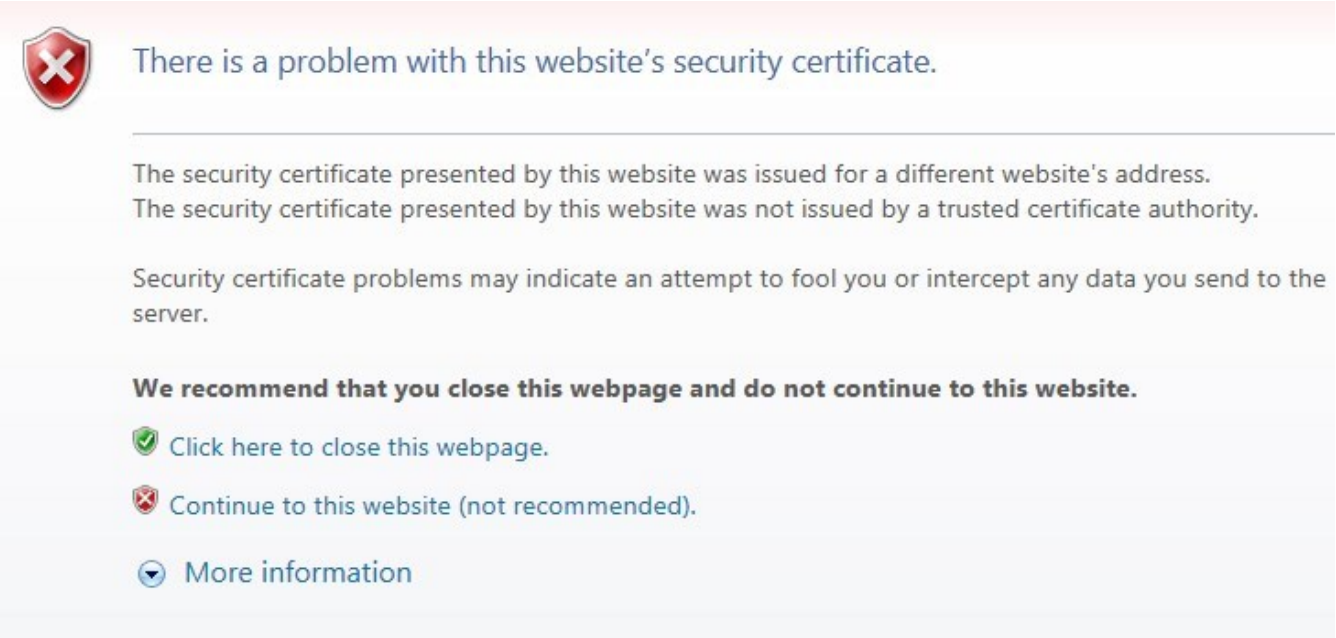


All changes should be confirmed by clicking *"Save"*.

After starting HTTPS encryption, connect to the camera via a browser, adding the prefix "https: //" before the address.

DEVICES ACCESS RESTRICTIONS

When selecting the certificate stored in the camera ("*HTTPS with unique certificate"* option), Internet Explorer may display a message about problems with the security certificate.



