# Access ANPR Kit

## User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.1

# Foreword

## General

This manual introduces the structure, installation and configurations of access ANPR kit (hereinafter referred to as "the Kit").

## Models

DHI-IPMECS-2201C

DHI-IPMECS-2201C-IR

## 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, may 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 |
|---|---|---|
| V1.0.1 | Update the lattice screen settings. | May 2020 |
| V1.0.0 | First release. | March 2019 |

## Privacy Protection Notice

As the device user or data controller, you might collect personal data of other such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to:

providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Manual

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

# Important Safeguards and Warnings

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

## Power Requirements

⚠

- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Kit; 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 the Device (I-type 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 aim the Kit at strong light (such as lamplight, sunlight) for focusing.
- Transport, use and store the Kit under the allowed humidity and temperature conditions.
- Prevent any liquid from flowing into the Kit.
- Do not block the ventilation opening near the Kit.
- Do not press, vibrate or soak the Kit during transportation, storage and installation.
- Pack the Kit with packaging materials provided by its manufacturer or materials with the same quality before transporting it.
- Ground the Kit to improve its reliability.

## Operation and Maintenance Requirements

- Do not dissemble the Kit.
- Clean the surface of access ANPR camera with a soft dry cloth or a clean soft cloth dipped in neutral detergent, and then dry the surface.
- Use accessories suggested by the manufacturer, and install and maintain the Kit by professional personnel.
- Do not provide two or more than two kinds of power supply modes; otherwise, the Kit may be damaged.

📖

For support tools, contact the technical support.

# Table of Contents

# 1 Structure

This 2 MP access ANPR kit consists of access ANPR camera, universal joint, and the LED display.

The access ANPR camera adopts deep learning intelligent algorithm, and supports various intelligent functions including vehicle detection, LPR (license plate recognition), vehicle logo recognition, vehicle type recognition, vehicle color recognition, H.265 coding, voice broadcast, and displaying vehicle information on LED, and more.

The Kit can be widely applied in several scenarios such as parking lot and community road, and more.

## 1.1 Dimensions

Figure 1-1 Access ANPR kit dimensions (mm)

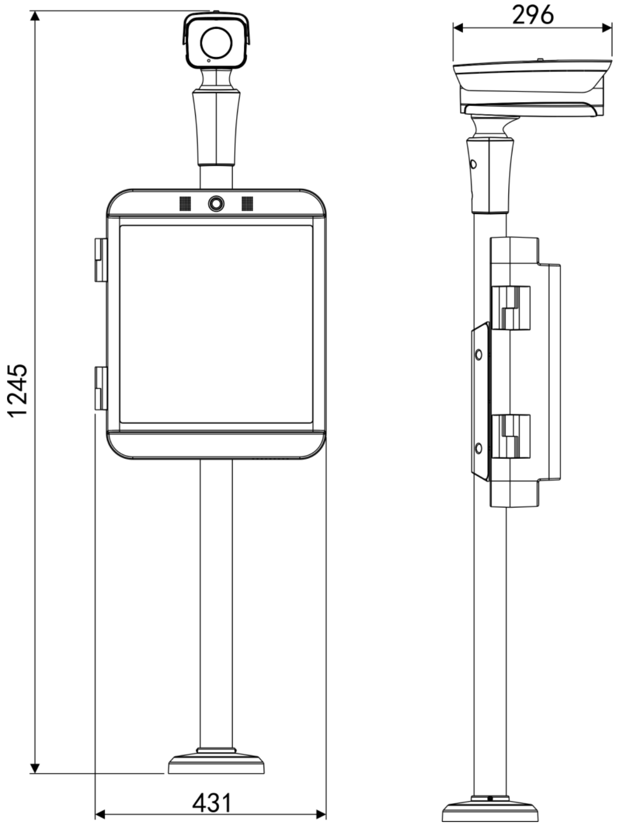
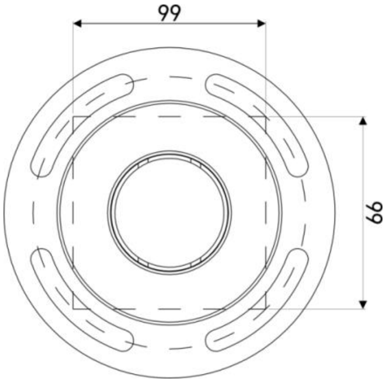


Figure 1-2 Base dimensions (mm)



## 1.2 Structure

Figure 1-3 Access ANPR kit structure

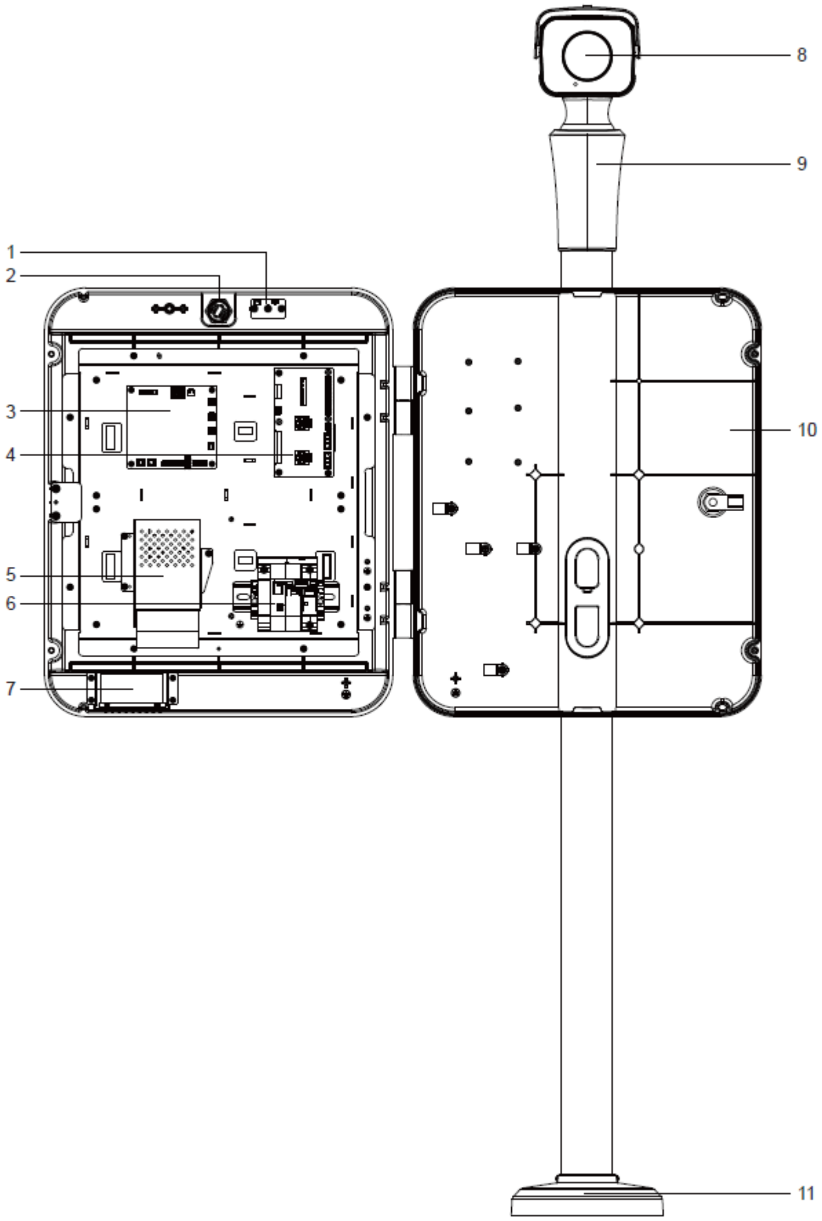


Table 1-1 Access ANPR kit structure

| No. | Description | No. | Description |
|---|---|---|---|
| 1 | Microphone | 7 | Speaker |
| 2 | Intercom button | 8 | Access ANPR camera |
| 3 | Mainboard | 9 | Universal joint |
| 4 | Wiring board | 10 | LED display |
| 5 | Power | 11 | Base |
| 6 | Earth leakage circuit breaker (ELCB) | — | — |

# 1.3 Ports

## 1.3.1 Control Panel Ports

Figure 1-4 Control panel ports

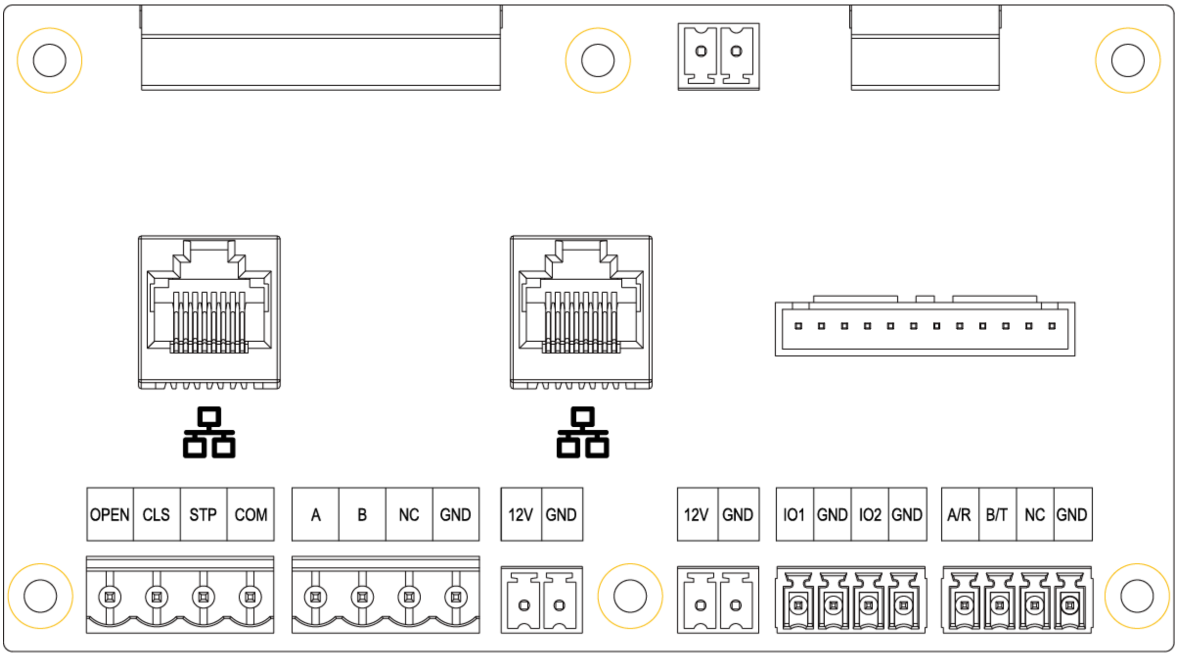


Table 1-2 Control panel port description

| Interface | | Description |
|---|---|---|
| 🖧 | Ethernet port | Connect to standard Ethernet cable. |
| OPEN, CLS, STP, COM | — | Alarm output, control the open, close or stop running of barrier. |
| A, B | RS-485 | RS-485_A and RS-485_B, connecting to the LED display. |
| NC | — | No connection. |
| GND | — | Grounding connection. |
| 12 V DC | Power port (inside the Kit) | 12 V DC power output port, supplying power for external device. |
| GND | | Ground terminal. |

| Interface | | Description |
|---|---|---|
| IO1, GND,<br>IO2, GND | I/O port | 2-channel I/O input. |
| A/R, B/T, NC, GND | RS-485\RS-232 port | Reserved function. Receive 485 or 232 signals, or connect to laser device, radar, etc. |

