

# **Smart Video Parking Detector**

## **Quick Start Guide**



V1.0.0

# Foreword

## General






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

## Models

Models	Power Supply	Pixel	Sensor
ITC214-PH5B-F3-POE	PoE	2 MP	Single sensor
ITC414-PH5B-F2-POE		4 MP	
ITC414-PH5B-TF2-POE			Dual-sensor
ITC214-PH5B-F3	Cascading with network cables to provide 48 V power supply	2 MP	Single sensor
ITC414-PH5B-F2		4 MP	
ITC414-PH5B-TF2			Dual-sensor

## Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 <b>TIPS</b>	Provides methods to help you solve a problem or save time.
 <b>NOTE</b>	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



- 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

<b>Foreword .....</b>	<b>I</b>
<b>Important Safeguards and Warnings.....</b>	<b>III</b>
<b>1 Overview .....</b>	<b>1</b>
<b>1.1 Appearance.....</b>	<b>1</b>
<b>1.2 Dimensions .....</b>	<b>1</b>
<b>2 Cable Connection .....</b>	<b>2</b>
<b>2.1 PoE Cable Connection .....</b>	<b>2</b>
<b>2.2 Cascading Power Supply.....</b>	<b>3</b>
<b>3 Installation .....</b>	<b>4</b>
<b>3.1 Cable Wiring .....</b>	<b>4</b>
<b>3.2 Installing the Camera.....</b>	<b>4</b>
<b>4 Network Settings .....</b>	<b>6</b>
<b>4.1 Initialization .....</b>	<b>6</b>
<b>4.2 Changing IP Address .....</b>	<b>7</b>
<b>4.3 Login .....</b>	<b>7</b>
<b>5 Configuring Parking Space.....</b>	<b>9</b>
<b>6 Update.....</b>	<b>10</b>
<b>6.1 Update by ConfigTool .....</b>	<b>10</b>
<b>6.2 Update on Web Client.....</b>	<b>11</b>
<b>Appendix 1 Cybersecurity Recommendations .....</b>	<b>12</b>

# 1 Overview

The Camera is mainly applied to intelligent parking lot management system for parking guidance and reverse vehicle search in indoor parking lots.



The Camera structure might vary depending on different models.

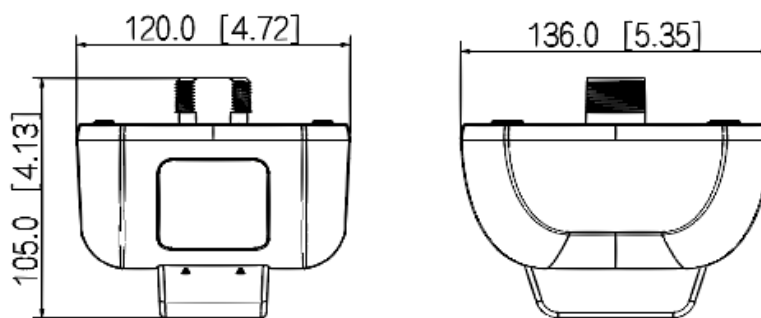
## 1.1 Appearance

Figure 1-1 Appearance



## 1.2 Dimensions

Figure 1-2 Dimensions (mm [inch])



## 2 Cable Connection

### 2.1 PoE Cable Connection

Figure 2-1 PoE

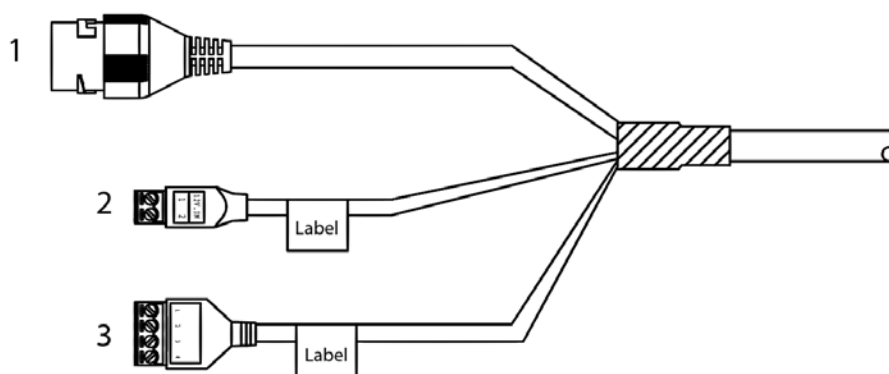


Table 2-1 PoE cable description

No.	Name	Description
1	Network port	Connect to standard Ethernet cable. PoE is supported.
2	Power	<ul style="list-style-type: none"><li>• 1: 12 VDC_IN.</li><li>• 2: GND_IN.</li></ul>
3	External light	<ul style="list-style-type: none"><li>• 1: 12V_OUT.</li><li>• 2: GND_OUT.</li><li>• 3: RS-485_A.</li><li>• 4: RS-485_B.</li></ul>