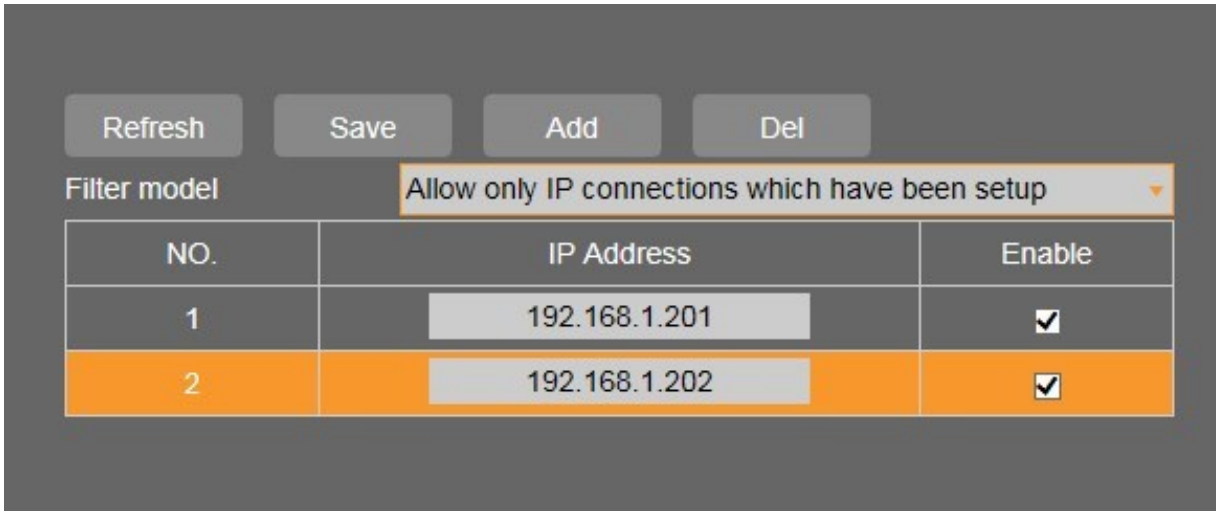
This is because the certificate was issued by a certification authority that is not recognized by the browser. Click on the *"Continue to this website (not recommended)"* link. After clicking, the camera login page should open.
To prevent this prompt from appearing on your next camera login, you can install the certificate on your system.

2.2.4. Devices access restrictions

According to the above recommendations, in order to provide adequate protection against unauthorized access, it is recommended to prepare a separate LAN subnet dedicated only to the monitoring system. In addition, remote access to devices located in a dedicated subnet (such as a recorder, cameras) should be secured by a firewall that filters traffic at the TCP / IP level.

The additional solution is to use IP filtering. This functionality is available directly on the device. It allows to define devices that will be able to connect to the device remotely. The rule can be set by adding the IP address of the trusted device (L3 layer).

To configure the list, enable the filtering function in the *„Network"* menu, *„IP filter"* submenu. Then enable *„Allow only IP connections which have been setup"* and add IP addresses which will be able to connect to the device remotely.



After defining the list, all changes have to be accepted by *„Save”* button.

2.2.4. Remote access to device – VPN

According to the above recommendations, the preferred option of remote access to devices from / through untrusted networks (e.g. Internet) is to set up a VPN tunnel that will protect communication between devices.

VPN architecture:

- *P2S VPN (Point to Site)* – in case of connecting to the device directly from a user station located in an untrusted network. This station should have an application installed to set up session. The tunnel is usually set up for the purposes of logging in to the system once.
- *S2S VPN (Site to Site)* – in case of connecting to a device from a trusted network (e.g., a second company location). A tunnel set up permanently between locations on edge devices.

AAT Holding S.A.
ul. Puławska 431, 02-801 Warszawa
tel.: (22) 546 0 700, fax: (22) 546 0 719
www.novuscctv.com

9.10.2019 TF PF v.1.0

Rekomendacje ustawień bezpieczeństwa

Kamery IP serii 4000

NOVUS®

SPIS TREŚCI

pl

KONFIGURACJA WSTĘPNA

1. Informacje wstępne

Poniższa instrukcja opisuje rekomendowane ustawienia kamery serii 4000 marki Novus, umożliwiające w odpowiedni sposób chronić dostęp do urządzania oraz dane na nim przetwarzane.
Obszary:

- wstępna konfiguracja
- nadawanie uprawnień / zarządzanie kontami
- polityka haseł
- konfiguracja sieciowa urządzenia
- zdalny dostęp