## 1.3.2 Earth Leakage Circuit Breaker (ELCB) Ports

Figure 1-5 ELCB ports

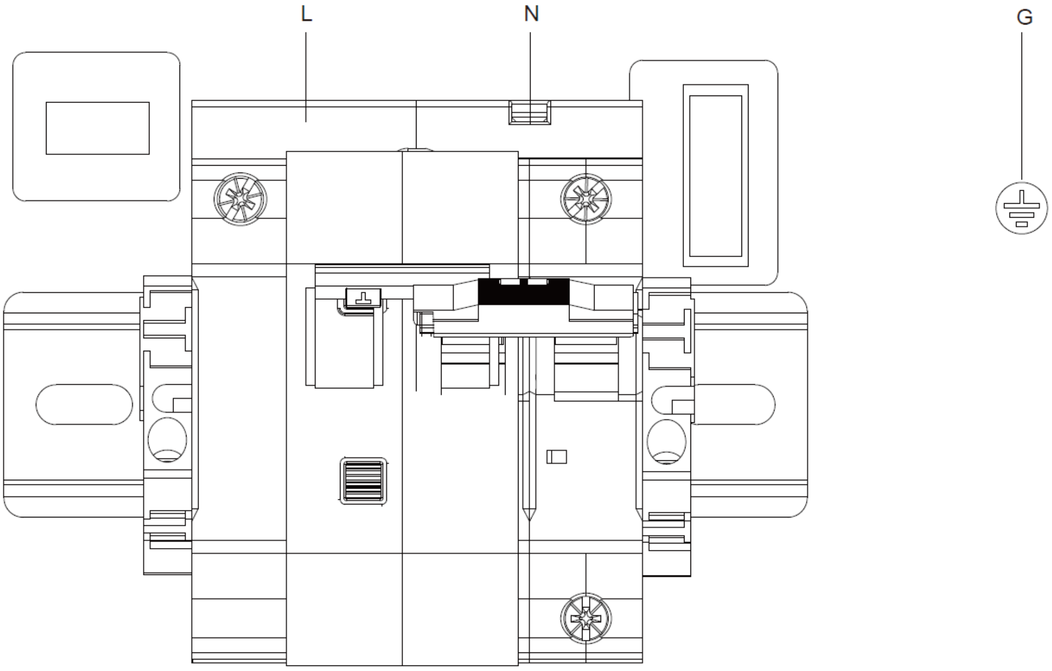


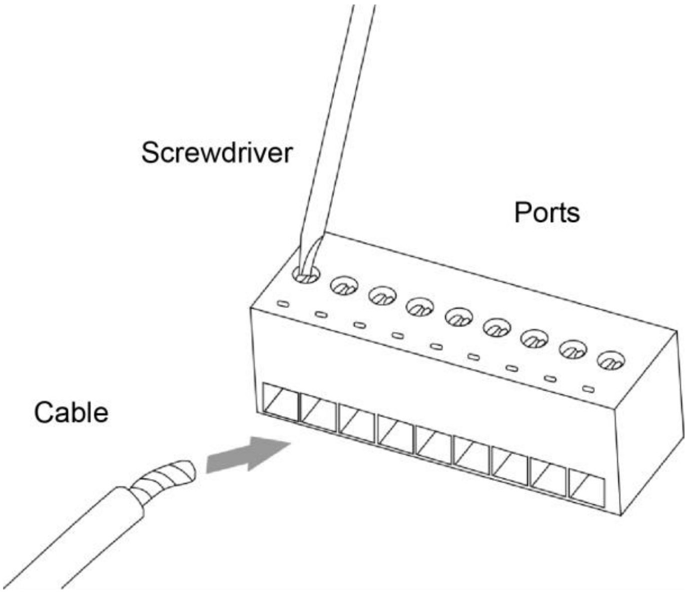
Table 1-3 ELCB port description

| Port | Description |
|---|---|
| L | Connect to 110 V – 220 V AC live wire. |
| N | Connect to 110 V – 220 V AC neutral wire. |
| G | Ground. |

# 2 Installation

## 2.1 Connecting the Cable

Figure 2-1 Connecting the cable



Step 1 Align the screwdriver with the screw in the cable slot, and turn the screwdriver counterclockwise to loosen the screw.

Step 2 Insert the cable into the corresponding slot.

Step 3 Align the screw with the slot, and then turn the screwdriver clockwise to tighten the screw.

📖

To remove the cable, align the screwdriver with the screw in the cable slot, turn the screwdriver counterclockwise to loosen the screw, and then pull the cable out of the slot.

After connecting the cable, see "1.3 Ports" to insert the cable into the corresponding port.

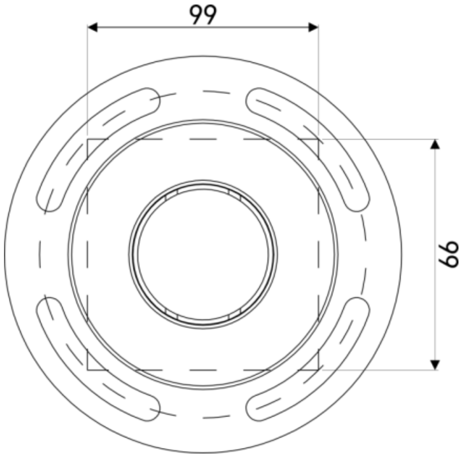
## 2.2 Installing the Kit

Step 1 Confirm the position of holes on the mounting surface.

Step 2 Use M8×80 expansion anchors to fix the base to the mounting surface.

There are four holes in the base, and every two holes are 99 mm apart.

Figure 2-2 Holes in the base (mm)



Step 3 Mount the Kit to the base, and screw the nut into the base to fix the Kit.

# 3 Basic Configuration

## 3.1 ConfigTool

- This section is only applicable to the configuration and upgrade of access ANPR camera (hereinafter referred to as "the Camera").
- This section only introduces the general operations of quick configuration tool. For details, see *ConfigTool User's Manual.*
- The figures shown in this section are for reference only, and the actual interface shall prevail.

The default IP of the Camera is 192.168.1.108. Modify the IP address according to network plan when you use the Camera for the first time or network is adjusted.

You can modify IP address individually or in batches by ConfigTool, or you can login web client of the Camera to modify IP address.

- IP address can be modified individually when there are fewer devices or login passwords of devices are different.
- When there are multiple devices and device login passwords are the same, you can modify IP addresses in batches.

### Preparation

- Acquire the ConfigTool setup package. If not, contact technical support.
- The PC which is installed with ConfigTool is interconnected with device through network.

### 3.1.1 Initializing Camera

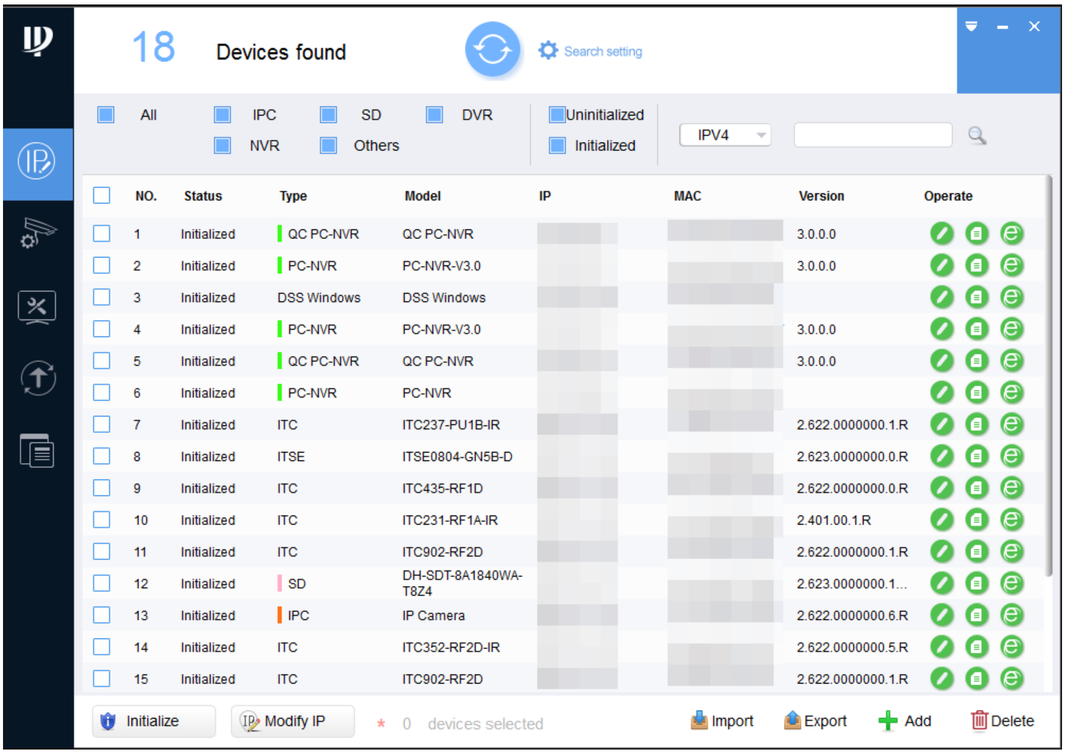
It supports initializing cameras in the same LAN individually or in batches.

No operations can be done before device is initialized. Uninitialized devices will be displayed in gray in the device list, and corresponding information of such devices will not be displayed on other interfaces of ConfigTool.

Step 1 Double-click the shortcut icon on the desktop.

Step 2 Click .

