Security settings recommendations for NHDR and NVR 4000 series Novus recorders

NOVUS®

TABLE OF CONTENTS

Table of contents

1. Preliminary informations

The following instructions describe the recommended settings of the Novus NHDR or NVR 4000 series recorder 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 recorder should be located in a safe place preventing unauthorized access (e.g. server room, locked room, etc.)
- the system should be updated regularly by security patches
- 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
- administrator 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 "admin" to another
  - ◊ account password should be written down and properly secured (sheet of paper, PenDrive or other medium located in a safe place, e.g. safe)
  - ◊ account password
    - * random
    - * 10-15 characters long

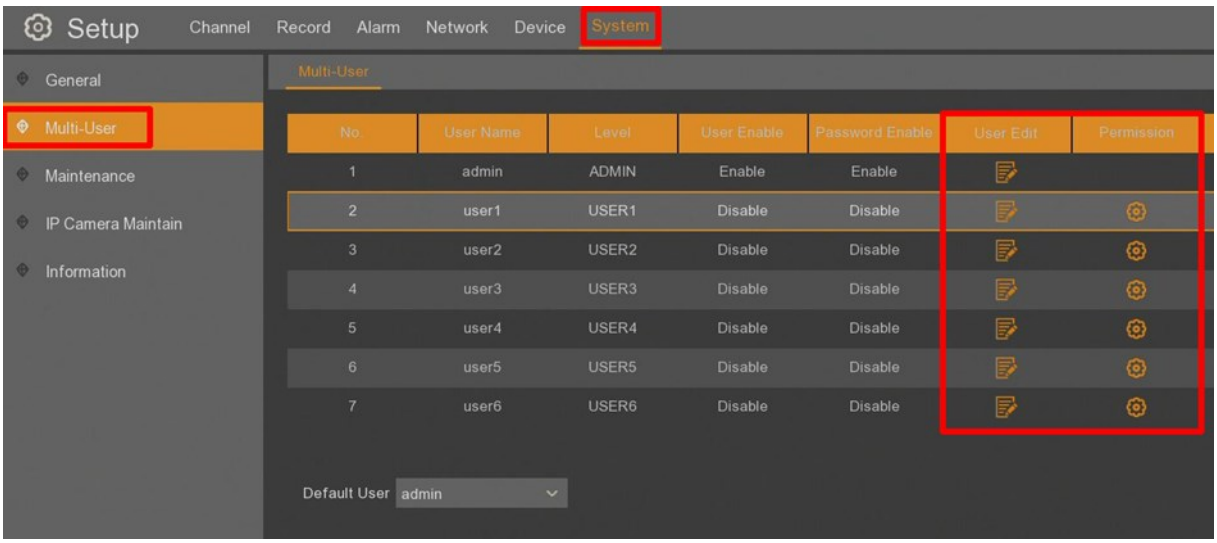
INITIAL CONFIGURATION

        - contains a minimum 2 special characters
        - contains a minimum one number and one upper case letter
        - does not contain dictionary words
        - does not contain the username in the password
    - it is recommended not to enable the function unlock pattern
- password policy and recommended password settings for other account
    - password policy
        - random
        - minimum length of 8 characters
        - contains a minimum 2 special characters
        - contains a minimum one number and one upper case letter
        - does not contain dictionary words
        - does not contain the username in the password
- it is recommended not to configure the *„Email”* settings in the *„Network”* recorder menu

2. 1. 2. Detailed configuration

In the *„System”* recorder menu, select the *„Multi-user”* submenu.

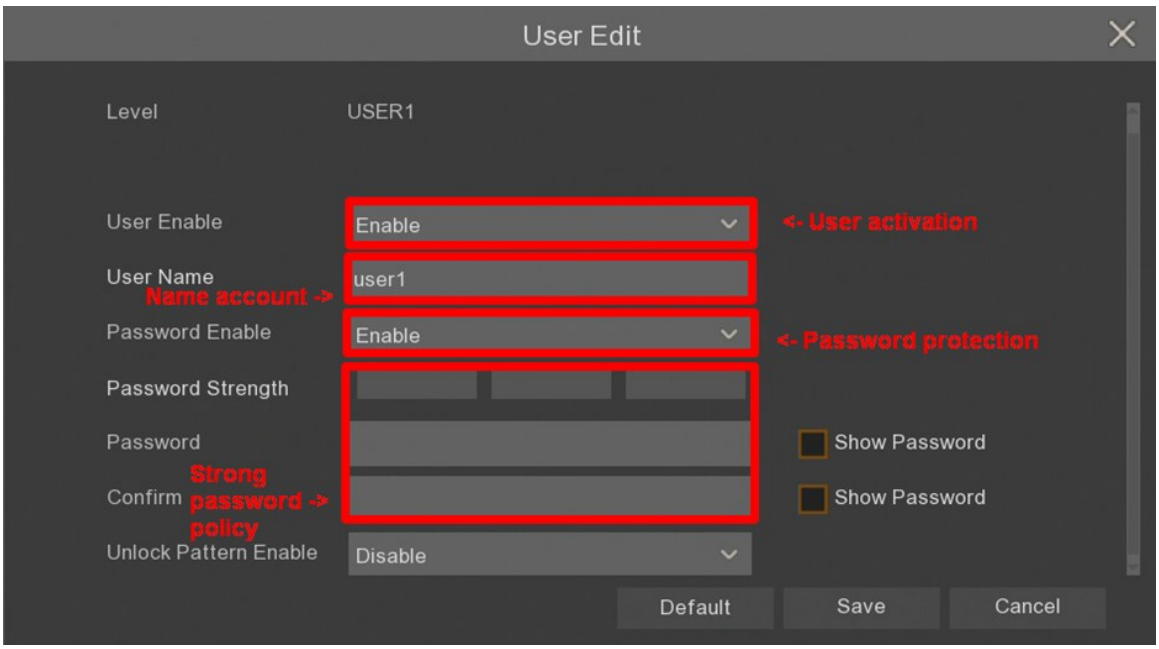
The icon in the *„User Edit”* column allows to activate a new user account. The icon in the *„Permission”* column allows to define its permissions.