2. Konfiguracja wstępna

2.1 Konta i dostęp

2.1.1 Rekomendacje dotyczące dostępu do systemu

- Kamera powinna być zlokalizowana w bezpiecznym miejscu uniemożliwiającym dostęp do niej osobom nieupoważnionym. W przypadku, gdyby było niemożliwe, należy stosować kamery w obudowach wandaloodpornych.
- System powinien być aktualizowany na bieżąco pod kątem poprawek dotyczących bezpieczeństwa.
- Każdy z użytkowników systemu powinien posiadać własne, indywidualne konto, które w łatwy sposób można powiązać z konkretną osobą.
- Uprawnienia do systemu powinny być nadawane na podstawie zgody właściciela systemu bądź osoby do tego uprawnionej.
- Raz na pół roku powinna odbywać się weryfikacja aktywnych kont w systemie.
- Weryfikacja powinna być wykonywana przez właściciela systemu bądź osoby do tego uprawnione.
- Dostęp administracyjny powinien być nadany tylko i wyłącznie osobie odpowiedzialnej za konfigurację systemu.
- Wbudowane konto administratora powinno być odpowiednio zabezpieczone i wykorzystywane w nagłych przypadkach.
- Nazwa konta administratora powinna być zmieniona z domyślnego na inną.
- Hasło do konta powinno zostać spisane oraz odpowiednio zabezpieczone (kartka, PenDrive bądź inne medium zlokalizowane w bezpiecznym miejscu, np. sejf).

Polityka hasła do konta administratora. Hasło powinno być:

- losowe
- o maksymalnej dostępnej długości
- posiadać minimum 2 znaki specjalne
- zawierać minimum jedną cyfrę oraz jedną dużą literę
- nie zawierać wyrazów słownikowych
- nie zawierać nazwy użytkownika w haśle

KONFIGURACJA SZCZEGÓŁOWA

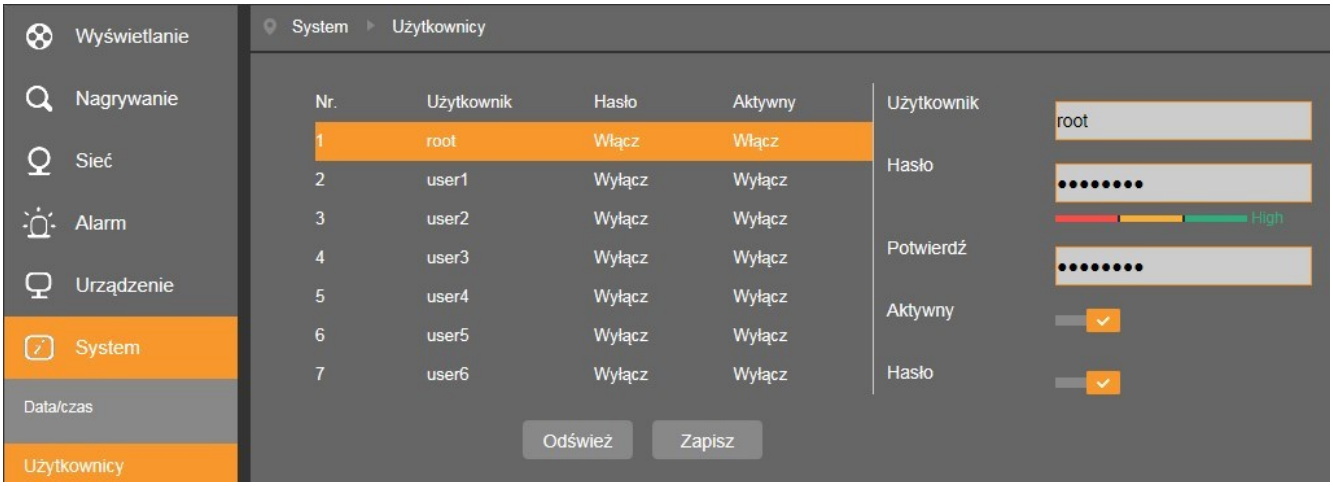
pl

Polityka haseł oraz rekomendowane ustawienia haseł dla pozostałych kont:
Hasło do pozostałych kont powinno być:

- losowe
- o maksymalnej dostępnej długości
- posiadać minimum 2 znaki specjalne
- zawierać minimum jedną cyfrę oraz jedną dużą literę
- nie zawierać wyrazów słownikowych
- nie zawierać nazwy użytkownika w haśle
-

