



Smart Video Parking Detector

User's Manual



Foreword

General






This manual introduces the functions and operations of smart video parking detector (hereinafter referred to as the "Device").

Models

Models	Working Mode	Pixel
DHI-ITC214-PH3A	Parking Space Detection	2 MP
DHI-ITC314-PH3A	Parking Space Detection	3 MP
DHI-ITC314-PH3A-TF	Parking Space Detection	3 MP
DHI-ITC314-PH3A-TBF	Parking Space Detection	3 MP

Safety Instructions

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

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2020

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the Device, hazard prevention, and prevention of property damage. Read these contents carefully before using the Device, comply with them when using, and keep the manual well for future reference.

Power Requirements



- Improper battery use might result in fire, explosion, or inflammation.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.
- Connect device (type-I structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

Application Environment Requirements

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust, or soot.
- Keep the Device installed horizontally or on a stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into the device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the Device within the rated range of power input and output.
- Do not disassemble the Device.
- Transport, use, and store the Device under the allowed humidity and temperature conditions.

Maintenance Requirements

- Do not directly touch and wipe the surface of the Device.



WARNING

- Use accessories suggested by the manufacturer, and install and maintain the Device by professionals.
- Do not provide two or more power supply modes; otherwise, the Device might be damaged.

Table of Contents

Foreword	I
Important Safeguards and Warnings	II
1 Production Introduction	1
1.1 Overview	1
1.2 Functions.....	1
2 Structure and Cable Connection	3
2.1 Appearance	3
2.2 Dimensions.....	3
2.3 Structure.....	4
2.4 Cable Connection	5
3 Installation	7
3.1 Cable Wiring.....	7
3.2 Installing the Device	7
4 Quick Configuration with ConfigTool	9
4.1 Initialization.....	9
4.2 Modifying IP Address.....	10
4.3 Updating System.....	11
4.4 Logging in to Device Web.....	15
5 Web Operations	16
5.1 Basic Web Configurations	16
5.1.1 Recommended PC Configuration.....	16
5.1.2 Initialization	16
5.1.3 Login.....	18
5.1.4 Logout.....	19
5.1.5 Resetting Password.....	19
5.1.6 Web Functions	20
5.2 Live	20
5.2.1 Video Stream	21
5.2.2 Live View.....	21
5.2.3 Logged Plate Number.....	23
5.2.4 Plate Snapshot	23
5.2.5 System Functions.....	23
5.2.6 Functions of the Live Interface	23
5.2.7 Vehicle Snapshot.....	24
5.2.8 Event List.....	24
5.3 Query	24
5.3.1 Picture Query.....	24
5.3.2 Record Query.....	25
5.4 Settings.....	27
5.4.1 ITC (Intelligent Traffic Camera).....	27
5.4.2 Camera.....	36

5.4.3 Video	39
5.4.4 Network.....	42
5.4.5 TCP/IP	42
5.4.6 Port.....	43
5.4.7 ONVIF.....	44
5.4.8 Auto Registration	44
5.4.9 Event.....	45
5.4.10 Storage	45
5.4.11 System	46
5.4.12 System Information	65
5.5 Alarm	67
Appendix 1 FAQ.....	69
Appendix 2 Cybersecurity Recommendations	70

1 Production Introduction

1.1 Overview

This Device is an intelligent parking space detector that can be used in intelligent parking lot management system for parking guidance and reverse vehicle search in indoor parking lots.

- It detects and captures vehicles, recognizes license plates, detects parking space status (empty or occupied), and controls the indicator light of parking space.
- By connecting to parking management system, LED display, and reverse vehicle search device, it provides parking guidance for drivers and facilitates reverse vehicle search for improved parking experience.

1.2 Functions

Intelligent Recognition

- Supports drawing detection area to detect parking space status (empty or occupied), and automatically capture pictures.
- Recognizes license plate.
- Supports detecting vehicles without license plates, and the detection threshold can be set.
- OSD overlay on video and snapshots.

Attractive Design

Attractive dome design, parking space indicator light, and ceiling installation allow the Device to meet the needs of indoor parking lots.

Wide Dynamic Range (WDR)

WDR is available on select models, making these models work well in both dark and bright scenes.

Integration

- It integrates dome design and parking space indicator light, and adopts ceiling mount to meet the needs of the parking lot.
- Some models support wide dynamic mode, which can automatically adapt to brighter and darker scenes.

Multi-color Indicator Light

- 7 colors are available for the indicator light, and the indicator light status can be adjusted as needed.

- The Device detects vehicles by video detection and recognizes license plates. The indicator light displays the status of the parking space (empty or occupied) according to the detection results.
- Supports configuring the indicator color according to the network port status.

Multiple Parking Space Detection

- DHI-ITC214-PH3A series support detecting 1–2 parking spaces at the same time.
- DHI-ITC314-PH3A series support detecting 1–3 parking spaces at the same time.
- DHI-ITC314-PH3A-TF series and DHI-ITC314-PH3A-TBF series support detecting 1–6 parking spaces at the same time.

360° Rotation

- The lens can be rotated by 360°, and the elevation angle can be adjusted by 90°.

Power Supply

- Standard 48V DC power supply, and adaptable to 12V DC–48V DC voltage.

Cascading Network

- For DHI-ITC214-PH3A and DHI-ITC314-PH3A series parking detectors, only the first device needs to be supplied with power (48V DC). Supports power supply cascading through network, with the number of devices no more than 10.
- For DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series parking detectors, only the first device needs to be supplied with power (48V DC). Supports power supply cascading through network, with the number of devices no more than 6.

2 Structure and Cable Connection



The device structure might vary with different models, and the actual product shall prevail.

2.1 Appearance

- Figure 2-1: Applicable to DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series.
- Figure 2-2: Applicable to DHI-ITC214-PH3A and DHI-ITC314-PH3A series.

Figure 2-1 Appearance (1)



Figure 2-2 Appearance (2)



2.2 Dimensions

- Figure 2-3 is applicable to DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series devices.
- Figure 2-4 is applicable to DHI-ITC214-PH3A and DHI-ITC314-PH3A series devices.

Figure 2-3 Dimensions (mm)

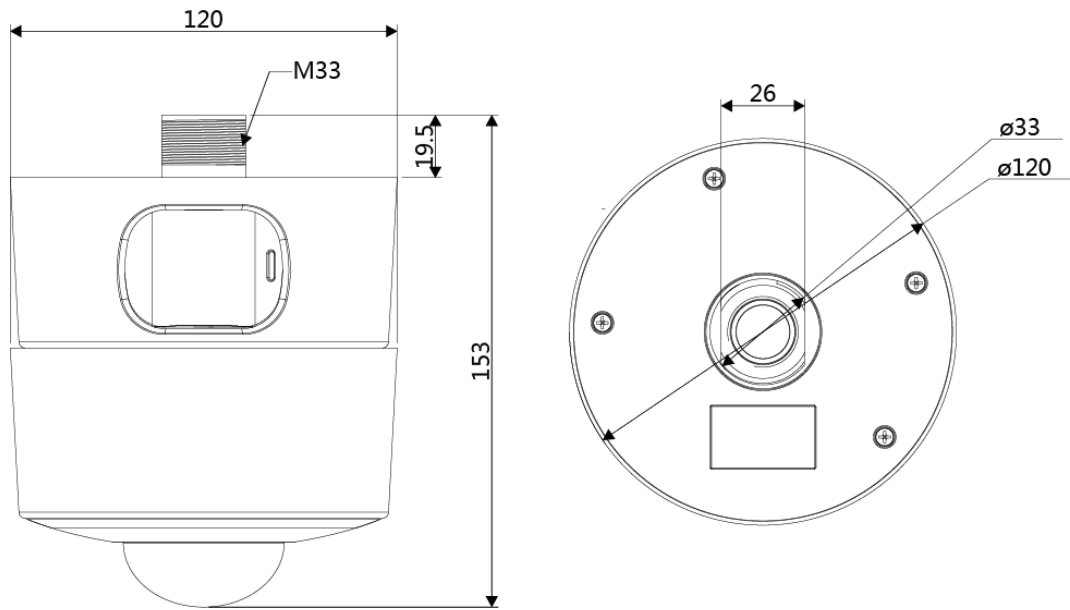
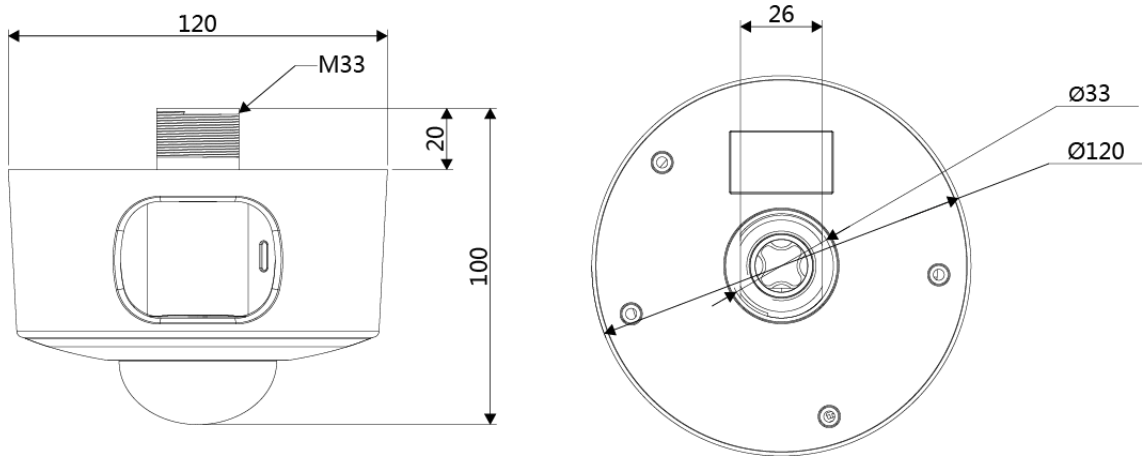


Figure 2-4 Dimensions (mm)



2.3 Structure



Structure shown in Figure 2-5 is applicable to DHI-ITC214-PH3A, DHI-ITC314-PH3A, DHI-ITC314-PH3A-TF, and DHI-ITC314-PH3A-TBF series devices. Only DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series devices are designed with lower housing 2.

Figure 2-5 Structure

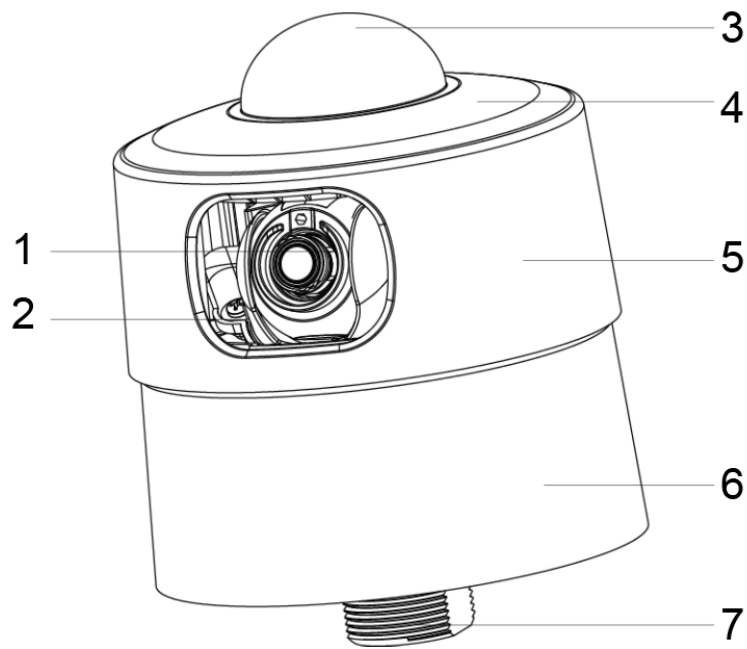


Table 2-1 Device structure description

No.	Description	No.	Description
1	Lens	5	Lower housing 1
2	Transparent cover	6	Lower housing 2
3	Indicator light cover	7	Base
4	Bracket for indicator light cover	—	—

2.4 Cable Connection

Figure 2-6 Cable connection

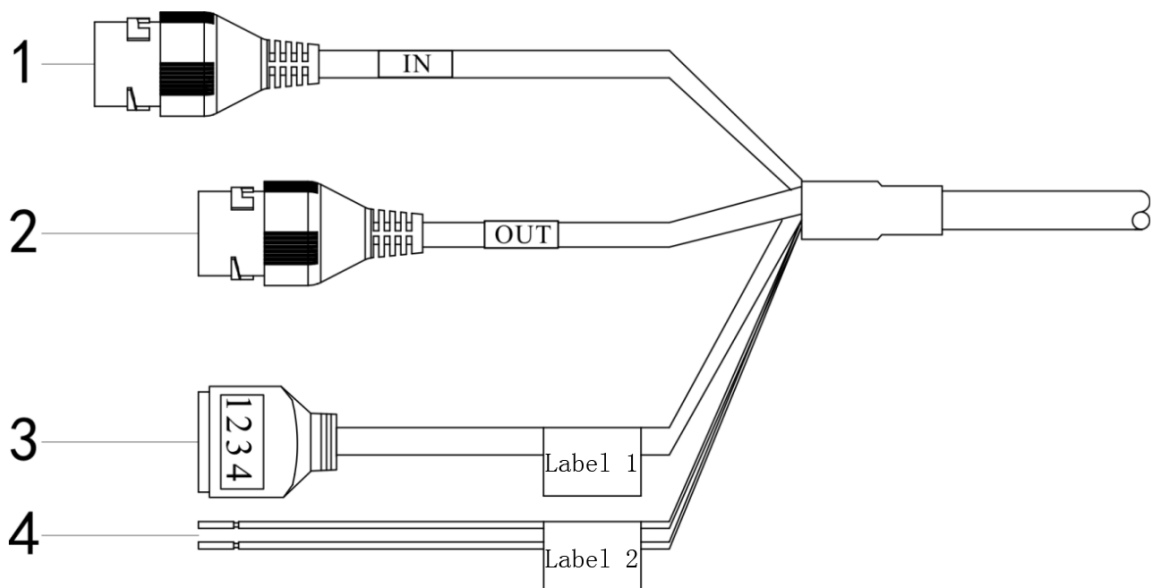


Table 2-2 Cable description

No.	Name	Description
1	Network port (IN)	Network power input port.
2	Network port (OUT)	Network power output port.
3	Power input port	1: 48V_IN. 2: GND_IN. 3: 48V_OUT. 4: GND_OUT.
4	RS-485 port	Yellow: RS-485_A. Orange: RS-485_B.

3 Installation

3.1 Cable Wiring

- For DHI-ITC214-PH3A and DHI-ITC314-PH3A series devices, only the first device needs to be supplied with power (48V DC). Supports power supply cascading through network, with the number of devices no more than 10.
- For DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series devices, only the first device needs to be supplied with power (48V DC). Supports power supply cascading through network, with the number of devices no more than 6.

3.2 Installing the Device



Mount the Device to the ceiling mounting tray, and the installation surface must be able to bear at least 3 times the weight of the Device.



- The stud diameter is 33 mm.
- The installation takes DHI-ITC314-PH3A-TF as an example. The installation diagram is for reference only, and the actual interface shall prevail.

Step 1 Use a hole saw to drill a hole with a diameter of 35 mm at the device mounting position.

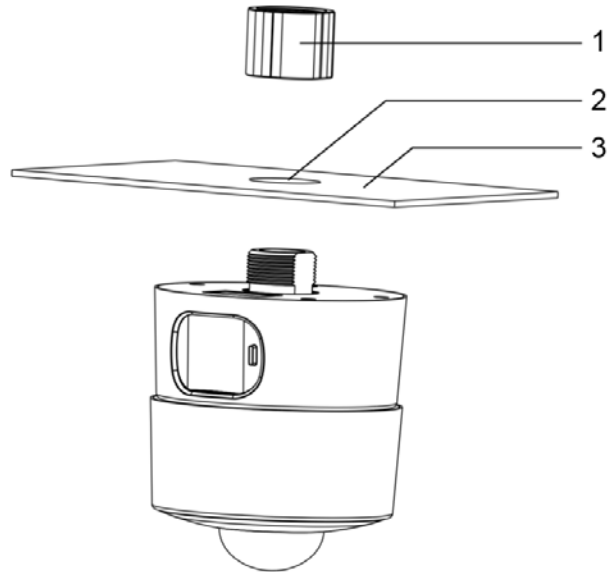
Figure 3-1 Hole saw



Step 2 Thread the cables of the Device through the hole of mounting tray.

Step 3 Loosen the nut, thread the cable through the nut, and then fix it to the mounting tray.

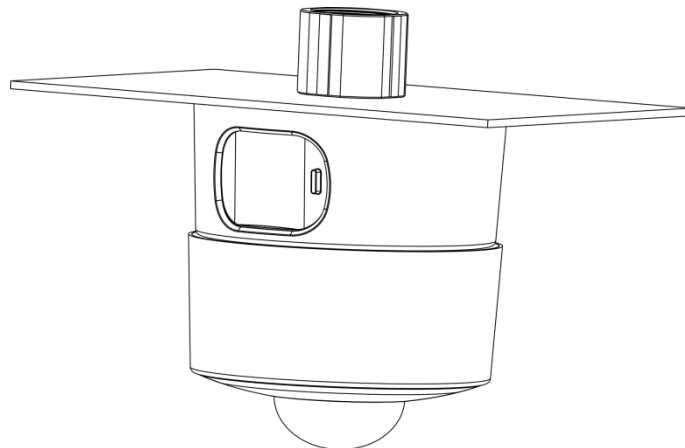
Figure 3-2 Installation (1)



1: Nut; 2: Ceiling mounting tray; 3: Hole of ceiling mounting tray

Step 4 Refer to "2.4 Cable Connection" to connect the cables.

Figure 3-3 Installation (2)



Step 5 Remove the cover, and adjust the monitoring view according to the position of the Device.

Step 6 Tighten the cover.

4 Quick Configuration with ConfigTool

The Device is delivered with the same default IP address (192.168.1.108 by default. IP address of the auxiliary camera of the DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series is 192.168.1.107 by default). Plan available IP network segments properly based on actual network conditions.

4.1 Initialization

The Device is delivered in an uninitialized status. You need to initialize it, and modify the default password before it can be used.

To acquire the configuration tool, go to Dahua official website, and then select **Support > Download Center > ToolBox**, follow the onscreen instructions to download and install the tool.