INITIAL CONFIGURATION

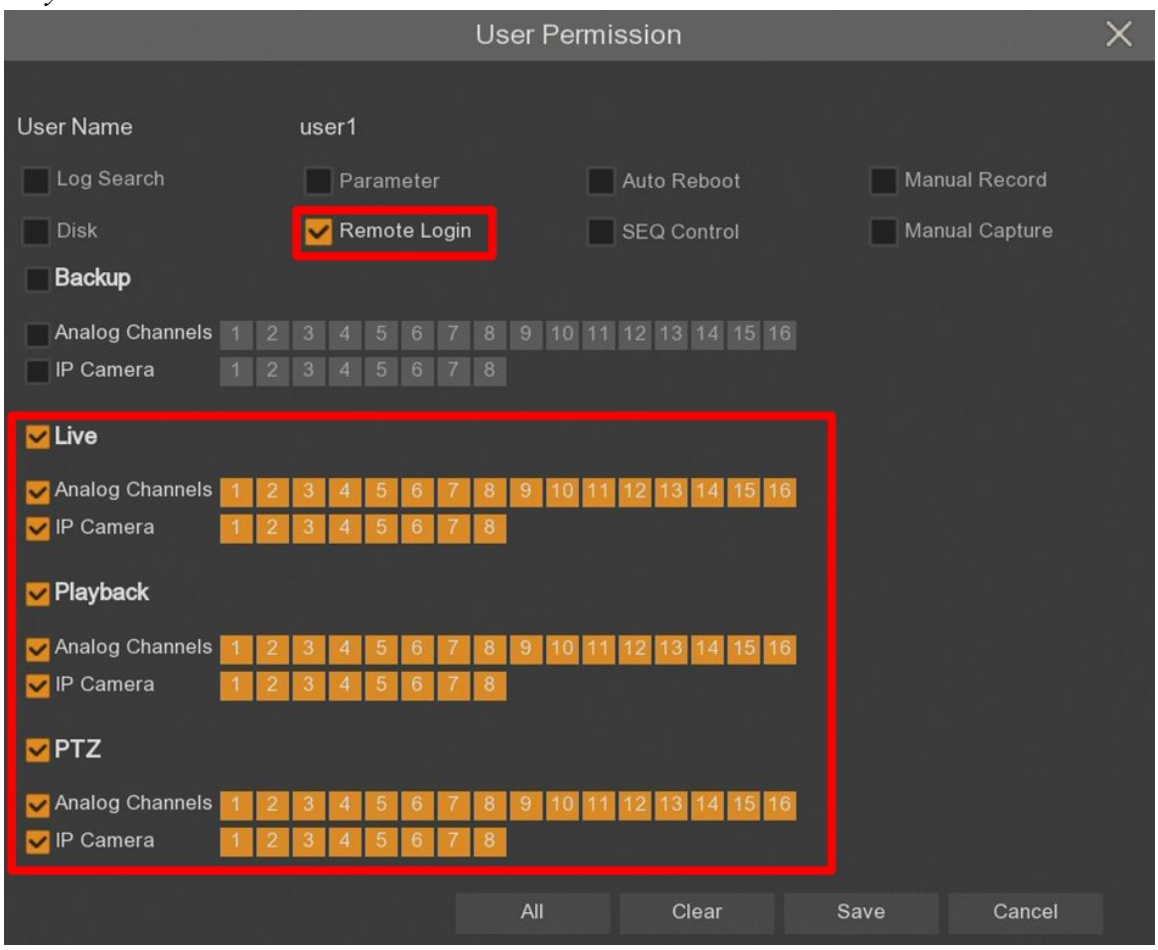
New account activation

Menu -> System -> Multi-User -> User Edit



User permission settings

Menu -> System -> Multi-User -> Permission



eng

INITIAL CONFIGURATION

2. 2. Network Configuration

2. 2. 1. LAN configuration

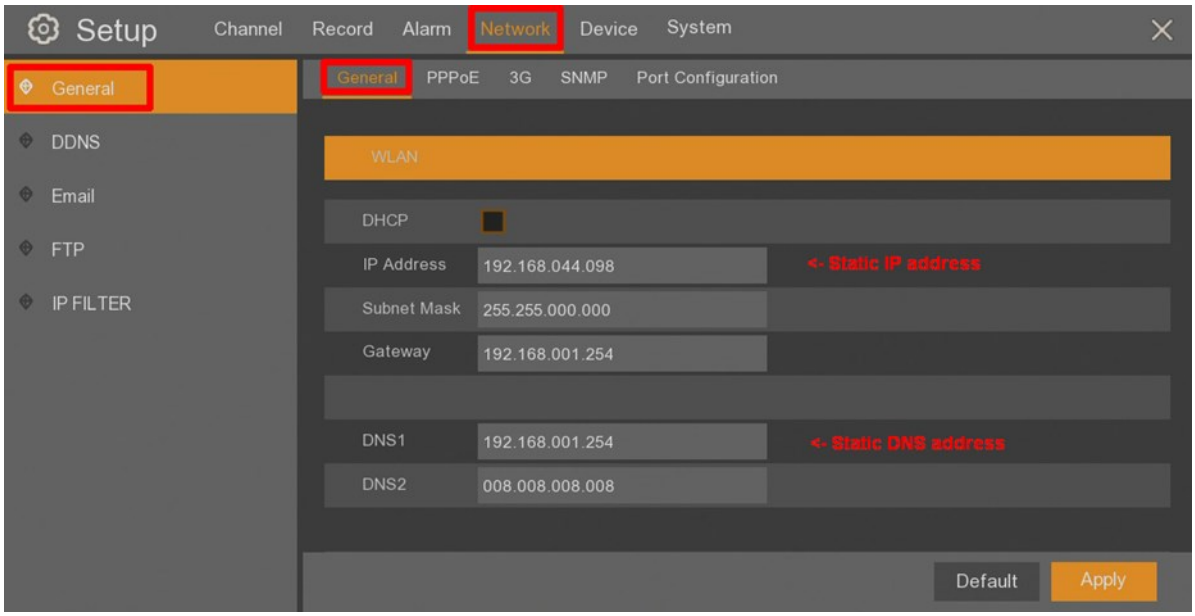
It is recommended to have physical access to the recorder (connected mause and monitor). It is important especially for access with administrator privileges to configure the device.

Recommendations for remote access:

- it is suggested to set the recorder static IP address
- it is recommended to prepare a separate LAN subnet dedicated only to the monitoring system to provide adequate protection against unauthorized access
- 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 recorder possible only from a dedicated device
  - ◊ open network ports
    - * HTTP – 80 TCP port
    - * HTTPS – 443 TCP port (recommended communication port with the recorder)
    - * Server port – 9000 TCP port
    - * RTSP – 554 TCP port
  - ◊ for security reasons it is not recommended to set the public IP address on the device and share it directly from the Internet
  - ◊ in the case of required access to the device from another location or directly from the Internet, it is recommended to use an encrypted VPN tunnel

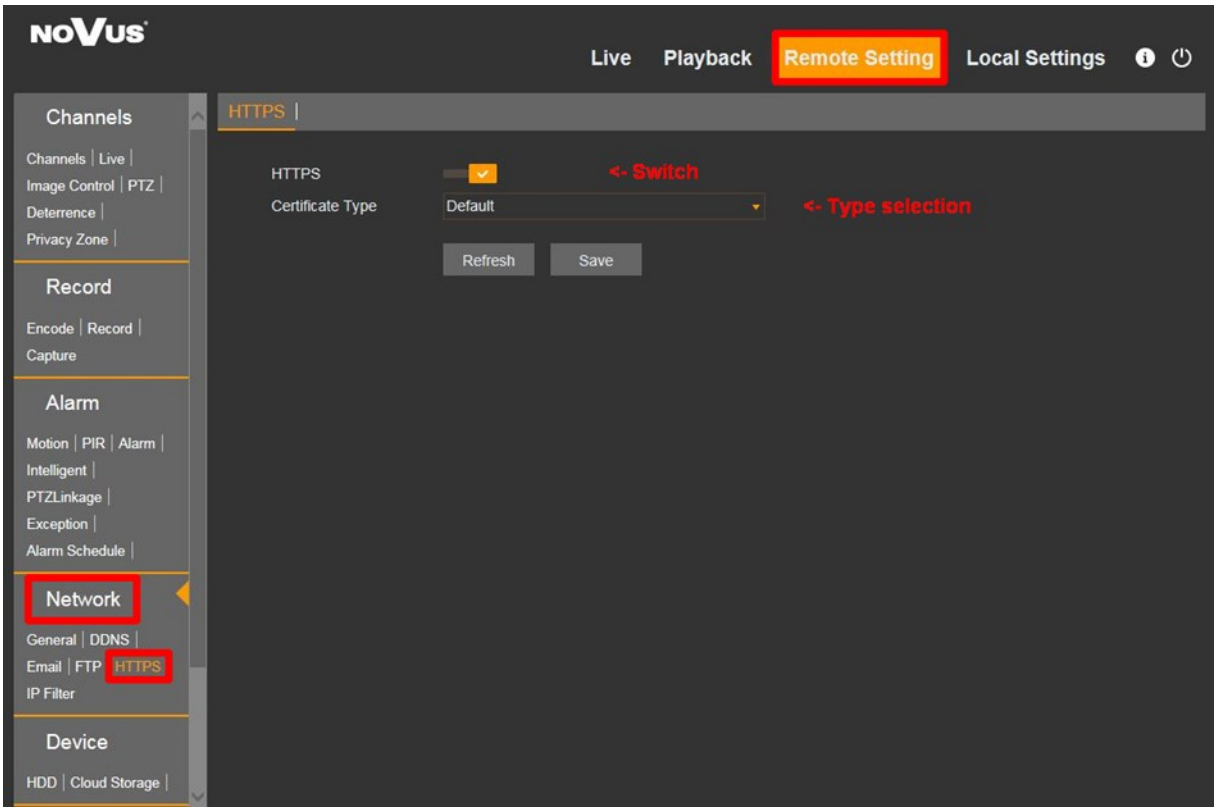
Detailed network configuration

Select the *„General”* submenu in the *„Network”* recorder menu. The *„General”* tab has TCP / IP settings.