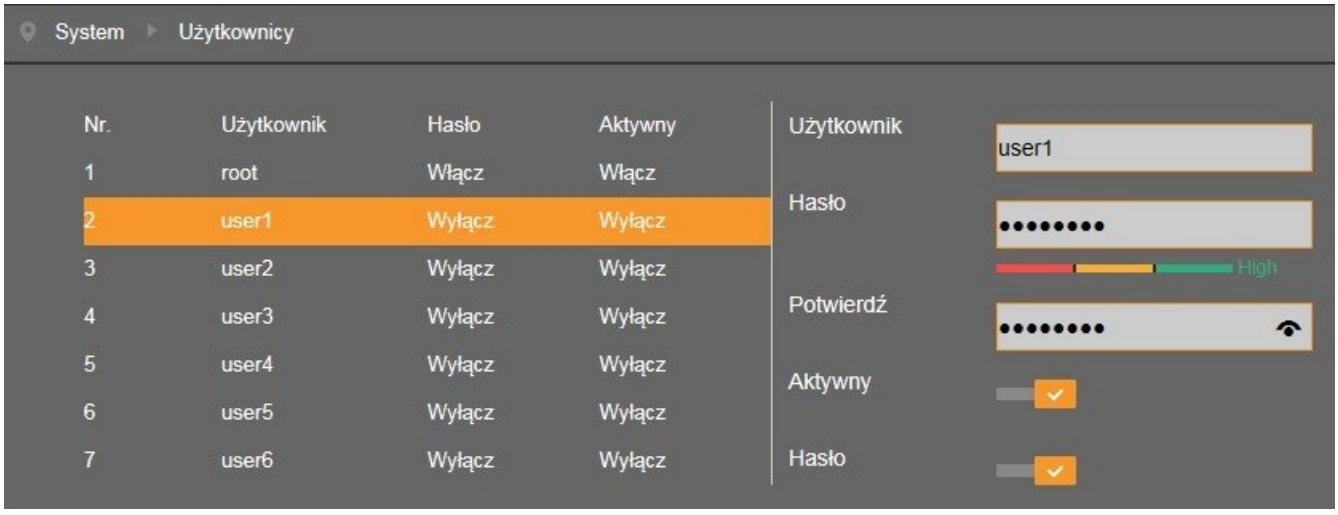
2.1.2 Konfiguracja szczegółowa

W menu kamery *„System”*, wybieramy podmenu *„Użytkownicy”*.



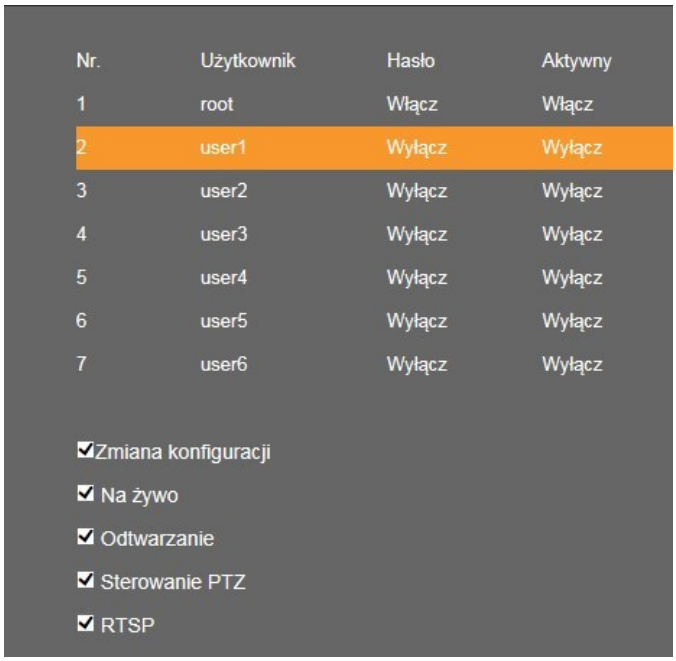
Aktywacja i nadanie odpowiednich uprawnień nowemu użytkownikowi rozpoczynamy przez zaznaczenie odpowiedniego wiersza na liście użytkowników.