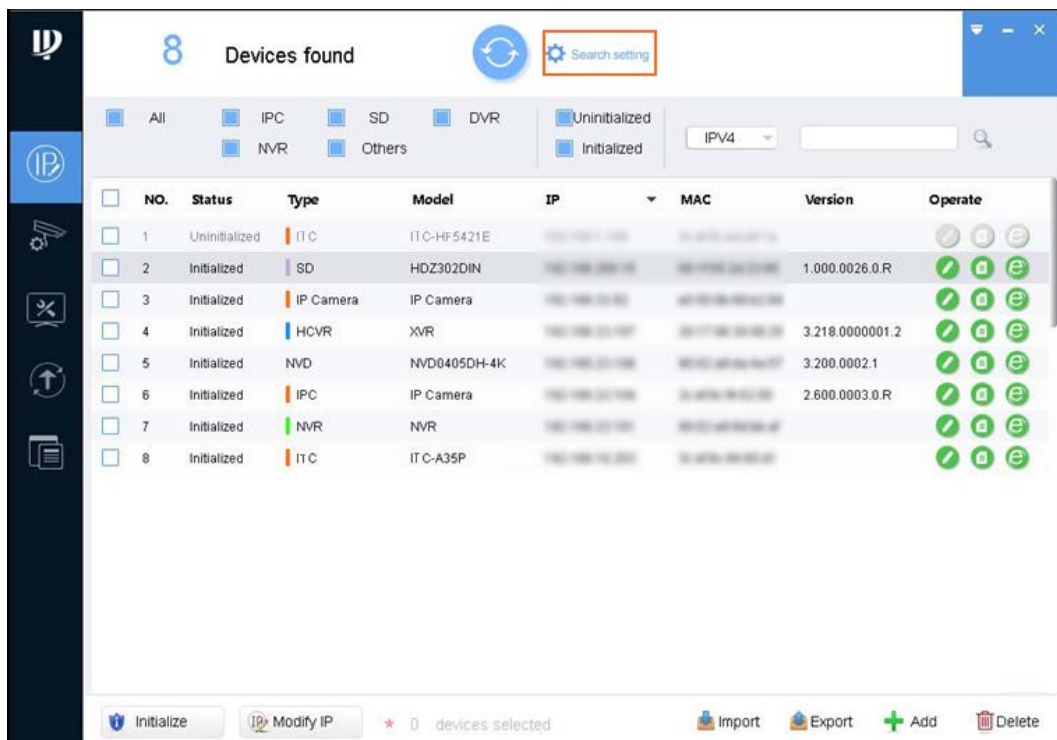


- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stay in the same network segment.
- Plan useable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only, and the actual product shall prevail.

Step 1 Double-click "ConfigTool.exe" to open the tool.

Step 2 Click .

Figure 4-1 Modify IP



Step 3 Click **Search setting**.

Step 4 Enter the start IP address and end IP address of the network segment in which you want to search devices, and then click **OK**.

- Step 5 All the devices found in the network segment are listed.
- Step 6 Select one or several devices with **Status** shows **Uninitialized**, and then click **Initialize**.
- Step 7 Select the devices that need initialization, and then click **Initialize**.

Figure 4-2 Password setting

- Step 8 Set and confirm the password of the devices, then enter a valid email address, and then click **Next**.



Password can be modified or reset in **System Settings**.

- Step 9 Select the options according to your needs, and then click **OK**.
- Step 10 The **Initialization** interface is displayed after initialization is completed. Click the success icon (✓) or the failure icon (⚠) for the details.
- Step 11 Click **Finish**.
- Step 12 The device status in the **Modify IP** interface turns to **Initialized**.

4.2 Modifying IP Address



- You can modify IP address of one or multiple devices in one time. This section is based on modifying IP addresses in batches.
- Modifying IP addresses in batches is available only when the corresponding devices have the same login username and password.

- Step 1 Do "Step 1" to "Step 4" in "4.1 Initialization" to search for devices in your network segment.



After clicking **Search setting**, enter the username and password, and make sure that that they are the same as what you set during initialization, otherwise there will be "wrong password" notice.

- Step 2 Select the devices which IP addresses need to be modified, and then click **Modify IP**.

Figure 4-3 Modify IP Address

Step 3 Select **Static** mode, and then enter start IP, subnet mask, and gateway. All the IP addresses will be modified sequentially from the start IP.



- IP addresses of multiple devices will be set to the same if you select the **Same IP** checkbox.
- If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select **DHCP**.

Step 4 Click **OK**.

4.3 Updating System

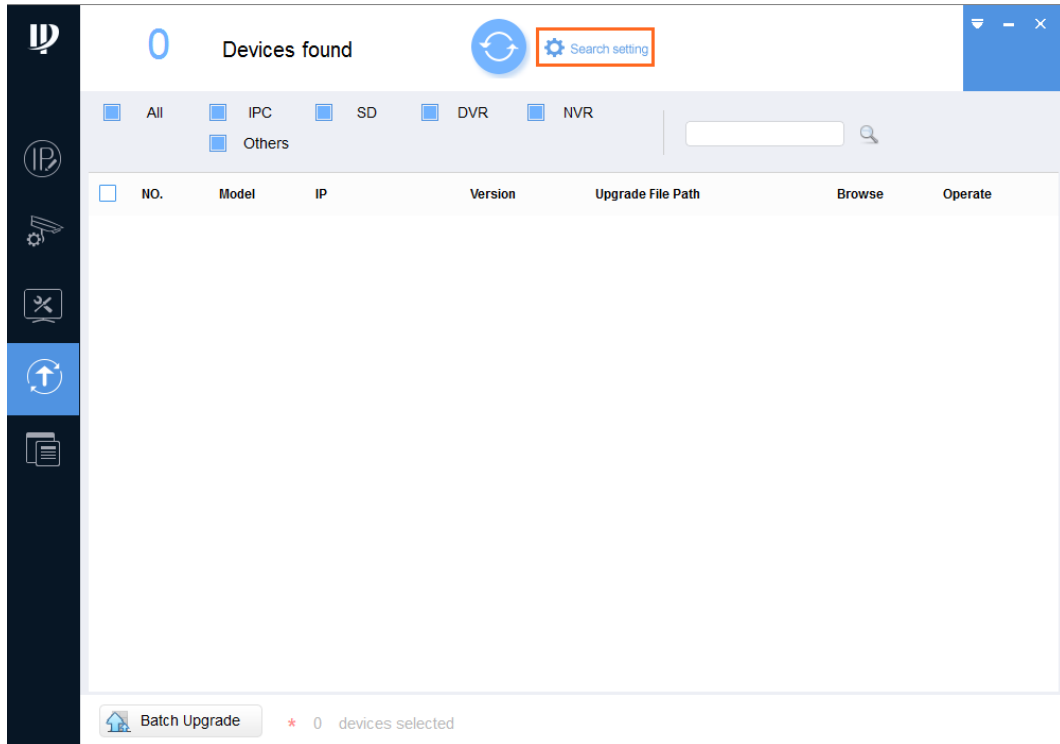
ConfigTool supports updating devices one by one or in batches.

- Updating devices one by one is ideal when few devices are involved, and login username and password of the devices are different.
- Updating devices in batches is recommended when multiple devices are involved, and login username and passwords of devices are the same.

Step 1 Double-click "ConfigTool.exe" to open the tool.

Step 2 Click .

Figure 4-4 Update

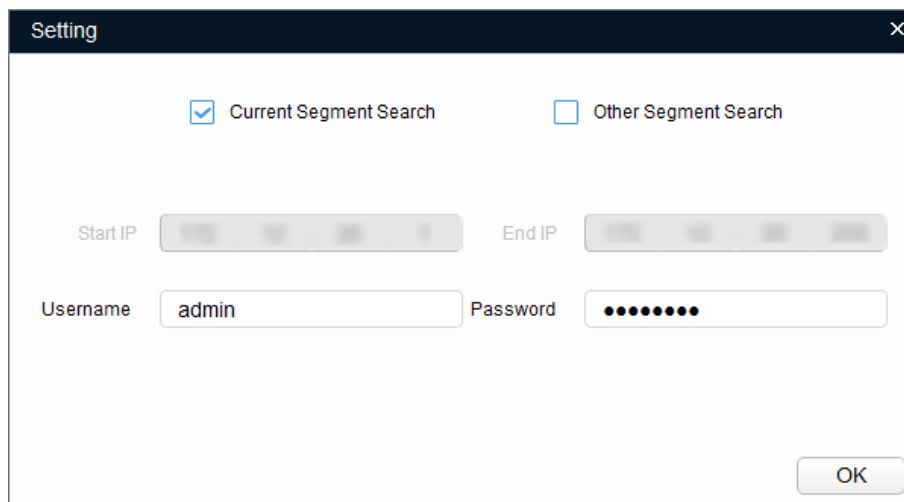


Step 3 Click **Search setting**.

Step 4 Select the network segment for the target device.

- If the IP address of the target device is in the current network segment, select **Current Segment Search**, and then enter the user name and the password of the target device.

Figure 4-5 Current segment search



- If the IP address of the target device is in other network segment, select **Other Segment Search**, then enter the start IP address and end IP address of the network segment you need, and then enter the user name and the password of the target device.

Figure 4-6 Other segment search

Step 5 Click **OK**.

The search result is displayed.

Figure 4-7 Search result

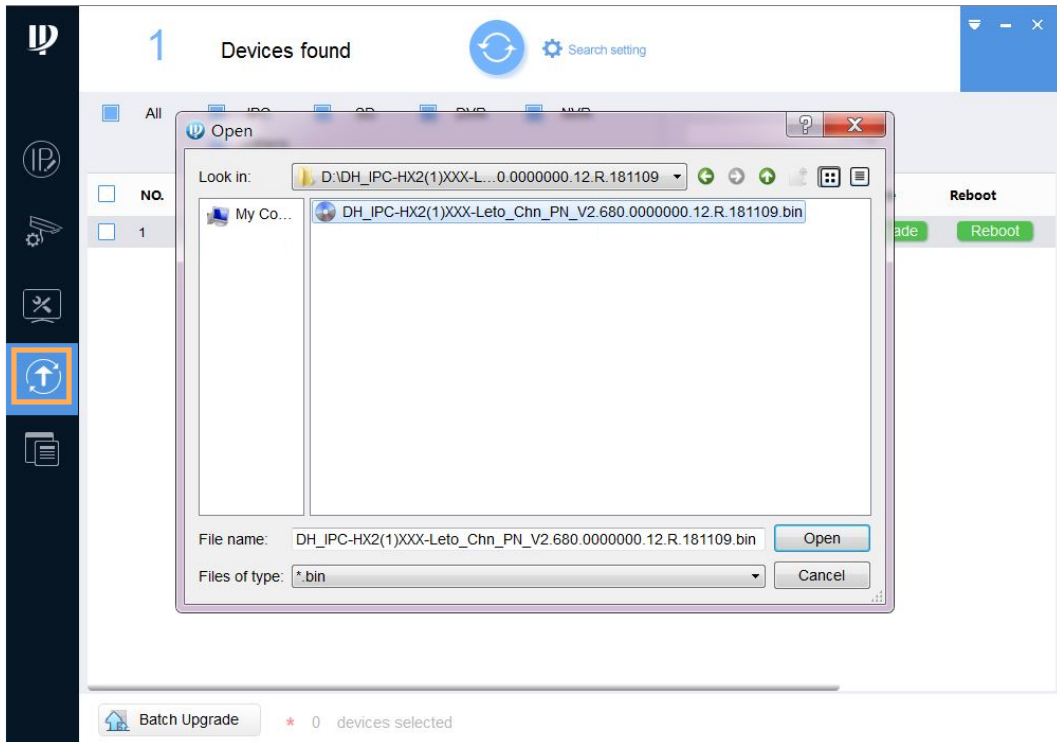
NO.	Model	IP	Version	Upgrade File Path	Browse	Operate
1	PC-NVR				Browse	Upgrade
2	PC-NVR-V3.0		3.0.0.0		Browse	Upgrade
3	IPC-HFW7243X-B-E2		2.622.0000000.0.R		Browse	Upgrade
4	Thermal Camera		2.622.0000000.3.R		Browse	Upgrade
5	NVR		4.002.0000000.0		Browse	Upgrade
6	DH-NVR5864-I_TELNET		3.215.0000010.0		Browse	Upgrade

Step 6 Select the devices to update.

- Update devices one by one: Select the corresponding device, and then click **Browse**.
- Update devices in batches: Select multiple devices, and then click **Batch Upgrade**.

Step 7 Select the update file.

Figure 4-8 Browse

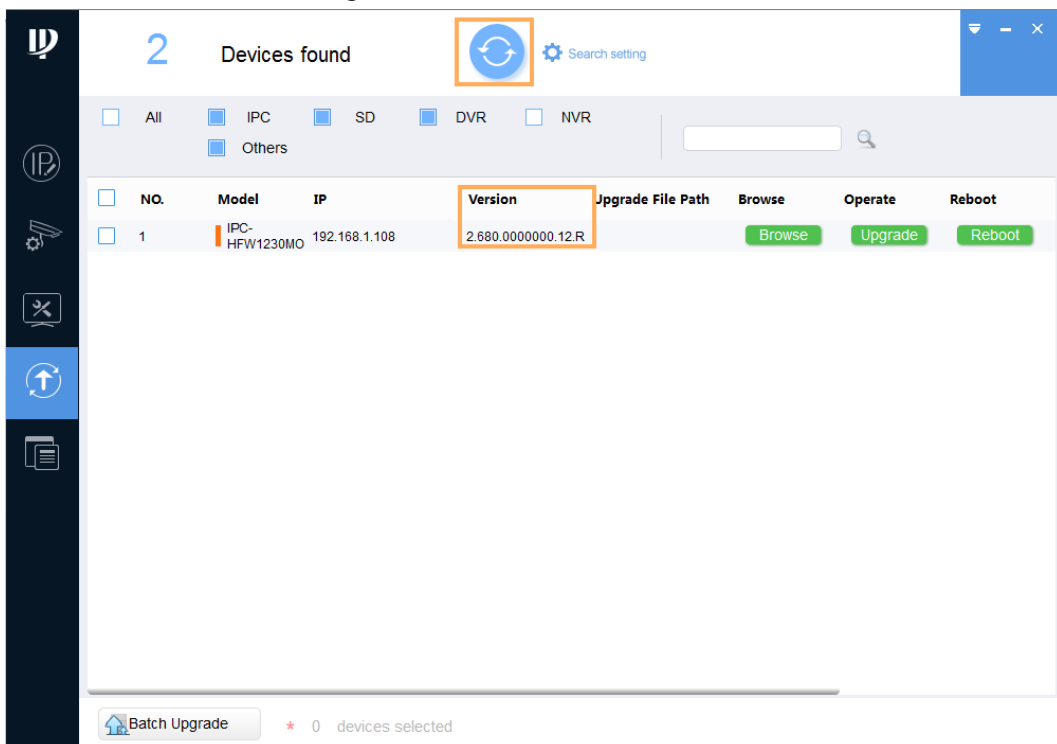


Step 8 Update the devices.

- Update the devices one by one: Click **Upgrade**, and the system starts updating. You can see the update progress.
- Update the devices in batches: Click **OK**, and the system starts updating.

Step 9 After restarting the device, click the refresh button to confirm the system version.

Figure 4-9 Confirm version



The update succeeded if the **Version** is the same as the version of the update file.



If the update failed, you can:

- Check whether the update file is correct.
- Restart the ConfigTool and do the update again.

4.4 Logging in to Device Web


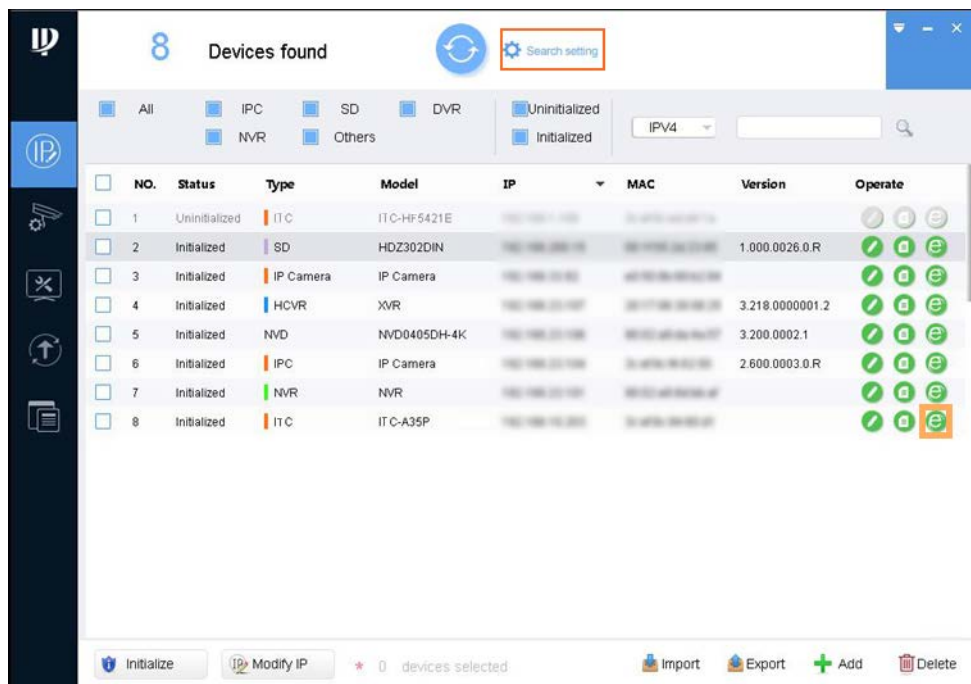
On the interface of modifying IP address, click  of the corresponding device to go to the device login interface.

Figure 4-10 Log in to device web



5 Web Operations

After mounting the Device, you need to power on the Device, connect it to the network, and make proper settings, then you can get the desired detection results.



The actual interface might vary depending on the model you purchased and the version of software. The figures in this manual are only for reference, and the actual interface shall prevail.

5.1 Basic Web Configurations

5.1.1 Recommended PC Configuration

Requirements of PC for logging in to the web interface of the Device is shown in the following table.

Table 5-1 Recommended PC configuration

PC Components	Recommended Configuration
Operating System	Windows 7 and newer.
CPU	Intel core i3 and newer.
Graphics Card	Intel HD Graphics and above.
Memory	2GB and more.
Display	1024×768 and higher.
Browser	Internet Explorer 8/9/10/11, Chrome33/44, and Firefox 49.

5.1.2 Initialization

Skip this section if you have initialized the Device with ConfigTool by following instructions in "4.1 Initialization."



- Initialization is required for first-time login or logging in after restoring factory default settings.
- Make sure that both PC IP and device IP are in the same network segment, otherwise it might fail to enter initialization interface.

Step 1 Set IP address, subnet mask, and gateway of PC and device respectively.

- If there is no router in the network, distribute IP address of the same segment.
- If there is router in the network, configure the corresponding gateway and subnet mask.

The IP address is 192.168.1.108 by default.

Step 2 Use ping `***.***.***.***` (device IP address) command to check whether network is connected.

Step 3 Open browser, enter the IP address of the Device in the address bar, and then press the Enter key.

Figure 5-1 Device Initialization

Step 4 Enter **Password** and **Confirm Password**.



- The new password must consist of 8–32 characters and contain at least two types from upper cases, lower cases, numbers, and special characters (excluding ' " ; : and &).
- If you want to change your password again, go to **Setup > System > Account > Account**.

Step 5 Select the **Email Address** check box, and then enter your email address. The email address is used for resetting password. It is recommended to set.

Step 6 Click **Confirm**.

The **Online Upgrade** interface is displayed.

Step 7 Click **Confirm**.

The login interface is displayed.

Figure 5-2 Login

Step 8 Enter the username and password, and then click **Login**.



Prompt box will pop out when username or password is incorrect, and it will remind you of remaining attempts. The account will be locked for 300 s if user enters incorrect username or password for 5 times consecutively.

Step 9 Click **Please click here to download and install the plug-in** in the video window.

