Outdoor Parking Space Detector

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the outdoor parking space detector (hereinafter referred to as "the Camera"). Read carefully before using the device, and keep the manual safe for future reference.

Models

Models	Lens
ITC439-PW1H-LZ	Short range
ITC439-PW1H-LZF1050	Long range

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	January 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions.

For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

 WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Disconnect the device when installing and connecting the lens.

Operation Requirements

- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.

- 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 it.
- Do not disassemble the device.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the device in liquid during transportation, storage or installation.
- Do not block the ventilation near the device.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function earthing portion of the device (grounding cable or lightning surge protector) to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be used with the protective cover for outdoor scenarios to avoid the risk of water damage to the device.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Modify the default password of the device after first-time login to prevent the device from being stolen.

Maintenance Requirements

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before sending it back for repair.
- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.
- Clean the surface of the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

1 Overview

1.1 Appearance

Figure 1-1 ITC439-PW1H-Z

Figure 1-2 ITC439-PW1H-Z1050

1.2 Dimensions

Figure 1-3 ITC439-PW1H-Z (mm [inch])

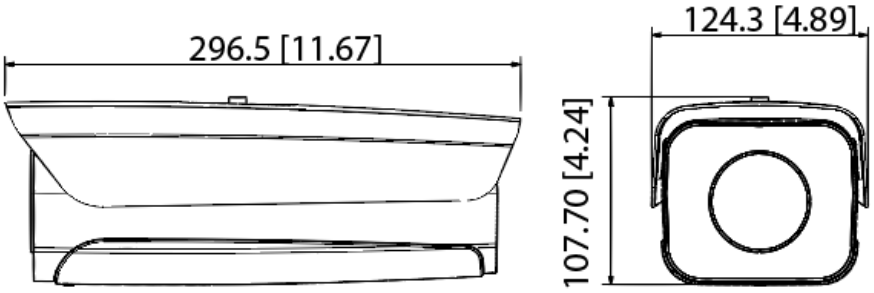
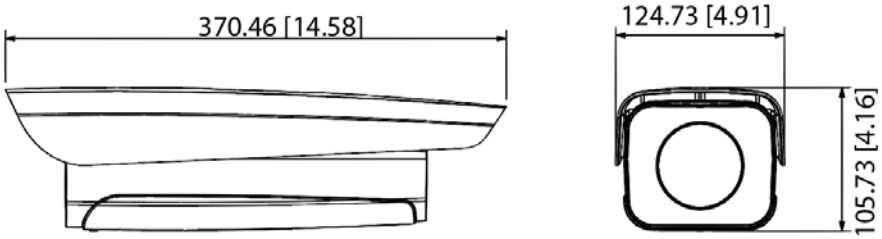


Figure 1-4 ITC439-PW1H-Z1050 (mm [inch])



1.3 Structure

Figure 1-5 Structure

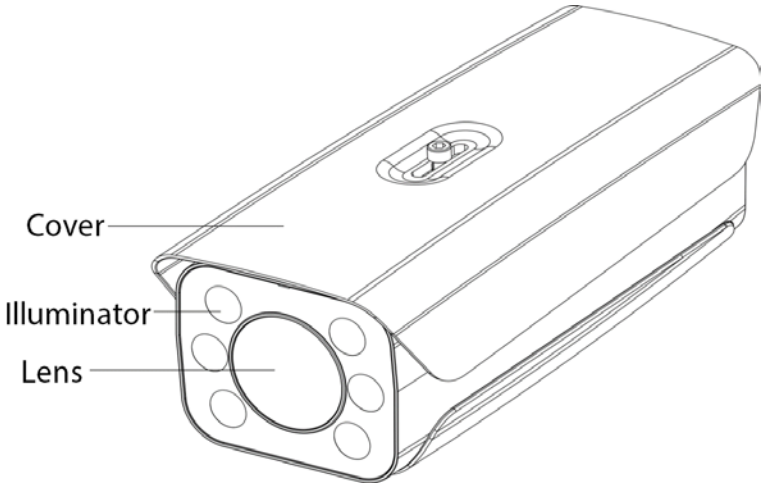
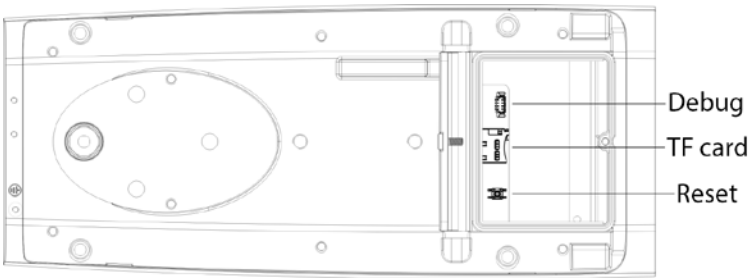