Aktywowanie nowego konta



Po zaznaczeniu wiersza z kontem użytkownika aktywujemy je przełącznikiem *„Aktywuj”* i włączamy ochronę hasłem przełącznikiem *„Hasło”*. Następnie ustalamy nazwę konta i hasło zgodnie z zaleceniami podanymi w rozdziale 2.1.1

Ustawienia uprawnień użytkownika



W kolejnym etapie ustalamy uprawnienia przyznane użytkownikowi, przez zaznaczenie odpowiedniej opcji. Po zakończeniu konfiguracji zapisujemy zmiany przyciskiem „Zapisz”.

2.2 Konfiguracja sieciowa

2.2.1 Konfiguracji sieci LAN

Zalecane jest ustawienie statycznego adresu IP kamery.

W celu zapewnienia odpowiedniej ochrony przed nieautoryzowanym dostępem, zalecane jest przygotowanie oddzielnej podsieci LAN dedykowanej tylko i wyłącznie dla systemu monitoringu. Zdalny dostęp do urządzeń znajdujących się w dedykowanej podsieci (takich jak rejestrator, kamery) powinien być zabezpieczony przez zaporę sieciową filtrującą ruch na poziomie warstwy L3 oraz L4:

- zdalny dostęp do rejestratora możliwy tylko z dedykowanego urządzenia
- otwarte porty sieciowe:
  - HTTP – port TCP 80
  - HTTPS – port TCP 443 (rekomendowany port komunikacji z rejestratorem)
  - Port serwera – TCP 9988
  - RTSP – port TCP 554

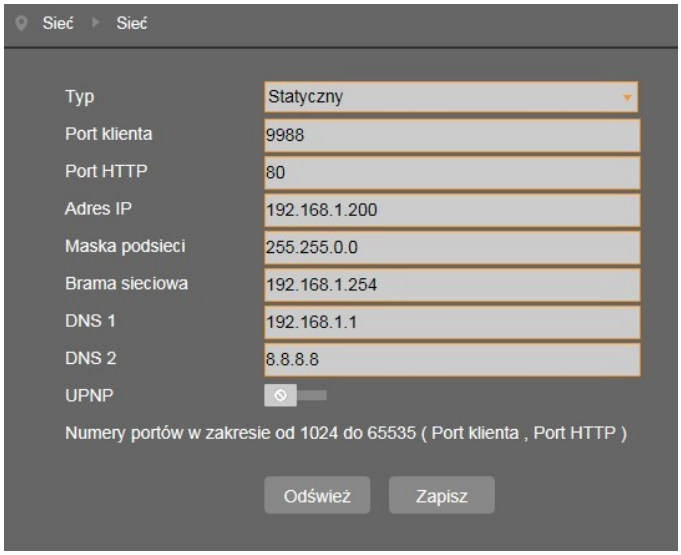
Ze względów bezpieczeństwa nierekomendowane jest ustawienia publicznego adresu IP na urządzeniu oraz udostępnianie go bezpośrednio z Internetu.

W przypadku wymaganego dostępu do urządzenia z innej lokalizacji bądź bezpośrednio z Internetu, rekomendowane jest wykorzystanie szyfrowanego tunelu VPN.

KONFIGURACJA SIECIOWA

Szczegółowa konfiguracja sieci

W menu kamery *„Sieć”*, wybieramy podmenu *„Sieć”*. W tej zakładce znajdują się ustawienia TCP/IP



2.2.2 Konfiguracja sieci WiFi

W przypadku kamer z możliwością pracy w sieciach bezprzewodowych, konieczne jest odpowiednie skonfigurowanie sieci WiFi.

