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

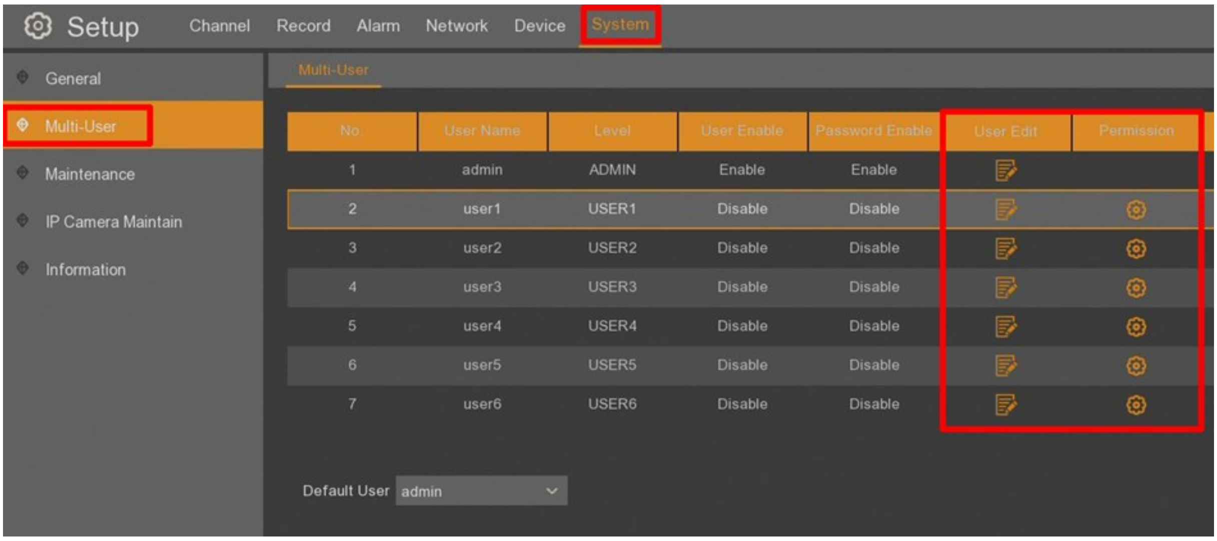
- the recorder should be located in a safe place preventing unauthorized access (e.g. server room, locked room, etc.)
- the system should be updated regularly by security patches
- each of the system users should have their own personal account, which can be easily linked to a specific person
- system 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

        - ∗ 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.