Figure 3-1 Modify IP



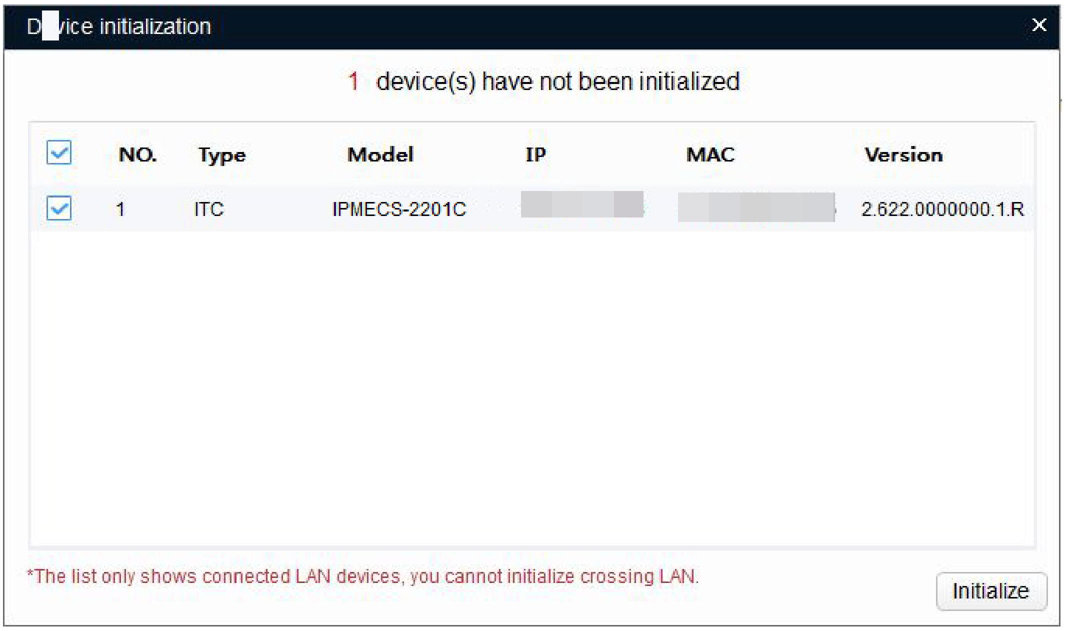
18 Devices found

□ All □ IPC □ SD □ DVR □ NVR □ Others □ Uninitialized □ Initialized IPV4

| □ | NO. | Status | Type | Model | IP | MAC | Version | Operate |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | Initialized | QC PC-NVR | QC PC-NVR | [redacted] | [redacted] | 3.0.0.0 | |
| □ | 2 | Initialized | PC-NVR | PC-NVR-V3.0 | [redacted] | [redacted] | 3.0.0.0 | |
| □ | 3 | Initialized | DSS Windows | DSS Windows | [redacted] | [redacted] | | |
| □ | 4 | Initialized | PC-NVR | PC-NVR-V3.0 | [redacted] | [redacted] | 3.0.0.0 | |
| □ | 5 | Initialized | QC PC-NVR | QC PC-NVR | [redacted] | [redacted] | 3.0.0.0 | |
| □ | 6 | Initialized | PC-NVR | PC-NVR | [redacted] | [redacted] | | |
| □ | 7 | Initialized | ITC | ITC237-PU1B-IR | [redacted] | [redacted] | 2.622.0000000.1.R | |
| □ | 8 | Initialized | ITSE | ITSE0804-GN5B-D | [redacted] | [redacted] | 2.623.0000000.0.R | |
| □ | 9 | Initialized | ITC | ITC435-RF1D | [redacted] | [redacted] | 2.622.0000000.0.R | |
| □ | 10 | Initialized | ITC | ITC231-RF1A-IR | [redacted] | [redacted] | 2.401.00.1.R | |
| □ | 11 | Initialized | ITC | ITC902-RF2D | [redacted] | [redacted] | 2.622.0000000.1.R | |
| □ | 12 | Initialized | SD | DH-SDT-8A1840WA-T8Z4 | [redacted] | [redacted] | 2.623.0000000.1... | |
| □ | 13 | Initialized | IPC | IP Camera | [redacted] | [redacted] | 2.622.0000000.6.R | |
| □ | 14 | Initialized | ITC | ITC352-RF2D-IR | [redacted] | [redacted] | 2.622.0000000.5.R | |
| □ | 15 | Initialized | ITC | ITC902-RF2D | [redacted] | [redacted] | 2.622.0000000.1.R | |

Step 3 Select the uninitialized device. Click Initialize.

Figure 3-2 Device initialization (1)



D vice initialization

1 device(s) have not been initialized

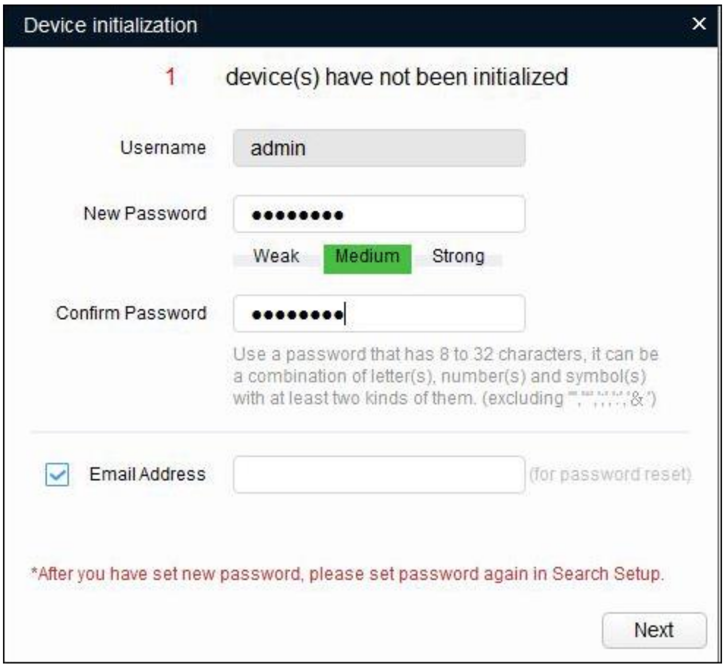
| ☑ | NO. | Type | Model | IP | MAC | Version |
|---|---|---|---|---|---|---|
| ☑ | 1 | ITC | IPMECS-2201C | [redacted] | [redacted] | 2.622.0000000.1.R |

*The list only shows connected LAN devices, you cannot initialize crossing LAN.

Step 4 Select the device which needs to be initialized. Click **Initialize**.

- The interface might be different depending on the model you purchased, and the actual product shall prevail.
- The initialization interface of the first selected device will be displayed during initialization in batches.

Figure 3-3 Device initialization (2)



Device initialization ×

1 device(s) have not been initialized

Username: admin

New Password: ●●●●●●●●●

Weak | Medium | Strong

Confirm 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. (excluding ''',''',';',':','&')

☑ Email Address: (for password reset)

*After you have set new password, please set password again in Search Setup.

Step 5 Configure the parameters.

Table 3-1 Parameter description

| Parameter | Description |
|---|---|
| User Name | The user name is admin by default. |
| New Password | ● The new password can be set from 8 characters to 32 characters and contains at least two categories from upper cases, lower cases, numbers and special characters (excluding “'”, “"”, “;”, “:” and “&”)<br>● Follow the password strength prompt to set a high security level password.<br>● The new password should be in accordance with the confirm password. |
| Confirm Password | |
| Email | **It is selected by default, the Email will be used for** password retrieval and reset**.** |

Step 6 Click **Initialize** and the system begins to initialize device.

If initialization succeeded, ✓ will be displayed. If initialization failed, ⚠ will be displayed. Click the icon to check more details.

Step 7 Click **Complete**, and then device initialization is finished.

After initialization is completed, the device status becomes **Initialized** on the main interface, and the device information will be displayed on other interfaces.

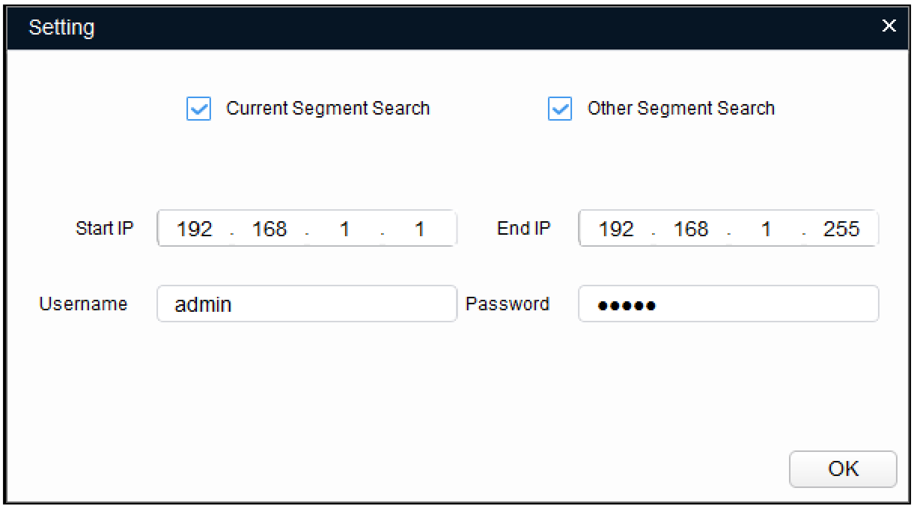
## 3.1.2 Modifying IP Address

### 3.1.2.1 Modifying One IP Address

Step 1 Click IP.

Step 2 Click **Search setting**.

Figure 3-4 Setting



Setting

☑ Current Segment Search ☑ Other Segment Search

Start IP 192 . 168 . 1 . 1 End IP 192 . 168 . 1 . 255

Username admin Password •••••

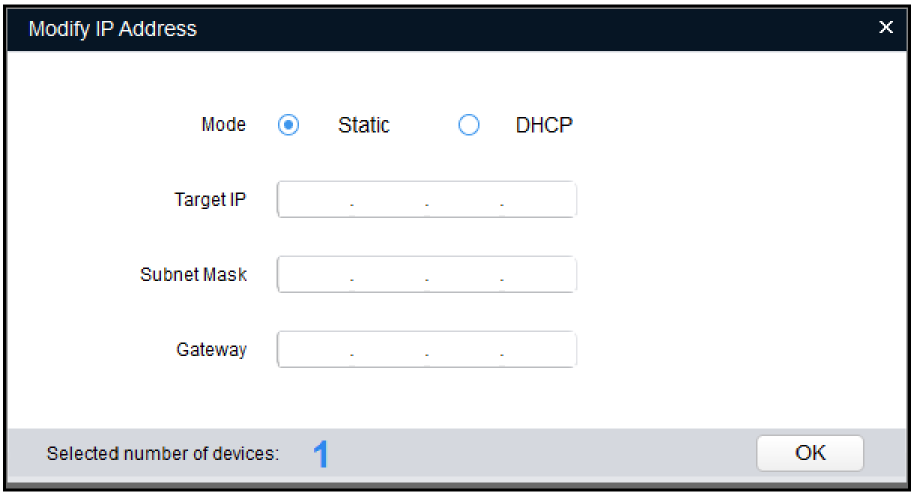
Step 3 Configure device segment, enter login user name and password. Click **OK**.

