HIKVISION

Camara para estacionamientos

Manual de uso

UD.6L0201D1673A01

User Manual

This user manual is intended for users of Parking Camera. It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, SECURITY BREACHES, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF OR RELIANCE ON THIS MANUAL, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY OR CERTAIN DAMAGES, SO SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

Privacy Notice

Surveillance laws vary by jurisdiction. Check all relevant laws in your jurisdiction before using this product for surveillance purposes to ensure that your use of this product conforms.

Support

Should you have any questions, please do not hesitate to contact your local dealer.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with “CE” and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information, see www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information, see www.recyclethis.info.

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into ‘Warnings’ and ‘Cautions’:

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

⚡	⚠
Follow these safeguards to prevent serious injury or death.	Follow these precautions to prevent potential injury or material damage.

⚡Warnings:

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. And source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Cautions:

- Make sure the power supply voltage is proper before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to it.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30℃ to 60℃, or -40℃ to 60℃ if the camera model has an “H” in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required.
- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed in its original packing.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

CHANGE THE DEFAULT PASSWORD

The default password (12345) for the Admin account is for first-time log-in purposes only. You **must** change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Table of Contents

Chapter 1Overview

1.1 Product Introduction

The parking camera is an embedded digital surveillance product that combines the traditional analog camera with the network video server. Integrating with the high bright parking space indicator, the parking camera is the camera used for detecting whether the parking spaces are occupied in the Parking Guidance and Vehicle Searching System. The camera adopts the embedded operation system and high-performance processing platform and ensures a high reliability and stability.

1.2 Performance and Function

- HD 1.3MP/3.0MP camera and is applicable to the low-illumination scene like parking lot;
- 3D DNR technology can effective reduce the image noise;
- Integrating the VCA function to intelligently detects the parking space status;
- Supports live view, recording and playback of the parking space;
- Adopts the energy-saving and high bright LED luminescent tube with high brightness and low consumption;
- Support network connection with easy installation and maintenance;
- Multiple compression standard are selectable: such as H.264, MJPEG and so on;
- Supports accessing by the web browser to realize the live view, parameter configuration, checking status and network storage;
- Remote upgrading and maintenance.

Chapter 2 System Requirement

Operating System: Microsoft Windows XP SP1 and above version / Vista / Win7 / Server 2003 / Server 2008 32bits

CPU: Intel Pentium IV 3.0 GHz to Core i7-4000 series or higher, depending on different video resolutions

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 7.0 and above version, Safari 5.02 and above version, Mozilla Firefox 3.5 and above version and Google Chrome8 and above versions.

Chapter 3 Network Connection

Before you start:

- If you want to set the parking camera via a LAN (Local Area Network), please refer to *Section 3.1* ***Setting the Parking Camera over the LAN***.
- If you want to set the parking camera via a WAN (Wide Area Network), please refer to *Section 3.2* ***Setting the Parking Camera over the WAN***.

3.1 Setting the Parking Camera over the LAN

Purpose:

To view and configure the camera via a LAN, you need to connect the parking camera in the same subnet with your computer, and install the SADP or iVMS-4200 software to search and change the IP address of the parking camera.

Note: For the detailed introduction of SADP, please refer to Appendix 1.

3.1.1 Wiring over the LAN

The following figures show the two ways of cable connection of a parking camera and a computer:

Purpose:

- To test the parking camera, you can directly connect the parking camera to the computer with a network cable as shown in Figure 3-1.
- Refer to the Figure 3-2 to set parking camera over the LAN via a switch or a router.

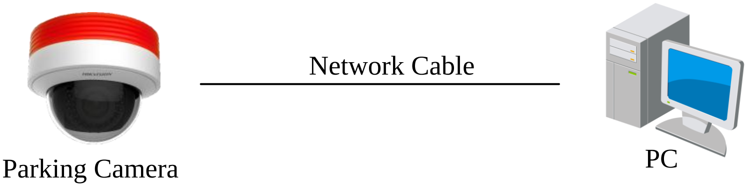


Figure 3-1 Connecting Directly

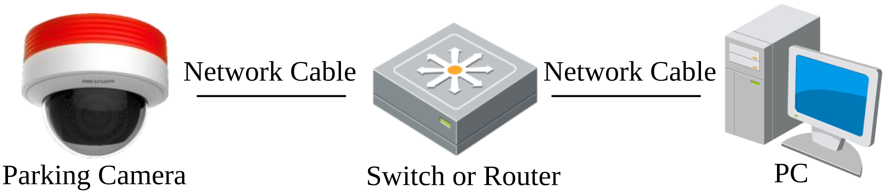


Figure 3-2 Connecting via a Switch or a Router

3.1.2 Detecting and Changing the IP Address

You need the IP address to visit the parking camera.

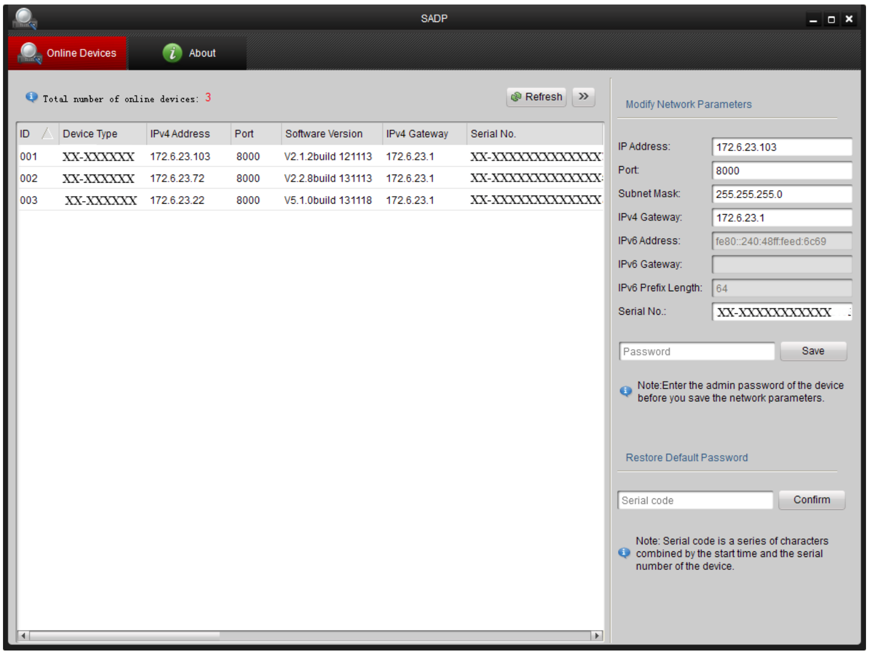
Steps:

1. To get the IP address, you can choose either of the following methods:
   - ♦ Use SADP, a software tool which can automatically detect the online parking cameras in the LAN and list the device information including IP address, subnet mask, port number, device serial number, device version, etc., shown in Figure 2-3.
   - ♦ Use the iVMS-4200 client software to list the online devices. Please refer to the user manual of iVMS-4200 client software for detailed information.
2. Change the IP address and subnet mask to the same subnet as that of your computer.
3. Enter the IP address of parking camera in the address field of the web browser to view the live video.

Notes:

- The default IP address is 192.0.0.64 and the port number is 8000.
- For accessing the parking camera from different subnets, please set the gateway for the parking camera after you logged in. For detailed information, please refer to *Section 7.3.1* ***Configuring TCP/IP Settings***.

YOU MUST CHANGE THE DEFAULT PASSWORD – The default Admin account password (12345) is for first-time log-in purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.
See Section 12.1, Managing User Accounts.



Total number of online devices: 3

ID	Device Type	IPv4 Address	Port	Software Version	IPv4 Gateway	Serial No.
001	XX-XXXXXX	172.6.23.103	8000	V2.1.2build 121113	172.6.23.1	XX-XXXXXXXXXXXXX
002	XX-XXXXXX	172.6.23.72	8000	V2.2.8build 131113	172.6.23.1	XX-XXXXXXXXXXXXX
003	XX-XXXXXX	172.6.23.22	8000	V5.1.0build 131118	172.6.23.1	XX-XXXXXXXXXXXXX

IP Address:	172.6.23.103
Port:	8000
Subnet Mask:	255.255.255.0
IPv4 Gateway:	172.6.23.1
IPv6 Address:	fe80::240:48ff:feed:6c69
IPv6 Gateway:	
IPv6 Prefix Length:	64
Serial No.:	XX-XXXXXXXXXXX

Password

Note:Enter the admin password of the device before you save the network parameters.

Serial code

Note: Serial code is a series of characters combined by the start time and the serial number of the device.

Figure 3-3 SADP Interface

3.2 Setting the Parking Camera over the WAN

Purpose:

This section explains how to connect the parking camera to the WAN with a static IP or a dynamic IP.

3.2.1 Static IP Connection

Before you start:

Please apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the parking camera via a router or connect it to the WAN directly.

- **Connecting the parking camera via a router**

Steps:

1. Connect the parking camera to the router.
2. Assign a LAN IP address, the subnet mask and the gateway. Refer to *Section 3.1.2* ***Detecting and Changing the IP Address*** for detailed IP address configuration of the camera.
3. Save the static IP in the router.
4. Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

Note: Refer to Appendix 2 for detailed information about port mapping.

5. Visit the parking camera through a web browser or the client software over the internet.

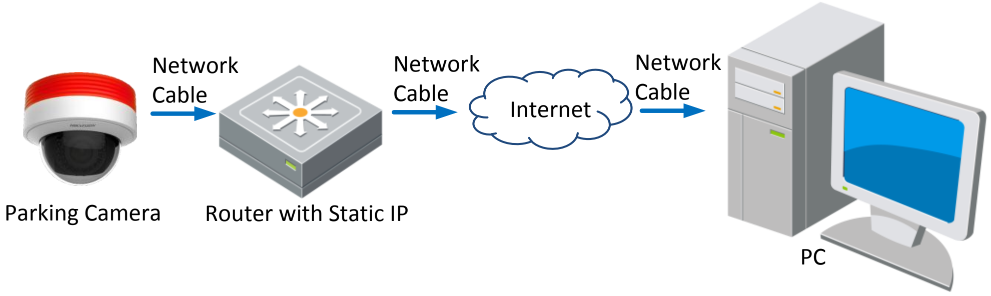


Figure 3-4 Accessing the Camera through Router with Static IP

- Connecting the parking camera with static IP directly

You can also save the static IP in the camera and directly connect it to the internet without using a router. Refer to *Section 3.1.2* ***Detecting and Changing the IP Address*** for detailed IP address configuration of the camera.

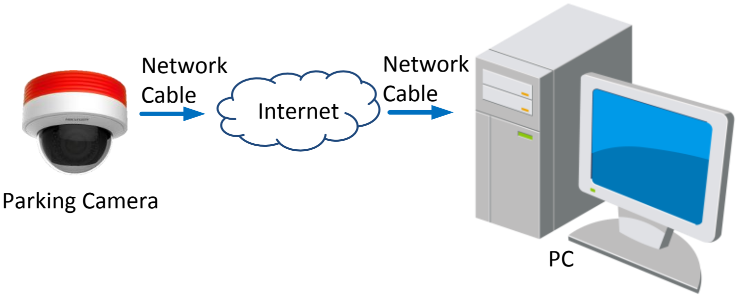


Figure 3-5 Accessing the Camera with Static IP Directly

3.2.2 Dynamic IP Connection

Before you start:

Please apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the parking camera to a modem or a router.

- **Connecting the parking camera via a router**

Steps:

1. Connect the parking camera to the router.
2. In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to *Section 3.1.2* ***Detecting and Changing the IP Address*** for detailed LAN configuration.
3. In the router, set the PPPoE user name, password and confirm the password.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. Set port mapping. E.g. 80, 8000, and 554 ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with port mapping.

Note: Refer to Appendix 2 for detailed information about port mapping.

5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

- **Connecting the parking camera via a modem**

Purpose:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the parking camera. Refer to *Section*

*7.3.3 **Configuring PPPoE Settings*** for detailed configuration.

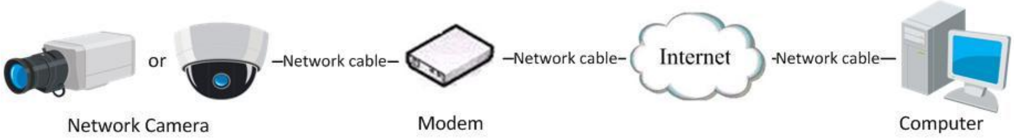


Figure 3-6 Accessing the Camera with Dynamic IP

Note: The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

- ♦ Normal Domain Name Resolution

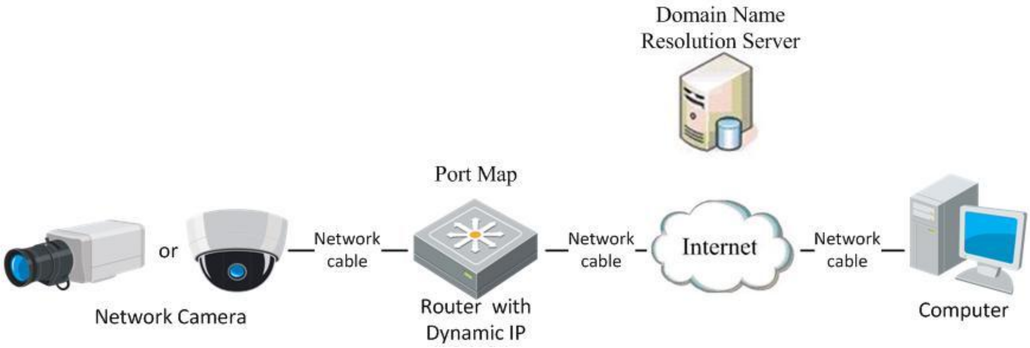


Figure 3-7 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the parking camera. Refer to *Section 7.3.4 **Configuring DDNS Settings*** for detailed configuration.
3. Visit the camera via the applied domain name.

- ♦ Private Domain Name Resolution

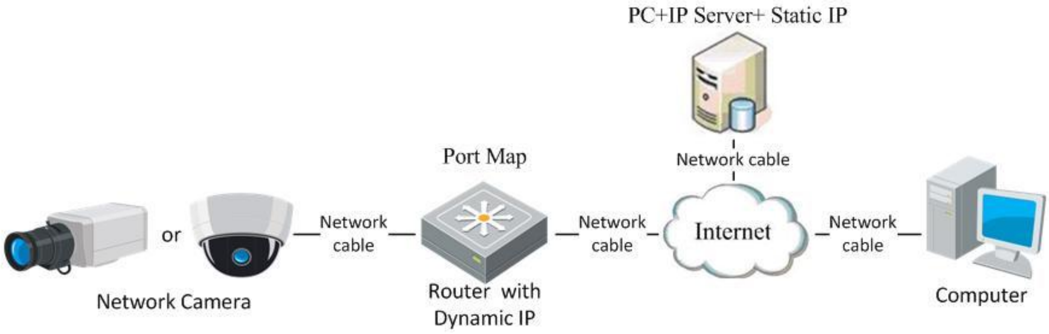


Figure 3-8 Private Domain Name Resolution

Steps:

1. Install and run the IP Server software in a computer with a static IP.
2. Access the parking camera through the LAN with a web browser or the client software.
3. Enable DDNS and select IP Server as the protocol type. Refer to *Section*

7.3.4 ***Configuring DDNS Settings*** for detailed configuration.

Chapter 4 Access to the Parking Camera

4.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. Input the IP address of the parking camera in the address bar, e.g., 192.0.0.64 and press the **Enter** key to enter the login interface.
3. Input the user name and password and click **Login**.

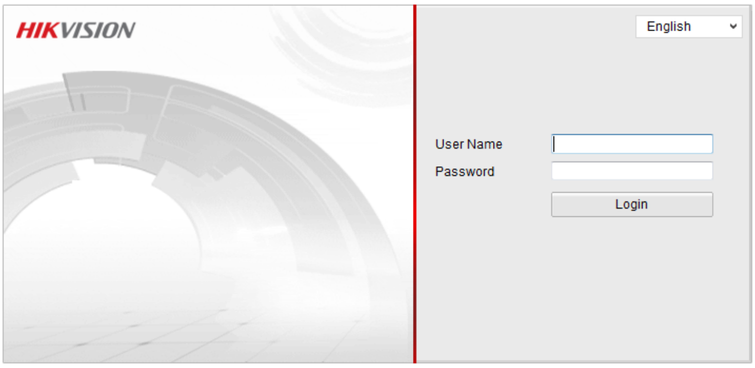
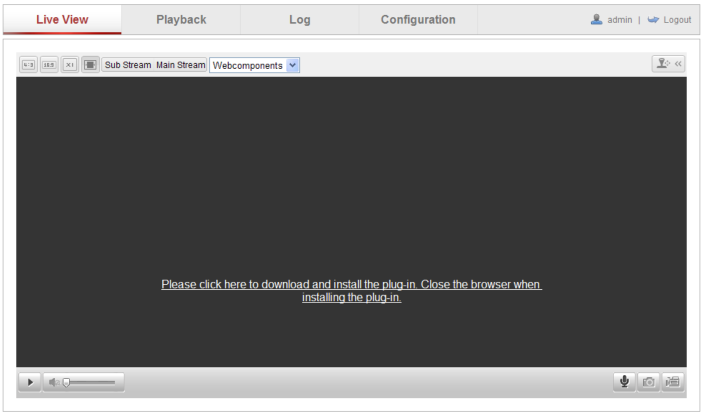


Figure 4-1 Login Interface

<u>YOU MUST CHANGE THE DEFAULT PASSWORD</u> – The default Admin account password (12345) is for first-time log-in purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

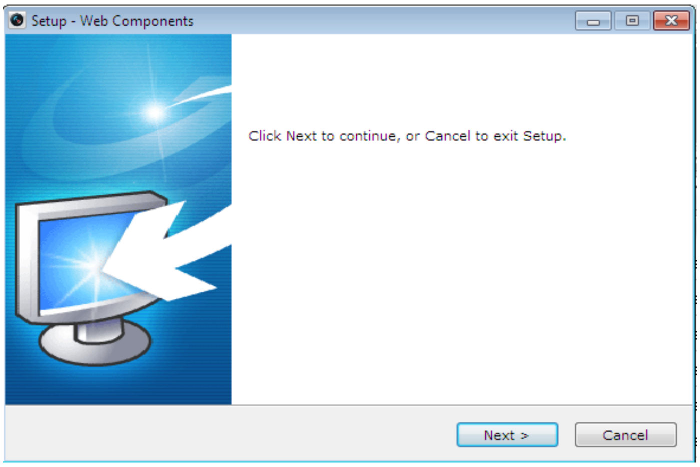
See Section 12.1, Managing User Accounts.

4. Install the plug-in before viewing the live video and operating the camera. Please follow the installation prompts to install the plug-in.



Please click here to download and install the plug-in. Close the browser when installing the plug-in.

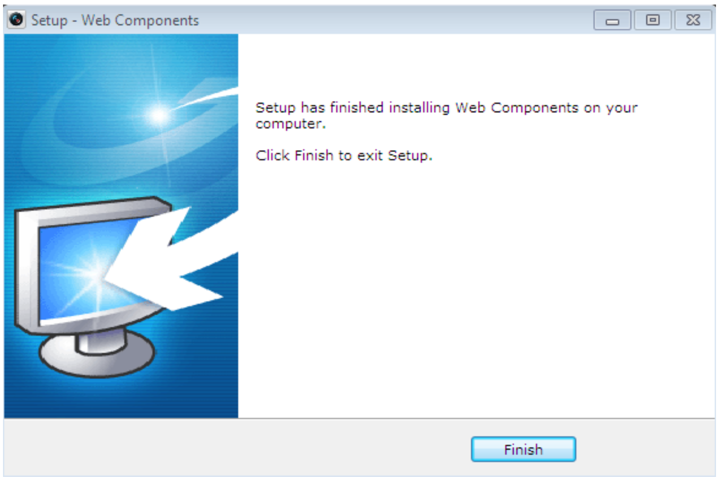
Figure 4-2 Download and Install Plug-in



Setup - Web Components

Click Next to continue, or Cancel to exit Setup.

Figure 4-3 Install Plug-in (1)



Setup - Web Components

Setup has finished installing Web Components on your computer.

Click Finish to exit Setup.

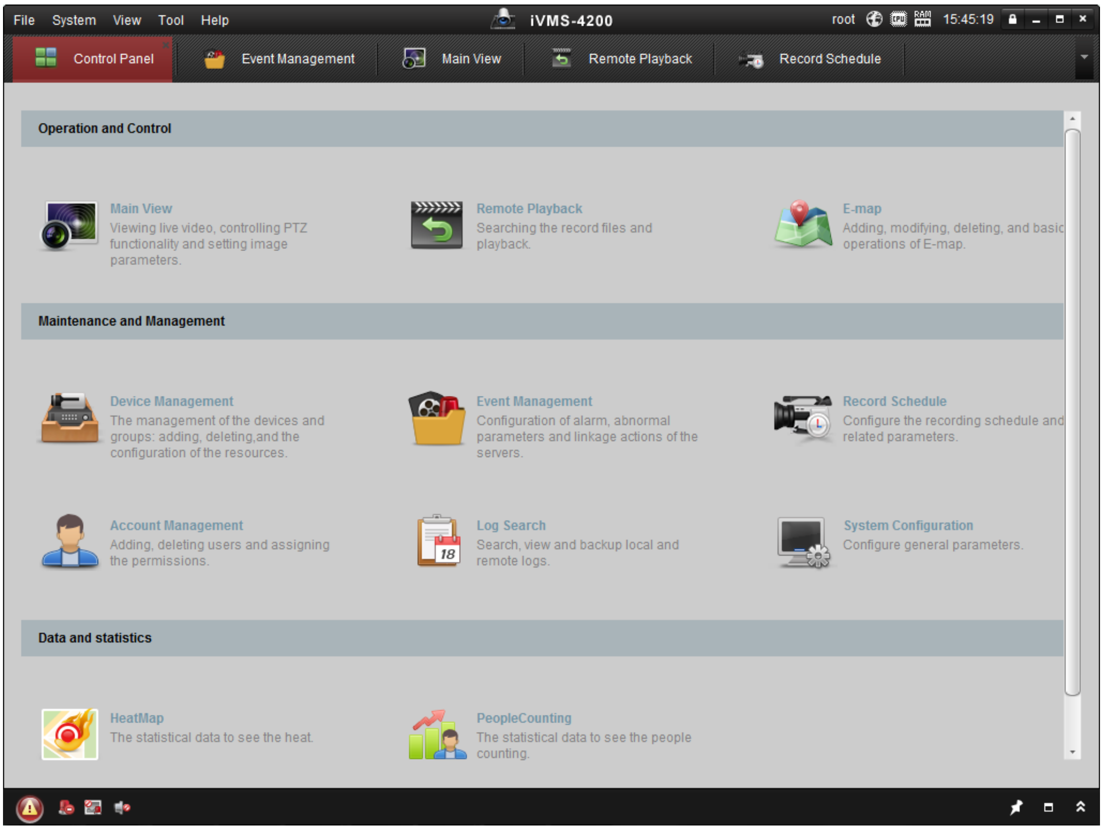
Figure 4-4 Install Plug-in (2)

Note: You may have to close the web browser to install the plug-in. Please reopen the web browser and log in again after installing the plug-in.

4.2 Accessing by Client Software

The product CD contains the iVMS-4200 client software. You can view the live video and manage the camera with the software.

Follow the installation prompts to install the software. The control panel and live view interface of iVMS-4200 client software are shown as below.



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Maintenance and Management

Device Management
The management of the devices and groups: adding, deleting,and the configuration of the resources.

Event Management
Configuration of alarm, abnormal parameters and linkage actions of the servers.

Record Schedule
Configure the recording schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Search, view and backup local and remote logs.

System Configuration
Configure general parameters.

Data and statistics

HeatMap
The statistical data to see the heat.

PeopleCounting
The statistical data to see the people counting.

Figure 4-5 iVMS-4200 Control Panel

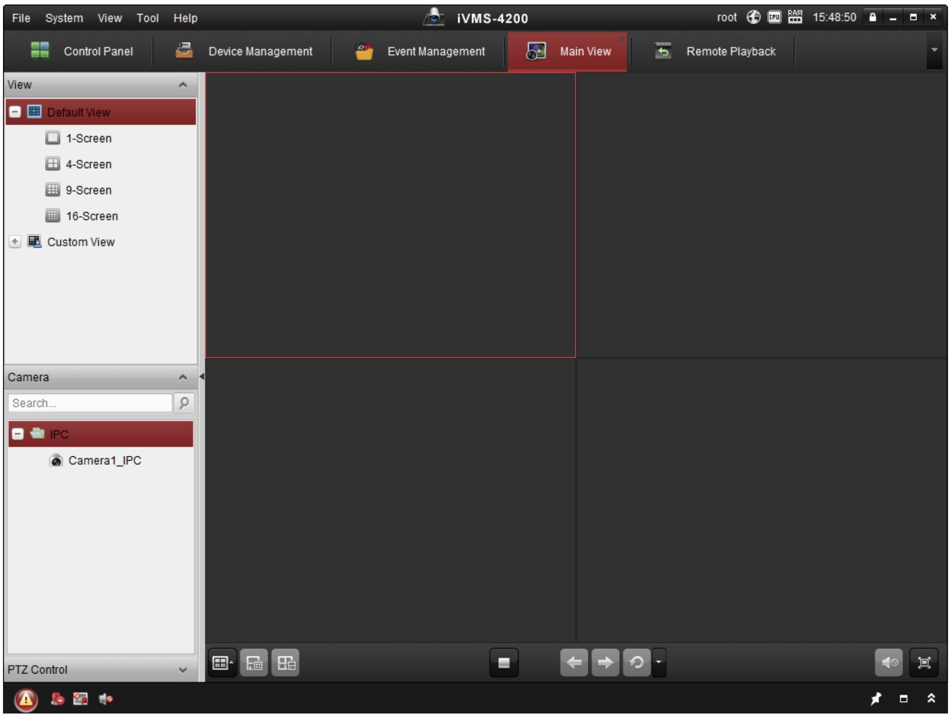


Figure 4-6 iVMS-4200 Main View

Note: For detailed information about the software, please refer to the user manual of the iVMS-4200.

