MyEye

Video Recorder 16

Smart Video Recording up to 16 cameras

EN - Instructions and warnings for installation and use

Nice

CONTENTS

1 FOREWORD

1.1 - General

This Quick Start Guide (hereinafter referred to as “the Guide”) introduces the functions, installation, and operations of the camera.

1.2 - Safety Instructions

The following categorized signal words with defined meaning might appear in the guide.

Signal Words	Meaning
Warning	Indicates a medium or low potential hazard which could result in slight or moderate injury, if not avoided.
Caution	Indicates a potential risk that may result in property damage, data loss, lower performance, or unpredictable result, if not avoided.
Meaning	Provides additional information as the emphasis and supplement to the text.

1.3 - Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as faces, fingerprints, car plate numbers, Email addresses, phone numbers, GPS, and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures including but not limited to: providing clear and visible identification to inform the data subject about the existence of the surveillance area and providing related contact.

1.4 - About this Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the QR code or our official website. If there is inconsistency between the paper User’s Guide and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact customer service for the latest program and supplementary documentation.
- There still might be a deviation in technical data, functions, and operations description, or print errors. If there is any doubt or dispute, please refer to our final explanation.
- All trademarks, registered trademarks, and the company names in the Guide are the properties of their respective owners.
- Please visit our website and contact the supplier or customer service if there is any problem when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

2 IMPORTANT SAFEGUARDS AND WARNINGS

2.1 - Electrical safety

- All the installation and operations described here should conform to the local electric safety rules.
- Use a power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Make sure the power supply is correct before operating the device.
- A readily accessible disconnect device shall be incorporated into the building installation wiring.
- Prevent the power cable from being trampled or pressed, especially the plug, power socket, and the junction extruded from the device.

2.2 - Environment

- Do not aim the device to focus on strong light, such as lamp light and sunlight; otherwise, it may cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp or dusty environment, extremely hot or cold temperatures, or locations with strong electromagnetic radiation or unstable lighting.
- Keep the device away from any liquid to avoid damage to the internal components.
- Keep the indoor device away from rain or dampness to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.
- Transport, use, and store the device within the range of allowed humidity and temperature.
- Heavy stress, violent vibration, or water splash are not allowed during transportation, storage, and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting it.
- Install the device in a location where only professional staff with relevant knowledge of safeguards and warnings can access it. The accidental injury might happen to the non-professionals who enter the installation area when the device is operating normally.

2.3 - Operation and Daily Maintenance

- Do not touch the heat dissipation component of the device to avoid scalds.
- Carefully follow the instructions in the Guide when performing any disassembling of the device; unprofessional disassembling may cause water leakage or poor image quality. Please contact after-sale service for desiccant replacement if there is condensed fog found on the lens after unpacking or when the desiccant turns green (Not all models are included with the desiccant).
- It is recommended to use the device together with a lightning arrester to improve lightning protection effect.
- It is recommended to connect the grounding hole to the ground to enhance the reliability of the device.
- Do not touch the image sensor directly (CMOS). Dust and dirt could be removed with an air blower, or you can wipe the lens gently with a soft cloth moistened with alcohol.
- The device body can be cleaned with a soft dry cloth, which can also be used to remove stubborn stains when moistened with mild detergent. To avoid possible damage to the device body coating which could cause a decrease in performance, do not use volatile solvents such as alcohol, benzene, diluent, or strong and abrasive detergents.
- The dome cover is an optical component, do not touch or wipe the cover with your hands directly during installation or operation. To remove dust, grease, or fingerprints, wipe gently with moistened oil-free cotton with diethyl or a moistened soft cloth. You can also use an air blower to remove dust.

Warning

- Strengthen the protection of your network, device data, and personal information through measures that include, but are not limited to, using a strong password, modifying your password regularly, updating your device software to the latest version, and setting up a private computer network. For some devices with old software versions, the ONVIF password will not be automatically modified when the system password is changed, and you will need to update the software or manually update the ONVIF password.
- Use standard components or accessories provided by the manufacturer and ensure that the device is installed and maintained by professional engineers.
- The image sensor surface should not be exposed to laser beam radiation in the environment where the laser beam device is used.
- Do not power the device with two or more power sources. Unless stated otherwise. Failure to follow these instructions may damage the device.