Figure 1-6 Rear panel



1.4 Cables

Figure 1-7 External cables

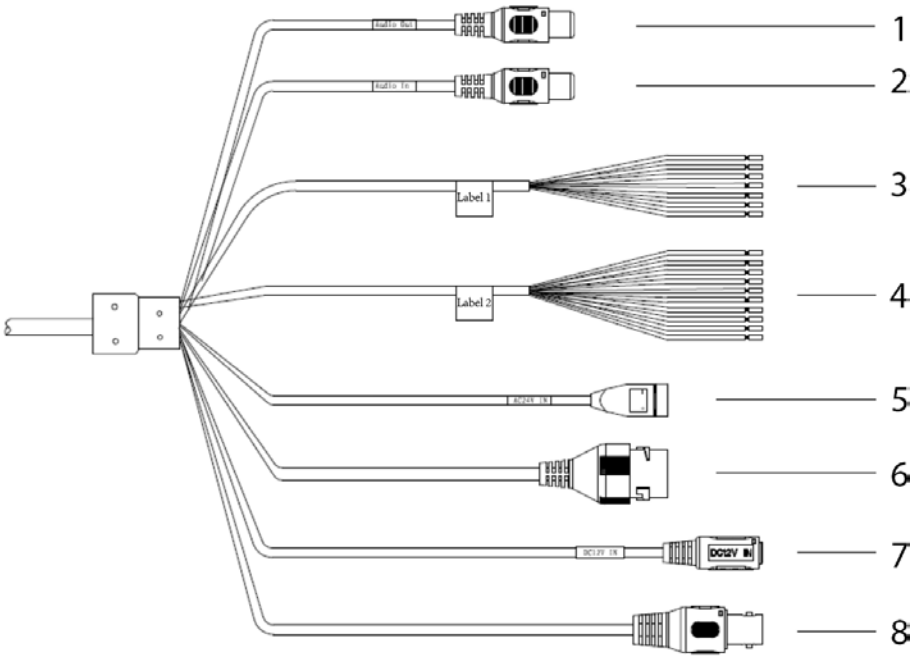


Table 1-1 Description of external cables

No.	Port	Description
1	AUDIO OUT	Outputs audio
2	AUDIO IN	Inputs audio
3	RS-485/RS-232	● White and red: RS-485_A1 ● White and orange: RS-485_B1 ● Yellow and gray: RS-485_A2 ● Yellow and black: RS-485_B2 ● White and yellow: RS-232_RXD ● White and brown: RS-232_TXD ● White and black: GND
4	ALARM	Gray: ALARM_IN_GND ● Alarm output ◇ Brown: ALARM_NO1 ◇ Green: ALARM_COM1 ◇ White and pink: ALARM_NO2 ◇ Light green: ALARM_COM2 ◇ Red: ALARM_NO3 ◇ Black: ALARM_COM3 ● Alarm input ◇ Blue: ALARM_IN1 ◇ White: ALARM_IN2 ◇ Yellow: ALARM_IN3
5	24 VAC	Inputs 24 VAC power supply. Make sure to supply power to the Camera under the instructions on the label. ⚠ The Camera might be damaged if the power supply is incorrect.
6	LAN	Connects to standard Ethernet cables for power supply. PoE is available.
7	12 VDC	Inputs 12 VDC power supply. Make sure to supply power to the Camera under the instructions on the label. ⚠ The Camera might be damaged if the power supply is incorrect.
8	BNC	Connects to panorama cameras.