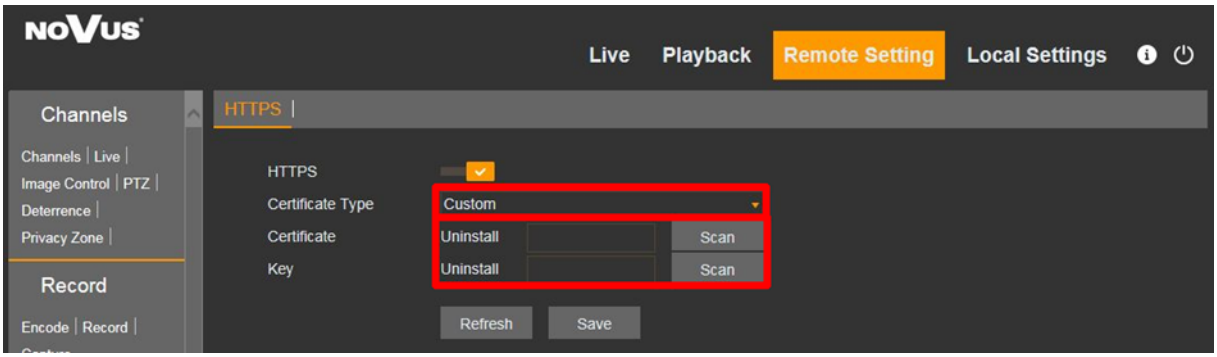


2. 2. 2. HTTPS connection configuration

To enable logging into the administration panel using HTTPS protocol, log in to the recorder through the browser, enter *„Remote settings”* and select *„HTTPS”* in the *„Network”* section.



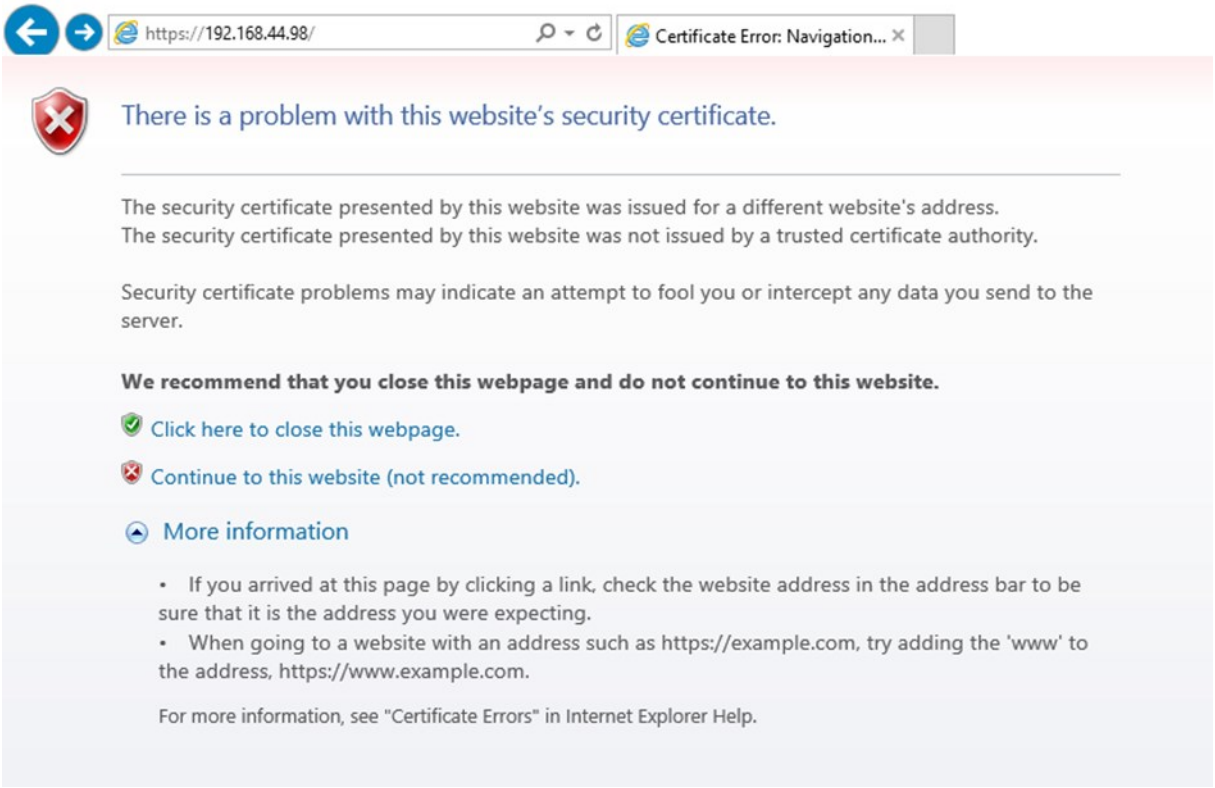
In the next step, enable HTTPS encryption and select the *„Certificate Type”*. It can be used the *„Default”* type of recorder certificate or upload another certificate and key by selecting the *„Custom”* option.



All changes should be confirmed using *„Save”* button.

INITIAL CONFIGURATION

After starting HTTPS encryption, run a browser and connect to the recorderusing the prefix *„https://”*. In the Internet Explorer browser, expand the MORE INFORMATION button and click on CONTINUE TO THIS WEBSITE (NOT RECOMMENDED). After that, the recorder login page should open.



eng

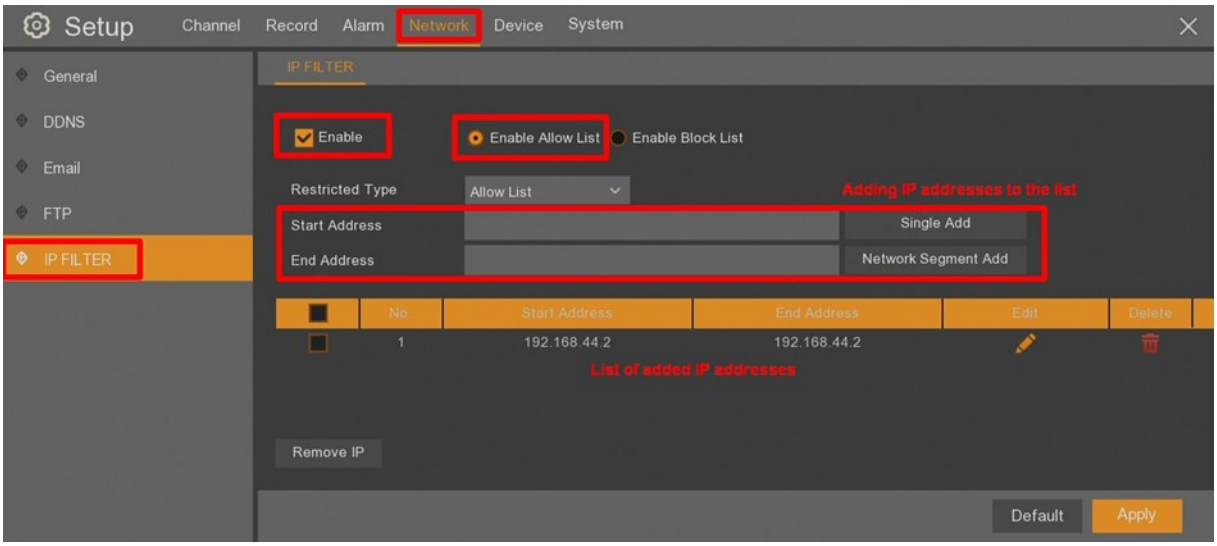
2. 2. 3. Devices access restrictions

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 filtering”* submenu. Then enable *„Alow white list”* 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 *„Apply”* button.