3 INSTALLATION

Caution

All the installation and operations described here should conform to the local electric safety rules. The device does not support wall mounting with the front panel facing down.

- The following figures are for reference only. The actual product shall prevail.

3.1 - Dimensions

The following figures are for reference only, and the actual product shall prevail.

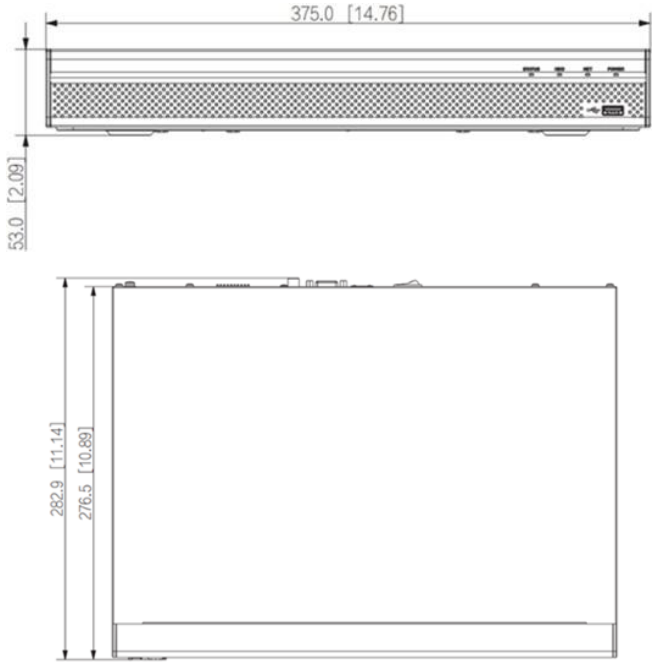


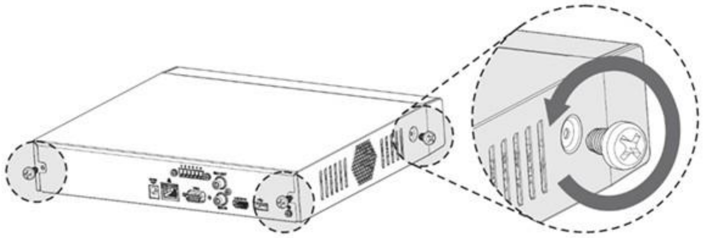
Figure 3-1 Dimensions (Unit: mm[inch])

3.2 - Installing HDD

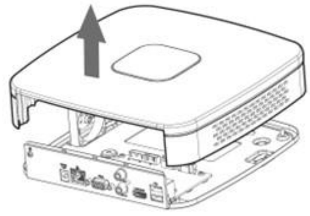
Shut down the NVR and unplug the power cord before opening the cover to replace the HDD.

During the first-time installation, check whether the HDD has been installed or not. It is recommended to use HDD of enterprise-level or surveillance level. It is not recommended to use a PC HDD.

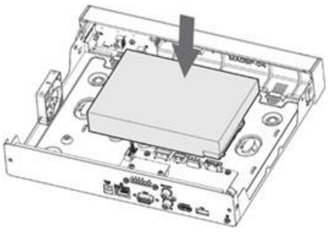
1. Remove the fixing screws of the case cover (including the two screws on the rear panel and two screws on the left and right panels).



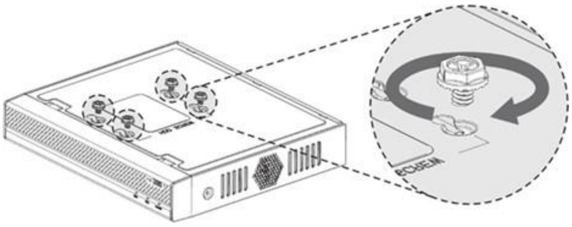
2. Remove the cover along the direction shown by the following arrow.



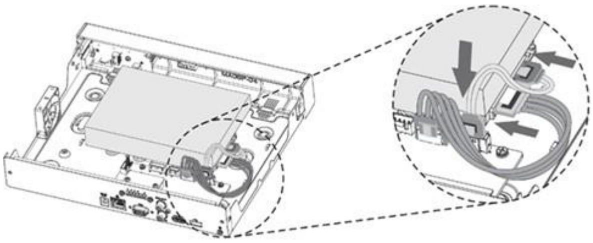
3. Match the four holes on the base board to place the HDD.