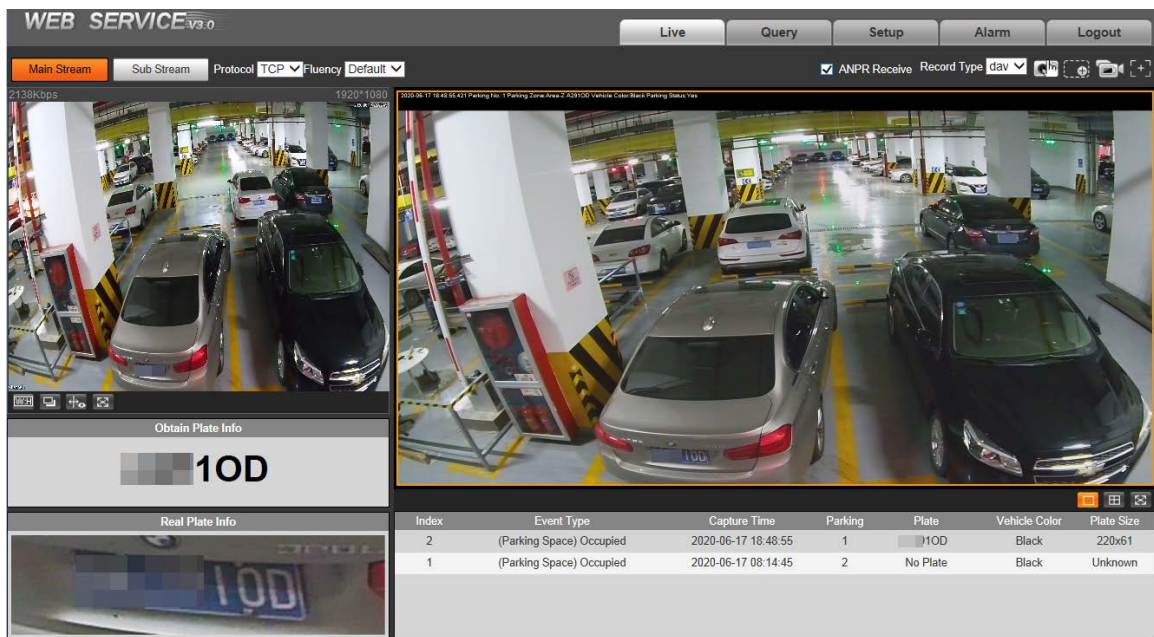
The system automatically downloads webplugin.exe and installs it according to prompt.



Before installing plug-in, make sure that the associated plug-in option of active has been modified as **Enable** or **Prompt** in **Internet Option > Security Settings**.

After installation is completed, the web interface is displayed.

Figure 5-3 Web interface



It will pop out the prompt box of authorization failed when there is no operation on the web interface for a long time. In this case, you need to log in again.

5.1.3 Login

Step 10 You can log in to the web by following the steps below. For first-time login, see "5.1.2 Initialization."

Step 1 Enter the IP address of the Device in the browser address bar, and press Enter.

Step 2 Enter username and password on the displayed interface, and then click **Login**.



- A box pops up when the username or password is incorrect.
- If you enter invalid username or password for five times, the account will be locked for five minutes.

5.1.4 Logout

Click **Logout** at the upper-right side of the web interface to log out.

You can enter the username and password to log in again.

5.1.5 Resetting Password

You can reset your password through email when it is lost or forgotten. Make sure that your email is correctly entered during initialization (see "5.1.2 Initialization"). Email address of admin user can be modified from **Setup > System > Account > Account > Username**.

Details of resetting the password are as follows:

Step 1 Enter the IP address of the Device in the browser address bar, and press Enter.

Step 2 On the login interface, click **Forgot password?**

Step 3 In the pop-up dialog box, click **OK**.

Step 4 Scan the QR code according to the interface prompt, and send the scanning result to the designated email to acquire security code.



Scan the actual QR code. Do not scan the QR code in this manual.

Step 5 Enter received security code in the text box of **Security code**.

Figure 5-4 Reset password

Reset the password(1/2)

QR code:

Note(For admin only):
Please use an APP to scan the left QR code to get special strings. And then send the strings to support_gpwd@htmicrochip.com.

The security code will be delivered to 1***@gmail.com.

Security code:

Cancel Next

Step 6 Click **Next**.

Step 7 Set **Password**, and enter your new password again in **Confirm Password**.

Step 8 The new password must consist of 8–32 characters, and contain at least two types from upper cases, lower cases, numbers and special characters (excluding ' ' ; : and &). The new password must be the same as the **Confirm Password**. Follow the password security notice to set a high-security password.

Step 9 Click **Yes** and the password is reset.

Figure 5-1 Reset password (2)

Reset the password(2/2)

Username: admin

Password:

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.

Confirm Password:

5.1.6 Web Functions

You can view real-time video captured by the Device, set detection rules of number plate recognition and traffic violations, and play back video recordings and snapshots to trace back event (if any). Here introduces the overview of each function button on the **Live** interface.

Table 5-2 Web functions

Operation	Description
Live	Displays real-time video and picture. You can record video and capture pictures, and configure video play and picture settings. See "5.2 Live."
Query	You can search for pictures and records on this interface. See "5.3 Query."
Setup	You can configure the way that the Device works, the rules for detecting violations, and the internet protocol for device network connection. You can also view version and system information of the Device. See "0 Settings."
Alarm	You can configure how the Device responds when alarms occur. See "5.5 Alarm."
Logout	Log out the web interface. See "5.1.4 Logout."

5.2 Live

The **Live** interface is displayed after you successfully log in to web. On this interface, you can view the live video image and the captured number plate, take snapshots, view the event details, and more.

Figure 5-2 Live

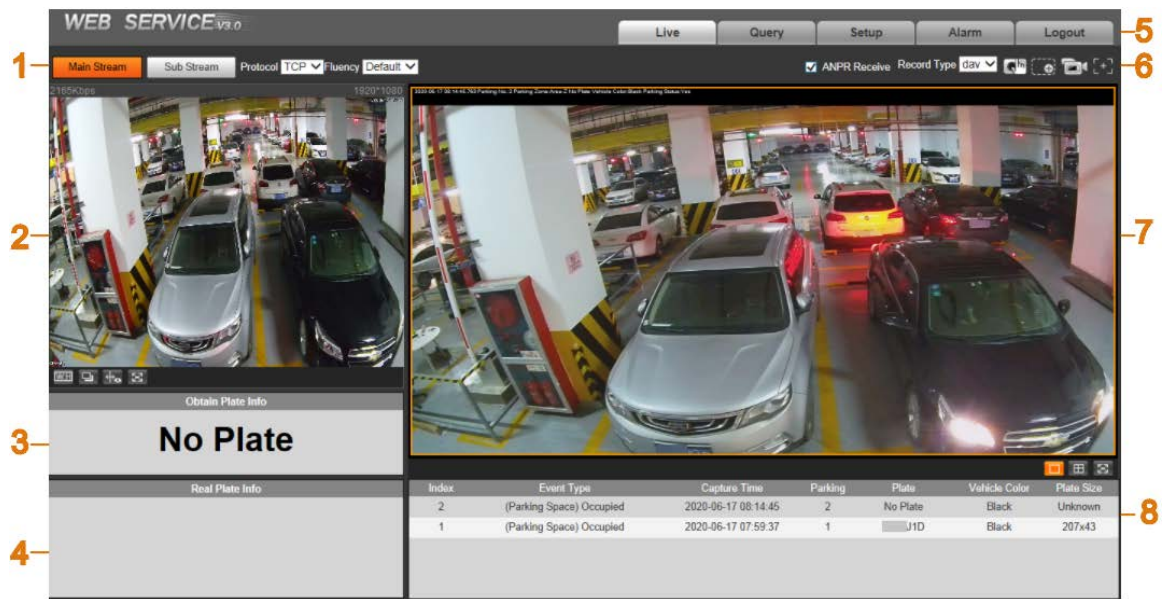


Table 5-3 Description of Live interface

No.	Description	No.	Description
1	Video stream	5	System functions
2	Live view	6	Functions of Live interface
3	Logged plate number	7	Vehicle snapshot
4	Plate snapshot	8	Event list

5.2.1 Video Stream

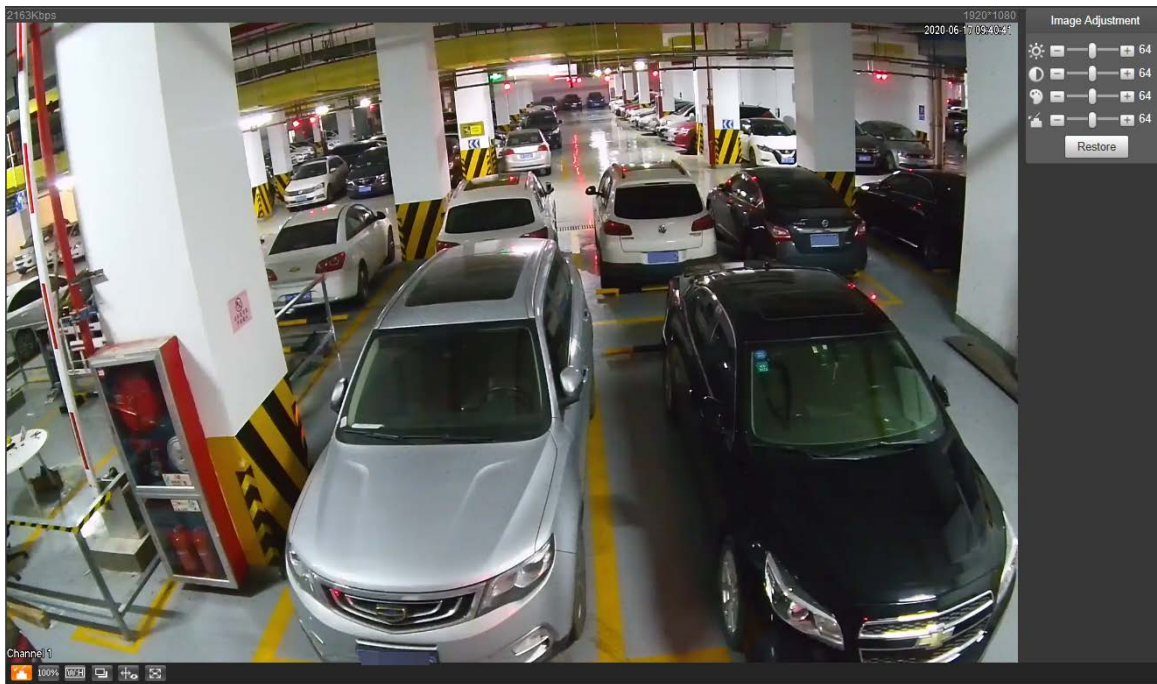
- **Main Stream:** Make sure that the Device can record video and carry out network surveillance when the network is normal. You can configure main stream resolution within the supported range of the Device.
- **Sub Stream:** Replaces main stream to make network surveillance and reduce the network bandwidth possession when network bandwidth is insufficient.
- **Protocol:** Video surveillance protocol, currently it only supports **TCP**.
- **Fluency:** Fluency of viewing the live video. The fluency can be set to **High**, **Middle**, **Low** and **Default** (recommended).

5.2.2 Live View

Displays the live video captured by the Device. You can also click the icons to change the display mode of live view.

- : Adjust the image to original size or adaptive window.
- : Click it to switch to big window, and then the image adjustment interface is displayed. Click it again to exit big window.

Figure 5-3 Big window















- ◇ : Click it to open image adjustment window on the right, meanwhile the button turns to . Click  to close image adjustment window. For image adjustment description, see Table 5-4.
- ◇ : Click it and the image is 100% displayed, meanwhile the button turns to . Click  to switch back to original size.
- : Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed in the video image.
- : Click it and the window is displayed in full screen; double-click or right-click to exit full screen.

Table 5-4 Image adjustment

Icon	Name	Description
	Brightness	Adjust the overall image brightness. Change the value when the image is too bright or too dark. The range is from 0 to 128 (64 by default).
	Contrast	Change the value when the image brightness is proper but contrast is not enough. The range is from 0 to 128 (64 by default).
	Hue	Adjust the image hue. For example, change red into blue. The default value is made by the light sensor and normally it does not have to be adjusted. The range is from 0 to 128 (64 by default).
	Saturation	Adjust the color vividness and will not influence the image overall brightness. The range is from 0 to 128 (64 by default).

Icon	Name	Description
	—	Click it to restore brightness, contrast, saturation, and hue to default values.



In this image adjustment window, you can only adjust image brightness, contrast, hue, and saturation of local web. To adjust system brightness, contrast, hue and saturation, go to **Setup > Camera > Camera Attribute > General**.

5.2.3 Logged Plate Number

Displays the plate number recognized by the Device in real-time when a vehicle passes.

5.2.4 Plate Snapshot

Displays the snapshot of license plate when a vehicle passes.

5.2.5 System Functions








Click the icons to set system functions, which include playback, video recording and snapshot query, intelligent rules setting, alarm event setting, and system logout. See more details in the following chapters.

5.2.6 Functions of the Live Interface

Set functions of the **Live** interface, and then the system will display the desired information on the **Live** interface.

Table 5-5 Function description of the Live interface

Icon	Name	Description
	ANPR Receive	Select the check box, and the Device automatically receives vehicle snapshots and detects event information triggered by sources such as radar or video detection, and displays such snapshots and information at the lower part of the interface. The snapshots are saved in the storage path defined by Setup > Storage > Destination > Save Path .
	Record Type	Select the format of video recordings (dav by default). It is required to be ps for GB 28181.

Icon	Name	Description
	Manual Snapshot	Click it, and the Device takes a snapshot when a vehicle passes. The snapshot is saved in the storage path.  <ul style="list-style-type: none"> • Enable ANPR Receive first. • To change the storage path of snapshots, go to Setup > Storage > Destination > Save Path.
	Digital Zoom	Drag left mouse button and select any area in the video window, and then the area will be zoomed in. In any area of the video window, click  or right-click to exit.
	Video Recording	Click it to start recording. Click  again to stop recording. You can set the storage path of video recordings from Setup > Storage > Destination > Save Path .
	Easy Focus	Click it to start auto focus, local focus, and license plate check for the monitoring image.

5.2.7 Vehicle Snapshot

Select **ANPR Receive**, and then snapshots will be displayed when vehicles pass.

5.2.8 Event List

Select **ANPR Receive**, and the event information will be displayed, including No., event types, capture time, lanes, plates, vehicle color, speed, vehicle signs, and vehicle types.

5.3 Query

You can search for snapshots, vehicle flow, and video recordings on the **Query** interface.

5.3.1 Picture Query

You can view pictures saved on your PC and verify picture watermark.



To view or set the save path of pictures on your PC, go to **Setup > Storage > Destination > Save Path**.

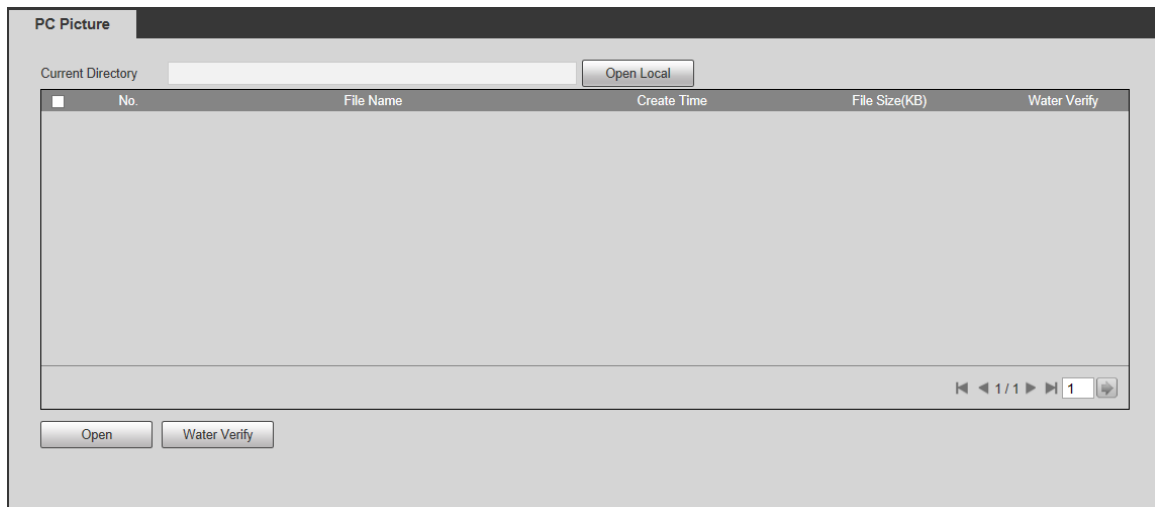
Step 1 Select **Query > Picture Query**.

Step 2 Click **Open Local** to select the file that includes the picture to be verified.

Step 3 Select the picture to be verified, and click **Water Verify**. The verify result can be viewed.

Step 4 Select a picture and click **Open**, or double-click a picture to view the picture in a photo viewer.

Figure 5-4 PC picture




5.3.2 Record Query

Search for the video recordings stored on your PC to trace back abnormal event (if any).

5.3.2.1 Record

You can search for the recorded video on your PC and also play back the video.



- Click  on the **Live** interface, and the Device starts recording. Click the icon again, and the Device stops recording; otherwise, the Device will keep recording until the web interface is closed or you log out. The recorded video is saved on your PC and to the path defined in **Setup > Storage > Destination > Save Path**.
- The function is available on select models, and the actual product shall prevail.

Step 1 Select **Query > Record Query > Record**.

Step 2 Click **Open Record** to select the recorded video on your PC, and then you can play back the video.

Figure 5-5 Record

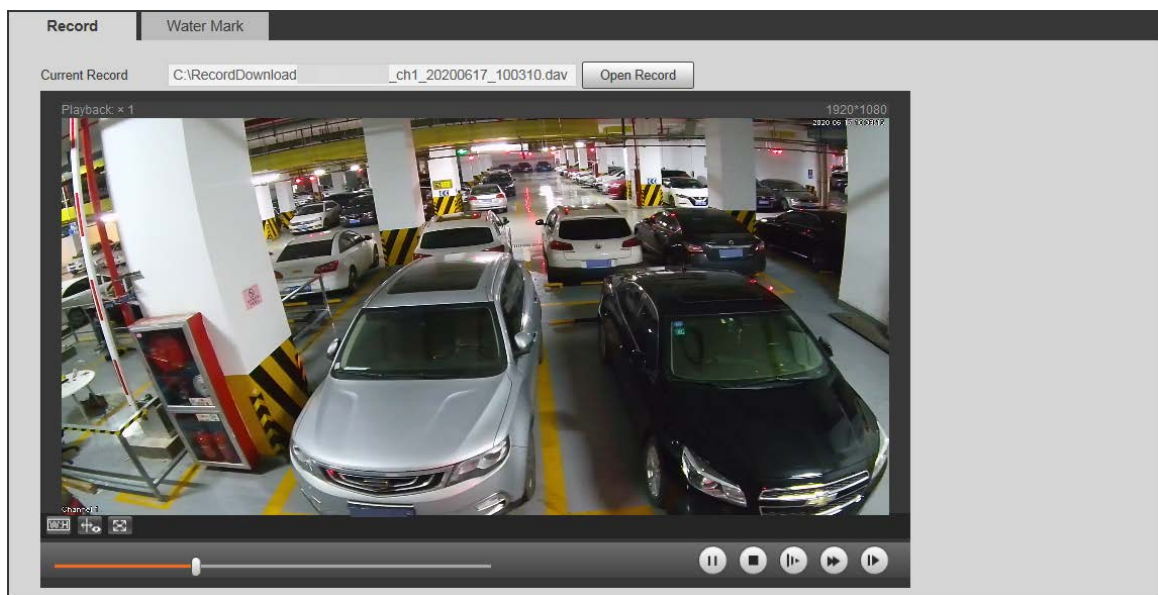


Table 5-6 Play parameters

Icon	Description
	Click it, and then you can select Original or Adaptive playback.
	Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed in the video image.
	Click it to enter full screen. Double-click the video image or press Esc to exit full screen.
	Click it to play back the video. Click to pause.
	Click it to stop playing back the current video.
	Click it for slow playback. Click to restore normal playback.
	Click it for quick playback. Click to restore normal playback.
	Click it to play back next frame.