2. 2. 4. Remote access to device – VPN

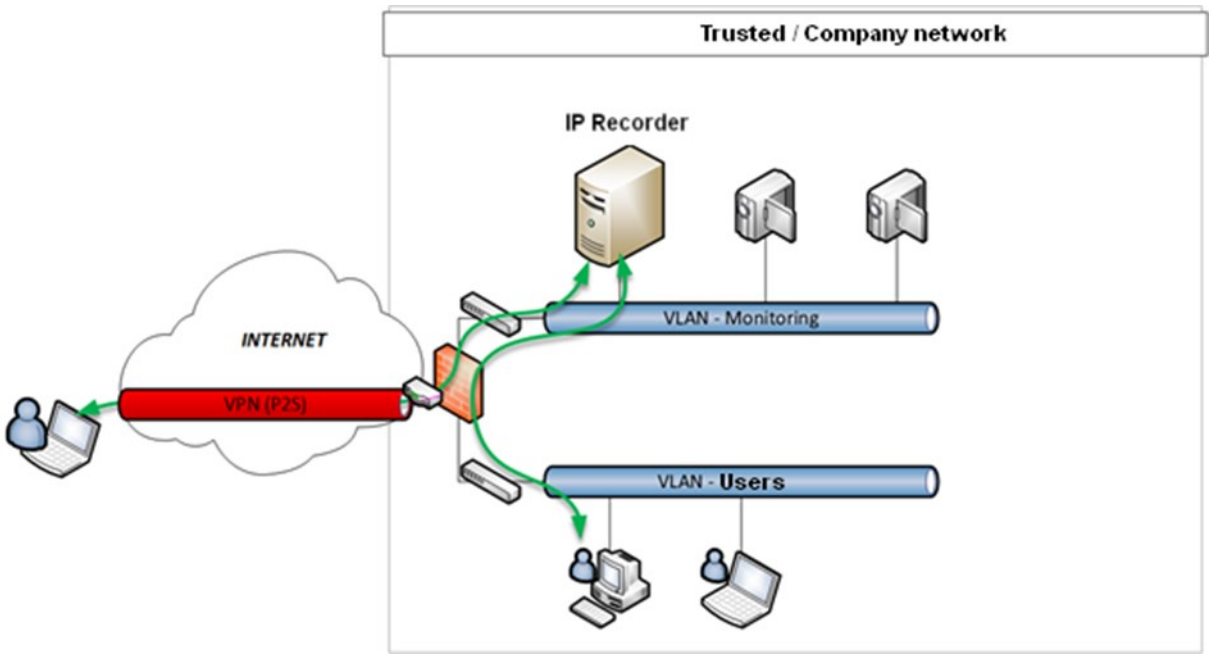
According to the above recommendations, the preferred option of remote access to devices from / through untrusted networks (e.g. Internet) is to set up a VPN tunnel that will protect communication between devices.

VPN architecture:

1. *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.
2. *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.

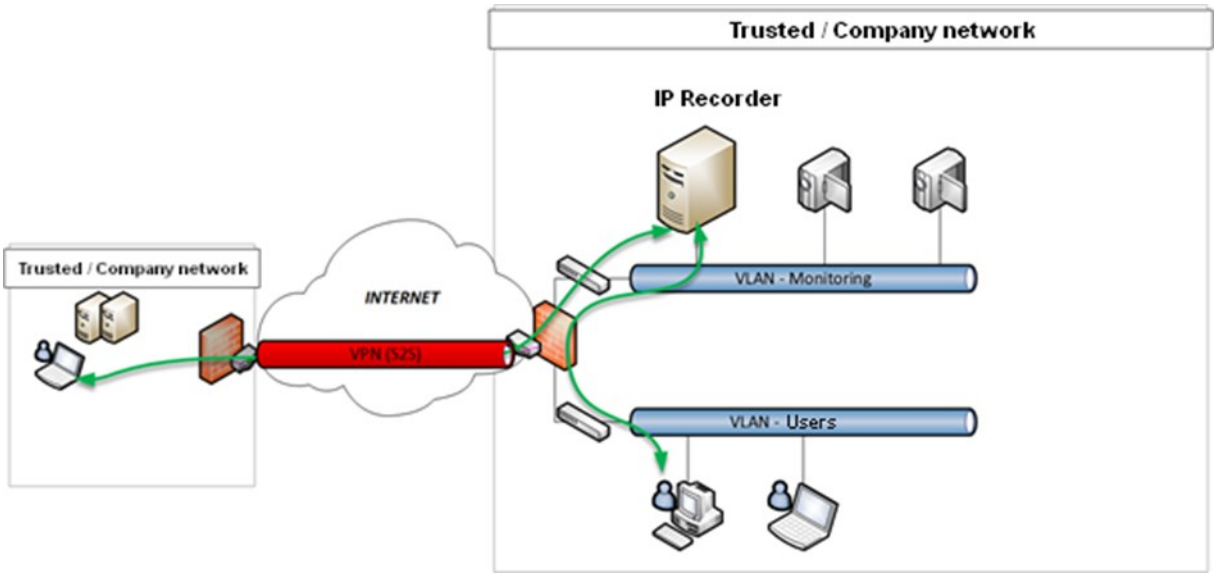
INITIAL CONFIGURATION

1. P2S VPN scheme (Point to Site)



Point to Site VPN

2. S2S VPN scheme (Site to Site)



Site to Site VPN

INITIAL CONFIGURATION

Recommended encryption algorithms for the connection

Acceptable algorithms	
Symmetric Key Algorithms	AES-128, AES-192, AES-256
Cipher modes	GCM, CBC with integrity check (SHA),
Hashing Algorithms	SHA-256, SHA-512, SHA-3
Diffie-Hellman	Group 14 (2048) or higher
RSA	Factoring modulus ≥ 2048
Elliptic Curves (f)	f ≥ 256
Key Exchange	IKEv2
Transport layer protocols	TLS1.2

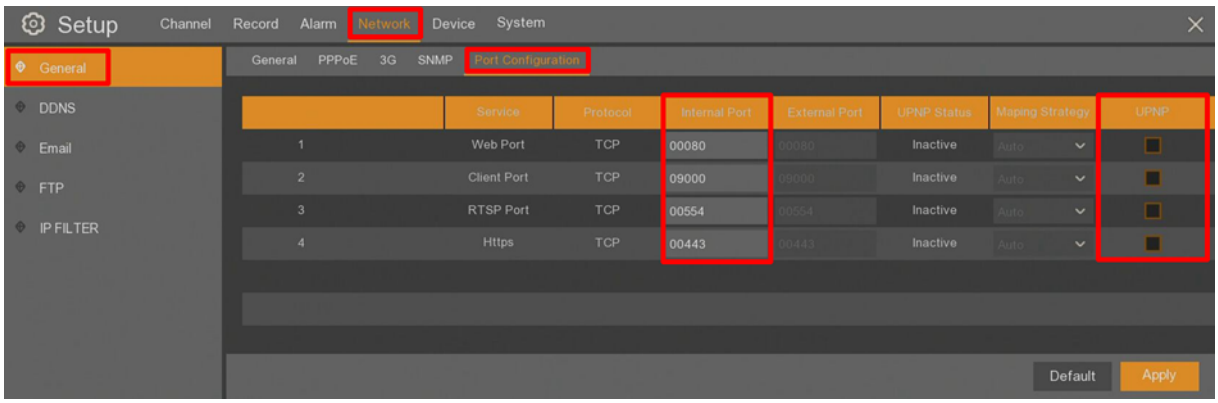
The device also allows to use the UPnP (Universal Plug-and-Play) protocol to connect to some network services remotely. To use this option:

- activate the option directly on the device (see instructions below)
- in case of providing Internet services, run the UPnP option on the edge router

IMPORTANT: for security reasons, it is not recommended to use the UPnP protocol in remote access to devices (with particular emphasis on access from untrusted networks such as the Internet). An alternative option is to set up a VPN tunnel or ultimately provide network services on a "Port Forwarding" basis with restrictive firewall rules.

Running the UPnP option

To configure UPnP in the *„Network”* menu, *„General”* submenu, select the *„Port Configuration”* tab. The UPNP options can by enabled for individual ports in the *„UPNP”* column. It is possible to change default TCP / IP port for each service. After setting all parameters, all changes have to be accepted by *„Apply”* button.