2 Installation

2.1 Installation Requirements

For perpendicular parking and diagonal parking, the installation positions of the Camera are different.

Installation Requirements

- The Camera must face the head of the vehicle.
- The installation height can be 6 m–15 m, 20 m and 25 m.
- Make sure that vehicles do not block each other.
- Targets blocked by trees might not be recognized. When the vehicle to be recognized is blocked by other vehicles, make sure the blockage is less than 40%.
- The Camera can only recognize small vehicles. Large vehicles, such as a truck, might not be recognized.
- The recognition is ensured only when the vehicle width is no less than 80 pixels.
- The number of vehicles that can be monitored depends on the installation height and the horizontal distance between the Camera and the sparking space.

2.2 Installing the Camera

The Camera can be installed with universal bracket, on a wall or a pole.

This section takes the installation method with universal bracket as an example.

Figure 2-1 Universal bracket

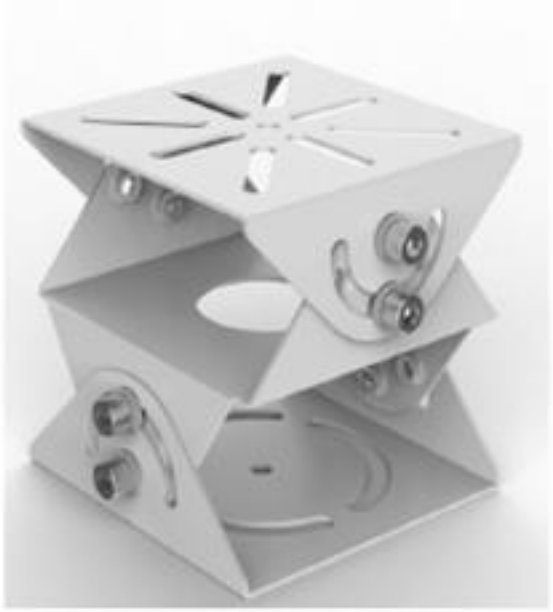
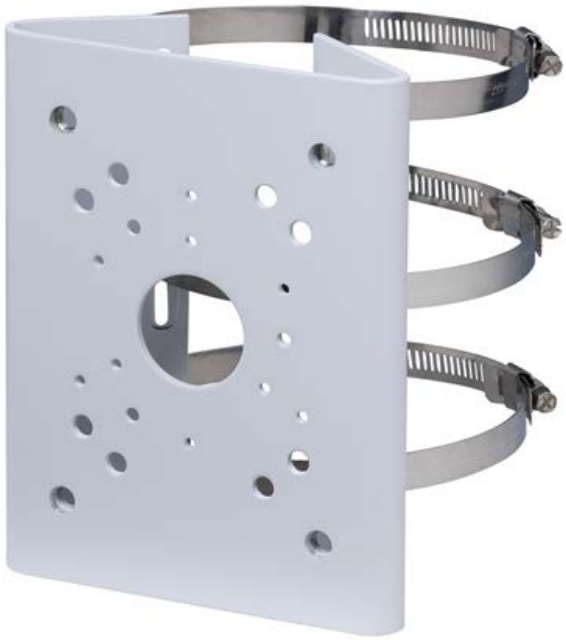


