Mobile Network Camera

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class 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 RE Directive 2014/53/EU, EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, 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

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Note	Provides additional information to emphasize or supplement important points of the main text.
Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet limited power source or PS2 requirements according to the IEC60950-1 or IEC 62368-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Product Features

This Network camera is a digital monitoring product that integrates video and audio acquisition, intelligent coding and compression, network transmission and other functions. With embedded operating system and high-performance hardware processing platform, it has high stability and reliability, and can meet the needs of various industries.

Based on Ethernet control, the network camera can realize image compression and transmit it to different users through the network. Centralized storage based on NAS can greatly facilitate the storage and call of data.

You can control the webcam through the browser, and set the webcam parameters, intelligent functions, audio and video parameters, image parameters, etc. through the browser. Please refer to the actual equipment for specific function parameters.

1.2 Product Function

This chapter explains the camera from the product function, so that you can get to know and get familiar with the camera more quickly.

System function

- Video recording and capturing pictures

The camera supports instant capture and video recording during preview, and can also configure video recording plan after installing memory card, so as to realize planned video recording.

- User Management

You can manage many different users through the administrator "admin" user, and configure different permissions for each user.

Network function

The camera supports TCP/IP, UDP and other network communication protocols; Support open interconnection protocols such as ONVIF.

The function of the product depends on the model, please refer to the technical parameters of the actual product.

Chapter 2 Operation Instructions

Note

- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.
- To ensure the network security of the network camera, we recommend you to have the network camera assessed and maintained termly. You can contact us if you need such service.

2.1 Setting the Network Camera over the LAN

Purpose:

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

Note

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

2.1.1 Wiring over the LAN

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

Purpose:

Step 1 To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.

Step 2 Refer to the Figure 2-2 to set network camera over the LAN via a switch or a router.

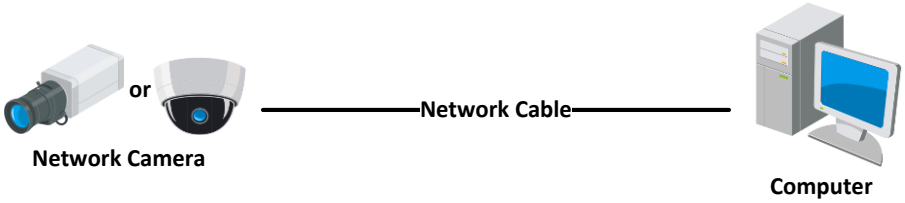


Figure 2-1 Connecting Directly

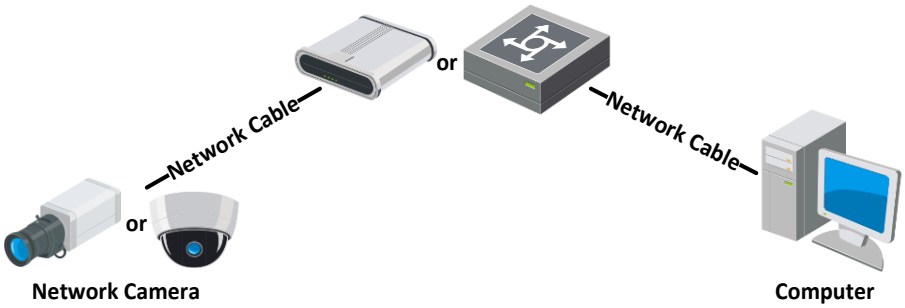


Figure 2-2 Connecting via a Switch or a Router

2.2 Activating the Camera

You are required to activate the camera first by setting a strong password for it before you can use the camera.

Activation via Web Browser, Activation via SADP is supported.

2.2.1 Activation via SADP Software

SADP software is used for detecting the online device, activating the camera, and resetting the password.

Get the SADP software from the official website, and install the SADP according to the prompts. Follow the steps to activate the camera.

Step 1 Run the SADP software to search the online devices.

Step 2 Check the device status from the device list, and select the inactive device.

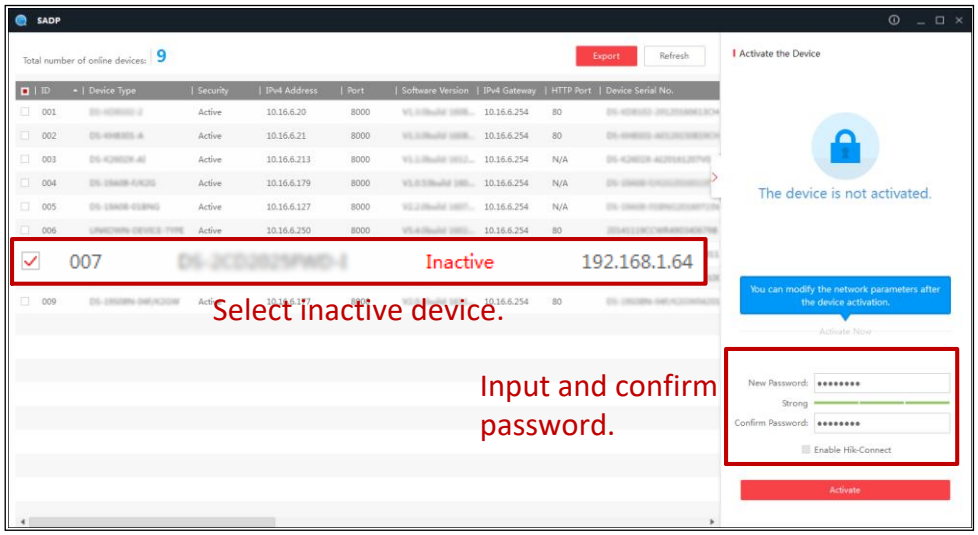


Figure 2-3 SADP Interface

Note

The SADP software supports activating the camera in batch. Refer to the user manual of SADP software for details.

Step 3 Create and input the password in the password field, and confirm the password. A password with user name in it is not allowed.

Caution

STRONG PASSWORD RECOMMENDED

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

You can enable the Hik-Connect service for the device during activation.

Step 4 Click Activate to start activation. You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and try again.

Step 5 Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

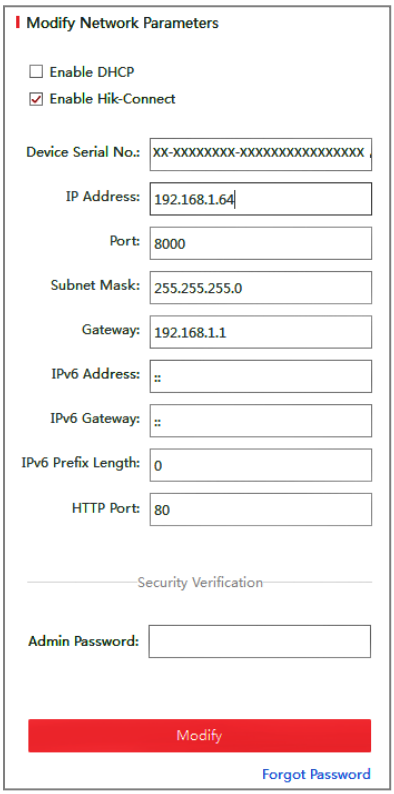


Figure 2-4 Modify the IP Address

Step 6 Input the admin password and click Modify to activate your IP address modification.

2.2.2 Activation via Web Browser

Step 1 Power on the camera, and connect the camera to the network.

Step 2 Input the IP address into the address bar of the web browser, and click Enter to enter the activation interface.

Note

- The default IP address of the camera is 192.168.1.64.
- The computer and the camera should belong to the same subnet.
- For the camera enables the DHCP by default, you need to use the SADP software to search the IP address.

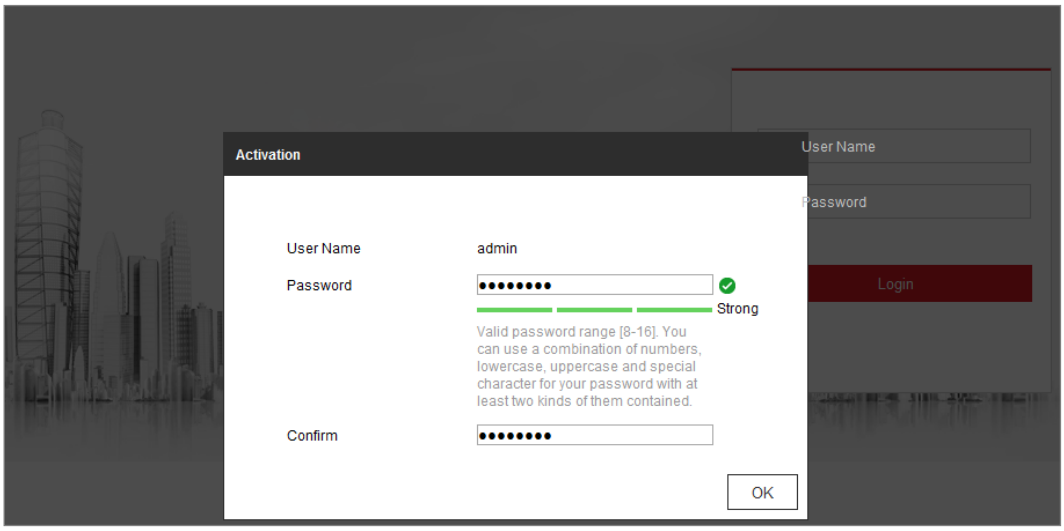


Figure 2-5 Activation via Web Browser

Step 3 Create and input a password into the password field. A password with user name in it is not allowed.

Caution

STRONG PASSWORD RECOMMENDED

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 Confirm the password.

Step 5 Click OK to save the password and enter the live view interface.

2.2.3 (Optional) Setting Security Question

Security question is used to reset the admin password when admin user forgets the password.

Admin user can follow the pop-up window to complete security question settings during camera activation. Or, admin user can go to User Management interface to set up the function.

2.3 Login and Logout

2.3.1 Login

For certain camera models, HTTPS is enabled by default and the camera creates an unsigned certificate automatically. When you access to the camera the first time, the web browser prompts a notification about the certificate issue.

To cancel the notification, install a signed-certificate to the camera.

Step 1 Open the web browser.

Step 2 In the browser address bar, input the IP address of the network camera, and press the Enter key to enter the login interface.

Note

The default IP address is 192.168.1.64. You are recommended to change the IP address to the same subnet with your computer.

Step 3 Input the user name and password.

The admin user should configure the device accounts and user/operator permissions properly. Delete the unnecessary accounts and user/operator permissions.

Note

The IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).

Figure 2-6 Login Interface

Step 4 Click **Login**.

Step 5 (Optional) Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.

Table 2-1 Install Plugins

OS	Browser Version	Plugin
Windows	• IE 8 and upper	Install the plugin according to instructions.
	• Google Chrome 57 and upper • Mozilla Firefox 52 and upper • Edge and upper	Click  in the preview page to download and install the plugin for high quality view and device functions.
Mac OS	• Google Chrome 57 and upper • Mozilla Firefox 52 and upper • Mac Safari 16 and upper • Edge and upper	To preview, enter Configuration > Network > Advanced Setting > Network Service, and enbale WebSocket. Some functions will be limited after enbling this function, such as video play. The actual equipment shall prevail.

Note

The camera supports only Windows and Mac OS, not Linux.

2.3.2 Logout

To logout, click the  icon.

2.4 Main Interface

The main interface is shown as follows.

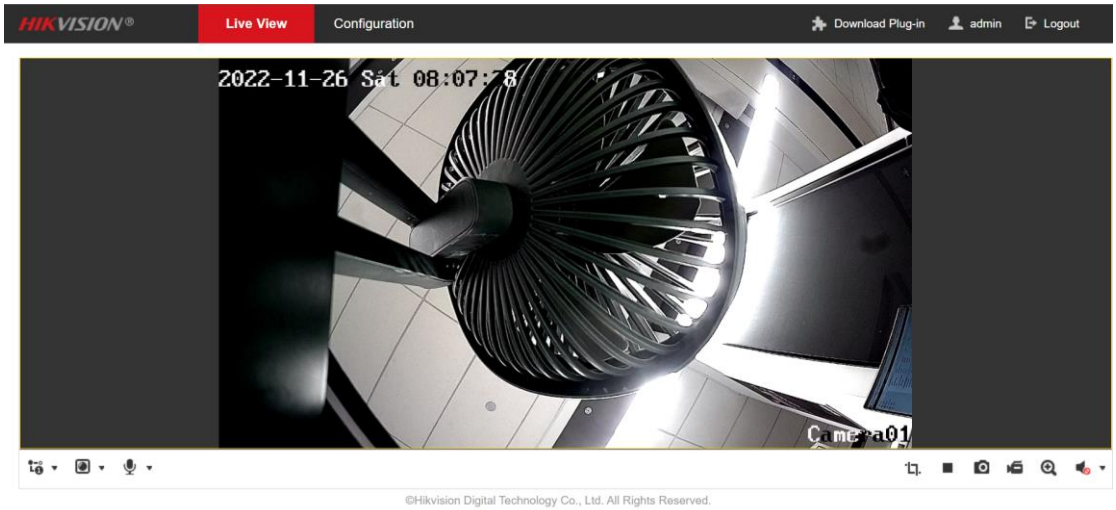


Figure 2-7 Main Interface

Live View: to view the camera and set parameters.