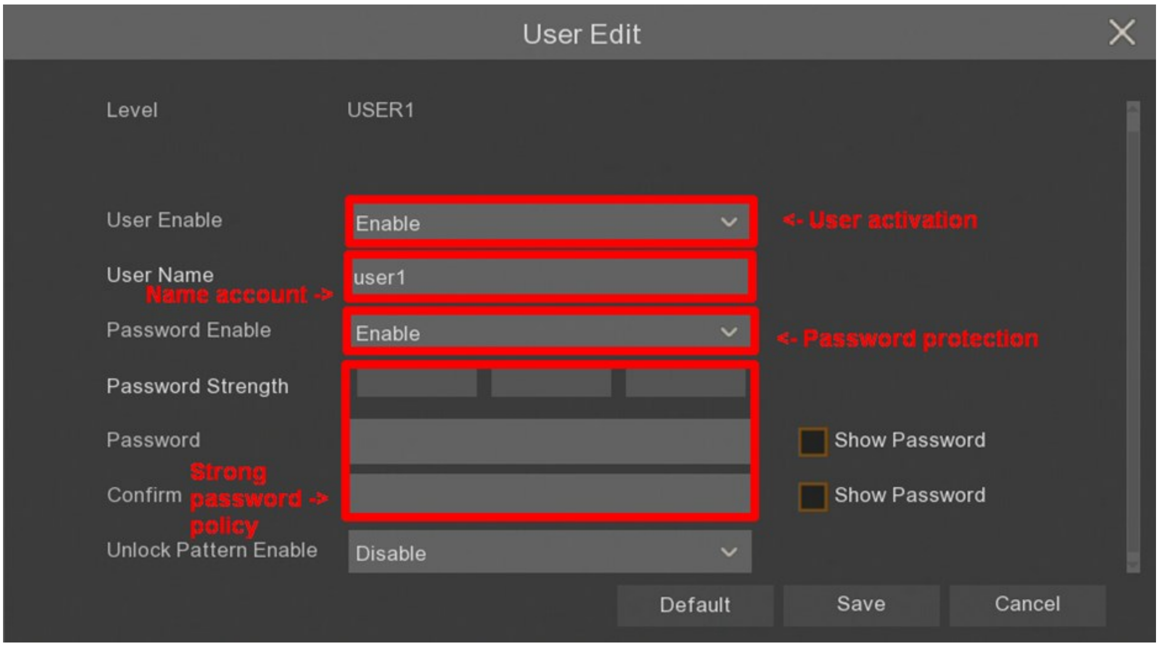


No.	User Name	Level	User Enable	Password Enable	User Edit	Permission
1	admin	ADMIN	Enable	Enable	✎	
2	user1	USER1	Disable	Disable	✎	⚙
3	user2	USER2	Disable	Disable	✎	⚙
4	user3	USER3	Disable	Disable	✎	⚙
5	user4	USER4	Disable	Disable	✎	⚙
6	user5	USER5	Disable	Disable	✎	⚙
7	user6	USER6	Disable	Disable	✎	⚙

Default User admin

New account activation

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



User Edit

Level USER1

User Enable: Enable <- User activation

User Name: user1 (Name account ->)