Figure 2-2 Wall mount bracket

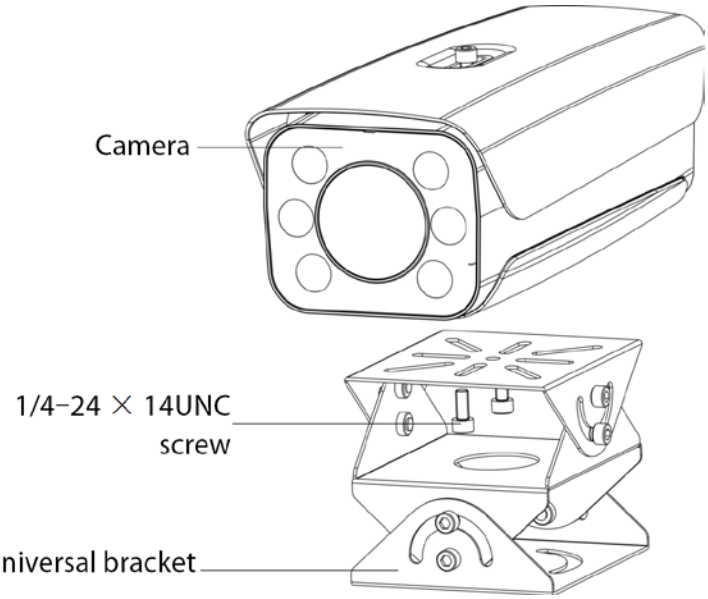
Figure 2-3 Pole mount bracket



Step 1 Use M6 × 14 screws to fix the universal joint on the bracket.

Step 2 Use two 1/4-20 × 14UNC screws to fix the camera on the universal bracket.

Figure 2-4 Universal bracket installation



Step 3 Adjust the position of the universal bracket and the Camera.

3 Camera Configurations

3.1 Initialization

Prerequisites

- The Camera is delivered uninitialized by default. You need to initialize it and modify its password before further operations.
- Before initialization, make sure both IP of the computer and the Camera are on the same network segment, otherwise the initialization might fail.

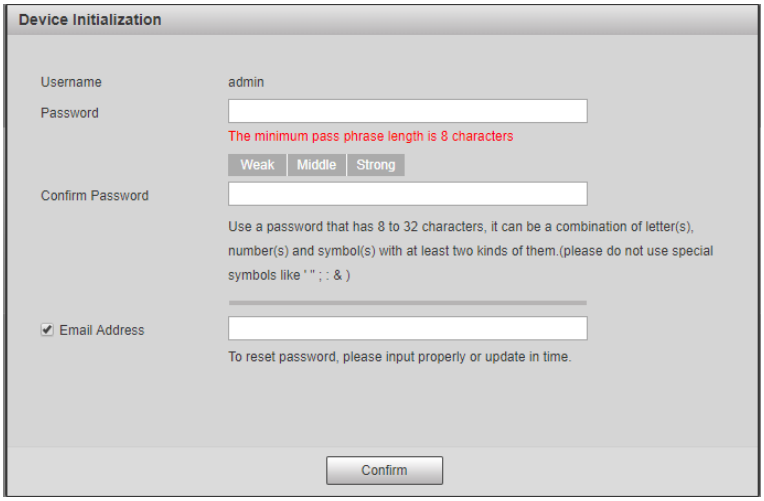
Procedure

Step 1 Set IP address, subnet mask, and gateway of the computer and camera respectively.

The IP address is 192.168.1.108 by default.

Step 2 Open browser, enter the IP address of the Camera in the address bar, and then press the Enter key.

Figure 3-1 Device Initialization



Step 3 Enter and confirm the password.

The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).

Step 4 Select **Email Address**, and then enter your email address for resetting your password.

Step 5 Click **Confirm**.

3.2 Changing IP Address

You can acquire and change the IP address of devices accessed through wired network. This section takes changing IP address with ConfigTool as the example. For other methods of changing IP

address, see the user's manual.

Step 1 Start ConfigTool, and then click **Modify IP** on the homepage.