W celu zapewnienia odpowiedniej ochrony przed nieautoryzowanym dostępem, zalecane jest przygotowanie oddzielnej podsieci WiFi, dedykowanej tylko i wyłącznie dla systemu monitoringu. Ze względów bezpieczeństwa należy zmodyfikować ustawienia routera tak, by uniemożliwić a przynajmniej w znacznym stopniu utrudnić nieautoryzowany dostęp do sieci WiFi. Podstawowe zalecenia to:

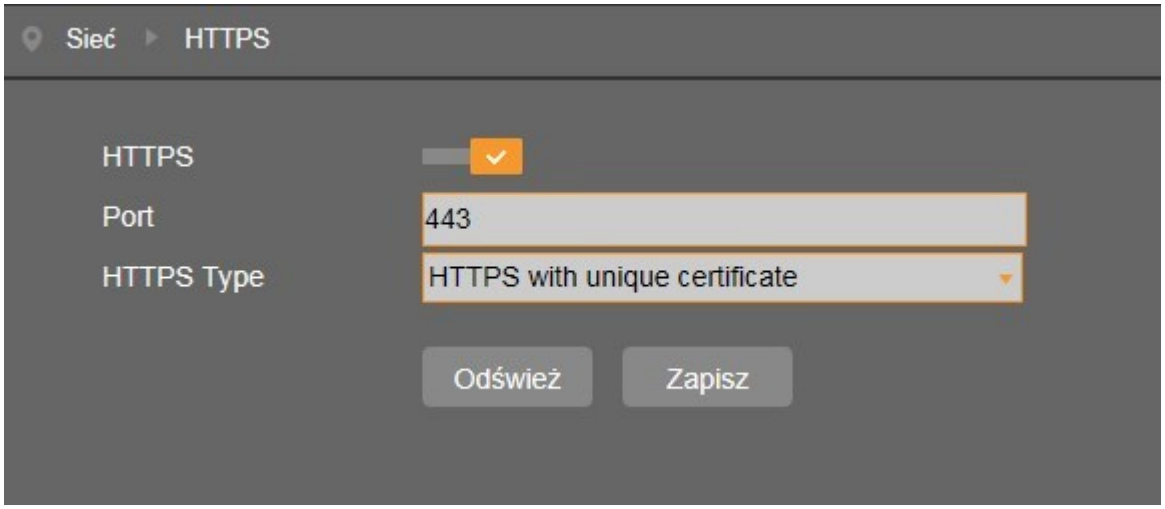
- zmiana danych potrzebnych do zalogowania się do routera zgodnie z zaleceniami podanymi w rozdziale 2.1.1
- w konfiguracji zabezpieczeń należy włączyć szyfrowanie WPA lub WPA2
- należy zmienić nazwę sieci bezprzewodowej (SSID) z domyślnej na inną, nie kojarzącą się z systemem CCTV, a najlepszym rozwiązaniem jest ukrycie nazwy sieci
- należy ograniczyć liczbę dozwolonych połączeń. Należy włączyć opcję definiowania listy urządzeń, które mogą połączyć się z siecią („white list” lub „allow list”), i dodać tam adresy MAC urządzeń CCTV
- należy wyłączyć obsługę Wifi Protected Setup (WPS)
- należy wyłączyć możliwość zdalnego dostępu do routera - “Remote access”
- należy wyłączyć serwer DHCP w routerze i należy ustawić stałe adresy IP wszystkich urządzeń w sieci

Ze względów bezpieczeństwa nierekomendowane jest ustawienia publicznego adresu IP na urządzeniu oraz udostępnianie go bezpośrednio z Internetu.