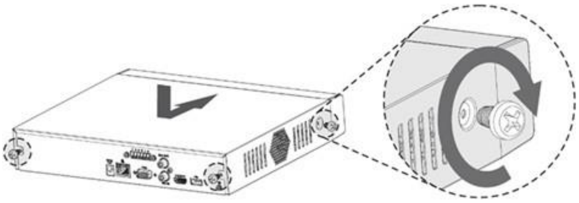
4. Turn the device upside down, match the screws with the holes on the HDD and then fasten them. The HDD is fixed to the base board.



5. Connect the HDD data cable and power cable to the device.

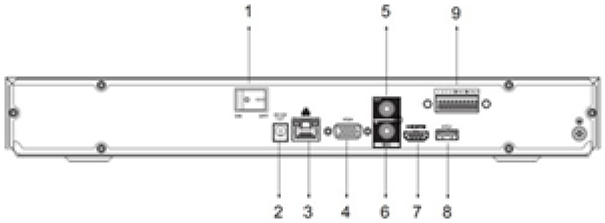


6. Put back the cover and fasten the four screws on the base board to complete the installation.



3.3 - Connection

- The following figures are for reference only. The actual product shall prevail.
- Please check the icons on the rear panel carefully and refer to the actual product for detailed information.
- If the icon is DC12V, input DC 12V power. If the icon is DC48V, input DC 48V power.



1	Power Switch	2	PoE Ports
3	Network Port	4	Power Input
5	Mic Out	6	VGA Port
7	HDMI Port	8	HDMI Port
9	Alarm Input/Output		

4 CONFIGURATION

4.1 - Booting up

Before the boot up, please make sure:

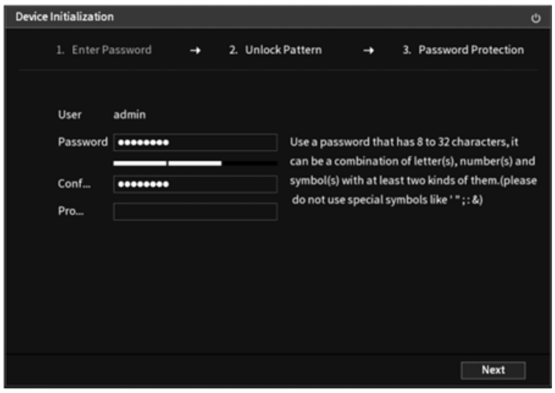
- The rated input voltage matches the NVR's power requirements.
- The power wire connection is ready.
- For device security, connect the NVR to the power adapter first and then connect it to the power socket.
- Always use a stable current. It is recommended to use UPS as the power source.
- Devices of some series do not have the power on-off button. You can boot up the device once the power is connected.

Connect the device to the monitor or TV using an HDMI cable, plug it into the power socket, and then press the power button to boot up the device.

4.2 - Initializing the device

When booting up for the first time, you need to configure the password information for admin (by default). To guarantee device security, keep the login password for the admin properly hidden and modify it regularly.

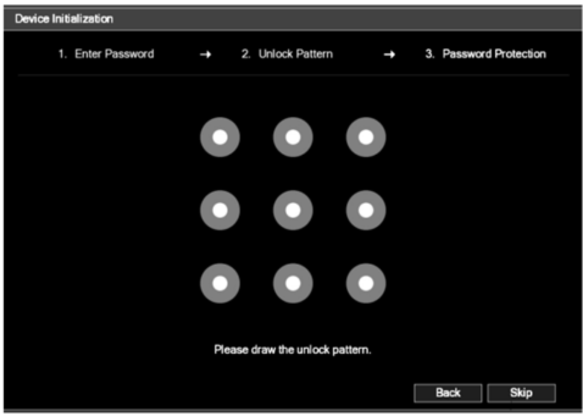
1. Turn on the device. The device initialization interface is displayed
2. Set location, language, and video standard. From the drop-down list, select region, language, and video standard as needed.
3. Read the Software License Agreement and select "I have read and agree to all the terms"
4. Select time zone and configure system time.
5. Configure the password information for the admin. For details, see the table below



Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' " ; : &)

Parameter	Description
User	By default, the user is admin.
Password	In the Password box, enter the password for admin. The new password can be set from 8 to 32 characters. Characters need to contain at least two types of numbers, letters and special characters (excluding"'", """, ";", ":" and "&").
Confirm Password	
Prompt Question	In the Prompt Question box, enter the information that can remind you of the password.