Configuration: to set the system and function parameters.

Note

The interface may vary according to the model of the camera.

Chapter 3 Basic Functions

3.1 Local Parameters

Click Configuration on the main interface to enter the configuration page, where the user can set up system, network, video/audio, image and storage parameters.

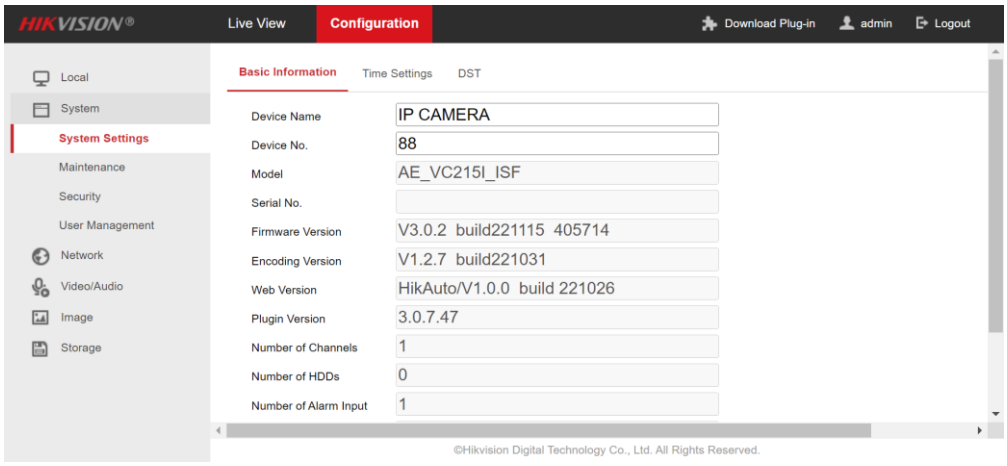


Figure 3-1 Configuration Page Overview

Go to **Configuration > Local** to configure local configurations. Live View Parameters, Record File Settings, Picture and Clip Settings can be configured.

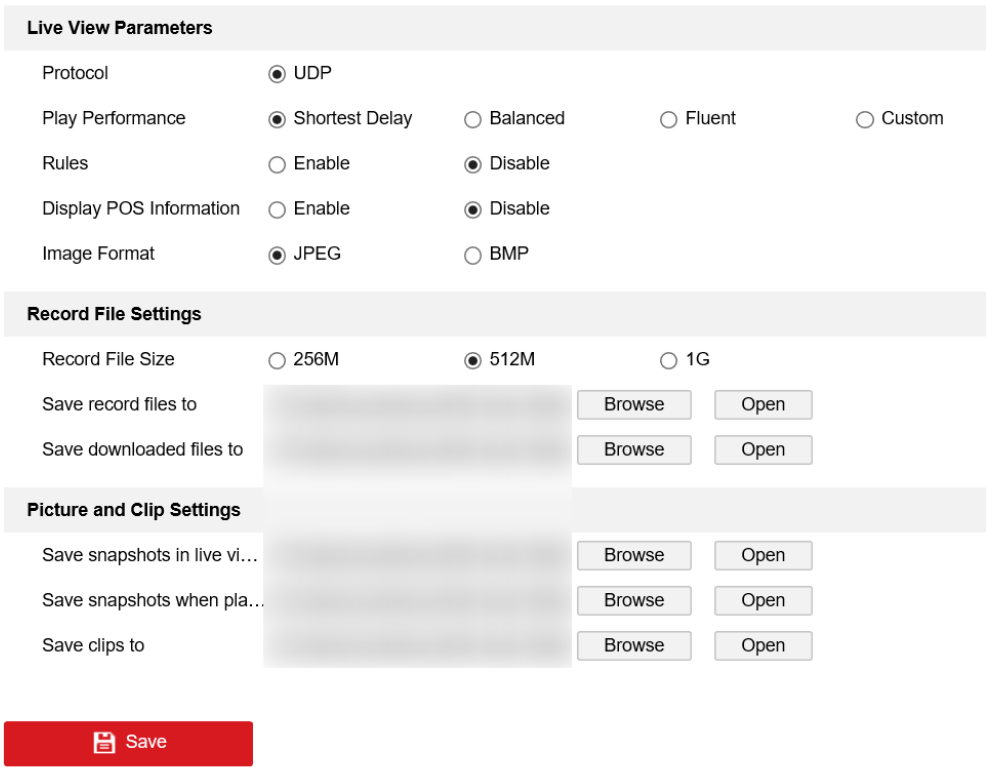


Figure 3-2 Local Parameters

Note

The playback function of this camera may vary according to different types. Please refer to the actual product.

3.1.1 Live View Parameters

- Protocols

The default protocol is UDP, which is suitable for the situation that the requirement of video fluency is not high and the network environment is unstable.

- Play Performance:

You can choose the shortest delay, Balanced, Fluent and Custom, and the default is Custom.

- Shortest delay: Real-time is good, but it may affect the fluency of video.
- Balanced: Give consideration to the real-time and fluency of video playback.
- Good fluency: In the same network situation, it takes up less network resources, and the video is smoother than other modes.
- Custom: the frame rate can be set according to the network conditions.
- Display POS Information: You can choose to enable or disable it. When enabled, information boxes will appear on the live screen, including the dynamic analysis box of motion detection and the face target box.
- Picture and Clip Settings: set the format of captured pictures, with optional JPEG and BMP.

3.1.2 Record File Setting

- Record File Size: it can be set to 256 M, 512 M and 1 G, indicating the size of a single video file stored locally.
- Save record files to: the path where video files are stored locally. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.

3.1.3 Picture and Clip Setting

- Save snapshots in live view to: the path where the captured pictures are stored locally during preview. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.

3.2 Live View

3.2.1 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 network 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:

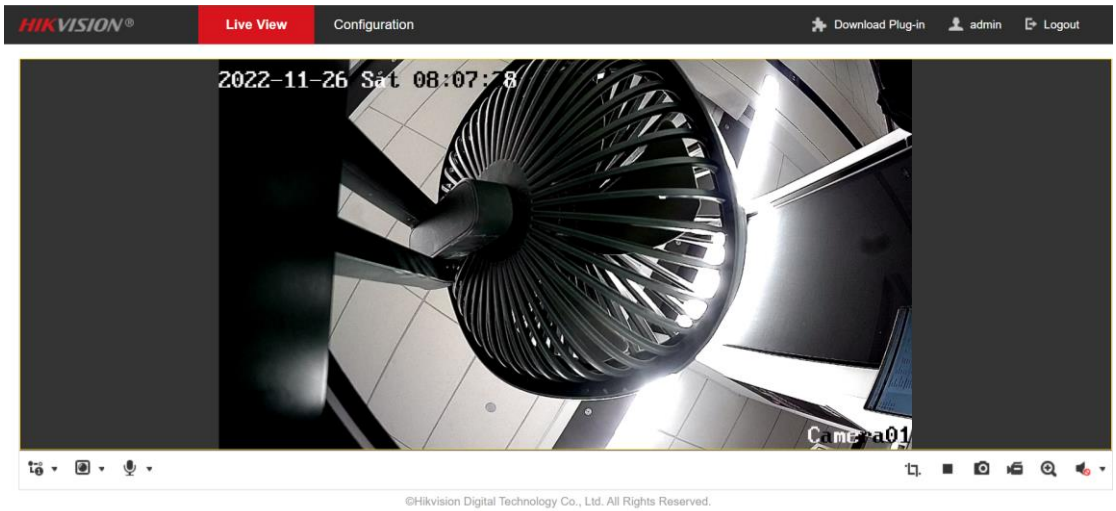


Figure 3-3 Live View Page

- Menu Bar

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

- Live View Window

Display the live video.

- Toolbar

Toolbar allows you to adjust the live view window size, the stream type, and the plug-ins. It also allows you to process the operations on the live view page, e.g., start/stop live view, capture, record, audio on/off, two-way audio, start/stop digital zoom, etc.

For IE (Internet Explorer) users, plug-ins as webcomponents and quick time are selectable. And for Non-IE users, webcomponents, quick time, VLC or MJPEG are selectable if they are supported by the web browser.

Note

For camera that supports plug-in free live view, when Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version are used, plug-in installation is not required. But Picture and Playback functions are hidden. To use mentioned

function via web browser, change to their lower versions, or change to Internet Explorer 8.0 and its above version.

3.2.2 Starting Live View

In the live view window, click ▶ on the toolbar to start the live view of the camera.

Figure 3-4 Live View Toolbar

Table 3-1 Descriptions of the Toolbar

Icon	Description
▶/■	Start/Stop live view.
	Supported video streams vary according to camera models.
	Click to select the third-party plug-in.
	Manually capture the picture.
/	Manually start/stop recording.
/	Audio on and adjust volume /Mute.
/	Start/stop digital zoom function.

Note

The icons vary according to the different camera models.

3.2.3 Record and Capture Pictures Manually

3.3 In the live view interface, click on the toolbar to capture the live pictures; click to record the live view. The saving paths of the captured pictures and clips can be set on the **Configuration** > **Local** page. To configure remote scheduled recording, please refer to 8.1 Storage Management

Steps:

Step 1 Go to **Configuration** > **Storage** > **Storage Management** > **HDD Management**, in which you can view the capacity, free space, status, type and property of the storage media.

Step 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.

Step 3 When the initialization completed, the status of disk will become **Normal**.

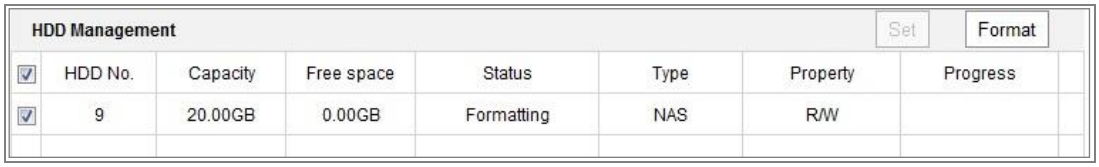


Figure 3-5 View Disk Status

Record Schedule.

Note

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

Chapter 4 System Configuration

4.1 Configure System Settings

Purpose:

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

4.1.1 Check Device Information

Step 1 Go to **Configuration** > **System** > **System Settings** > **Basic Information**.

Step 2 Edit the **Device Name** and **Device No.**

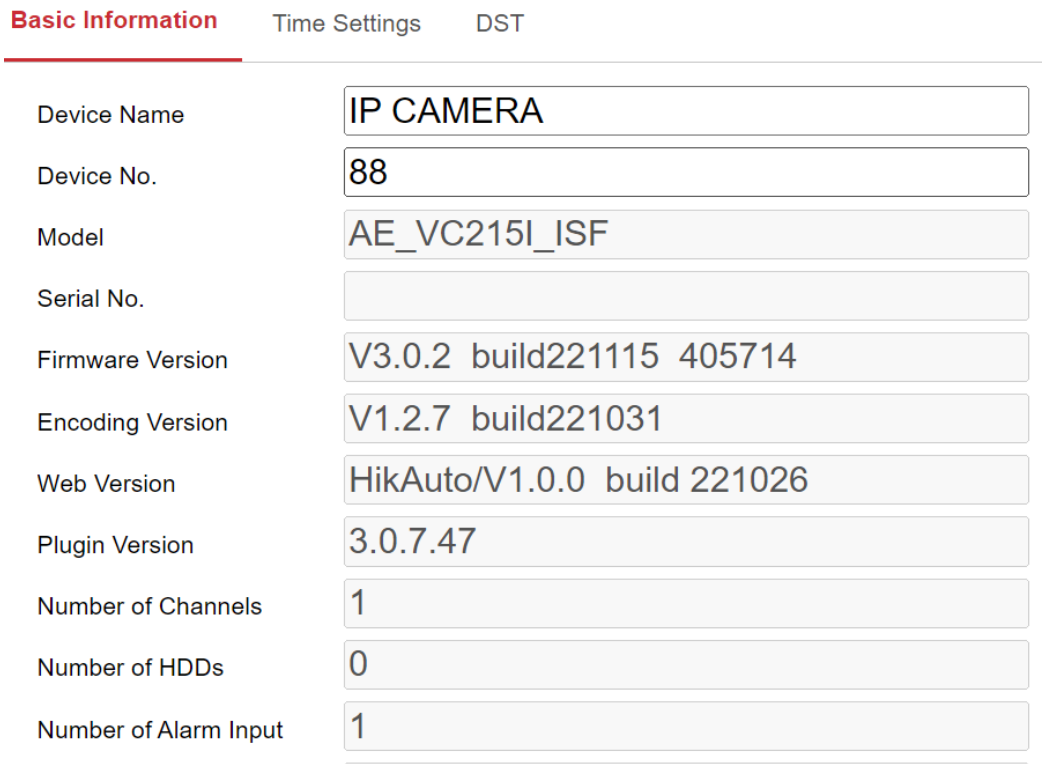


Figure 4-1 Basic Information

Note

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

4.1.2 Time Settings

Purpose:

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

Step 1 Go to **Configuration** > **System**> **System Settings** > **Time Settings**.