The devices searched will be displayed after searching is completed.

Uninitialized devices can be used after initialization.

Step 4 Click the corresponding ✎ of the device whose IP address needs to be modified.

Figure 3-5 Modify IP address



Modify IP Address

Mode ● Static ○ DHCP

Target IP . . .

Subnet Mask . . .

Gateway . . .

Selected number of devices: 1

Step 5 Select the mode of configuring IP address according to the actual situation.

- DHCP (Dynamic Host Configuration Protocol) mode: When there is DHCP server in the network, set **Mode** to **DHCP**, and then the device can automatically acquire IP address from DHCP server.

- Manual mode: Set **Mode** as **Static**, and fill in **Target IP**, **Subnet Mask** and **Gateway**, and then the device can automatically acquire IP address from DHCP server.

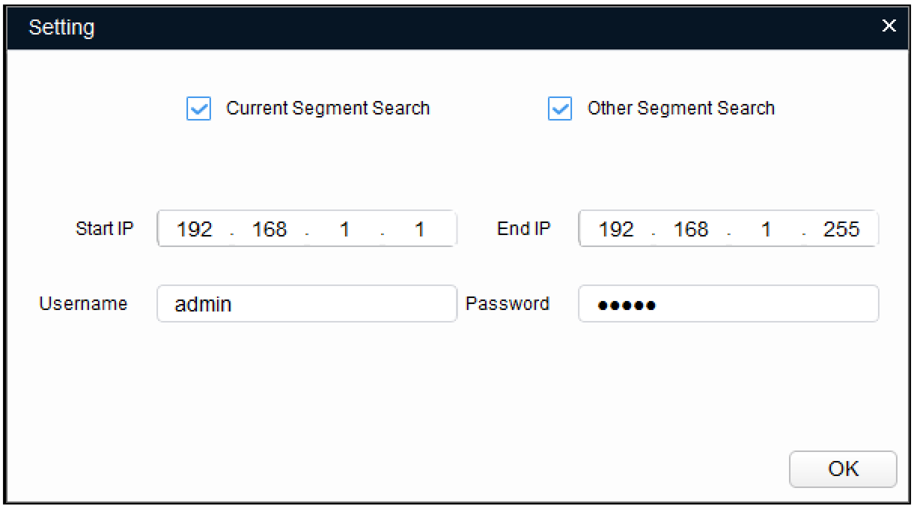
Step 6 Click **OK**.

### 3.1.2.2 Batch Modifying

Step 1 Click IP.

Step 2 Click **Search setting**.

Figure 3-6 Setting



Setting ✕

☑ Current Segment Search ☑ Other Segment Search

Start IP 192 . 168 . 1 . 1 End IP 192 . 168 . 1 . 255

Username admin Password ●●●●●

OK

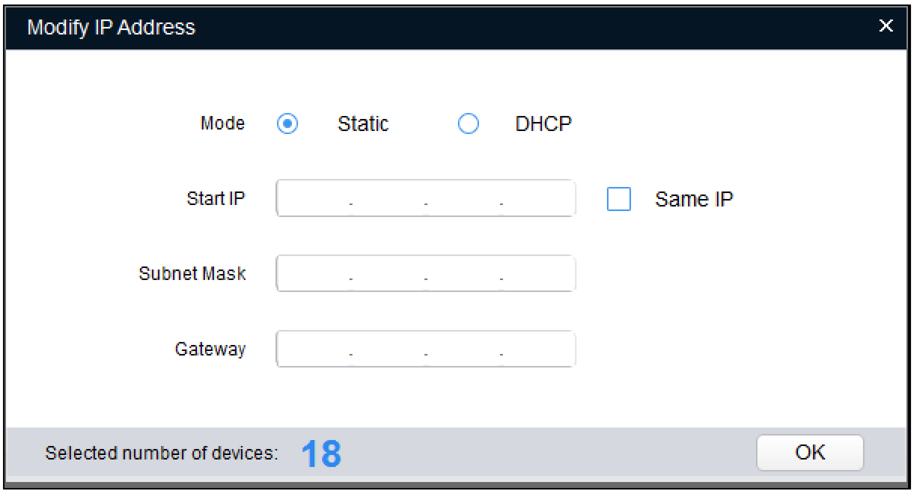
Step 3 Configure device segment, enter user name and password. Click **OK**.

The devices searched will be displayed after searching is completed.

Uninitialized devices can be used after initialization.

Step 4 Select devices whose IP address need to be modified, click Modify IP.

Figure 3-7 Modify IP address



Modify IP Address ✕

Mode ● Static ○ DHCP

Start IP . . . □ Same IP

Subnet Mask . . .

Gateway . . .

Selected number of devices: 18 OK

Step 5 Select the mode of configuring IP address according to the actual situation.

- DHCP (Dynamic Host Configuration Protocol) mode: When there is DHCP server in the network, set **Mode** as **DHCP**, and then the device can automatically acquire IP address from DHCP server.
- Manual mode: Set **Mode** as **Static**, and enter **Start IP**, **Subnet Mask** and **Gateway**, and then the device IP addresses will be modified successively from start IP.

Select **Same IP**, and the selected device will be set as the same IP address.

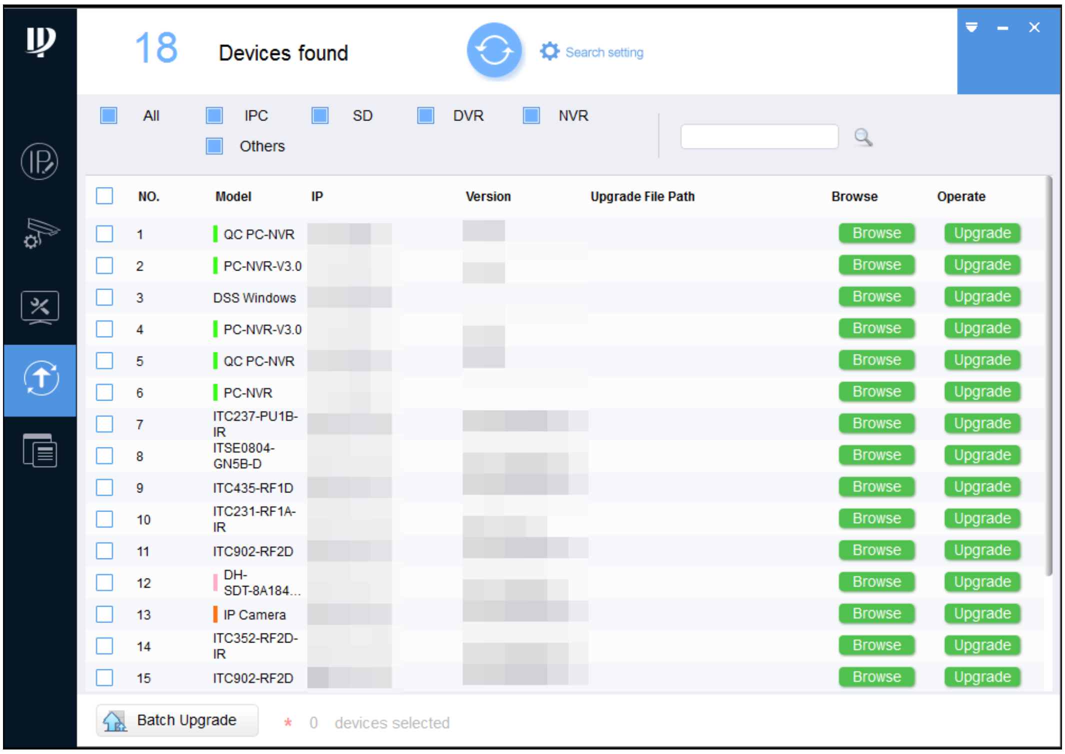
Step 6 Click **OK**.

### 3.1.3 Upgrading Device

Device upgrade supports upgrading one device and batch upgrading.

Step 1 Click .

Figure 3-8 Upgrade



18 Devices found

■ All ■ IPC ■ SD ■ DVR ■ NVR ■ Others

| □ | NO. | Model | IP | Version | Upgrade File Path | Browse | Operate |
|---|---|---|---|---|---|---|---|
| □ | 1 | QC PC-NVR | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 2 | PC-NVR-V3.0 | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 3 | DSS Windows | [redacted] |  |  | Browse | Upgrade |
| □ | 4 | PC-NVR-V3.0 | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 5 | QC PC-NVR | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 6 | PC-NVR | [redacted] |  |  | Browse | Upgrade |
| □ | 7 | ITC237-PU1B-IR | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 8 | ITSE0804-GN5B-D | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 9 | ITC435-RF1D | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 10 | ITC231-RF1A-IR | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 11 | ITC902-RF2D | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 12 | DH-SDT-8A184... | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 13 | IP Camera | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 14 | ITC352-RF2D-IR | [redacted] | [redacted] |  | Browse | Upgrade |
| □ | 15 | ITC902-RF2D | [redacted] | [redacted] |  | Browse | Upgrade |

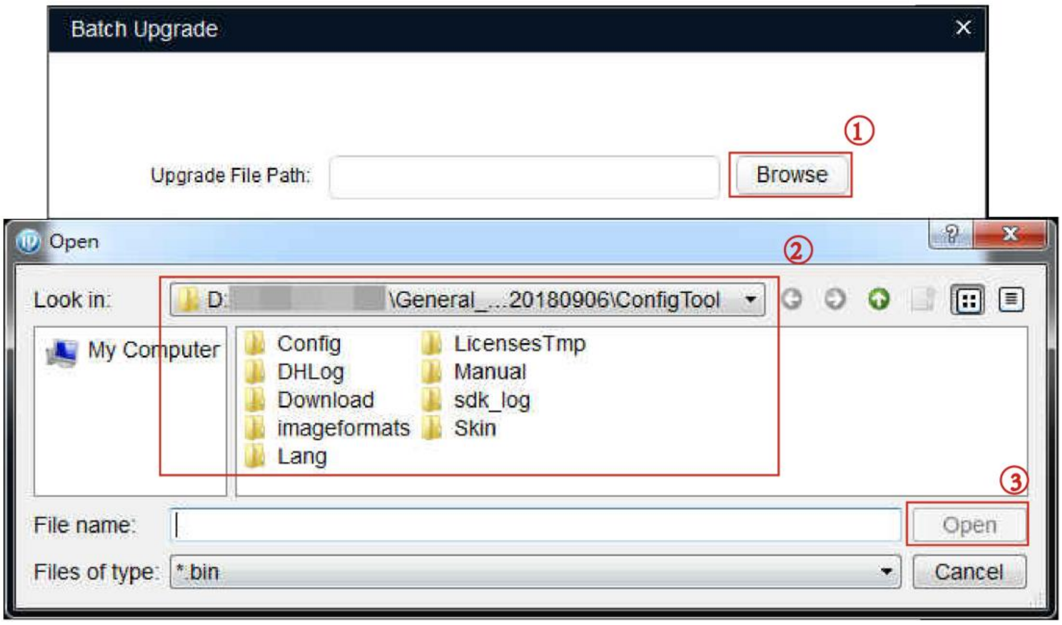
Batch Upgrade * 0 devices selected

Step 2 Select the device that you want to upgrade.