Password Enable: Enable <- Password protection

Password Strength

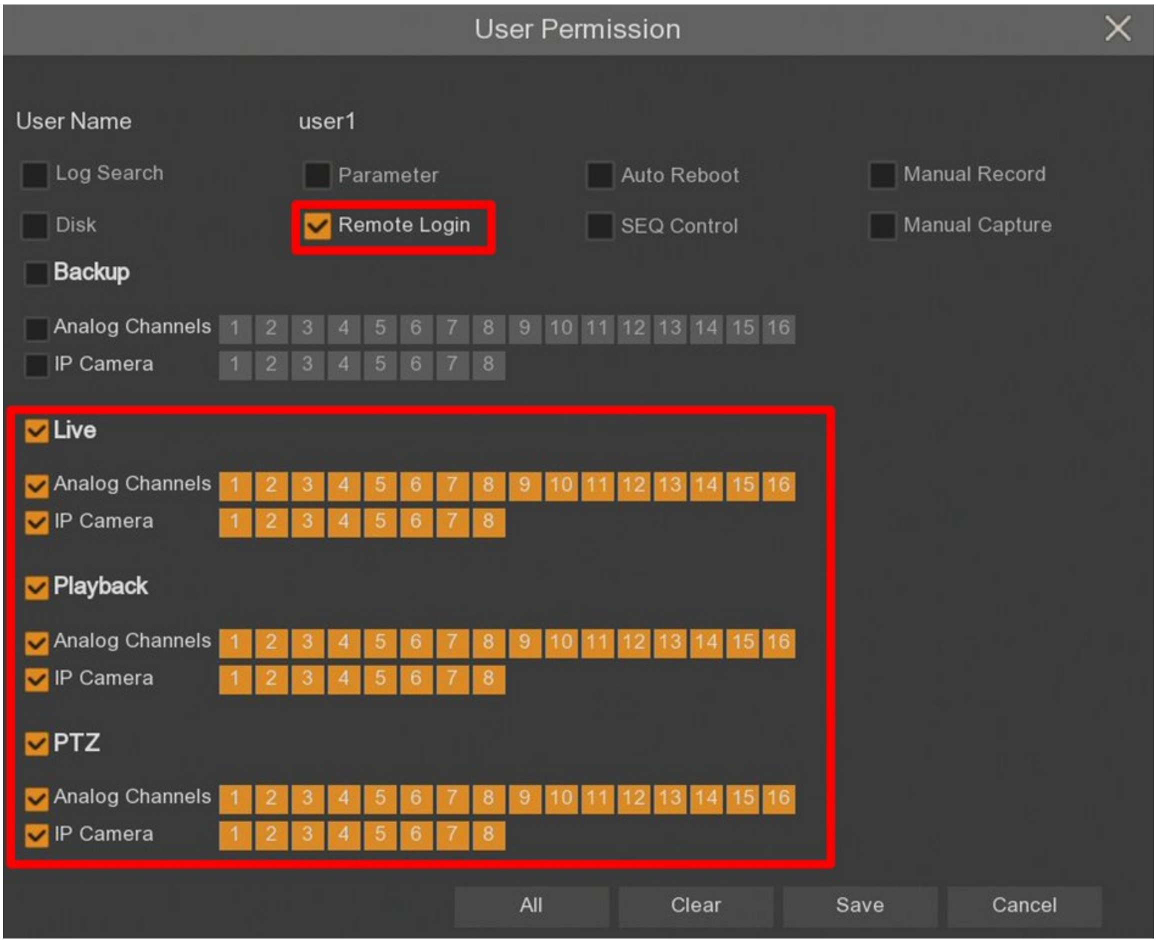
Password □ Show Password

Confirm □ Show Password (Strong password -> policy)

Unlock Pattern Enable: Disable

User permission settings

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



User Permission

User Name user1

□ Log Search □ Parameter □ Auto Reboot □ Manual Record

□ Disk ☑ Remote Login □ SEQ Control □ Manual Capture

□ Backup

□ Analog Channels 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ IP Camera 1 2 3 4 5 6 7 8

☑ Live