5.3.2.2 Watermark

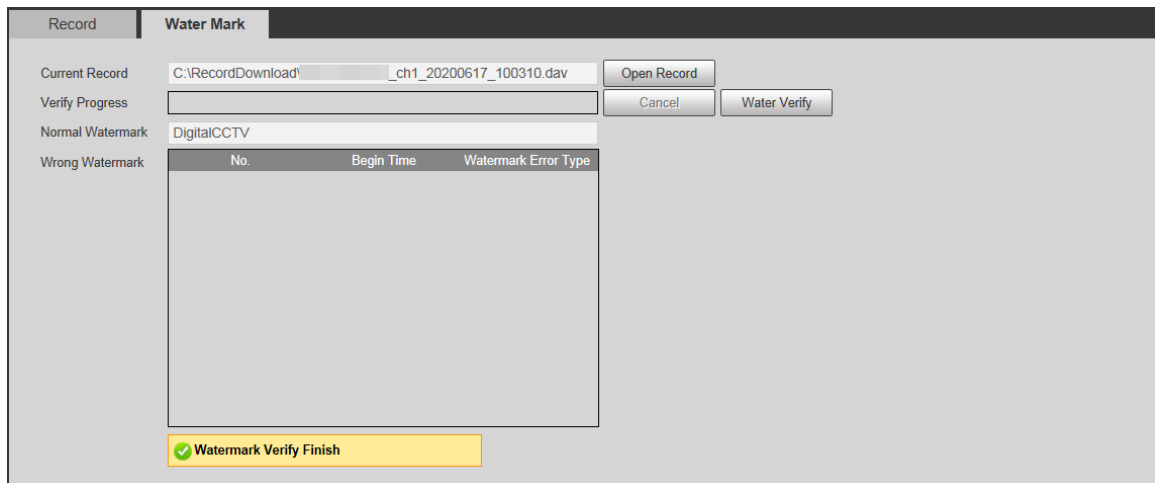
Verify the watermark of selected video recording. Only .dav recording is supported.



Before verifying the watermark, you need to select **Water Settings** and configure **Watermark Character** from **Setup > Camera > Video > Video > Main Stream**. The watermark character is **DigitalCCTV** by default.

Step 1 Select **Query > Record Query > Water Mark**.

Figure 5-6 Watermark



- Step 2** Click **Open Record** to select the record.
 Click **Water Verify**. The system will display the verify progress and normal watermark information.

5.4 Settings

You can configure device attributes to make the Device clearly display the monitoring image of the scenario, set the detection rules to make the Device detect parking space status (occupied or empty), set network parameters of the Device, and view device and system information.

5.4.1 ITC (Intelligent Traffic Camera)

Set parameters related to parking space, OSD, indicator light, and more.

5.4.1.1 Parking Space Configuration

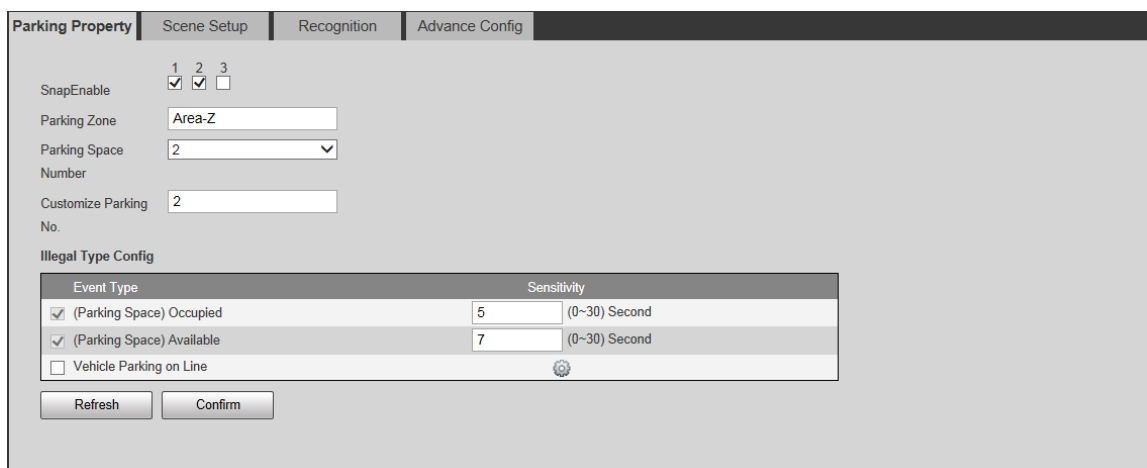
Configure parameters and event type related to the parking space, and draw the parking space detection area.

5.4.1.1.1 Setting Parking Space Property

Set the parking lot, parking space No., and event type related to the parking space.

- Step 1** Select **Setup > ITC > Parking Space Config > Parking Property**.

Figure 5-7 Parking property




Event Type	Sensitivity
<input checked="" type="checkbox"/> (Parking Space) Occupied	5 (0-30) Second
<input checked="" type="checkbox"/> (Parking Space) Available	7 (0-30) Second
<input type="checkbox"/> Vehicle Parking on Line	

Step 2 Enable capturing parking spaces according to the number of parking spaces actually detected.

Step 3 Enter the current parking area or zone in **Parking Zone**.

Step 4 Select parking space No. from **Parking Space Number (Customize Parking No. changes according to the defined Parking Space Number)**.

Step 5 Configure the event type that triggers capture.

- **(Parking Space) Occupied:** The Device takes a snapshot when the parking space is occupied. Sensitivity can be set. The higher the sensitivity value, the longer the capture time, and the higher the detection stability.
- **(Parking Space) Available:** The Device takes a snapshot when the parking space becomes available. Sensitivity can be set. The higher the sensitivity value, the longer the capture time, and the higher the detection stability.
- **Vehicle Parking on Line:** The Device takes a snapshot when the vehicle crosses the parking line. Click , and you can set the sensitivity and **Overline Check Threshold** (the threshold of detecting crossing the parking line). The higher the sensitivity value, the longer the capture time, and the higher the detection stability.

Step 6 Click **Confirm**.

5.4.1.1.2 Configuring Parking Space

Configure the detection area of parking space. You can draw the parking space in the video image according to the actual parking line.


Step 1 Select **Setup > ITC > Parking Space Config > Scene Setup**.

Step 2 Enable **Intelligent Frame**, and then you can view the CL level of parking space that you have drawn. The higher the CL level, the greater the chances that a vehicle is detected.

Step 3 Click **Park Region**, and then draw the parking space in the video image.

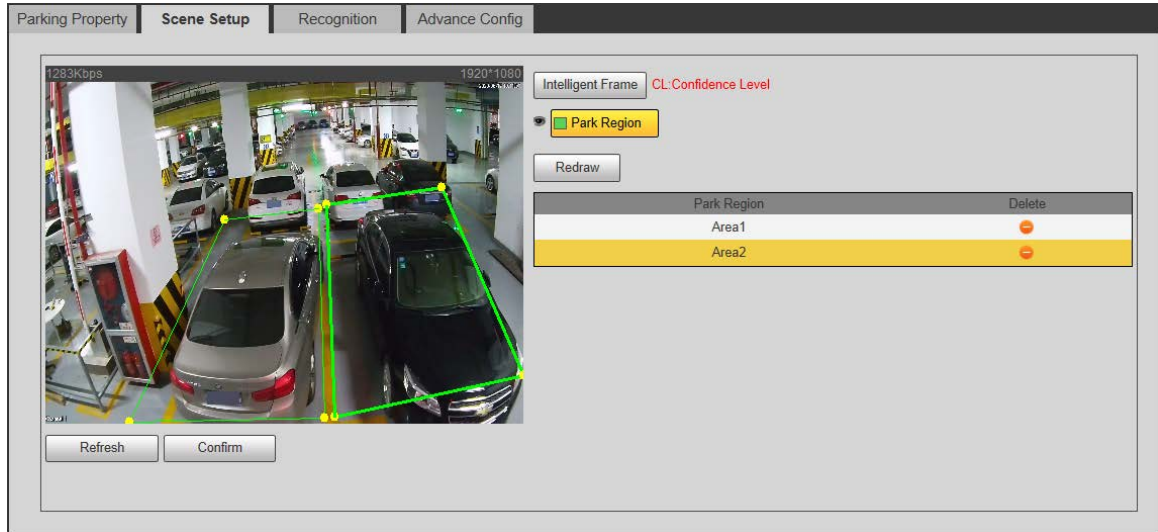


- The number of parking spaces that you can draw is 2-3, depending on the selected device model.
- You can draw four lines to define a parking space.

- Select a parking space that you have drawn, and then click Redraw, or click  to delete the selected parking space.

Step 4 Click **Confirm**.

Figure 5-8 Scene configuration



5.4.1.1.3 Recognition

Set the vehicle recognition parameters, including local plate characters, detection threshold, and more.

Step 1 Select **Setup > ITC > Parking Space Config > Recognition**.

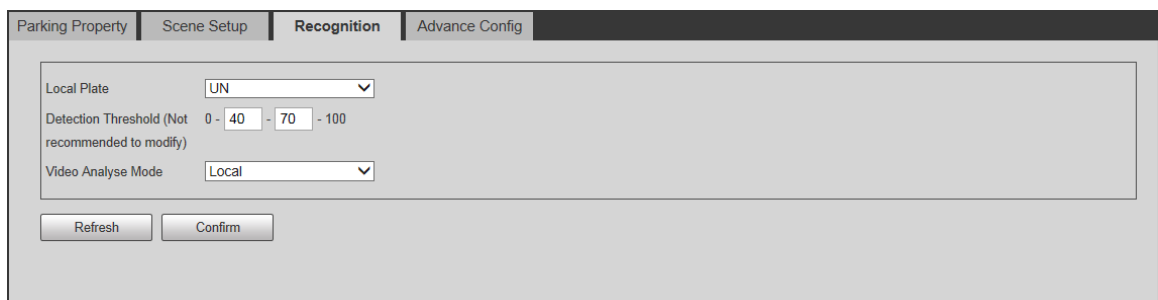
Step 2 Select the local plate that the Device detects. Currently, it supports **UN**, **RU**, and **EU**.

Step 3 Set the detection threshold. It is recommended to keep the default range.

Step 4 Select video analysis mode from **Local** (license plate recognition by the Device) and **Remote** (license plate recognition by platform).

Step 5 Click **Confirm**.

Figure 5-9 Recognition



5.4.1.1.4 Advance Config

You can enter custom algorithm expressions for custom functions.

Step 1 Select **Setup > ITC > Parking Space Config > Advance Config**.

Step 2 Enter the custom algorithm expressions in **Advanced Options**.

Step 3 Click **Confirm**.

Figure 5-10 Advanced config



5.4.1.2 OSD Config

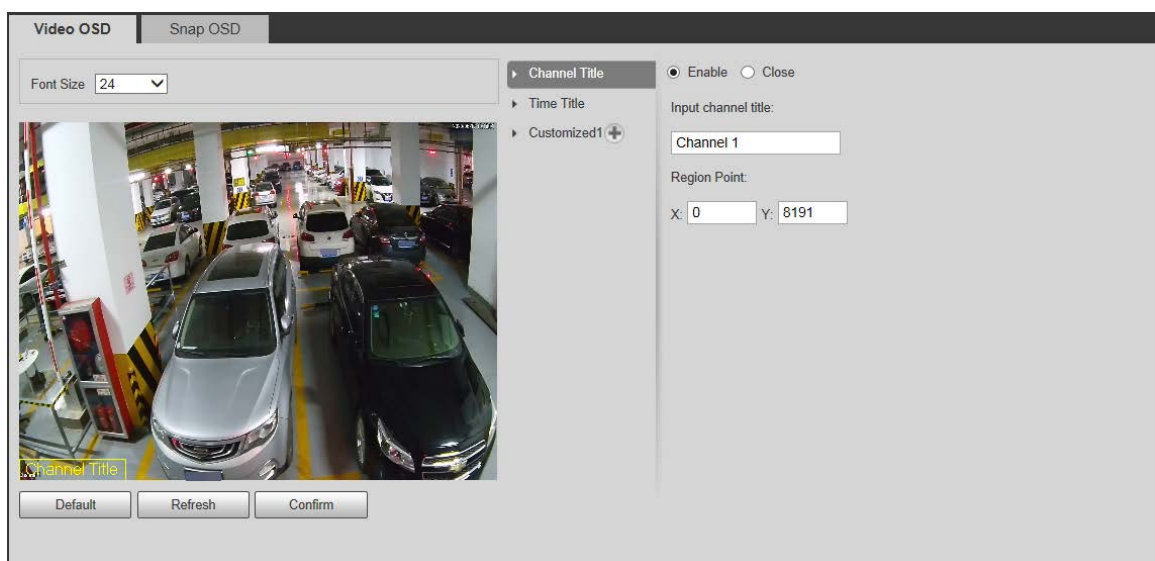
OSD (On-screen Display) refers to characters overlaid in the video or picture, so users can easily view related information.

5.4.1.2.1 Video OSD

Configure OSD information of video channel, including channel title, time title, and more, and then the OSD information will be overlaid on the video.

Step 1 Select **Setup > ITC > OSD Config > Video OSD**.

Figure 5-11 Video OSD




Step 2 Configure the font size.

Step 3 Configure channel title and position of the title.

- 1) Click **Channel Title**, and then select the **Enable** check box.
- 2) Enter channel title.
- 3) Drag the yellow box in the video image, or enter the coordinates to configure the position of the channel title.

Step 4 Configure the time title and the position of title.

- 1) Click **Time Title**, and then select the **Enable** check box.
- 2) Select the **Week Display** check box.
- 3) Drag the yellow box in the video image, or enter the coordinates to configure the position of the time title.

Step 5 Click  to add customized title. You can configure other OSD information and its position as needed.

Step 6 The system supports up to 5 customized titles.

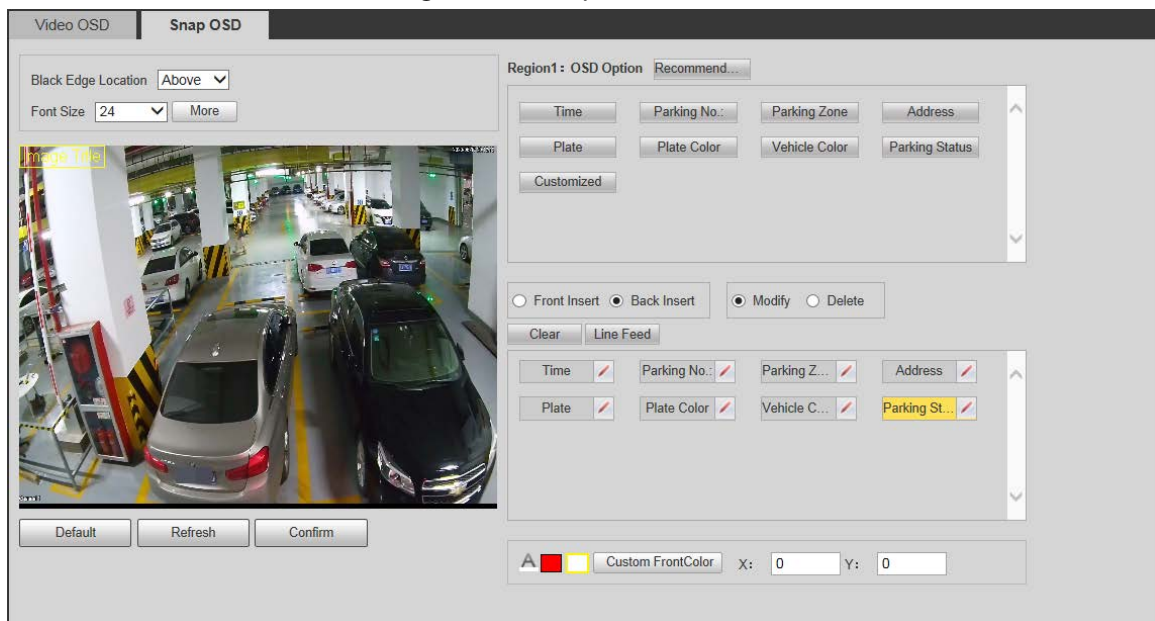
Step 7 Click **Confirm**.

5.4.1.2.2 Snap OSD

Configure the OSD information and position of image, and then the OSD information will be overlaid on the snapshots.

Step 1 Select **Setup > ITC > OSD Config > Snap OSD**.

Figure 5-12 Snap OSD



Step 2 Drag your mouse to select any area in the image to add image title. Drag the box to the position that you want, or enter the value in X/Y boxes at the lower-right side.



- The system supports up to 8 image titles. You can customize OSD options of each image title.
- Right-click an image title to delete it.

Step 3 Select the **Black Edge Location** (location of OSD black strip) which includes **Above**, **Below**, and **None**.

Step 4 Select the **BlackRegion Height**, which ranges from 8 pixels through 32 pixels.

Step 5 Configure the font size and font color of OSD information.

Step 6 You can configure the font color by clicking **Custom FontColor** at the lower side.

Step 7 Click **More**, and the box of configuring new line and separator is displayed.

- 1) Select the **New Line** check box as needed.
- 2) Configure the OSD separator, which includes **Blank Space**, **Vertical Line** and **Customized**. By selecting **Customized**, you can enter other separator.
- 3) Click **Yes**.

Figure 5-13 New line and separator

Step 8 Configure **OSD Option**.



Click **Recommend Overlay** to configure general overlay OSD options with one click.

Table 5-7 Snap OSD parameters

Parameter	Description
Insert Front	Select an OSD option, and then click Insert Front or Insert Back before selecting another OSD option, the new OSD option will be shown before after the original OSD option.
Insert Back	
Modify	Click Modify , and the status of OSD information (New Line excluded) will change to . Click to modify the prefix, postfix, content and separator of corresponding OSD option.
Delete	Click Delete , and the status of all selected OSD information will change to . Click to delete the corresponding OSD option.
Clear	Delete all the OSD information.
Line Feed	Select one OSD information, and then click Line Feed . The option next to the selected OSD information will be shown in a new line in the snapshots captured by clicking ANPR Receive on Live interface.

Step 9 Click **Confirm**.

5.4.1.3 Indicator Light Control

Configure the corresponding indicator color for different statuses of parking spaces, and then the corresponding light will turn on when the parking space status changes.

You can also configure the remote control parameters to control the parking space indicator lights of another parking detector, or make the indicator lights detected by the Device controlled by another parking detector.




- This function is not available for auxiliary camera of DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series devices.
- Remote control of indicator light is not available for DHI-ITC314-PH3A-TF and DHI-ITC314-PH3A-TBF series devices.


Step 1 Select **Setup > ITC > Light Control**.

Figure 5-14 Light control

Step 2 Configure the parameters.