Chapter 5 Wi-Fi Settings

Purpose:

By connecting to the wireless network, you don't need to use cable of any kind for network connection, which is very convenient for the actual surveillance application.

Note: This chapter is only applicable for the cameras with the built-in Wi-Fi module.

5.1 Configuring Wi-Fi Connection in Manage and Ad-hoc Modes

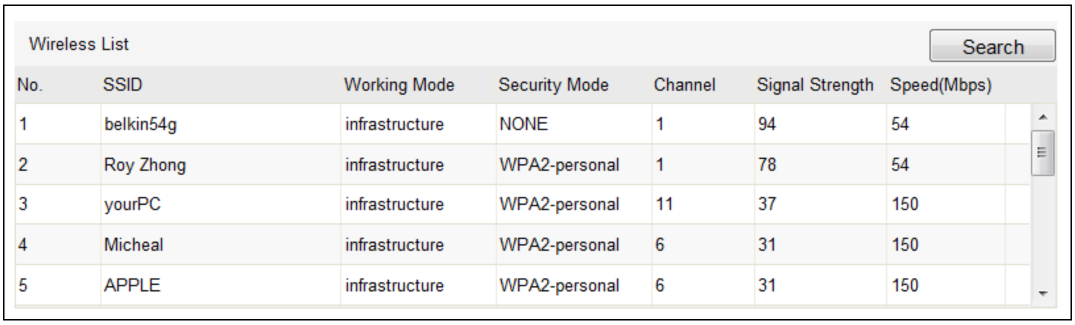
Before you start:

A wireless network must be configured.

- **Wireless Connection in Manage Mode**

Steps:

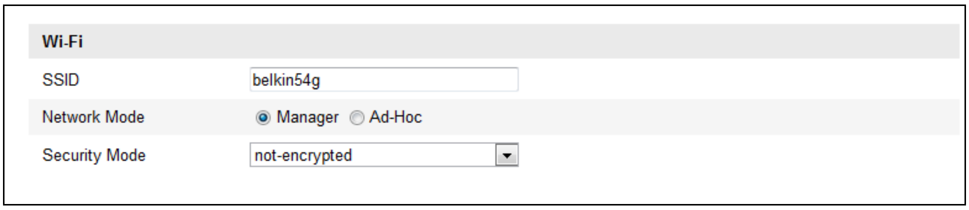
1. Enter the Wi-Fi configuration interface.
   Configuration> Advanced Configuration> Network> Wi-Fi



No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
1	belkin54g	infrastructure	NONE	1	94	54
2	Roy Zhong	infrastructure	WPA2-personal	1	78	54
3	yourPC	infrastructure	WPA2-personal	11	37	150
4	Micheal	infrastructure	WPA2-personal	6	31	150
5	APPLE	infrastructure	WPA2-personal	6	31	150

Figure 5-1 Wireless Network List

2. Click **Search** to search the online wireless connections.
3. Click to choose a wireless connection on the list.



Wi-Fi

SSID: belkin54g

Network Mode: ● Manager ○ Ad-Hoc

Security Mode: not-encrypted

Figure 5-2 Wi-Fi Setting- Manage Mode

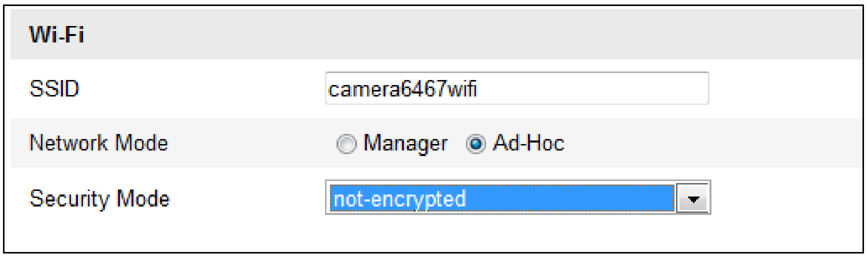
4. Check the checkbox to select the *Network mode* as *Manage*, and the *Security mode* of the network is automatically shown when you select the wireless network, please do not change it manually.
   Note: These parameters are exactly identical with those of the router.
5. Enter the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

- **Wireless Connection in Ad-hoc Mode**

If you choose the Ad-hoc mode, you don't need to connect the wireless camera via a router. The scenario is the same as you connect the camera and the PC directly with a network cable.

Steps:

1. Choose Ad-hoc mode.



Wi-Fi

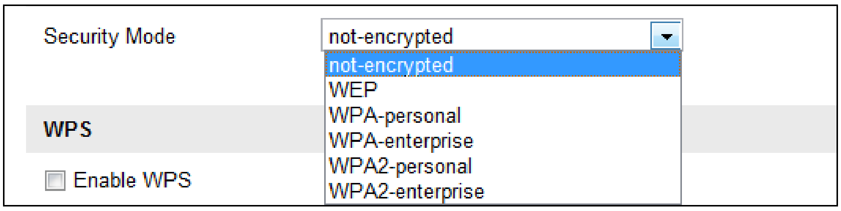
SSID: camera6467wifi

Network Mode: ○ Manager ● Ad-Hoc

Security Mode: not-encrypted

Figure 5-3 Wi-Fi Setting- Ad-hoc

2. Customize a SSID for the camera.
3. Choose the Security Mode of the wireless connection.



Security Mode: not-encrypted

Figure 5-4 Security Mode- Ad-hoc Mode

4. Enable the wireless connection function for your PC.
5. On the PC side, search the network and you can see the SSID of the camera listed.

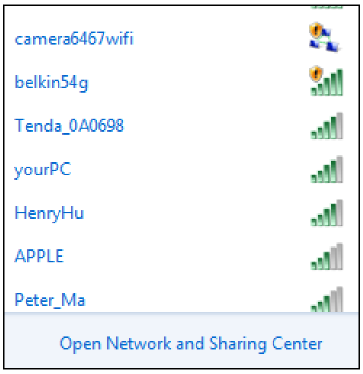
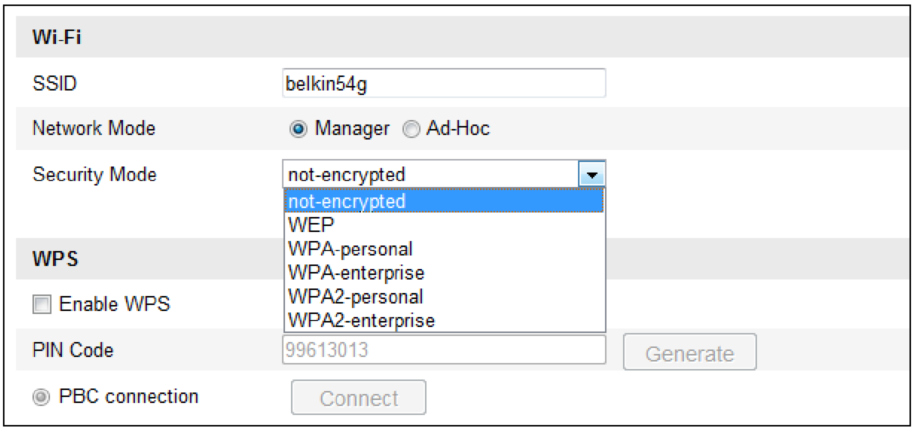


Figure 5-5 Ad-hoc Connection Point

6. Choose the SSID and connect.

Security Mode Description:



Wi-Fi

SSID: belkin54g

Network Mode: ● Manager ○ Ad-Hoc

Security Mode: not-encrypted

WPS

□ Enable WPS

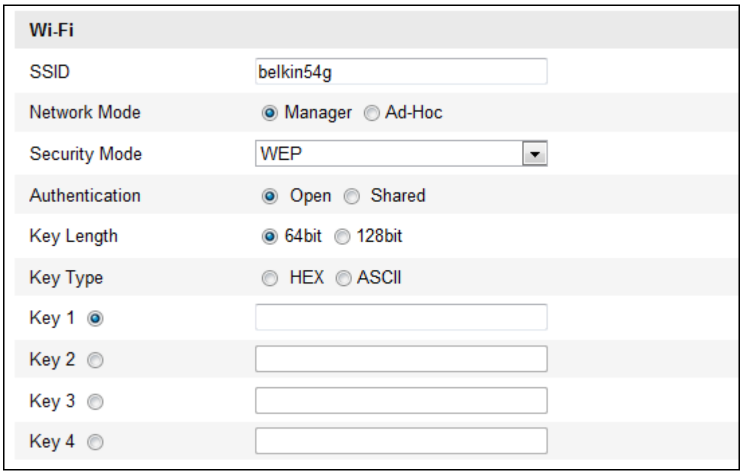
PIN Code: 99613013

○ PBC connection

Figure 5-6 Security Mode

You can choose the Security Mode as not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, and WPA2-enterprise.

WEP mode:



Wi-Fi

SSID: belkin54g

Network Mode: ● Manager ○ Ad-Hoc

Security Mode: WEP

Authentication: ● Open ○ Shared

Key Length: ● 64bit ○ 128bit

Key Type: ○ HEX ○ ASCII

Key 1 ●

Key 2 ○

Key 3 ○

Key 4 ○

Figure 5-7 WEP Mode

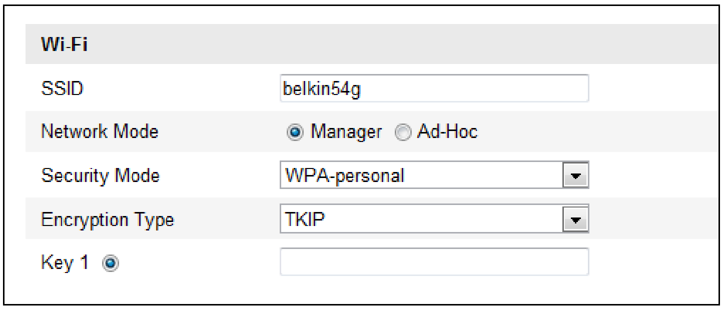
- Authentication - Select Open or Shared Key System Authentication, depending on the method used by your access point. Not all access points have this option, in which case they probably use Open System, which is sometimes known as SSID Authentication.
- *Key length* - This sets the length of the key used for the wireless encryption, 64 or 128 bit. The encryption key length can sometimes be shown as 40/64 and 104/128.
- Key type - The key types available depend on the access point being used. The following options are available:

  HEX - Allows you to manually enter the hex key.

  ASCII - In this method the string must be exactly 5 characters for 64-bit WEP and 13 characters for 128-bit WEP.

WPA-personal and WPA2-personal Mode:

Enter the required Pre-shared Key for the access point, which can be a hexadecimal number or a passphrase.



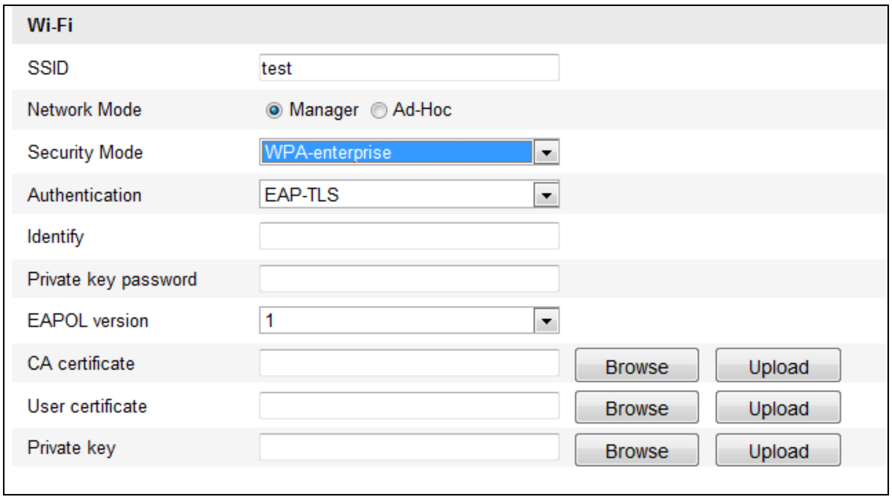
Wi-Fi	
SSID	belkin54g
Network Mode	● Manager ○ Ad-Hoc
Security Mode	WPA-personal
Encryption Type	TKIP
Key 1 ●	

Figure 5-8 Security Mode- WPA-personal

WPA- enterprise and WPA2-enterprise Mode:

Choose the type of client/server authentication being used by the access point; EAP-TLS or EAP-PEAP.

EAP-TLS



Wi-Fi			
SSID	test		
Network Mode	● Manager ○ Ad-Hoc		
Security Mode	WPA-enterprise		
Authentication	EAP-TLS		
Identify			
Private key password			
EAPOL version	1		
CA certificate		Browse	Upload
User certificate		Browse	Upload
Private key		Browse	Upload

Figure 5-9 EAP-TLS

- Identity - Enter the user ID to present to the network.
- Private key password – Enter the password for your user ID.
- EAPOL version - Select the version used (1 or 2) in your access point.
- CA Certificates - Upload a CA certificate to present to the access point for authentication.

EAP-PEAP:

- User Name - Enter the user name to present to the network
- Password - Enter the password of the network
- PEAP Version - Select the PEAP version used at the access point.
- Label - Select the label used by the access point.
- EAPOL version - Select version (1 or 2) depending on the version used at the access point
- CA Certificates - Upload a CA certificate to present to the access point for authentication

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network* *devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

5.2 Easy Wi-Fi Connection with WPS function

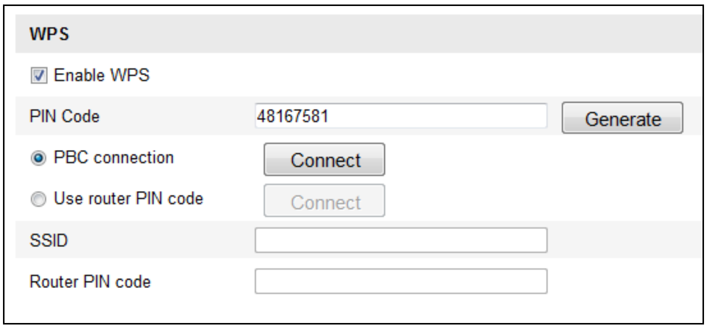
Purpose:

The setting of the wireless network connection is never easy. To avoid the complex setting of the wireless connection you can enable the WPS function.

WPS (Wi-Fi Protected Setup) refers to the easy configuration of the encrypted connection between the device and the wireless router. The WPS makes it easy to add new devices to an existing network without entering long passphrases. There are two modes of the WPS connection, the PBC mode and the PIN mode.

Note: If you enable the WPS function, you do not need to configure the parameters such as the encryption type and you don't need to know the key of the wireless connection.

Steps:



WPS

☑ Enable WPS

PIN Code: 48167581 [Generate]

● PBC connection [Connect]

○ Use router PIN code [Connect]

SSID:

Router PIN code:

Figure 5-10 Wi-Fi Settings - WPS

PBC Mode:

PBC refers to the Push-Button-Configuration, in which the user simply has to push a button, either an actual or virtual one (as the [Connect] button on the configuration interface of the IE browser), on both the Access Point (and a registrar of the network) and the new wireless client device.

1. Check the checkbox of ☑ Enable WPS to enable WPS.
2. Choose the connection mode as PBC.

● PBC connection [Connect]

Note: Support of this mode is mandatory for both the Access Points and the connecting devices.

3. Check on the Wi-Fi router to see if there is a WPS button. If yes push the button and you can see the indicator near the button start flashing, which means the WPS function of the router is enabled. For detailed operation, please see the user guide of the router.

4. Push the WPS button to enable the function on the camera.

If there is not a WPS button on the camera, you can also click the virtual button to enable the PBC function on the web interface.

5. Click **Connect** button.

● PBC connection   Connect

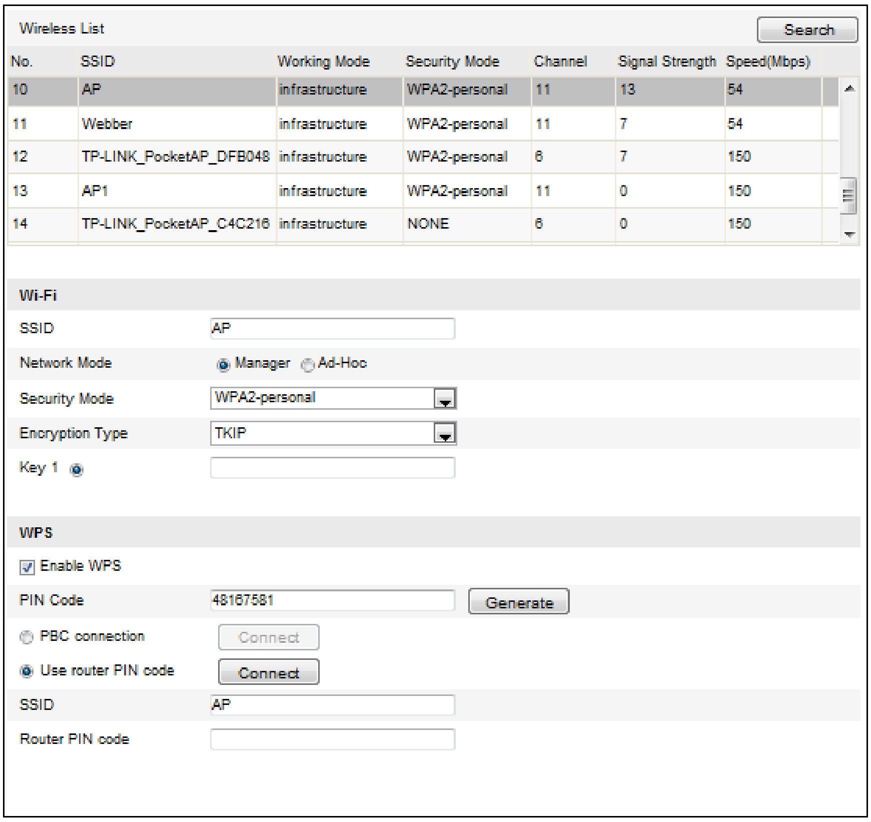
When the PBC mode is both enabled in the router and the camera, the camera and the wireless network is connected automatically.

PIN Mode:

The PIN mode requires a Personal Identification Number (PIN) to be read from either a sticker or the display on the new wireless device. This PIN must then be entered to connect the network, usually the Access Point of the network.

Steps:

1. Choose a wireless connection on the list and the SSID is shown.



Wireless List   Search

No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
10	AP	infrastructure	WPA2-personal	11	13	54
11	Webber	infrastructure	WPA2-personal	11	7	54
12	TP-LINK_PocketAP_DFB048	infrastructure	WPA2-personal	6	7	150
13	AP1	infrastructure	WPA2-personal	11	0	150
14	TP-LINK_PocketAP_C4C216	infrastructure	NONE	6	0	150

Wi-Fi

SSID	AP
Network Mode	● Manager ○ Ad-Hoc
Security Mode	WPA2-personal
Encryption Type	TKIP
Key 1 ●	

WPS

☑ Enable WPS

PIN Code	48167581 Generate
○ PBC connection	Connect
● Use router PIN code	Connect
SSID	AP
Router PIN code	

Figure 5-11 Wi-Fi Settings – WPS PIN Mode

2. Choose Use route PIN code.

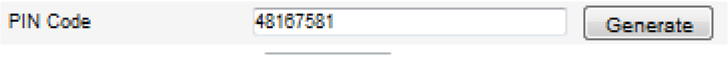
If the PIN code is generated from the router side, you should enter the PIN code you get from the router side in the **Router PIN code** field.

3. Click **Connect**.

Or

You can generate the PIN code on the camera side. And the expired time for the PIN code is 120 seconds.

1. Click Generate.



PIN Code 48167581 Generate

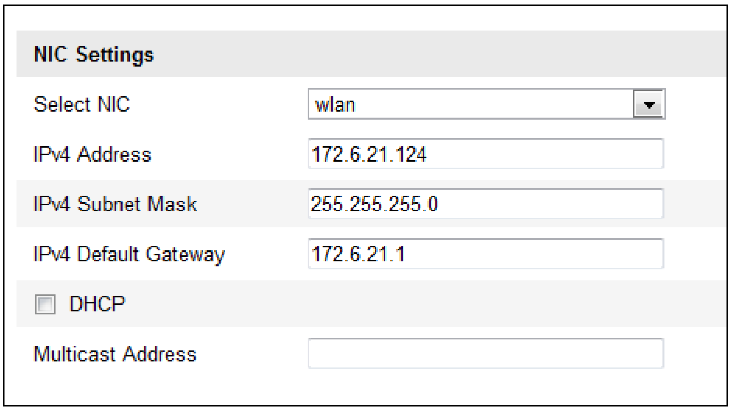
2. Enter the code to the router, in the example, enter 48167581 to the router.

5.3 IP Property Settings for Wireless Network Connection

The default IP address of wireless network interface controller is 192.168.1.64. When you connect the wireless network you can change the default IP.

Steps:

1. Enter the TCP/IP configuration interface.
   Configuration> Advanced Configuration> Network> TCP/IP
   Or
   Configuration> Basic Configuration> Network> TCP/IP



NIC Settings

Select NIC	wlan
IPv4 Address	172.6.21.124
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	172.6.21.1
□ DHCP	
Multicast Address	

Figure 5-12 TCP/IP Settings

2. Select the NIC as wlan.
3. Customize the IPv4 address, the IPv4 Subnet Mask and the Default Gateway.
   The setting procedure is the same with that of LAN.
   If you want to be assigned the IP address you can check the checkbox to enable the DHCP.

Chapter 6 Live View

6.1 Live View Page

Purpose:

The live view page allows you to view the real-time video, capture images, realize PTZ control, set/call presets and configure video parameters.

Log in the parking camera to enter the live view page, or you can click **Live View** on the menu bar of the main page to enter the live view page.

Descriptions of the live view page:

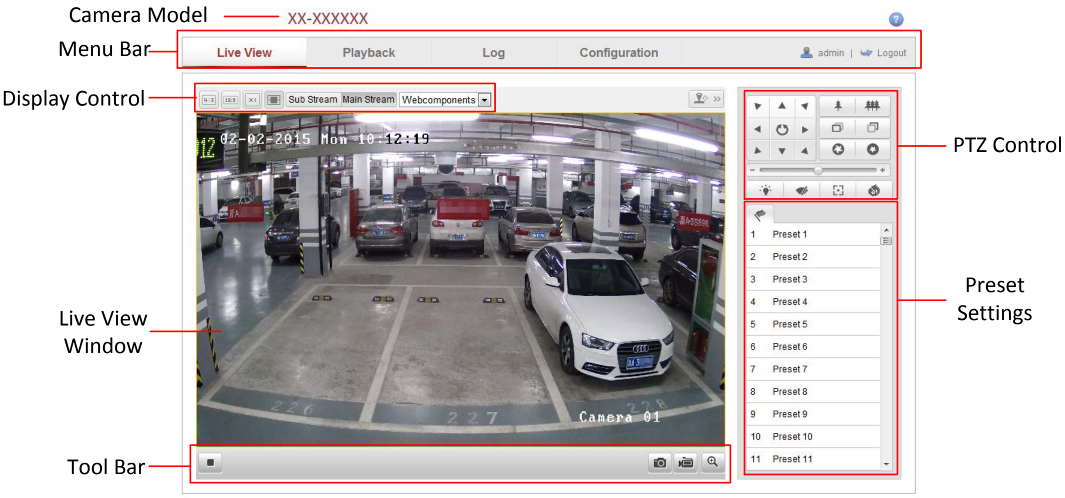


Figure 6-1 Live View Page

Camera Model:

It displays the camera model you are connecting to.

Menu Bar:

Click each tab to enter Live View, Playback, Log and Configuration page respectively.

Display Control:

Click each tab to adjust the layout and the stream type of the live view. And you can click the drop-down to select the plug-in. For IE (Internet Explorer) user, webcomponents and quick time are selectable. And for Non-IE user, webcomponents, quick time, VLC or MJPEG is selectable if they are supported by the web browser.

Live View Window:

Display the live video.

Toolbar:

Operations on the live view page, e.g., live view, capture, record, audio on/off, two-way audio, etc.

PTZ Control:

Panning, tilting and zooming actions of the camera and the light and wiper control. (Only available for cameras supporting PTZ function)

Preset Settings:

Set/call/delete the presets for PTZ cameras.

6.2 Starting Live View

In the live view window as shown in Figure 6-2, click ▶ on the toolbar to start the live view of the camera.

