HIKVISION®

Hikvision Network Security Hardening Guide

Copyright Disclaimer

About This Document

The guide introduces users to the security features of Hikvision network devices and how to use and manage network devices safely. While this document provides a general safety overview, users should select security settings that are appropriate to their actual situation. The introduction and configuration path of network security functions in this document is based on a camera device of version 5.7 as an example. This guide can be used as a reference for other devices, though some settings and navigation paths may vary depending on the device version.
Hikvision reserves the right to update this documentation. Please kindly find the latest version on the company website (https://www.hikvision.com/en).

Trademarks Acknowledgement

海康威视, HIKVISION and other Hikvision trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CONTENT DESCRIBED IN THIS DOCUMENTATION IS PROVIDED “AS IS", AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, FITNESS FOR COMMERCIAL USE OR A PARTICULAR PURPOSE.

HIKVISION PROVIDES NO WARRANTY ON THE ACCURACY OF THIS DOCUMENTATION CONTENT AND RESERVES THE RIGHT TO CORRECT OR MODIFY THE CONTENT WITHOUT FURTHER NOTICE. ANY DECISIONS RELIED ON OR BY THE USE OF THIS DOCUMENTATION, TOGETHER WITH ANY CONSEQUENCES THAT IT MAY CAUSE SHALL BE UNDER YOUR OWN RESPONSIBILITY.

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

CONTENTS

1 Introduction

This document is written as a general security hardening guideline for users to protect their own devices. Measurements should be taken into consideration depending on the application scenarios. If issues arise after implementing any of the recommended security enhancements, reverting to default settings may resolve them.

You can find more cybersecurity information by visiting the Hikvision Official Cybersecurity Center:

https://www.hikvision.com/en/support/cybersecurity/.

If you have any feedback for the Hikvision cybersecurity team, please email HSRC@hikvision.com.

1.1 Passwords

Passwords are a critical part of securing network devices. To protect your system from unauthorized access, it is essential to create strong, unique passwords and follow best practices for password management. This section provides guidance on setting and maintaining secure passwords in line with international standards.

How to create a strong password?

Strong passwords are a critical first line of defense. Follow these best practices to ensure your passwords are secure:

- Use at least 8 characters. Longer passwords or passphrases are more secure because they are harder to guess.
- Include at least three of the following character types: numbers, uppercase letters, lowercase letters, and special characters.
- Avoid including the following items in your password: your account's username, "123", "admin", 4 consecutive digits in ascending or descending order, or 4 consecutive repeated characters.
- Do not use passwords that are commonly found in password breach lists, such as "1qaz2wsx", "p@ssword", or similar risky choices.

The Password Phrase Method:

A passphrase is a memorable sentence or phrase that is difficult for others to guess.

Here are some tips for creating a strong but memorable passphrase.

- Choose a phrase that has numbers.
- Use only the first letter in each word.
- Maintain the original case of each letter, just as it appears in the phrase.
- Use actual numbers whenever possible. Use “2” for “two” or “to” and “4” for “four” or “for”.
- Include punctuation.

Let’s take the following phrase as an example:

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

Using the Password Phrase method explained above, the password becomes:

"MftNYwla3ita!".

Some general password/security tips

- Avoid using dictionary words in any language.
- Do not use sequences or repeated characters.
- Change the password at a recurring interval.
- Do not allow browsers (e.g., Internet Explorer) to store passwords.
- Do not type passwords on computers that you do not control.
- Never share your password or send it by email.
- Never respond to an email asking for personal information. (Hikvision will never ask for your personal information in an email).
- Keep your software updated and be cautious with email attachments and links.

2 Standard Configuration

This guide outlines the minimum recommended settings for small monitoring systems and uses network camera as the example throughout. The following configuration is recommended for home, office or small business scenarios. Configurations will be different based on the network and the size of the system you are installing.

ALL device configuration presented in this article is performed via a web browser except for some activation contents.

2.1 Activate The Device by Setting a Strong Password

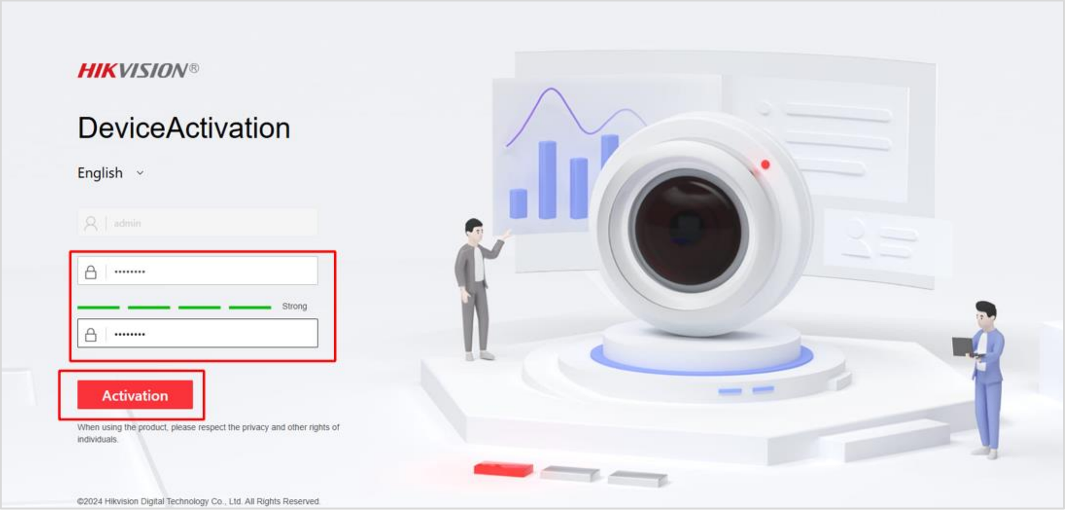
Before using your device, you must activate it by creating a strong password.