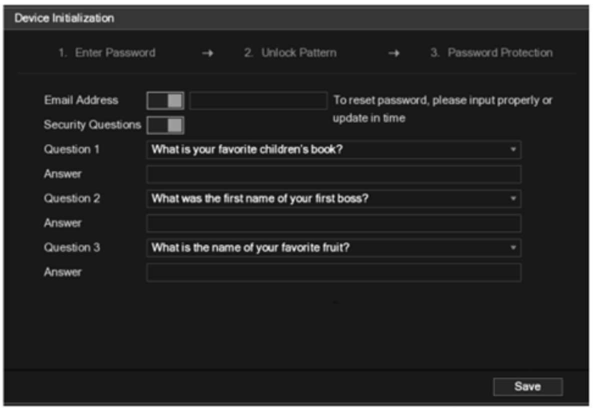
6. Use the mouse to draw an unlock pattern, and then draw it again for confirmation.



Please draw the unlock pattern.

- The pattern that you want to set must cross at least four points.
- If you do not want to configure the unlock pattern, click Skip.
- Once you have configured the unlock pattern, it will be used as the default authentication method. If you skip this setting option, enter the password for login

7. Apply a reserved email address and security questions to the NVR.



Device Initialization

1. Enter Password → 2. Unlock Pattern → 3. Password Protection

Email Address: To reset password, please input properly or update in time

Security Questions

Question 1: What is your favorite children's book?

Answer

Question 2: What was the first name of your first boss?

Answer

Question 3: What is the name of your favorite fruit?

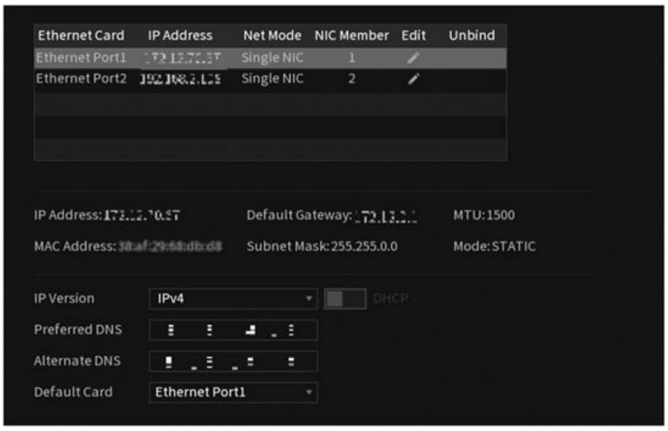
Answer

- Enable Email address checkbox and enter an email address.
- Enable Security Questions check box, and then enter the answers to those questions.
- After configuration, if you forget the password for the admin user, you can reset the password through the reserved email address or security questions.
- If you do not want to configure the settings, disable the email address and security questions functions on the interface.

8. Click OK to complete the initialization.

4.3 - Network configuration

1. Select Main Menu > Network > TCP/IP. The TCP/IP interface is displayed. Click ✎ to modify the IP address according to the actual home network settings (the default IP address is 192.168.1.108)



Ethernet Card	IP Address	Net Mode	NIC Member	Edit	Unbind
Ethernet Port1	[redacted]	Single NIC	1	✎	
Ethernet Port2	[redacted]	Single NIC	2	✎	

IP Address: [redacted] Default Gateway: [redacted] MTU:1500

MAC Address: [redacted] Subnet Mask:255.255.0.0 Mode:STATIC

IP Version: IPv4 DHCP

Preferred DNS: [redacted]

Alternate DNS: [redacted]

Default Card: Ethernet Port1

Parameter	Description
IP Version	In the IP Version list, you can select IPv4 or IPv6. Both versions are supported for access.
MAC Address	Displays the MAC address of the NVR.
DHCP	Enable the DHCP function. The IP address, subnet mask, and default gateway are not available for configuration once DHCP is enabled. • If DHCP is effective, the obtained information will be displayed in the IP Address, Subnet Mask and Default Gateway. If not, all values will show 0.0.0.0. • If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP will not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. NOTE IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Enter the IP address of DNS.
Alternate DNS	Enter the IP address of the alternate DNS.
MTU	Enter a value for the network card. The value ranges from 1280 byte to 1500 byte. The default value is 1500. The suggested MTU values are as below. 1500: The biggest value of Ethernet information package. This value is typically selected if there is no PPPoE or VPN connection, and it is also the default value of some routers, network adapters and switches. 1492: Optimized value for PPPoE. 1468: Optimized value for DHCP. 1450: Optimized value for VPN.
Test	Click Test to test if the entered IP address and gateway are interworking.