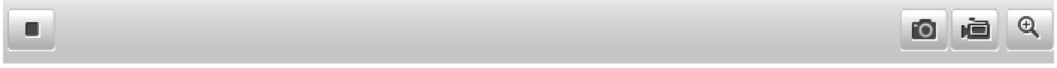


Figure 6-2 Live View Toolbar

Table 6-1 Descriptions of the Toolbar

Icon	**Description**
▶/■	Start/Stop live view.
4:3	The window size is 4:3.
16:9	The window size is 16:9.
×1	The original widow size.
▣	Self-adaptive window size.
Main Stream	Live view with the main stream.
Sub Stream	Live view with the sub stream.
Webcomponents ▾	Click to select the third-party plug-in.
📷	Manually capture the picture.
🎥/🎥	Manually start/stop recording.
🔊/🔇	Audio on and adjust volume /Mute.
🎤/🎤	Turn on/off microphone.
🔍/🔍	Turn on/off digital zoom function.

6.3 Recording and Capturing Pictures Manually

In the live view interface, click 📷 on the toolbar to capture the live pictures or click 🎥 to record the live view. The saving paths of the captured pictures and clips can be set on the **Configuration** > **Local Configuration** page. To configure remote scheduled recording, please refer to *Section 9.2*.

Note: The captured image will be saved as JPEG file or BMP file in your computer.

6.4 Operating PTZ Control

Purpose:

In the live view interface, you can use the PTZ control buttons to realize pan/tilt/zoom control of the camera.

Before you start:

To realize PTZ control, the camera connected to the network must support the PTZ function or a pan/tilt unit has been installed to the camera. Please properly set the PTZ parameters on RS-485 settings page referring to *Section 10.8* ***RS-485 Settings***.

6.4.1 PTZ Control Panel

On the live view page, click « to show the PTZ control panel or click » to hide it.

Click the direction buttons to control the pan/tilt movements.

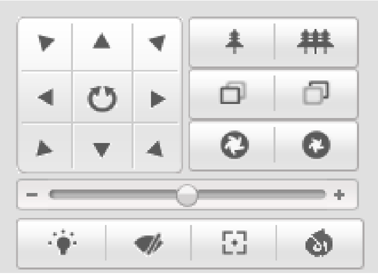


Figure 6-3 PTZ Control Panel

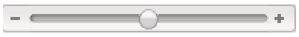
Click the zoom/iris/focus buttons to realize lens control.

Notes:

- There are 8 direction arrows (△,▽,◁, ▷,◸,◹,◺,◿) in the live view window when you click and drag the mouse in the relative positions.
- For the cameras which support lens movements only, the direction buttons are invalid.

Table 6-2 Descriptions of PTZ Control Panel

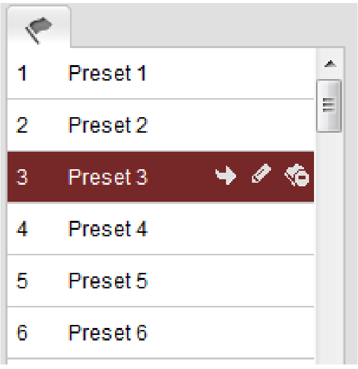
Icon	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	Light on/off
	Wiper on/off
	Auxiliary focus
	Initialize lens

	Adjust speed of pan/tilt movements

6.4.2 Setting / Calling a Preset

- Setting a Preset:

1. In the PTZ control panel, select a preset number from the preset list.



1 Preset 1
2 Preset 2
3 Preset 3
4 Preset 4
5 Preset 5
6 Preset 6

Figure 6-4 Setting a Preset

2. Use the PTZ control buttons to move the lens to the desired position.

• Pan the camera to the right or left.
• Tilt the camera up or down.
• Zoom in or out.
• Refocus the lens.

3. Click ✎ to finish the setting of the current preset.

4. You can click ⊗ to delete the preset.

***Note*:** You can configure up to 256 presets.

- Calling a Preset:

This feature enables the camera to point to a specified preset scene manually or when an event takes place.

For the defined preset, you can call it at any time to the desired preset scene.

In the PTZ control panel, select a defined preset from the list and click ➜ to call the preset.

Or you can place the mouse on the presets interface, and call the preset by typing the preset No. to call the corresponding presets.

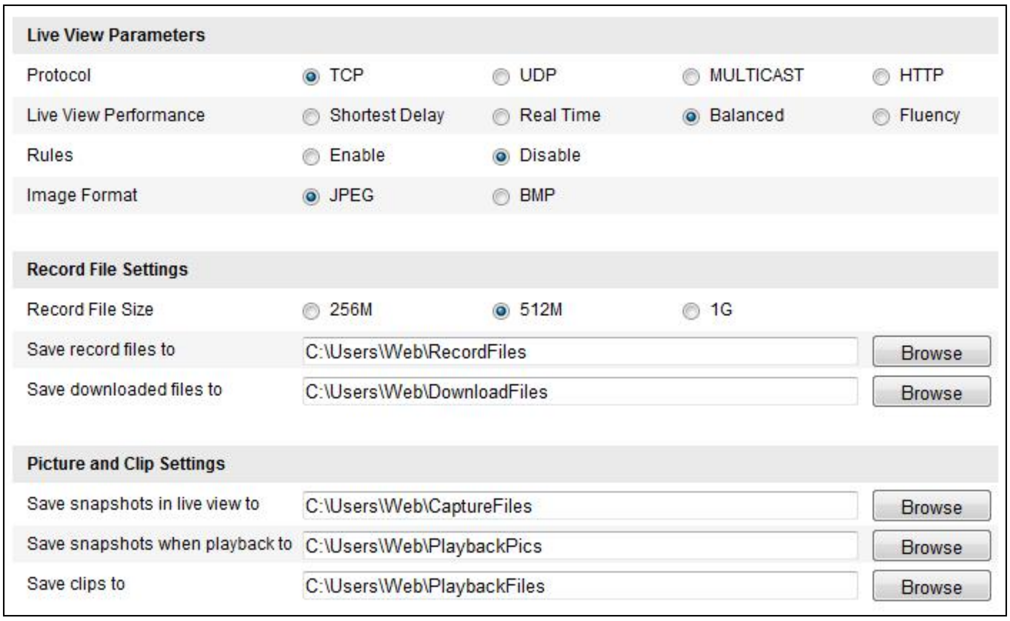
Chapter 7Parking Camera Configuration

7.1 Configuring Local Parameters

Note: The local configuration refers to the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and captured using the web browser and thus the saving paths of them are on the PC running the browser.

Steps:

1. Enter the Local Configuration interface:
   Configuration > Local Configuration



Live View Parameters					
Protocol	● TCP	○ UDP	○ MULTICAST	○ HTTP	
Live View Performance	○ Shortest Delay	○ Real Time	● Balanced	○ Fluency	
Rules	○ Enable	● Disable			
Image Format	● JPEG	○ BMP			
Record File Settings					
Record File Size	○ 256M	● 512M	○ 1G		
Save record files to	C:\Users\Web\RecordFiles				Browse
Save downloaded files to	C:\Users\Web\DownloadFiles				Browse
Picture and Clip Settings					
Save snapshots in live view to	C:\Users\Web\CaptureFiles				Browse
Save snapshots when playback to	C:\Users\Web\PlaybackPics				Browse
Save clips to	C:\Users\Web\PlaybackFiles				Browse

Figure 7-1 Local Configuration Interface

2. Configure the following settings:

- **Live View Parameters:** Set the protocol type and live view performance.
  - **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.

    TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.

    UDP: Provides real-time audio and video streams.

    HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.

    MULTICAST: It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to *Section 7.3.1* ***Configuring TCP/IP Settings***.
  - **Live View Performance:** Set the live view performance to Shortest Delay, Realtime, Balanced or Fluency.
  - **Rules:** It refers to the rules on your local browser, select enable or disable to

display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g.: enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.

- ♦ **Image Format:** Choose the image format for picture capture.

- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
  - ♦ **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.
  - ♦ **Save record files to:** Set the saving path for the manually recorded video files.
  - ♦ **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you captured with the web browser.
  - ♦ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.
  - ♦ **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
  - ♦ **Save clips to:** Set the saving path of the clipped video files in playback mode.

***Note*:** You can click **Browse** to change the directory for saving the clips and pictures.

3. Click **Save** to save the settings.

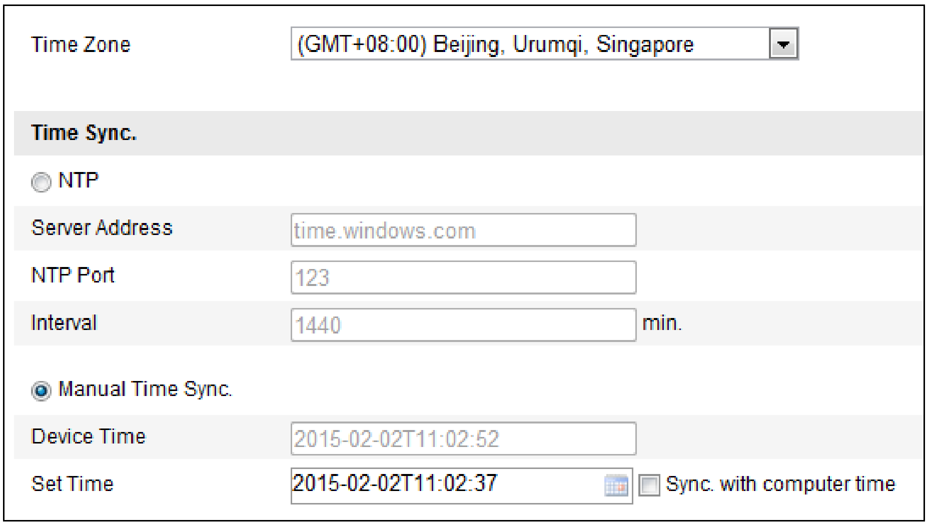
7.2 Configuring Time Settings

Purpose:

You can follow the instructions in this section to configure the time synchronization and DST settings.

Steps:

1. Enter the Time Settings interface:
   Configuration > Basic Configuration > System > Time Settings
   Or Configuration > Advanced Configuration > System > Time Settings



Time Zone: (GMT+08:00) Beijing, Urumqi, Singapore

Time Sync.

○ NTP

Server Address: time.windows.com

NTP Port: 123

Interval: 1440 min.

● Manual Time Sync.

Device Time: 2015-02-02T11:02:52

Set Time: 2015-02-02T11:02:37 □ Sync. with computer time

Figure 7-2 Time Settings

- Select the Time Zone.

 Select the Time Zone of your location from the drop-down menu.

♦ Synchronizing Time by NTP Server.

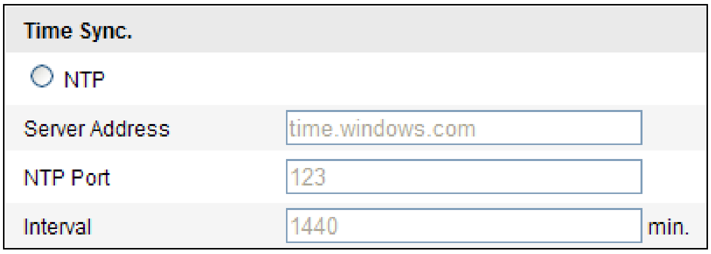
(1) Check the checkbox to enable the **NTP** function.

(2) Configure the following settings:

Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP server.



Time Sync.

○ NTP

Server Address: time.windows.com

NTP Port: 123

Interval: 1440 min.

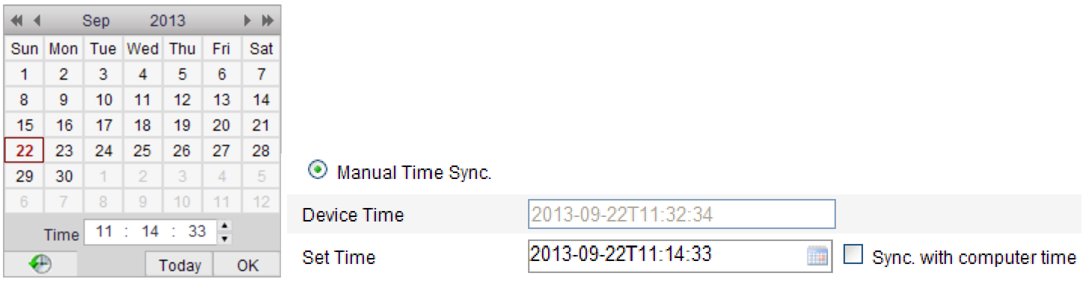
Figure 7-3 Time Sync by NTP Server

***Note*:** If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

♦ Synchronizing Time Synchronization Manually

Enable the **Manual Time Sync** function and then click 📅 to set the system time from the pop-up calendar.

Note: You can also check the **Sync with computer time** checkbox to synchronize the time of the camera with that of your computer.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

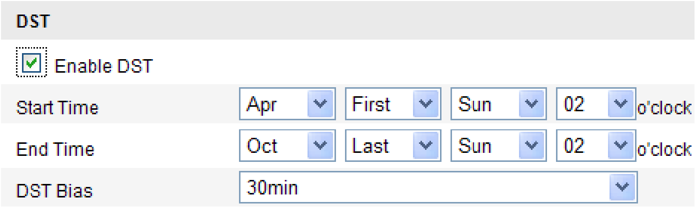
● Manual Time Sync.

Device Time: 2013-09-22T11:32:34

Set Time: 2013-09-22T11:14:33 □ Sync. with computer time

Figure 7-4 Time Sync Manually

- Click the **DST** tab page to enable the DST function and Set the date of the DST period.



DST

☑ Enable DST

Start Time: Apr, First, Sun, 02 o'clock

End Time: Oct, Last, Sun, 02 o'clock

DST Bias: 30min

Figure 7-5 DST Settings

2. Click **Save** to save the settings.

7.3 Configuring Network Settings

7.3.1 Configuring TCP/IP Settings

Purpose:

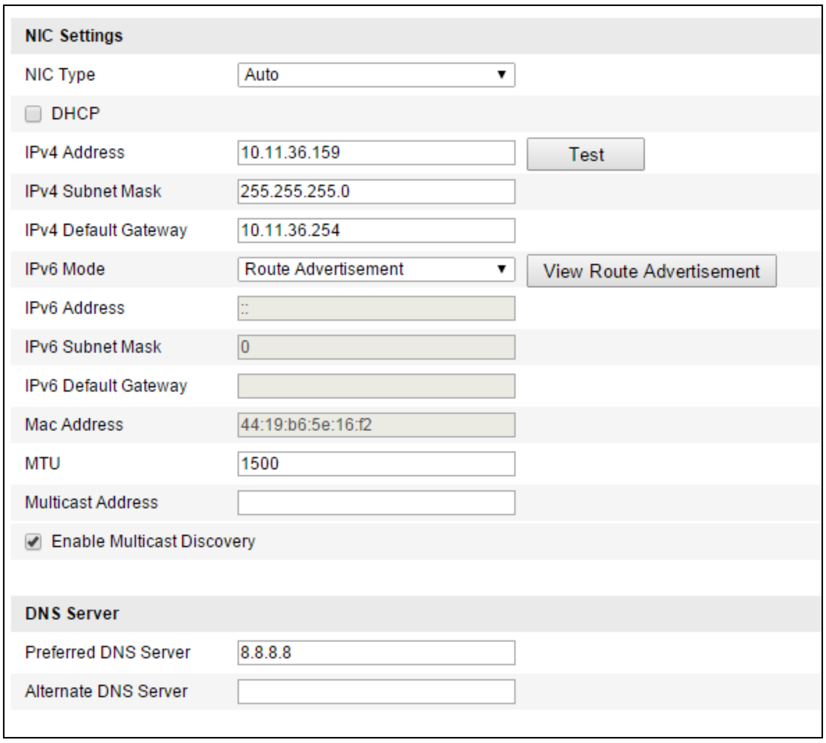
TCP/IP settings must be properly configured before you operate the camera over network. The camera supports both the IPv4 and IPv6. Both versions may be configured simultaneously without conflicting to each other, and at least one IP version should be configured.

Steps:

1. Enter TCP/IP Settings interface:

   Configuration > Basic Configuration > Network > TCP/IP

   Or Configuration > Advanced Configuration > Network > TCP/IP



NIC Settings

NIC Type	Auto ▼	
□ DHCP		
IPv4 Address	10.11.36.159	Test
IPv4 Subnet Mask	255.255.255.0	
IPv4 Default Gateway	10.11.36.254	
IPv6 Mode	Route Advertisement ▼	View Route Advertisement
IPv6 Address	::	
IPv6 Subnet Mask	0	
IPv6 Default Gateway		
Mac Address	44:19:b6:5e:16:f2	
MTU	1500	
Multicast Address		
☑ Enable Multicast Discovery		

DNS Server

Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Figure 7-6 TCP/IP Settings

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
3. (Optional) Check the checkbox of **Enable Multicast Discovery**, and then the online parking camera can be automatically detected by client software via private multicast protocol in the LAN.
4. Click **Save** to save the above settings.

Notes:

- The valid value range of MTU is 1280 ~ 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.
- A reboot is required for the settings to take effect.

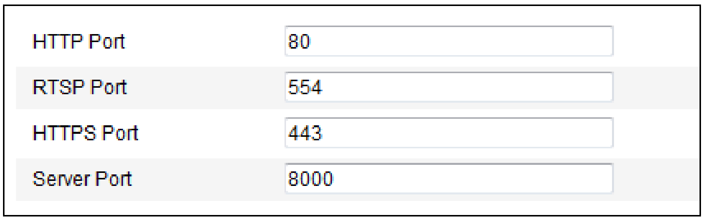
7.3.2 Configuring Port Settings

Purpose:

You can set the port No. of the camera, e.g. HTTP port, RTSP port and HTTPS port.

Steps:

1. Enter the Port Settings interface:
   Configuration > Basic Configuration > Network > Port
   Or Configuration > Advanced Configuration > Network > Port



HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000

Figure 7-7 Port Settings

2. Set the HTTP port, RTSP port, HTTPS port and server port of the camera.

   HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.

   RTSP Port: The default port number is 554 and it can be changed to any port No. ranges from 1024 to 65535.

   HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.

   Server Port: The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

3. Click **Save** to save the settings.

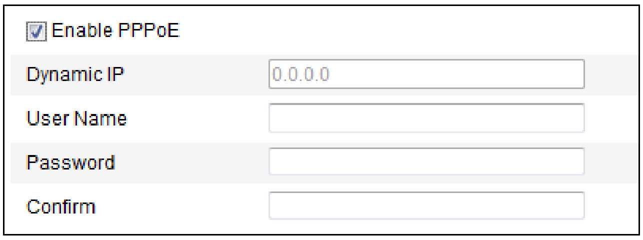
Note: A reboot is required for the settings to take effect.

7.3.3 Configuring PPPoE Settings

Steps:

1. Enter the PPPoE Settings interface:

   Configuration >Advanced Configuration > Network > PPPoE



☑ Enable PPPoE

Dynamic IP	0.0.0.0
User Name	
Password	
Confirm	

Figure 7-8 PPPoE Settings

2. Check the **Enable PPPoE** checkbox to enable this feature.
3. Enter **User Name**, **Password**, and **Confirm** password for PPPoE access.

Note: The User Name and Password should be assigned by your ISP.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. Click **Save** to save and exit the interface.

Note: A reboot is required for the settings to take effect.

7.3.4 Configuring DDNS Settings

Purpose:

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

Before you start:

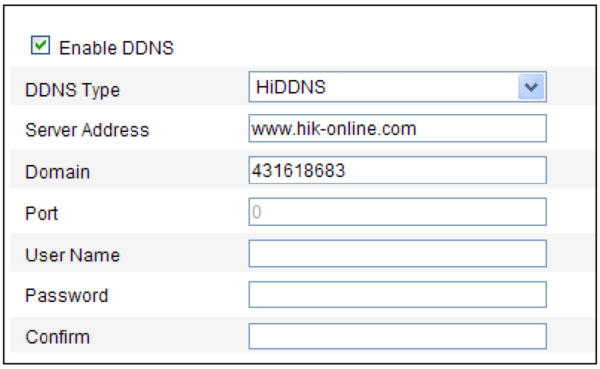
Registration on the DDNS server is required before configuring the DDNS settings of the camera.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the DDNS Settings interface:

   Configuration > Advanced Configuration > Network > DDNS



☑ Enable DDNS

DDNS Type	HiDDNS
Server Address	www.hik-online.com
Domain	431618683
Port	0
User Name	
Password	
Confirm	

Figure 7-9 DDNS Settings

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Four DDNS types are selectable: HiDDNS, IPServer, NO-IP, and DynDNS.
   - DynDNS:

   Steps:

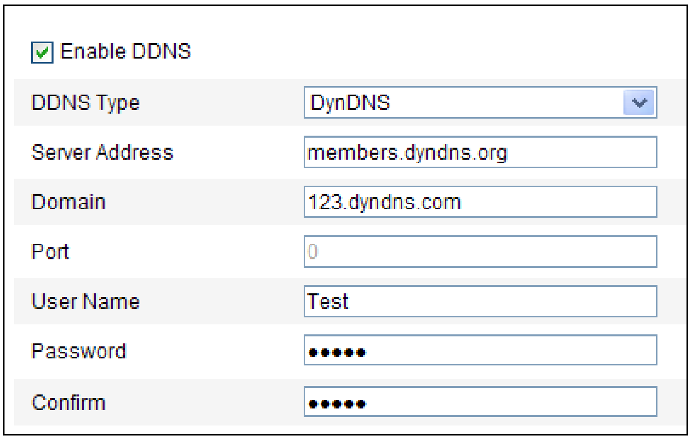
   (1) Enter **Server Address** of DynDNS (e.g. members.dyndns.org).

   (2) In the **Domain** text field, enter the domain name obtained from the DynDNS website.

   (3) Enter the **Port** of DynDNS server.

(4) Enter the **User Name** and **Password** registered on the DynDNS website.

(5) Click **Save** to save the settings.



☑ Enable DDNS

DDNS Type	DynDNS
Server Address	members.dyndns.org
Domain	123.dyndns.com
Port	0
User Name	Test
Password	●●●●●
Confirm	●●●●●

Figure 7-10 DynDNS Settings

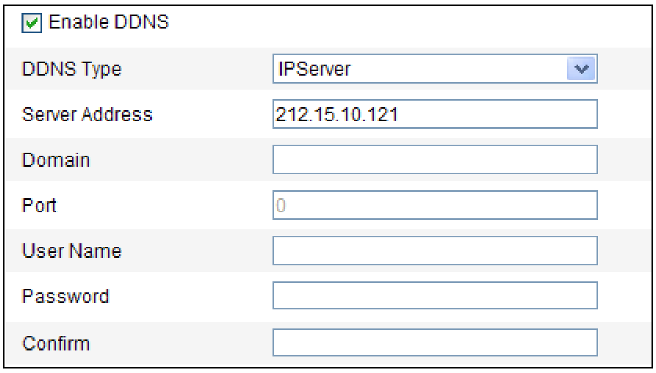
- IP Server:

Steps:

(1) Enter the Server Address of the IP Server.

(2) Click **Save** to save the settings.

Note: For the IP Server, you have to apply a static IP, subnet mask, gateway and preferred DNS from the ISP. The **Server Address** should be entered with the static IP address of the computer that runs the IP Server software.



☑ Enable DDNS

DDNS Type	IPServer
Server Address	212.15.10.121
Domain	
Port	0
User Name	
Password	
Confirm	

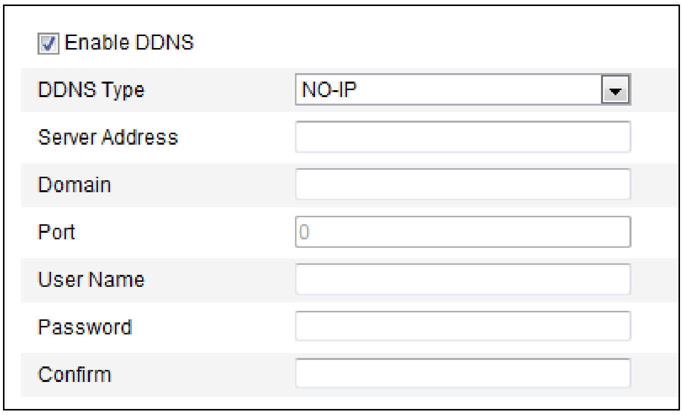
Figure 7-11 IPServer Settings

Note: For the US and Canada area, you can enter 173.200.91.74 as the server address.

- NO-IP:

Steps:

(1) Choose the DDNS Type as NO-IP.



☑ Enable DDNS	
DDNS Type	NO-IP
Server Address	
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 7-12 NO-IP Settings

(2) Enter the Server Address as www.noip.com

(3) Enter the Domain name you registered.

(4) Enter the Port number, if needed.

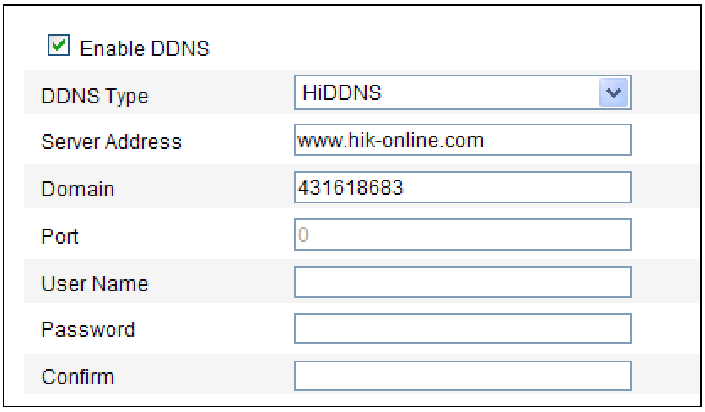
(5) Enter the User Name and Password.

(6) Click **Save** and then you can view the camera with the domain name.