Table 5-8 Description of indicator light control parameters

Parameter	Description
Light Config	
Controlled IP	<p>When the parking space indicator status of parking detector A needs to be remotely controlled by parking detector B, enter the IP address of B in Controlled IP, and the indicator light status of A will be controlled by B.</p>  <p>This configuration works after you setting the IP address of A by clicking Remote Control from Setup > ITC > Light Control on web interface of B. For details, see Step 3.</p>
Light Sensitivity Config	
Licensed Sensitivity	Set the sensitivity of the indicator responds when licensed vehicle, unlicensed vehicle, no vehicle or parking over parking line is detected. The smaller the value, the faster the indicator responds.
Unlicensed Sensitivity	
NoVehicle Sensitivity	
OverLineLightingSensitivity	
Light For Parking Spaces Status	
Space Free	Set the indicator status when Space Free (parking space is empty), Space Full (parking space is occupied) and Space
Space Full	

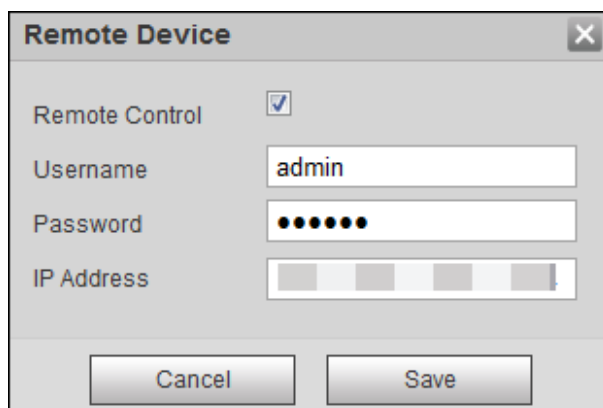
Parameter	Description
Space OverLine	<p>OverLine (parking over parking line).</p> <ul style="list-style-type: none"> Indicator colors available: Red, yellow, blue, green, cyan, white, and pink. You can also select Close to disable indicator light. By selecting Twinkle, the indicator flashes. If not, the indicator is always on. You can select Light Off, Always Lighting, or Customized to define the indicator status when Space OverLine (parking over parking line).
Net Status Config	
Single Net Exception	<p>Set the indicator status when network exception is detected.</p> <ul style="list-style-type: none"> Indicator colors available: Red, yellow, blue, green, cyan, white, and pink. You can also select Close to disable indicator light. By selecting Twinkle, the indicator flashes. If not, the indicator is always on.
Double Net Exception	
Parking Light Config	
Internal	<p>Link the built-in indicator light of the Device to parking space. Remote control can be set.</p> <p>For example, select Parking1, Parking2, and Parking3, and when the three parking spaces are occupied, the indicator shows the color defined from Space Full. When one of the three parking spaces become empty, the indicator shows the color defined from Space Free.</p>
External	<p>Link the external indicator light of the Device to parking space. Remote control can be set.</p> <p>For example, link External1 to Parking1, and when parking space 1 become empty, the indicator shows the color defined from Space Free.</p> <p>An external indicator light can be linked to multiple parking spaces.</p>  <p>To enable external indicator light function, set the Protocol to DHRS Device from Setup > ITC > RS485/232.</p>
Remote Control	
Remote Control	Control the indicator light status of another parking detector.

Step 3 (Optional) Configure remote control of indicator light.

After configuration, the parking detector can controls the indicator light status of the controlled parking detector.



- 1) Click **Remote Control**.

Figure 5-15 Remote control



- 2) Select the check box to enable remote control.
- 3) Enter the username, password, and IP address of the controlled parking detector.
- 4) Click **Save**.



Click  to add more parking detectors, or click  to delete the corresponding device.

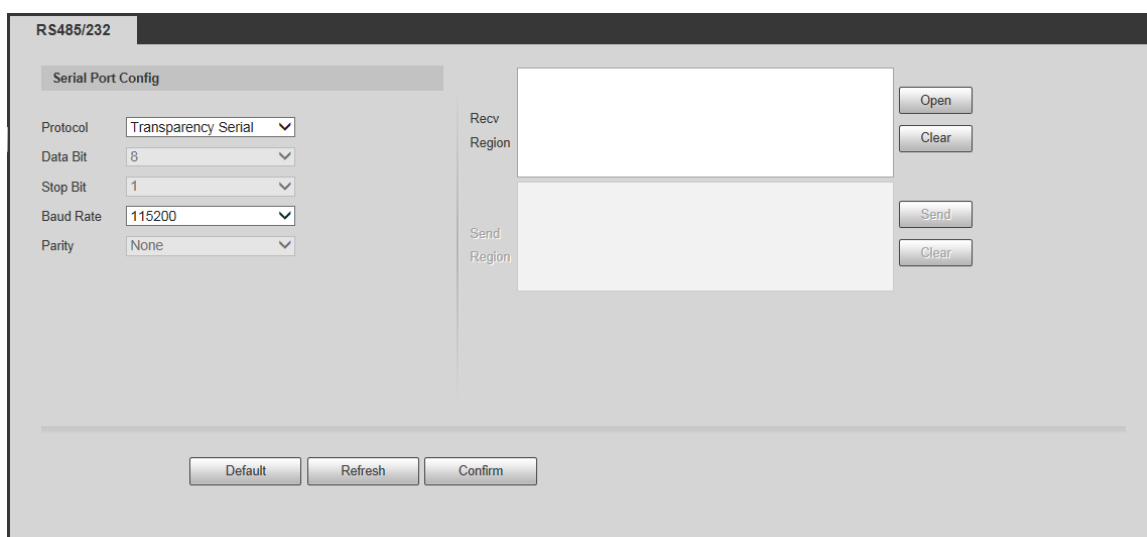
Step 4 Click **Confirm**.

5.4.1.4 RS485/232

Configure the serial port, so that external device such as indicator light can be connected to the Device.

Step 1 Select **Setup > ITC > RS485/232**.

Figure 5-16 RS485/232



Step 2 Configure the parameters.

Step 3



Step 4 Parameters in **Serial Port Config** must be consistent with the settings of serial port.

Table 5-9 Description of RS485/232 parameters

Parameter	Description
Protocol	Serial port protocol. Transparency Serial and DHRS Device are available. Select DHRS Device when external indicator light is connected.
Data Bit	It is 8 by default.
Stop Bit	It is 1 by default.
Baud Rate	Select the corresponding baud rate. A high baud rate helps move data fast, but needs a wide bandwidth.
Parity	It is None by default.

Step 5 Click **Open** to enable the **Recv Region** (receiving region) and **Send Region** (sending region).

Step 6 Enter communication data in the **Send Region**, and then click **Send**.

The Device sends data to the serial port, and the data returned by the serial port will be displayed in the **Recv Region**.

5.4.1.5 Intelligence Default

On the **Intelligence Default** interface, you can restore all settings of the **ITC** tab to factory settings.

Step 1 Select **Setup > ITC > Intelligence Default**.

Step 2 Click **Default**.

Step 3 In the pop-up box, click **OK**.

5.4.1.6 Relative Device

You can log in to the auxiliary device of the Device by selecting **Setup > ITC > Relative Device**, and entering the **IP Address**, **Subnet Mask**, and **Default Gateway** of the auxiliary device.



This function is available on select models, and the actual interface shall prevail.

Figure 5-17 Relative device

The screenshot shows a web interface titled 'Relative Device'. It contains three text input fields labeled 'IP Address', 'Subnet Mask', and 'Default Gateway'. Below these fields is a button labeled 'Login Relative'.

5.4.2 Camera

You can configure the camera attributes, video and snapshot parameters, and more.

5.4.2.1 Camera Attributes

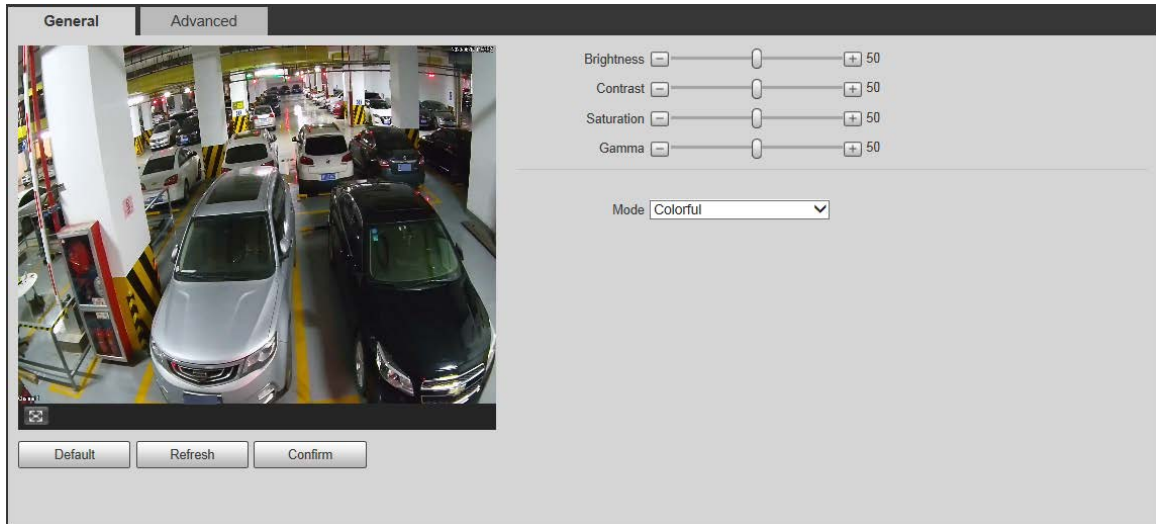
After connecting the Device to network and viewing the live video on its web interface, you can adjust the image parameters of the Device when necessary to get clear images.

5.4.2.1.1 General

You can configure the brightness, contrast, hue, saturation, mode, and more of the Device.

Step 1 Select **Setup > Camera > Camera Attribute > General**.

Figure 5-18 General



Step 2 Configure the parameters.

Table 5-10 General parameters

Parameter	Description
Brightness	<p>You can adjust the overall image brightness. Change the value when the image is too bright or too dark.</p> <ul style="list-style-type: none"> Both the darker area and the brighter area will have same changes when adjusting the brightness. The image might become blurry when the value gets bigger. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The larger the value, the brighter the image.
Contrast	<p>You can adjust the contrast when the image brightness is proper but contrast is not enough.</p> <ul style="list-style-type: none"> The larger the value, the darker the dark area, and the more exposed the bright area. The image might become blurry when the value gets smaller. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The larger the value, the bigger the contrast.
Saturation	<p>You can adjust the image saturation. Saturation value does not change overall image brightness.</p> <ul style="list-style-type: none"> The larger the value, the more saturated the image. It is 50 by default. The smaller the value, the more unsaturated the image. The recommended range is 40–60, and the available range is 0–100.
Gamma	<p>Adjust the image hue. For example, change red into blue. The default value is made by the light sensor and normally it doesn't have to be adjusted. The recommended value is from 40 to 60 and the range is from 0 to 100.</p> <p>It is 50 by default. The threshold is used to adjust image hue and it will not influence image overall brightness.</p>

Parameter	Description
Mode	<ul style="list-style-type: none"> • Colorful: The image is always colored. • Auto: When the brightness is higher than the threshold, the image automatically changes to color; when it is below the threshold, the image changes to black and white. • B/W: The image is always black and white.

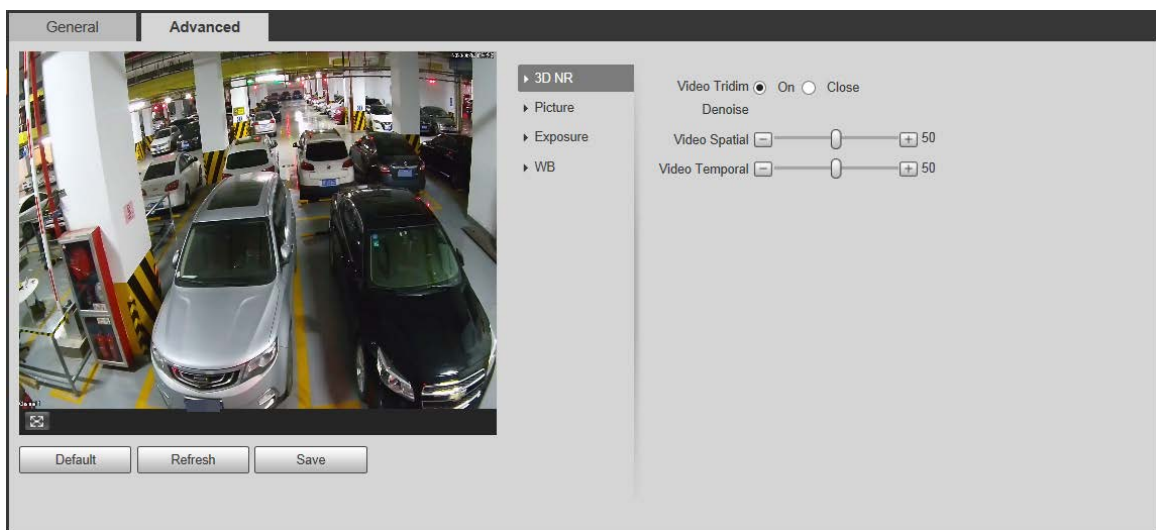
Step 3 Click **Confirm**.

5.4.2.1.2 Advanced

You can configure noise reduction, exposure mode, white balance, and more.

Step 1 Select **Setup > Camera > Camera Attribute > Advanced**.

Figure 5-19 Advanced



Step 2 Configure the parameters.

Table 5-11 Description of advanced parameters

Parameter	Description
3D NR	
Video Tridim Denoise	When it is On , 3D NR is enabled to reduce noise of video.
Video Spatial	Spatial video denoising. 50 by default. The higher the value, the fewer the noise.
Video Temporal	Temporal video denoising. 50 by default. The higher the value, the fewer the flicker noise.
Picture	
Scene	You can change the scene and adjust the sharpness of corresponding scene. Scenes available: Dawn/Dusk , Daytime , and Night .
Sharpness	You can set the sharpness of corresponding scene. The higher the value, the clearer the image. But there will be noise if sharpness is too high.

Parameter	Description
BLC Mode	Enable BLC, and adjust the WDR range to get clear image in the condition of strong background light. <ul style="list-style-type: none"> ● Close: Always close BLC. ● WDR: Enable WDR (wide dynamic range) to help provide clear video images in bright and dark light. It is 50 by default. ● BLC: Adjust the video brightness of a region or globally. <ul style="list-style-type: none"> ◇ Default: Automatically switch the WDR mode, and adjust the video brightness globally. ◇ Customized: Manually set the BLC region. Drag the yellow box or its corners to adjust the position or size of the region. ● GlareInhibition: Highlight compensation. The greater the value, the more obvious the effect of highlight compensation. ● SSA: Automatically adjust BLC mode according to the scene.
Exposure	
Mode	<ul style="list-style-type: none"> ● Select the way of adjusting exposure mode. ● In Auto mode, drag the slider to adjust the exposure compensation. ● In Manual mode, you can adjust the exposure compensation, shutter, shutter scope and gain scope. <ul style="list-style-type: none"> ◇ Shutter: You can select the shutter value, or select Customized Range, and then set the shutter range. ◇ Shutter Scope: Set the time range of shutter. ◇ Gain Scope: Set the value range of gain.
WB	
Mode	Set scene mode to adjust the image to its best status.

Step 3 Click **Confirm**.

5.4.3 Video

After connecting the Device to network and viewing the live video on its web interface, you can configure encoding parameters when necessary to get clear and smooth video image.

5.4.3.1 Video

Configure the parameters of video stream.

Step 1 Select **Setup > Camera > Video > Video**.

Figure 5-20 Video stream

Video	Snapshot	Interest Area
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p>Main Stream</p> <p>Stream Type: Normal</p> <p>Encode Mode: H.264M</p> <p>Resolution: 1920*1080(1080P)</p> <p>Frame Rate(FPS): 20</p> <p>Bit Rate Type: CBR</p> <p>Reference Bit Rate: 885-7078Kb/S</p> <p>Bit Rate: 2048</p> <p>I Frame Interval: 40 (20-150)</p> <p><input checked="" type="checkbox"/> Watermark Settings</p> <p>Watermark Character: DigitalCCTV</p> </div> <div style="width: 48%;"> <p>Sub Stream</p> <p><input type="checkbox"/> Enable</p> <p>Stream Type: Normal</p> <p>Encode Mode: H.264M</p> <p>Resolution: 704*576(D1)</p> <p>Frame Rate(FPS): 10</p> <p>Bit Rate Type: VBR</p> <p>Quality: 5</p> <p>Reference Bit Rate: 87-692Kb/S</p> <p>Max Bit Rate: 448</p> <p>I Frame Interval: 20 (10-150)</p> </div> </div>		
<input type="button" value="Default"/> <input type="button" value="Refresh"/> <input type="button" value="Confirm"/>		

Step 2 Configure the parameters.

Table 5-12 Video stream parameter

Parameter	Description
Stream Type	Currently, only Normal stream is supported.
Encode Mode	Modes of H.264B, H.264M, H.264H, MJPEG, and H.265 can be selected.
Resolution	The higher the value, the clearer the overall image. For each resolution, the recommended bit stream value is different. The resolution of sub stream cannot be greater than that of main stream.
Frame Rate (FPS)	The higher the value, the smoother the video image. The frame rate might vary due to different resolutions.
Bit Rate Type	You can select from VBR (variable bitrate) and CBR (constant bitrate). <ul style="list-style-type: none"> VBR: Gives best balance between quality and file as the bitrate can be altered depending on the video. CBR keeps the bitrate the same during the encoding, and it's more advantageous when the network connection is limited to performing at, say, 320 Kbps.
Quality	6 quality levels are available. The higher the value, the better the quality. You need to configure the image quality when VBR is set to Bit Rate Type .
Bit Rate	Higher bit rate signifies greater picture or video quality, but also occupies higher storage space. You need to configure the bit rate when CBR is set to Bit Rate Type .
Max. Bit Rate	It is the upper limit of stream in VBR. In CBR, the value is fixed.
I Frame Interval	The number of P-frame between two I-frames. The number varies according to the frame rate. The range is 25-150. It is recommended to configure the number as twice of the frame rate.

Parameter	Description
Watermark Settings	You can verify the watermark to check whether the video has been tampered. Select the Watermark Settings check box to enable watermark verification. The watermark character is DigitalCCTV by default. Watermark character consists of up to 85 characters from numbers, letters and underlines.
Enable	Enable sub stream when your network bandwidth is insufficient or other conditions that influences the video smoothness in main stream.

Step 3 Click **Confirm**.

5.4.3.2 Snapshot

Configure the snapshot size, quality, and coding size.

Step 1 Select **Setup > Camera > Video > Snapshot**.

Step 2 Select the **Quality** check box, and then adjust the quality of snapshots. 6 quality levels are available. The higher the value, the better the quality, and the higher requirements on storage.

Step 3 Select the **Picture Coding Size (KB)** check box, and then configure the coding size of snapshots.



You can configure either **Quality** or **Picture Coding Size**.

Step 4 Click **Confirm**.

Figure 5-21 Snapshot

5.4.3.3 Region of Interest

Set region of interest in the video image, and then the selected image will be displayed with the configured quality.

Step 1 Select **Setup > Camera > Video > Interest Area**.

Step 2 Drag your mouse in the video image to define the region of interest. You can draw more than one region when necessary (3 regions at most).

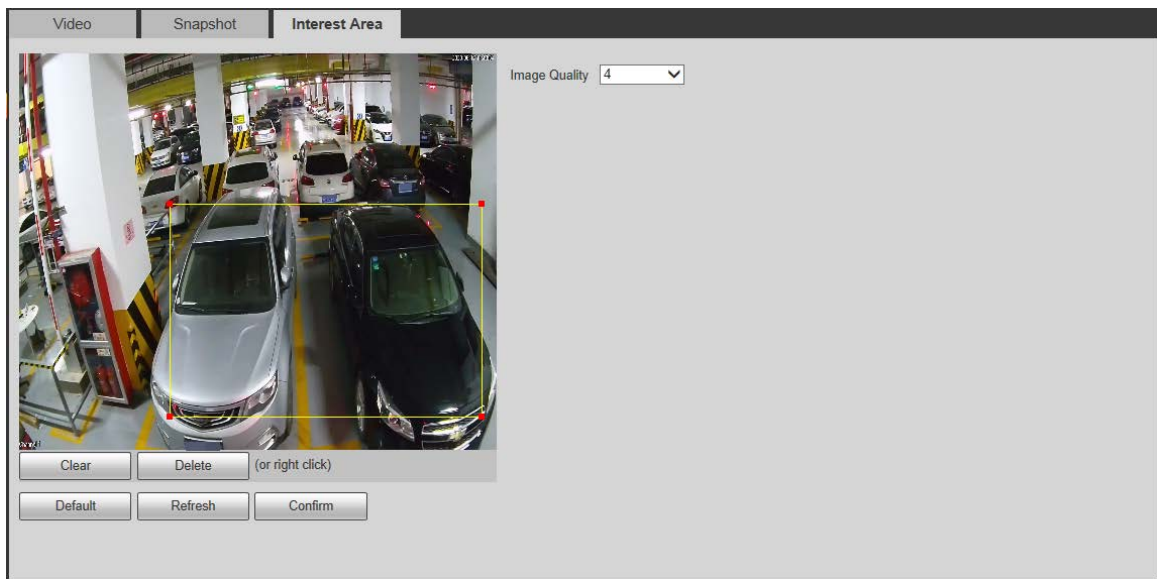


You can click **Clear** to delete all the regions of interest, or click **Delete** or right-click on the video image to delete the most recently configured region.