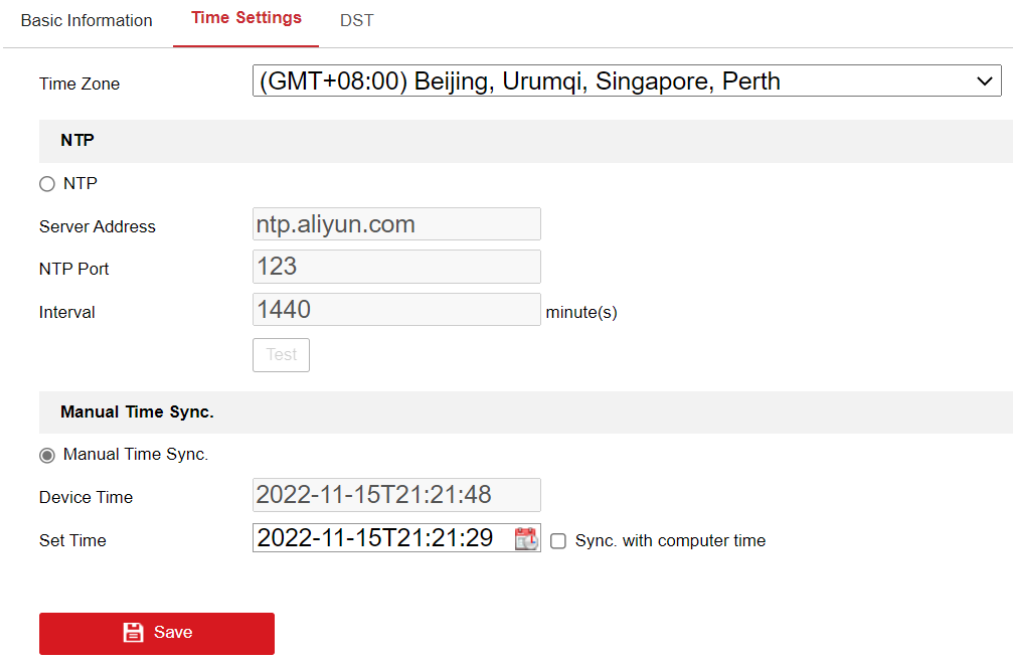


Figure 4-2 Time Settings

Step 2 Select the Time Zone of your location from the drop-down menu.

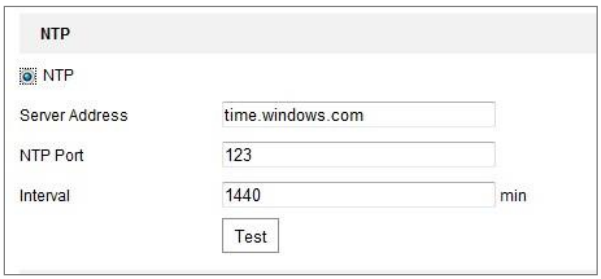
Step 3 Configure the NTP settings.

Step 4 Click to enable the NTP function.

Step 5 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.

Step 6 (Optional) You can click the Test button to test the time synchronization function via NTP server.



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.

Step 7 Configure the manual time synchronization.

1) Check the Manual Time Sync. item to enable the manual time synchronization function.
2) Click the icon to select the date, time from the pop-up calendar.
3) (Optional) You can check Sync. with computer time item to synchronize the time of the device with that of the local PC.

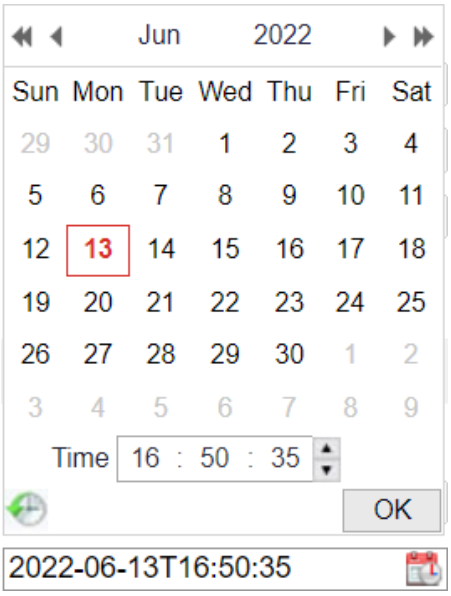


Figure 4-3 Time Sync Manually

Step 8 Click Save to save the settings.

4.1.3 DST

Purpose:

Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Step 1 Go to **Configuration** > **System** > **System Settings** > **DS**T

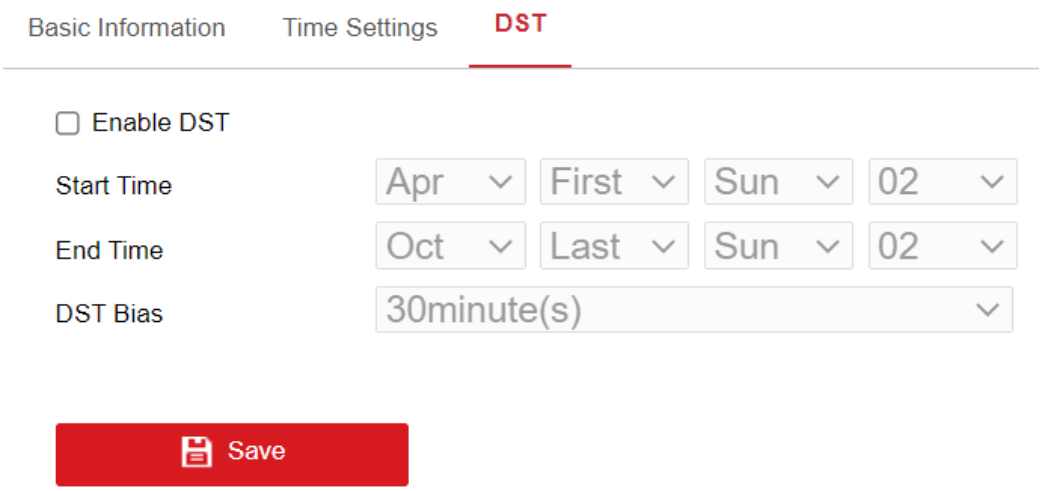


Figure 4-4 DST Settings

Step 2 Check Enable DST.

Step 3 Select the start time and the end time.

Step 4 Select the DST Bias.

Step 5 Click Save to activate the settings.

4.2 Maintenance

4.2.1 Upgrade & Maintenance

Purpose:

The upgrade & maintenance interface allows you to process the operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

Step 1 Go to **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.

- Reboot: Restart the device.
- Restore: Reset all the parameters, except the IP parameters and user information, to the default settings.
- Default: Restore all the parameters to the factory default.

Note

- After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.
- For camera that supports Wi-Fi, wireless dial, or wlan function, Restore action does not restore the related settings of mentioned functions to default.

- Information Export

Device Parameters: click to export the current configuration file of the camera.

This operation requires admin password to proceed.

For the exported file, you also have to create an encryption password. The encryption password is required when you import the file to other cameras.

Diagnose Information: click to download log and system information.

- Import Config. File

Configuration file is used for the batch configuration of the cameras.

Step 2 Click Browse to select the saved configuration file.

Step 3 Click Import and input the encryption password that you set during exporting.

Note

The camera needs rebooting after importing configuration file.

Upgrade: Upgrade the device to a certain version.

Step 4 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.

Step 5 Click Browse to select the local upgrade file and then click Upgrade to start remote upgrade.

Note

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

4.2.2 Log

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.

Step 1 Go to **Configuration** > **System** > **Maintenance** > **Log**.

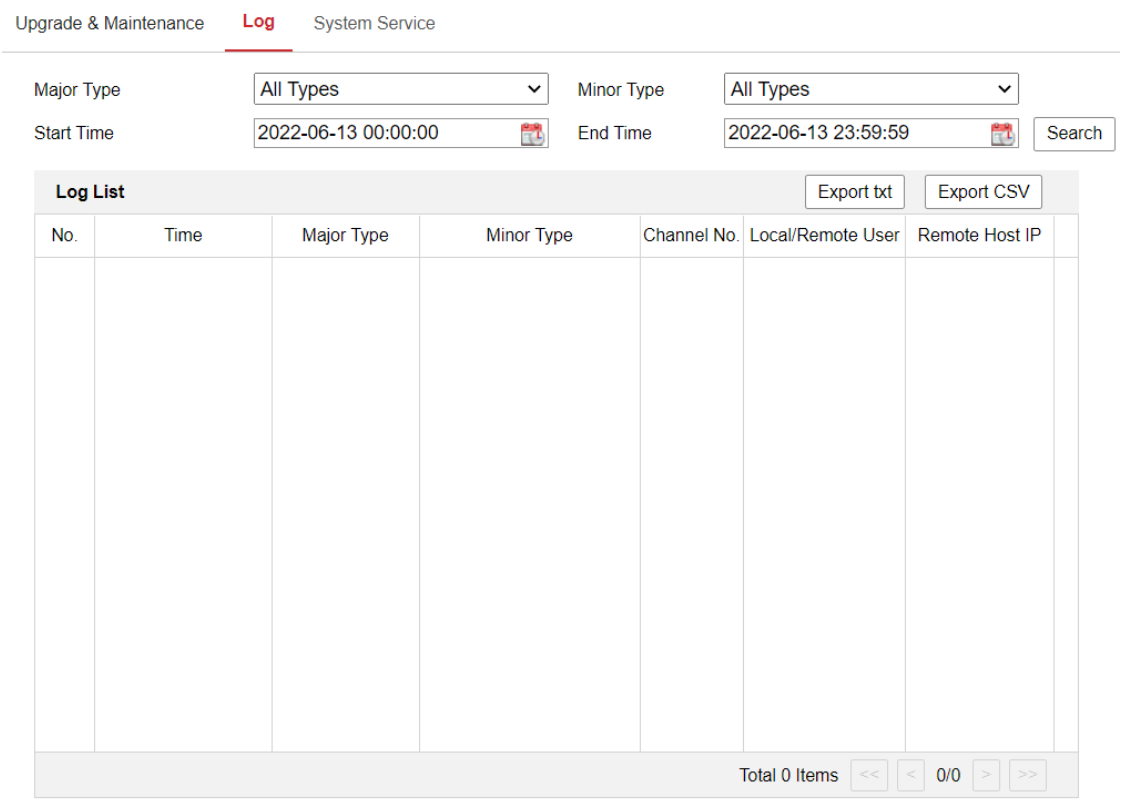


Figure 4-5 Log Searching Interface

Step 2 Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.

Step 3 Click **Search** to search log files. The matched log files will be displayed on the log list interface.

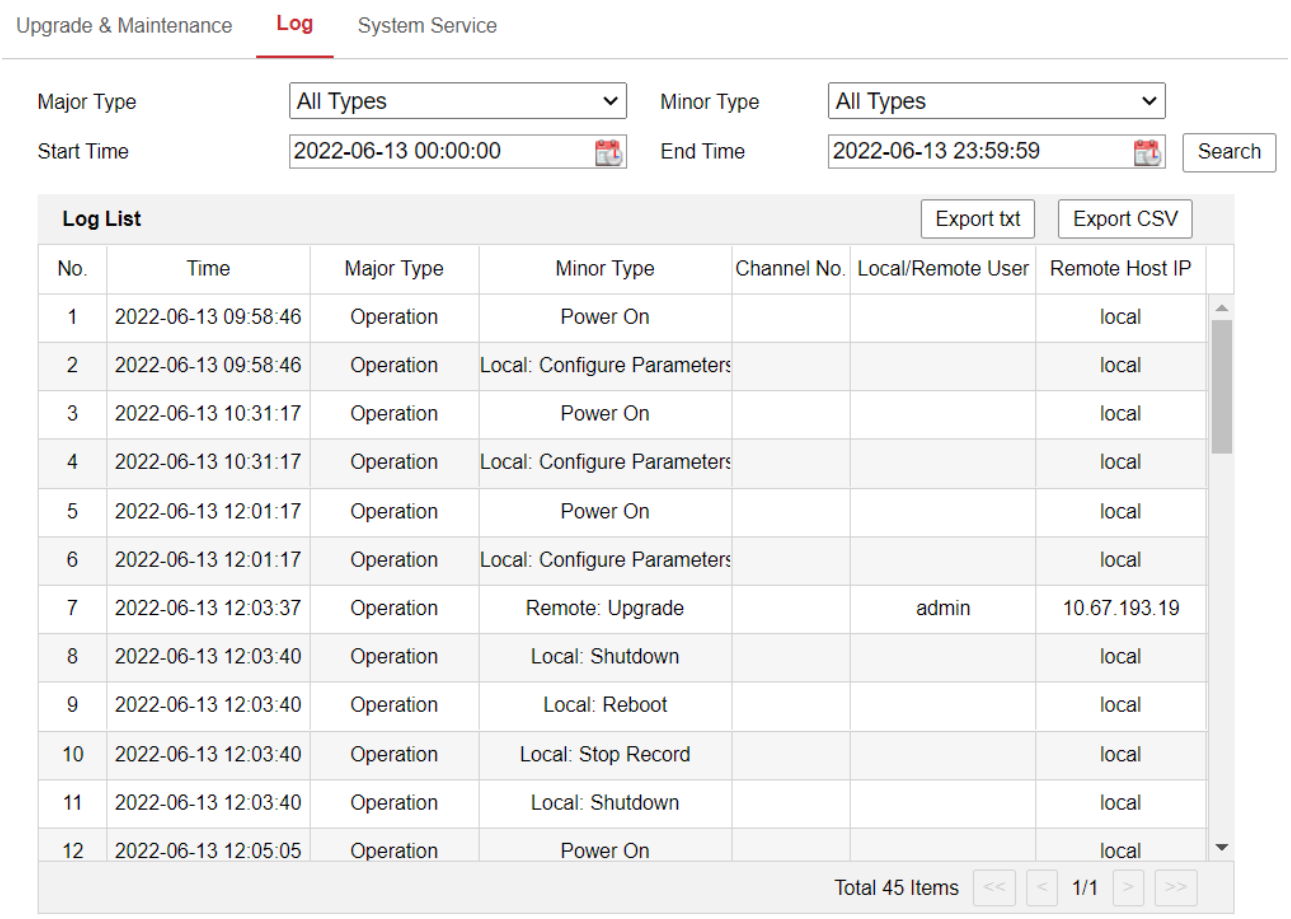


Figure 4-6 Log Searching

Step 4 To export the log files, click **Export** to save the log files.