- HiDDNS

Steps:

(1) Choose the DDNS Type as HiDDNS.



☑ Enable DDNS	
DDNS Type	HiDDNS
Server Address	www.hik-online.com
Domain	431618683
Port	0
User Name	
Password	
Confirm	

Figure 7-13 HiDDNS Settings

(2) Enter the Server Address *www.hik-online.com.*

(3) Enter the Domain name of the camera. The domain is the same with the device alias in the HiDDNS server.

(4) Click **Save** to save the new settings.

Note: A reboot is required for the settings to take effect.

7.3.5 Configuring SNMP Settings

Purpose:

You can set the SNMP function to get camera status, parameters and alarm related information and manage the camera remotely when it is connected to the network.

Before you start:

Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Note:

The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

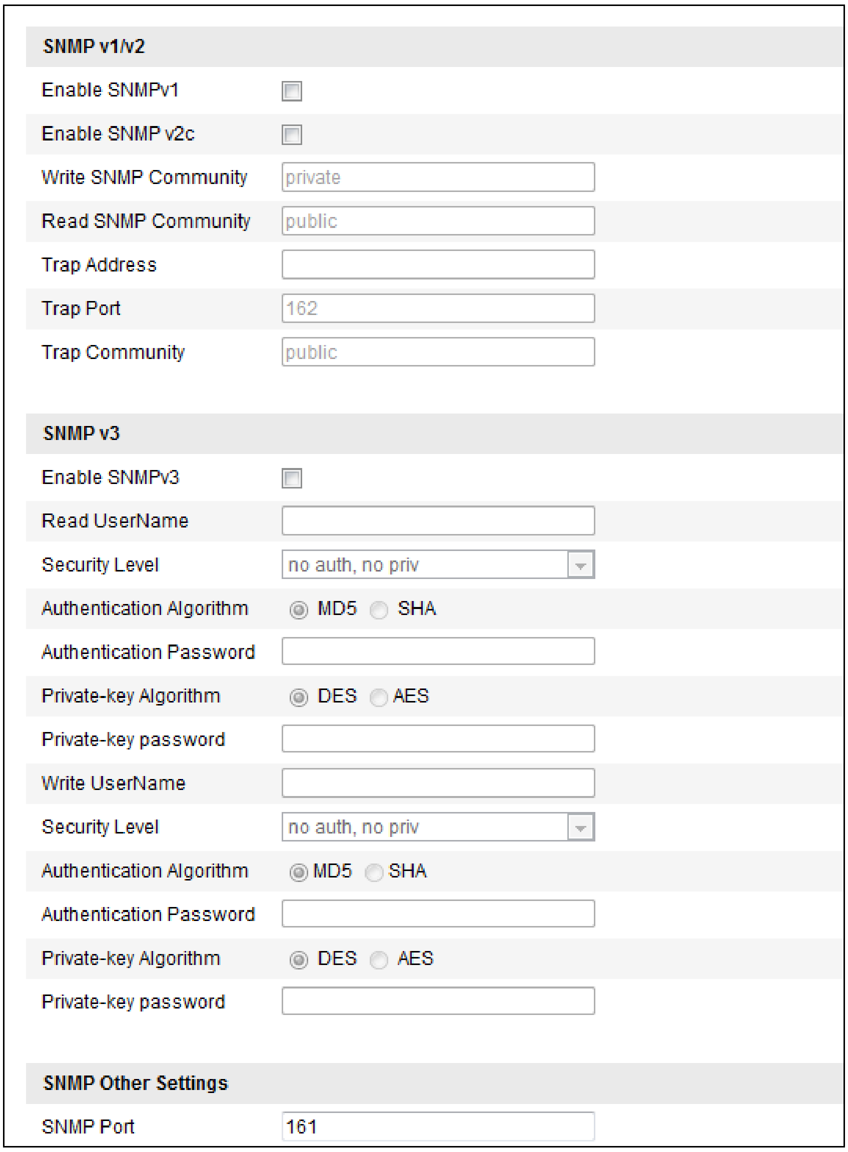
⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the SNMP Settings interface:

   Configuration > Advanced Configuration > Network > SNMP



SNMP v1/v2

Enable SNMPv1	□
Enable SNMP v2c	□
Write SNMP Community	private
Read SNMP Community	public
Trap Address	
Trap Port	162
Trap Community	public

SNMP v3

Enable SNMPv3	□
Read UserName	
Security Level	no auth, no priv
Authentication Algorithm	● MD5 ○ SHA
Authentication Password	
Private-key Algorithm	● DES ○ AES
Private-key password	
Write UserName	
Security Level	no auth, no priv
Authentication Algorithm	● MD5 ○ SHA
Authentication Password	
Private-key Algorithm	● DES ○ AES
Private-key password	

SNMP Other Settings

SNMP Port	161

Figure 7-14 SNMP Settings

2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2c, Enable SNMPv3) to enable the feature.
3. Configure the SNMP settings.

   Note: The settings of the SNMP software should be the same as the settings you configure here.
4. Click **Save** to save and finish the settings.

Note: A reboot is required for the settings to take effect.

7.3.6 Configuring 802.1X Settings

Purpose:

The parking camera supports IEEE 802.1X standard.

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN. When devices connect to this network with IEEE 802.1X standard, the authentication is needed. If the authentication fails, the devices don't connect to the network.

Before you start:

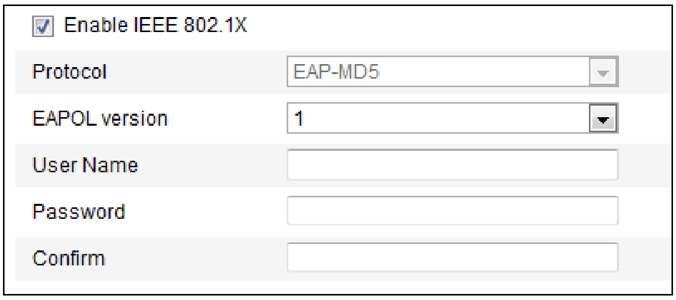
The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the 802.1X Settings interface:
   Configuration > Advanced Configuration > Network > 802.1X



☑ Enable IEEE 802.1X

Protocol	EAP-MD5
EAPOL version	1
User Name	
Password	
Confirm	

Figure 7-15 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name and password.

Note: The EAPOL version must be identical with that of the router or the switch.

4. Enter the user name and password to access the server.
5. Click **Save** to save the settings.

Note: A reboot is required for the settings to take effect.

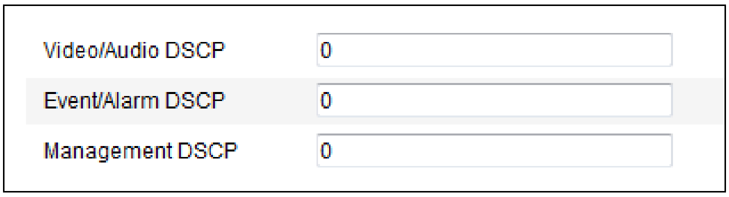
7.3.7 Configuring QoS Settings

Purpose:

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending.

Steps:

1. Enter the QoS Settings interface:
   Configuration >Advanced Configuration > Network > QoS



Video/Audio DSCP	0
Event/Alarm DSCP	0
Management DSCP	0

Figure 7-16 QoS Settings

2. Configure the QoS settings, including video / audio DSCP, event / alarm DSCP and Management DSCP.

The valid value range of the DSCP is 0-63. The bigger the DSCP value is, the higher the priority is.

Note: DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

3. Click **Save** to save the settings.

Note: A reboot is required for the settings to take effect.

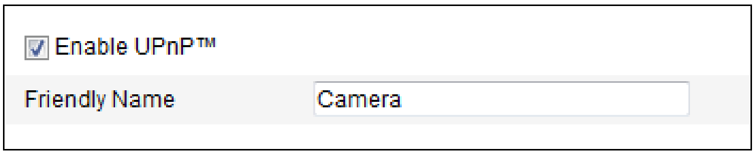
7.3.8 Configuring UPnP™ Settings

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don’t need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

Steps:

1. Enter the UPnP™ settings interface.
   Configuration >Advanced Configuration > Network > UPnP
2. Check the checkbox to enable the UPnP™ function.
   The name of the device when detected online can be edited.



☑ Enable UPnP™

Friendly Name	Camera

Figure 7-17 UPnP Settings

7.3.9 Email Sending Triggered by Alarm

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before you start:

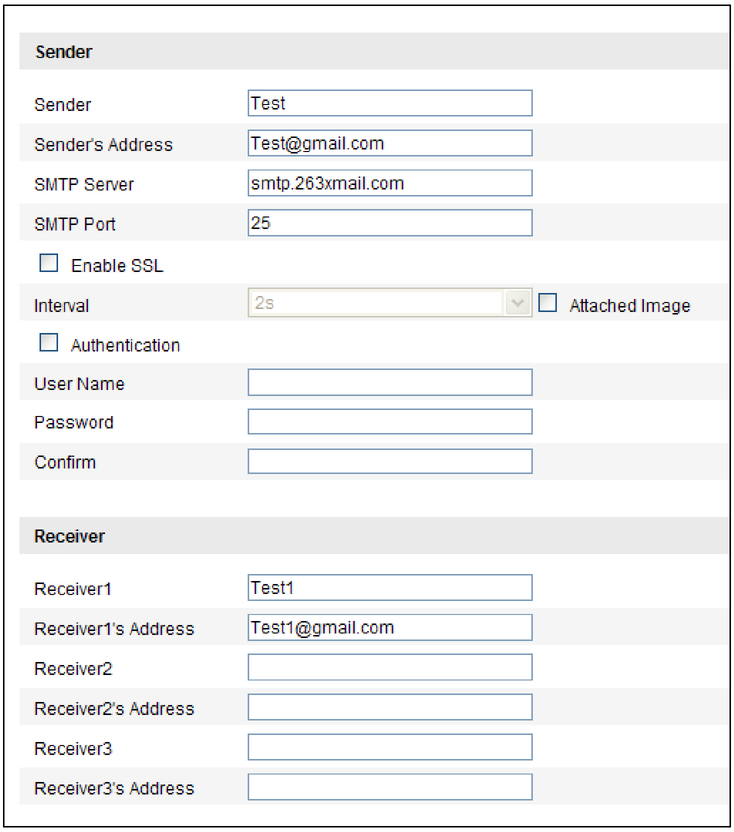
Please configure the DNS Server settings under **Basic Configuration** > **Network** > **TCP/IP** or **Advanced Configuration** > **Network** > **TCP/IP** before using the Email function.

Steps:

1. Enter the TCP/IP Settings (**Configuration** > **Basic Configuration** > **Network** > **TCP/IP** or **Configuration** > **Advanced Configuration** > **Network** > **TCP/IP)** to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

Note: Please refer to *Section 7.3.1* ***Configuring TCP/IP Settings*** for detailed information.

2. Enter the Email Settings interface:
   Configuration > **Advanced Configuration** > **Network** > **Email**



Sender		
Sender	Test	
Sender's Address	Test@gmail.com	
SMTP Server	smtp.263xmail.com	
SMTP Port	25	
□ Enable SSL		
Interval	2s	□ Attached Image
□ Authentication		
User Name		
Password		
Confirm		
Receiver		
Receiver1	Test1	
Receiver1's Address	Test1@gmail.com	
Receiver2		
Receiver2's Address		
Receiver3		
Receiver3's Address		

Figure 7-18 Email Settings

3. Configure the following settings:
   Sender: The name of the email sender.
   Sender's Address: The email address of the sender.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.

Enable SSL: Check the checkbox to enable SSL if it is required by the SMTP server.

Attached Image: Check the checkbox of Attached Image if you want to send emails with attached alarm images.

Interval: The interval refers to the time between two actions of sending attached pictures.

Authentication (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and enter the login user Name and password.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Choose Receiver: Select the receiver to which the email is sent. Up to 2 receivers can be configured.

Receiver: The name of the user to be notified.

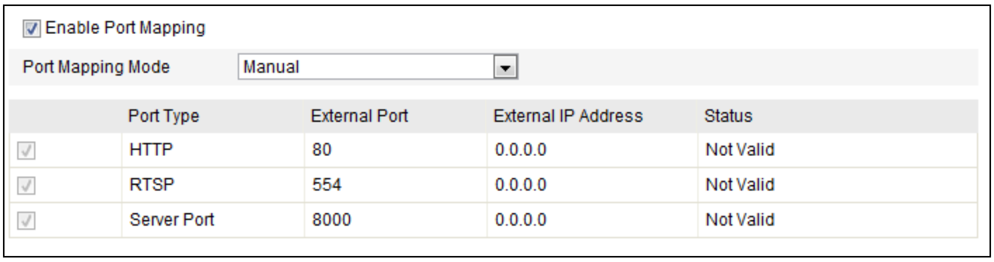
Receiver's Address: The email address of user to be notified.

4. Click **Save** to save the settings.

7.3.10 Configuring NAT (Network Address Translation) Settings

Purpose:

1. Enter the NAT settings interface.
   Configuration >Advanced Configuration > Network > NAT
2. Choose the port mapping mode.
   To port mapping with the default port numbers:
   Choose Port Mapping Mode as **Auto**.
   To port mapping with the customized port numbers:
   Choose Port Mapping Mode as **Manual**.
   And for manual port mapping, you can customize the value of the port number by yourself.



☑ Enable Port Mapping

Port Mapping Mode: Manual

	Port Type	External Port	External IP Address	Status
☑	HTTP	80	0.0.0.0	Not Valid
☑	RTSP	554	0.0.0.0	Not Valid
☑	Server Port	8000	0.0.0.0	Not Valid

Figure 7-19 Configure NAT Settings

3. Click **Save** to save the settings.

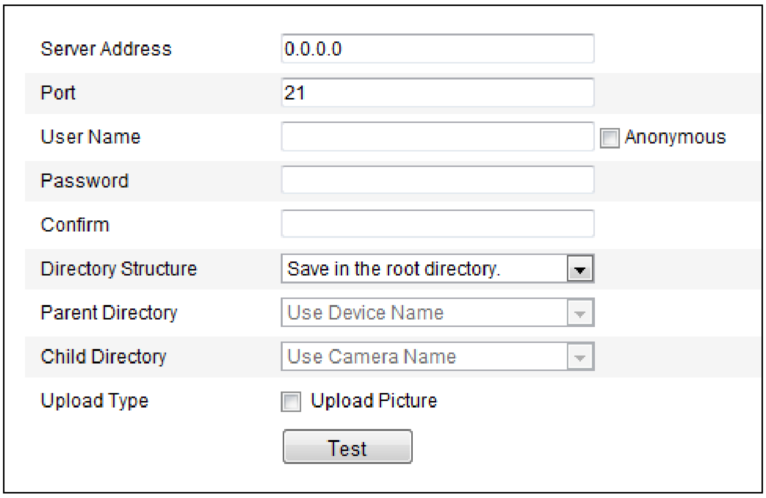
7.3.11 Configuring FTP Settings

Purpose:

You can configure the FTP server related information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

Steps:

1. Enter the FTP Settings interface:
   Configuration >Advanced Configuration > Network > FTP



Server Address	0.0.0.0
Port	21
User Name	☐ Anonymous
Password	
Confirm	
Directory Structure	Save in the root directory.
Parent Directory	Use Device Name
Child Directory	Use Camera Name
Upload Type	☐ Upload Picture

Figure 7-20 FTP Settings

2. Configure the FTP settings; and the user name and password are required for login the FTP server.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

Upload type: To enable uploading the captured picture to the FTP server.

Anonymous Access to the FTP Server (in which case the user name and password won't be required.): Check the Anonymous checkbox to enable the anonymous access to the FTP server.

Note: The anonymous access function must be supported by the FTP server.

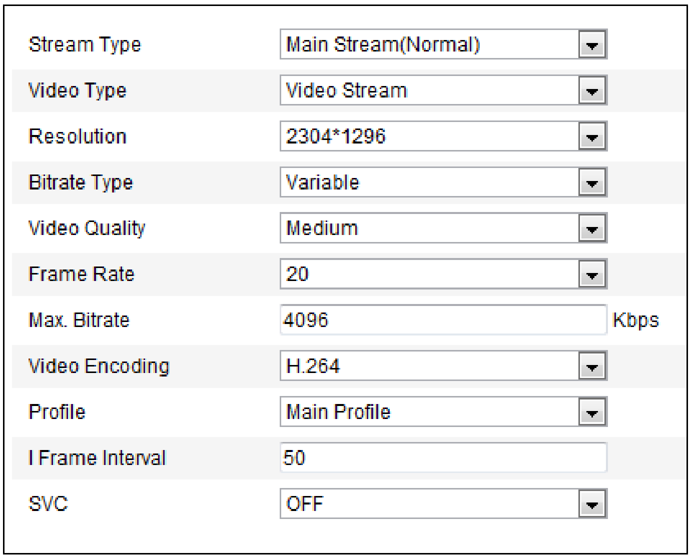
3. Click **Save** to save the settings.

7.4 Configuring Video and Audio Settings

7.4.1 Configuring Video Settings

Steps:

1. Enter the Video Settings interface:
   Configuration >Basic Configuration > Video / Audio > Video
   Or Configuration > Advanced Configuration > Video / Audio > Video



Stream Type	Main Stream(Normal)
Video Type	Video Stream
Resolution	2304*1296
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	20
Max. Bitrate	4096 Kbps
Video Encoding	H.264
Profile	Main Profile
I Frame Interval	50
SVC	OFF

Figure 7-21 Video Settings

2. Select the **Stream Type** of the camera to main stream (normal) or sub-stream. The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited.
3. You can customize the following parameters for the selected main stream or sub-stream:

   Video Type: The video type can only be set as the **Video Stream**.

Resolution: Select the resolution of the video output.

Bitrate Type: Select the bitrate type to constant or variable.

Video Quality: When bitrate type is selected as **Variable**, 6 levels of video quality are selectable.

Frame Rate: Set the frame rate to 1/16~25 fps. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate: Set the max. bitrate to 32~16384 Kbps. The higher value corresponds to the higher video quality, but the higher bandwidth is required.

Video Encoding: Only H.264 is selectable.

Note: The supported video encoding may differ according to the different platform.

Profile: Only Main Profile is selectable.

I Frame Interval: Set the I-Frame interval to 1~400.

SVC: Scalable Video Coding is an extension of the H.264/AVC standard. Select OFF / ON to disable / enable the SVC function. Turn on the function, and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Intelligent Encoding: Enabling this function will reduce the frame rate when the parking space is free to save the storage space.

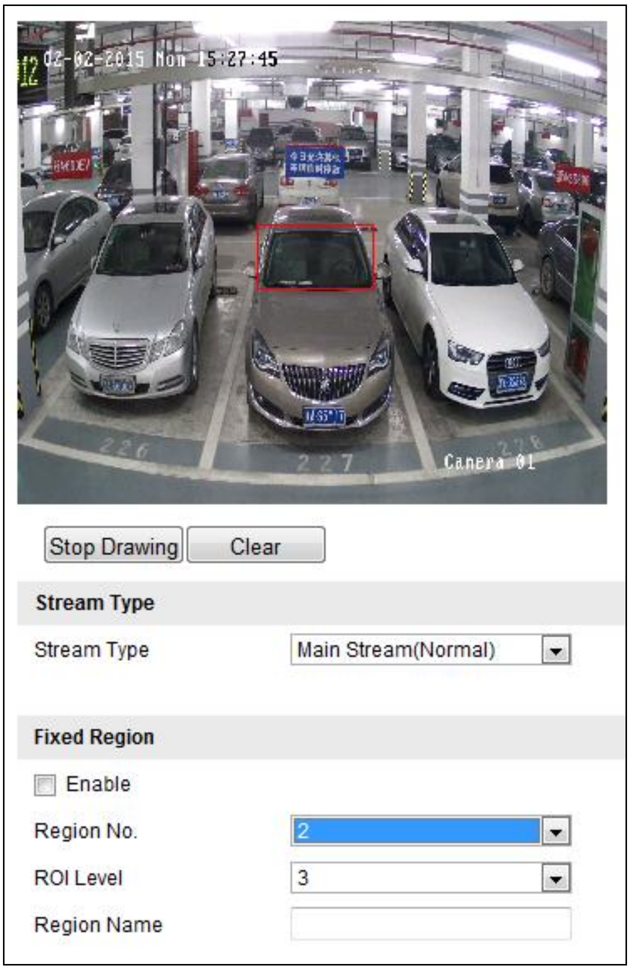
4. Click **Save** to save the settings.

7.4.2 Configuring ROI Encoding

Purpose:

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression, which means, the technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Note: ROI function varies according to different camera models.



Stream Type

Stream Type	Main Stream(Normal)

Fixed Region

□ Enable

Region No.	2
ROI Level	3
Region Name	

Figure 7-22 Region of Interest Settings

Configuring Fixed Region for ROI:

Steps:

1. Enter the ROI settings interface:
   Configuration> Advanced Configuration> Video/Audio> ROI
2. Check the checkbox of **Enable** under Fixed Region item.
3. Select the stream type for ROI encoding.
4. Select the region from the drop-down list for ROI settings. There are four fixed regions selectable.
5. Click the **Draw Area** button, and then click-and-drag the mouse to draw the region of interest on the live video.
6. Select the ROI level to set the image quality enhancing level. The larger the value is, the better the image quality is.
7. Input the region name for ROI as desired.
8. Click **Save** to save the settings.

7.5 Configuring Image Parameters

7.5.1 Configuring Display Settings

Purpose:

You can set the image quality of the camera, including brightness, contrast, saturation, hue, sharpness, etc.

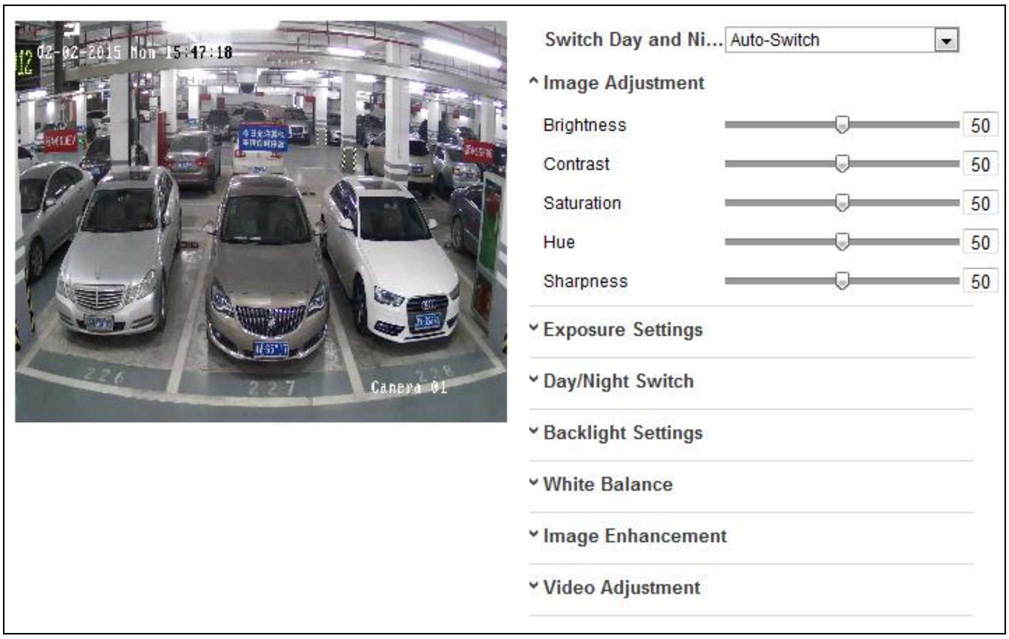
Note: The display parameters vary according to the different camera model. Please refer to the actual interface for details.

Steps:

1. Enter the Display Settings interface:
   Configuration > Basic Configuration> Image> Display Settings
   Or Configuration > Advanced Configuration> Image> Display Settings
2. Set the image parameters of the camera.

Note: In order to guarantee the image quality in the different illumination, it provides two sets of parameters for user to configure.

Day/Night Auto-switch



Switch Day and Ni... Auto-Switch

Image Adjustment

Brightness	50
Contrast	50
Saturation	50
Hue	50
Sharpness	50

Figure 7-23 Display Settings of Day/night Auto-switch

- **Image Adjustment**

Brightness describes bright of the image, which ranges from 1~100, and the default value is 50.

Contrast describes the contrast of the image, which ranges from 1~100, and the default value is 50.

Saturation describes the colorfulness of the image color, which ranges from 1~100, and the default value is 50.

Hue describes the lightness of the image color, which ranges from 1~100, and the default value is 50.

Sharpness describes the edge contrast of the image, which ranges from 1~100, and the default value is 50.

- **Exposure Settings**

If the camera is equipped with the fixed lens, only **Manual** is selectable, and the iris mode is not configurable.

The exposure time refers to the electronic shutter time, which ranges from 1/3 ~ 1/100,000s. Adjust it according to the actual luminance condition.

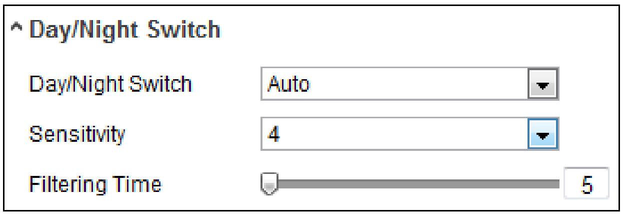
The value of Gain refers to the gain of the image; you can drag the slider to adjust the value.