4.4 - Adding IP cameras

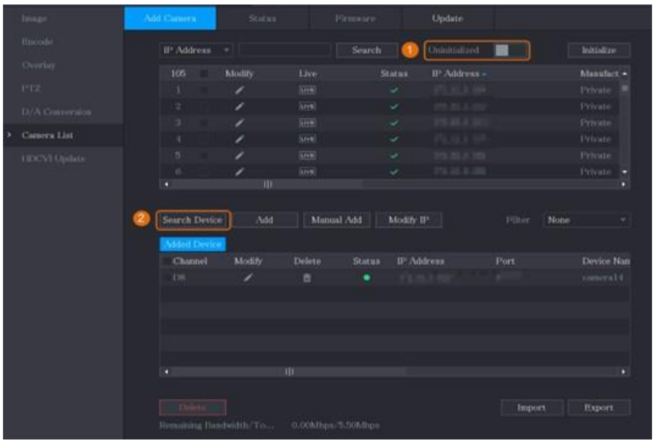
You can add an IP camera by search result or by manually entering IP information.

4.4.1 - Initializing IP cameras

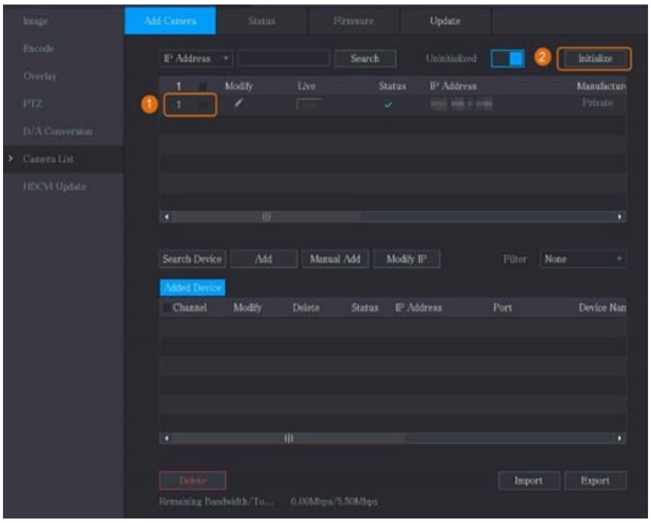
The topic shows how to initialize new cameras or the cameras after restoring factory defaults.

- When connecting a camera to the NVR through the built-in PoE port, the NVR will automatically initialize the camera. The camera adopts the password and email information of the NVR by default.

1. Select Main Menu > Camera > Camera List > Add Camera.
2. Enable Uninitialized checkbox and then click Search Device button.



3. Select the camera to be initialized and then click initialize button.



4. Apply password and email information to the IP camera

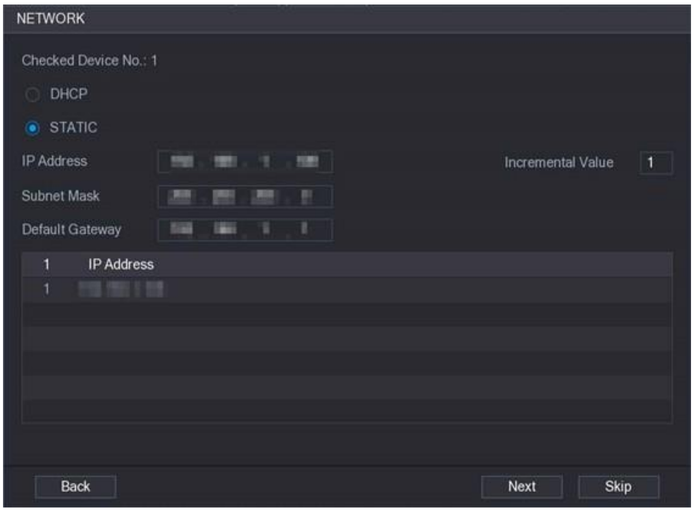
- Select “Using current device password and email info” to leave the same credentials for the camera as on NVR
- Deselect “Using current device password and email info” to define different credentials for the camera