Activation can be performed via web browser, SADP software and client software. Before activating device, please make sure your PC and device connect to the same LAN. You can refer to ***Appendix A*** to get detailed configuration steps.

2.1.1 Activation via Web Browser

Steps:

1. Input the default IP address of your device (e.g., 192.168.1.64) into the address bar of the web browser, and press **enter** to access the activation page.



HIKVISION®

DeviceActivation

English

admin

••••••••

Strong

••••••••

Activation

When using the product, please respect the privacy and other rights of individuals.

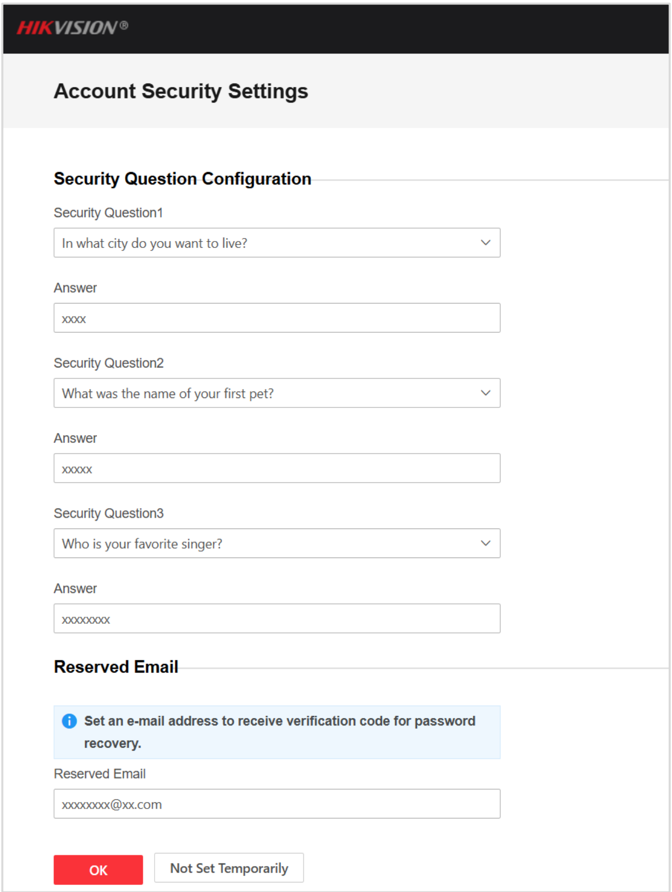
©2024 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

Figure 1 Activation via Web Browser

2. Create a strong password and enter it into the password field.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters) to increase the security of your product.

3. Confirm the password.
4. Click "**Activation**" to save the password and access the Account Security Settings page.



HIKVISION®

Account Security Settings

Security Question Configuration

Security Question1: In what city do you want to live?

Answer: xxxx

Security Question2: What was the name of your first pet?

Answer: xxxxx

Security Question3: Who is your favorite singer?

Answer: xxxxxxxx

Reserved Email

Set an e-mail address to receive verification code for password recovery.

Reserved Email: xxxxxxxx@xx.com

Figure 2 Activation via Web Browser

5. We strongly recommend that you immediately select and fill in three security questions. The answers to these questions should not be the same. After filling in, enter your reserved email address.
6. If you don't want to set this now, you can click "**Not Set Temporarily**".

