HIKVISION

Network Camera Security Guide

January 2018

About This Document

This Guide includes instructions for using and managing the product safely.

User Manual

About this Manual

This Manual is applicable to iVMS-4200 Client Software.

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 in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Contact Information

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China

Tel: +86-571-8807-5998

Fax: +86-571-8993-5635

Email: overseasbusiness@hikvision.com; sales@hikvision.com

Technical Support: support@hikvision.com

HSRC (Hikvision Security Response Center) Email: HSRC@hikvision.com

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. 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, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS TO

THE APPLICABLE LAWS. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

Contents

1 Abstract

Various types of security attacks on the Internet have become a severe threat for network devices and users' privacy. Hikvision network cameras have integrated a variety of reliable security features to defend against these threats without the owner even knowing their device has been compromised. Hikvision has added a number of cybersecurity protections and removed many features by default. This allows the user to open specified security functions according to their needs.

Note: This document provides a general security overview; users should choose the appropriate security settings that apply to their actual situation.

2 Security Function Configurations

2.1 Identity Authorization

Account usernames and passwords are important data, used to identify and authenticate users. Default passwords and weak passwords pose a critical threat to user accounts and should not be used.

2.1.1 Creating a strong password

How to set a strong password?

A general strong password rule for Hikvision devices:

(1) Valid character range [8-16].

(2) You can use a combination of numbers, lowercase, uppercase and special character for your password using at least two of the above. .

'Passphrases" are easy to remember but hard to crack. Here's a simple way to set a 'Passphrase'.

(1) Choose a phrase with number in it;

(2) Only use the first letter of a word;

(3) Letters should follow the case sensitivity of original phrase;

(4) Use numbers rather than letter, for example, use '2' to replace 'to', use 4 to replace 'for';

(5) Don't delete punctuation.

Let's take the phrase below as an example:

'**My flight to New York will leave at three in the afternoon!** ' .

'Phrase password' should be '**MftNYwla3ita!** '.

Some tips for a strong password：

(1) Don’t use sequential letters or numbers like ‘cdef’, ‘12345’;
(2) Don’t allow web browser to remember password on public computers;
(3) Don’t email your passwords to anyone.
(4) Consider using a password manager so you don’t have to remember the password.
(5) Does not include anything in the dictionary and is not just using dictionary words with numbers replacing letters.

2.1.2 Activating a Camera by Setting a Strong Password

Users are required to activate the camera first by setting a strong password for it before they can use the camera. 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 to protect your privacy information or data.
Activation via web browser, SADP, and client software are all supported.

Note: The rules of password levels are:
Strong password: it uses at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.
Medium password: It is a combination of the following categories: numbers and symbols, lower case letters and symbols, upper case letters and symbols, lower case letters and upper case letters.
Weak password: It is a combination of number and lower case letters or numbers and upper case letters.
Risk password:
It is no longer than 8 characters.
It includes only one category of characters.
It is the same or the reverse of user name.

To protect your privacy and to increase the security of your product, we highly recommend you to use strong password.

2.1.2.1 Activation via SADP Software

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

Run the SADP software from the disk included with product or from the official website, and install the SADP by following the prompts. Run the SADP software to search for devices on the LAN. The device status, such as device model, IP address, security status, and serial number, can be displayed in the software (Fig. 2-1).

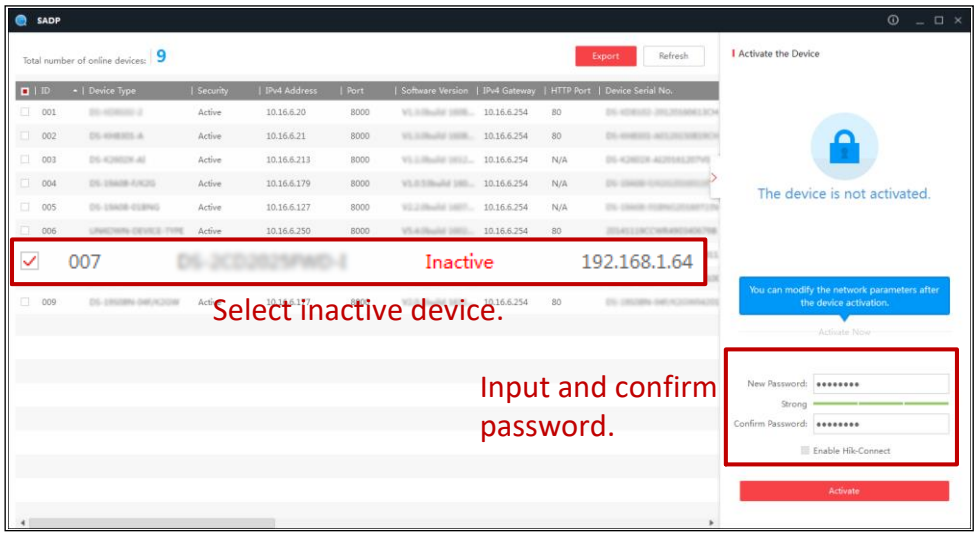

Fig. 2-1 SADP software interface

Click to select the device to be activated. The status of the device is shown on the right side of the window. Enter the password in the password field and click **Activate** to start the process.

2.1.2.2 Activation via Client Software

Run the client software from the disk included with product or from the official website, and install the software by following the prompts. Run the client software to search for devices on the LAN in the **Device Management** interface. The device status, such as device model, IP address, Security status, serial number, can be displayed in the software.

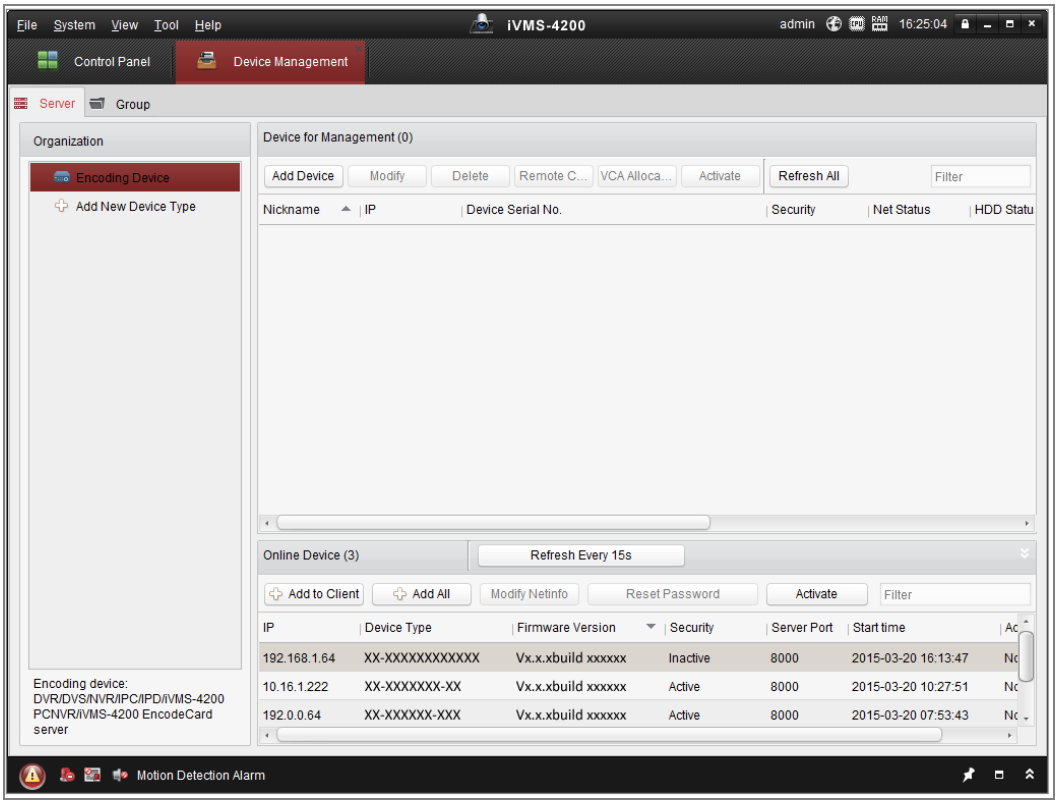

Fig. 2-2 Device Management

Select an inactive device and click the **Activate** button to pop up the Activation interface. Create a password and enter it into the password field, retype the password to confirm. Click the **OK** button to start the activation. When complete, the security status for that device will be changed to **Active**.