Step 3 Set the image quality of the region of interest. 6 quality levels are available. The higher the value, the better the quality.

Step 4 Click **Confirm**.

Figure 5-22 Interest area



5.4.4 Network

You can configure network parameters such as IP address, MAC address, subnet mask, default gateway, and more.

5.4.5 TCP/IP

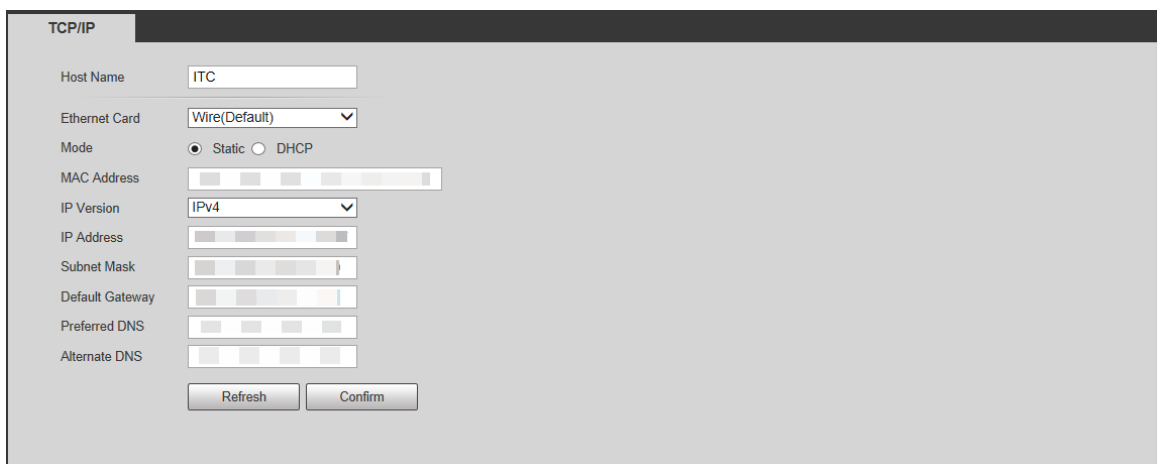
You can configure host name, IP address, and more.

Step 1 Select **Setup > Network > TCP/IP**.



Some models are designed with two network ports. Do not configure the ports in the same network segment; otherwise, the network might fail.

Figure 5-23 TCP/IP



Step 2 Configure the parameters.

Table 5-13 TCP/IP parameters

Parameter	Description
Host Name	Configure the host name (not exceeding 32 characters).
Ethernet Card	Only supports wire cards.
Mode	<p>Static and DHCP modes are available.</p> <ul style="list-style-type: none"> When DHCP is selected, the Device automatically searches IP. In this case, the IP Address, Subnet Mask, and Default Gateway cannot be configured. When Static is selected, the IP Address, Subnet Mask, and Default Gateway need to be manually configured.
MAC address	Displays host MAC address.
IP Version	IPv4 and IPv6 are available. Both IP versions can be accessed.
IP Address	IP address of the Device.
Subnet Mask	The subnet mask that masks the IP address of the Device.
Default Gateway	The default gateway corresponding to IP address of the Device.
Preferred DNS	IP address of preferred DNS.
Alternate DNS	IP address of alternate DNS.

Step 3 Click **Confirm**.

5.4.6 Port

You can set the port information, so you can access the Device through different protocols or configuration tools.

Step 1 Select **Setup > Network > Connection > Port**.

Figure 5-24 Port

Step 2 Configure each port number of the Device.

Table 5-14 Description of port parameters

Parameter	Description
Max Connection	The maximum number of clients (such as web client and platform client) that is allowed to access the Device simultaneously. It is 10 by default.
TCP Port	TCP protocol communication port. It is 37777 by default.
UDP Port	User data packet protocol port. It is 37778 by default.
HTTP Port	HTTP communication port. It is 80 by default.

Parameter	Description
RTSP Port	Media streaming control port. It is 554 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Confirm**.

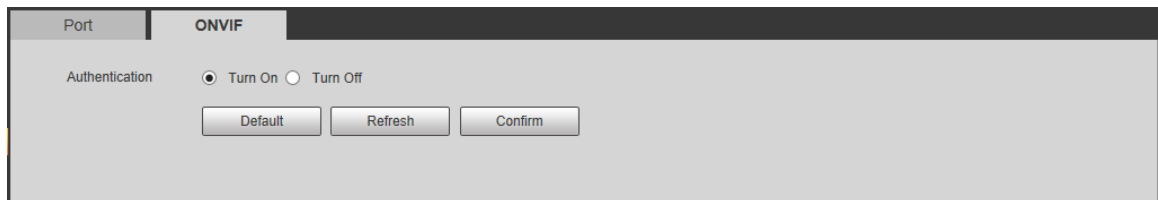
5.4.7 ONVIF

Open Network Video Interface Forum (ONVIF) is an open industry forum with the goal of providing and promoting standardized interfaces for interoperability of physical IP-based security products, such as IP camera, network recorder, and more.

Select **Setup > Network > Connection**, and the **ONVIF** interface is displayed.

Verification of username and password will be required for logging in to ONVIF when ONVIF authentication is turned on. If it is turned off, then no verification is required.

Figure 5-25 ONVIF



5.4.8 Auto Registration

When the Device is connected to network, it will automatically report its location to the server specified by user. This helps client software to access the Device through the server for viewing its live video and monitoring.

Step 1 Select **Setup > Network > Auto Register**.

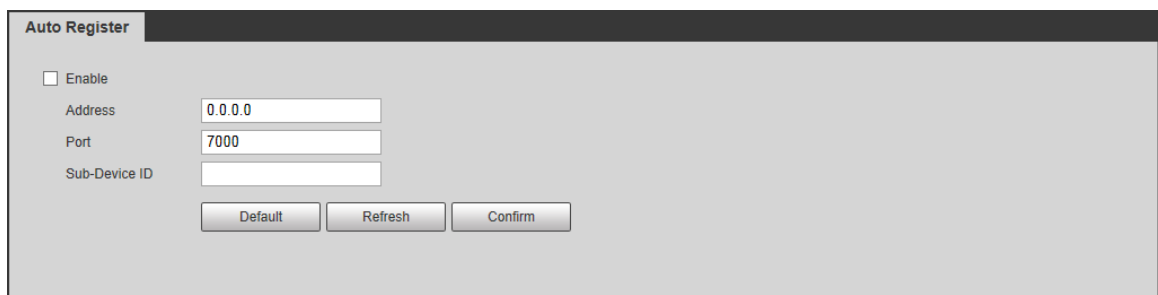
Step 2 Select the **Enable** check box to enable auto registration function.

Step 3 Enter the IP address of server that needs to be registered, and also the port for auto registration.

Step 4 Enter the **Sub-Device ID**, meaning the ID assigned by the server for auto registration device. Make sure that there is no repeated device IP.

Step 5 Click **Confirm**.

Figure 5-26 Auto register



5.4.9 Event

An alarm will be triggered when an abnormal event occurs to the Device. The event types include:

- **Network Error:** Alarm will be triggered when there is **Off-line Event** (the Device is offline) or **IP Conflict**.
- **Illegal Access:** Alarm will be triggered when unauthorized access is detected by the system.
- **Security Exception:** Alarm will be triggered when security problem occurs.

Step 1 Select **Setup > Event > Abnormality**.



The following figure takes **Network Error** as an example. For other events, click the **Illegal Access** or **Security Exception** tab.

Figure 5-27 Network error event



Step 2 Configure the parameters.



Refer to the actual interface to view the parameters that you need to configure for each abnormality.

Table 5-15 Parameters of abnormality events

Parameter	Description
Enable	Select it to enable alarm of abnormality event.
Event Type	Alarm will be triggered when there is Off-line Event (the Device is offline) or IP Conflict .
Login Error	Configure the number of login error allowed. The range is 3–10 times. This parameter is available when the Illegal Access tab is selected.

Step 3 Click **Confirm**.

5.4.10 Storage

You can configure the names and storage paths of snapshots and video recordings.

Step 1 Select **Setup > Storage > Destination**.

Step 2 Name the snapshots in the **Input Name** section. You can click **Help...** to view the **Picture Naming Help**, or click **Restore** to restore the naming rule to the default.

After setting the naming rule, you can view the name example in the **Name Preview** section.

Step 3 Click **Browse...** to set the save paths of snapshots and video recordings respectively.

Step 4 Click **Confirm**.

Table 5-16 Save path

5.4.11 System

You can configure system information, add users, restore to factory settings, import and export system configuration files, and more.

5.4.11.1 General

You can configure display language, video standard, and also set the time and time zone of the Device.

5.4.11.1.1 General Settings

You can configure the device code, system, video standard, and more.

Step 1 Select **Setup > System > General Setup > General Setup**.

Figure 5-28 General

Step 2 Configure the parameters.

Table 5-17 General setting parameters

Parameter	Description
Device SN	The device serial number consisting of letters, numbers, underlines and strikethroughs.

Parameter	Description
Device Code	No. of the Device. The device code cannot be overlaid in OSD information.
Language	Language of web browser interface. You need to log in again when switching to another language. Currently, only English is supported.
Video Standard	<p>PAL and NTSC are available.</p> <ul style="list-style-type: none"> PAL: Much more common around the world, and can be found in most of Western Europe, Australia, China, and elsewhere. NTSC: Mostly limited to North America, parts of South America, Japan, and the Philippines.
Machine Group	The group or entity that uses the Device.
Machine Address	The snapshot places of the Device.

Step 3 Click **Confirm**.

5.4.11.1.2 Date & Time

You can configure date, time, time zone, and more of the Device.

Step 1 Select **Setup > System > General Setup > Date&Time**.

Figure 5-29 Date & time

The screenshot shows the 'Date & Time' configuration page. It includes the following fields and options:

- Date Format: YYYY-MM-DD
- Time Format: 24-Hour
- Current Time: 2020-06-17 13:56:39 (with a 'Sync PC' button)
- DST: DST
- DST Type: Date, Week
- Begin Time: Jan 1 00:00:00
- End Time: Jan 2 00:00:00
- NTP Setting: NTP Setting
- NTP Server: clock.isc.org
- Port: 123
- Time Zone: GMT+08:00
- Interval: 10 minute(s) (1~30)

Buttons at the bottom: Default, Refresh, Confirm.

Step 2 Configure the parameters.

Table 5-18 Date & time parameters

Parameter	Description
Date Format	Select the date format. Three formats are available: YYYY-MM-DD , MM-DD-YYYY and DD-MM-YYYY .
Time Format	Select the time format. Two formats are available: 24-Hour and 12-Hour .
Current Time	The current time of the Device.
Sync PC	Configure the time of the Device as the time of PC. Click Sync PC , and settings will immediately take effect.
DST	Select the DST (means daylight saving time) check box, set the DST Type by Date or by Week , and then configure the Start Time and End Time of DST.

Parameter	Description
NTP Setting	Select the check box to enable NTP (network time protocol) time synchronization.
NTP Server	The IP address and the port number of NTP server.
Port	Required when NTP Setting is selected.
Time Zone	The time zone where the Device locates.
Interval	The time synchronization interval of the Device and the NTP.

Step 3 Click **Confirm**.

5.4.11.2 Account Management

You can add or delete users and user groups, assign permissions to new users and user groups, modify password, and manage users and user groups.

5.4.11.2.1 Account

Management Rules

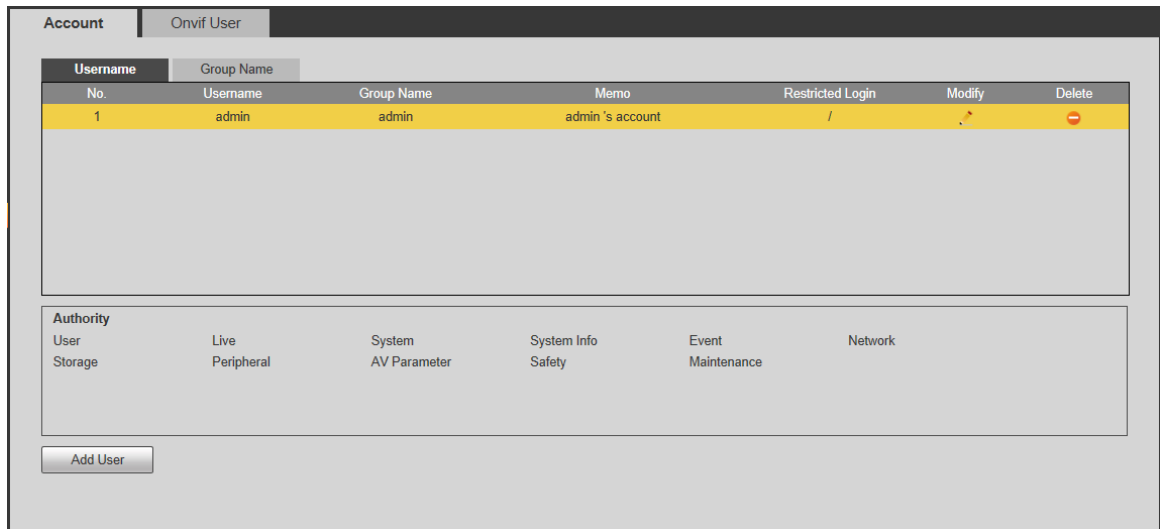
- The system manages both users and user groups. You can set up to 8 user groups and 18 users. The factory settings cover two groups: User and admin.
- Group name cannot be repeated, so is the user name. Each user must belong to a group, and can only belong to one group. You can add or delete user group(s).
- The user name can be 31 characters at most, consisting of letters, numbers, "_", "@" and ".".
- The name of user group can be 15 characters at most, and contains characters from at least two of the following categories: Letters, numbers, underlines, and hyphens.
- The default user name and password are both admin. There is one admin user by default which has highest authority.
- It is recommended to give fewer authorities to normal users than premium users.

User Management

You can view user information, add or delete user(s), change user password, assign user permissions, restrict user login, and more.

Step 1 Select **Setup > System > Account > Account > Username**.

Figure 5-30 Account



Step 2 Add a user.

- 1) Click **Add User**.
- 2) On the **Add User** interface, configure the user information including username, password, group name, memo, and operation permissions (see Figure 5-31).
- 3) Set login restrictions (if necessary), and then the restricted IP address will be unable to log in to the Device during the restricted period. See Figure 5-32.
- 4) Click **Save**.

Figure 5-31 Add user

Add User

Username **Must**

Password

The minimum pass phrase length is 8 characters

Confirm Password

Group Name

Memo

Operation Permission **Restricted Login**

- All
- User
- Live
- System
- System Info
- Event
- Network
- Storage
- Peripheral
- AV Parameter
- Safety
- Maintenance

Figure 5-32 Set log restriction

You can also:



- Delete a user: Click  to delete the corresponding user.
- Modify user information: Click  corresponding to the user. You can modify the information such as username, password, email address, group name, and memo. Click **Save** to save the settings.

Figure 5-33 Modify user

- **Modify password:** On the **Modify User** interface, select the **Modify Password** check box. Enter the old and new passwords, and confirm password. Click **Save** after configuration. Configure the password according to the password strength prompt. The new password must be 8–32 characters and contain at least two types from numbers, upper case letters, lower case letters and special characters (excluding ' " ; : &).



Password strength prompts will be made according to the points obtained from password length, letters, numbers, characters, and combination. See the table below.

Table 5-19 Password strength evaluation

Item	Evaluation
Length	<ul style="list-style-type: none"> • 5 points: Not more than 4 characters. • 10 points: 5–7 characters. • 25 points: 8 characters or more.
Letter	<ul style="list-style-type: none"> • 0: No letter. • 10 points: Only upper or lower case letters. • 20 points: A combination of upper and lower case letters.
Number	<ul style="list-style-type: none"> • 0: No number. • 10 points: 1 number. • 20 points: 3 numbers or more.
Special character	<ul style="list-style-type: none"> • 0: No special character. • 10 points: 1 special character. • 25 points: More than 1 special character.

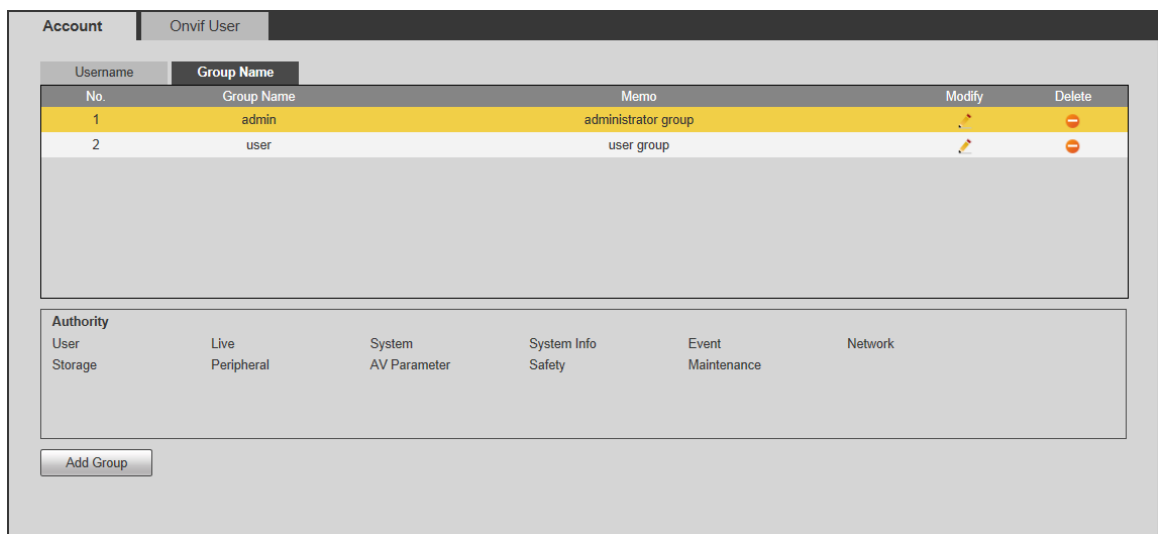
Item	Evaluation
Combination	Categories: Upper case letters, lower case letters, numbers and special characters. <ul style="list-style-type: none"> • 2 points: A combination of two categories. • 3 points: A combination of three categories. • 5 points: A combination of four categories.
Strength	<ul style="list-style-type: none"> • ≥ 70 points: Strong. • ≥ 50 points: Medium. • ≥ 0 points: Weak.

User Group Management

You can view user group information, add or delete user group(s), and modify user group password.

Step 1 Select **Setup > System > Account > Account > Group Name**.

Figure 5-34 User group



Step 2 Manage groups.

- Add a group: Click **Add Group**, and then configure the **Group Name** and **Authority** of the group. Click **Save** after configuration.

Figure 5-35 Add group

- Delete a group: Click to delete the corresponding group.