4.3 Security

Configure the parameters, including Authentication, IP Address Filter, and Security Service from security interface.

4.3.1 Authentication

Purpose:

You can specifically secure the stream data of live view. Digest and digest/basic are selection.

Step 1 Go to **Configuration** > **System** > **Security** > **Authentication**.

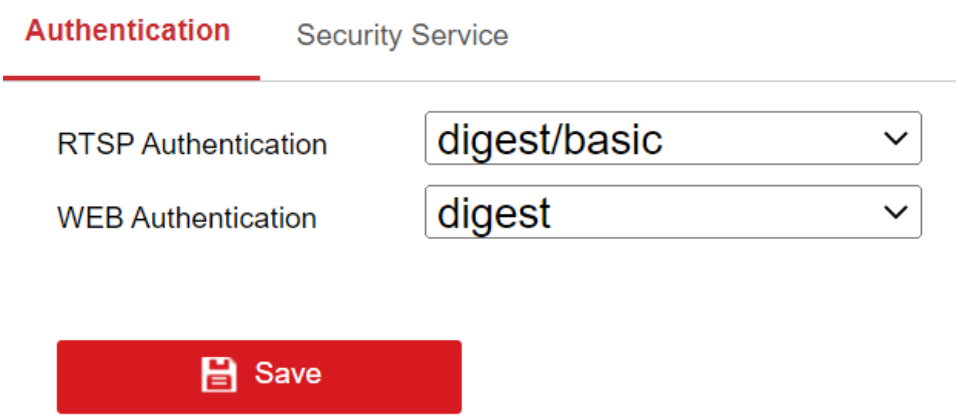


Figure 4-7 Authentication

Step 2 Set up authentication method for RTSP authentication and WEB authentication.

Caution

Digest is the recommended authentication method for better data security. You must be aware of the risk if you adopt basic as the authentication method. If you are uncertain what to choose, choose “digest/basic” to auto-adapt to your security condition.

Step 3 Click **Save**.

4.3.2 Security Service

To enable the remote login, and improve the data communication security, the camera provides the security service for better user experience.

Step 1 Go to Configuration > System > Security > Security Service.

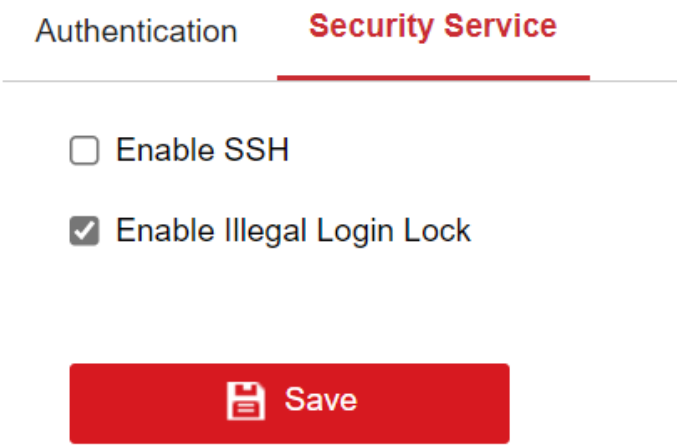


Figure 4-8 Security Service

Step 2 Check the checkbox of Enable Illegal Login Lock.

Step 3 Illegal Login Lock: it is used to limit the user login attempts. Login attempt from the IP address is rejected if admin user performs 7 failed user name/password attempts (5 times for the operator/user).

Note

If the IP address is rejected, you can try to login the device after 30 minutes.

4.4 User Management

4.4.1 User Management

Administrator

The admin user can add, delete or modify user accounts, and grant them different permissions. We highly recommend you manage the user accounts and permissions properly.

Step 1 Go to **Configuration** > **System** > **User Management**.

Note

Admin password if required for adding and modifying a user account.

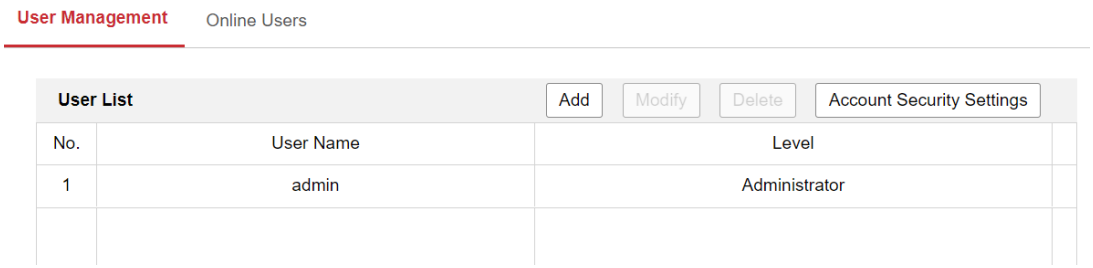


Figure 4-9 User Management Interface

Adding a User

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.

Step 2 Click **Add** to add a user.

Step 3 Input the Admin Password, User Name, select Level and input Password.

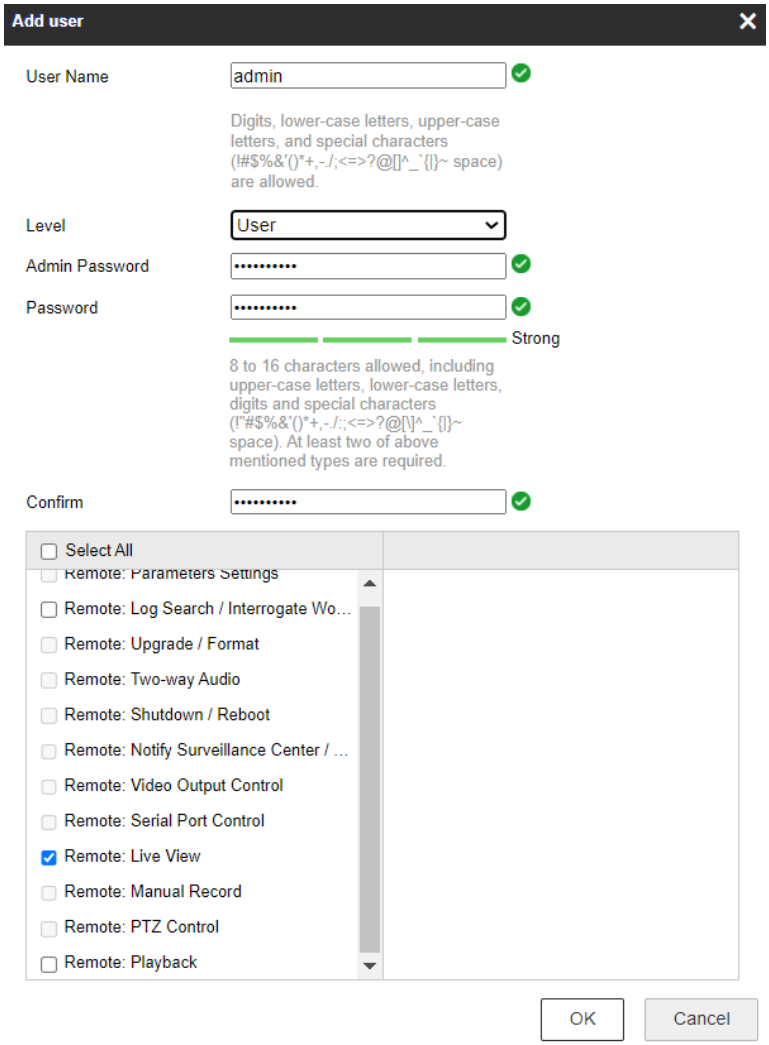


Figure 4-10 Add a User

Note

Up to 16 user accounts can be created.

Users of different levels own different default permissions. Operator and user are selectable.

Caution

Strong Password recommended

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 You can check or uncheck the permissions for the new user.

Step 5 Click **OK** to finish the user addition.

Modify a User

Step 6 Left-click to select the user from the list and click **Modify**.

Step 7 Modify the User Name, Level and Password.

Caution

Strong Password recommended

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 8 You can check or uncheck the permissions.

Step 9 Click **OK** to finish the user modification.

Step 10 Deleting a User

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

Operator/User

Operator or user can modify password. Old password is required for this action.

4.4.2 Security Question

Purpose:

Security question is used to reset the admin password when admin user forgets the password.

Set Security Questions

You can set the security questions during camera activation. Or you can set the function at user management interface.

Security question setting is not cleared when you restore the camera (not to default).

Steps:

Step 1 Go to **Configuration** > **System** > **User Management**.

Step 2 Click Account Security Question.

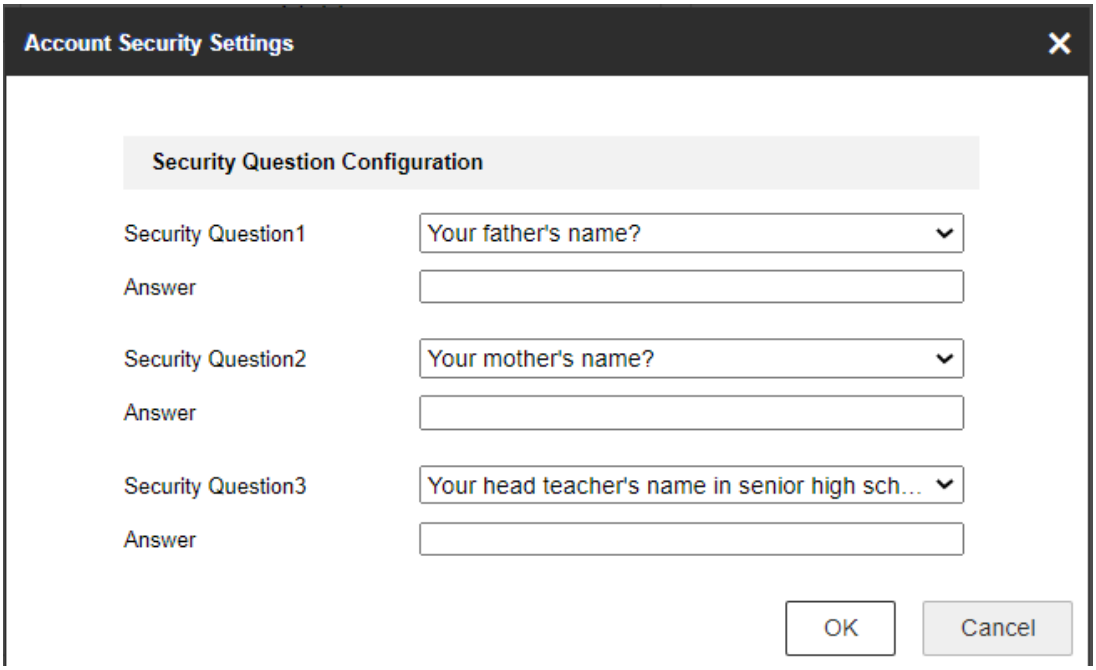


Figure 4-11 Account Security Question

Step 3 Select questions and input answers.

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

Reset Admin Password:

Note

The PC used to reset password and the camera should belong to the same IP address segment of the same LAN.

4.4.3 Online Users

Purpose:

You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address, and operation time, is displayed in the User List.

Click **Refresh** to refresh the list.

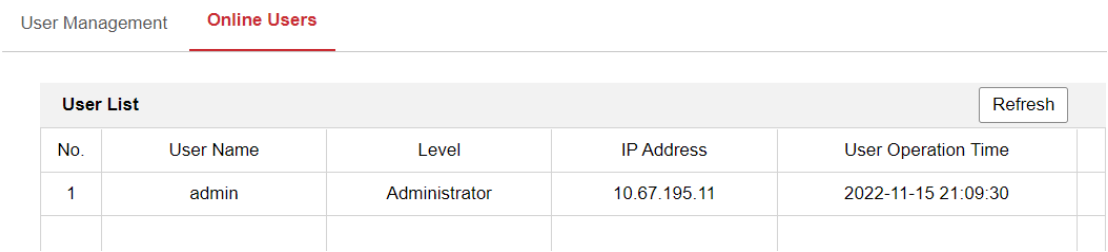


Figure 4-12 View the Online Users

Chapter 5 Network Settings

Purpose:

Follow the instructions in this chapter to configure the basic settings and advanced settings.