- **Focus Settings**

For the camera supports electronic lens, you can set the focus mode as Auto, Manual or Semi-auto. If auto is selected, the focus is adjusted automatically according to the actual monitoring scenario; if manual is selected, you can control the lens by adjusting the zoom, focus, lens initialization, and auxiliary focus via the PTZ control interface; if semi-auto is selected, the camera will focus automatically when you adjust the zoom parameters.

- **Day/Night Switch**

Select the day/night switch mode, and configure the smart IR settings from this option.



Day/Night Switch: Auto

Sensitivity: 4

Filtering Time: 5

Figure 7-24 Day/Night Switch

Day, night, auto, schedule, and triggered by alarm input are selectable for day/night switch.

Day: the camera stays at day mode.

Night: the camera stays at night mode.

Auto: the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0~7, the higher the value is, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.

Schedule: Set the start time and the end time to define the duration for day/night mode.

- **Backlight Settings**

BLC Area: If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right, Center and customize are selectable.

WDR: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

- ♦ **White Balance**

White balance is the white rendition function of the camera used to adjust the color temperature according to the environment.

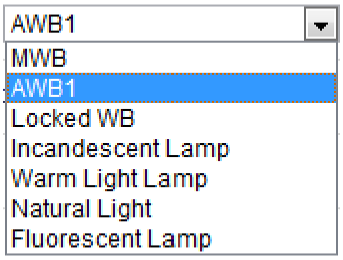


Figure 7-25 White Balance

- ♦ **Image Enhancement**

Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal Mode and Expert Mode are selectable. Set the DNR level from 0~100, and the default value is 50 in Normal Mode. Set the DNR level from both space DNR level [0~100] and time DNR level [0~100] in Expert Mode.

- ♦ **Video Adjustment**

Mirror: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.

Rotate: To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.

When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.

Video Standard: 50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

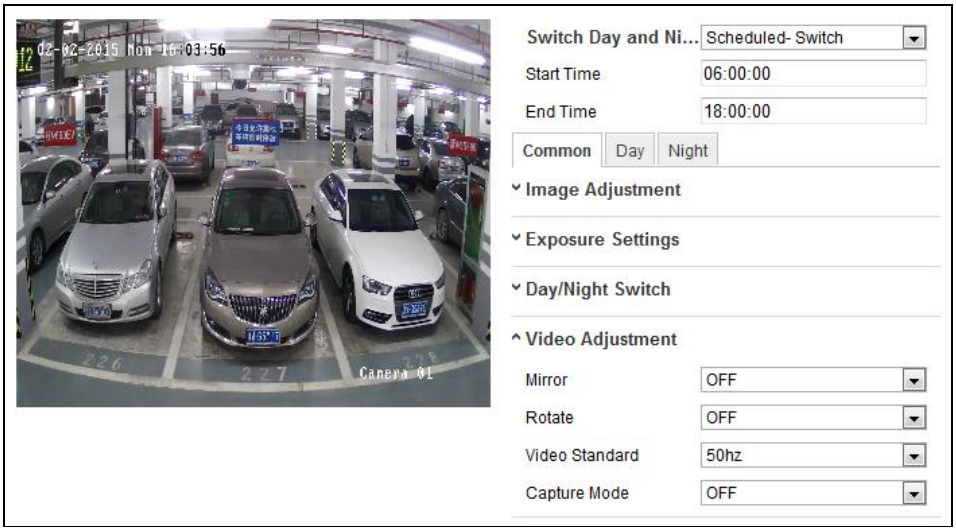
Capture Mode: It’s the selectable video input mode to meet the different demands of field of view and resolution.

- ♦ **Other**

Some of the camera supports CVBS, SDI, or HDMI output. Please refer to the actual camera model for details.

Day/Night Scheduled-Switch

Day/Night scheduled-switch configuration interface enables you to set the separate camera parameters for day and night to guarantee the image quality in different illumination.



Switch Day and Ni... Scheduled- Switch

Start Time 06:00:00

End Time 18:00:00

Common | Day | Night

˅ Image Adjustment

˅ Exposure Settings

˅ Day/Night Switch

˄ Video Adjustment

Mirror	OFF
Rotate	OFF
Video Standard	50hz
Capture Mode	OFF

Figure 7-26 Day/Night Scheduled-Switch Configuration Interface

Steps:

1. Click the time line to select the start time and the end time of the switch.
2. Click Common tab to configure the common parameters applicable to the day mode and night mode.

Note: The detailed information of each parameter please refers to day/night auto switch session.

3. Click Day tab to configure the parameters applicable for day mode.
4. Click Night tab to configure the parameters applicable for night mode.

Note: The settings saved automatically if any parameter is changed.

7.5.2 Configuring OSD Settings

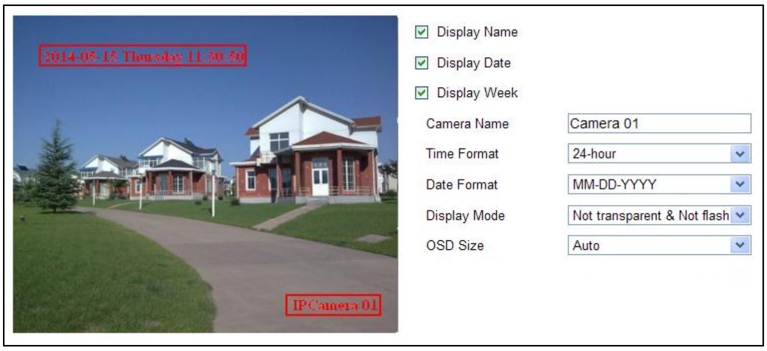
Purpose:

You can customize the camera name and time on the screen.

Steps:

1. Enter the OSD Settings interface:

   Configuration > Advanced Configuration > Image > OSD Settings



☑ Display Name

☑ Display Date

☑ Display Week

Camera Name	Camera 01
Time Format	24-hour
Date Format	MM-DD-YYYY
Display Mode	Not transparent & Not flash
OSD Size	Auto

Figure 7-27 OSD Settings

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format, date format, display mode and the OSD font size.
5. You can use the mouse to click and drag the text frame IPCamera 01 in the live view window to adjust the OSD position.
6. Click **Save** to activate the above settings.

7.5.3 Configuring Text Overlay Settings

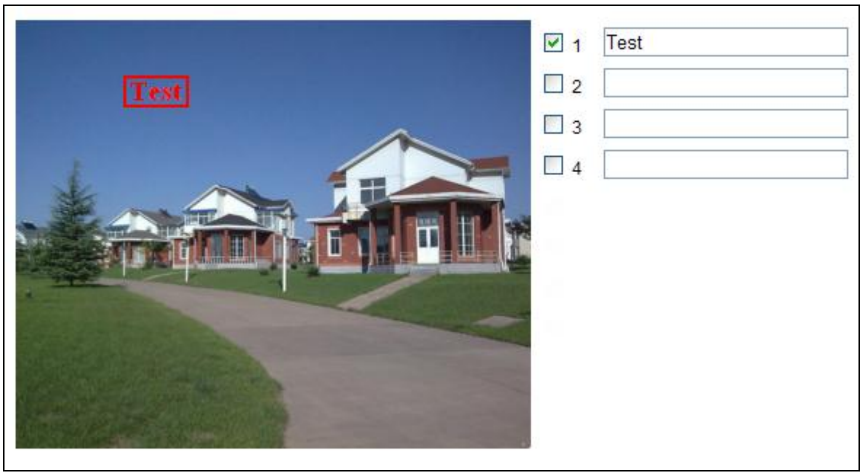
Purpose:

You can customize the text overlay.

Steps:

1. Enter the Text Overlay Settings interface:

Configuration > Advanced Configuration > Image > Text Overlay



☑ 1 Test

□ 2

□ 3

□ 4

Figure 7-28 Text Overlay

2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. (Optional)Use the mouse to click and drag the red text frame Test in the live view window to adjust the text overlay position.
5. Click **Save** to save the settings.

Note: Up to 4 text overlays are configurable.

7.5.4 Configuring Privacy Mask

Purpose:

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps:

1. Enter the Privacy Mask Settings interface:
   Configuration > Advanced Configuration> Image > Privacy Mask
2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click Draw Area.

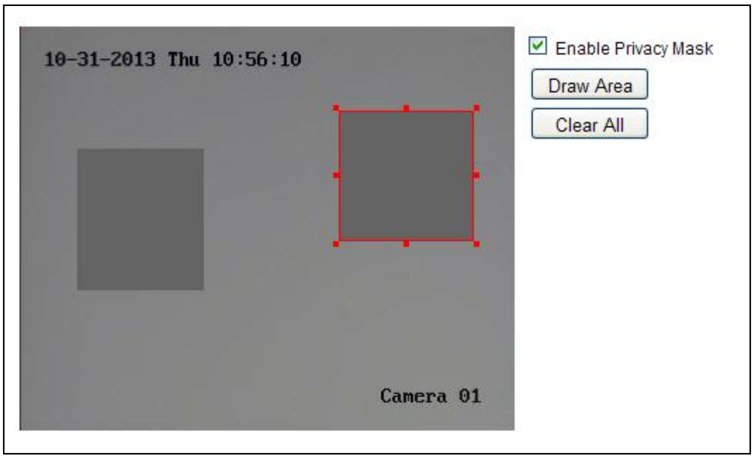


Figure 7-29 Privacy Mask Settings

4. Click and drag the mouse in the live video window to draw the mask area.

Note: You are allowed to draw up to 4 areas on the same image.

5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
6. Click **Save** to save the settings.

7.6 Configuring and Handling Alarms

This section explains how to configure the parking camera to respond to alarm events, including motion detection and exceptions. These events can trigger the linkage methods, such as Notify Surveillance Center.

Notes:

Check the checkbox of Notify Surveillance Center if you want the alarm information to be pushed to PC or mobile client software as soon as the alarm is triggered.

7.6.1 Configuring Motion Detection

Purpose:

Motion detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

Steps:

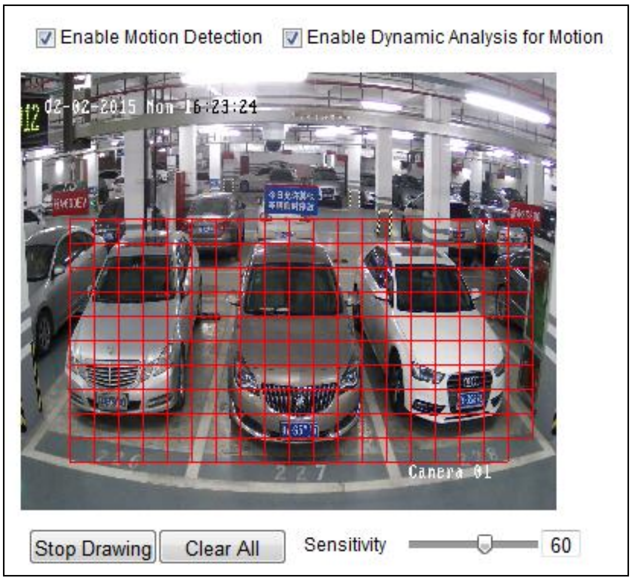
1. Set the Motion Detection Area.

(1) Enter the motion detection settings interface
Configuration > Advanced Configuration> Basic Event > Motion Detection

(2) Check the checkbox of Enable Motion Detection.

(3) Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles.

Note: Select Disable for rules if you don't want the detected objected displayed with the rectangles. Select disable from **Configuration>Local Configuration>Live View Parameters>rules**.



☑ Enable Motion Detection ☑ Enable Dynamic Analysis for Motion

Sensitivity 60

Figure 7-30 Enable Motion Detection

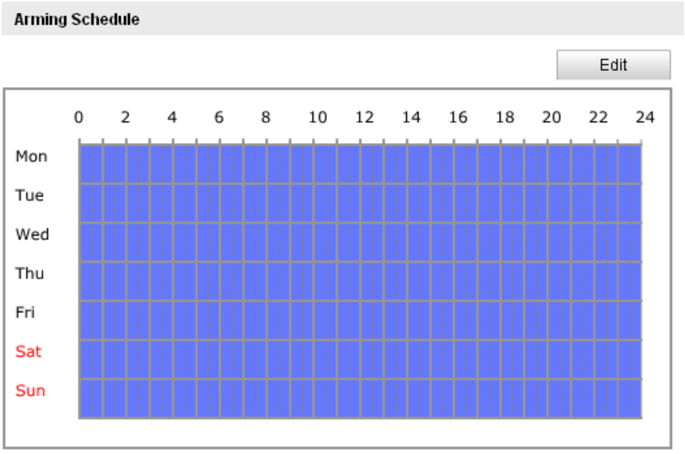
(4) Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area.

(5) Click **Stop Drawing** to finish drawing one area.

(6) (Optional) Click **Clear All** to clear all of the areas.

(7) (Optional) Move the slider to set the sensitivity of the detection.

2. Set the Arming Schedule for Motion Detection.



Arming Schedule

Figure 7-31 Arming Time

(1) Click **Edit** to edit the arming schedule. The Figure 6-34 shows the editing interface of the arming schedule.

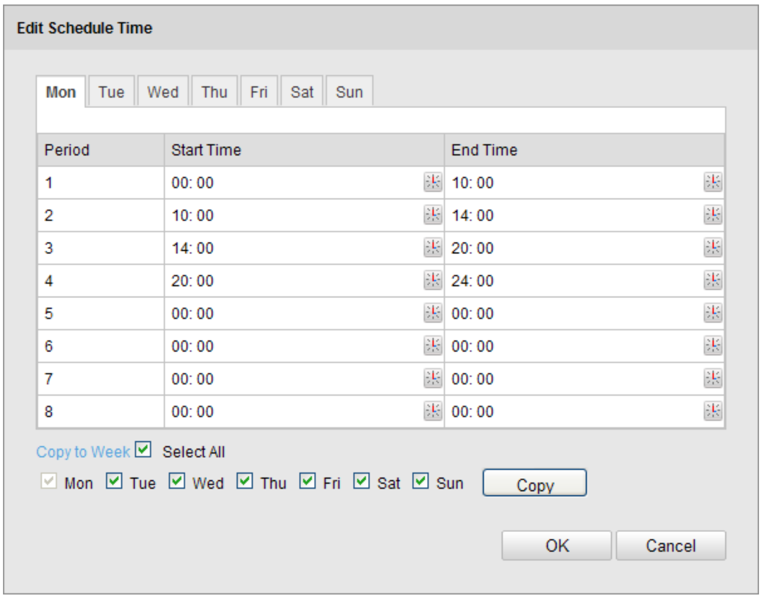
(2) Choose the day you want to set the arming schedule.

(3) Click 🕒 to set the time period for the arming schedule.

(4) (Optional) After you set the arming schedule, you can copy the schedule to other days.

(5) Click **OK** to save the settings.

Note: The time of each period cannot be overlapped. Up to 8 periods can be configured for each day.



Edit Schedule Time

Mon | Tue | Wed | Thu | Fri | Sat | Sun

Period	Start Time	End Time
1	00: 00	10: 00
2	10: 00	14: 00
3	14: 00	20: 00
4	20: 00	24: 00
5	00: 00	00: 00
6	00: 00	00: 00
7	00: 00	00: 00
8	00: 00	00: 00

Copy to Week ☑ Select All

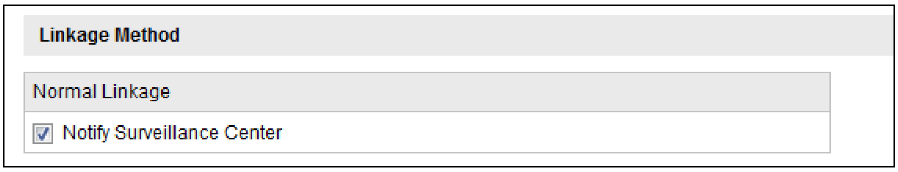
☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun Copy

OK Cancel

Figure 7-32 Arming Time Schedule

3. Set the Alarm Actions for Motion Detection.

Check the checkbox to select the linkage method. Notify surveillance center, send email, upload to FTP, trigger channel and trigger alarm output are selectable. You can specify the linkage method when an event occurs.



Linkage Method

Normal Linkage

☑ Notify Surveillance Center

Figure 7-33 Linkage Method

- Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

7.6.2 Handling Exception

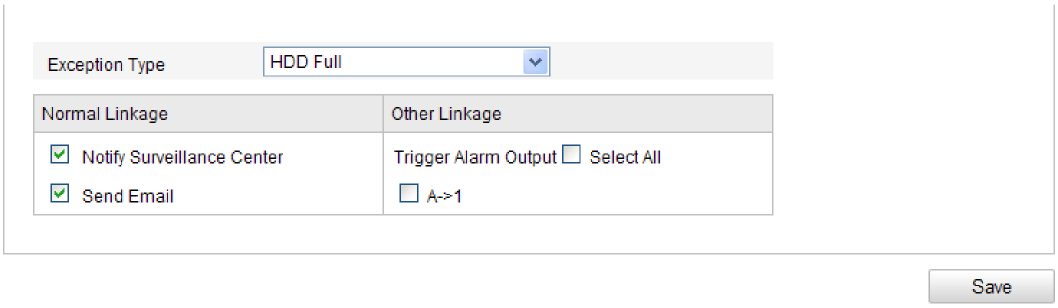
The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the cameras.

Steps:

1. Enter the Exception Settings interface:

Configuration > Advanced Configuration> Basic Event > Exception

2. Check the checkbox to set the actions taken for the Exception alarm. Refer to *Task 3* ***Set the Alarm Actions Taken for Motion Detection*** in *Section 6.6.1*.



Exception Type: HDD Full

Normal Linkage	Other Linkage
☑ Notify Surveillance Center	Trigger Alarm Output □ Select All
☑ Send Email	□ A->1

Figure 7-34 Exception Settings

3. Click **Save** to save the settings.

Chapter 8 Configuration Parking Space Detection

Purpose:

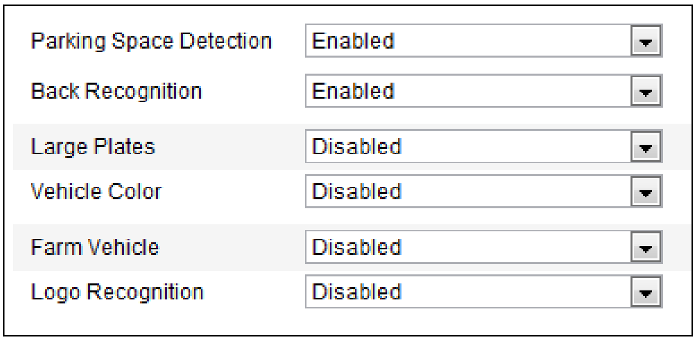
To detecting the parking space, you should enable the VCA function and configure the corresponding parameters. Follow the instructions below to realize the parking space detection.

8.1 Configuring Detection Rules

Steps:

1. Enter the VCA configuration interface.

   Configuration > Advanced Configuration > VCA



Parking Space Detection: Enabled
Back Recognition: Enabled
Large Plates: Disabled
Vehicle Color: Disabled
Farm Vehicle: Disabled
Logo Recognition: Disabled

Figure 8-1 Setting Basic Parameters

2. Click the Basic Parameters tab and configure the following options.

   Parking Space Detection: Select the Enable in the dropdown list to turn on the Parking Space Detection.

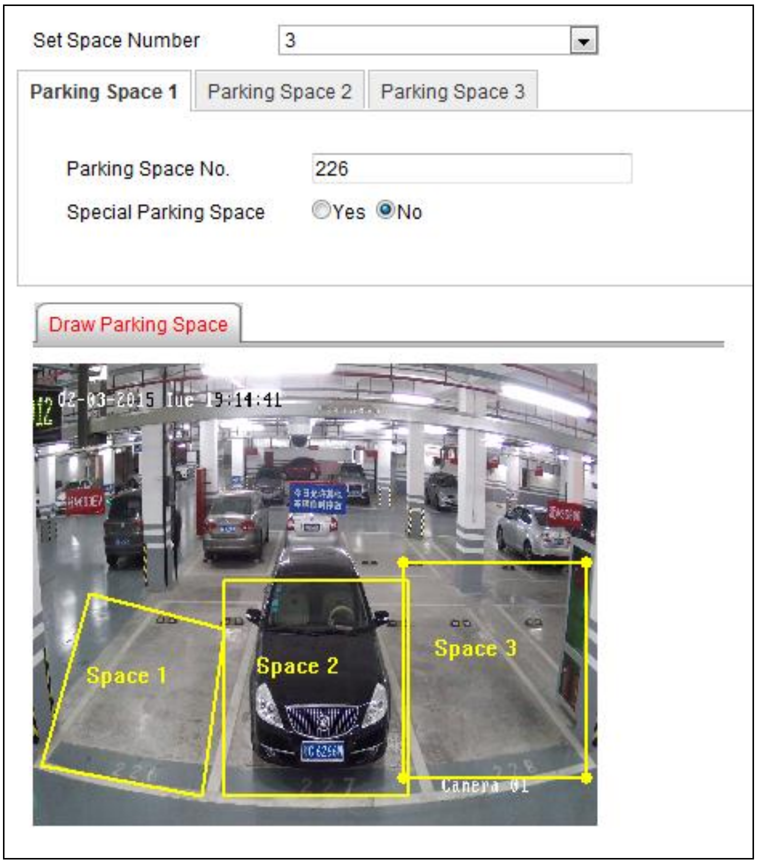
   Back Recognition: Select the Enable in the dropdown list to enable the license plate recognition when the vehicle is back parked into the space.

   Large Plates: Normally, the camera is recommended to be placed about 5 m away from the parking spaces to ensure the plate recognition accuracy. But if the parking camera is placed much nearer to the spaces than the recommended distance, the license plate possesses greater pixels in the image which will make it looks large, then you should enable the Large Plate function to improve the accuracy of the license plate recognition.

   Farm Vehicle: For the license plate of fame vehicles, there are much different from other ones of normal vehicles. Enable the Farm Vehicle function to recognize the license plate number of farm vehicles.

   Logo Recognition: Enable the function to recognize the logo of the vehicle.

3. Click the Analysis Parameters tab and configure the following options.



Set Space Number: 3

Parking Space 1 | Parking Space 2 | Parking Space 3

Parking Space No.: 226

Special Parking Space: ○Yes ●No

Draw Parking Space

Figure 8-2 Setting Analysis Parameters

1) Set the number of the spaces in the dropdown list.

   Note: The selectable value may vary according the camera models.

2) Click the tab of the parking space number to configure the parameters.

3) You can input the Parking Space No. in the text filed (e.g. the space is the No. 119 of the parking lot; you may input 119 in the text field).

4) If the space is a special space, click the **Yes** radio to set it.

4. Draw parking spaces.

   1) According to the number of spaces you set, the quadrilaterals appear in the image.

   2) Click a quadrilateral to select it and switch to the edit mode, click and drag corner of the quadrilateral to adjust the shape of it, and click and drag the side of the quadrilateral to adjust the location of it.

   3) Repeat the above 2 steps to configure other quadrilaterals.

5. Click the **Save** button to activate the settings.

8.2 Configuring Space Indicator

Purpose:

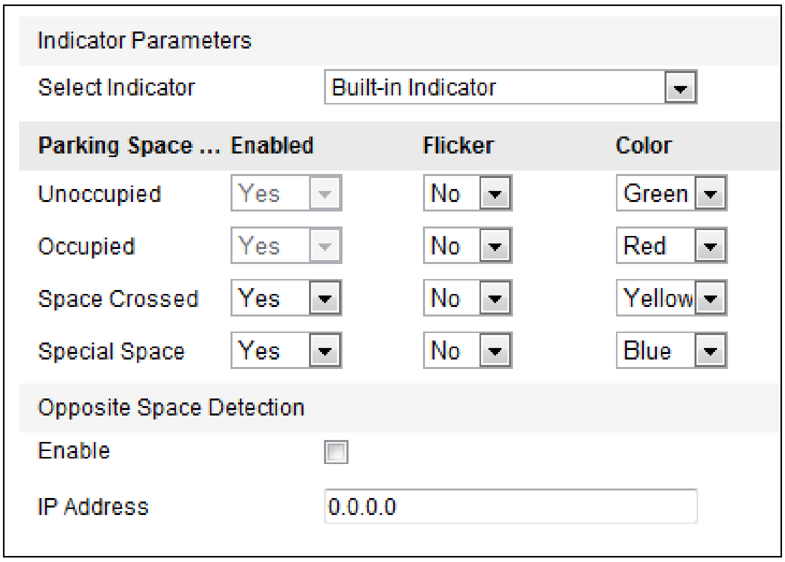
The indicator displays the space status, different colors stand for different status. You can select the indicator and the color of different status.