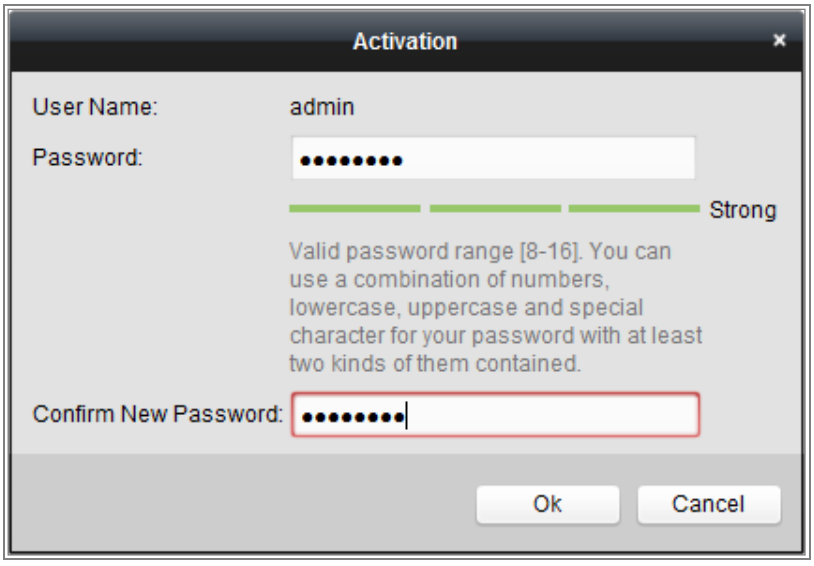

Fig. 2-3 Activation via client software

2.1.2.3 Activation via Web Browser

Set the IP address of the PC and network camera to be on the same subnet. Enter the IP address of the network camera into the address bar of the web browser, and click **Enter** to enter the activation interface (Fig. 2-6).

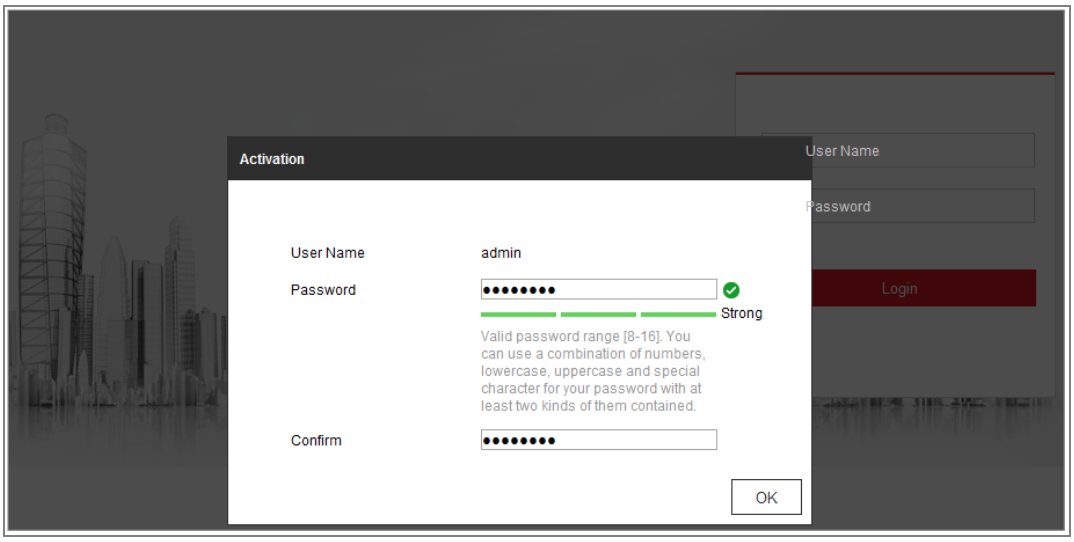

Fig. 2-4 Activation via Web Browser

If there are two or more devices on the network, the IP addresses of devices should be configured to avoid IP address confliction.

2.1.3 Illegal Login Lock

The illegal login lock is used to limit the number of user login attempts. Login attempts from the IP address are rejected for 30 mins if the admin user performs 7 failed user name/password attempts (5 times for the operator/user). Notifications are shown when the IP address is rejected by the camera. The illegal login lock defends against 'brute-force' password attacks. It's highly recommended that this feature is enabled. (Fig. 2-5).

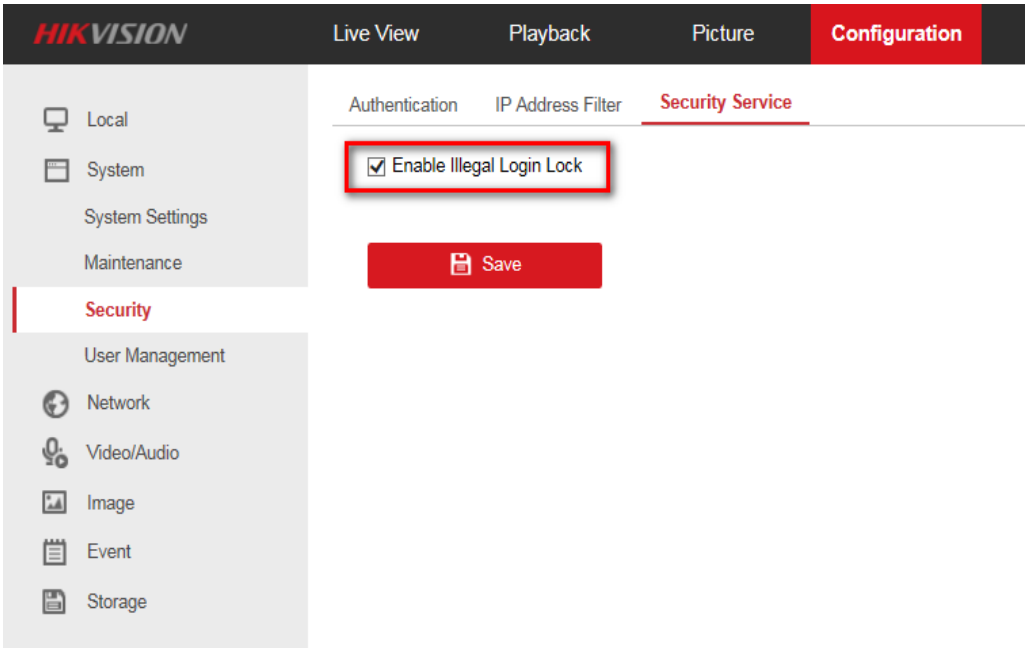

Fig. 2-5 Enable Illegal Login Lock

2.1.4 Resetting password by Security Question

The security question is used to reset the admin password via client software or a web browser.

The user can set a list of **Security Questions** in the **User Management menu**.