AAT Holding S.A.
431 Pulawska St., 02-801 Warsaw, Poland
tel.: +4822 546 07 00, fax: +4822 546 07 59
www.novuscctv.com

2019-10-23 PF v1.0

Rekomendacje ustawień bezpieczeństwa dla rejestratorów NHDR i NVR serii 4000 marki Novus

NOVUS®

SPIS TREŚCI

Spis treści

pl

1. Informacje wstępne

Poniższa instrukcja opisuje rekomendowane ustawienia rejestratorów NHDR lub NVR 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. Wstępna konfiguracja

2. 1. Konta i dostęp

2. 1. 1. Rekomendacje dotyczące dostępu do systemu

- rejestrator powinien być zlokalizowany w bezpiecznym miejscu uniemożliwiającym dostęp do niego osobom nieupoważnionym (np. serwerownia, zamykane pomieszczenie itp.)
- system powinien być aktualizowany na bieżąco pod kątem poprawek dotyczących bezpieczeństwa
- każdy z użytkowników systemu powinien posiadać własne, imienne 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 „admin” na inną
  - ◊ hasło do konta powinno zostać spisane oraz odpowiednio zabezpieczone (kartka, PenDrive bądź inne medium zlokalizowane w bezpiecznym miejscu, np. sejf)
  - ◊ hasło do konta
    - * losowe
    - * długość 10-15 znaków

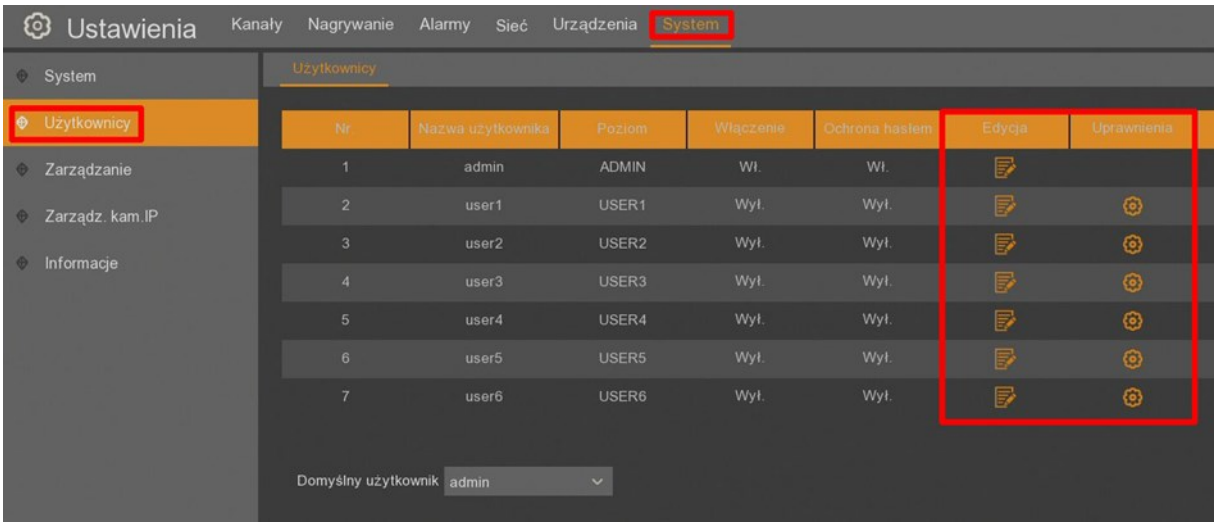
WSTĘPNA KONFIGURACJA

        - posiada minimum 2 znaki specjalne
        - zawiera minimum jedną cyfrę oraz jedną dużą literę
        - nie zawiera wyrazów słownikowych
        - nie zawiera nazwy użytkownika w haśle
    - zalecane jest niewłączanie funkcji odblokowywania wzorem
- polityka haseł oraz rekomendowane ustawienia haseł dla pozostałych kont
    - polityka haseł
        - losowe
        - długość minimum 8 znaków
        - posiada minimum 2 znaki specjalne
        - zawiera minimum jedną cyfrę oraz jedną dużą literę
        - nie zawiera wyrazów słownikowych
        - nie zawiera nazwy użytkownika w haśle
- nie należy konfigurować ustawień „Email” w Menu rejestratora *„Sieć”*

pl

2. 1. 2. Szczegółowa konfiguracja

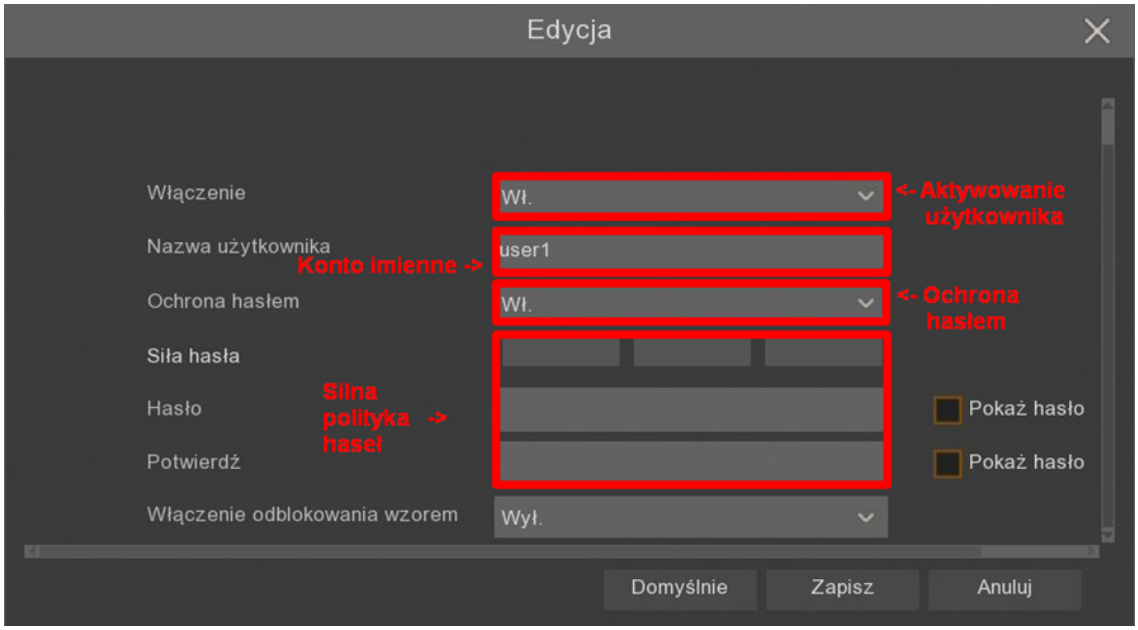
W menu rejestratora *„System”*, wybieramy podmenu *„Użytkownicy”*.



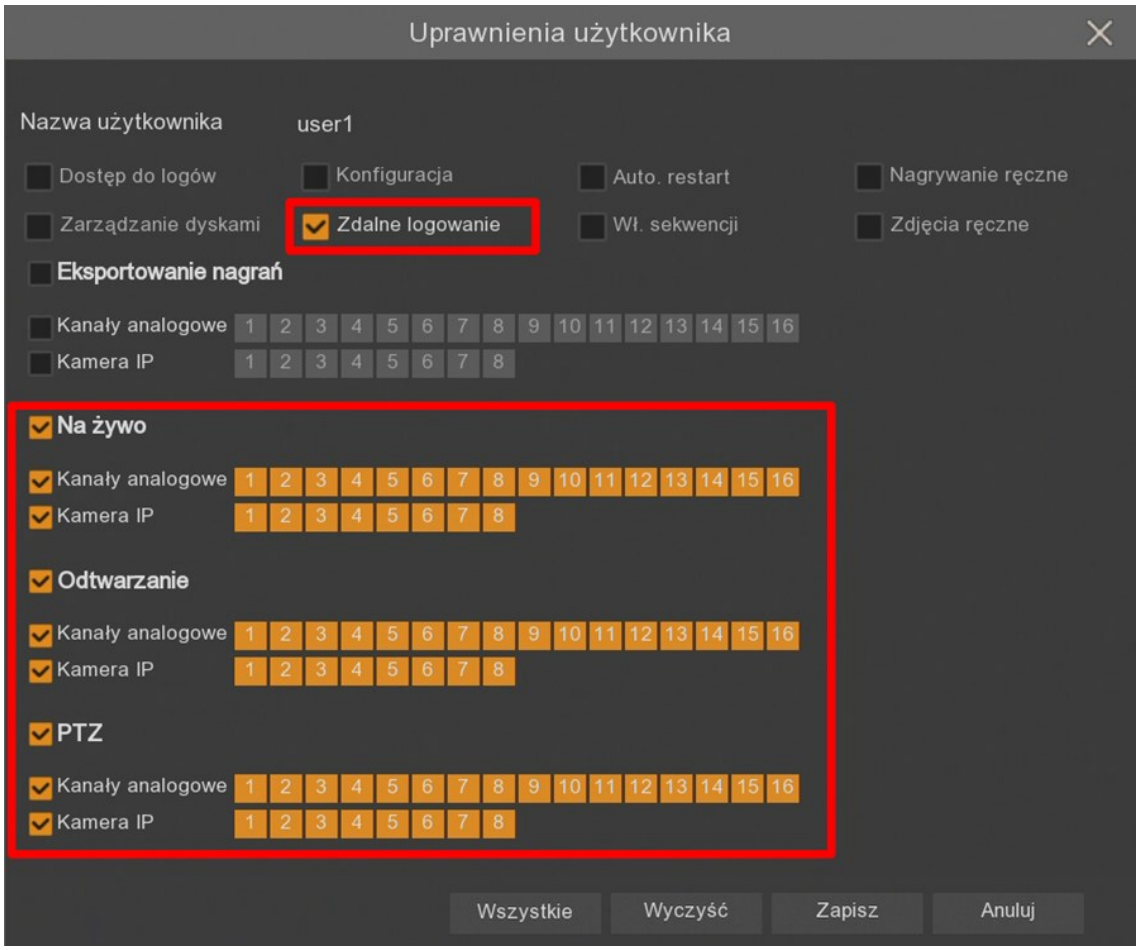
Ikona w kolumnie *„Edycja”* pozwala aktywować konto nowego użytkownika. Ikona w kolumnie *„Uprawnienia”* pozwala zdefiniować jego uprawnienia.