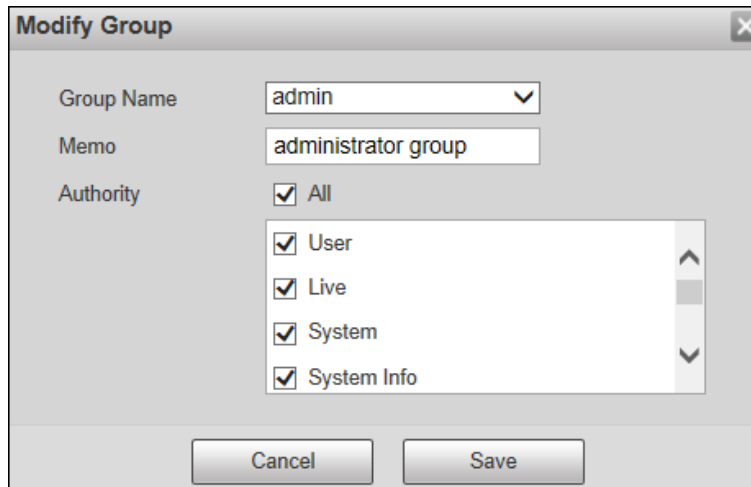
- Modify group information: Click  corresponding to the group, and then you can modify the memo and authority of the group. Click **Save** after configuration.

Figure 5-36 Modify group




- The admin and user groups cannot be deleted.
- A group cannot be deleted if the group has user(s).

5.4.11.2.2 ONVIF User

ONVIF user can be separately managed with account users and user groups.

Management Rules

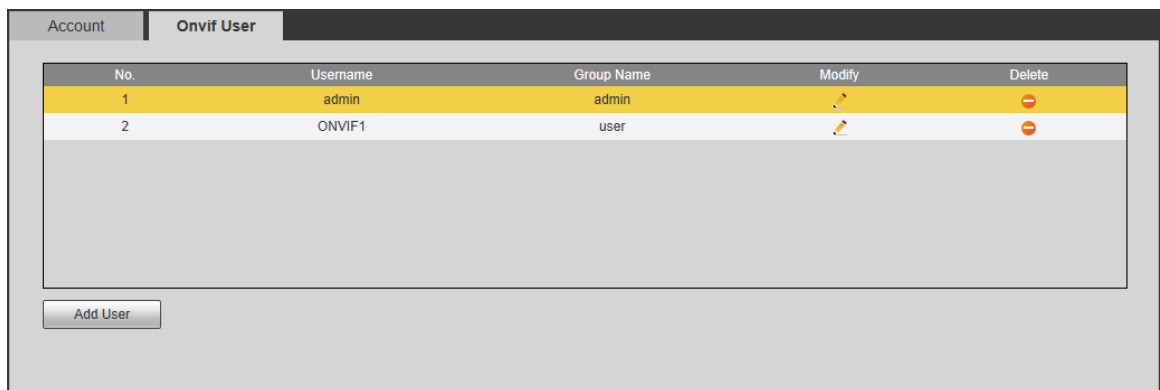
- The system manages both ONVIF users and user groups. The factory settings cover one group: admin. You can set up to 18 ONVIF users.
- ONVIF user name cannot be repeated. Each ONVIF user must belong to a group, and can only belong to one group. The user name can be 31 characters at most, consisting of letters, numbers, "_", "@", and "!".
- The default ONVIF user name and password are both admin. There is one admin by default which has highest authority.

ONVIF User Management

You can view ONVIF user information, add or delete user(s), and modify user password.

Step 1 Select **Setup > System > Account > Onvif User**.

Figure 5-37 Onvif user



Step 2 Manage ONVIF users.

- Add ONVIF user: Click **Add User**, and then you can configure user information such as username, password, and group name. Click **Save** after configuration.

Figure 5-38 Add User

- Modify user information: Click corresponding to the user, and then you can modify the information such as username, password, and group name. Click **Save** after configuration.

Figure 5-39 Modify user

- Modify password: On the **Modify User** interface, select the **Modify Password** check box. Enter the old and new passwords, and confirm password. Click **Save** after configuration. Configure the password according to the password strength prompt. The new password must be 8–32 characters and contain at least two types from numbers, upper case letters, lower case letters and special characters (excluding ' ' ; : &).



For password strength evaluation, see Table 5-19.

5.4.11.3 Safety

5.4.11.3.1 System Service

You can enable multiple system services to secure network safety.

Step 1 Select **Setup > System > Safety > System Service**.

Figure 5-40 System service

Step 2 Enable the service(s). For details, see the table below.

Table 5-20 System service

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. It is a method for secure remote login, providing secure access for users.
Multicast/Broadcast Search	Multicast identifies logical groups of computers group members. This allows a single message to be sent to the group. Broadcast allows all devices on the same network segment will see the same message.
Password Reset	Enable it so you can reset the password.
CGI Service	Select the Enable check box to enable Common Gateway Interface (CGI) service.
Onvif Service	Select the Enable check box to enable Open Network Video Interface Forum (ONVIF) service.
Audio and Video Transmission Encryption	Select the Enable check box to enable encryption during audio and video transmission. Make sure that the matched device or software supports video decryption function; otherwise, do not enable it.

Parameter	Description
RTSP over TLS	Select the Enable check box to enable RTSP over TLS service.
Private Protocol Authentication Mode	Keep the recommended Security Mode .

Step 3 Click **Confirm**.

5.4.11.3.2 HTTPS

On the **HTTPS** interface, you can create certificate or install signed certificate, so that you can log in to the web page by HTTPS. This helps ensure the security of data and the Device.

Creating Certificate

Step 1 Select **Setup > System > Safety > HTTPS**.

Figure 5-41 HTTPS

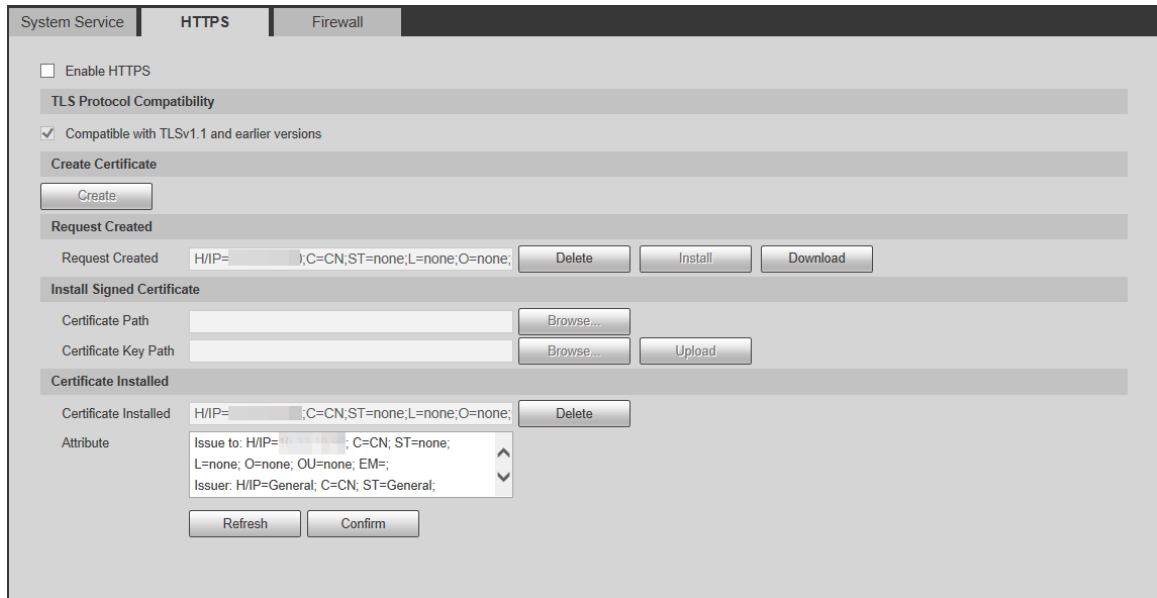
Step 2 Click **Create**.

Figure 5-42 HTTPS setting

Step 3 Configure the region, and IP address or domain name of the Device, and then click **Create**.

- Step 4** The system prompts **Operation succeeded!** when it is done successfully.
- Step 5** Click **Install** to install the certificate.
- Step 6** The system prompts **Operation succeeded!** after installation, and the information of the HTTPS certificate will be displayed in **Attribute**.

Figure 5-43 Certificate installation



The screenshot shows a web management interface with tabs for System Service, HTTPS, and Firewall. The HTTPS tab is active. It contains several sections:

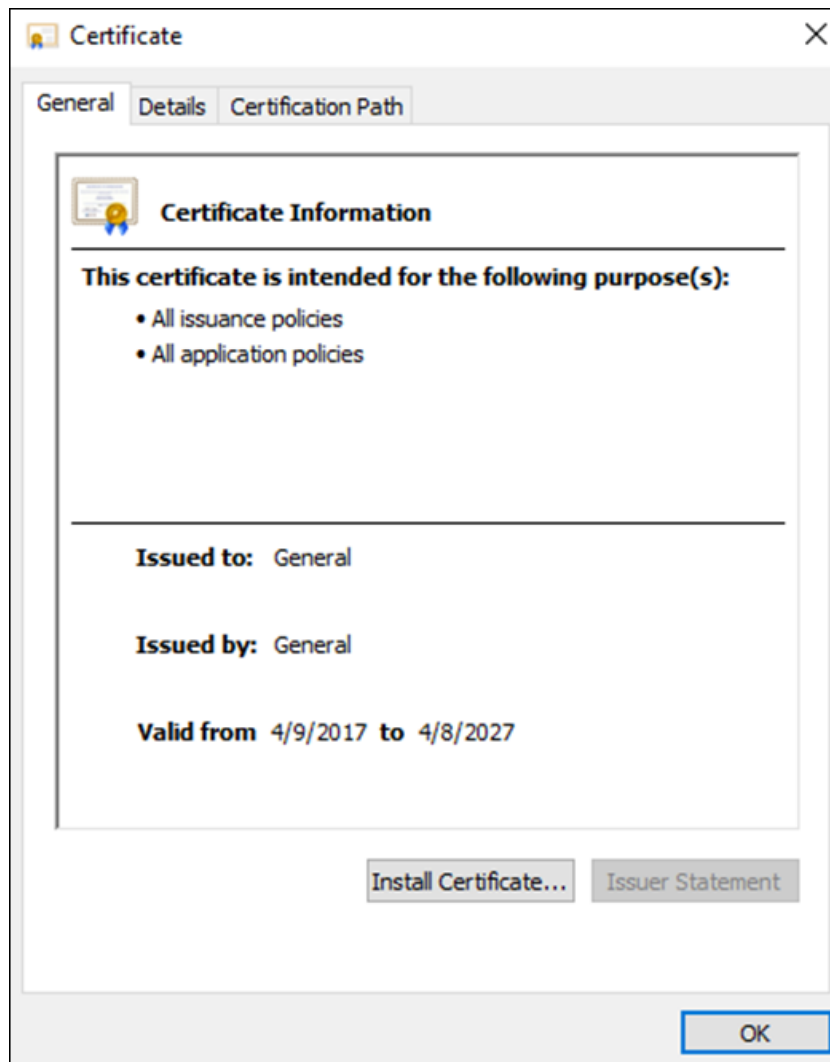
- Enable HTTPS:** A checkbox that is currently unchecked.
- TLS Protocol Compatibility:** A section with a checked checkbox for "Compatible with TLSv1.1 and earlier versions".
- Create Certificate:** A section with a "Create" button.
- Request Created:** A section showing a list of certificate requests. One request is visible with fields for "Request Created" (containing a domain name), "C=CN; ST=none; L=none; O=none;", and buttons for "Delete", "Install", and "Download".
- Install Signed Certificate:** A section with fields for "Certificate Path" and "Certificate Key Path", each with a "Browse..." button, and an "Upload" button.
- Certificate Installed:** A section showing a list of installed certificates. One certificate is visible with fields for "Certificate Installed" (containing a domain name), "C=CN; ST=none; L=none; O=none;", and a "Delete" button. Below this is an "Attribute" field with a dropdown menu showing details like "Issue to: H/IP=...; C=CN; ST=none; L=none; O=none; OU=none; EM=;" and "Issuer: H/IP=General; C=CN; ST=General;". There are "Refresh" and "Confirm" buttons at the bottom of this section.

- Step 7** Click **Download**, and then select the path to save the certificate.
- Step 8** Import the certificate to the browser.



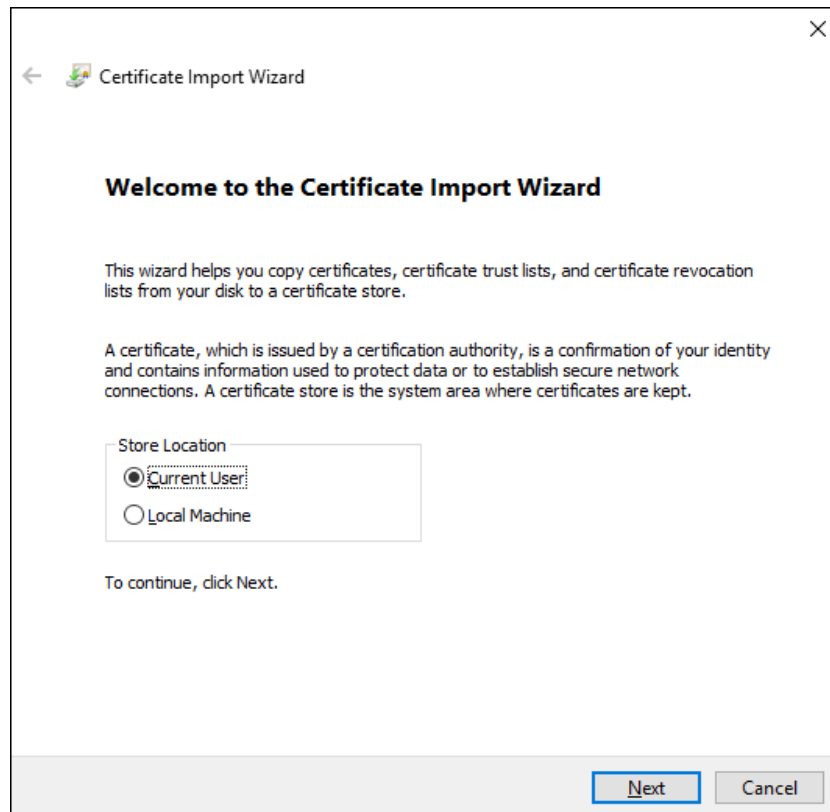
- The following steps take Internet Explorer as the example.
 - Different browsers support different ways of importing the certificate, and the actual browser shall prevail.
- 1) Go to the save path of the certificate, and then double-click the certificate.

Figure 5-44 Certificate



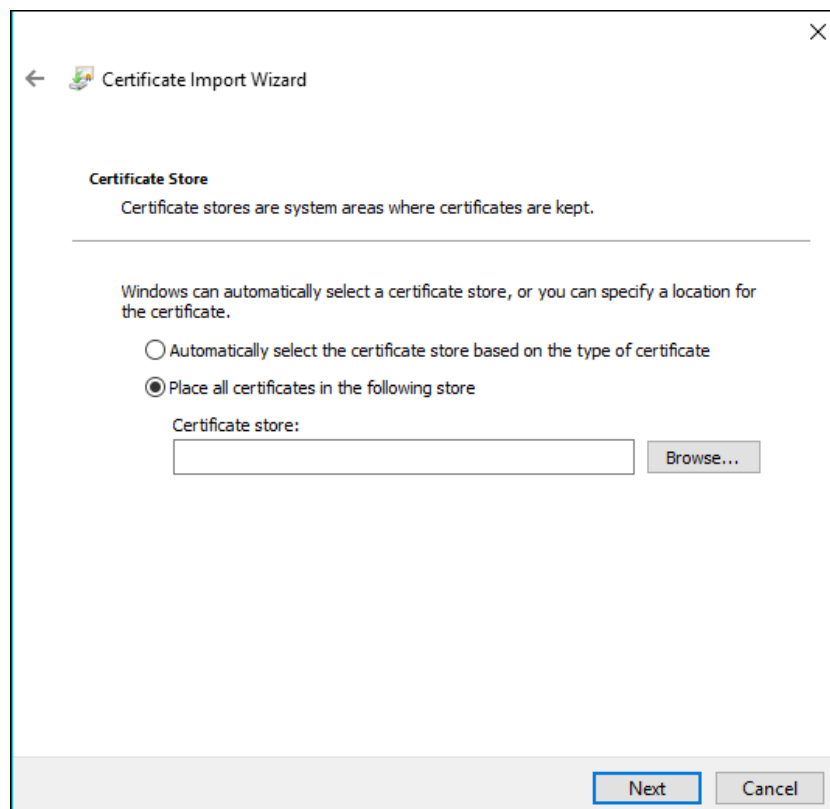
- 2) Click **Install Certificate...**, and then click **OK**.

Figure 5-45 Certificate import wizard



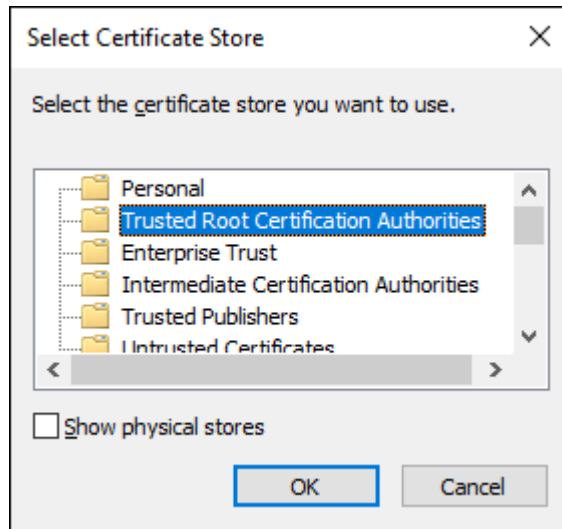
- 3) Click **Next**.

Figure 5-46 Certificate store



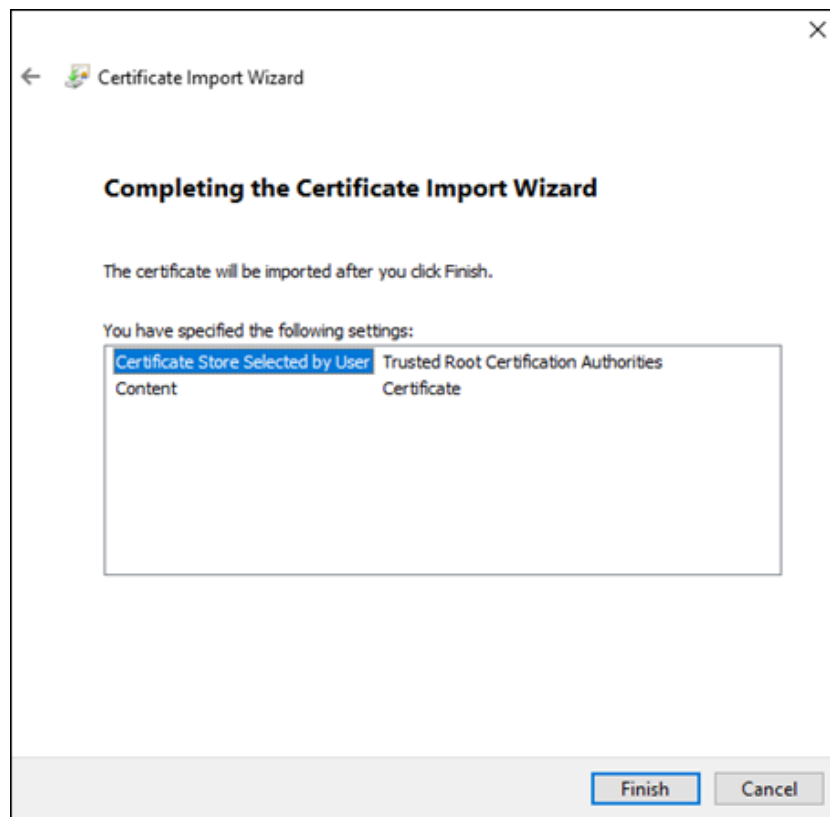
- 4) Click **Next**.