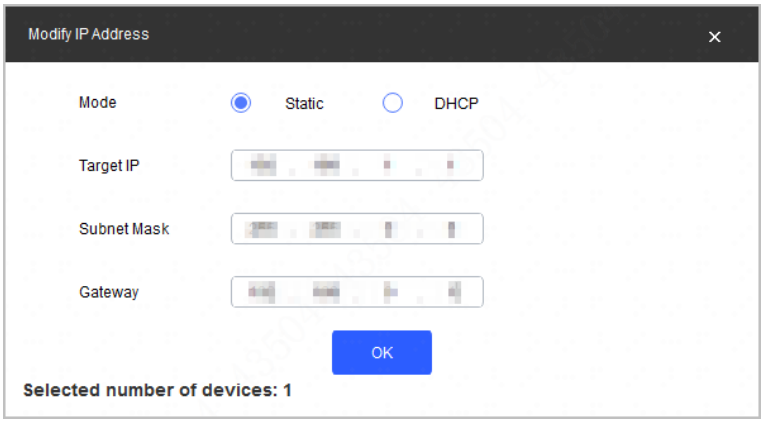
Step 2 Select the device(s) whose IP need(s) to be changed.

- Change one IP address: Click corresponding to the device.
- Change IP addresses in batches: Select the devices, and then click **Modify IP**.

Step 3 Set mode, IP, subnet mask and gateway.

Step 4 Click **OK**.

Figure 3-2 Change IP addresses in batches



3.3 Login

You can log in to the web client by following the steps below. For first-time login or logging in after restoring factory default settings, see "3.1 Initialization".

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

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

Step 3 For first-time login, click **Please click here to download and install the plug-in**, and then install the plug-in according to system prompt.

Before installing the plug-in, make sure that **ActiveX controls** (in IE browser) from **Tools** > **Internet Options** > **Security** > **Custom Level** is enabled.

Step 4 After successfully installing the plug-in, the live view of the Camera is displayed.

3.4 Parking Space Configuration

The Camera can detect whether the parking space is occupied, count available spaces in an area and monitor events such as crossing lines while parking.

3.4.1 Detecting Parking Space

Set a parking zone and parking spaces inside the zone, so the Camera can detect whether the specified parking space is occupied and recognize the vehicle.

Step 1 Select **Setting** > **ITC** > **Park Space Config** > **Parking Space Management**.

Step 2 Under **Intelligence**, set **Mode** to **Parking Space Detection**.

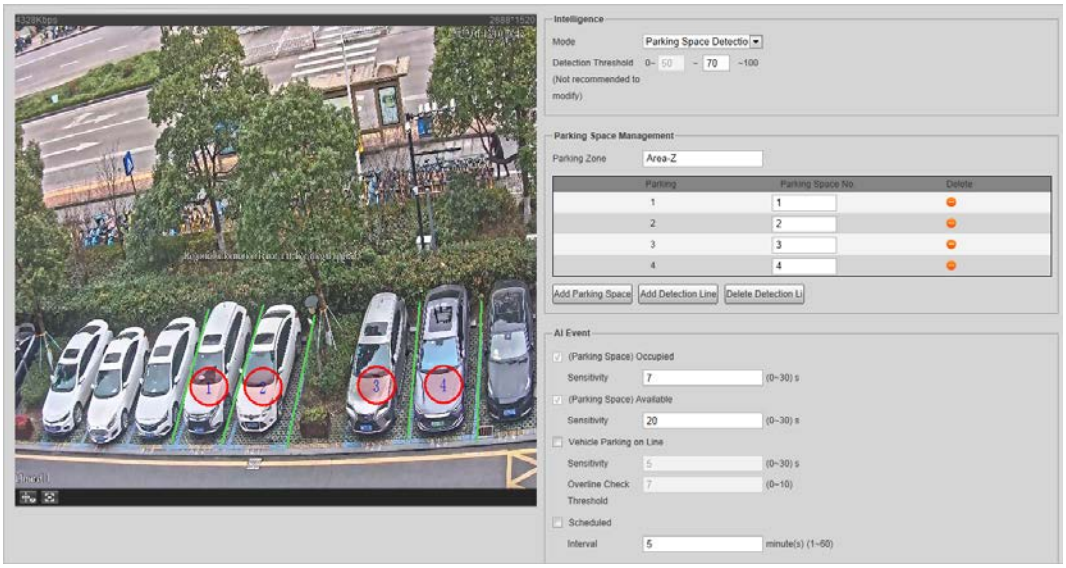
For **Detection Threshold**, we recommend you leave it as default.