☑ Analog Channels 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

☑ IP Camera 1 2 3 4 5 6 7 8

☑ Playback

☑ Analog Channels 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

☑ IP Camera 1 2 3 4 5 6 7 8

☑ PTZ

☑ Analog Channels 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

☑ IP Camera 1 2 3 4 5 6 7 8

INITIAL CONFIGURATION

2. 2. Network Configuration

2. 2. 1. LAN configuration

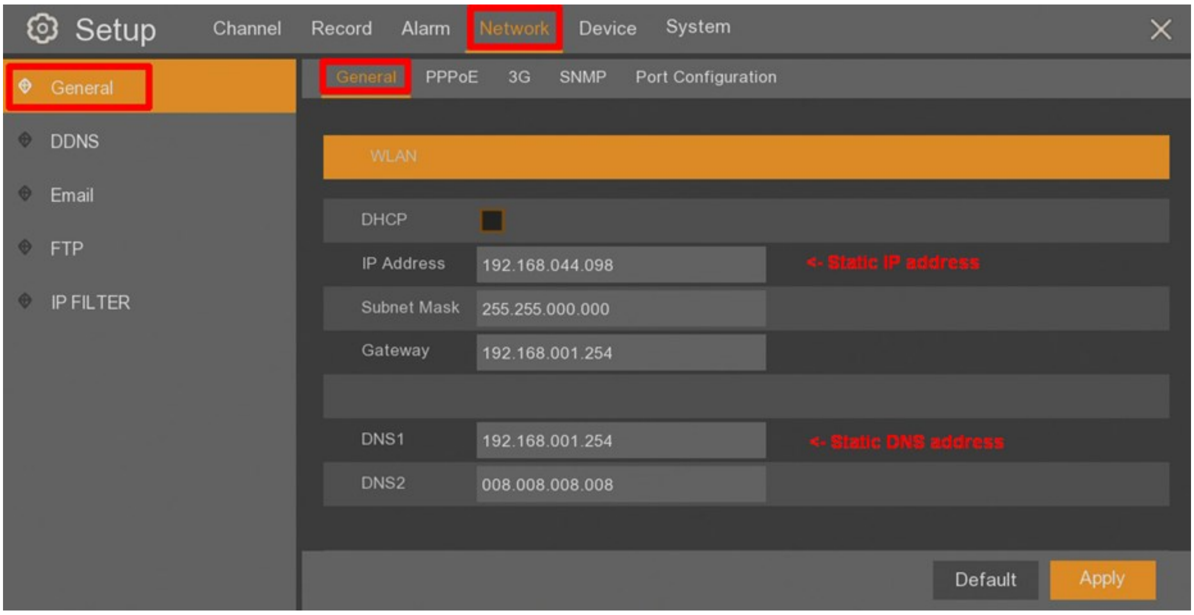
It is recommended to have physical access to the recorder (connected mause and monitor). It is important especially for access with administrator privileges to configure the device.