# 2.2 Cascading Power Supply

Figure 2-2 Network cable

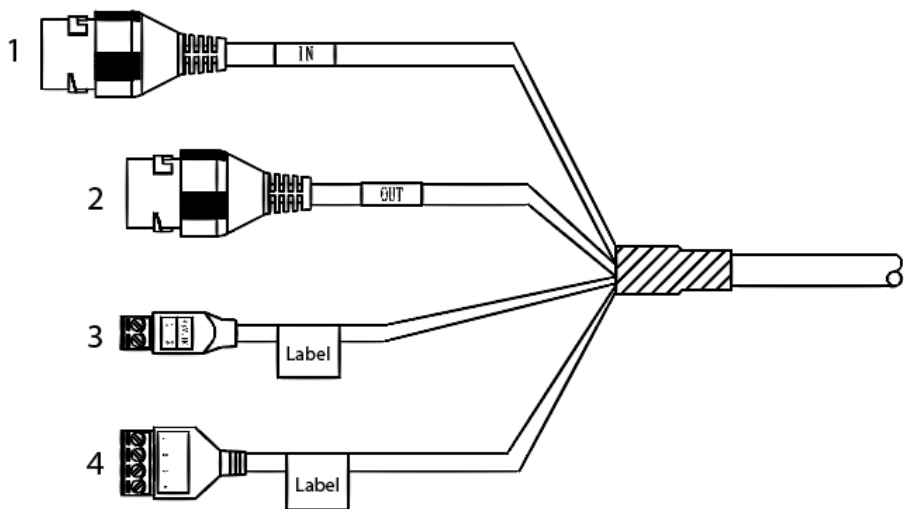


Table 2-2 Network cable description

No.	Name	Description
1	Network port (IN)	Network power input port.
2	Network port (OUT)	Network power output port.
3	Power	<ul style="list-style-type: none"><li>• 1: 48V_IN.</li><li>• 2: GND_IN.</li></ul>
4	External light	<ul style="list-style-type: none"><li>• 1: 12V_OUT.</li><li>• 2: GND_OUT.</li><li>• 3: RS-485_A.</li><li>• 4: RS-485_B.</li></ul>

## 3 Installation

### 3.1 Cable Wiring

- For ITC214-PH5B-F3-POE, ITC414-PH5B-F2-POE and ITC414-PH5B-TF2-POE series devices are supplied with PoE.
- For ITC214-PH5B-F3, ITC414-PH5B-F2 and ITC414-PH5B-TF2 series devices are cascading with network cables to provide 48 V power supply. 4 dual-sensor cameras or 8 single-sensor cameras can be supplied at the same time.

### 3.2 Installing the Camera



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



- The stud diameter is 33 mm.
- The installation takes ITC214-PH5B-F3-POE as an example. The installation diagram is for reference only, and might differ from the actual device.

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

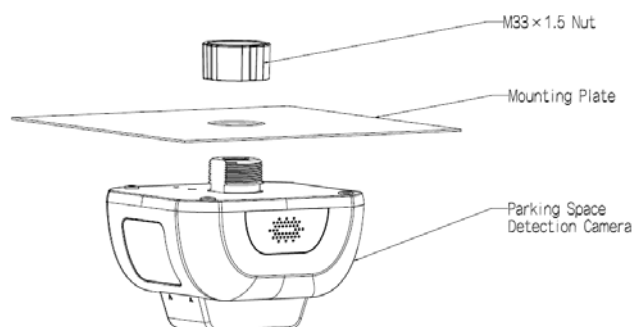
Figure 3-1 Hole saw



**Step 2** Feed the cables of the Camera through the hole on the mounting plate.

**Step 3** Loosen the nut, feed the cable through the nut, and then fix it to the mounting plate.

Figure 3-2 Installation



Step 4 Refer to "2 Cable Connection" to connect the cables.

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

Step 6 Tighten the cover.

# 4 Network Settings

The Camera is delivered with the same IP address (192.168. 1.108 by default). Plan available IP network segments properly based on the actual network conditions.



Figures in the manual are for reference only, and might differ from the actual page.

## 4.1 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 that both PC IP and device IP are on the same network segment, otherwise the initialization might fail.

### Procedure

- 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 Camera in the address bar, and then press the Enter key.