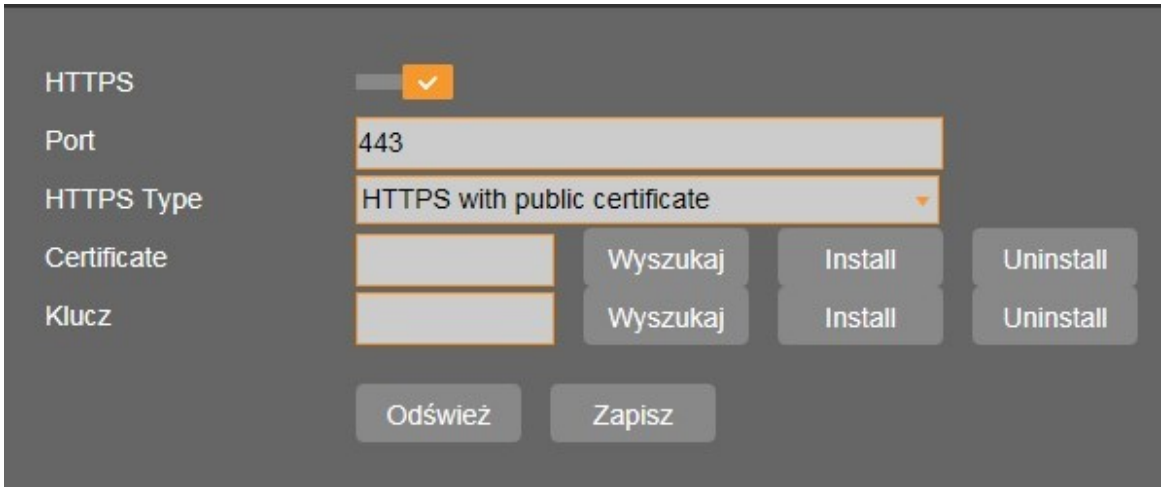
pl

2.2.3 Konfiguracja połączenia HTTPS

Aby uruchomić możliwość logowania się do panelu administracyjnego po HTTPS, należy zalogować się z do kamery przez przeglądarkę, wejść do zakładki *„Ustawienia zdalne”* i wybrać opcję *„HTTPS”* w sekcji *„Sieć”*.



W następnym kroku należy włączyć szyfrowanie HTTPS. Kolejne opcje pozwalają zmienić port HTTPS (zalecane jest pozostawienie domyślnego portu 443), oraz wybrać typ certyfikatu. Można wykorzystać certyfikat zapisany w kamerze (opcja *„HTTPS with unique certificate”*), lub wybrać opcję *„HTTPS with public certificate”* i wgrać własny certyfikat i klucz.



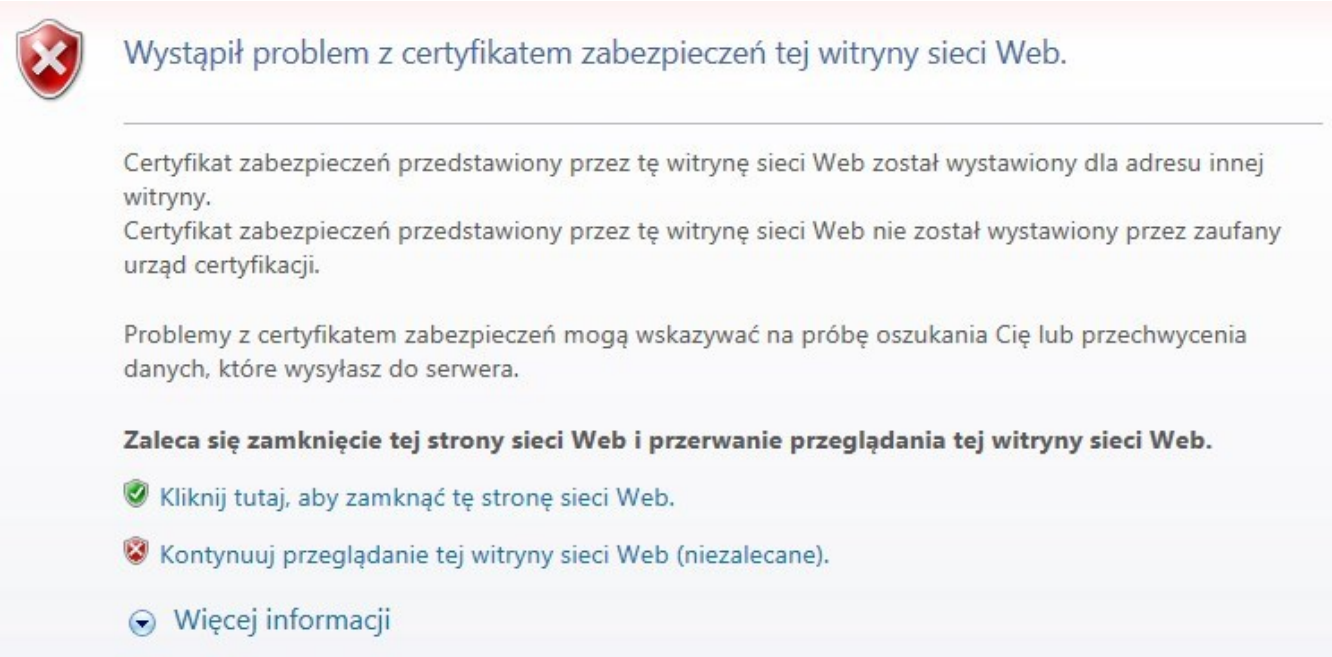
Wszystkie zmiany należy zatwierdzić przyciskiem *„Zapisz”*.