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.



DHCP □

IP Address 192.168.044.098 <- Static IP address

Subnet Mask 255.255.000.000

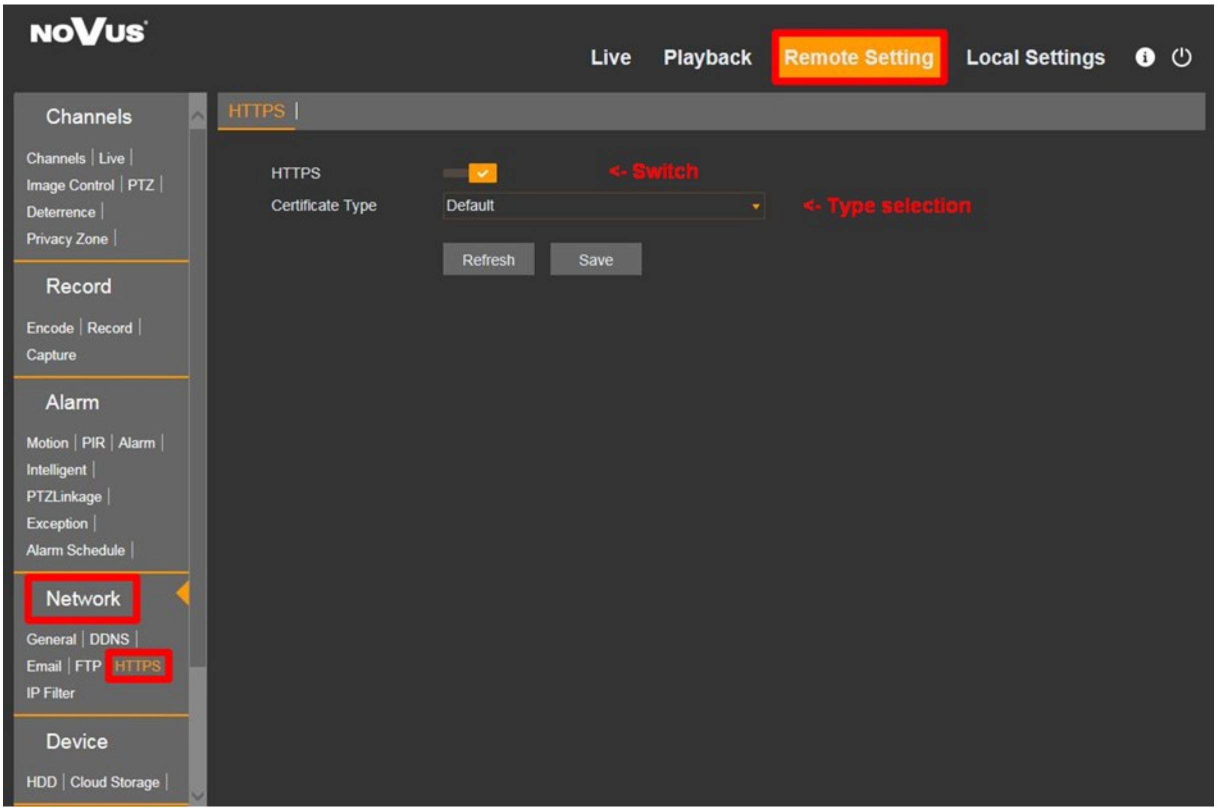
Gateway 192.168.001.254

DNS1 192.168.001.254 <- Static DNS address

DNS2 008.008.008.008

2. 2. 2. HTTPS connection configuration

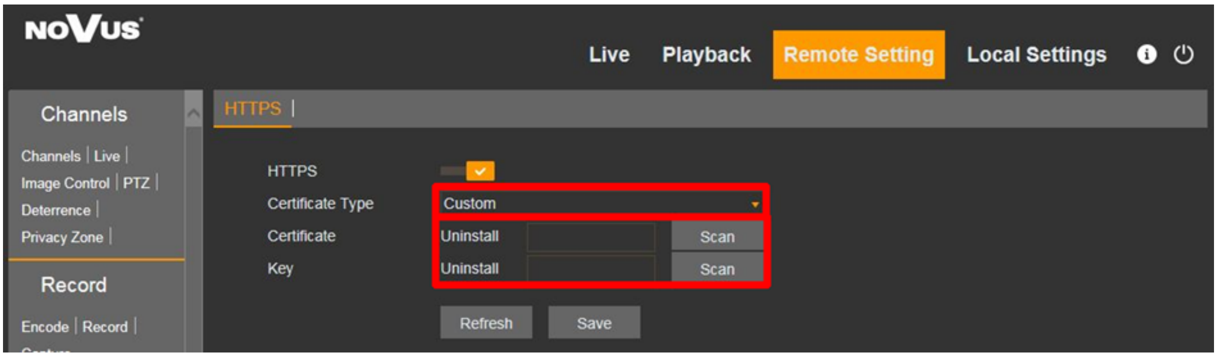
To enable logging into the administration panel using HTTPS protocol, log in to the recorder through the browser, enter „*Remote settings*” and select „*HTTPS*” in the „*Network*” section.



HTTPS ✓ <- Switch

Certificate Type: Default <- Type selection

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.