Figure 4-1 Device Initialization

The screenshot shows a web browser window titled "Device Initialization". It contains several input fields and a "Confirm" button at the bottom. The "Username" field is pre-filled with "admin". The "Password" field is empty, with a red warning message below it: "The minimum pass phrase length is 8 characters". Below the password field are three buttons labeled "Weak", "Middle", and "Strong". The "Confirm Password" field is also empty. Below this field is a text instruction: "Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' ' ; : & )". There is a checkbox labeled "Email Address" which is checked, followed by an empty text field. Below this field is a note: "To reset password, please input properly or update in time." At the bottom center is a "Confirm" button.

- Step 4 Enter **Password** and **Confirm 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 ' " ; : & ).
- 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 (recommended to set for resetting your password).

**Step 6** Click **Confirm**.

The **Live** page of the Camera is displayed.


## 4.2 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** Double-click .

**Step 2** Click **Modify IP** on the homepage.

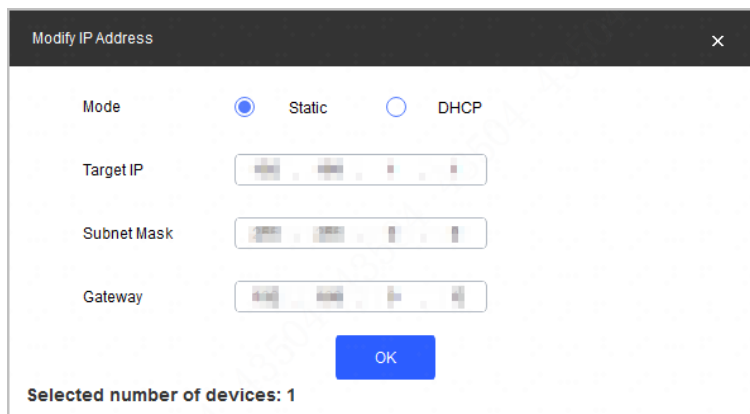
**Step 3** Select the device(s) whose IP need(s) to be changed.

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

**Step 4** Set mode, IP, subnet mask and gateway.

**Step 5** Click **OK**.

Figure 4-2 Change IP addresses in batches



## 4.3 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 "4.1 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 Internet Explorer) 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.

Figure 4-3 Live

The screenshot displays the WEB SERVICE v1.0 interface. At the top, there are tabs for 'Live', 'Query', 'Setting', 'Alarm', and 'Logout'. Below the tabs, there are controls for 'Channel' (Channel 1), 'Main Stream', 'Sub Stream', 'Protocol' (TCP), and 'Agency' (Default). A 'Get Current Status' button and a 'Record Type' dropdown are also visible. The main area is split into two video feeds. The left feed shows a blurred view of a parking lot, and the right feed shows a closer view of a vehicle. Below the video feeds, there is a 'Road Plate Info' section with three columns for 'Parking1', 'Parking2', and 'Parking3'. Each column contains fields for 'Parking Space No.', 'Parking Status', 'Plate Number', and 'Vehicle Property'. To the right of this section is a table with the following data:

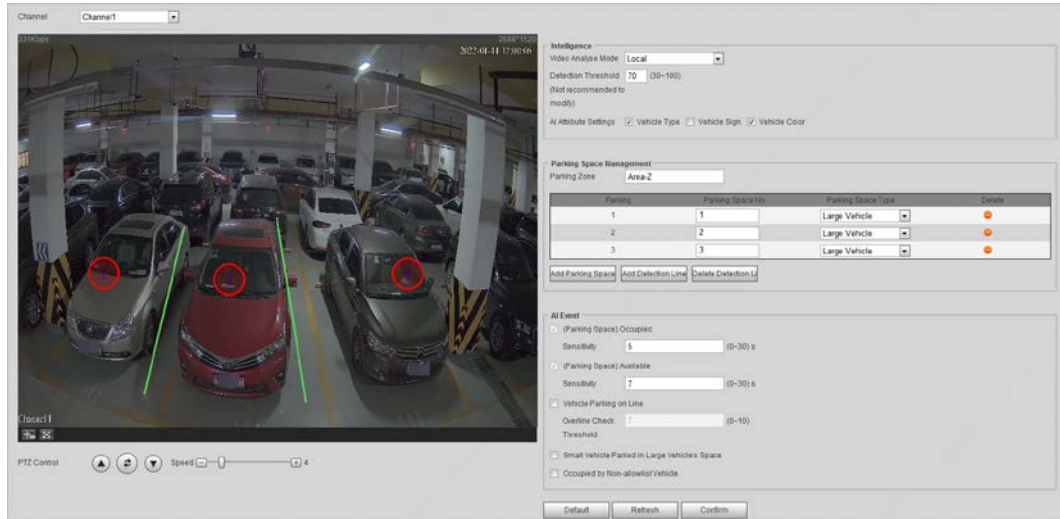
Index	Event Type	Capture Time	Channel	Space No.	Plate	Vehicle Color	Plate Size
5	(Parking Space) Available	2000-01-25 01:02:38	2	5	No Plate	Unknown	Unknown
5	(Parking Space) Available	2000-01-25 01:02:38	2	5	No Plate	Unknown	Unknown
4	(Parking Space) Available	2000-01-25 01:02:38	2	4	No Plate	Unknown	Unknown
3	(Parking Space) Available	2000-01-25 01:02:50	1	2	No Plate	Unknown	Unknown
2	(Parking Space) Available	2000-01-25 01:02:38	1	3	No Plate	Unknown	Unknown
1	(Parking Space) Available	2000-01-25 01:02:38	1	1	No Plate	Unknown	Unknown