5.1 Basic Settings

Purpose:

You can configure the parameters, including TCP/IP, DDNS, Port, and , etc., by following the instructions in this section.

5.1.1 TCP/IP

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network.

Step 1 Go to **Configuration > Network > Basic Settings > TCP/IP**.

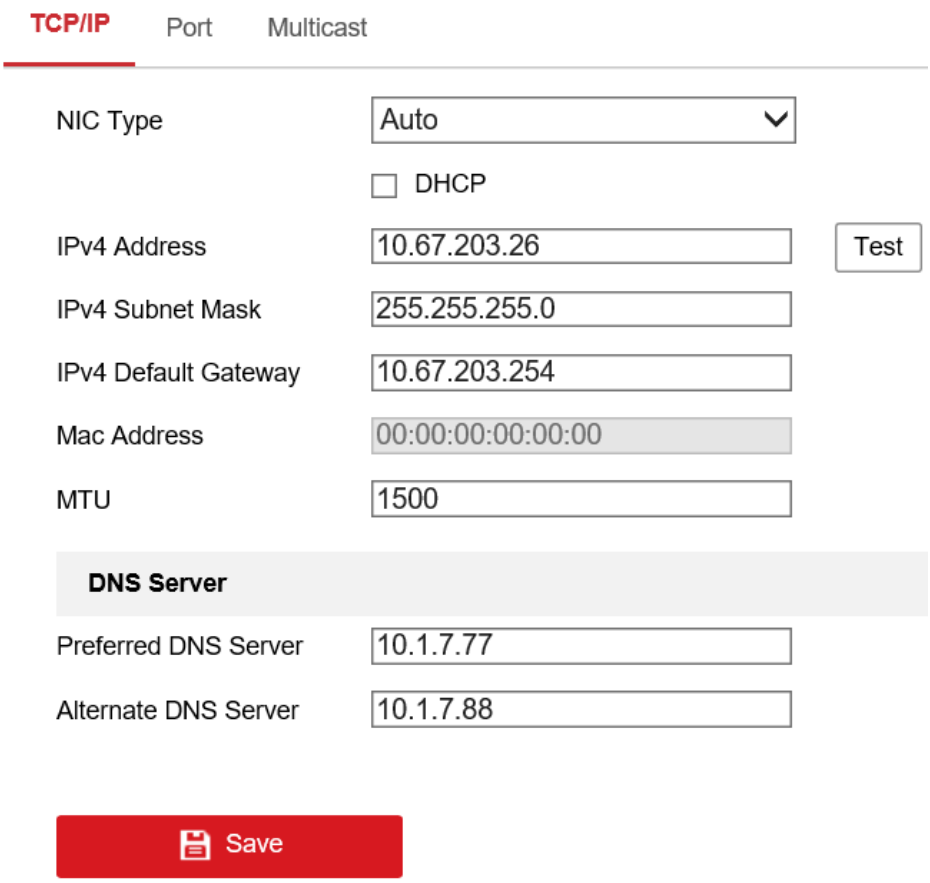


Figure 5-1 TCP/IP Settings

Step 2 Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, and MTU settings.

Step 3 Configure the DNS server. Input the preferred DNS server, and alternate DNS server.

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

Note

- The valid value range of MTU is 1280 to 1500.
- A reboot is required for the settings to take effect.

5.1.2 Port

Step 1 Go to **Configuration > Network > Basic Settings > Port**.

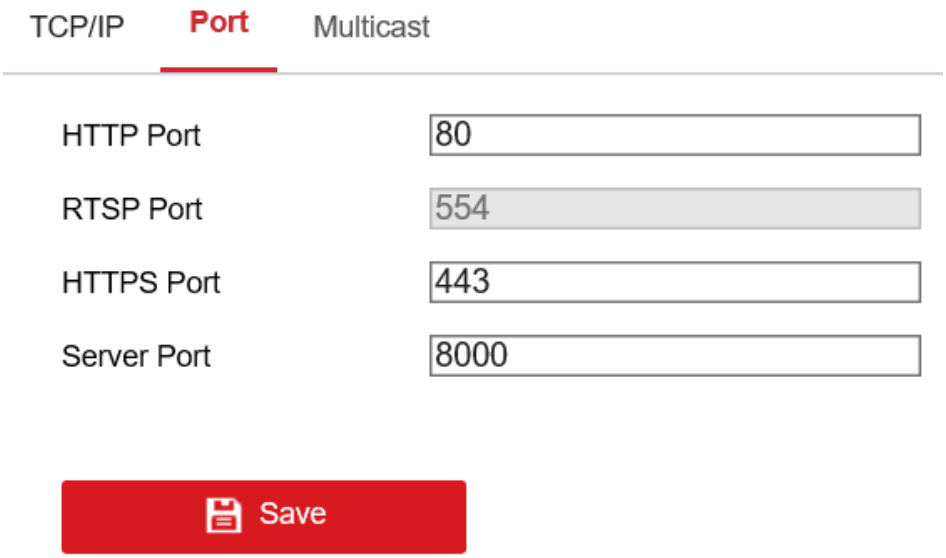


Figure 5-2 Port Settings

Step 2 Set the ports of the camera.

HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied. For instance, if you changed the port number to 81, you need to login in with the URL http://192.168.1.64:81.

RTSP Port: The default port number is 554 and it can be changed to any port No. ranges from 1 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. If you changed the Server Port, you need to add its value to the login page.

Note

The WebSocket protocol is used for plug-in free live view. For detailed information, see *5.2.4* .

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

Note

A reboot is required for the settings to take effect.

5.1.3 Multicast

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.

Step 1 Go to **Configuration > Network > Basic Settings > Multicast**.

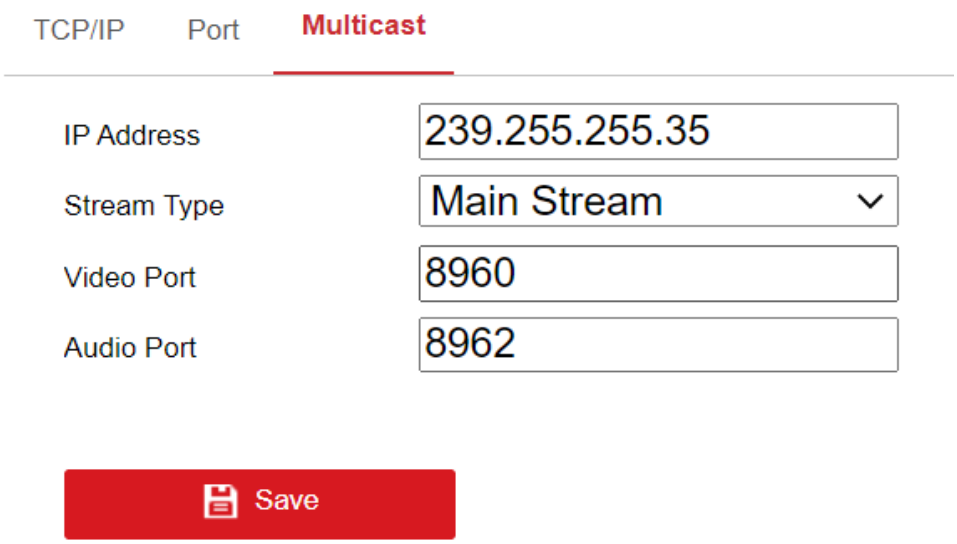


Figure 5-3 Multicast

Step 2 Configure the parameters for Multicast.

- IP Address: The IP address of the multicast host.

Note

The range for multicast IP address is 224.0.0.19~239.255.255.255

- Stream Type
  Choose the type of stream according to your needs.

Note

- For some models, the **Third Stream** is not enabled by default. Go to **System** > **Maintenance** > **System Service**> **Software** to enable the function is required.
- The main stream is usually for recording and live view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is limited.
- You can customize the following parameters for the selected stream type.

- Video Port and Audio Port: Port for Video and Audio.

Step 3 Click **Save**.

5.2 Advanced Settings

Purpose:

You can configure the parameters, including SNMP, FTP, Email, HTTPS, QoS, 802.1x, etc., by following the instructions in this section.

5.2.1 HTTPS

Purpose:

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

Note

- If HTTPS is enabled by default, the camera creates an unsigned certificate automatically. When you visit the camera via HTTPS, the web browser will send a notification about the certificate issue. Install a signed-certificate to the camera to cancel the notification.

Step 1 G to **Configuration > Network > Advanced Settings > HTTPS**.

Step 2 Check Enable to access the camera via HTTP or HTTPS protocol.

Step 3 Check Enable HTTPS Browsing to access the camera only via HTTPS protocol.

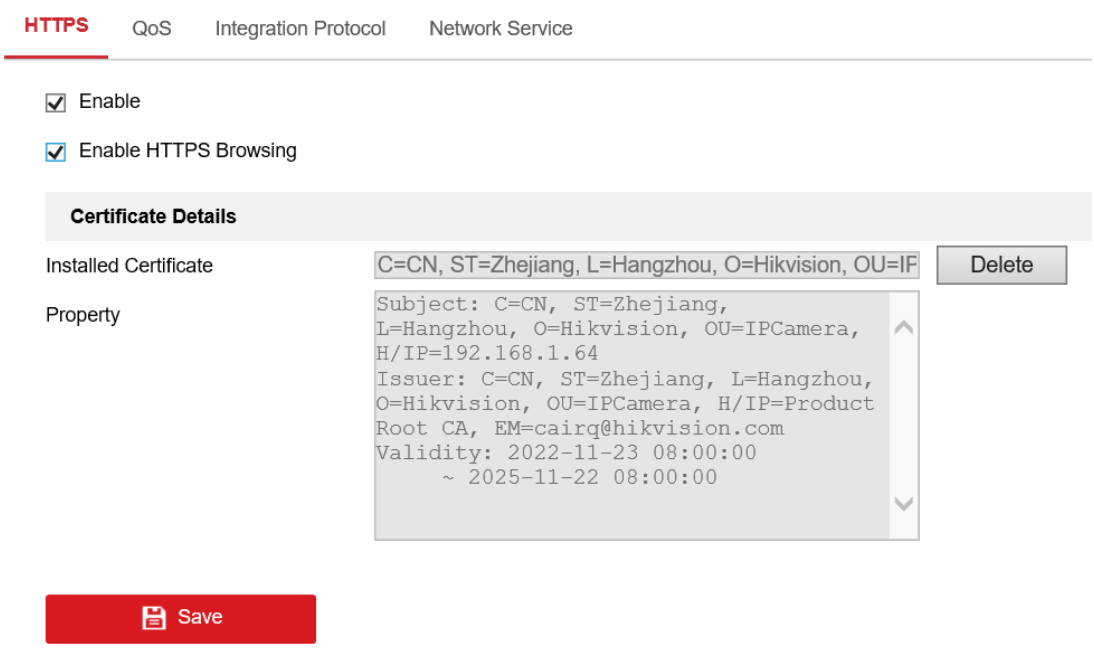


Figure 5-4 HTTPS Configuration Interface

Note

If you already had a certificate installed, the Create Self-signed Certificate is grayed out. (Optional) Click **Delete** to delete the certificate.

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

5.2.2 QoS

Purpose:

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

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. The higher the DSCP value, the higher the priority of transmission.

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

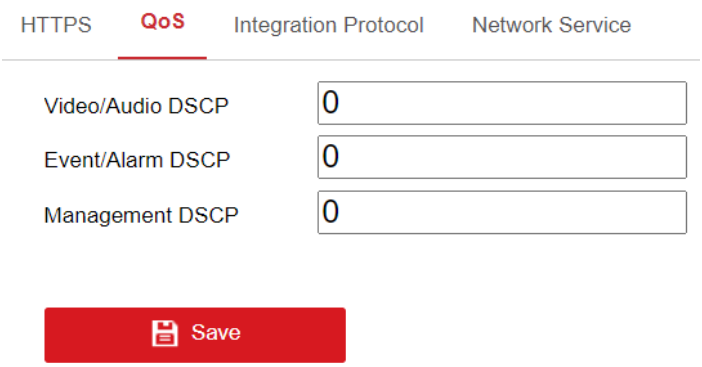


Figure 5-5 QoS Settings

Step 2 Configure the QoS settings, including Video/Audio DSCP, Event/Alarm DSCP and Management DSCP.

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

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

Note

A reboot is required for the settings to take effect.

5.2.3 Integration Protocol

Purpose:

If you need to access to the camera through the third party platform, you can enable CGI function. And if you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

ONVIF

Step 1 Check the Enable ONVIF checkbox to enable the function.