HTTPS ✓

Certificate Type: Custom

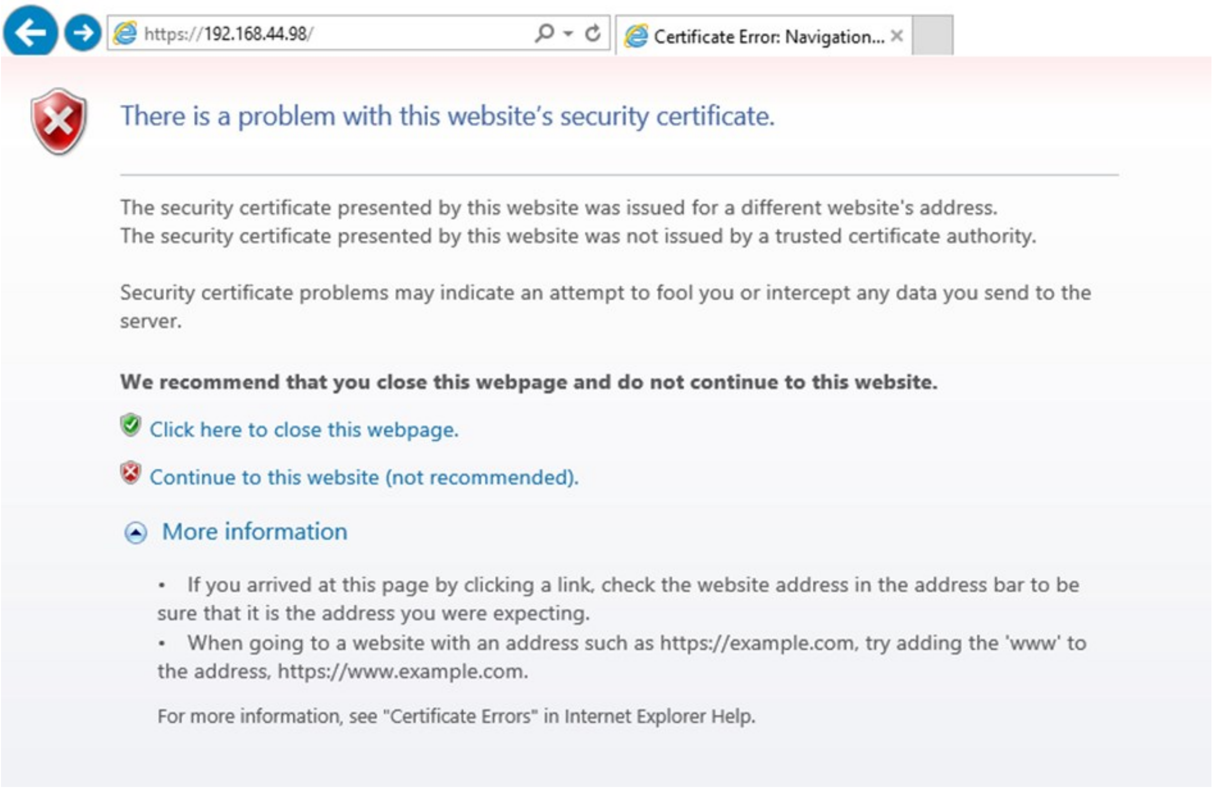
Certificate: Uninstall

Key: Uninstall

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.



There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.
The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.

For more information, see "Certificate Errors" in Internet Explorer Help.

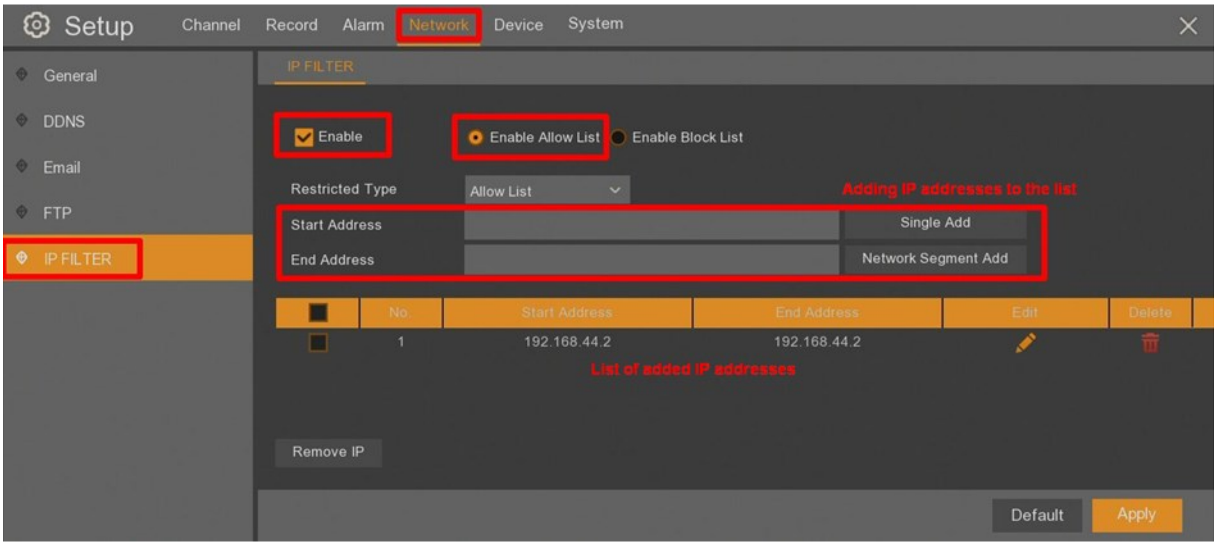
2. 2. 3. Devices access restrictions

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.