Steps:

1. Enter the space indicator settings interface.

   Configuration > Advanced Configuration > Parking Indicator

2. Select the indicator in the dropdown list of **Select Indicator** on your demand, including **Built-in Indicator** and **Built-in Indicator and External Indicator**



Indicator Parameters

Select Indicator: Built-in Indicator

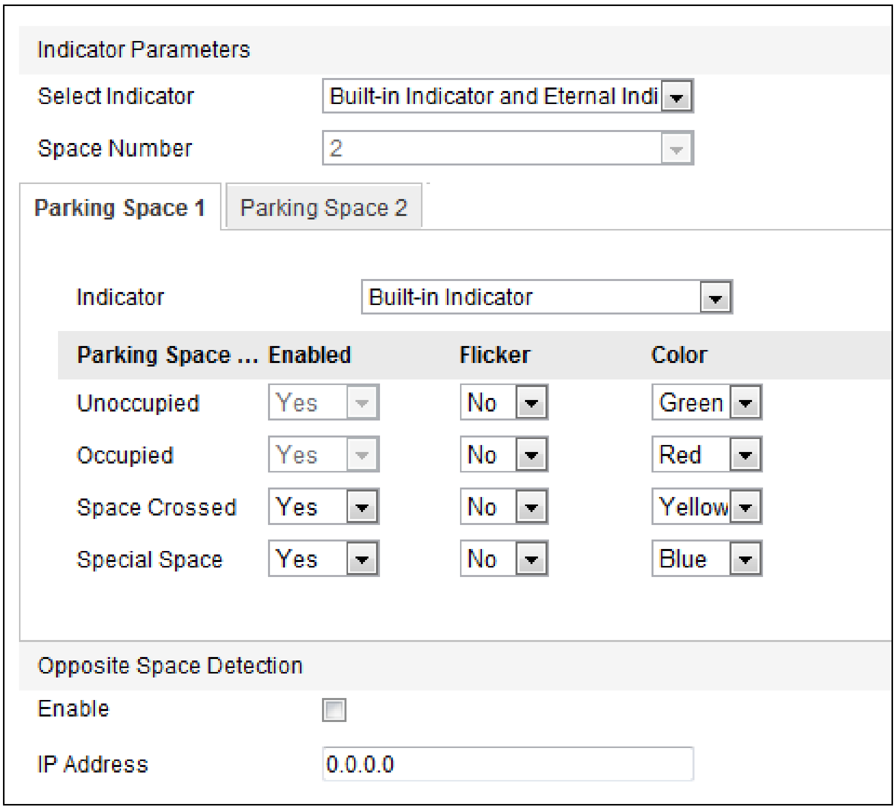
Parking Space ...	Enabled	Flicker	Color
Unoccupied	Yes	No	Green
Occupied	Yes	No	Red
Space Crossed	Yes	No	Yellow
Special Space	Yes	No	Blue

Opposite Space Detection

Enable ☐

IP Address: 0.0.0.0

Figure 8-3 Configuring the Built-in Indicator



Indicator Parameters

Select Indicator: Built-in Indicator and Eternal Indi

Space Number: 2

Parking Space 1 | Parking Space 2

Indicator: Built-in Indicator

Parking Space ...	Enabled	Flicker	Color
Unoccupied	Yes	No	Green
Occupied	Yes	No	Red
Space Crossed	Yes	No	Yellow
Special Space	Yes	No	Blue

Opposite Space Detection

Enable ☐

IP Address: 0.0.0.0

Figure 8-4 Configuring the Built-in Indicator and External Indicator

Notes:

- The built-in indicator is on the bottom of the camera.
- If you have external indicators, you should connect the indicators to the external interfaces of the camera.
- After connecting the external indicators to the camera and powering up, the indicator will start the self-test by lighting red, green and blue. If the self-test fails, please check whether the cable connection is right.
- If you select the **Built-in Indicator**, and when all the detected parking spaces are occupied, the indicator turns to the occupied color; when the detected parking spaces are not all occupied, the indicator remains the unoccupied color.
- If you select the **Built-in Indicator and External Indicator**, the indicators work at the same time, you can respectively configure the indicator to display the status of each parking space.

3. Set the indicator parameters for different parking space status.

   The description different status is shown below:

   Unoccupied: The space is free.

   Occupied: The space is occupied by a vehicle.

   Space Crossed: A vehicle occupied two parking spaces.

   Special Space: The space is specified to a certain vehicle.

   1) If you choose the **Built-in Indicator and External Indicator**, click the tab of the parking space No. (e.g. Parking Space 1) and select the indicator in the **Indicator** dropdown list.
   2) Configure the following parameters on your demand.

      Enabled: Select Yes or No to enable or disable the indicating for the corresponding status.

      Flicker: Set the indicator flicker or not for the corresponding status.

      Color: Choose the color of the indicator for the corresponding status.

4. (Optional) Configure the Opposite Space Detection.

   The Opposite Space Detection is applicable to the parking lot that the aisle between the opposite parking spaces is very narrow. After you configure the function, the indicator of the current parking camera displays the status of opposite spaces, and vice versa.

   1) Check the Enable checkbox.
   2) Input the IP address of the parking camera of the opposite spaces.

5. Click the **Save** button to activate the settings.

8.3 Uploading Pictures

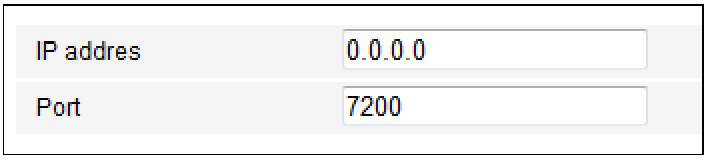
Purpose:

The pictures of the parking spaces can be uploaded to the remote host or the ftp, perform the following instructions to configure the parameters.

- **Uploading Pictures to Remote Host**

Steps:

1. Enter the remote host settings interface.
   Configuration > Advanced Configuration > Upload Picture



IP addres	0.0.0.0
Port	7200

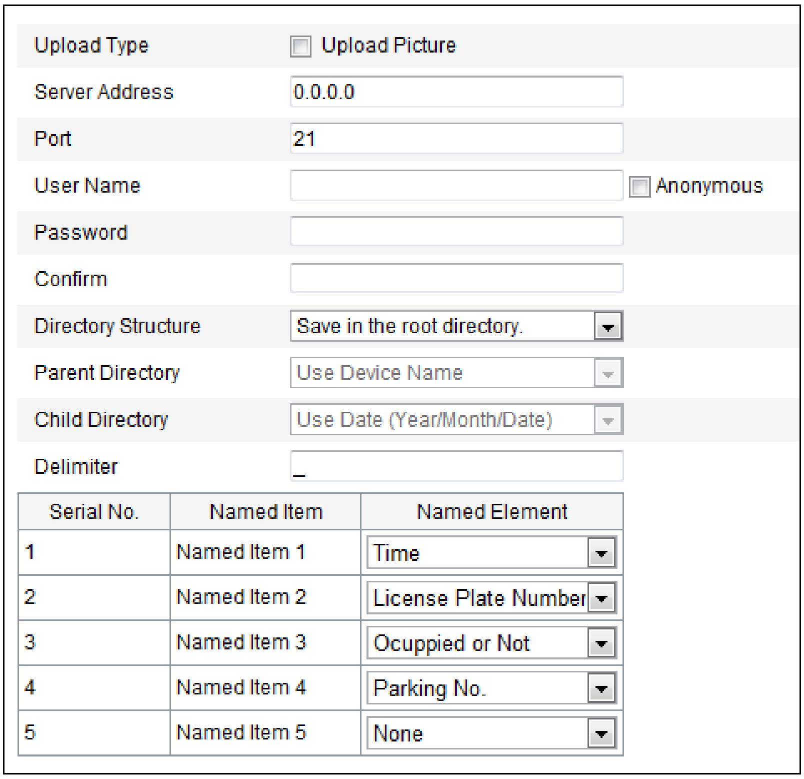
Figure 8-5 Configuring Remote Host

2. Configure the IP address and the port number of the remote host.
3. Click the **Save** button to activate the settings.

- **Uploading Pictures to FTP**

Steps:

1. Enter the FTP settings interface by Configuration > Advanced Configuration > Upload Picture, and then click the FTP tab.



Upload Type	□ Upload Picture	
Server Address	0.0.0.0	
Port	21	
User Name		□ Anonymous
Password		
Confirm		
Directory Structure	Save in the root directory.	
Parent Directory	Use Device Name	
Child Directory	Use Date (Year/Month/Date)	
Delimiter	_	

Serial No.	Named Item	Named Element
1	Named Item 1	Time
2	Named Item 2	License Plate Number
3	Named Item 3	Ocuppied or Not
4	Named Item 4	Parking No.
5	Named Item 5	None

Figure 8-6 Configuring FTP

2. Check the checkbox of Upload Picture.

3. Configure the FTP address and port number; and the user name and password are required for login the FTP server.

   Anonymous Access to the FTP Server (in which case the user name and password won't be required.): Check the Anonymous checkbox to enable the anonymous access to the FTP server.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. Configure the uploading directory of the FTP.

   In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number, Device IP Address or Date for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Parking No. as the name of the directory.

5. The uploaded can be named by 5 elements, and each element can be customized as Time, Device IP Address, License Plate Number, Space Status, Parking No. or None. And you can set the Delimiter between the elements.

   Note: The named items cannot be duplicated.

6. (Optional) Normally, a single parking camera detects the status of several spaces, thus the captured picture contains several spaces as well. If you want to divide the picture into several pictures according to the parking spaces, you can enable the Picture Division function by selecting Enable in the dropdown list.
7. Click the **Save** button to activate the settings.

8.4 Checking Space Status

1. Enter the space indicator settings interface.

   Configuration > Advanced Configuration > Parking Indicator
2. Click the Parking Space Status tab to view the space status, including license plate number, indicator flicker status, indicator color, etc..

8.5 Typical Applications

8.5.1 Built-in Indicator Application

Note: A parking camera for three parking spaces is taken as the example below.

Steps:

1. Set the detection rules; refer to *section 8.1 Configuring Detection Rules*.
2. Select the Built-in Indicator in the **Select Indicator** dropdown list.
3. Set the Enabled, Flicker and Color parameters for the Occupied, Unoccupied and Space Crossed status.
4. Save the configuration by clicking the **Save** button.

The indicator displays the color of occupied status when the three spaces are all occupied; and the indicator displays the color of occupied status when any of the space is free; and the indicator displays the color of space crossed when a parked vehicle occupies two spaces.

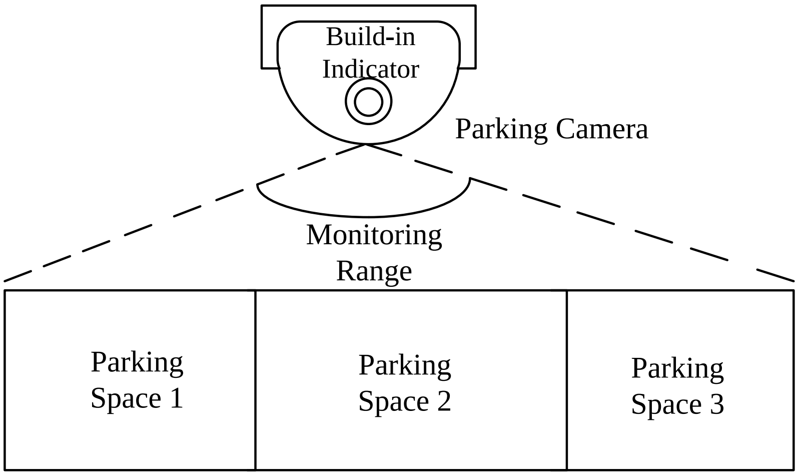


Figure 8-7 Application Diagram of Built-in Indicator Mode

8.5.2 Opposite Spaces Detection Application

The Opposite Space Detection is applicable to the parking lot that the aisle between the opposite parking spaces is very narrow. After you configure the function, the indicator of the current parking camera displays the status of opposite spaces, and vice versa.

Note: Two parking camera for six parking spaces is taken as the example below.

Steps:

1. Set the detection rules, refer to *section 8.1 Configuring Detection Rules*.
2. Select the Built-in Indicator in the **Select Indicator** dropdown list.
3. Set the Enabled, Flicker and Color parameters for the Occupied, Unoccupied and

Space Crossed status.

4. Check the Enable checkbox of the Opposite Space Detection and input the IP address of the parking camera of the opposite spaces.
5. Save the configuration by clicking the **Save** button.
6. Repeat the above steps to configure the other parking camera.

The Parking Camera A controls the Indicator B and detects the status of the Parking Spaces B1-B3, while the Parking Camera B controls the Indicator A and detects the status of the Parking Spaces A1-A3, as shown in the Figure 8-8.

The indicator displays the color of occupied status when the three spaces are all occupied; and the indicator displays the color of occupied status when any of the space is free; and the indicator displays the color of space crossed when a parked vehicle occupies two spaces.

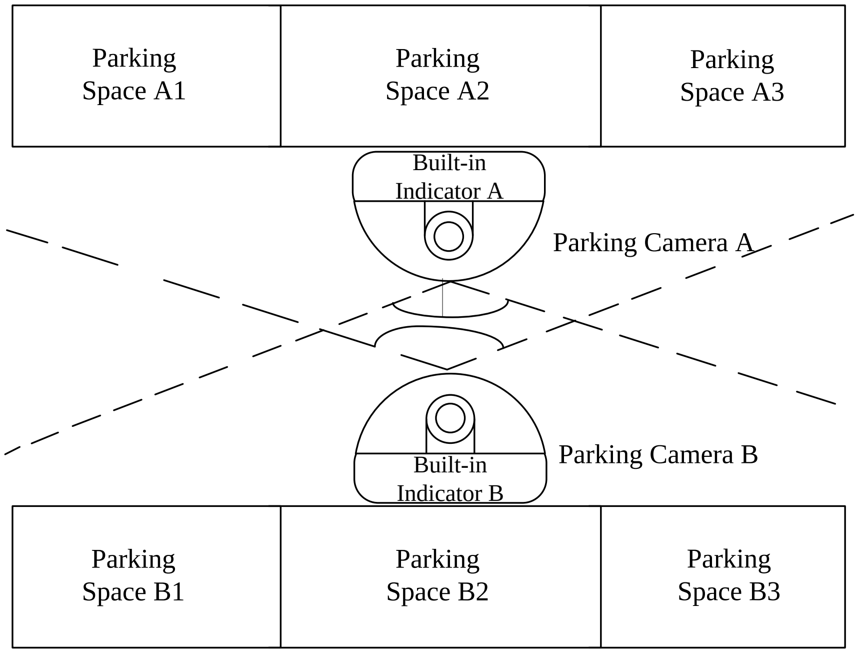


Figure 8-8 Application Diagram of Opposite Space Detection Mode

8.5.3 External Indicator Application

Note: A parking camera for three parking spaces is taken as the example below.

Steps:

1. Set the detection rules, refer to *section 8.1 Configuring Detection Rules*.
2. Select the Built-in Indicator and External Indicator in the **Select Indicator** dropdown list.
3. Respectively select the indicator in the **Indicator** dropdown list for each space according to the actual situation.
4. Set the Enabled, Flicker and Color parameters for the Occupied, Unoccupied and Space Crossed status.
5. Save the configuration by clicking the **Save** button.

The indicator displays the color of occupied status when the corresponding space is occupied; and the corresponding indicators display the color of space crossed when a vehicle occupies two spaces.

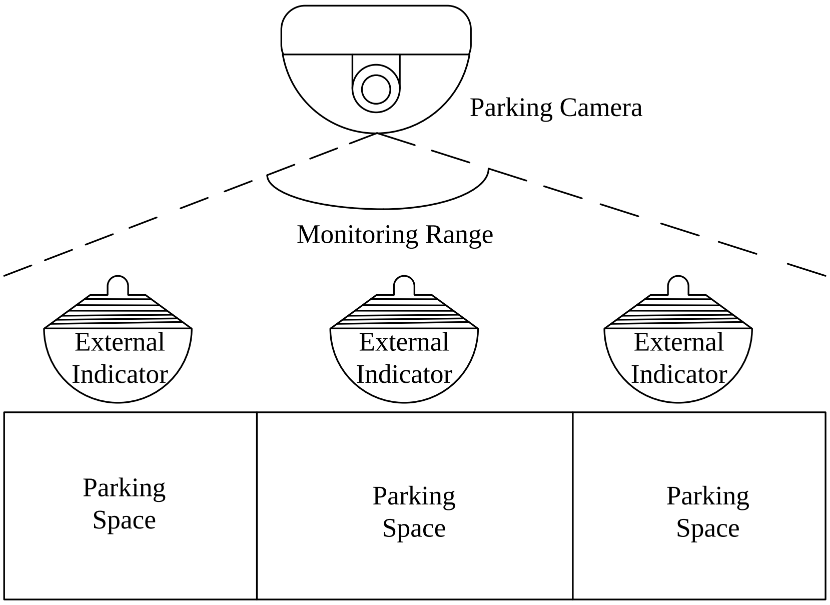
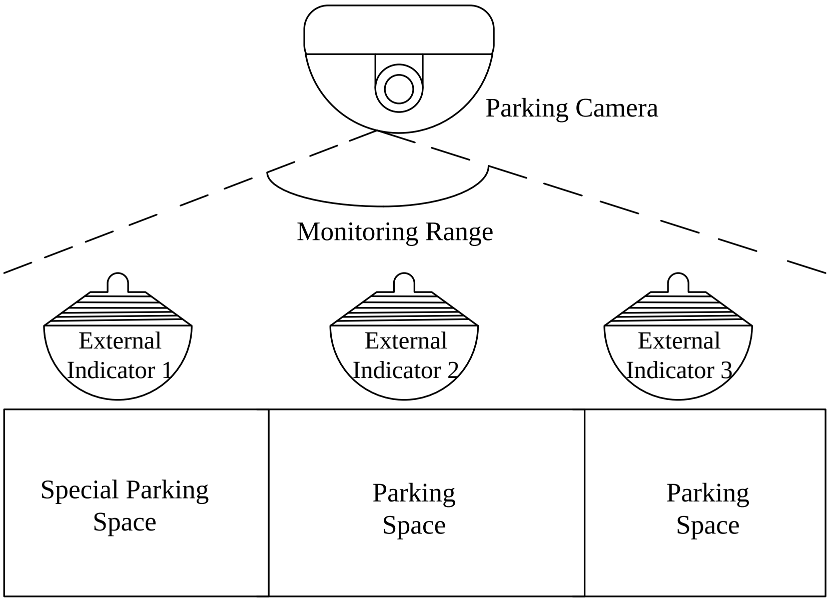


Figure 8-9 External Indicator Application Mode

8.5.4 Special Space Application

If the parking space a is a special space (as shown in figure below), perform the following steps to set the indicator for the special space.



Steps:

1. Set the detection rules and the parking space as the special parking space, refer to *section 8.1 Configuring Detection Rules*.
2. Select the Built-in Indicator and External Indicator in the **Select Indicator** dropdown list.

3. Set the indicator parameters for the special space.
4. Save the configuration by clicking the **Save** button.

   The external indicator 1 displays the color of the configured special space status, and the occupied and unoccupied status are invalid to the space.

Chapter 9 Storage Settings

Before you start:

To configure record settings, please make sure that you have the network storage device within the network or the SD card inserted in your camera.

9.1 Configuring NAS Settings

Before you start:

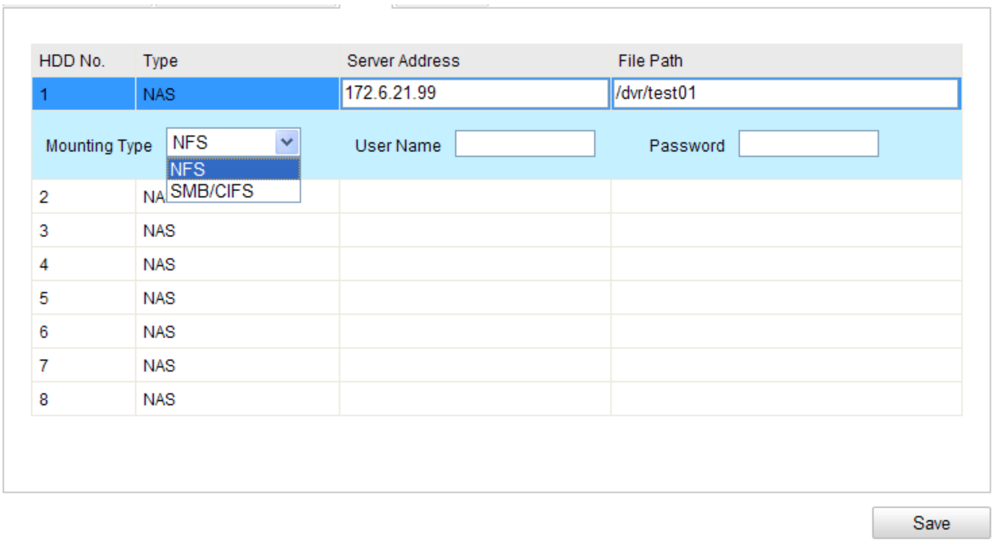
The network disk should be available within the network and properly configured to store the recorded files, log files, etc.

Steps:

1. Add the network disk

    (1) Enter the NAS (Network-Attached Storage) Settings interface:

    Configuration > Advanced Configuration > Storage > NAS



HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
Mounting Type	NFS	User Name	Password
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

Figure 9-1 Add Network Disk

    (2) Enter the IP address of the network disk, and enter the file path.

    (3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

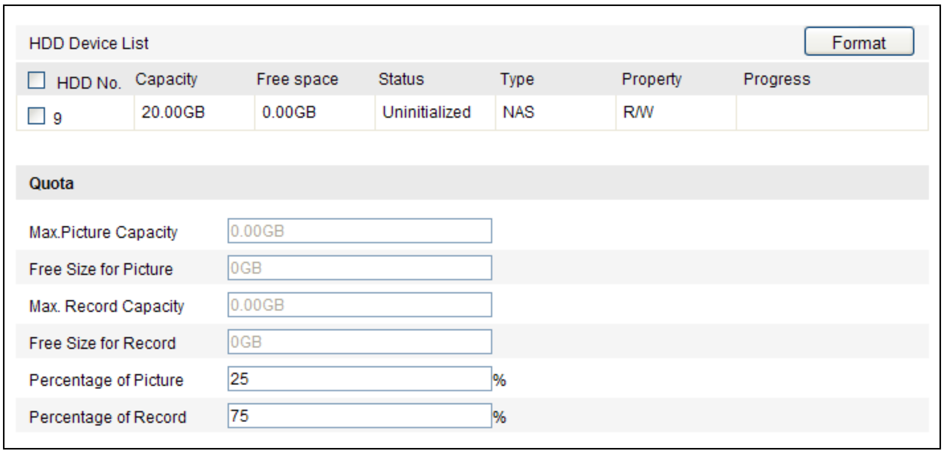
Note: Please refer to the *User Manual of NAS* for creating the file path.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

(4) Click **Save** to add the network disk.

2. Initialize the added network disk.

   (1) Enter the HDD Settings interface (**Advanced Configuration** > **Storage** > **Storage Management**), in which you can view the capacity, free space, status, type and property of the disk.



HDD Device List

☐ HDD No.	Capacity	Free space	Status	Type	Property	Progress
☐ 9	20.00GB	0.00GB	Uninitialized	NAS	R/W	

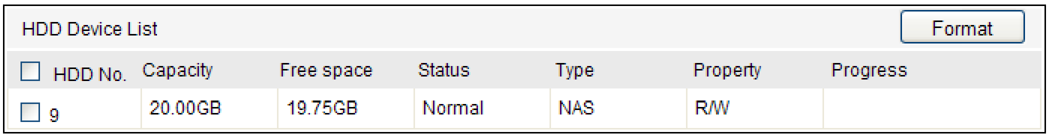
Quota

Max.Picture Capacity	0.00GB
Free Size for Picture	0GB
Max. Record Capacity	0.00GB
Free Size for Record	0GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figure 9-2 Storage Management Interface

   (2) If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.

   When the initialization completed, the status of disk will become **Normal.**



HDD Device List

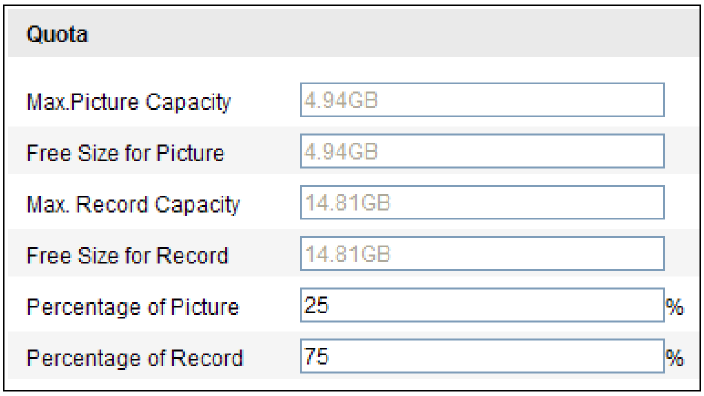
☐ HDD No.	Capacity	Free space	Status	Type	Property	Progress
☐ 9	20.00GB	19.75GB	Normal	NAS	R/W	

Figure 9-3 View Disk Status

3. Define the quota for record and pictures.

   (1) Input the quota percentage for picture and for record.

   (2) Click **Save** and refresh the browser page to activate the settings.



Quota

Max.Picture Capacity	4.94GB
Free Size for Picture	4.94GB
Max. Record Capacity	14.81GB
Free Size for Record	14.81GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figure 9-4 Quota Settings

Notes:

- Up to 8 NAS disks can be connected to the camera.
- To initialize and use the SD card after insert it to the camera, please refer to the

steps of NAS disk initialization.