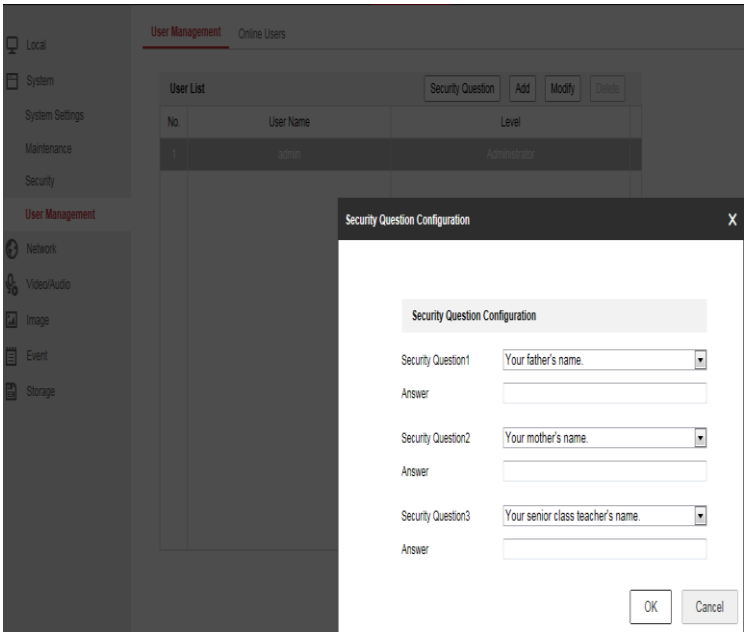

Fig. 2-6 Security Question

In the login interface, you may click **Forget Password** and answer all 3 security questions to reset the password.

Fig. 2-7 Forget Password

Note: 1. The PC used to reset the password and the camera should be on the same IP address segment of the same LAN.

2. Only the administrator is able to reset a password.

2.1.5 Authentication

RTSP Authentication and WEB Authentication support “digest” and “digest/basic” authentication modes. If there are no compatibility requirements of “basic” authentication, it’s recommended that you select “digest” mode.

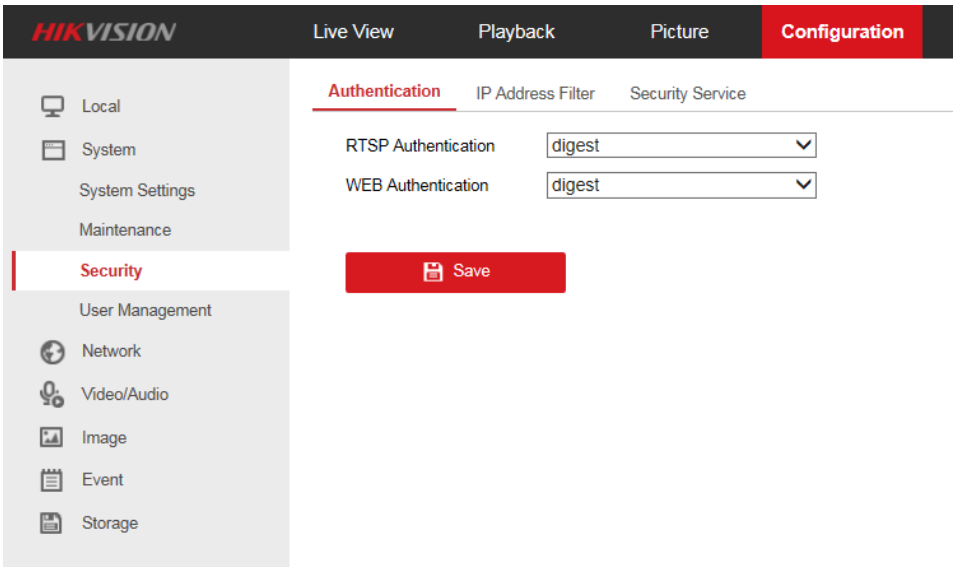

Fig. 2-8 Authentication Modes

2.2 Authorization Management

2.2.1 User Management

Three levels of users are supported: Administrator (admin), Operator, and User. The admin user can add, delete or modify user accounts, and grant them different permissions.

Enter the User Management interface: **Configuration** > **System** > **User Management**

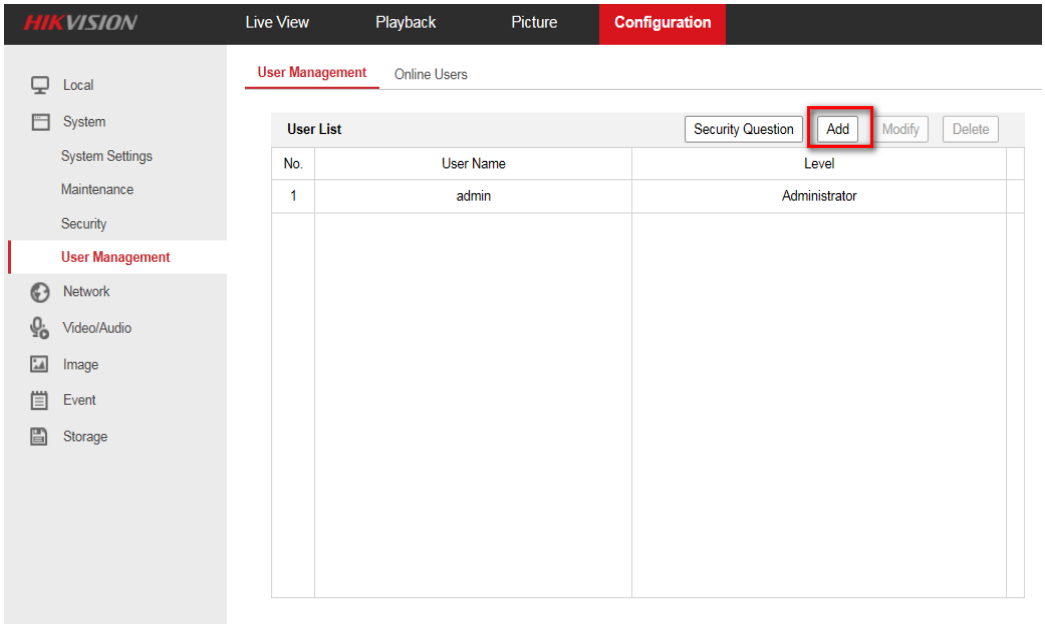

Fig. 2-9 User Management

The interface for adding a user account is shown in Fig. 2-12. The Administrator is able to check or uncheck the permissions for the new user.