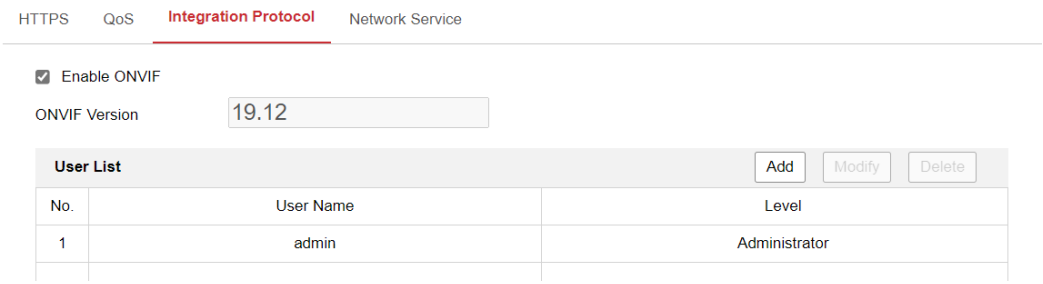


Figure 5-6 Integration Protocol

Step 2 Add ONVIF users. Up to 32 users are allowed.

Step 3 Set the user name and password, and confirm the password. You can set the user as media user, operator, and administrator.

Note

ONVIF user account is different from the camera user account. You have set ONVIF user account independently.

Step 4 Save the settings.

Note

User settings of ONVIF are cleared when you restore the camera.

5.2.4 Network Service

You can control the ON/OFF status of certain protocol that the camera supports.

Note

- Keep unused function OFF for security concern.
- Supported functions vary according to camera models.

- SDK Service and Enhanced SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

  - **SDK Service:** SDK protocol is used.
  - **Enhanced SDK Service:** SDK over TLS protocol is used. Communication between the device and the client software is secured by using TLS (Transport Layer Security) protocol.

- TLS (Transport Layer Security)

The device offers TLS 1.1 and TLS 1.2. Enable one or more protocol versions according to your need.

Chapter 6 Video/Audio Settings

Purpose:

Follow the instructions below to configure the video setting, audio settings, ROI, Display info. on Stream, etc.

6.1 Video

For certain camera models, you can configure parameters for available video streams, for example, the main stream, the sub-stream, etc. And you can also customize additional video streams for further needs.

Step 1 Go to **Configuration** > **Video/Audio** > **Video**

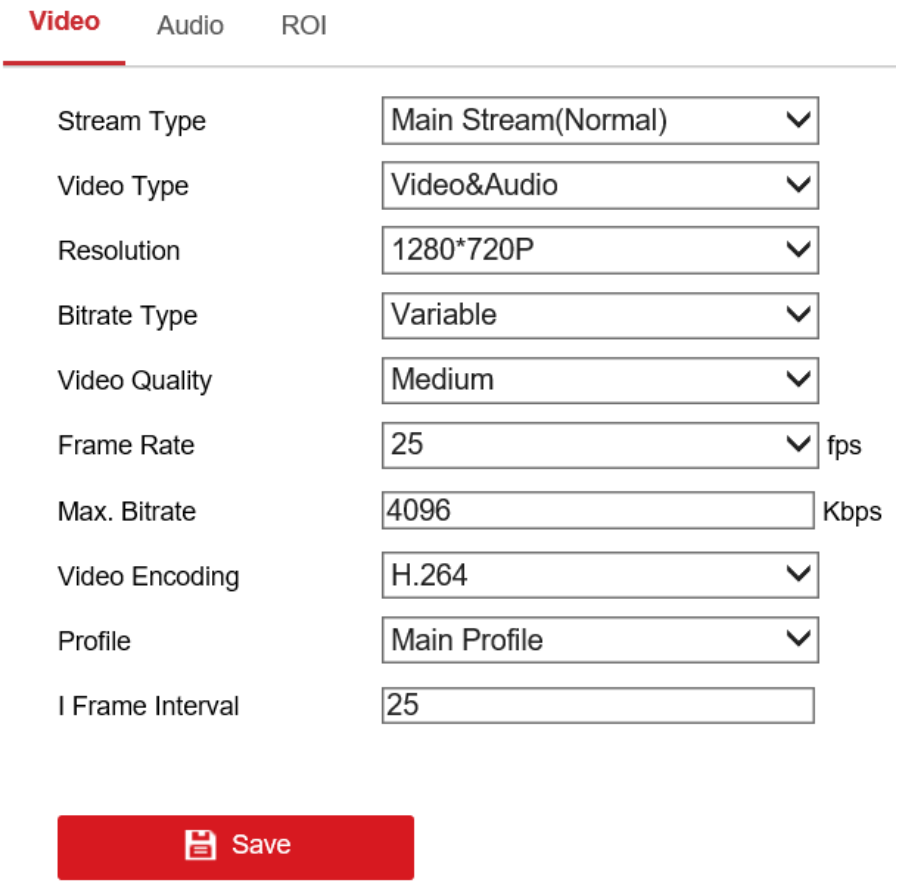


Figure 6-1 Video Settings

Step 2 Select the Stream Type.

Supported stream types are listed in the drop-down list.

Note

- The main stream is usually for recording and live view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is limited.
- You can customize the following parameters for the selected stream type.

- Video Type:

Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

- 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.

When bitrate type is selected as constant, the video quality is default to Medium.

- Frame Rate:

Set the frame rate. 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 from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Note

The maximum limit of the max. bitrate value varies according to different camera platforms. For certain cameras, the maximum limit is 8192 Kbps or 12288 Kbps.

- Video Encoding:

The camera supports multiple video encodings types, such as H.264, H.265, and MJPEG. Supported encoding type for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate and image quality.

Note

Selectable video encoding types may vary according to different camera modes.

- Max. Average Bitrate:

When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.

- Profile:

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to camera models.

- I Frame Interval:

Set I Frame Interval from 1 to 400.

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

Note

The video parameters vary according to different camera models. Refer to the actual display page for camera functions.

6.2 Audio

Step 1 Go to **Configuration** > **Video/Audio** > **Audio**.

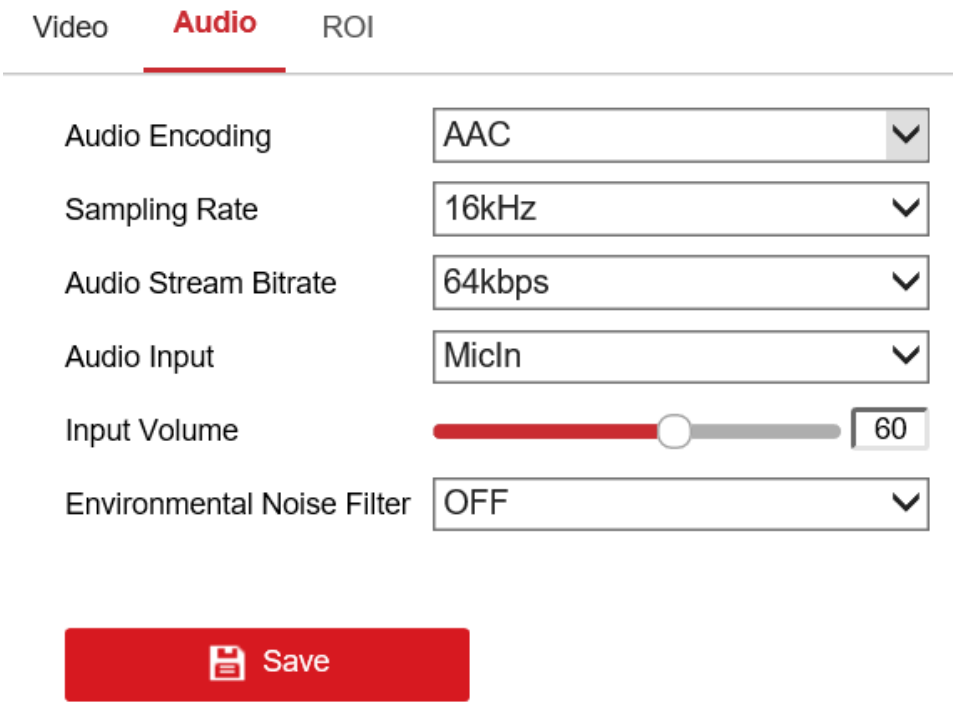


Figure 6-2 Audio Settings

Step 2 Configure the following settings.

Note

Audio settings vary according to different camera models.

Audio Encoding: G.722.1, G.711 ulaw, G.711alaw, G.726 and PCM are selectable. For PCM, the Sampling Rate can be set.

Audio Input: MicIn are selectable for the connected microphone.

Input Volume: 0-100 adjustable.

Environmental Noise Filter: Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

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

6.3 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.

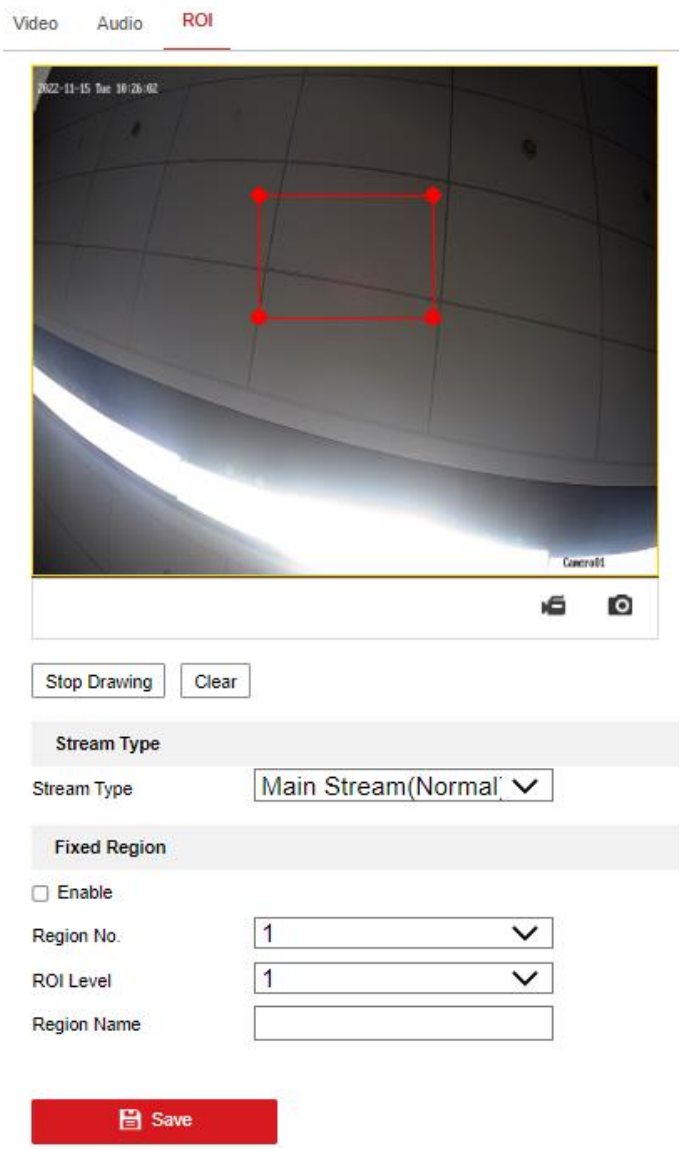


Figure 6-3 Region of Interest Settings

Step 2 Go to **Configuration** > **Video/Audio** > **ROI**.

Step 3 Select the Stream Type for ROI encoding.

Step 4 Check the checkbox of Enable under Fixed Region item.

Step 5 Set Fixed Region for ROI.

1) Select the Region No. from the drop-down list.
2) Check the **Enable** checkbox to enable ROI function for the chosen region.
3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.
4) Select the ROI level from 1 to 6.
5) Enter a region name for the chosen region.
6) Click **Save** the save the settings of ROI settings for chosen fixed region.
7) Repeat steps (1) to (6) to setup other fixed regions if available.

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

Note

ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

Chapter 7 Image Settings

Purpose:

Follow the instructions in this chapter to configure the image parameters, including display settings, OSD settings, privacy mask, and picture overlay.

7.1 Settings Parameters

Purpose:

Configure the image adjustment, exposure settings, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.

Note

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

Step 1 Go to **Configuration > Image > Display Settings**.

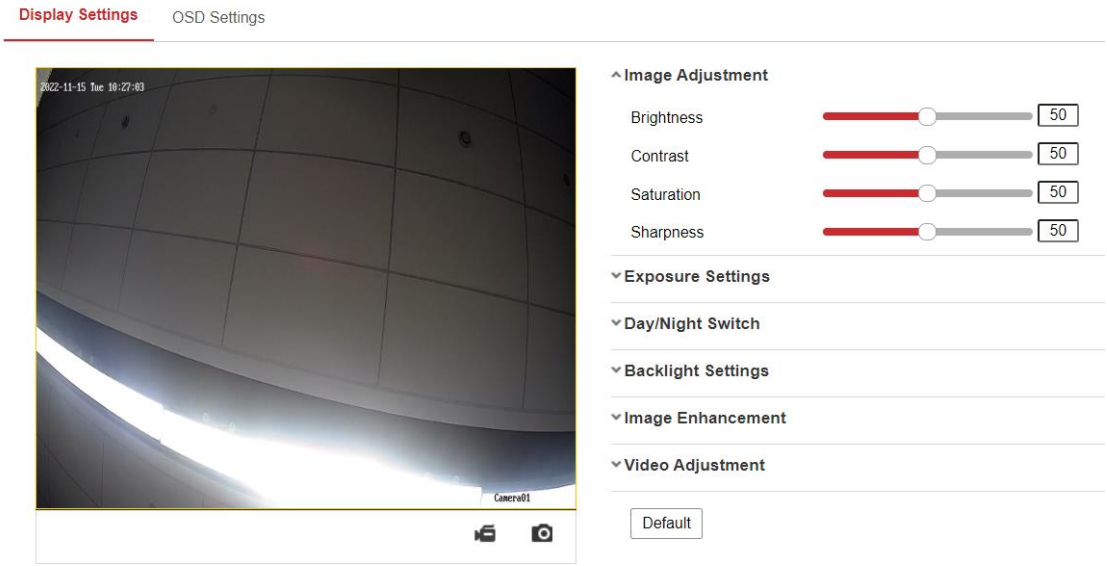


Figure 7-1 Display Settings of Day/Night Auto-Switch

Step 2 Set the image parameters of the camera.