5. Configure camera IP address

- Select DHCP if there is a DHCP server deployed.
- Select Static (preferred one), and then input IP address, subnet mask, default gateway, and incremental value

Note

- Set the incremental value when you need to change the IP addresses of multiple cameras at the same time. The NVR will incrementally add the value to the fourth section of the IP address after allocating the IP address for those cameras


NETWORK

Checked Device No.: 1

○ DHCP

● STATIC

IP Address [redacted]   Incremental Value 1

Subnet Mask [redacted]

Default Gateway [redacted]

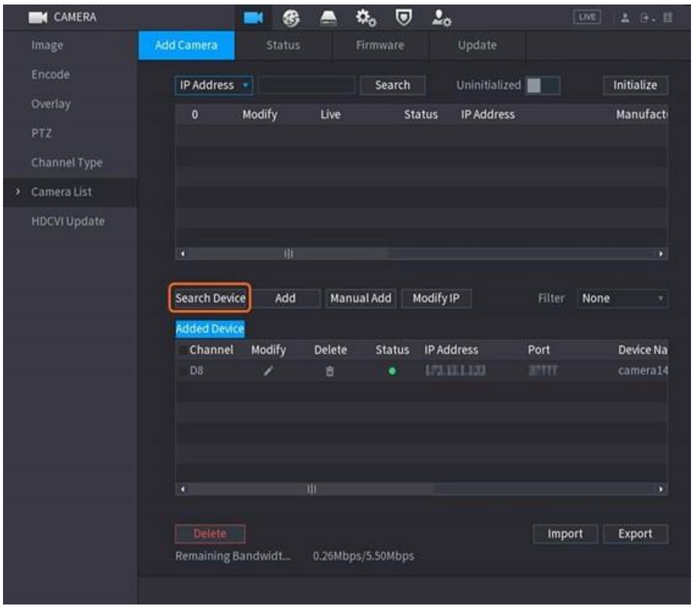
1	IP Address
1	[redacted]

6. Click Next. Wait 1-2 minutes for the initialization procedure to be completed. Click Finished.

4.4.2 - Adding IP Cameras by Search Result

Make sure that the cameras you want to add have already been initialized and connected to the right network.

1. Select Main Menu > Camera > Camera List > Add Camera.
2. Click Search Device button.

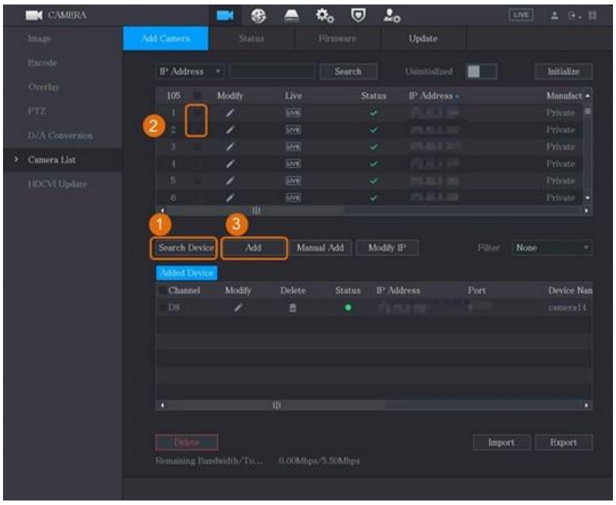


Channel	Modify	Delete	Status	IP Address	Port	Device Na
D8			●	[redacted]	[redacted]	camera14

Remaining Bandwidt... 0.26Mbps/5.50Mbps

3. Add IP cameras:

- Add by double-click: Double-click the target camera to add it to Added Device list
- You can add only one camera at one time via this method.
- Add by check box: Select the check box of the target camera, and then click Add button to add it to Added Device list.
- You can select more than one check box and add cameras in batches.