9.2 Configuring Recording Schedule

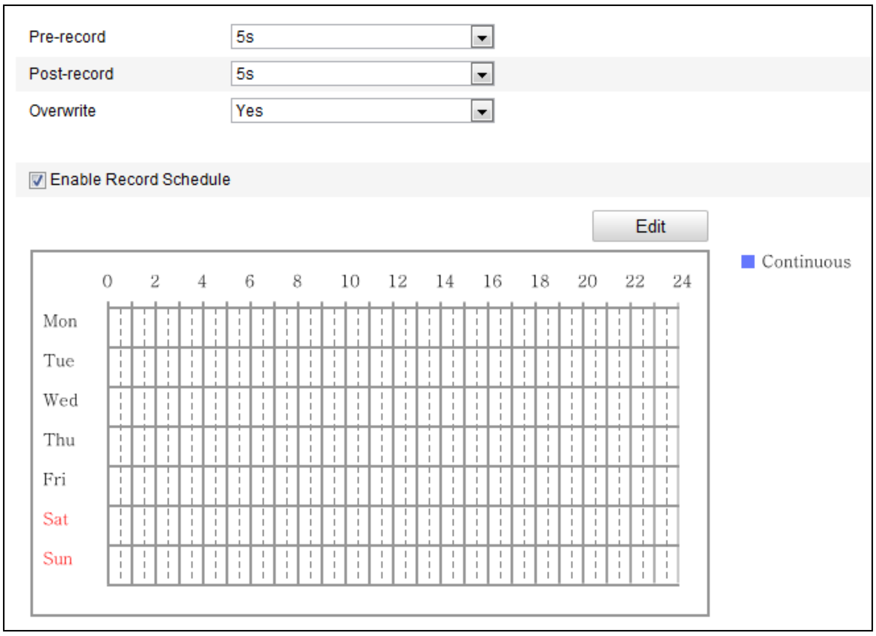
Purpose:

There are two kinds of recording for the cameras: manual recording and scheduled recording. For the manual recording, refer to *Section 6.3* ***Recording and Capturing Pictures Manually***. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the SD card (if supported) or in the network disk.

Steps:

1. Enter the Record Schedule Settings interface:

Configuration > Advanced Configuration> Storage > Record Schedule



Pre-record: 5s

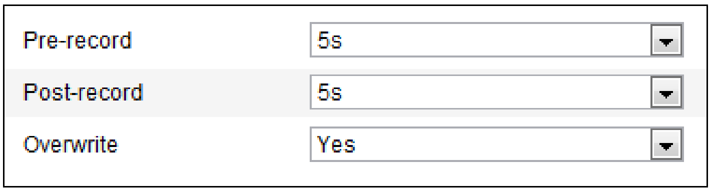
Post-record: 5s

Overwrite: Yes

☑ Enable Record Schedule

Figure 9-5 Recording Schedule Interface

2. Check the checkbox of **Enable Record Schedule** to enable scheduled recording.
3. Set the record parameters of the camera.



Pre-record: 5s

Post-record: 5s

Overwrite: Yes

Figure 9-6 Record Parameters

- Pre-record: The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

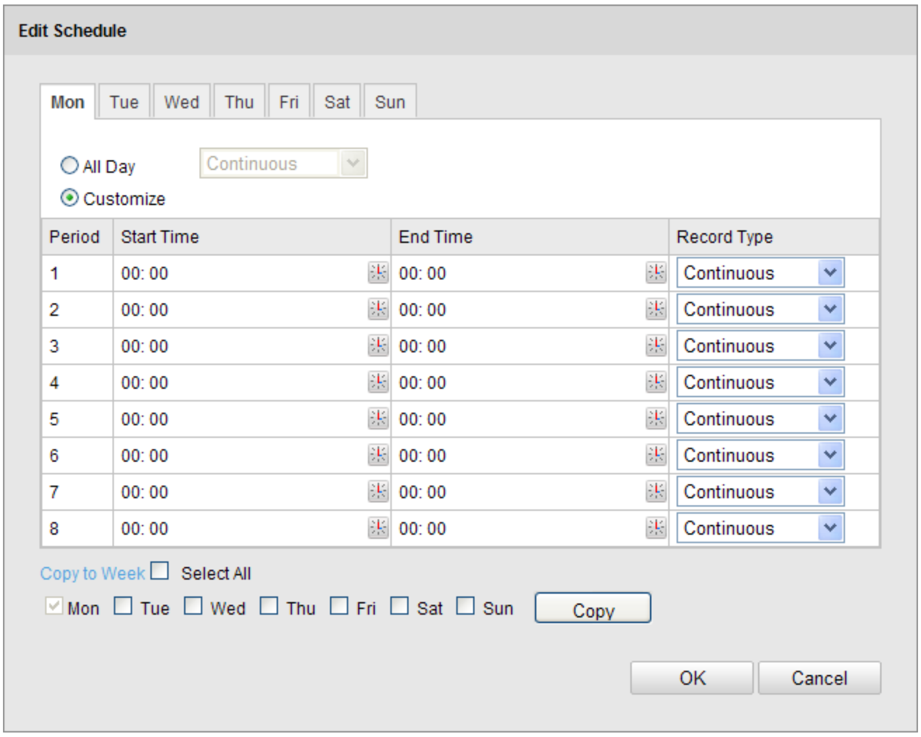
  The Pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.

- Post-record: The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

  The Post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.

Note: The record parameter configurations vary depending on the camera model.

4. Click **Edit** to edit the record schedule.



○ All Day Continuous

● Customize

Period	Start Time	End Time	Record Type
1	00: 00	00: 00	Continuous
2	00: 00	00: 00	Continuous
3	00: 00	00: 00	Continuous
4	00: 00	00: 00	Continuous
5	00: 00	00: 00	Continuous
6	00: 00	00: 00	Continuous
7	00: 00	00: 00	Continuous
8	00: 00	00: 00	Continuous

Copy to Week □ Select All

☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Figure 9-7 Record Schedule

5. Choose the day to set the record schedule.

   (1) Set all-day record or segment record:

♦ If you want to configure the all-day recording, please check the **All Day** checkbox.

♦ If you want to record in different time sections, check the **Customize** checkbox. Set the **Start Time** and **End Time.**

Note: The time of each segment cannot be overlapped. Up to 8 segments can be configured.

   (2) Select a **Record Type**. The record type can be Continuous for the camera.

   Continuous: The video will be recorded automatically according to the time of the schedule.

   (3) Check the checkbox of **Select All** and click **Copy** to copy settings of this day to the whole week. You can also check any of the checkboxes before the date and click **Copy**.

   (4) Click **OK** to save the settings and exit the **Edit Record Schedule** interface.

6. Click **Save** to save the settings.

Chapter 10 Playback

Purpose:

This section explains how to view the remotely recorded video files stored in the network disks or SD cards.

Steps:

1. Click **Playback** on the menu bar to enter playback interface.

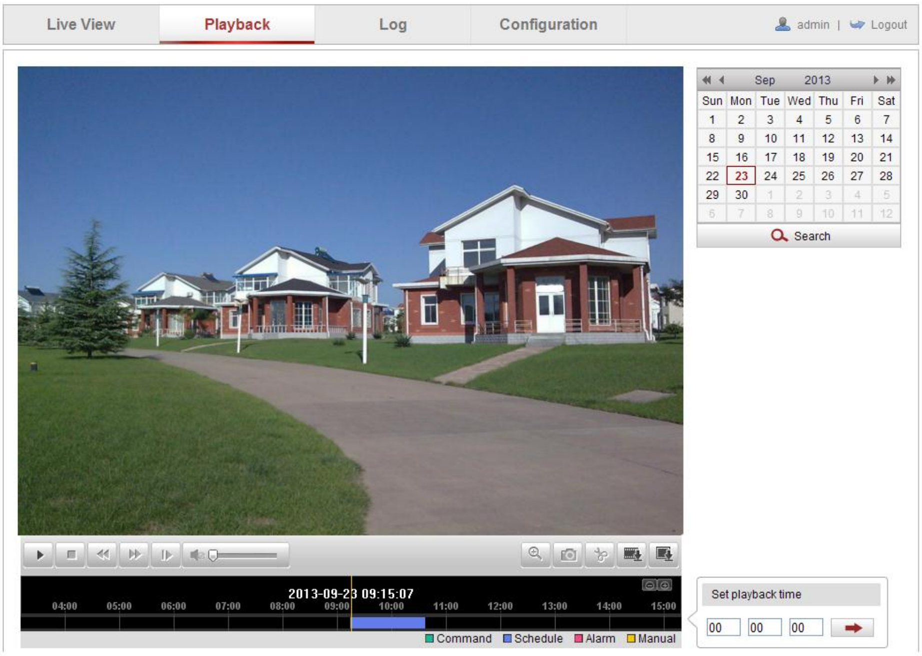
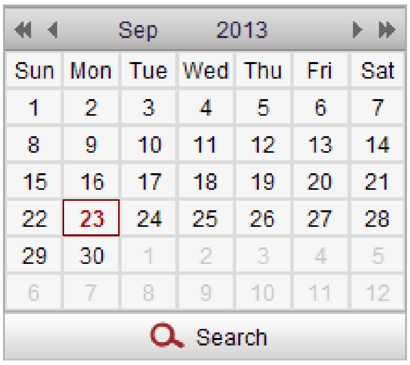


Figure 10-1 Playback Interface

2. Select the date and click **Search**.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Figure 10-2 Search Video

3. Click ▶ to play the video files found on this date.

The toolbar on the bottom of Playback interface can be used to control playing process.

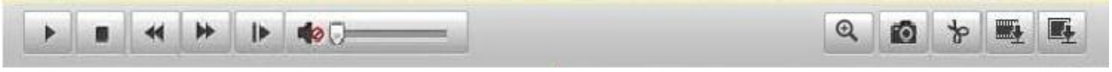


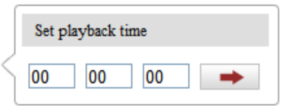
Figure 10-3 Playback Toolbar

Table 10-1 Description of the buttons

Button	Operation	Button	Operation
▶	Play	📷	Capture a picture
⏸	Pause	✂/✂	Start/Stop clipping video files
■	Stop	🔊 /🔇	Audio on and adjust volume/Mute
⏪	Speed down	⬇	Download video files
⏩	Speed up	⬇	Download captured pictures
⏯	Playback by frame	🔍/🔍	Enable/Disable digital zoom

Note: You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface. Please refer to *Section 7.1* for details.

Drag the progress bar with the mouse to locate the exact playback point. You can also input the time and click ➡ to locate the playback point in the **Set playback time** field. You can also click ⊖⊕ to zoom out/in the progress bar.



Set playback time

00 00 00 ➡

Figure 10-4 Set Playback Time

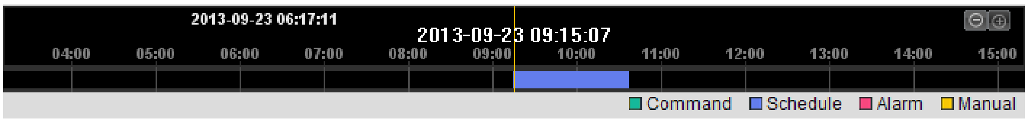
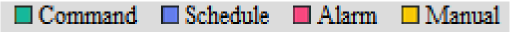


Figure 10-5 Progress Bar

The different colors of the video on the progress bar stand for the different video types.



🟩 Command 🟦 Schedule 🟥 Alarm 🟨 Manual

Figure 10-6 Video Types

Chapter 11 Log Searching

Purpose:

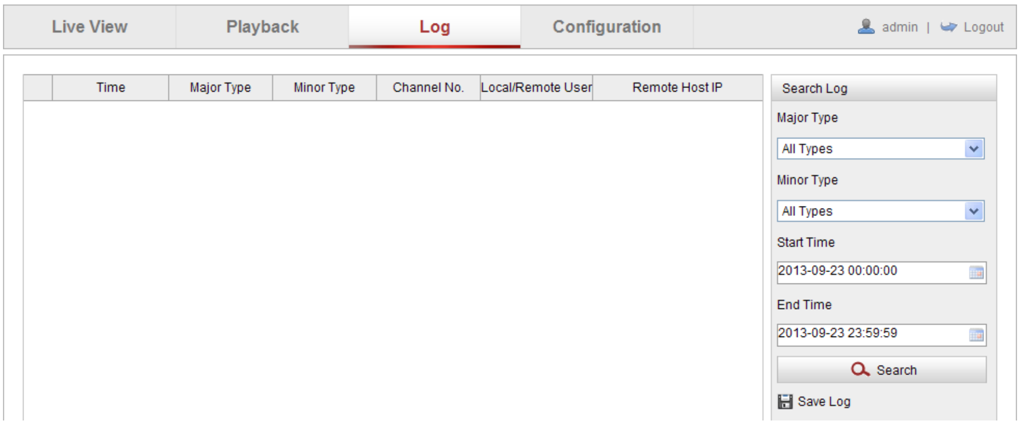
The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

Please configure network storage for the camera or insert a SD card in the camera.

Steps:

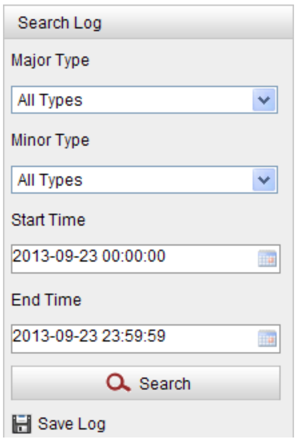
1. Click **Log** on the menu bar to enter log searching interface.



Major Type: All Types
Minor Type: All Types
Start Time: 2013-09-23 00:00:00
End Time: 2013-09-23 23:59:59

Figure 11-1 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
3. Click **Search** to search log files. The matched log files will be displayed on the **Log** interface.



Major Type: All Types
Minor Type: All Types
Start Time: 2013-09-23 00:00:00
End Time: 2013-09-23 23:59:59

Figure 11-2 Log Searching

4. To export the log files, click **Save log** to save the log files in your computer.

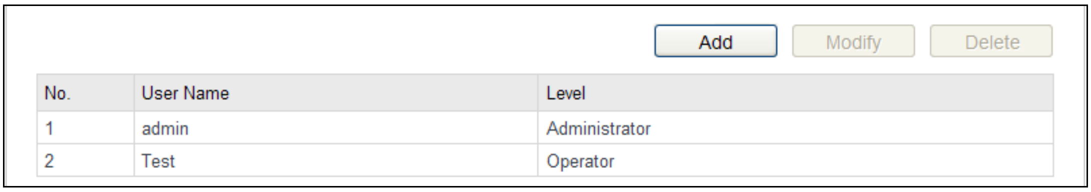
Chapter 12 Others

12.1 Managing User Accounts

Enter the User Management interface:

Configuration >Basic Configuration> Security > User

Or Configuration > Advanced Configuration> Security > User



No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Figure 12-1 User Information

- Change the Admin Password

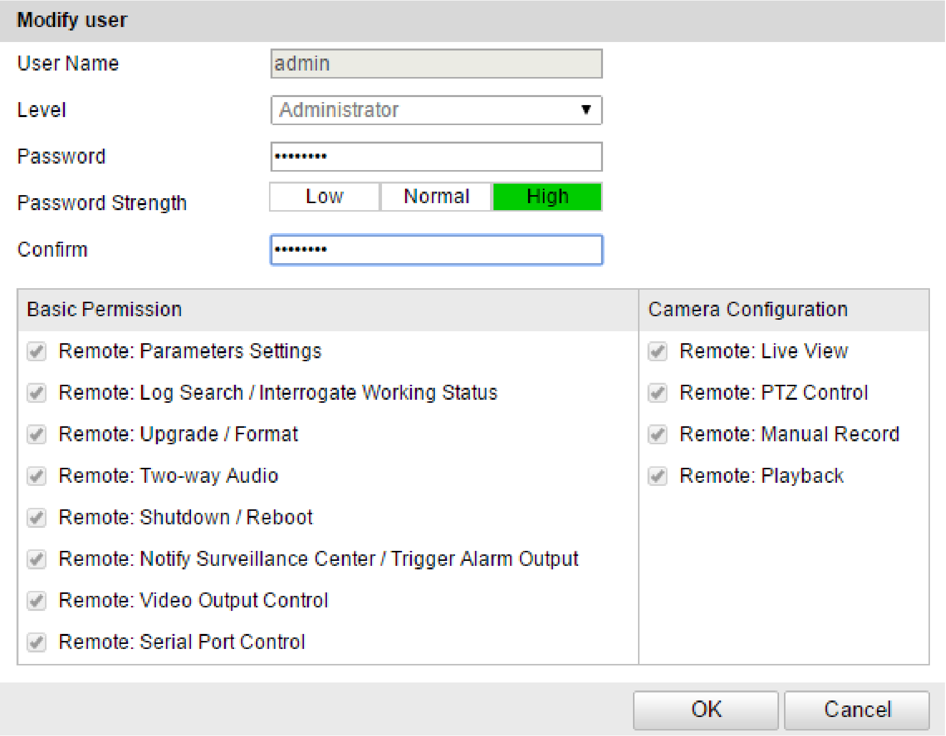
<u>YOU MUST CHANGE THE DEFAULT PASSWORD</u> – The default Admin account password (12345) is for first-time log-in purposes only.

Steps:

1. Select the *admin* user from the user list on the User Management interface.
2. Click **Modify** to enter the Modify User page.
3. Input the new password in the Password text field.
4. Input the confirm password in the Confirm text field.
5. Click **OK** to save the settings.

Notes:

- The system will judge the password strength automatically and it is highly recommended to set a password with high security level to ensure the security. A good password should contain no less than 6 characters, and is the combination of numeric, upper case letters and lower case letters.
- The *admin* user has all permissions by default and can create / modify / delete other accounts.
- The *admin* user cannot be deleted and you can only change the *admin* password.



Modify user

User Name	admin
Level	Administrator ▼
Password	••••••••
Password Strength	Low · Normal · 🟩 High
Confirm	••••••••

Basic Permission	Camera Configuration
☑ Remote: Parameters Settings	☑ Remote: Live View
☑ Remote: Log Search / Interrogate Working Status	☑ Remote: PTZ Control
☑ Remote: Upgrade / Format	☑ Remote: Manual Record
☑ Remote: Two-way Audio	☑ Remote: Playback
☑ Remote: Shutdown / Reboot	
☑ Remote: Notify Surveillance Center / Trigger Alarm Output	
☑ Remote: Video Output Control	
☑ Remote: Serial Port Control	

Figure 12-2 Change the Admin Password

- Add a User

Steps:

1. Click **Add** to add a user.
2. Input the **User Name**, select **Level** and input **Password.**

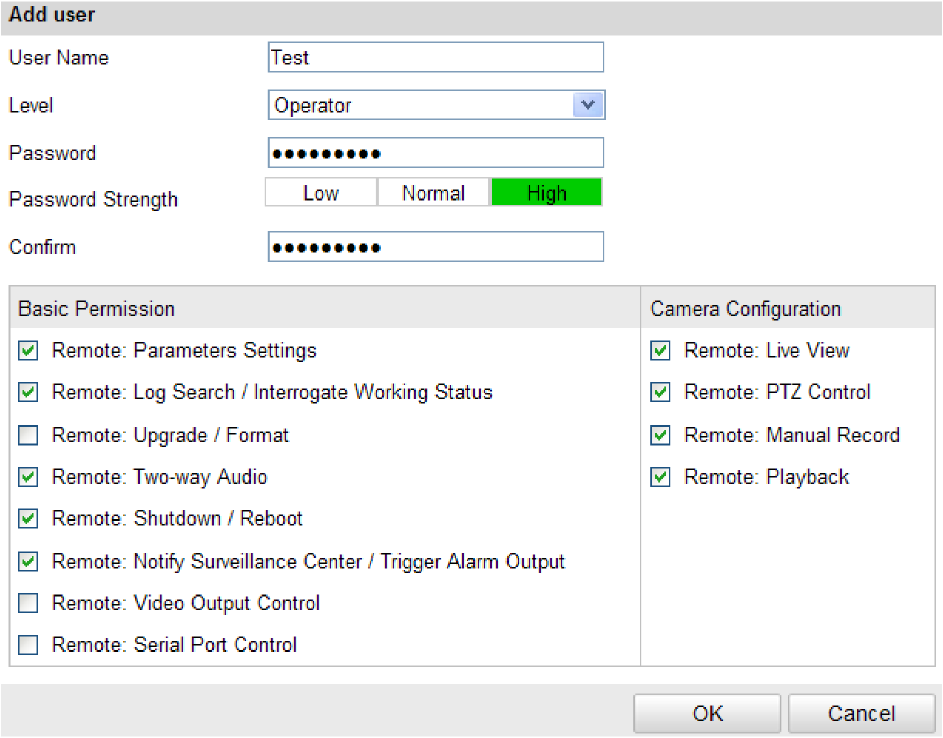
Notes:

- Up to 31 user accounts can be created.
- Different level user owns different permissions. Operator and user are selectable.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions for the new user.
4. Click **OK** to finish the user addition.



Add user

User Name: Test

Level: Operator

Password: ●●●●●●●●●

Password Strength: Low | Normal | High

Confirm: ●●●●●●●●●

Basic Permission	Camera Configuration
☑ Remote: Parameters Settings	☑ Remote: Live View
☑ Remote: Log Search / Interrogate Working Status	☑ Remote: PTZ Control
□ Remote: Upgrade / Format	☑ Remote: Manual Record
☑ Remote: Two-way Audio	☑ Remote: Playback
☑ Remote: Shutdown / Reboot	
☑ Remote: Notify Surveillance Center / Trigger Alarm Output	
□ Remote: Video Output Control	
□ Remote: Serial Port Control	

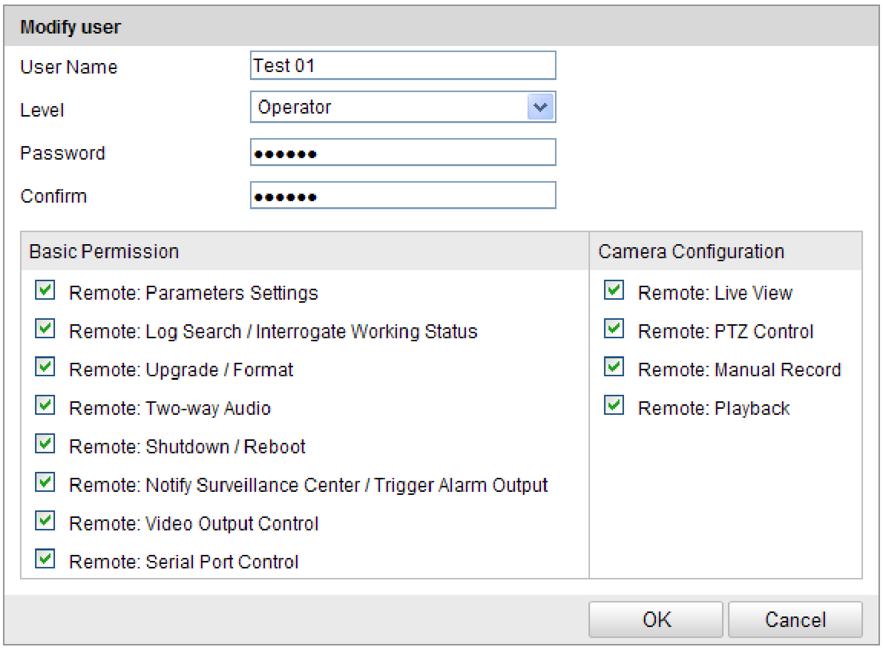
Figure 12-3 Add a User

- Modify a User

Steps:

1. Left-click to select the user from the list and click **Modify**.
2. Modify the User Name, Level or Password.
3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions.
4. Click **OK** to finish the user modification.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*



Modify user

User Name: Test 01

Level: Operator

Password: ●●●●●●

Confirm: ●●●●●●

Basic Permission

☑ Remote: Parameters Settings
☑ Remote: Log Search / Interrogate Working Status
☑ Remote: Upgrade / Format
☑ Remote: Two-way Audio
☑ Remote: Shutdown / Reboot
☑ Remote: Notify Surveillance Center / Trigger Alarm Output
☑ Remote: Video Output Control
☑ Remote: Serial Port Control

Camera Configuration

☑ Remote: Live View
☑ Remote: PTZ Control
☑ Remote: Manual Record
☑ Remote: Playback

Figure 12-4 Modify a User

- Delete a User

Steps:

1. Click to select the user you want to delete and click **Delete**.
2. Click **OK** on the pop-up dialogue box to delete the user.

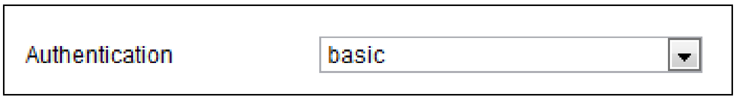
12.2 RTSP Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface: Configuration> Advanced Configuration> Security > RTSP Authentication



Authentication: basic

Figure 12-5 RTSP Authentication

2. Select the RTSP **Authentication** type **basic** or **disable** in the drop-down list to enable or disable the RTSP authentication.

Note: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol via the IP address.

3. Click **Save** to save the settings.

12.3 Anonymous Visit

Purpose:

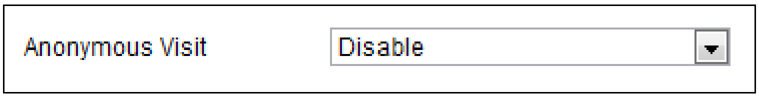
Enabling this function allows visit for whom doesn't have the user name and password of the device.

Note: Only live view is available for the anonymous user.

Steps:

1. Enter the Anonymous Visit interface:

Configuration> Advanced Configuration> Security > Anonymous Visit

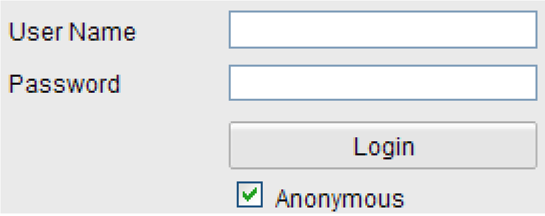


Anonymous Visit: Disable

Figure 12-6 Anonymous Visit

2. Set the **Anonymous Visit** permission **Enable** or **Disable** in the drop-down list to enable or disable the anonymous visit.
3. Click **Save** to save the settings.