Note

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

- Image Adjustment
  - **Brightness** describes how bright the image is, which ranges from 1 to 100.
  - **Contrast** describes the contrast of the image, which ranges from 1 to 100.
  - **Saturation** describes how colorful of the image is, which ranges from 1 to 100.
  - **Sharpness** describes the edge contrast of the image, which ranges from 1 to 100.
- Exposure Settings
  - If the camera is equipped with the fixed lens, only **Manual** is selectable, and the iris mode is not configurable.
  - If **Auto** is selected, you can set the auto iris level from 0 to 100.
  - The **Exposure Time** refers to the electronic shutter time, which ranges from 1 to 1/100, 000 s. Adjust it according to the actual luminance condition.
  - **Gain** of image can also be manually configured from 0 to 100. The bigger the value is, the brighter would the image be, and the noise would also be amplified to a larger extent.

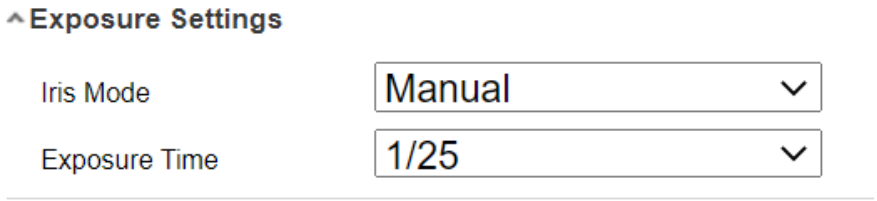


Figure 7-2 Exposure Settings

- Backlight Settings
  - **BLC Area:** Choose an area from up, down, left, right and center to avoid the overly bright or dark. Choose Custom to draw an area. Turn off BLC to configure WDR.
  - **WDR**: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene. Turn off WDR to configure BLC.

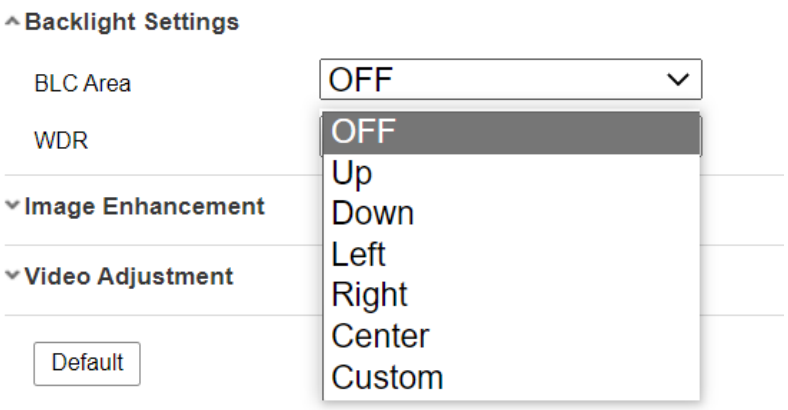


Figure 7-3 BLC Settings

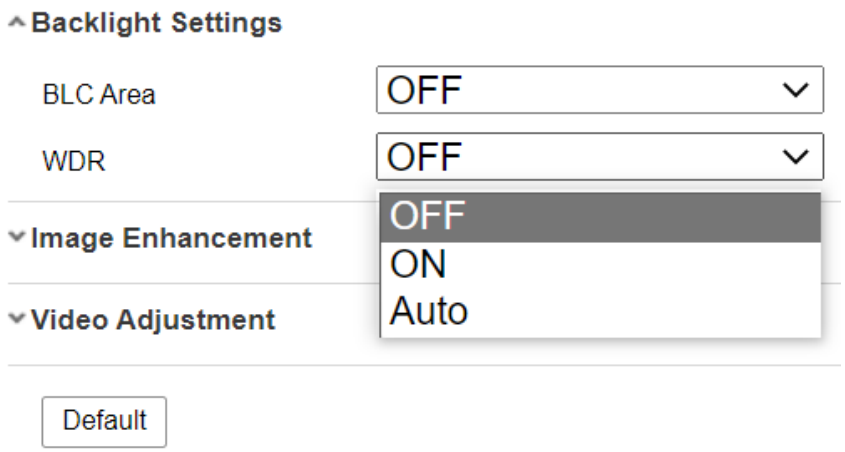


Figure 7-4 WDR Setting

- Image Enhancement
  - **Digital Noise Reduction**: DNR reduces the noise in the video stream. OFF, Normal and Expert are selectable. Set the DNR level from 0 to 100 in Normal Mode. Set the DNR level from both space DNR level [0-100] and time DNR level [0-100] in Expert Mode.
  - **Defog Mode**: You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.
  - **EIS (Electrical Image Stabilizer)**: EIS reduces the effects of vibration in a video.
  - **Grey Scale**: You can choose the range of the grey scale as [0-255] or [16-235].
- Video Adjustment
  - **Mirror**: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.
  - **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.

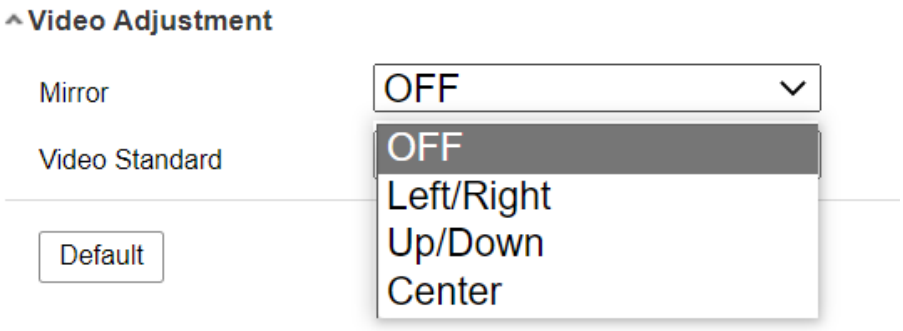


Figure 7-5 Mirror

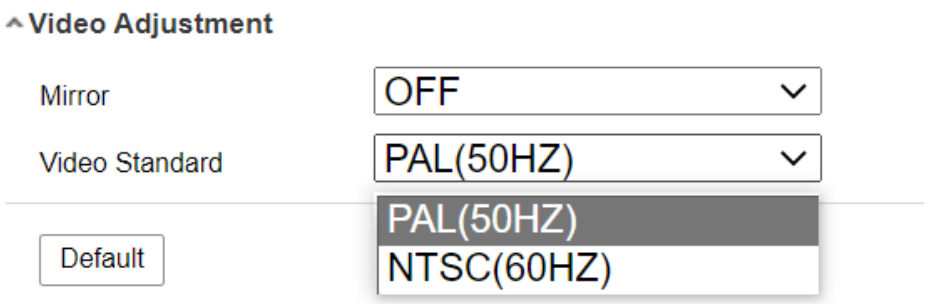


Figure 7-6 Video Standard

7.2 Day/Night Switch

7.2.1 Day/Night Auto-Switch

Select the Day/Night Switch mode according to different monitoring demand.

Day, Night, Auto, Scheduled-Switch, and Triggered by alarm input are selectable for day/night switch.

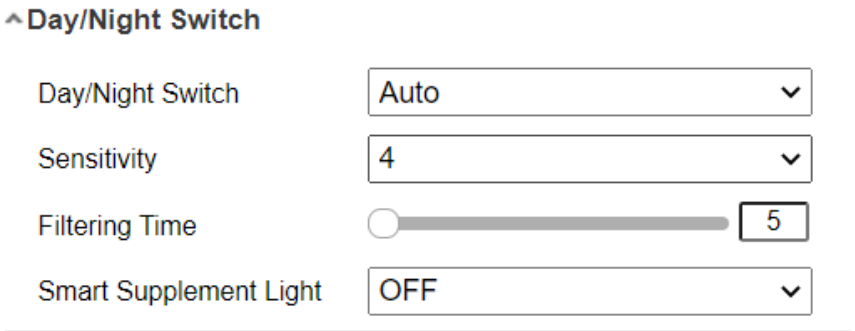


Figure 7-7 Day/Night Switch

- **Day:** the camera stays at day mode where the image is in color.
- **Night:** the camera stays at night mode where the image is black and white.
- **Auto:** the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0 to 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 5 s to 120 s.
- **Scheduled-Switch:** Set the start time and the end time to define the duration for day/night mode.
- **Triggered by alarm input:** The switch is triggered by alarm input. You can set the triggered mode to day or night.
- **Smart Supplement Light:** ON and OFF are selectable for light mode.

7.2.2 Day/Night Scheduled-Switch

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

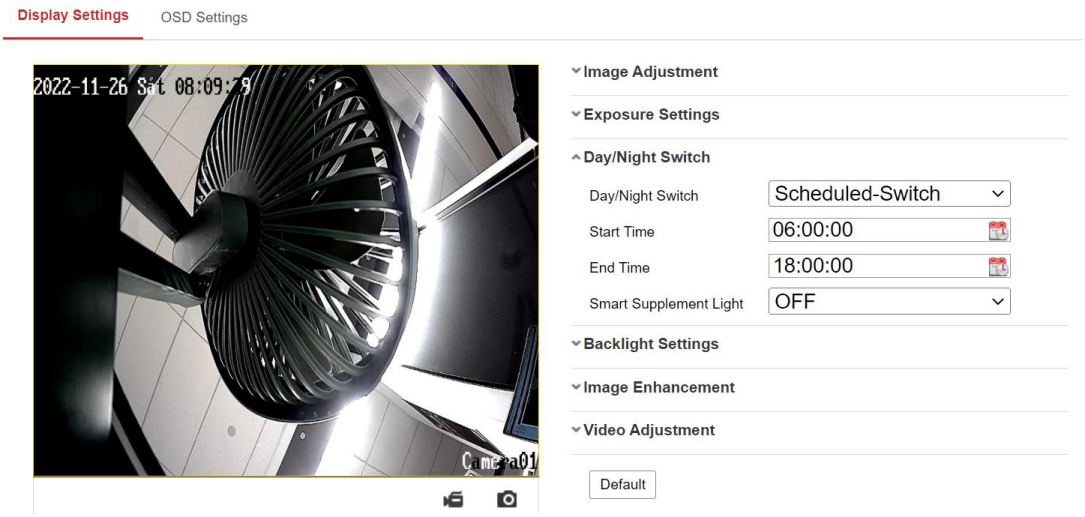


Figure 7-8 Day/Night Scheduled-Switch Configuration Interface

Step 1 Click the calendar icon to select the start time and the end time of the switch.

Note

- The start time and end time refer to the valid time for day mode.
- The time period can start and end on two days in a row. For example, if you set start time as 10:00 and end time as 1:00, the day mode will be activated at 10 o'clock in the morning and stopped at 1 o'clock early in the next morning.

Step 2 Click Common tab to configure the common parameters applicable to the day mode and night mode.

Step 3 Click Day tab to configure the parameters applicable for day mode.

Step 4 Click Night tab to configure the parameters applicable for night mode.

Note

The settings saved automatically if any parameter is changed.