Step 3 Under **Parking Space Management** section, enter the **Parking Zone** name, and then click **Add Parking Space** to add parking spaces for the Camera to monitor.

- Type and number are required for each parking region.
- The Camera can monitor 4 parking spaces at most.

Step 4 Click **Add Detection Line**, draw lines between parking spaces. The Camera detects events such as crossing line while parking and triggers alarms based on the drawn lines.

Figure 3-3 Parking space management



Step 5 Click **Confirm**.

3.4.2 Counting Available Spaces

Set a parking zone and divide parking areas inside the zone, so the Camera can monitor parking spaces in each area and output available spaces in real time.

Step 1 Select **Setting** > **ITC** > **Park Space Config** > **Parking Space Management**.

Step 2 Under **Intelligence**, set **Mode** to **Available Space Count**.

Select **Vehicle Box**, each vehicle will be marked with a frame for clearer view.

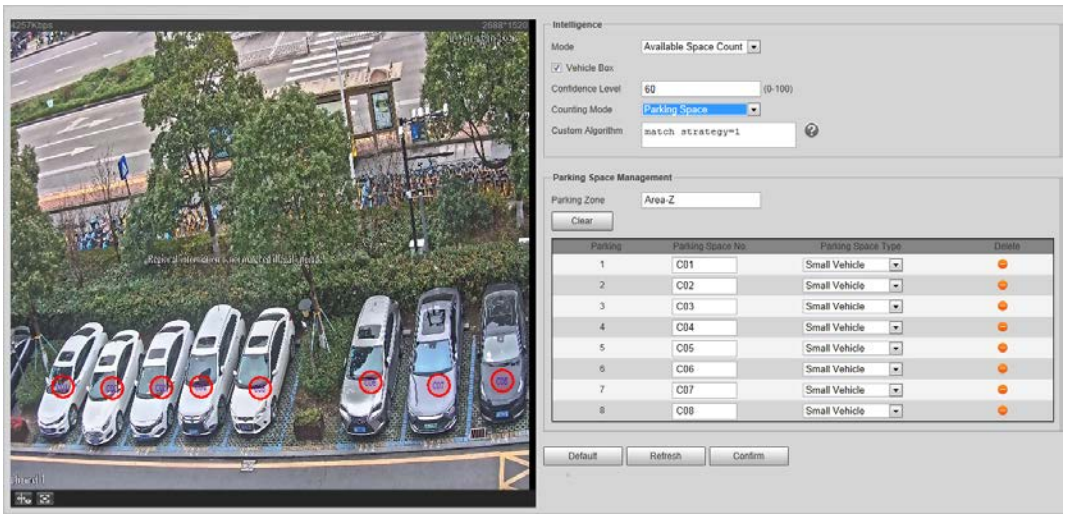
Step 3 Set **Confidence Level** to filter wrong detections.

Step 4 Set **Counting Mode**.

The Camera supports monitoring up to 50 parking spaces.