Channel	Modify	Delete	Status	IP Address	Port	Device Nan
D8			●	[redacted]	[redacted]	camera14

Remaining Bandwidth/To... 0.00Mbps/5.50Mbps

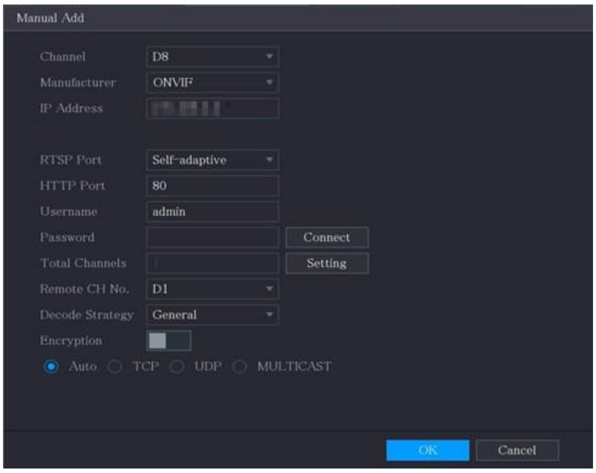
- If the status of the added camera is green, it indicates the camera has been properly added to the NVR.
- If the status of the added camera is red, it indicates connection failure between the camera and NVR. Check the parameters of the camera such as password, protocol and channel number, and then try adding it again.

4.4.3 - Manually adding IP cameras

You can add one IP camera by IP information at one time.

Make sure that the cameras you want to add have already been initialized and connected to the right network.

1. Select Main Menu > Camera > Camera List > Add Camera.
2. Click Manual Add button.
3. In the Manual Add dialog box configure parameters.



Manual Add

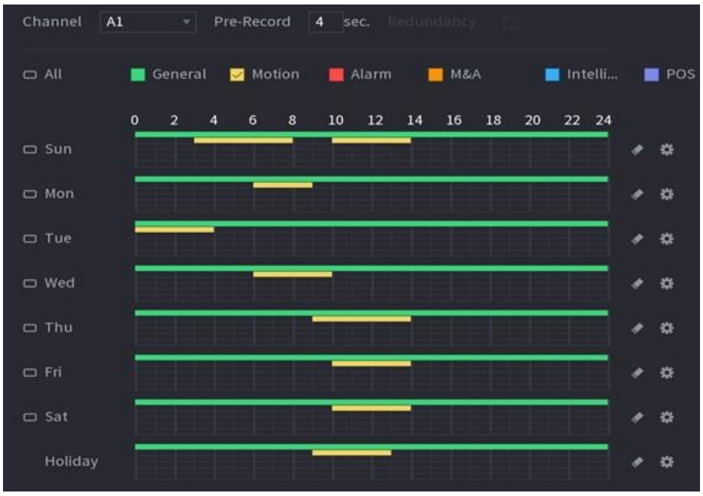
Channel: D8
Manufacturer: ONVIF
IP Address: [redacted]
RTSP Port: Self-adaptive
HTTP Port: 80
Username: admin
Password:
Total Channels:
Remote CH No.: D1
Decode Strategy: General
Encryption: □
● Auto ○ TCP ○ UDP ○ MULTICAST

Parameter	Description
Channel	From the Channel drop-down list, select the channel that you want to use on the NVR to connect the remote device.
Manufacturer	From the Manufacturer drop-down list, select the manufacturer of the remote device.
IP Address	In the IP Address field, enter the IP address of the IP camera. • Change the default value (192.168.0.0) which the system cannot connect to.
RTSP Port	The default value is 554. You can change the value as needed.
HTTP Port	The default value is 80. You can change the value as needed. • If you enter another value, for example, 70, then you should enter 70 after the IP address when logging in to the NVR by a browser.
TCP Port	The default value is 37777. You can change the value as needed.
Username	Enter the username of the remote device.
Password	Enter the password of the user for the remote device.
Remote CH No.	Enter the remote channel number of the remote device that you want to add.
Decoder Strategy	In the Decoder Strategy list, select Default, Realtime, or Fluent as needed.
Protocol Type	• If the IP camera is added through a private protocol, select TCP. • If the IP camera is added through ONVIF protocol, select Auto, TCP, UDP, or MULTICAST. • If the IP camera is added through other manufacturers, select TCP or UDP.
Encryption	If the IP camera is added through ONVIF protocol, enabling the Encryption check box will provide encryption protection to the data being transmitted. To use this function, the HTTPS function must be enabled for the remote IP camera.