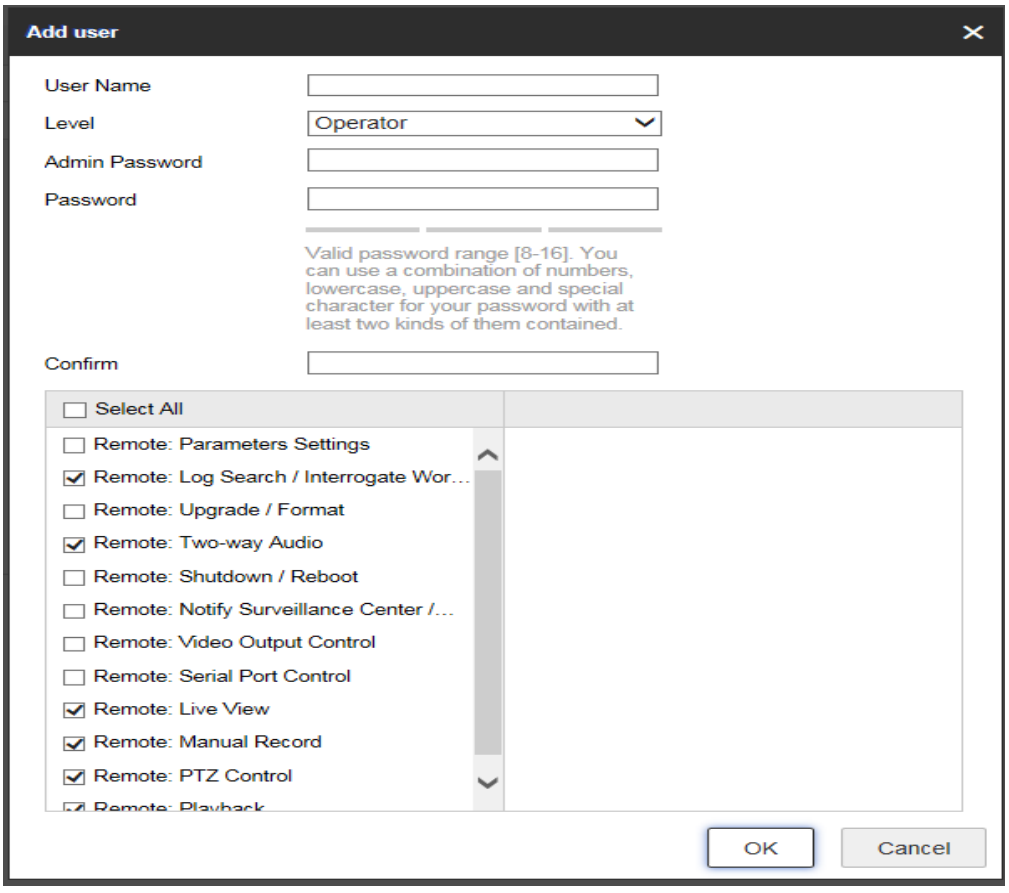

Fig. 2-10 Adding a user account

2.3 Log

The log files are stored on a SD card. Log information includes Number, Time, Major Type, Minor Type, Channel Number, Local/Remote User and Remote Host IP. Users can set query various search parameters, including the Major Type, Minor Type, Start Time and End Time. The log files can be exported in text format or Excel format. The log is saved sequentially in a binary file format. When log files are full, new logs will overwrite the oldest log. Logs cannot be modified or deleted.

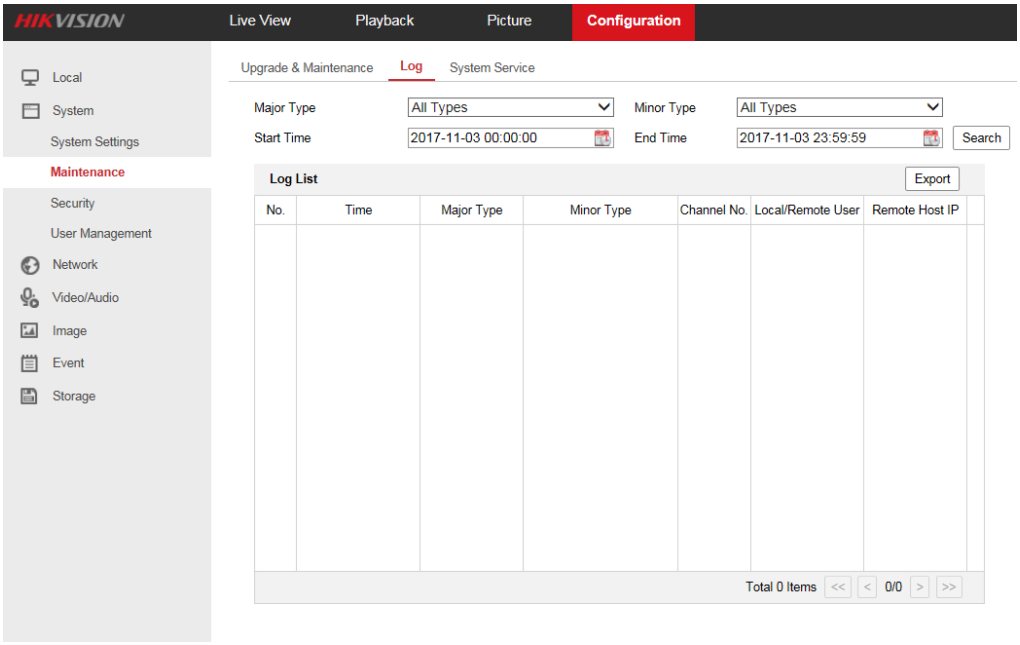

Fig. 2-11 Log

2.4 Encryption

2.4.1 HTTPS

HTTPS is a transmission encryption protocol based on SSL/TLS and HTTP. It improves the security of WEB access. If a certificate is already installed, the detailed information of the certificate will be shown. Check “Enable” to enable HTTPS (Fig. 2-14).

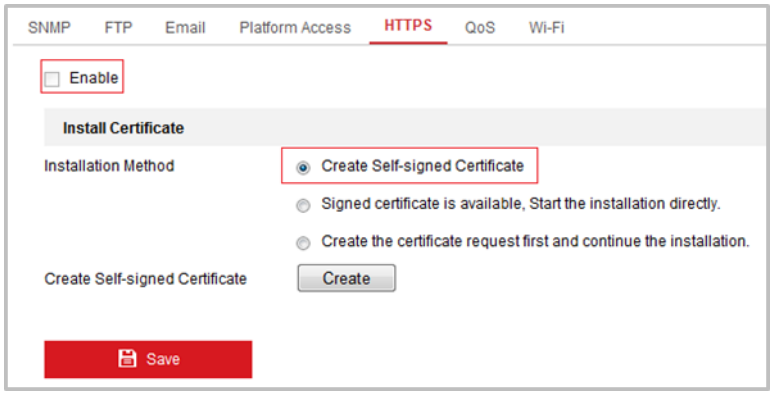

Fig. 2-12 Enable HTTPS

Three installation methods are available, “Create Self-signed Certificate”, “Signed Certificate is available, Start the installation directly” and “Create the Certificate request first and continue the installation”.

Create Self-signed Certificate: Select “Create Self-signed Certificate” as the Installation Method and click the “Create” button to enter the certificate creation interface. Enter the country, host name/IP, validity and other information. Click “OK” to save the settings.

Install a Signed Certificate: Select “Signed Certificate is available”, Start the installation directly as the Installation Method and click “Browse” to select a signed certificate. Click “Install” then click “Save”.

Create the authorized certificate: Select “Create the certificate request first and continue the installation” as the Installation Method. Click the “Create” button to create the certificate request. Fill in the required information in the popup window. Download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed valid certificate, import the certificate to the device.

Once a certificate is installed you will see the certificate information as shown in (Fig.2-15).

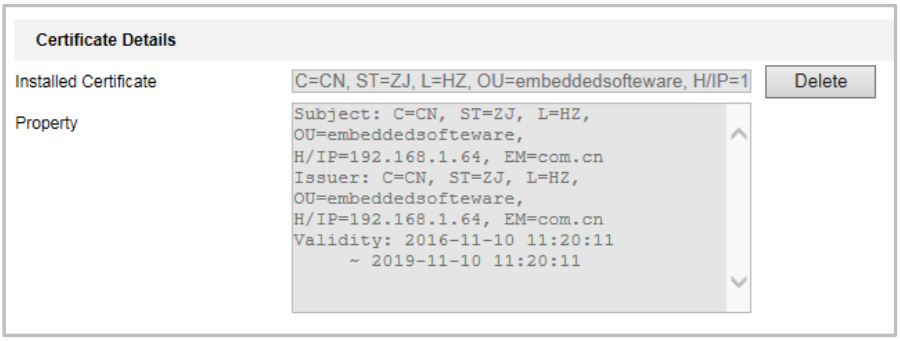

Fig. 2-13 Installed Certificate

Note:

1. The security notification (Fig. 2-16) will be shown in the browser when a user accesses the device via HTTPS with a self-signed certificate installed. This is because

the certificate is not issued by a trusted certificate authority (CA).

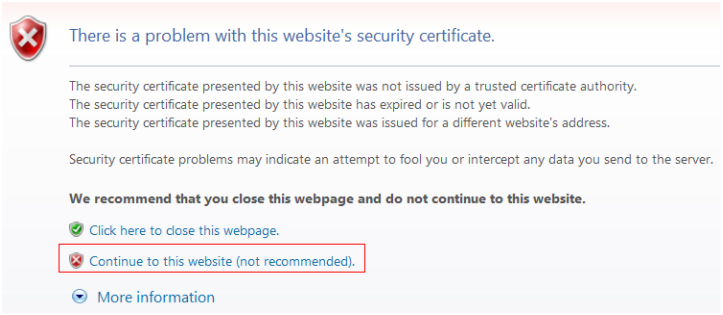

Fig. 2-14 Security Notification of Self-signed Certificate

2. It's recommended you install certificates issued by a certification authority (CA) to improve the security of web access. Generally a CA charges for issuing a digital certificate.