WSTĘPNA KONFIGURACJA

Aktywowanie nowego konta
Menu -> System -> Użytkownicy -> Edycja



Nadawanie uprawnień użytkownikówi
Menu -> System -> Użytkownicy -> Uprawnienia



pl

WSTĘPNA KONFIGURACJA

2. 2. Konfiguracja sieciowa

2. 2. 1. Konfiguracja sieci LAN

Rekomendowany jest fizyczny dostęp do rejestratora (podłączone urządzenia peryferyjne oraz monitor). Szczególnie dotyczy to dostępu z uprawnieniami administratora w celu konfiguracji urządzenia.

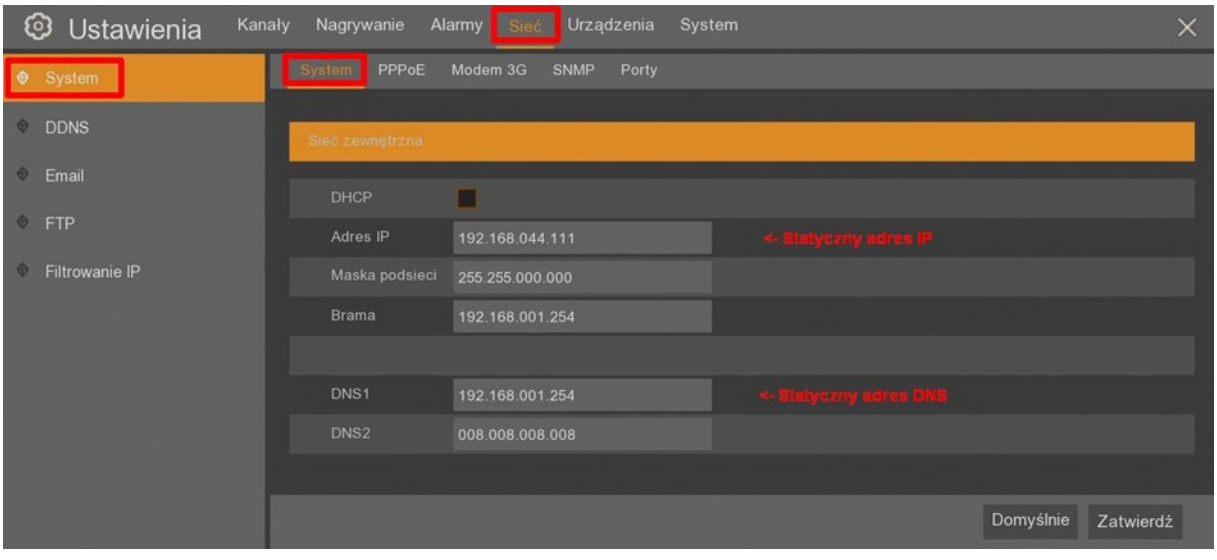
W przypadku wymaganego zdalnego dostępu

- sugerowane jest statyczne ustawienie adresu IP rejestratora
- 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 z dedykowanego urządzenia
  - ◊ otwarte porty sieciowe
    - * HTTP – port TCP 80
    - * HTTPS – port TCP 443 (rekomendowany port komunikacji z rejestratorem)
    - * Port serwera – TCP 9000
    - * 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

pl

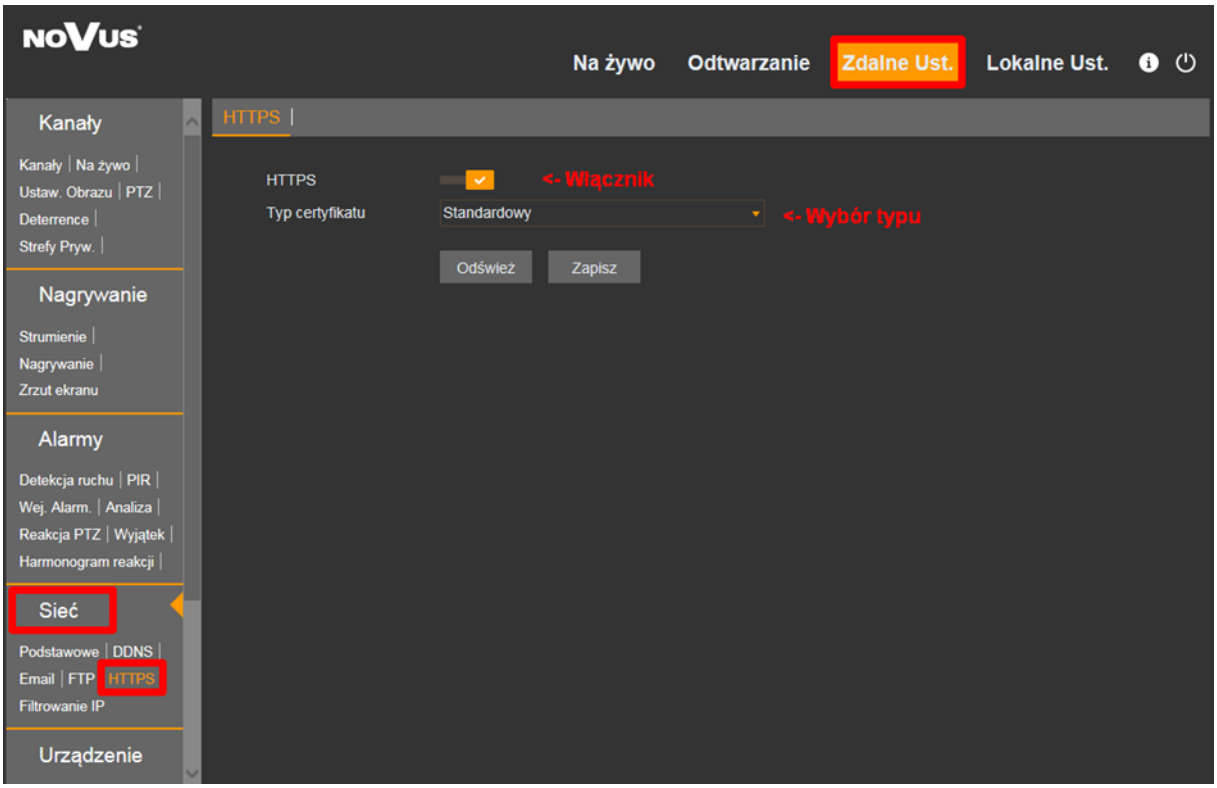
Szczegółowa konfiguracja sieci

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

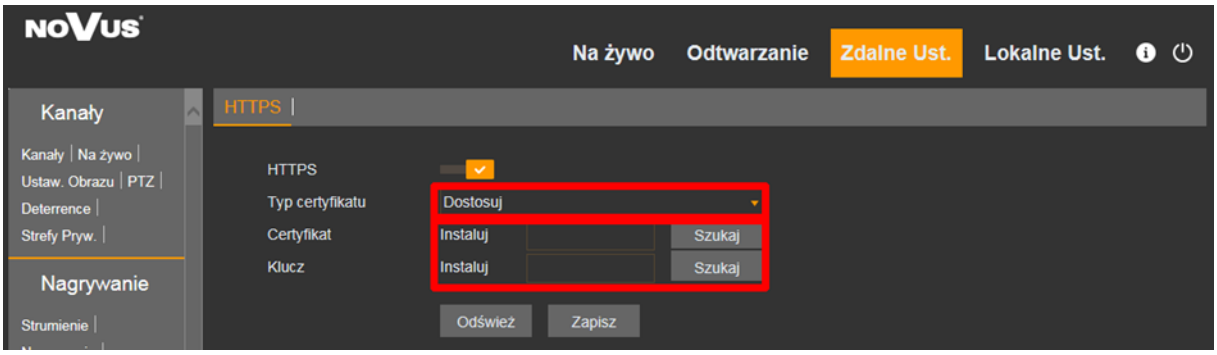


2. 2. 2. Konfiguracja połączenia HTTPS

Aby uruchomić możliwość logowania się do panelu administracyjnego używając protokołu HTTPS należy zalogować się do rejestratora przez przeglądarkę, wejść w *„Zdalne ustawienia”* i wybrać opcję *„HTTPS”* w sekcji *„Sieć”*.