# 5 Configuring Parking Space

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

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

Figure 5-1 Parking space management



Step 2 Under **Parking Space Management** section, enter the **Parking Zone** name, and then click **Add Parking Space** to add parking spaces for the current camera to monitor.

- Type and number are required for each parking space.
- The number of parking spaces that can be detected varies depending on the model of the Camera.

Step 3 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.

Step 4 Click **Confirm**.

# 6 Update

## 6.1 Update by ConfigTool

### Prerequisites

- You have obtained the ConfigTool installation package. If not, go to our official website, and then obtain the tool from **Support > Download Center > Tools > Toolbox**.
- The IP address of the PC installed with ConfigTool and that of the device are in the same network segment.

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.

### Procedure

Step 1 Open ConfigTool.

Step 2 Click **Device Upgrade**.


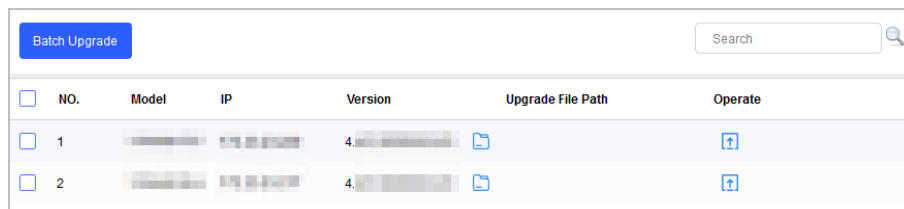





- Update device one by one
  1. Click  next to the device that you want to update, and then select the specific update file and click **Open**.

Figure 6-1 Update



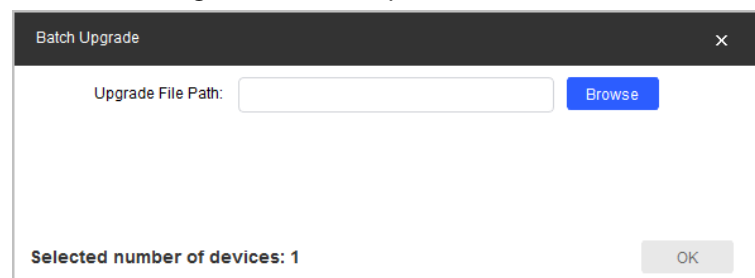
<input type="checkbox"/>	NO.	Model	IP	Version	Upgrade File Path	Operate
<input type="checkbox"/>	1			4.		
<input type="checkbox"/>	2			4.		

2. Click  to start upgrading.

After update is complete, a **Notice** dialog box will be displayed indicating the device will be rebooted. Then the device reboots automatically.

- Update devices in batches
  1. Select multiple devices to be updated, and then click **Batch Upgrade**.
  2. Click **Browse** to select the files that need to be updated.

Figure 6-2 Select update file



3. Click **OK**.





If the device is disconnected from network during updating, as long as the ConfigTool stays on the update page, the update will resume when the connection is restored.

## 6.2 Update on Web Client

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, and might differ from the actual page.

Figure 6-3 Upgrade

The screenshot shows the 'System Upgrade' web interface. It has a dark header bar with the title 'System Upgrade'. Below the header, there are two main sections: 'File Upgrade' and 'Online Upgrade'. The 'File Upgrade' section contains a text input field labeled 'Select Firmware File', followed by 'Import' and 'Upgrade' buttons. The 'Online Upgrade' section contains a checkbox labeled 'Auto-check for updates' which is checked, followed by a 'Confirm' button. Below this, it shows 'System Version' with a progress bar and 'Build Date: 2020-06-08', followed by a 'Manual Check' button.

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.