2.5 Port and Service Security

Only necessary services and ports are enabled by default to minimize the possibility of attacks and reduce security risks. The supported services and protocols, such as ONVIF, CGI, UPnP, QoS, Multicast, Platform Access, and SNMP are disabled by default. Users should only enable the required services and protocols that are necessary to their environment.

2.5.1 SNMP

The device supports SNMP v1, SNMP v2 and SNMP. You can set the SNMP function to retrieve the camera status, parameters and alarm related information, and manage the camera remotely when it is connected to the network. SNMP is disabled by default. If SNMP is not required, it should not be enabled. SNMP v3 is highly recommended to replace SNMP v1 or SNMP v2.

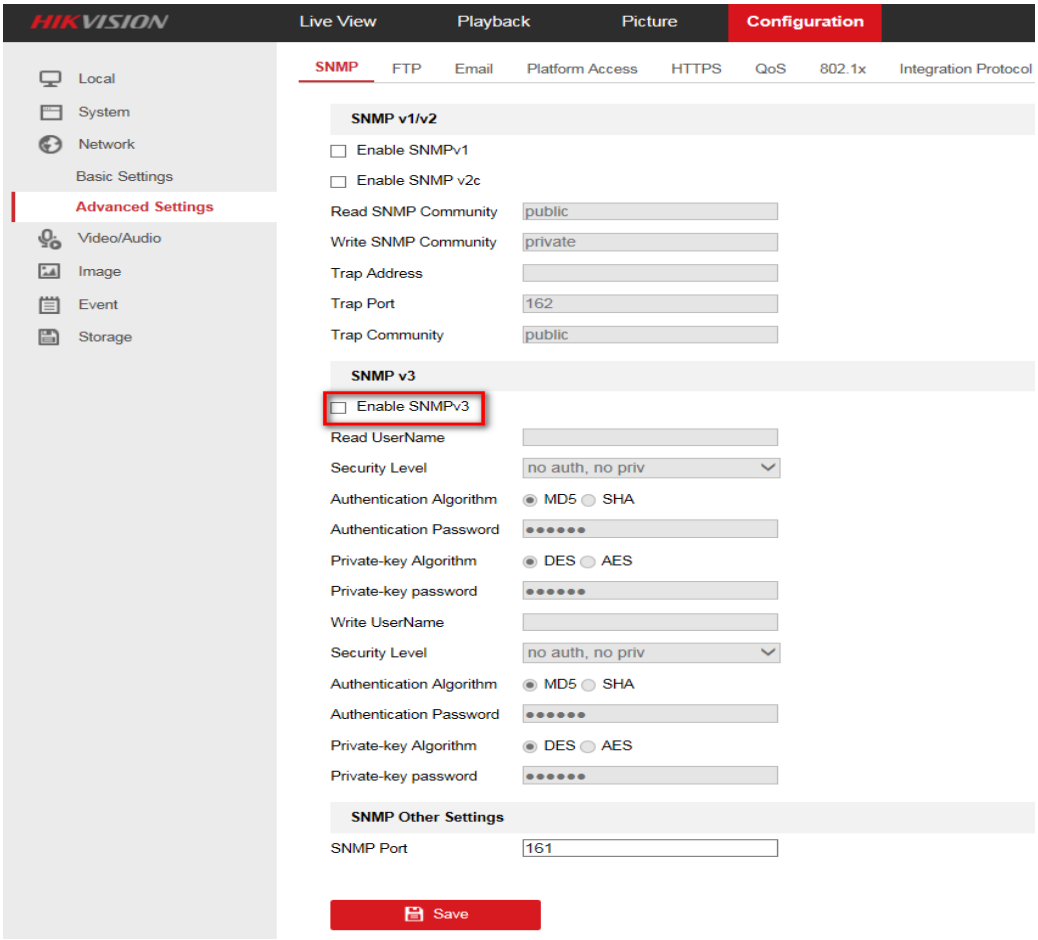

Fig. 2-15 SNMP Configuration

2.5.2 Disable UPnP™

Universal Plug and Play (UPnP™) is a networking protocol that provides compatibility between networking equipment, software and hardware devices. UPnP™ is disabled by default. If the device is not connected to hosted video services, UPnP™ should not be enabled.

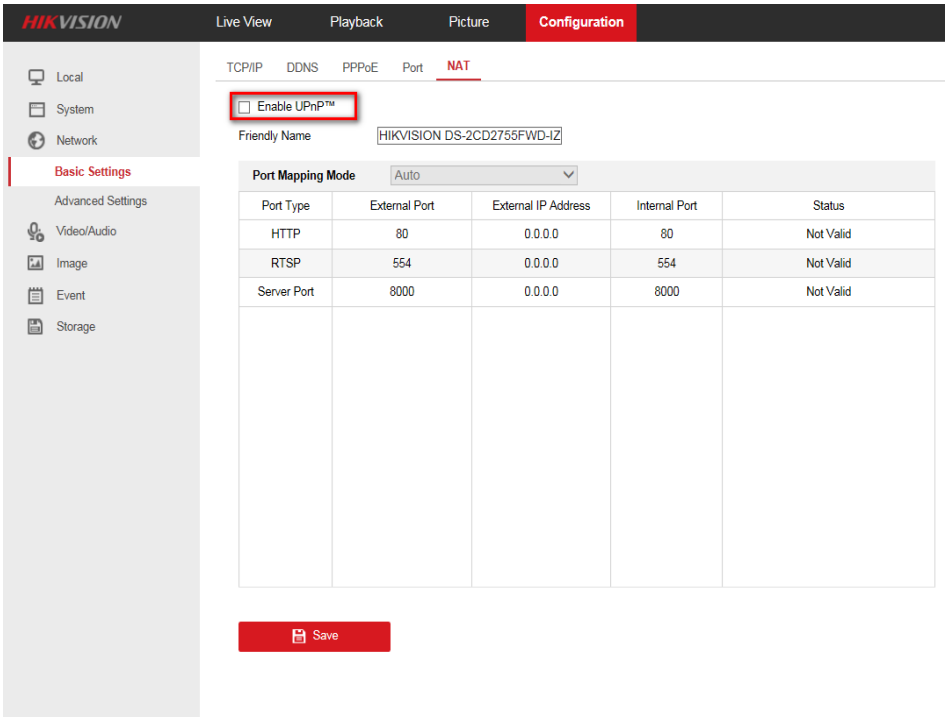

Fig. 2-16 UPnP Configuration

2.5.3 Port Forwarding

Port Forwarding can be configured when a device needs access to the Internet from behind a firewall. The following security best practices should be followed to reduce the risk of cyberattack against your Internet-facing device.

1. Minimize the number of ports that are accessible via the Internet. Configure port forwarding only when it is necessary. For example, forwarding port 443 when encrypted web services are needed.
2. Ensure that all accounts are set with very strong passwords. This is extremely important when a device is 'Internet-facing'.
3. Avoid the use of general ports but use a custom port instead. For example, port 80 is generally used in HTTP. It's recommended to use a custom port for a specific service. The custom port shall follow TCP/IP port definition (1-65535).

2.5.4 QoS

QoS (Quality of Service) is a mechanism that prioritizes network traffic for specified applications. It can help solve the network delay and network congestion by configuring the priority of data transmissions. Generally, QoS is not needed in a non-time-based application system. If QoS is not supported by the network infrastructure, set "Video/Audio DSCP", "Event/Alar DSCP" and "Management DSCP"to "0".