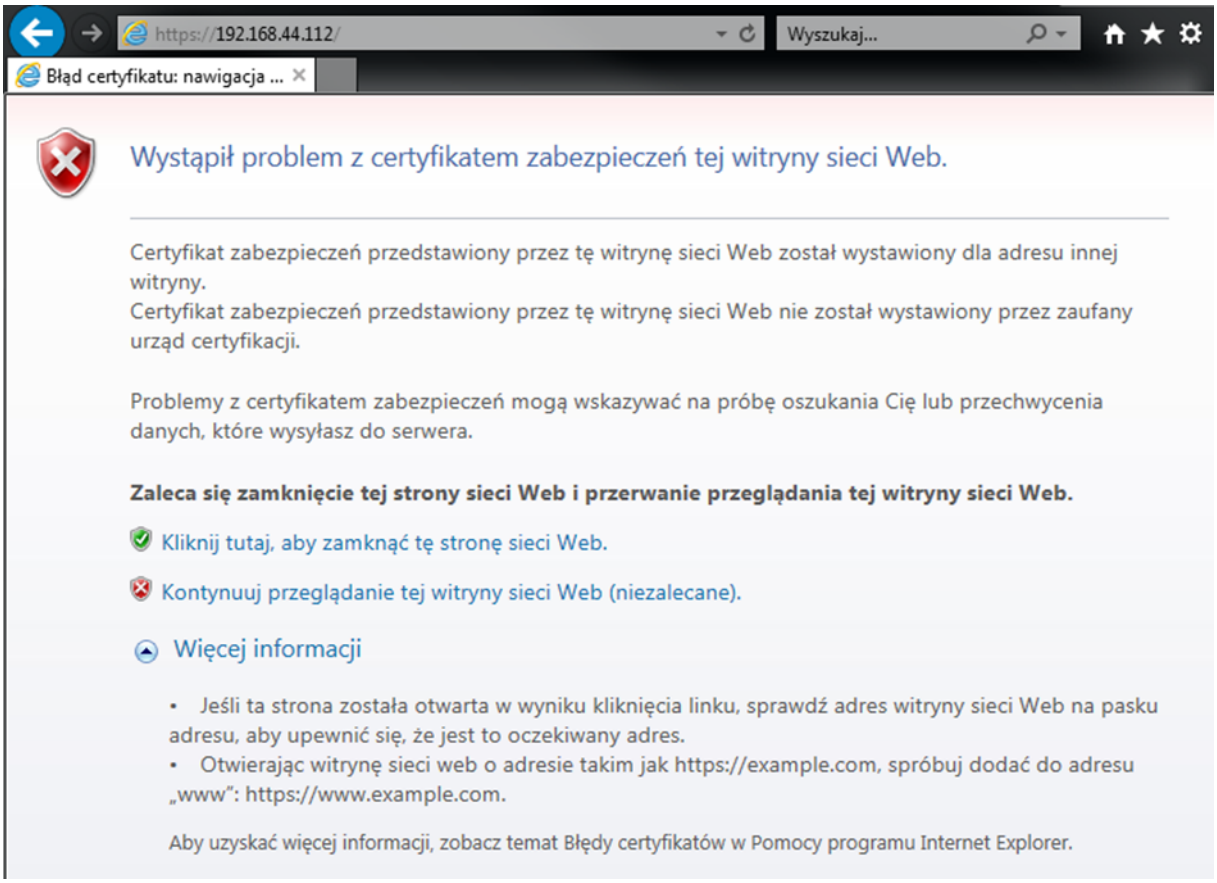
W następnym kroku należy włączyć szyfrowanie HTTPS oraz wybrać typ certyfikatu. Można wykorzystać *„Standardowy”* typ certyfikatu rejestratora lub wybierając opcję *„Dostosuj”* wgrać własny certyfikat i klucz.



Wszystkie zmiany należy zatwierdzić przyciskiem *„Zapisz”*.

WSTĘPNA KONFIGURACJA

Po uruchomieniu szyfrowania HTTPS należy połączyć się z rejestratorem przez przeglądarkę dodając przed adresem prefiks *„https://”*. W przeglądarce Internet Explorer należy rozwinąć przycisk *WIĘCEJ INFORMACJI* i kliknąć na *KONYNUUJ PRZEGLĄDANIE TEJ WITRYNY SIECI WEB (NIEZALECANE).* Po kliknięciu powinna otworzyć się strona logowania do rejestratora.



pl

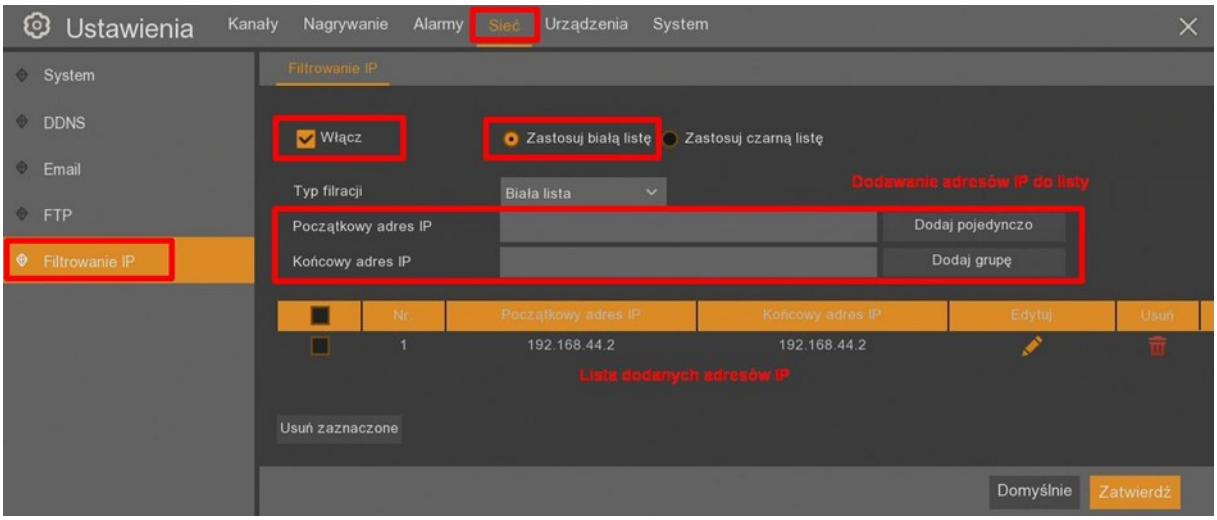
2. 2. 3. Ograniczenie dostępu do urządzeń

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 *„Zastosuj białą listę”* i dodać adresy IP, z których będzie możliwość zdalnego nawiązywania połączenia do urządzenia.