There will be a checkbox of Anonymous by the next time you logging in.



User Name:

Password:

Login

☑ Anonymous

Figure 12-7 Login Interface with an Anonymous Checkbox

4. Check the checkbox of **Anonymous** and click **Login**.

By permitting the Anonymous "Live View" function, you may enable others to access your camera and view live images without providing login credentials. It therefore is critical when permitting the Anonymous "Live View" function to ensure that your camera's field of view does not impact the privacy of individuals whose images might be captured without authorization.

Given its inherent intrusiveness, video surveillance is inappropriate in areas where people have a higher expectation of privacy.

12.4 IP Address Filter

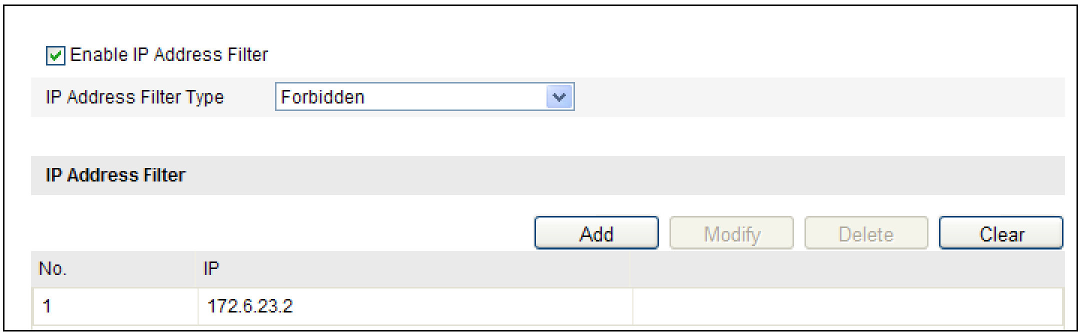
Purpose:

This function makes it possible for access control.

Steps:

1. Enter the IP Address Filter interface:

Configuration> Advanced Configuration> Security > IP Address Filter



☑ Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter

No.	IP
1	172.6.23.2

Figure 12-8 IP Address Filter Interface

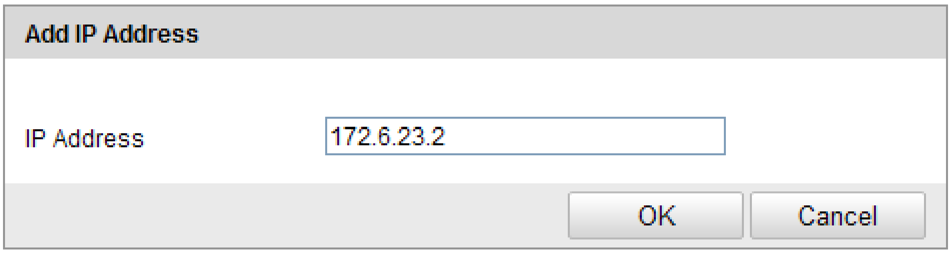
2. Check the checkbox of Enable IP Address Filter.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.

- Add an IP Address

Steps:

(1) Click the **Add** to add an IP.

(2) Input the IP Adreess.



Add IP Address

IP Address: 172.6.23.2

Figure 12-9 Add an IP

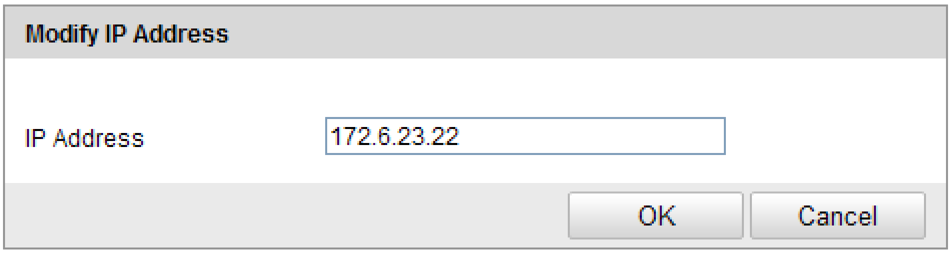
(3) Click the **OK** to finish adding.

- Modify an IP Address

Steps:

(1) Left-click an IP address from filter list and click **Modify**.

(2) Modify the IP address in the text filed.



Modify IP Address

IP Address: 172.6.23.22

Figure 12-10 Modify an IP

(3) Click the **OK** to finish modifying.

- Delete an IP Address

Left-click an IP address from filter list and click **Delete**.

- Delete all IP Addresses

Click **Clear** to delete all the IP addrsses.

5. Click **Save** to save the settings.

12.5 Viewing Device Information

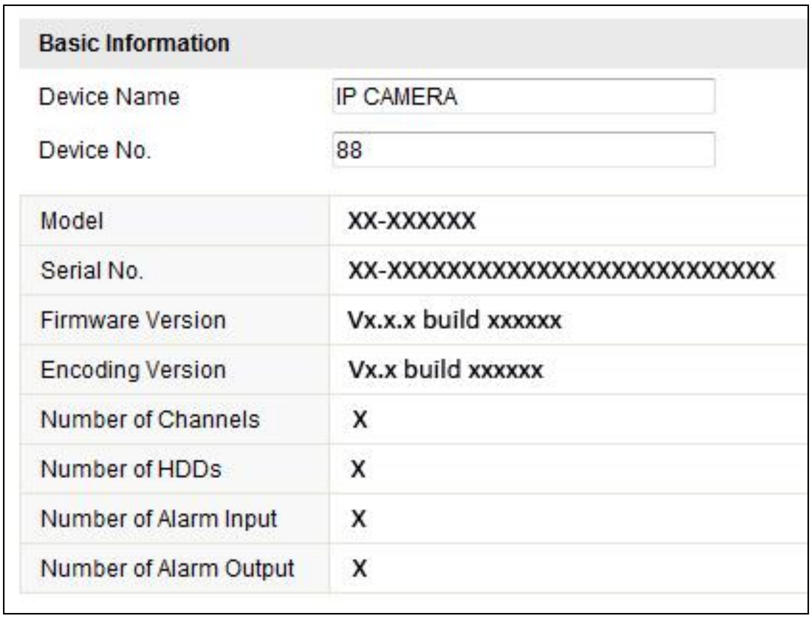
Enter the Device Information interface:

Configuration > Basic Configuration> System > Device Information

Or Configuration > Advanced Configuration> System > Device Information

In the **Device Information** interface, you can edit the Device Name.

Other information of the parking camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.



Basic Information

Device Name	IP CAMERA
Device No.	88
Model	XX-XXXXXX
Serial No.	XX-XXXXXXXXXXXXXXXXXXXXXXXXXX
Firmware Version	Vx.x.x build xxxxxx
Encoding Version	Vx.x build xxxxxx
Number of Channels	X
Number of HDDs	X
Number of Alarm Input	X
Number of Alarm Output	X

Figure 12-11 Device Information

12.6 Maintenance

12.6.1 Rebooting the Camera

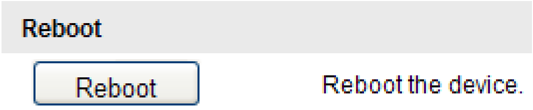
Steps:

1. Enter the Maintenance interface:

Configuration > Basic Configuration> System > Maintenance

Or Configuration > Advanced Configuration> System > Maintenance:

2. Click **Reboot** to reboot the parking camera.



Reboot

Reboot

Reboot the device.

Figure 12-12 Reboot the Device

12.6.2 Restoring Default Settings

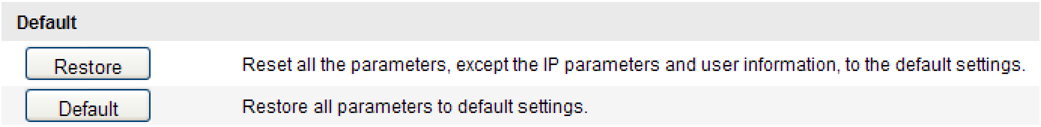
Steps:

1. Enter the Maintenance interface:

Configuration > Basic Configuration> System > Maintenance

Or Configuration > Advanced Configuration> System > Maintenance

2. Click **Restore** or **Default** to restore the default settings.



Default

Restore — Reset all the parameters, except the IP parameters and user information, to the default settings.

Default — Restore all parameters to default settings.

Figure 12-13 Restore Default Settings

Note: After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.

12.6.3 Exporting / Importing Configuration File

Purpose:

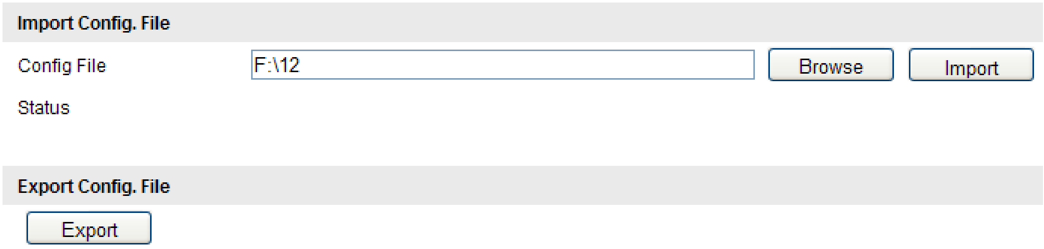
Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

Steps:

1. Enter the Maintenance interface:
   Configuration > Basic Configuration> System > Maintenance
   Or Configuration>Advanced Configuration> System > Maintenance
2. Click **Export** to export the current configuration file, and save it to the certain place.
3. Click **Browse** to select the saved configuration file and then click **Import** to start importing configuration file.

Note: You need to reboot the camera after importing configuration file.

4. Click **Export** and set the saving path to save the configuration file in local storage**.**



Import Config. File

Config File F:\12

Status

Export Config. File

Figure 12-14 Import/Export Configuration File

12.6.4 Upgrading the System

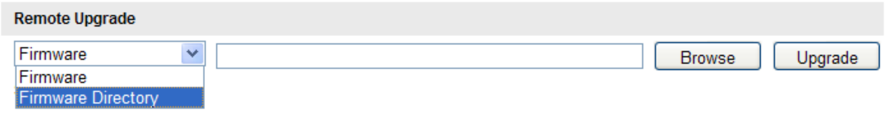
Steps:

1. Enter the Maintenance interface: Configuration > Basic Configuration> System > Maintenance , or Configuration > Advanced Configuration> System > Maintenance
2. Select firmware or firmware directory to locate the upgrade file.

Firmware: Locate the exact path of the upgrade file.

Firmware Directory: Only the directory the upgrade file belongs to is required.

3. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.



Remote Upgrade

Firmware

Figure 12-15 Remote Upgrade

Note: The upgrading process will take 1~10 minutes. Please don't disconnect power of the camera during the process, and the camera reboots automatically after upgrade.

12.7 RS-485 Settings

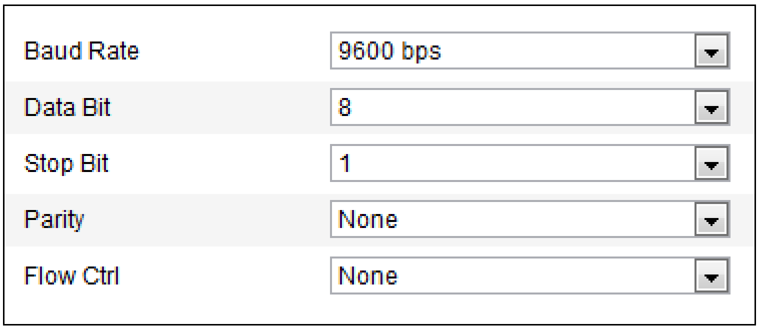
Purpose:

The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Enter RS-485 Port Setting interface:

Configuration> Advanced Configuration> System > RS485



Baud Rate	9600 bps
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None

Figure 12-16 RS-485 Settings

2. Set the RS-485 parameters and click **Save** to save the settings.

By default, the Baud Rate is set as 9600 bps, the Data Bit is 8, the stop bit is 1 and the Parity and Flow Control is None.

Note: The Baud Rate, PTZ Protocol and PTZ Address parameters should be exactly the same as the PTZ camera parameters.

12.8 Service Settings

Purpose:

Telnet function provides an easy way to get access to the camera. You can see the advanced information about the camera by inputting command; as well the configuration can also be realized through telnet connection.

Steps:

1. Go to Configuration> Advanced Configuration> System > Service to enter the service settings interface.
2. Check the checkbox of Telnet.
3. Click the **Save** button to save the settings.

Appendix

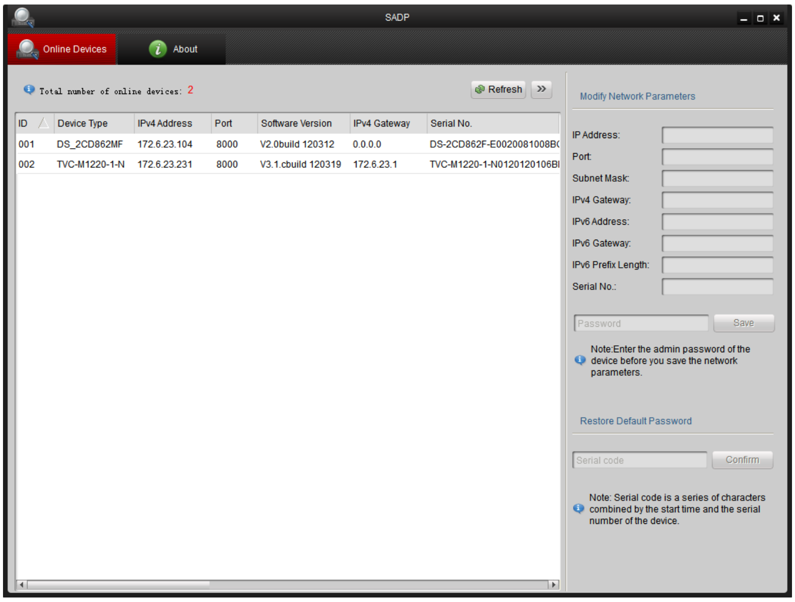
Appendix 1 SADP Software Introduction

- Description of SADP V 2.0

SADP (Search Active Devices Protocol) is a user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

- Search active devices online
  - ♦ Search online devices automatically

After launch the SADP software, it automatically searches the online devices every 15 seconds from the subnet where your computer locates. It displays the total number and information of the searched devices in the Online Devices interface. Device information including the device type, IP address, port number, gateway, etc. will be displayed.



Total number of online devices: 2

ID	Device Type	IPv4 Address	Port	Software Version	IPv4 Gateway	Serial No.
001	DS_2CD862MF	172.6.23.104	8000	V2.0build 120312	0.0.0.0	DS-2CD862F-E0020081008B(
002	TVC-M1220-1-N	172.6.23.231	8000	V3.1.cbuild 120319	172.6.23.1	TVC-M1220-1-N0120120106BI

Modify Network Parameters

IP Address:
Port:
Subnet Mask:
IPv4 Gateway:
IPv6 Address:
IPv6 Gateway:
IPv6 Prefix Length:
Serial No.:

Note:Enter the admin password of the device before you save the network parameters.

Restore Default Password

Note: Serial code is a series of characters combined by the start time and the serial number of the device.

Figure 12-17 Figure A.1.1 Search Online Devices

Figure 12-18 ***Note:*** Device can be searched and displayed in the list in 15 seconds after it went online; it will be removed from the list in 45 seconds after it went offline.

- ♦ Search online devices manually

You can also click **Refresh** to refresh the online device list manually. The newly searched devices will be added to the list.

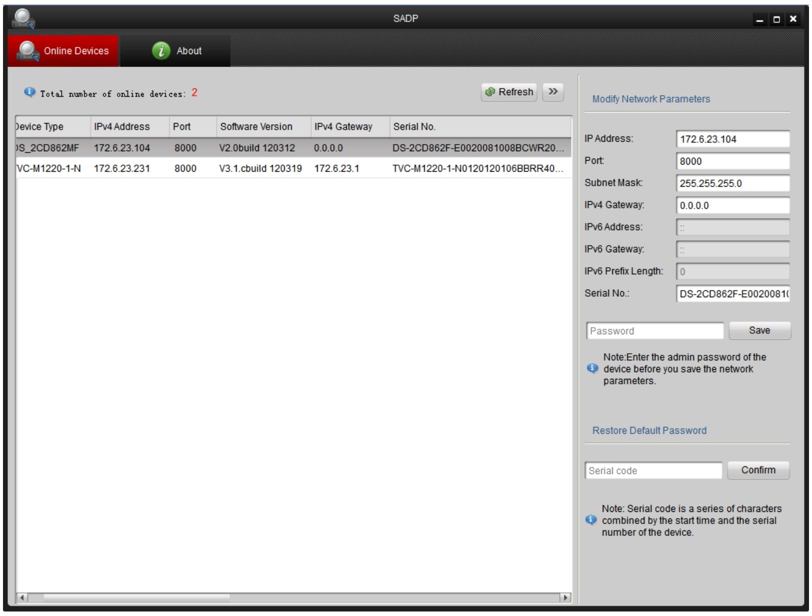
Note: You can click △ or ▽ on each column heading to order the information; you can click » to expand the device table and hide the network parameter panel on the right side, or click « to show the network parameter panel.

- Modify network parameters

Steps:

1. Select the device to be modified in the device list and the network parameters of the device will be displayed in the **Modify Network Parameters** panel on the right side.
2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the password of the *admin* account of the device in the **Password** field and click **Save** to save the changes.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*



Total number of online devices: 2

Device Type	IPv4 Address	Port	Software Version	IPv4 Gateway	Serial No.
DS_2CD862MF	172.6.23.104	8000	V2.0build 120312	0.0.0.0	DS-2CD862F-E0020081008BCWR20...
TVC-M1220-1-N	172.6.23.231	8000	V3.1.cbuild 120319	172.6.23.1	TVC-M1220-1-N0120120106BBRR40...

Modify Network Parameters

IP Address: 172.6.23.104
Port: 8000
Subnet Mask: 255.255.255.0
IPv4 Gateway: 0.0.0.0
IPv6 Address: ::
IPv6 Gateway: ::
IPv6 Prefix Length: 0
Serial No.: DS-2CD862F-E0020081(

Note:Enter the admin password of the device before you save the network parameters.

Restore Default Password

Note: Serial code is a series of characters combined by the start time and the serial number of the device.

Figure 12-19 Figure A.1.2 Modify Network Parameters

- Restore default password

Note:

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user. You have the responsibility to keep you password properly.

Steps:

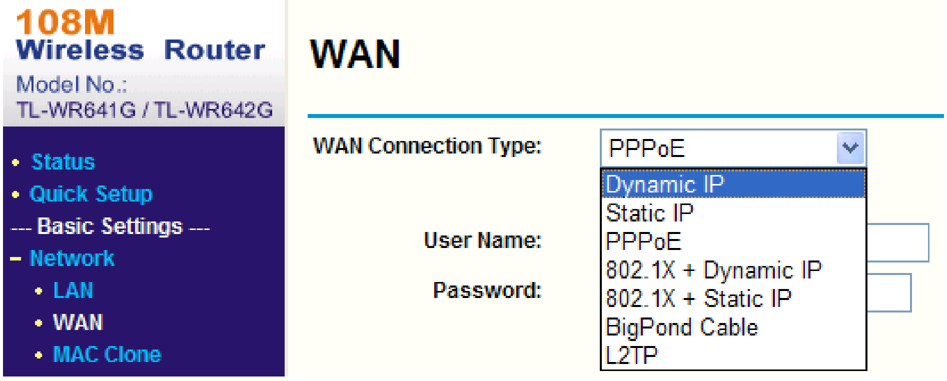
1. Contact our technical engineers to get the serial code.
2. Input the code in the **Serial code** field and click **Confirm** to restore the default password.

Appendix 2 Port Mapping

The following settings are for TP-LINK router (TL-WR641G). The settings vary depending on different models of routers.

Steps:

1. Select the **WAN Connection Type**, as shown below:



WAN

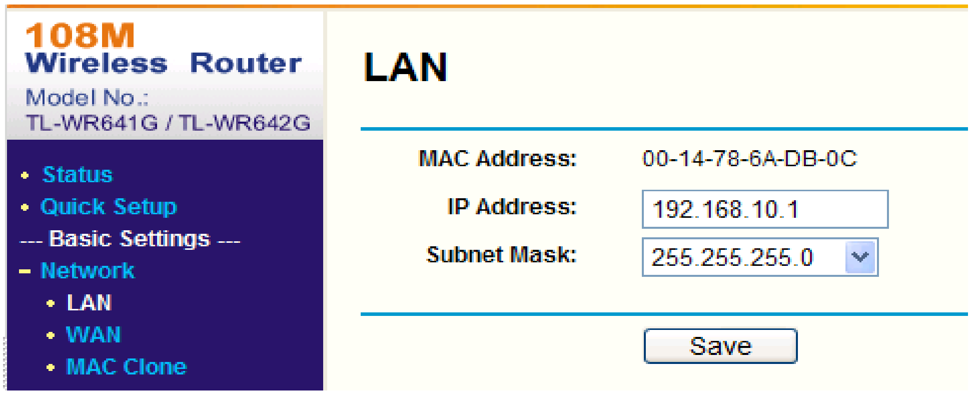
WAN Connection Type: PPPoE

User Name:

Password:

Figure 12-20 Figure A.2.1 Select the WAN Connection Type

2. Set the **LAN** parameters of the router as in the following figure, including IP address and subnet mask settings.



LAN

MAC Address: 00-14-78-6A-DB-0C

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Figure 12-21 Figure A.2.2 Set the LAN parameters

3. Set the port mapping in the virtual severs of **Forwarding**. By default, camera uses port 80, 8000 and 554. You can change these ports value with web browser or client software.

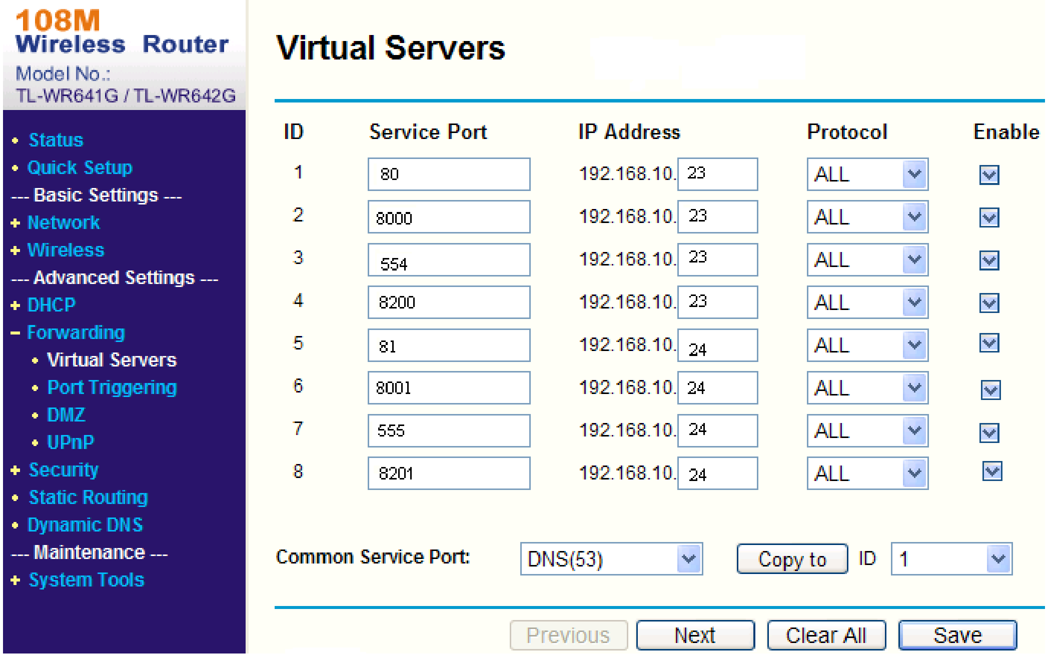
Example:

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24. Refer to the steps below:

Steps:

1. As the settings mentioned above, map the port 80, 8000, 554 and 8200 for the parking camera at 192.168.1.23
2. Map the port 81, 8001, 555 and 8201 for the parking camera at 192.168.1.24.
3. Enable **ALL** or **TCP** protocols.

4. Check the **Enable** checkbox and click **Save** to save the settings.



Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☑
2	8000	192.168.10.23	ALL	☑
3	554	192.168.10.23	ALL	☑
4	8200	192.168.10.23	ALL	☑
5	81	192.168.10.24	ALL	☑
6	8001	192.168.10.24	ALL	☑
7	555	192.168.10.24	ALL	☑
8	8201	192.168.10.24	ALL	☑

Common Service Port: DNS(53) Copy to ID 1

Figure 12-22 Figure A.2.3 Port Mapping

Note: The port of the parking camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

0502061041131

First Choice for Security Professionals

Grupo Instaladores

ventas@rosarioseguridad.com.ar
rosarioseguridadok
https://www.facebook.com/groups/591852618012744/

☎ +54 9 341 6708000
Rosario Seguridad
+54 9 341 6591429

☎ +54 9 341 6799822
Rosario Seguridad
☎ +54 9 341 4577532

Avenida Presidente Perón 3998 - Rosario - Santa Fe - Argentina

ROSARIO SEGURIDAD