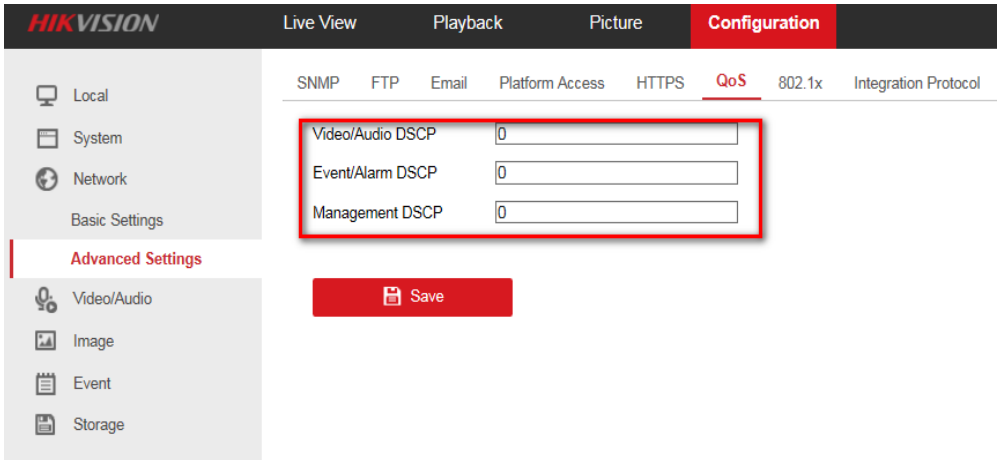

Fig. 2-17 QoS Configuration

2.5.5 Hik-Connect

Platform access provides you an option to manage devices via the Hik-Connect platform. Hik-Connect is disabled by default. If access to Hik-Connect is not needed, it should not be enabled.

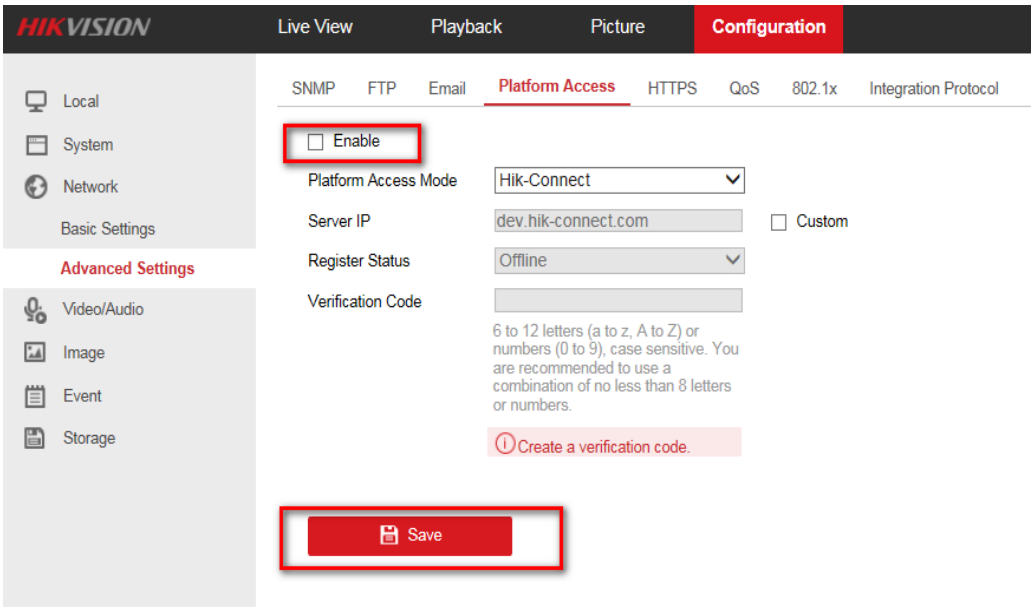

Fig. 2-18 Disable Hik-Connect

When a user enables platform access and selects Hik-Connect mode, they will create a verification code or change the verification code for the camera. The verification code should be more than 8 (preferably more than 12) characters composed of upper case letters, lower case letters numbers and special characters.

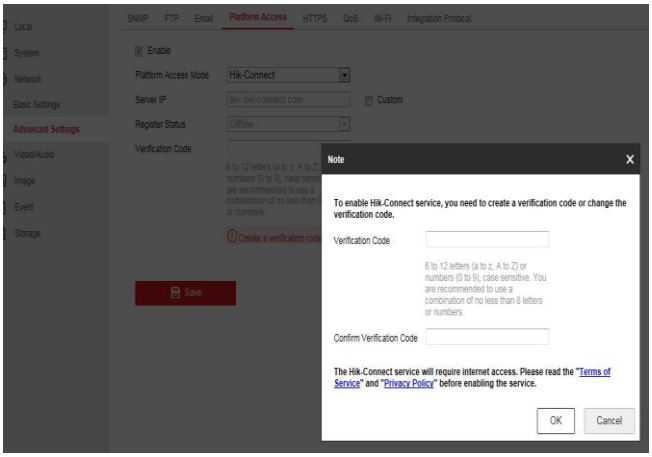

Fig. 2-19 Create verification code for Hik-Connect

By default, during transmission, the video stream is encrypted.

2.6 Security Management

2.6.1 IP Address Filter

The IP Address Filter prevents unauthorized clients from accessing a device. Click the **Enable IP Address Filter** checkbox to activate this feature.

Select the type of IP Address Filter in the drop-down list: **Forbidden** or **Allowed**

- **Allowed** mode indicates that only IP addresses on the IP Address Filter List are able to access the device. The maximum number of IP addresses that can be added to this list, is 48.
- **Forbidden** mode indicates that all IP addresses on the IP Address Filter List are forbidden to access the device. The maximum number of IP addresses that can be added to this list, is 48.

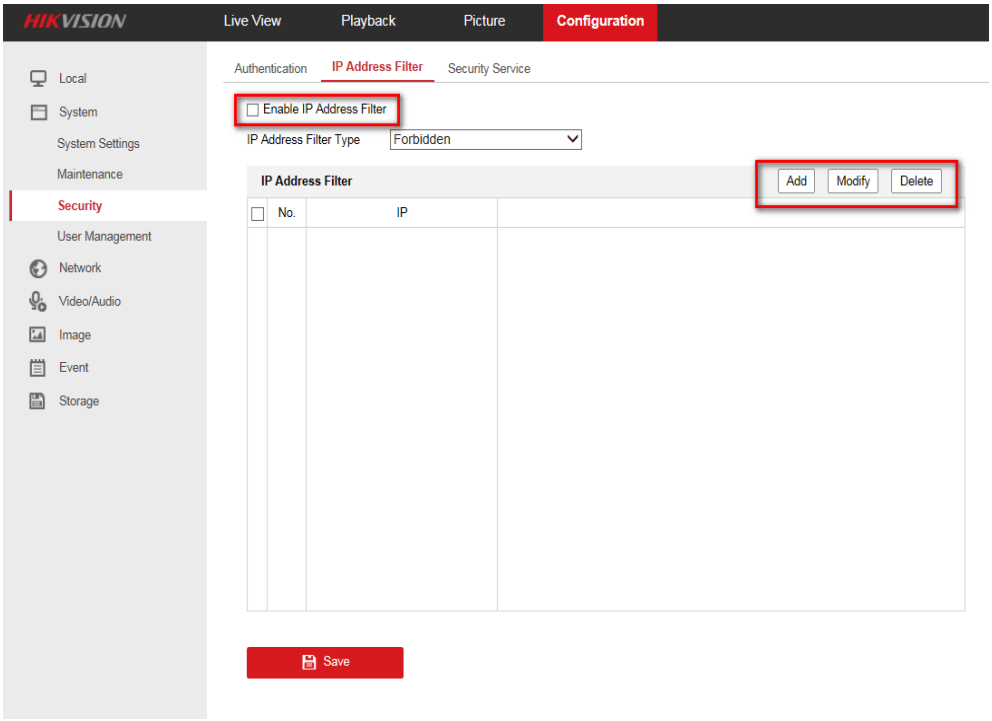

Fig. 2-20 IP Address Filter

2.6.2 802.1x

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X. A user can configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