7.3 OSD Settings

Purpose:

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

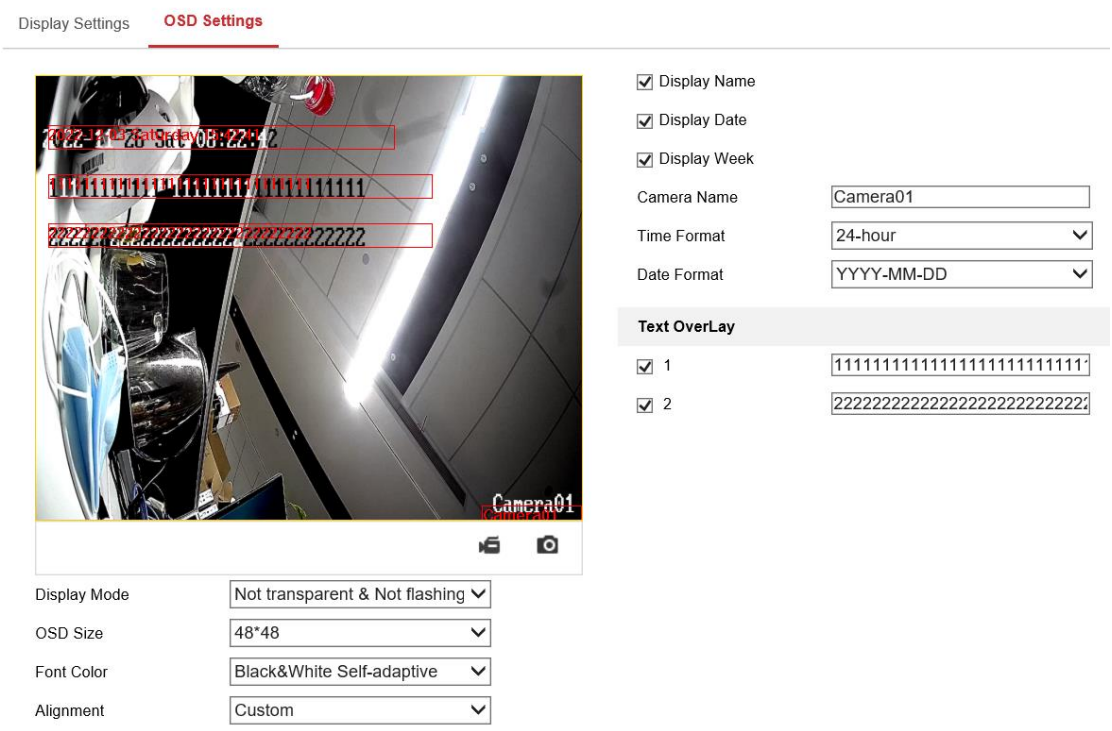


Figure 7-9 OSD Settings

Step 2 Go to **Configuration** > **Image** > **OSD Settings**.

Step 3 Check the corresponding checkbox to select the display of camera name, date or week if required.

Step 4 Edit the camera name in the text field of Camera Name.

Step 5 Select from the drop-down list to set the time format and date format.

Step 6 Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.

Step 7 Configure the text overlay settings.

1) Check the checkbox in front of the textbox to enable the on-screen display.
2) Input the characters in the textbox.

Note

Up to 2 text overlays (up to 31 digits) are configurable.

Step 8 Adjust the position and alignment of text frames.

Left align, right align and custom are selectable. If you select custom, you can use the mouse to click and drag text frames in the live view window to adjust their positions.

Note

The alignment adjustment is only applicable to Text Overlay items.

Step 9 Click **Save** to save the settings.

Chapter 8 Storage Settings

Before you start:

To configure record settings, make sure that you have the local storage media installed, without which the recording will not be possible

8.1 Storage Management

Steps:

Step 1 Go to **Configuration** > **Storage** > **Storage Management** > **HDD Management**, in which you can view the capacity, free space, status, type and property of the storage media.

Step 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.

Step 3 When the initialization completed, the status of disk will become **Normal**.

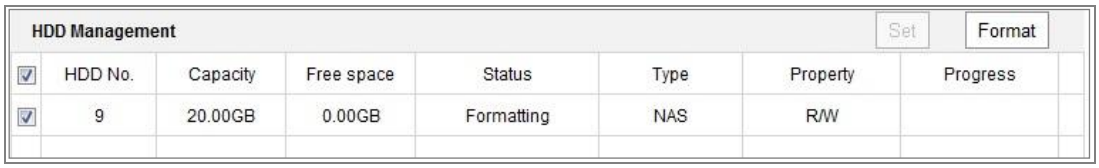


Figure 8-1 View Disk Status

8.2 Record Schedule

Purpose:

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 local storage media (for instance, a SD card).

Step 1 Go to **Configuration** > **Storage** > **Schedule Settings** > **Record Schedule**.

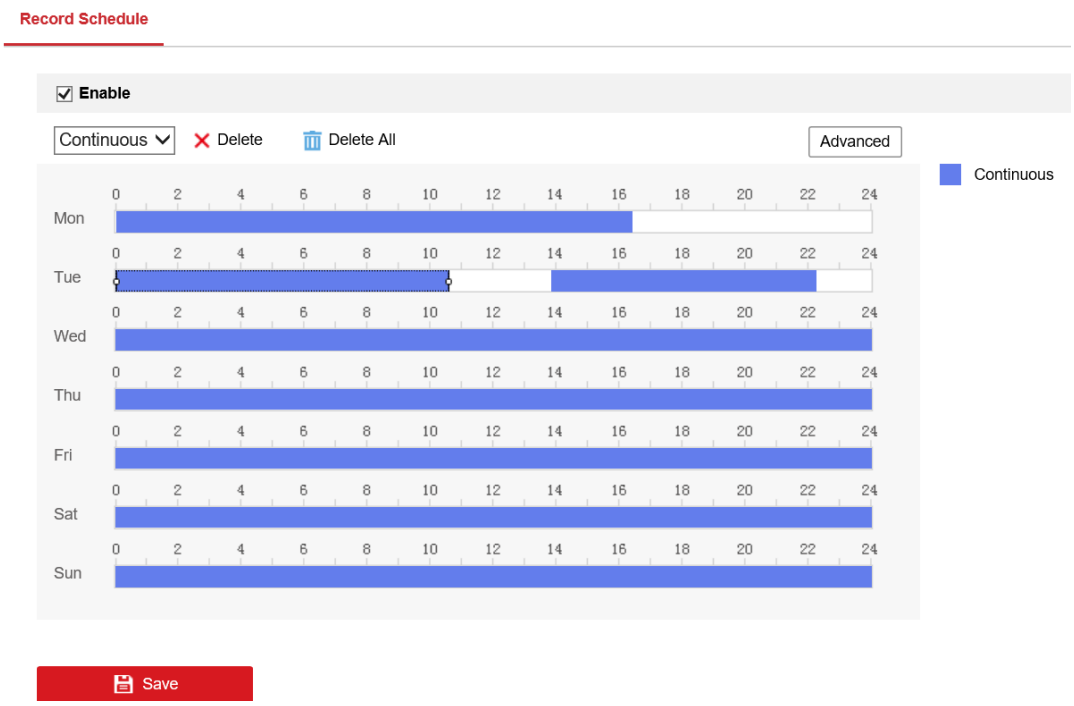


Figure 8-2 Recording Schedule Interface

Step 2 Check the checkbox of **Enable** to enable scheduled recording.

Note

The record parameter configurations vary depending on the camera model.

Step 3 Select a **Record Type**. The record type is default to Continuous.

If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.

Step 4 Click-and-drag the mouse on the time bar to set the record schedule.

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

Chapter 9 Access to the Network Camera

Purpose:

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

9.1.1 Via 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 network camera via a router or connect it to the WAN directly.

Connecting the network camera via a router

Step 1 Connect the network camera to the router.

Step 2 Assign a LAN IP address, the subnet mask and the gateway. Refer to Section 5.1.1 TCP/IP for detailed IP address configuration of the network camera.

Step 3 Save the static IP in the router.

Step 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.

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

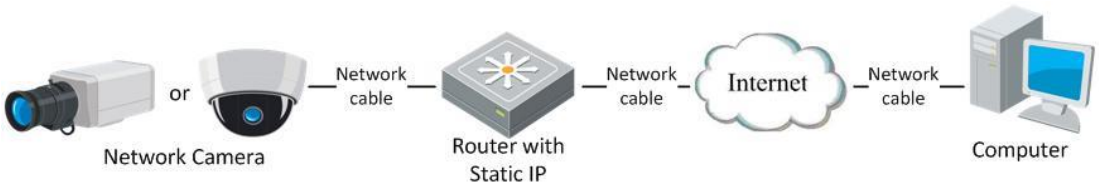


Figure 9-1 Accessing the Camera through Router with Static IP

Connecting the network 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 5.1.1 TCP/IP for detailed IP address configuration of the network camera.

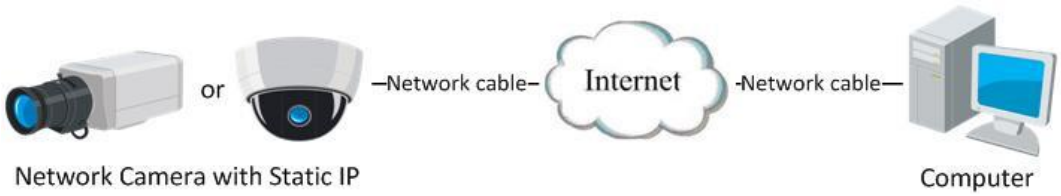


Figure 9-2 Accessing the Camera with Static IP Directly

9.1.2 Via Dynamic IP Connection

Before you start:

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

Connecting the network camera via a router

Step 1 Connect the network camera to the router.

Step 2 In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.

Step 3 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.

Step 4 Apply a domain name from a domain name provider.

Step 5 Configure the DDNS settings in the setting interface of the router.

Step 6 Visit the camera via the applied domain name.

Step 7 Connecting the network camera via a modem

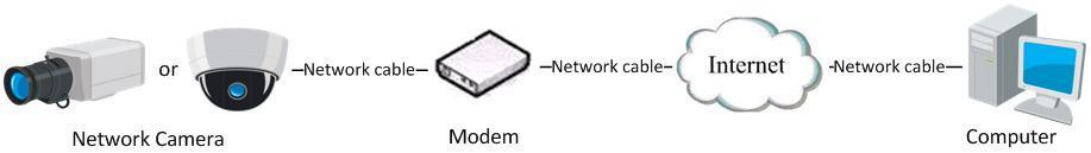


Figure 9-3 Accessing the Camera with Dynamic IP

Chapter 10 Appendix

10.1 Appendix 1 SADP Software Introduction

• Description of SADP

SADP (Search Active Devices Protocol) is a kind of 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

Step 1 Search online devices automatically

Step 2 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 and port number, etc. will be displayed.

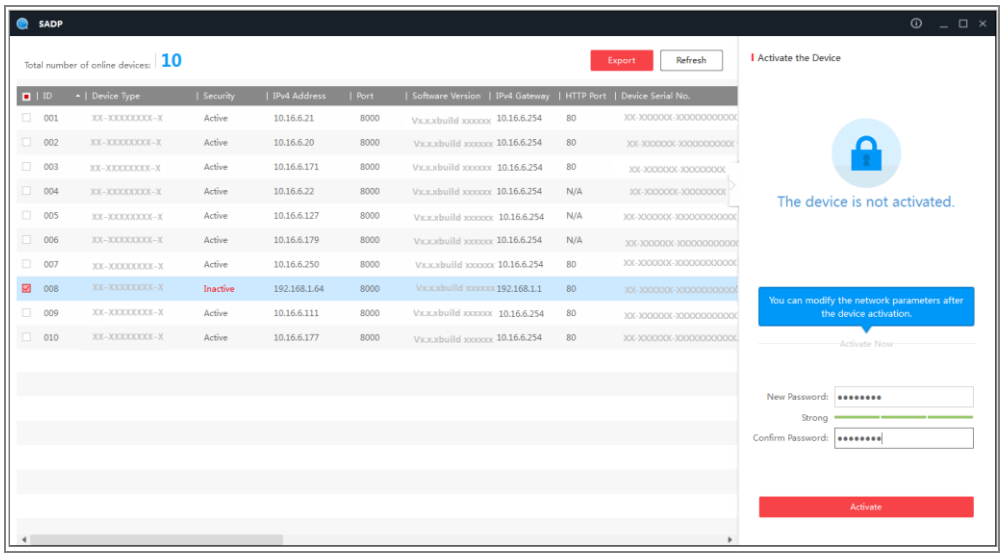


Figure A.1.1 Searching Online Devices

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.

Step 3 Search online devices manually

Step 4 You can also click Refresh to refresh the online device list manually. The newly searched devices will be added to the list.

Step 5  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**

Step 6 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.

Step 7 Edit the modifiable network parameters, e.g. IP address and port number.

Step 8 Enter the password of the admin account of the device in the **Admin Password** field and click Modify to save the changes.

Caution

STRONG PASSWORD RECOMMENDED

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

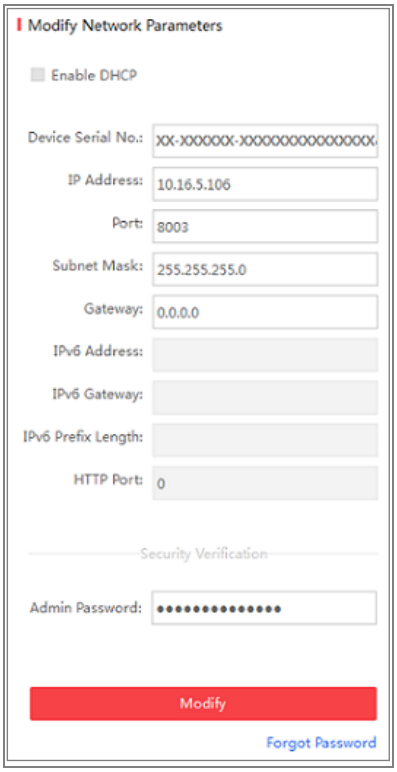


Figure A.1.2 Modify Network Parameters

10.2 Appendix 2 Device APP

Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision network cameras.

Figure 10-1 Device Communication Matrix

Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for all Hikvision network cameras.

Figure 10-2 device common serial port commands


See Far, Go Further