4.5 - Configuring Recorded Video Storage Schedule

By default, all cameras continuously record videos 24 hours a day. You can modify the settings as needed.

1. Select Main Menu > Storage > Schedule > Record



Channel A1 Pre-Record 4 sec. Redundancy □

2. Configure parameters.

Parameter	Description
Channel	Channel From the Channel drop-down list select the channel to change video recording settings.
Pre-record	In the Pre-record field set the time for capturing extra video that occurs before an event to provide context to a recording. Value range: 0 to 30 s.
Redundancy	Allows users to set one of the HDDs as the redundant HDD to save the recorded files into different HDDs. In case of HDD failure, you can find the backup recording in the redundant HDD. • Select Main Menu > STORAGE > Disk Manager, and then set an HDD as the redundant HDD. • Select Main Menu > STORAGE > Schedule > Record, and then select the Redundancy check box. • If the selected channel is not recording, the redundancy function will take effect the next time you record no matter whether you select the check box or not. • If the selected channel is recording, the currently recorded files will be packed, and then start recording according to the new schedule. • This function is available on select models. • The redundant HDD only backs up the recorded videos but not snapshots.
Event type	Select the check box of the event types. General: General recording means that the NVR records all videos for the specified time frame. The general recording is represented by the green color. Motion: Motion recording means that the NVR records video only when the motion detection is triggered. Motion recording is represented by the yellow color. Alarm: Alarm recording means that the NVR records video when an alarm is triggered. The alarm recording is represented by the red color. M&A: M&A recording combines motion recording and alarm recording. The device records video when the motion detection or any alarm is triggered. M&A recording is represented by the orange color. Intelligent: Intelligent recording means that the NVR records video when the smart detection is triggered. The intelligent recording is represented by the blue color. POS: POS recording means that the NVR records video when the POS machine is used to make a payment. POS recording is represented by the Purple color. Intelligent: Intelligent recording means that the NVR records video when the smart detection is triggered. The intelligent recording is represented by the blue color. POS: POS recording means that the NVR records video when the POS machine is used to make a payment. POS recording is represented by the Purple color.
Period	Defines a period during which the configured recording setting is active. The system only activates the alarm in the defined period.
Copy to	Click Copy to copy the settings to other channels.

3. Set the schedule by drawing or editing

- Drawing: Press and hold the left mouse button and drag the mouse to draw the period
- Editing: Click ⚙ to configure the period and then click OK

4. Click Apply

- The configured record schedule can come into effect only when the auto record function is enabled.

4.6 - Logging into the Web Interface

1. Open Internet Explorer browser, enter the IP address of the device in the address bar, and press Enter. If the setup wizard is displayed, follow the instructions to finish the settings.
2. Enter username and password in the log in box, and then click Login.
3. For the first-time login, click Click Here to Download Plugin and then install the plugin as instructed.
4. The main interface is displayed.

5 CYBERSECURITY RECOMMENDATIONS

Mandatory actions to be taken towards cybersecurity

A. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper- and lower-case letters.

B. Update Firmware

As it is a standard procedure in the tech-industry, we recommend keeping NVR and IP camera firmware up-to-date to ensure the system is using the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

A. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users can access the system.

B. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

C. Audio and Video Encrypted Transmission

If your audio and video data content is very important or sensitive, we recommend that you use the encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: the encrypted transmission will cause some loss in transmission efficiency.

D. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

E. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system credentials. You will need to either update the camera firmware to the latest revision or manually change the ONVIF password.

F. Enable Account Lock

The account lock feature is enabled by default, and we recommend that you keep it on to guarantee account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

G. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the IP address of the device.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

H. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has access to features and functions they need to use to perform their job.

I. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc. to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3 and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP and set up strong passwords.

- AP hotspot: Choose WPA2-PSK encryption mode and set up strong passwords.

J. Secure Auditing

Check online users: we suggest that you check online users regularly to see if the NVR is logged in without authorization.

Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

K. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

L. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a locked door.

M. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

N. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from an external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two subnetworks, it is suggested to use VLAN, network GAP, and other technologies to partition the network, to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

O. It is recommended that you enable your firewall or blocklist and allowlist feature to reduce the risk that your device might be attacked.

6 ADDITIONAL INFORMATION

For more information and to download the required software browse the following web page:

IS0900A00_26-09-2023

Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com