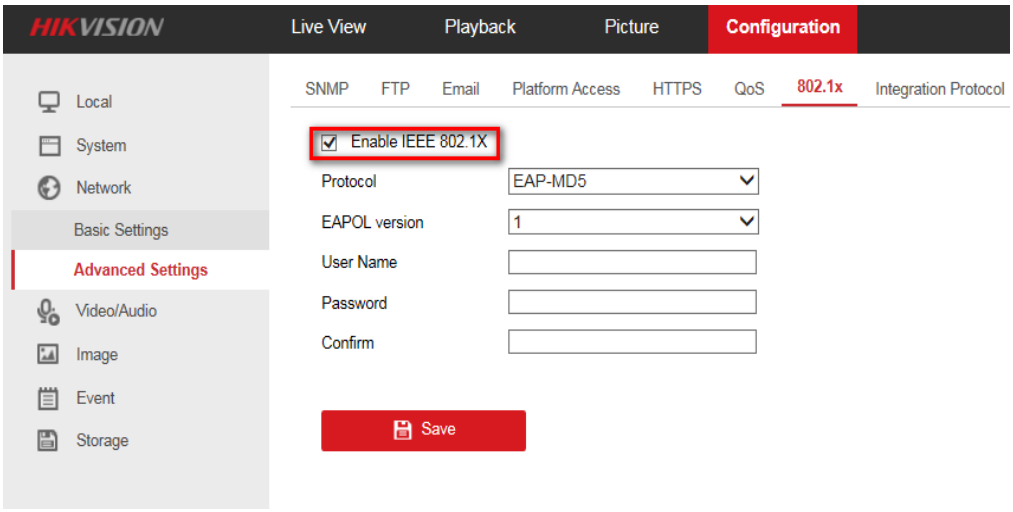

Fig. 2-21 802.1x Configuration

2.6.3 Encryption of Device Parameters Exporting/Importing

Device parameters can be exported by entering a password that is created by a user while exporting the device parameters file. The file doesn't include admin password information. A user needs to enter the password of the device parameters file while importing the file into a device.

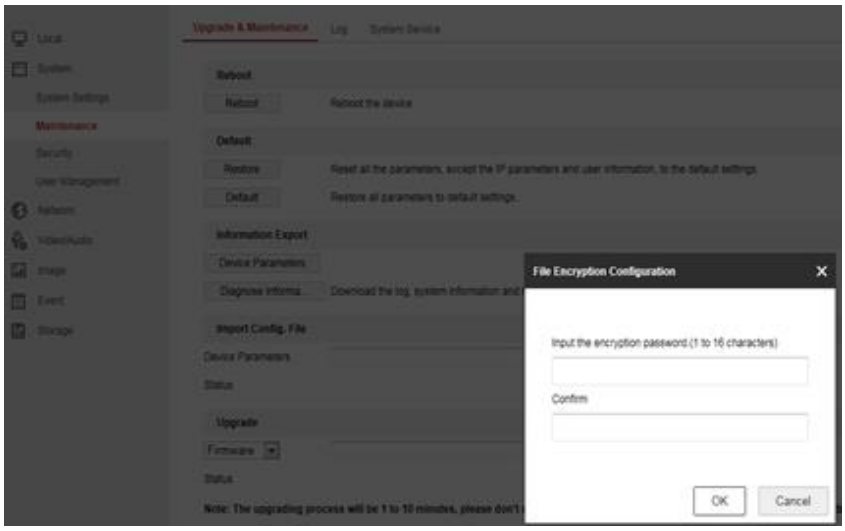

Fig. 2-22 Exporting Device Parameters

It's recommended to set a strong password for the file and store the file safely.

2.6.4 Default

If you are unsure about the configurations of a device, you can restore the device to make it recover to a known state.

There are two ways of restoring the device, **Restore** and **Default**.

- **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.

Enter the Maintenance interface: **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**. (Fig. 2-27)

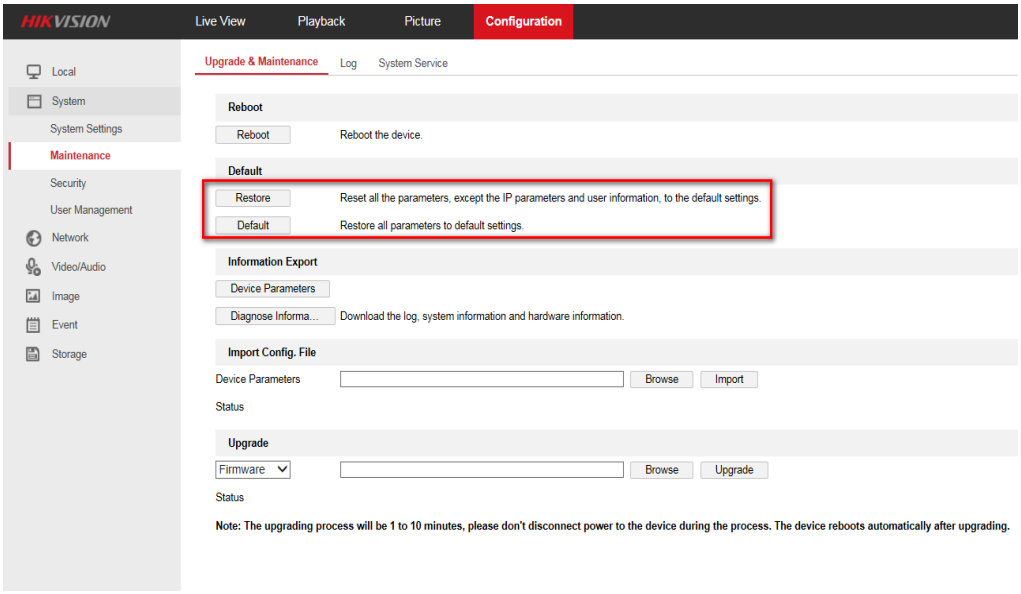

Fig. 2-23 Default

2.6.5 Time Synchronization

Time zone configuration and two time synchronization methods are supported.

1) **Manual Time Sync.** or **Sync. with computer time.**
2) Time synchronization with NTP server. NTP server address, port and interval can be configured.

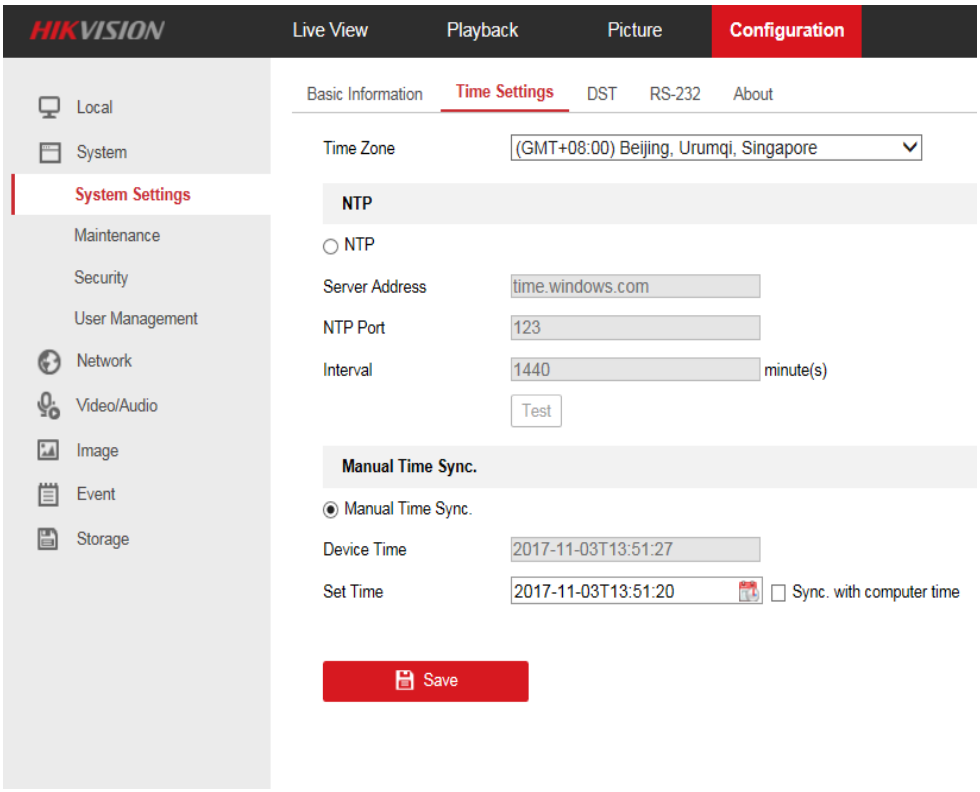

Fig. 2-24 Time Settings

2.7 Firmware upgrade

It is highly recommended that users regularly upgrade to the latest firmware to ensure security updates and bug fixes are installed.