Po uruchomieniu szyfrowania HTTPS, należy połączyć się z kamerą przez przeglądarkę, dodając przed adresem prefiks *„https://”*.

KONFIGURACJA SIECIOWA

pl

Przy wybraniu certyfikatu zapisanego w kamerze (opcja *„HTTPS with unique certificate”*), przeglądarka Internet Explorer może wyświetlić komunikat o problemach z certyfikatem zabezpieczeń.



Jest to spowodowane tym, że certyfikat został wystawiony przez urząd certyfikacji, który nie jest rozpoznawany przez przeglądarkę. Należy kliknąć na łącze *„Kontynuuj przeglądanie tej witryny sieci Web (niezalecane)”*. Po kliknięciu powinna otworzyć się strona logowania do kamery.
Aby przy kolejnych logowaniach do kamery nie wyświetlał się ten monit, można certyfikat zainstalować w systemie.

2.2.4. Ograniczenie dostępu do urządzeń

Zgodnie z powyższymi rekomendacjami, w celu zapewnienia odpowiedniej ochrony przed nieautoryzowanym dostępem zalecane jest przygotowanie oddzielnej podsieci LAN dedykowanej tylko i wyłącznie dla systemu monitoringu. Dodatkowo zdalny dostęp do urządzeń znajdujących się w dedykowanej podsieci (takich jak rejestrator, kamery) powinien być zabezpieczony przez zaporę sieciową filtrującą ruch na poziomie TCP/IP.

Dodatkowym rozwiązaniem będzie ustawienie tzw. „Czarnej i białej listy”. Funkcjonalność ta jest dostępna bezpośrednio w urządzeniu. Umożliwia ona definiowanie urządzeń, które będą mogły łączyć się zdalnie do urządzenia. Regułą może być ustawiona poprzez dodanie adresu IP zaufanego urządzenia (warstwa L3).

W celu skonfigurowania listy należy w Menu *„Sieć”*, podmenu *„Filtrowanie IP”* włączyć funkcję filtrowania. Następnie należy włączyć opcję *„Zezwalaj na poniższe adresy IP”* i dodać adresy IP, z których będzie możliwość zdalnego nawiązywania połączenia do urządzenia.

Po zdefiniowaniu listy, całość zmian akceptujemy przyciskiem „*Zapisz*”.

2.2.4. Zdalny dostęp do urządzenia – VPN

Zgodnie z powyższymi rekomendacjami, preferowaną opcją zdalnego dostępu do urządzeń z / przez sieci niezaufane (np. Internet) jest zestawienie tunelu VPN który będzie chronił komunikację pomiędzy urządzeniami.

Architektura VPN:

- *P2S VPN (Point to Site)* – w przypadku podłączenia się do urządzenia bezpośrednio ze stacji użytkownika znajdującego się w sieci niezaufanej. Stacja ta powinna mieć zainstalowaną aplikację umożliwiającą zestawienie sesji. Tunel najczęściej zestawiany jest na potrzeby jednorazowego zalogowania się do systemu.
- *S2S VPN (Site to Site)* – w przypadku podłączenia się do urządzenia z sieci zaufanej (np. drugiej lokalizacji firmy). Tunel zestawiany na stałe pomiędzy lokalizacjami na urządzeniach brzegowych.

AAT Holding S.A.
ul. Puławska 431, 02-801 Warszawa
tel.: (22) 546 0 700, fax: (22) 546 0 719
www.novuscctv.com

9.10.2019 TF PF v.1.0