- Upgrade one device: Click **Browse** corresponding to the device to be upgraded.
- Batch upgrade: Select the devices to upgrade, and the click **Batch Upgrade**.

Step 3 Select upgrade file.

Figure 3-9 Select upgrade file



Look in: D:[redacted]\General_...20180906\ConfigTool

Files of type: *.bin

Step 4 Upgrade the device.

- Upgrade one device: Click **Upgrade**, and the system starts upgrading. You can see the upgrade progress.
- Batch upgrade: Click **OK**, and the system starts upgrading.

If the device is disconnected during upgrading, as long as the ConfigTool stays on the upgrade interface, the upgrade will resume when the connection is restored.

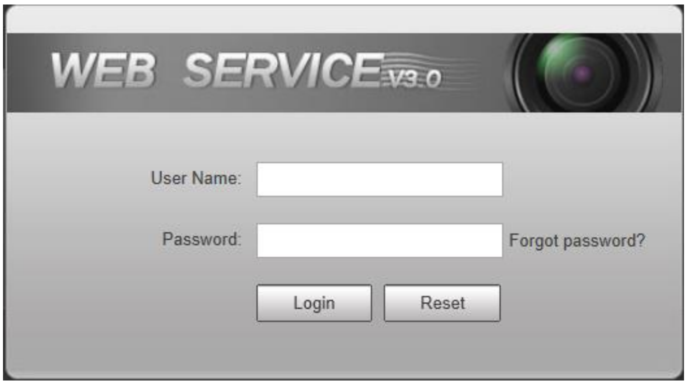
## 3.2 Logging in to Web

You can directly log in to the web interface if initialization is completed. This section is only applicable to the Camera.

Step 1 Open the browser, enter IP address of the Camera in the browser address bar, and then press Enter.

After it is successfully connected, the **Login** interface is displayed.

Figure 3-10 Logging in to web



Step 2 Enter **Username** and **Password**, and then click **Login**.

The main web interface is displayed.

# 4 Web Configuration

- Make sure the Camera is properly installed and powered up.
- For detailed configuration, see user’s manuals of corresponding Camera.
- The figures shown in this section are for reference only, and the actual interface shall prevail.

## 4.1 Initializing Camera

- For first-time login or login after restoring to factory default settings, you need to initialize the Camera.
- Make sure that both PC IP and IP of the Camera are in the same network segment, otherwise it might fail to enter initialization interface.

Step 1 Configure IP address, subnet mask and gateway of PC and the Camera respectively.

- Distribute IP address of the same segment if there is no router in the network.
- It needs to configure corresponding gateway and subnet mask if there is router in the network.

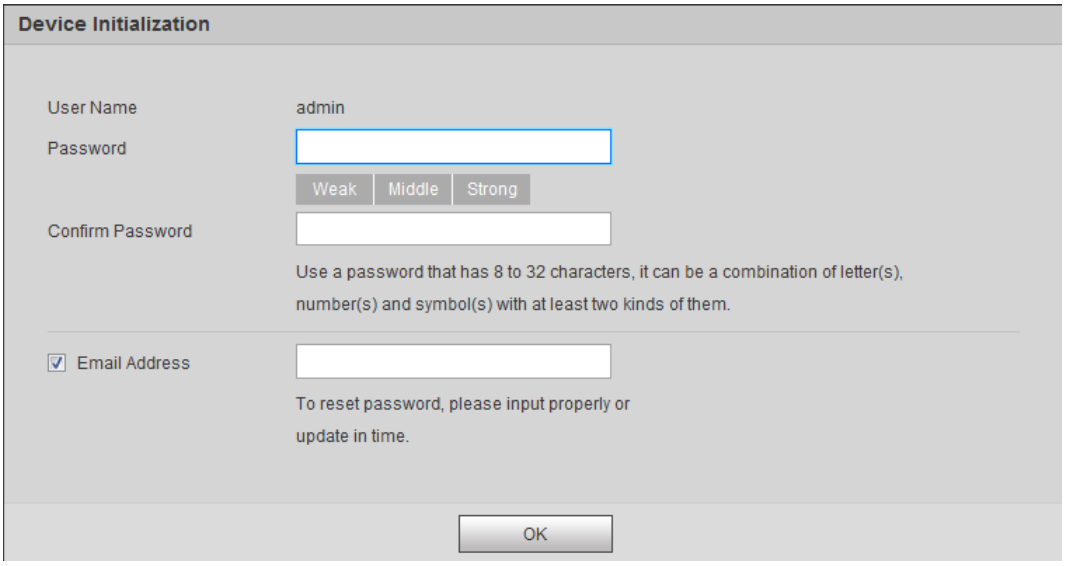
The IP address is 192.168.1.108 by default.

Step 2 Use ping ***.***. ***. *** (IP address of the Camera) command and check whether the network is connected. If not, check the settings of IP address, subnet mask and gateway of PC and the Camera according to the previous step.

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

After it is successfully connected, the **Device Initialization** interface is displayed.

Figure 4-1 Device initialization



Device Initialization

User Name admin

Password

Confirm 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.

☑ Email Address

To reset password, please input properly or update in time.

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

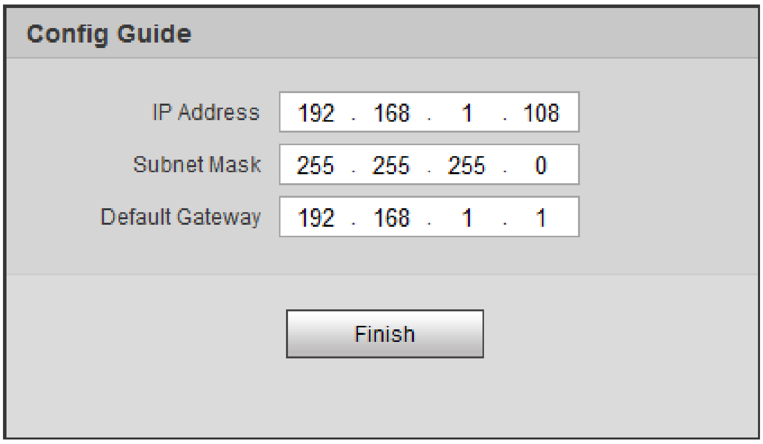
- The new password can be set from 8 characters to 32 characters and contains at least two categories from upper cases, lower cases, numbers and special characters (excluding "'", """, ";", ":" and "&")
- If you want to modify the password again, go to **Setting > System > Account > Account**.
- A prompt box will pop out when user name and/or password are/is incorrect, and the system will remind you of remaining attempts. The account will be locked for 5 minutes if user enters incorrect user name or password for 5 consecutive times.

Step 5 Check **Email Address** and then enter the email address.

This Email address can be used to reset the password, and it is recommended to finish this setting.

Step 6 Click **OK**.

Figure 4-2 Config guide



Config Guide

IP Address: 192 . 168 . 1 . 108

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Step 7 Modify the default IP address, and then click **Finish**.

The **Login** interface is displayed.

## 4.2 Password Reset

When you forgot the password of admin user, you can set new password through password reset function.

⚠

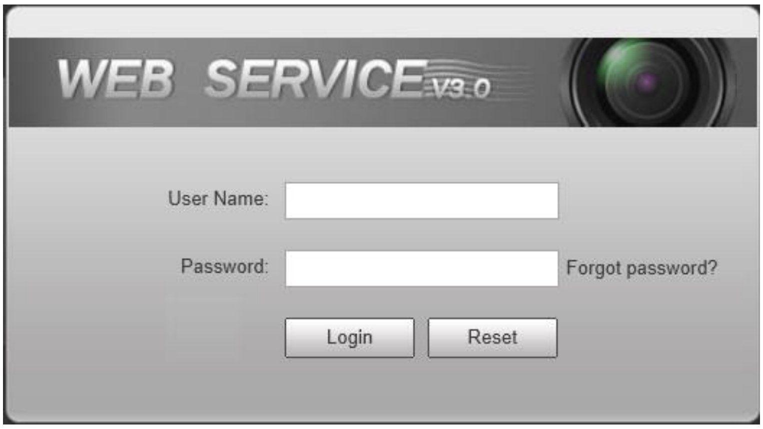
Pay attention to the following tips during password reset.

- When scanning QR code to acquire security code, one QR code supports security code acquisition up to twice.
- After receiving security code by email, you need to reset password within 24 hours, otherwise the security code will be invalid.
- One device is allowed to generate security code up to 10 times in one day, so the Camera can be reset up to 10 times.
- User email must be filled in during device initialization, which is used to receive security code; otherwise it fails to implement password reset. Reserved email of admin can be modified from **Setting** > **System** > **Account** > **Account**.

Step 1 Open the browser, enter the IP address of the Camera in the browser address bar, and then press Enter.

The **Login** interface is displayed. See Figure 4-3.