2.7.1 Checking the latest firmware version

Enter the System Settings interface to check the firmware version information: **Configuration** > **System** > **System Settings** > **Basic Information**. (Fig. 2-29)

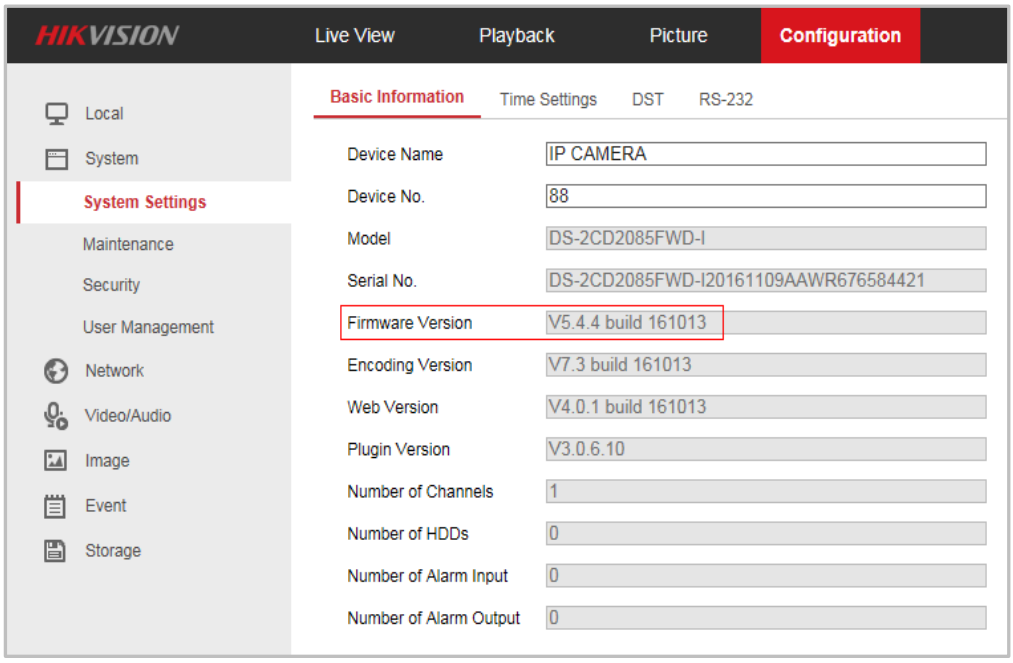

Fig. 2-25 Firmware Version

2.7.2 Upgrading to the Latest Firmware

The steps to upgrade to the latest firmware are:

1) Download the firmware to a computer on the same network as the camera.
2) Log into the camera's management interface from the computer with the firmware file and select **firmware** or **firmware directory** to locate the upgrade file.
3) Click **Upgrade** to start the upgrade. If the Firmware Directory is selected, the correct firmware in the directory is recognized automatically to start upgrading.

Note: The upgrade process will take 1 to 10 minutes. Please do not disconnect power to the camera during this process. The camera reboots automatically after the upgrade.

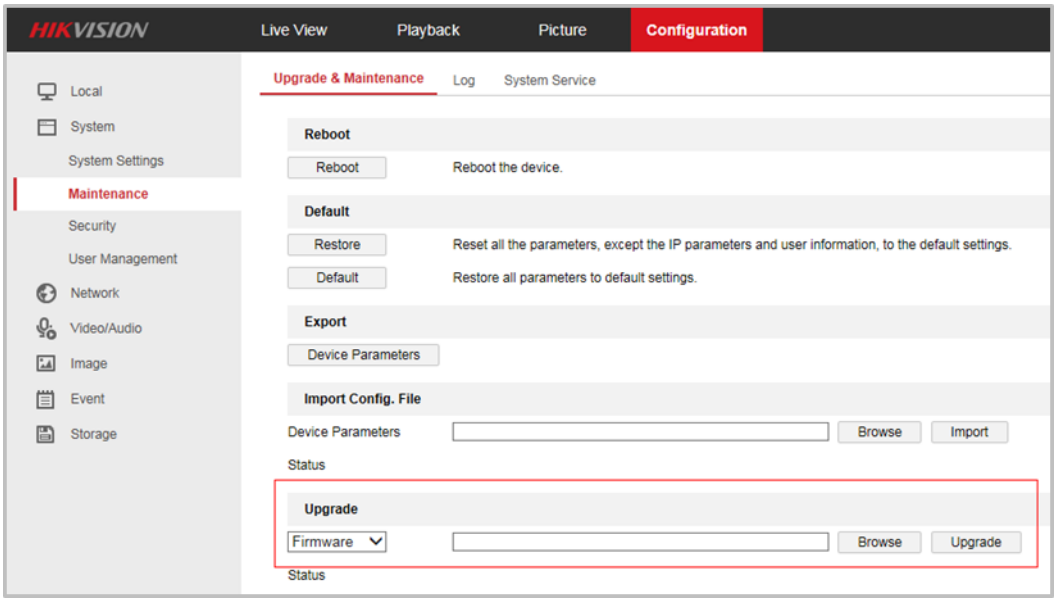

Fig. 2-26 Firmware Upgrade

2.8 Management Security

Security management is one of the most important elements of product security. None of the technical cybersecurity settings and configurations can secure a system on their own if users are not following cybersecurity best practices. Below, are some general rules for security management:

(1) Develop product security related systems, processes, plans, operating instructions and forms. Document all processes and run table-top exercises or drills to practice what to do in an incident.

(2) Use security scanning tools, configuration verification, and penetration testing to evaluate the security of networks and devices, then identify potential security risks, assess the risk and prepare a remediation plan.

(3) Compile the corresponding reinforcement proposal and operation guide, according to the results of the product security assessment. And then guide the reinforcement and keep track of the reinforcement effect.

(4) Monitor the security on all networks and devices, 24/7. This monitoring should include, but is not limited to, system and network availability, malware detection, and intrusion detection.

(5) Periodically initiate cybersecurity audits of your network and applications. Adjust the firewall of the video monitoring platform, server, and other network devices and host system security policy according to the results, to protect the security of products further.

(6) It can refer to the emergency response mechanism of the Internet industry, and combine its own emergency process to provide security emergency service for

video surveillance system.

(7) Strengthen the security awareness and system security management training for different types of video surveillance staff.

(8) Product security settings should follows the basic principles of information system security: the principle of least privilege, the principle of decentralization and balance, the principle of security isolation, etc.

3 Conclusion

This security guide will be updated regularly to show you the best practices of latest network security.

Hikvision have been devoted to the research of network security for many years and will provide users with industry-leading cybersecurity technology.

You can view http://www.hikvision.com/cn/support_list_591.html to find more cybersecurity information. If you have any question on cybersecurity, please email to HSRC@hikvision.com.