☑ Enable

● Enable Allow List ○ Enable Block List

Restricted Type: Allow List

Start Address | Single Add

End Address | Network Segment Add

Adding IP addresses to the list

■	No.	Start Address	End Address	Edit	Delete
□	1	192.168.44.2	192.168.44.2	✎	🗑

List of added IP addresses

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

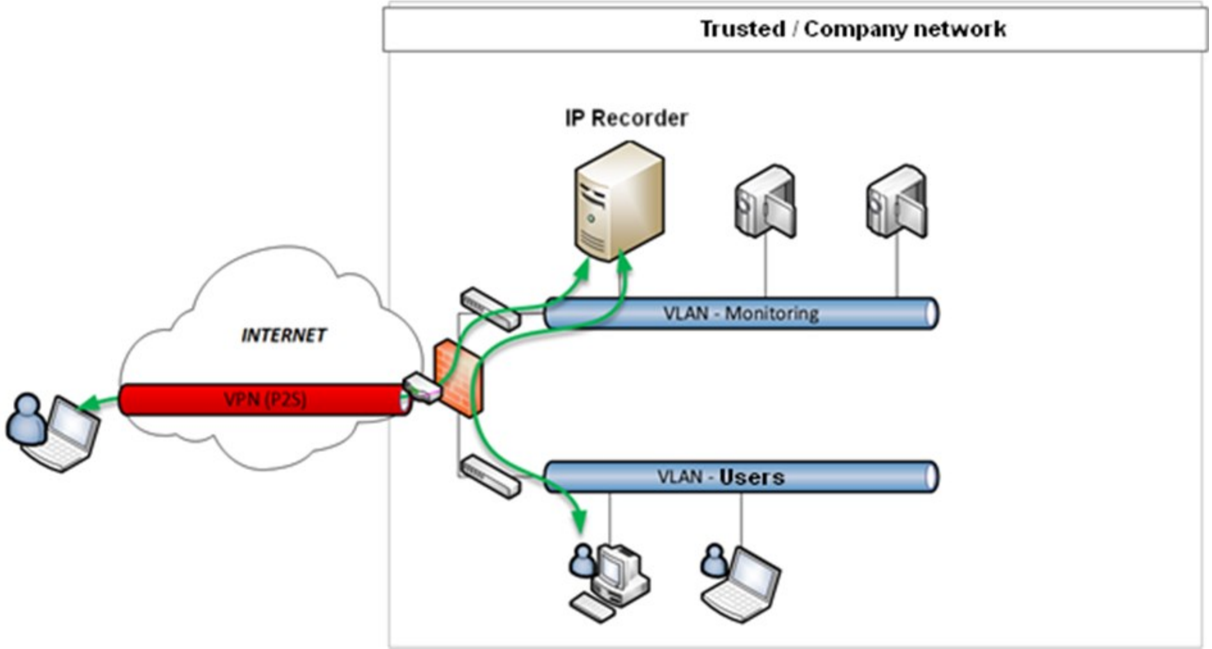
According to the above recommendations, the preferred option of remote access to devices from / through untrusted networks (e.g. Internet) is to set up a VPN tunnel that will protect communication between devices.

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.