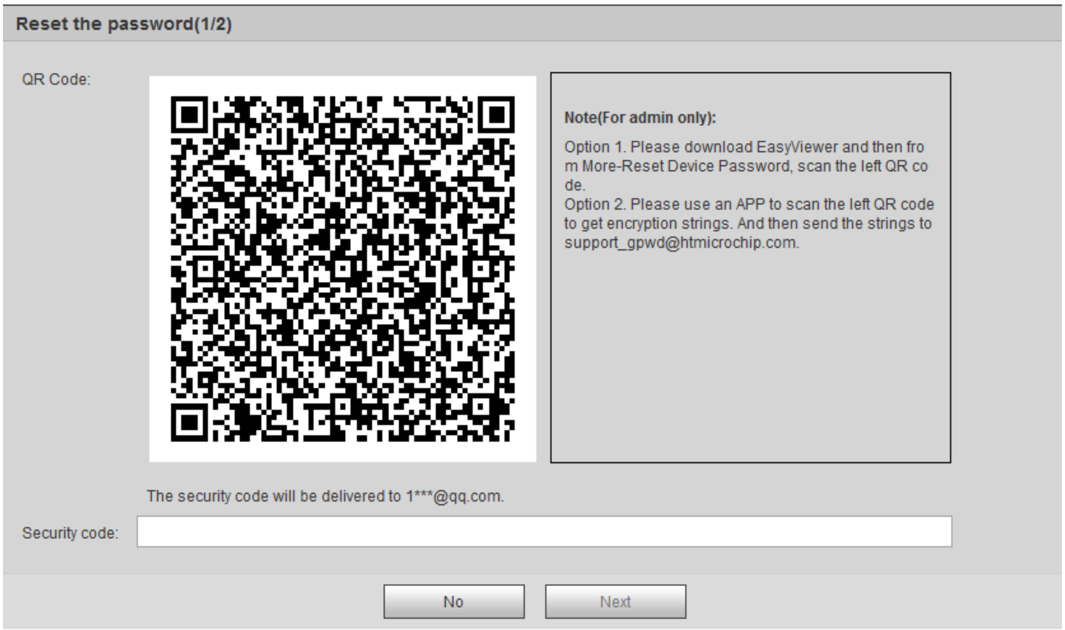
Figure 4-3 Login interface



Step 2 Click **Forgot password?**

If you use IE browser, the system might prompt **Stop running the script**, click **No** and continue to run the script.

Figure 4-4 Reset password (1)



Note(For admin only):

Option 1. Please download EasyViewer and then from More-Reset Device Password, scan the left QR code.
Option 2. Please use an APP to scan the left QR code to get encryption strings. And then send the strings to support_gpwd@htmicrochip.com.

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

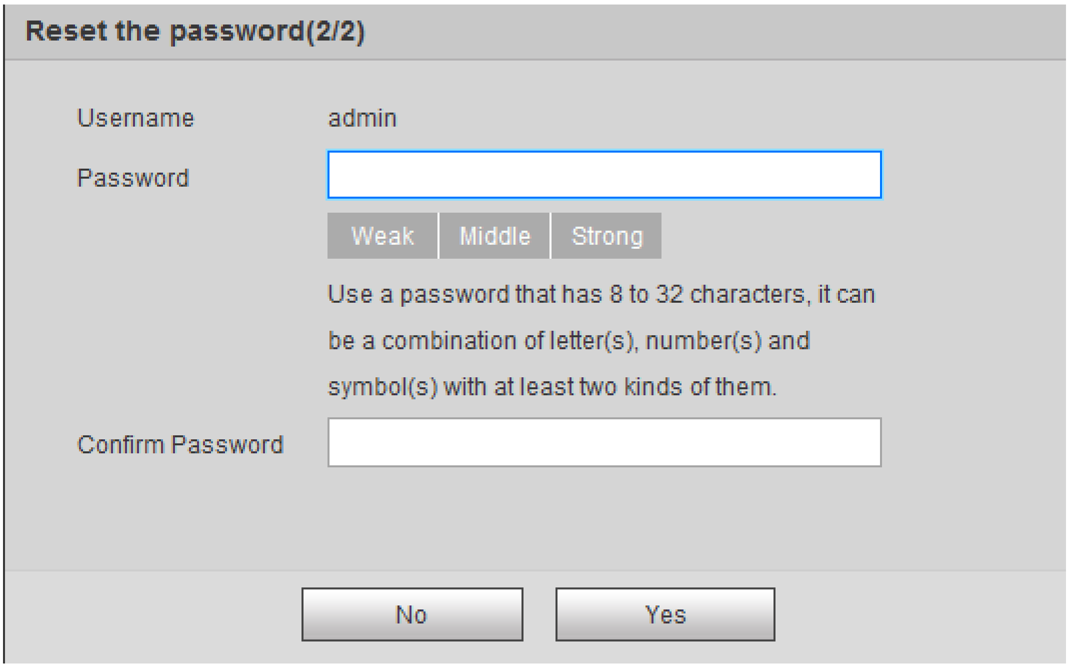
Step 3 Scan the QR code according to the interface prompt, and send the scanning result to designated email and acquire security code.

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

Step 4 Input received security code in the text box of **Security code**.

Step 5 Click **Next**.

Figure 4-5 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

Step 6 Set Password and Confirm Password.

The new password can be set from 8 characters to 32 characters and contains at least two categories from upper cases, lower cases, numbers and special characters (excluding "'", """, ";", ":" and "&"). The new password should be the same as the Confirm Password. Follow the password security notice to set a high security level password.

Step 7 Click **OK** and password reset is completed.

## 4.3 Guide

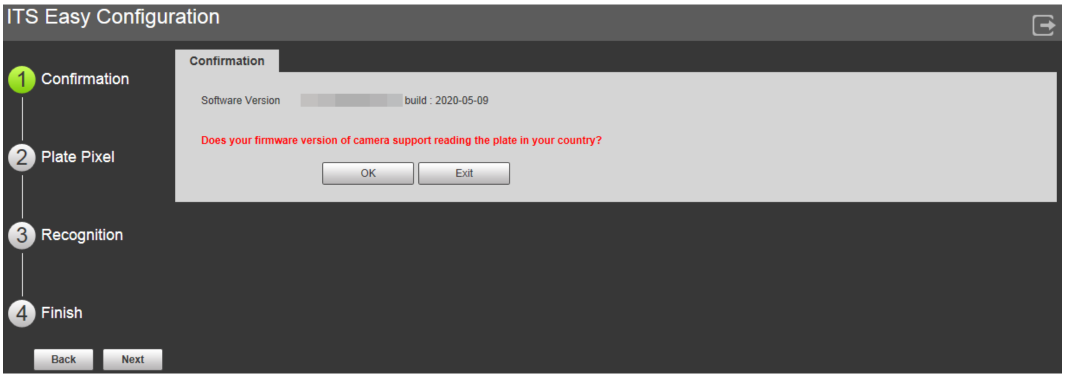
This section is only applicable to the Camera.

It provides guide for fast configuration of the Camera. You can quickly configure major functions of the Camera.

If you want to configure detailed functions and operations, click to skip **ITS Easy Configuration**, and configure the parameters in **Live**, **Query**, **Setup** and **Alarm**.

Step 1 Click **Guide** tab.

Figure 4-6 ITS easy configuration



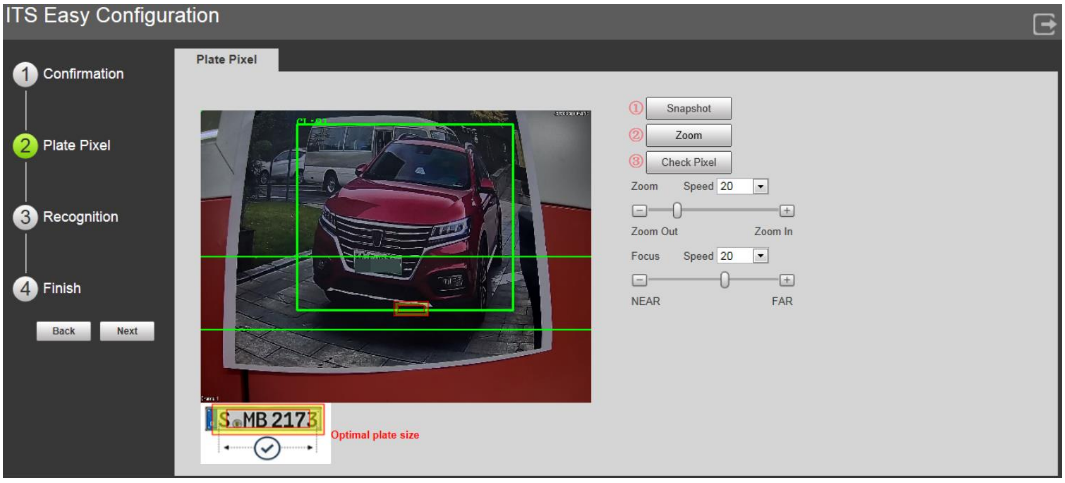
ITS Easy Configuration

Software Version [redacted] build : 2020-05-09

Does your firmware version of camera support reading the plate in your country?

Step 2 Confirm information of **Software Version**, and then click **OK**.

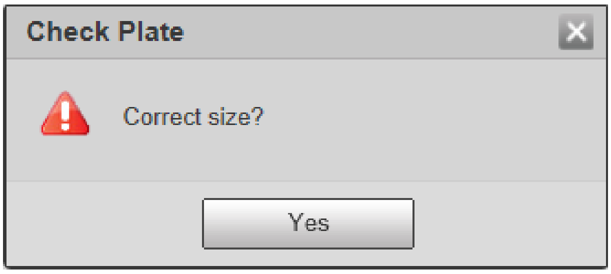
Figure 4-7 Plate pixel



Step 3 You can check whether the video image is properly zoomed and focused by checking the plate pixel.

1) Drag zoom and focus bar to adjust the video image properly.
2) When the vehicle plate comes into the green line area, click **Snapshot** to take a snapshot of the plate.
   **Snapshot** becomes **Resume**.
3) Drag the yellow plate pixel box to the position of the plate.
4) Click **Zoom**.
   Zoom in the picture selected by the plate pixel box. It can realize 2x or 4x zoom rate.
5) Adjust the position of plate pixel box and make it the optimal plate size.
6) Click **Check Pixel**.