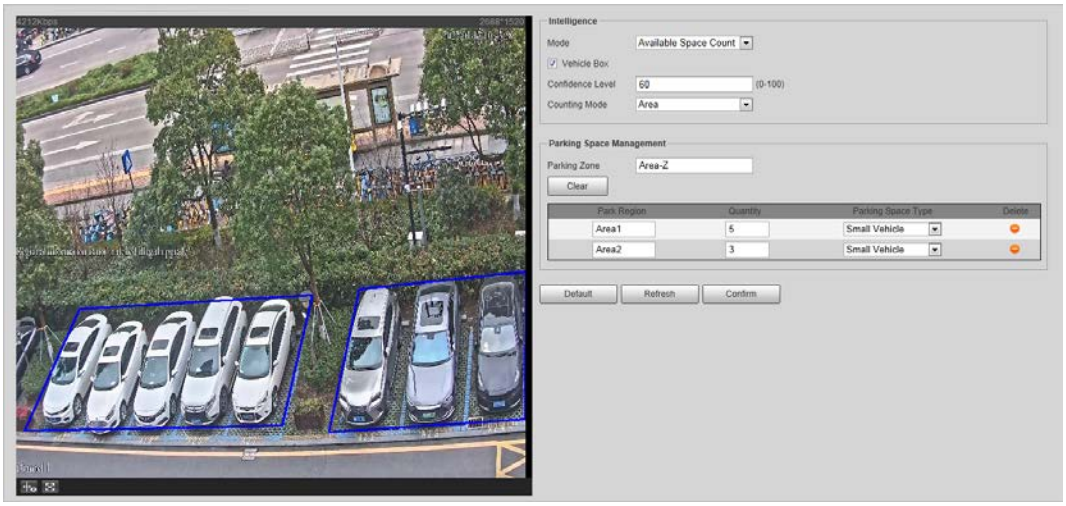
- **Parking Space**: Count available spaces based on the configured individual parking spaces.
  1. Click each parking space on the video image. With each click, a green circle (available) or red circle (occupied) is displayed.
  2. On the left side, set the parking space number and type.

Figure 3-4 Parking space management



- **Area**: Count available spaces based on the configured parking area.
  1. Click on the video image, draw a parking area according to the actual site, and then right-click to finish.
  2. On the left side, set the parking region name, the number of vehicles that the region contains and type.

Figure 3-5 Parking space management



Step 5 Click **Confirm**.

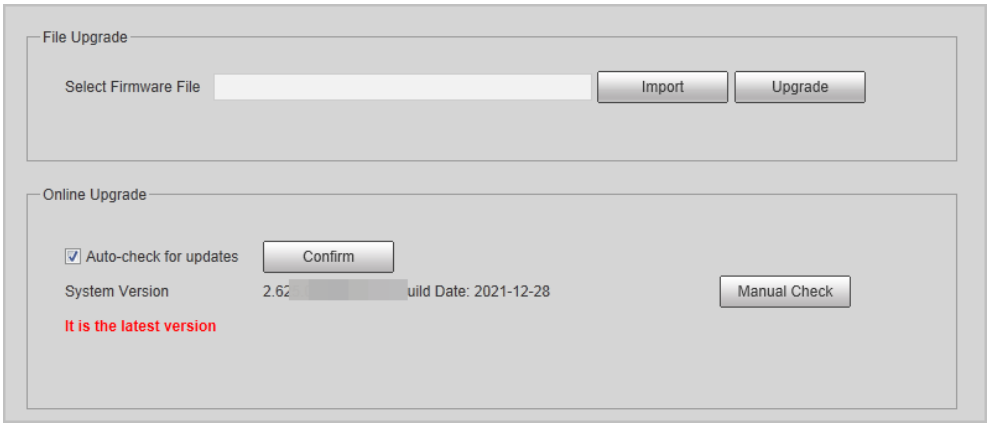
4 Update

Step 1 Log in to the web client of the Camera.

Step 2 Select **Setting** > **System Upgrade** > **System Upgrade**.

The pages might vary depending on the device model.

Figure 4-1 Upgrade



Step 3 Click **Import** to select the update file, and then click **Upgrade** to update the system.

Do not disconnect the power or network, or restart or shut down the Camera during update. Incorrect update programs might result in malfunctions of the Camera.

Appendix 1 Cybersecurity Recommendations

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 device 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. **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.

8. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **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.
10. **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.
11. **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.
12. **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.
13. **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.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.