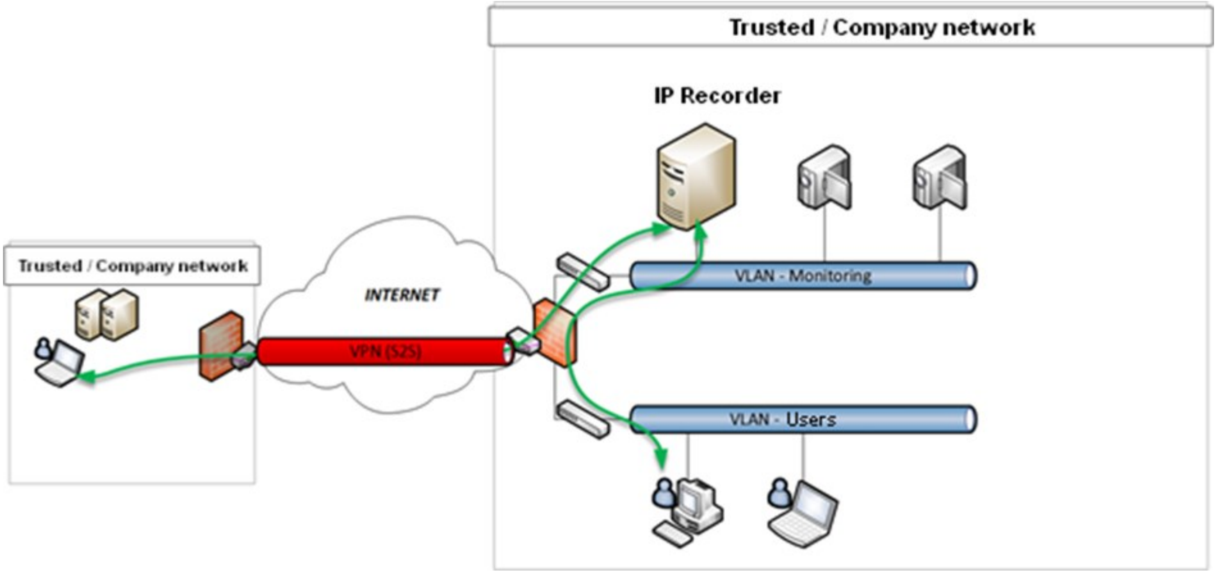
INITIAL CONFIGURATION

1. P2S VPN scheme (Point to Site)



Point to Site VPN

2. S2S VPN scheme (Site to Site)



Site to Site VPN

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

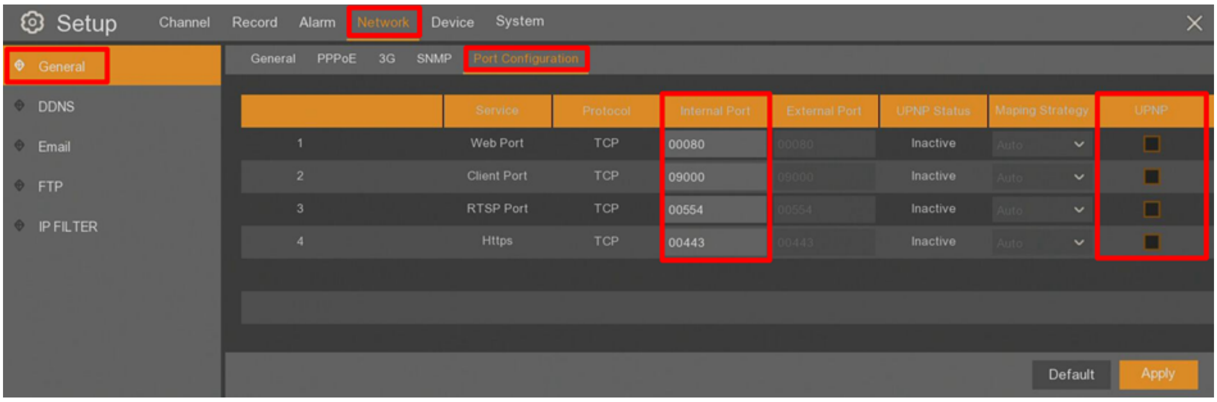
The device also allows to use the UPnP (Universal Plug-and-Play) protocol to connect to some network services remotely. To use this option:

- 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.



	Service	Protocol	Internal Port	External Port	UPNP Status	Maping Strategy	UPNP
1	Web Port	TCP	00080	00080	Inactive	Auto	□
2	Client Port	TCP	09000	09000	Inactive	Auto	□
3	RTSP Port	TCP	00554	00554	Inactive	Auto	□
4	Https	TCP	00443	00443	Inactive	Auto	□

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