Figure 4-8 Check plate



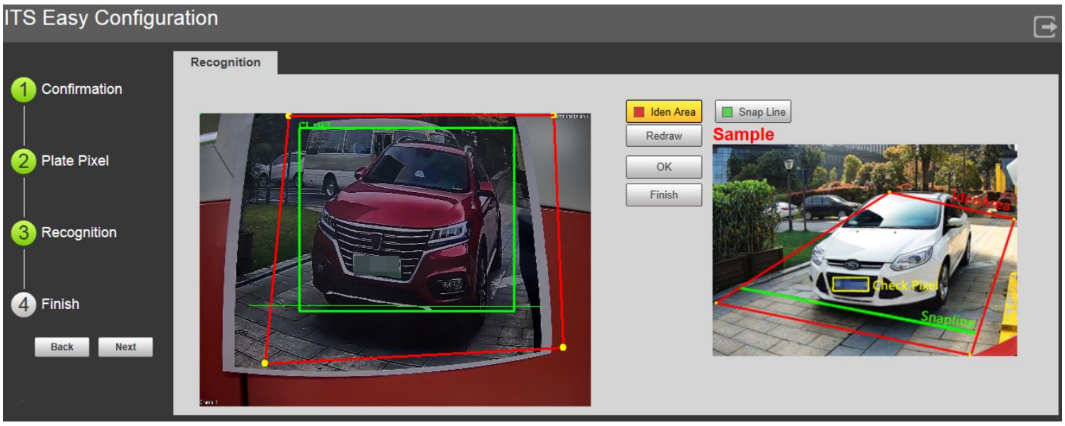
Check Plate

Correct size?

Yes

7) Click **Yes** and plate pixel config is finished.

Figure 4-9 Recognition



Step 4 Configure recognition area.

The config example on the right of video image can be used as a reference.

1) Click **Iden Area**.

Click and draw 4 lines on the video image and the recognition area is formed.

2) Click **Snap Line**.

Draw snap line via dragging mouse on the area. The snap line must cross the area.

3) Click **Save** to complete the settings.

Step 5 Click **Finish**, exit guide interface and enter **Live** interface.

# 4.4 Lattice Screen

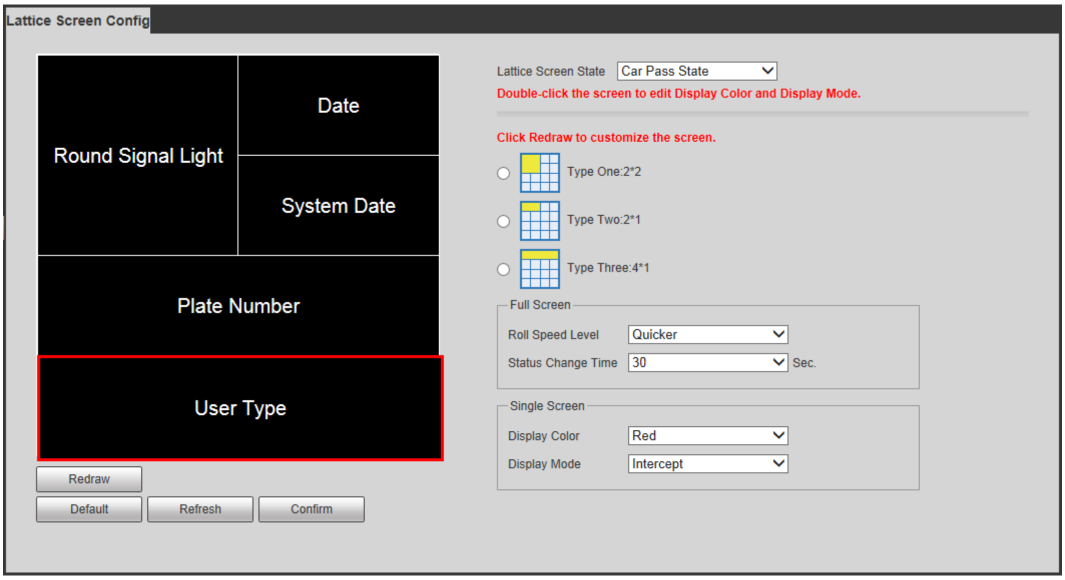
Lattice screen displays different information when vehicle passes and in normal state. The Kit also broadcast screen information according to the broadcast content settings.

## 4.4.1 Lattice Screen Config

You can configure the information displayed on the screen in **Car Pass State** and **Normal State**.

Step 1 Select **Setup > ITC > Lattice Screen Config**.

Figure 4-10 Lattice screen config



Lattice Screen Config

Lattice Screen State: Car Pass State

Double-click the screen to edit Display Color and Display Mode.

Click Redraw to customize the screen.

○ Type One:2*2

○ Type Two:2*1

○ Type Three:4*1

Full Screen

Roll Speed Level: Quicker

Status Change Time: 30 Sec.

Single Screen

Display Color: Red

Display Mode: Intercept

Step 2 Select **Lattice Screen State**. You can select from **Car Pass State** and **Normal State**. The information displayed on the screen may vary in different states.

Step 3 Select the display mode from **Type One:2*2**, **Type Two:2*1**, and **Type Three:4*1**. For example, if you select **Type Three:4*1**, it means an information display area consists of 4 small matrixes from 1 line.

Step 4 Set parameters applicable to the entire LED display.

- **Roll Speed Level**: The displaying speed of information on the screen. Five levels are available.
- **Status Change Time**: The time of vehicle pass information displayed on the screen. You can select from **10**, **20**, **30**, **40**, **50**, and **60** seconds.

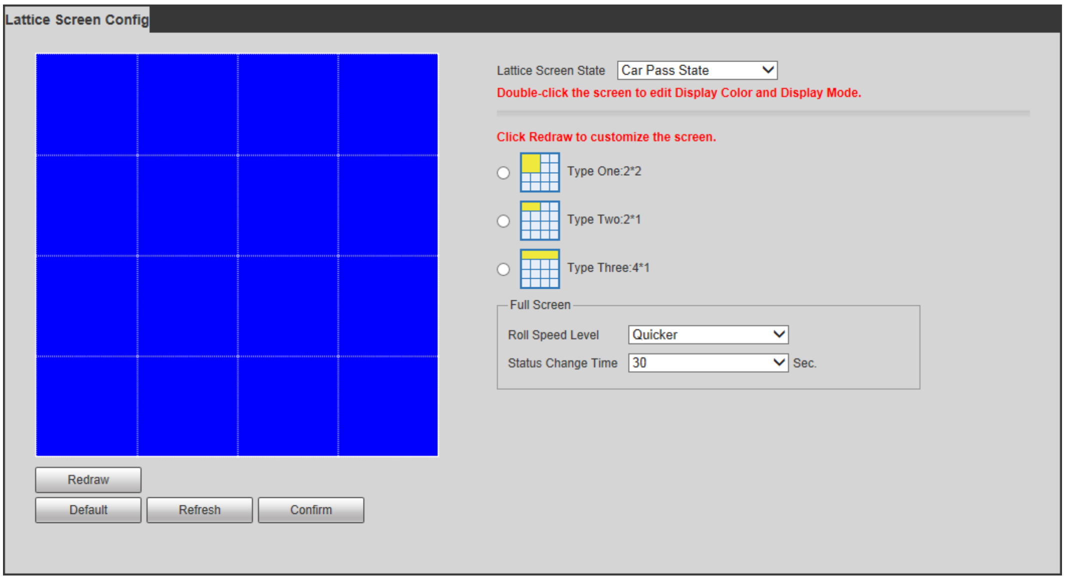
Step 5 Double-screen any screen to set its display parameters separately.

- **Display Color**: The color of displayed information. It is **Red** by default.
- **Display Mode**: The way that information displayed on the screen.

Step 6 Redraw the screen as needed.

1) Click **Redraw**, and the matrixes are displayed in blue, which means no information display area is drawn.

Figure 4-11 Redraw the screen



Lattice Screen Config

Lattice Screen State: Car Pass State

Double-click the screen to edit Display Color and Display Mode.

Click Redraw to customize the screen.

○ Type One:2*2

○ Type Two:2*1

○ Type Three:4*1

Full Screen

Roll Speed Level: Quicker

Status Change Time: 30 Sec.

2) Select one mode, and drag the left mouse button on the screen to redraw the matrix, or click on any small matrix, and the system will automatically generate the matrix based on the mode you selected.

3) After redrawing the matrix, right-click on the redrawn matrix to change the name of the matrix.
You can also select **Custom Info** to enter customized information.

4) Configure the parameters of each matrix that you have drawn.

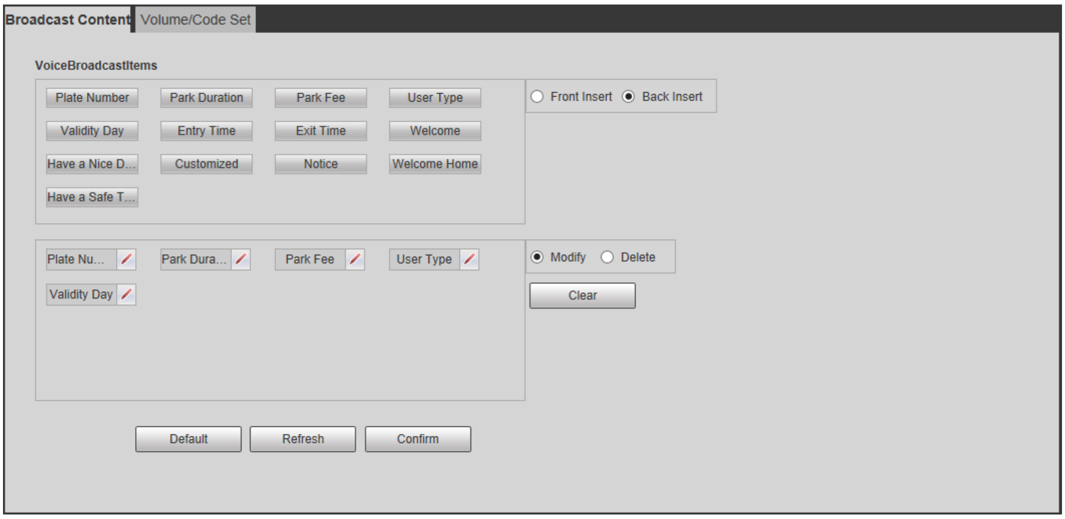
Step 7 Click **Confirm**.

## 4.4.2 Broadcast Content

You can configure the broadcast content of the Kit, and the content will be broadcast when vehicle passes.

Step 1 Select **Setup > ITC > Voice Broadcast > Broadcast Content**.

Figure 4-12 Broadcast content

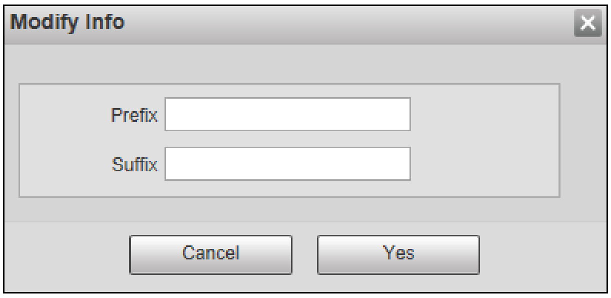


Step 2 Select **Front Insert** or **Back Insert**, and then select a voice broadcast item, this item will be inserted before or after the item selected (in yellow).