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



2. 2. 4. Zdalny dostęp do urządzenia – VPN

pl

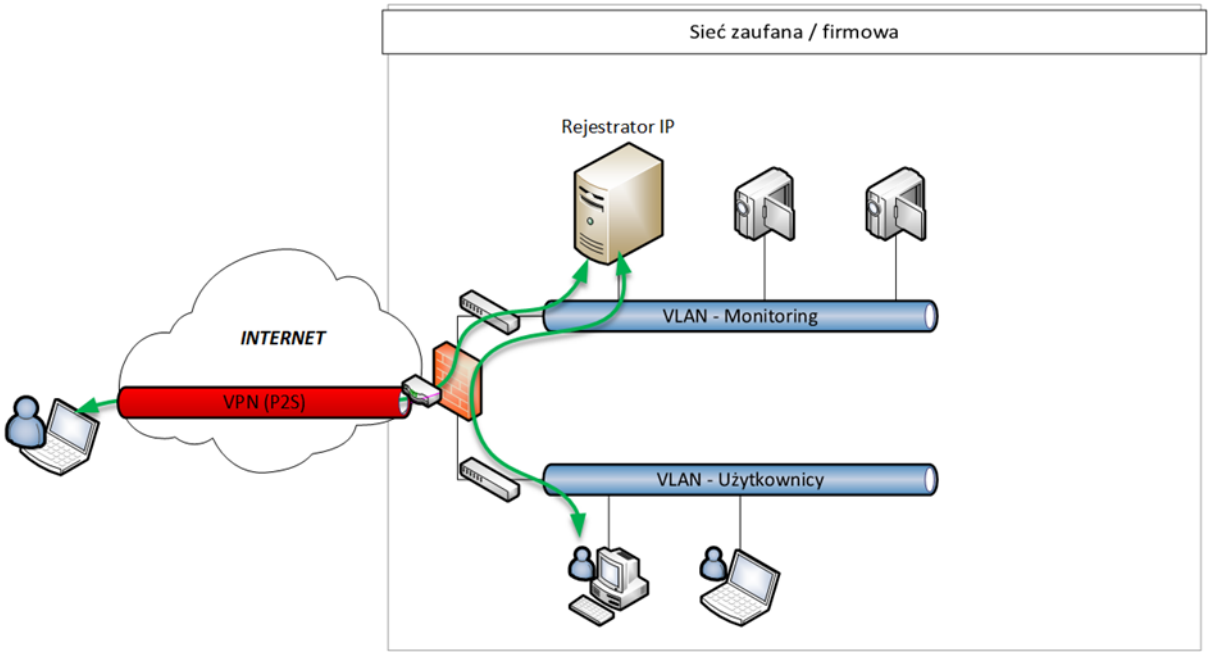
Zgodnie z powyższymi rekomendacjami, preferowaną opcją zdalnego dostępu do urządzeń z / przez sieci niezaufane (np. Internet) jest zestawienie tunelu VPN który będzie chronił komunikację pomiędzy urządzeniami.

Architektura VPN:

1. *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.
2. *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.

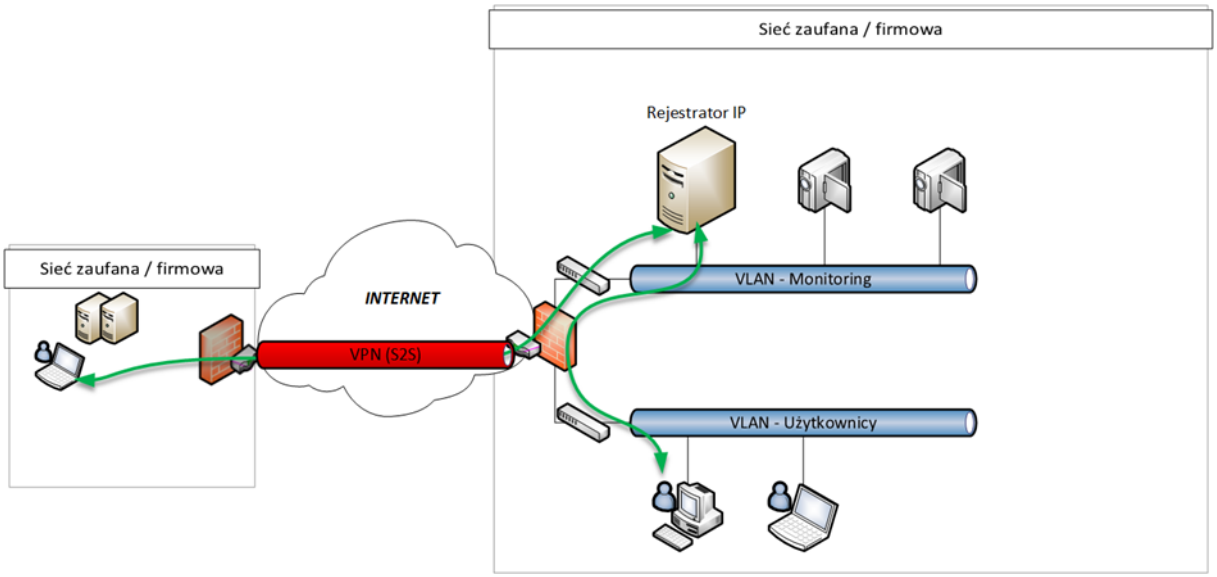
WSTĘPNA KONFIGURACJA

1. Schemat P2S VPN (Point to Site)



Point to Site VPN

2. Schemat S2S VPN (Site to Site)



Site to Site VPN

WSTĘPNA KONFIGURACJA

Rekomendowane algorytmy szyfrowania dla połączenia

Acceptable algorithms	
Symmetric Key Algorithms	AES-128, AES-192, AES-256
Cipher modes	GCM, CBC with integrity check (SHA),
Hashing Algorithms	SHA-256, SHA-512, SHA-3
Diffie-Hellman	Group 14 (2048) or higher
RSA	Factoring modulus ≥ 2048
Elliptic Curves (f)	f ≥ 256
Key Exchange	IKEv2
Transport layer protocols	TLS1.2

pl

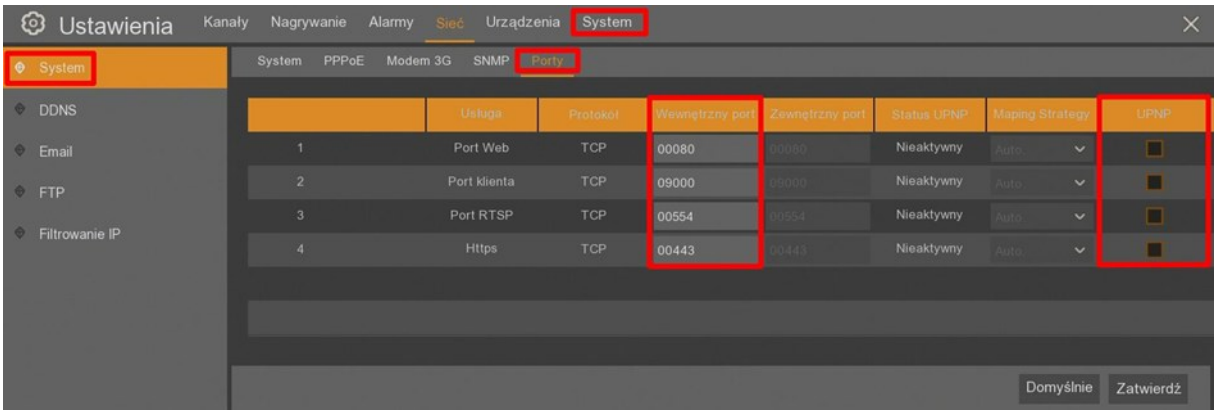
Urządzenie umożliwia również skorzystania z protokołu UPnP (Universal Plug-and-Play) w celu podłączenia się zdalnie do części usług sieciowych. Aby móc skorzystać z tej opcji należy:

- uaktywnić opcję bezpośrednio na urządzeniu (patrz instrukcja poniżej)
- w przypadku udostępniania usług do Internetu, uruchomić opcję UPnP na routerze brzegowym

UWAGA: ze względu na bezpieczeństwo nie rekomendowane jest korzystanie z protokołu UPnP w zdalnym dostępie do urządzeń (ze szczególnym uwzględnieniem dostępu z sieci niezaufanych takich jak Internet). Alternatywną opcją jest zestawienie tunelu VPN bądź ostatecznie udostępnienia usług sieciowych na zasadzie „Port Forwarding'u" z restrykcyjnymi regułami zapór sieciowych.

Uruchomienie opcji UPnP

W celu skonfigurowania UPnP w Menu *„Sieć"*, podmenu *„System"* należy wybrać zakładkę *„Porty"*. W kolumnie *„UPNP"* można włączyć opcję dla poszczególnych portów. Rozwiązanie umożliwia zmianę domyślnych portów TCP/IP po których będzie udostępniana dana usługa. Po ustawieniu wszystkich parametrów należy zapisać zmiany za pomocą przycisku *„Zatwierdź"*.



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

2019-10-23 PF, TF v1.0