Figure 5-47 Select certificate store



- 5) Select **Trusted Root Certification Authorities**, and then click **OK**.

Figure 5-48 Completing the certificate import wizard



- 6) Click **Finish**, and then it prompts that **The import was successful**.
- 7) Click **OK**.

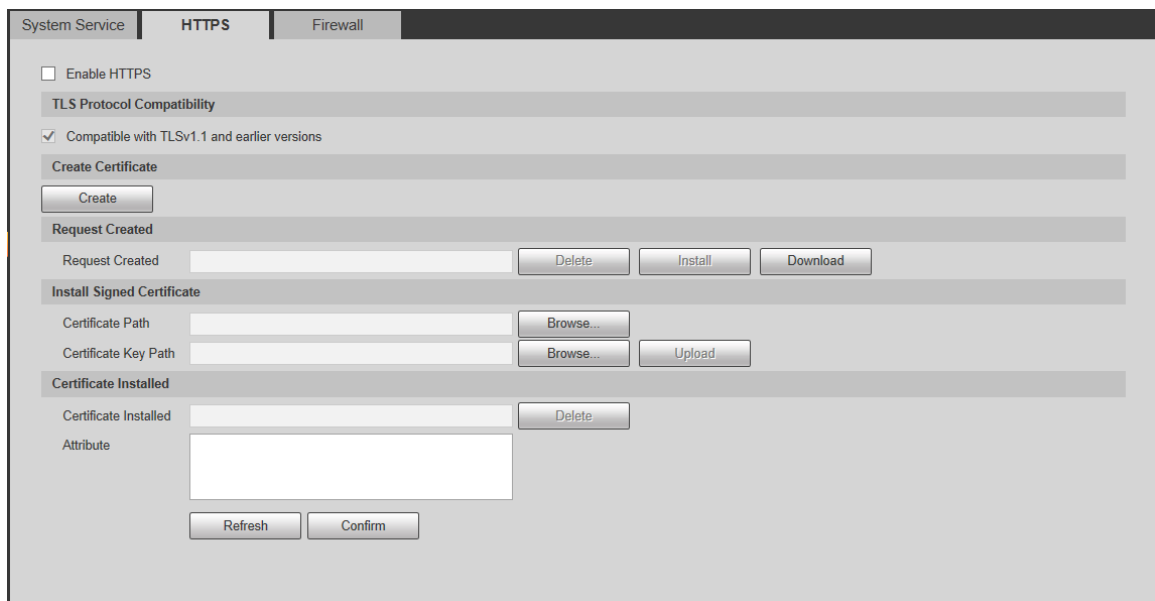
Step 9 Select the **Enable HTTPS** check box, and then click **OK**.

Step 10 The Device will restart. Wait for a few minutes, and then log in again.

Installing Signed Certificate

Step 1 Select **Setup > System > Safety > HTTPS**.

Figure 5-49 HTTPS



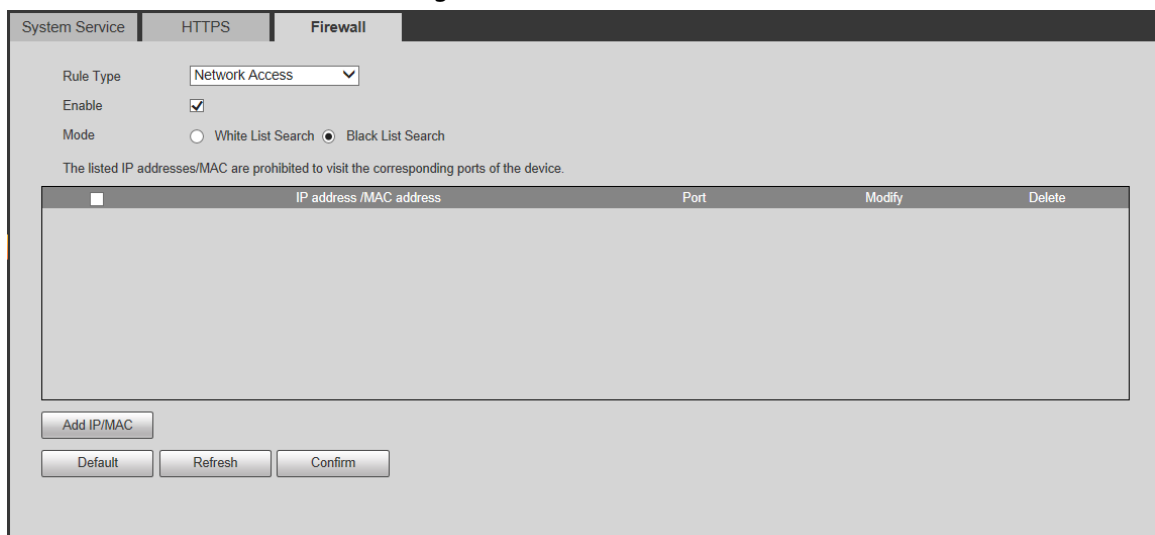
- Step 2 Click **Browse** corresponding to **Certificate Path** to select the signed certificate.
- Step 3 Click **Browse** corresponding to **Certificate Key Path** to select the private key file of certificate.
- Step 4 Install the root certificate. For details, see Step 6 of "Creating Certificate."
- Step 5 Select the **Enable HTTPS** check box, and then click **OK**.
- Step 6 Wait for a few minutes when the Device restarts, and then log in again.

5.4.11.3.3 Firewall

Set the security rules to protect the safety of your system.

- Step 1 Select **Setup > System > Safety > Firewall**.

Figure 5-50 Firewall



- Step 2 Select **Rule Type**.
 - **Network Access:** Add the IP address to allowlist or blacklist to allow or restrict it to access corresponding ports of the device.
 - **PING Prohibited:** IP address of your device is prohibited from ping. This helps prevent attempt of accessing your network system without permission.

- **Prevent Semijoin:** Prevents half-open SYN attacks.

Step 3 When **Network Access** is set to the **Rule Type**, you can select **Enable**, and then start configuring the blocklist and allowlist. Devices in the blocklist cannot access to the corresponding ports of the Device.

- 1) Select **Allowlist Search** or **Blocklist Search**, and then the devices will be added to allowlist or blocklist.
- 2) Click **Add IP/MAC**.
- 3) Add devices by **IP Address**, **IP Segment**, **MAC Address**, or **All IP addresses**.
When adding devices by IP address or IP segment, you can set the start port and end port, or all ports that will be added to allowlist or blocklist.
- 4) Click **Confirm**.

Figure 5-51 Add IP/MAC address

Step 4 Click **Confirm**.

5.4.11.4 Default

Select **Setup > System > Default**, and then you can:

- Click **Default** to restore most configurations of the Device to default settings (except information such as IP address, account, and log).
- Click **Factory Default** to restore all configurations of the Device to default settings, including IP address.

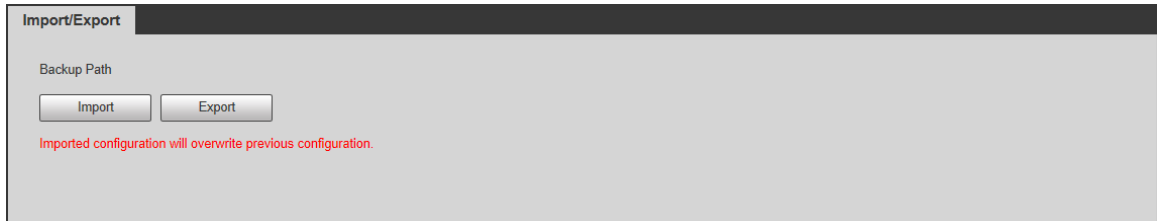
Figure 5-52 Default

5.4.11.5 Import/Export

The system supports exporting the configurations on web to local PC, and importing the configuration files from local backup.

Step 1 Select **Setup > System > Import/Export**.

Figure 5-53 Import/Export



Step 2 Click **Import** or **Export**.

- **Import:** Import the configuration files from local backup.
- **Export:** Export the configuration on the web interface to local PC.



The imported and exported files should be in the format of .backup.

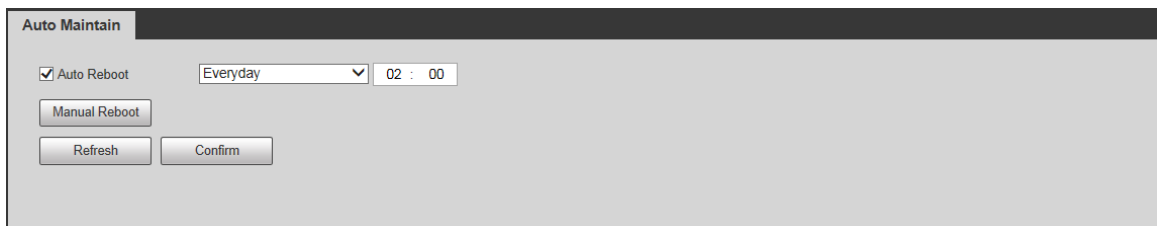
Step 3 Select the path of file to import, or the path of file to export.

5.4.11.6 Auto Maintain

You can select to either automatically restart the Device at the defined day and time, or manually restart the Device to solve problems such as stuck images.

Step 1 Select **Setup > System > Auto Maintain**.

Figure 5-54 Auto maintain



Step 2 Select the restart mode.

- **Auto Reboot:** Select the **Auto Reboot** check box, and then configure the day and time. The system will automatically restart at the defined day and time.
- **Manual Reboot:** Click it to manually restart the Device.

Step 3 Click **Confirm**.

5.4.11.7 System Upgrade

You need to update the firmware to the latest version to make the Device run properly. Import the update file in the format of .bin to the system, and then update the system.



- **Online Upgrade** function is currently not available.

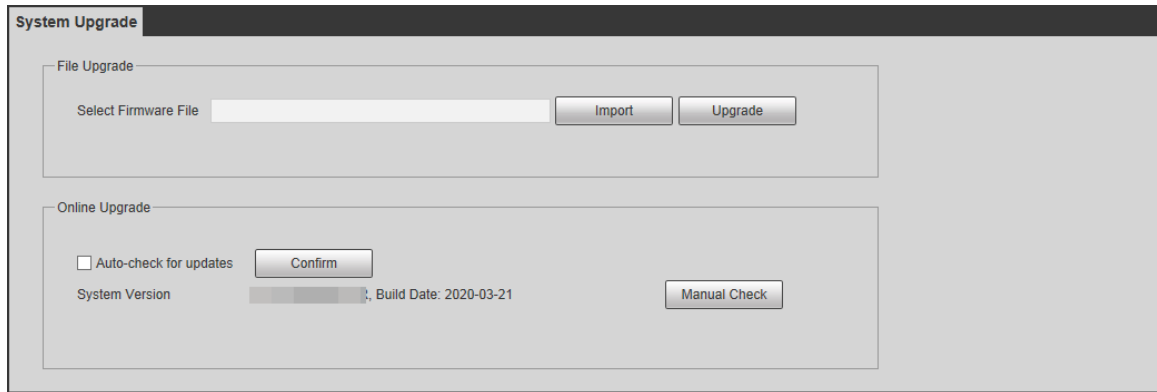
- Do not disconnect the power or network, or restart the Device during update. Incorrect update programs might result in the Device unable to work.

Step 1 Select **Setup > System > Upgrade**.

Step 2 Click **Import** to select the firmware update file (.bin).

Step 3 Click **Upgrade** to update the firmware.

Figure 5-55 Upgrade



5.4.12 System Information

You can view information such as version, log, and online user.

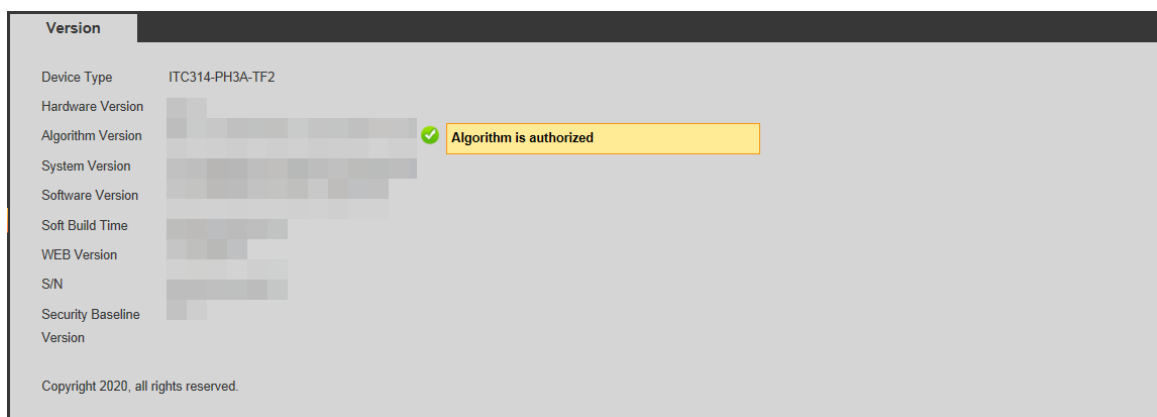
5.4.12.1 Version Information

Select **Setup > System Info > Version** to view information such as device model, version of hardware, system, and software, and more.



Versions of different devices might vary, and the actual product shall prevail.

Figure 5-56 Version



5.4.12.2 Log

5.4.12.2.1 System Log

You can search for and view logs by the time and type, and back up the logs. The log type includes **All, System, Setting, Data, Event, Record, Account, and Safety.**

Step 1 Select **Setup > System Info > Log > Log.**

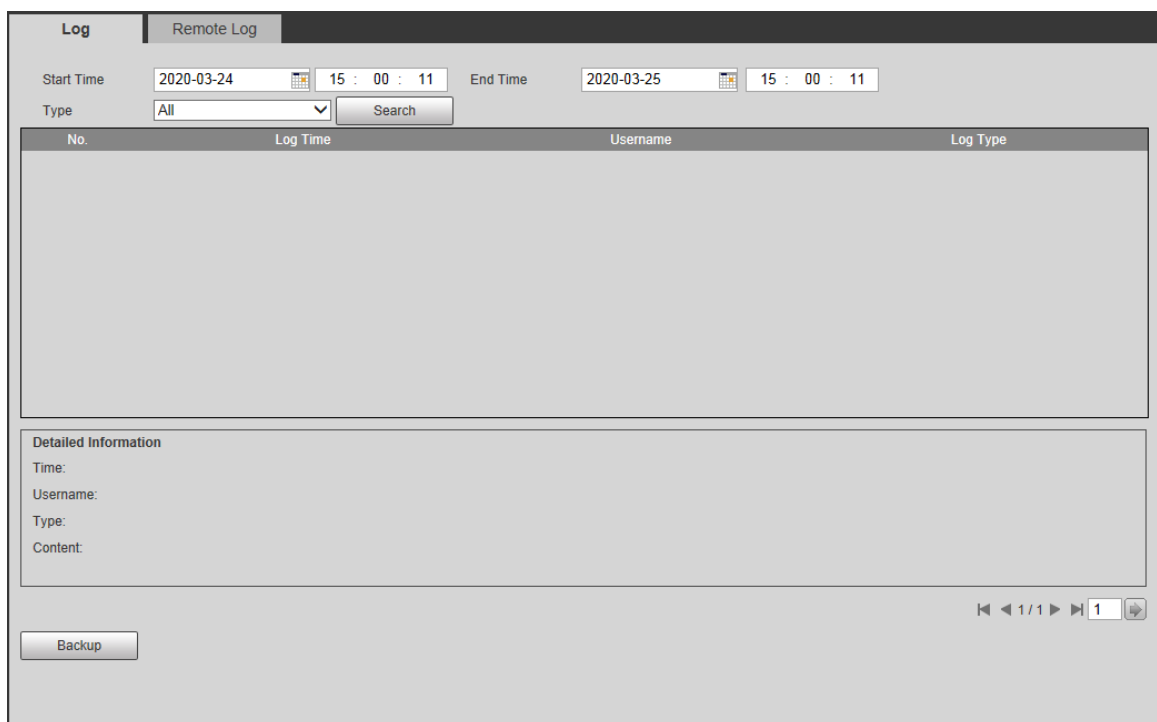
Step 2 Configure **Start Time** and **End Time**, and then select log type.

Step 3 Click **Search**. You can stop searching as needed.

Step 4 View and back up the search results.

You can save the search results to your PC in a .txt file.

Figure 5-57 Log



The screenshot displays the 'Log' management interface. At the top, there are two tabs: 'Log' and 'Remote Log'. Below the tabs, there are search filters for 'Start Time' (2020-03-24 15:00:11) and 'End Time' (2020-03-25 15:00:11). A 'Type' dropdown menu is set to 'All', and a 'Search' button is visible. Below the filters is a table with columns for 'No.', 'Log Time', 'Username', and 'Log Type'. The table is currently empty. Below the table is a 'Detailed Information' section with fields for 'Time:', 'Username:', 'Type:', and 'Content:'. At the bottom left, there is a 'Backup' button. At the bottom right, there are navigation controls including a '1' page indicator and a download icon.

5.4.12.2.2 Remote Log

Critical logs can be saved to log server. This helps provide important clues to the source of security incidents. Log server needs to be deployed in advance by a professional or system administrator.

Step 1 Select **Setup > System Info > Log > Remote Log.**

Step 2 Select **Enable** to enable **Remote Log.**

Step 3 Configure the IP address, port and device number.

Step 4 Click **Confirm.**

Figure 5-58 Remote log

5.4.12.3 Online User

Select **Setup > System Info > Online User**, and then you can view online users' information, such as username, user local group, IP address, user login time, and more.

Figure 5-59 Online user

No.	Username	User Local Group	Address	User Login Time	Login Type
2	admin	admin		2020-03-25 14:25:30	DVRIP
3	admin	admin		2020-03-25 14:25:31	RPC
4	admin	admin	1	2020-03-25 14:25:35	RPC
5	admin	admin		2020-03-25 14:25:57	DVRIP
6	admin	admin		2020-03-25 14:26:04	DVRIP
7	admin	admin		2020-03-25 14:26:08	DVRIP
8	admin	admin		2020-03-25 14:46:28	Web3.0
9	admin	admin		2020-03-25 14:46:28	DVRIP

5.5 Alarm

Select **Alarm** at the upper-right side of the web interface, and then you can select the event types that trigger an alarm, and also configure how to sound the alarm.



Different alarm types are supported in different work modes, and the actual interface shall prevail.

Figure 5-60 Alarm

Table 5-21 Alarm parameters

Name	Parameter	Description
Alarm Type	Illegal Access	Alarm is triggered when illegal access is detected.
	Security Exception	Alarm is triggered when network security problem is detected, such as session hijacking.
Operation	Listen Alarm	When there is alarm, the device will inform users on the web interface.
Alarm Tone	Play Alarm Tone	Select the Play Alarm Tone check box, and then click Choose to select the alarm tone. The system will play the defined alarm tone when alarm is triggered.
	Tone Path	

Appendix 1 FAQ

Question	Solution
Device error, unable to start or operate normally	Press and hold the Reset button for 10 seconds to restore the Device to factory settings.
Online upgrade failed	Restart the Device, and try upgrade again 2 minutes later after the power indicator is on.
The web control webrec.cab installation dialog box didn't pop up	Set the IE browser security level to Low , and enable ActiveX controls from Tools > Internet Options > Security > Custom Level .

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the 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.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. Enable Allowlist

We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. 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.

11. Audio and Video Encrypted Transmission

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

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

12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device 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.

13. 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.

14. 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 external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blocklist and allowlist feature to reduce the risk that your device might be attacked.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883