Step 3 Select **Modify**, and then click ✎.

- **Prefix**: The content that will be broadcast before the broadcast item.
- **Suffix**: The content that will be broadcast after the broadcast item.

Figure 4-13 Modify info



Step 4 Click **Yes** to save the settings.

Step 5 Select **Delete**, and then click ☒ to delete a broadcast item.

Click **Remove All** to delete all the broadcast items.

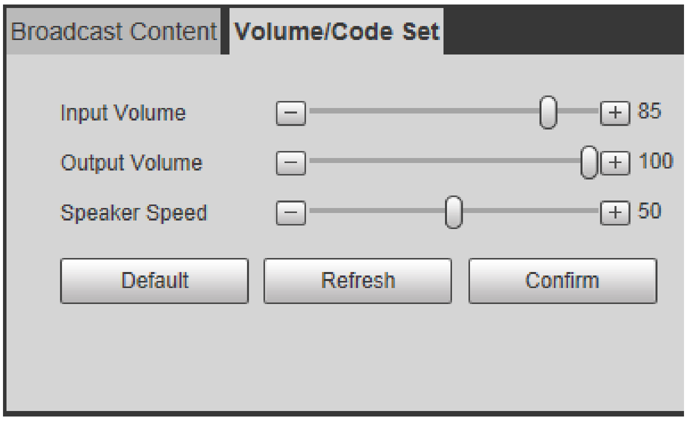
Step 6 Click **Confirm**.

### 4.4.3 Volume/Code Set

You can configure the input volume, and the volume and speed of speaker.

Step 1 Select **Setting > ITC > Voice Broadcast > Volume/Code Set**.

Figure 4-14 Volume/Code set



Input Volume 85

Output Volume 100

Speaker Speed 50

Step 2 Configure the parameters.

📖

It is recommended to click **Default** and then **Confirm** to use default configurations.

- **Volume Input**: The volume of user who wants to park vehicle.
- **Output Volume**: The volume of voice broadcast.
- **Speaker Speed**: The speed of voice broadcast.

Step 3 Click **Confirm**.

## 4.5 Config (LPR)

📖

This section is only applicable to the Camera.

Step 1 Open browser, enter IP address of the Camera in the address bar, and then press Enter.

The web login interface is displayed.

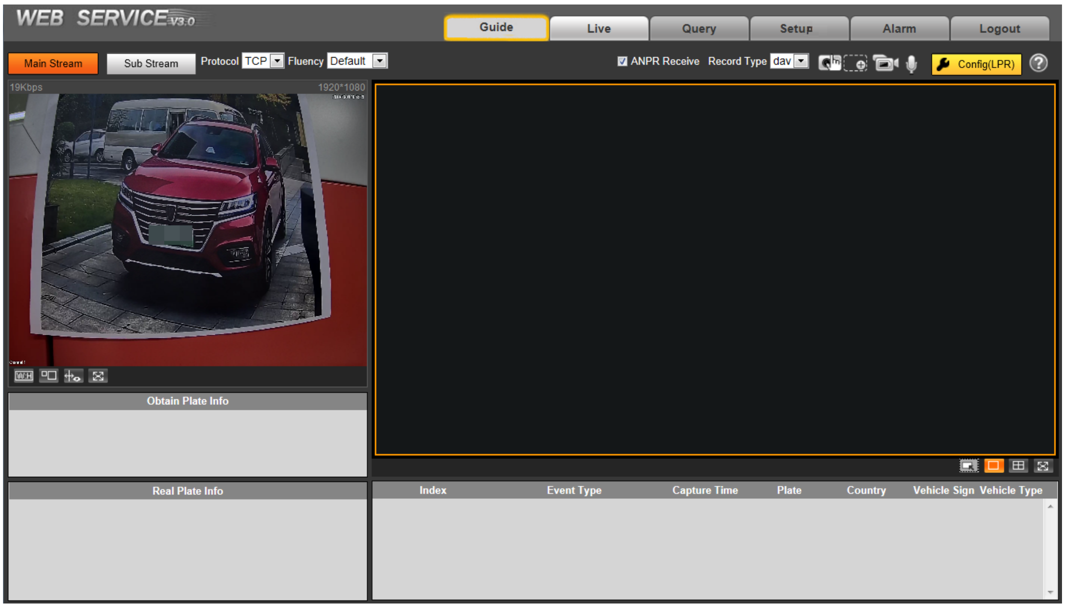
Step 2 Enter the username and password, and then click **Login**.

The main page of web interface is displayed.

📖

The IP address is 192.168.1.108 by default. The IP address shall be modified when login for the first time. To modify the IP address, see "4.1 Initializing Camera."

Figure 4-15 Live interface



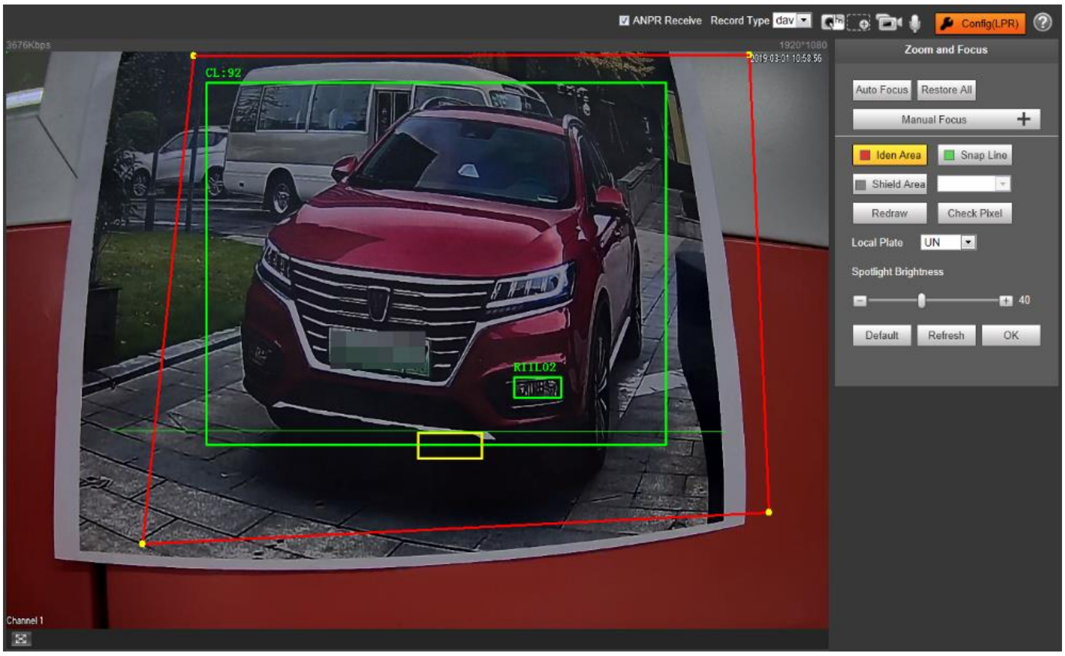
Protocol TCP

Fluency Default

Record Type dav

Step 3 Click Config(LPR).

Figure 4-16 Config (LPR)



Record Type dav

Local Plate UN

Spotlight Brightness 40

Step 4 Set focus and zoom mode, which is used to recognize vehicle.

Table 4-1 Focus parameter description

| Parameter | Description |
|---|---|
| Auto Focus | Auto adjust camera lens and make the scenario clearly focused. |

| Parameter | Description |
|---|---|
| Manual Focus | Manually set focus parameter and make the camera focus on the vehicle.<br>● Zoom:<br>◇ Step length: There are totally 3 levels to be selected.<br>◇ Zoom in, zoom out: Click + and add a step length, click − and reduce a step length; Or directly drag adjustment bar and set zoom.<br>● Focus:<br>◇ Step length: There are totally 3 levels to be selected.<br>◇ Focal length: Click +to add a speed, click − to reduce a speed; or it can directly drag adjustment bar to set near and far focal length. |
| Restore All | Restore all to initialized settings. |
| Refresh | Check the latest status. |

Step 5 Select the config line type which needs to be drawn.

Table 4-2 Config line parameters description

| Parameter | Description |
|---|---|
| Iden Area | Click it and draw the area range which needs to be detected.<br>The recognition area line is displayed as red box. |
| Snap Line | Draw the snap line which triggers video capture, it is as functional as the line in traffic. It will trigger and take snapshot when the vehicle crosses the snap line.<br>Snap line is displayed as green line. |
| Shield Area | Set the area range which needs to be shielded. LPR is not implemented within the shielded area. It supports setting max two shielded areas.<br>Area line is displayed as gray box. |
| Check Pixel | Click it, and drag the yellow plate pixel box to the range of vehicle plate on the video image.<br>If the plate within the yellow box is larger than the optimal plate size in the example, zoom out the video image by clicking **Manual Focus**; if smaller, zoom in the video image. |

Click **Redraw** to delete config line one by one.

Step 6 Adjust the vehicle snapshot location to yellow box.

Try to make sure the location and size of plate is in accordance with that of the yellow box.

The value of plate optimal width range is 150. To modify the value, go to **Setting > ITC > Intelligent > Video Analyse > Recognition**.

Step 7 Configure **Local Plate**. Select local plate according to the device location.

Step 8 Set the brightness of fill light. Drag the slider to adjust the brightness according to actual ambient brightness.

Step 9 Click **OK**.

# 5 FAQ

| FAQ | Solutions |
|---|---|
| Device error. Failed to normally operate or start | Press the **Reset** button for 5 seconds and make the Camera restore to default setting. |
| Storage card hot swap | Stop recording and snapshot before removing storage card. Operation can be made after 15 seconds in order to guarantee data completeness; otherwise it may cause the danger of data loss. |
| Write times limit of storage card | Do not set the storage card as the storage media of scheduled record, otherwise it will rapidly reach the write longevity and cause damage to the storage card. |
| Failed to use disk for storage | When the storage card shows sleep mode or 0 capacity, first format it through web interface. |
| Network upgrade failed | Check whether the right upgrade program (such as version, compatibility) is used. |
| Recommended TF card | Dahua 16GB, Dahua 32GB, Dahua 64GB, Kingston 16GB, Kingston 32GB, and Kingston 64GB. It is recommended to use class 10 high capacity card, which supports max 128G TF card. |
| Failed to pop up the installation dialog box of web control webrec.cab | Set the security level of IE browser as **Low**, **Active Plug-in and Control** is set as **Enable**. |

# Appendix 1 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 Whitelist**

   We suggest you to enable whitelist 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 whitelist.

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 blacklist and whitelist 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