2.1.2 Activation via SADP Software

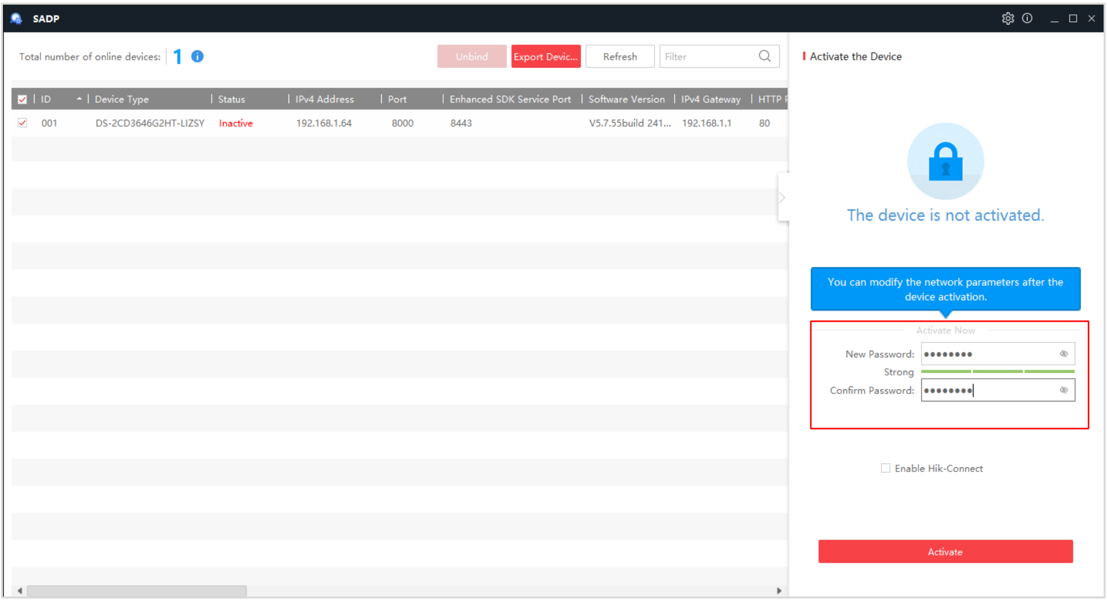
SADP software can detect devices on your network, activate them, and modify network configurations, etc.

You can get the SADP software from Hikvision official website and install it according to the instructions. Follow the steps to activate the device via SADP.

Steps:

1. Run the SADP software to search for devices on your network.

2. Check the device status in the device list and select your inactive device.



SADP

Total number of online devices: 1

☑ ID	Device Type	Status	IPv4 Address	Port	Enhanced SDK Service Port	Software Version	IPv4 Gateway	HTTP P
☑ 001	DS-2CD3646G2HT-LIZSY	Inactive	192.168.1.64	8000	8443	V5.7.55build 241...	192.168.1.1	80

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

Figure 3 Activation via SADP

3. Create a strong password and enter it into the password field, and then confirm it.

> **STRONG PASSWORD RECOMMENDED**– We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters) to increase the security of your product.

4. Click "**Activate**" to activate the device.

Note: If activation fails, please make sure that the password meets the requirements and try again.

2.1.3 Activation via iVMS-4200

iVMS-4200 is a client software that supports activation for multiple device types. You can get it from Hikvision official website and install it according to the instructions. Follow the steps to activate the device via iVMS-4200.

Steps:

1. Run the client software, then you can see the control panel, as shown in the figure below.

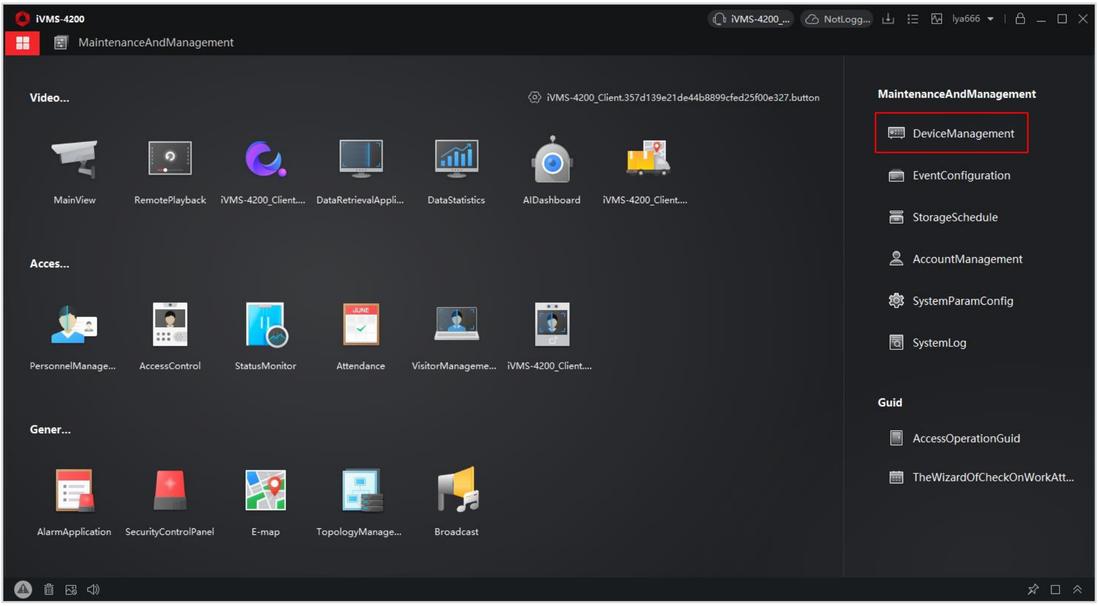
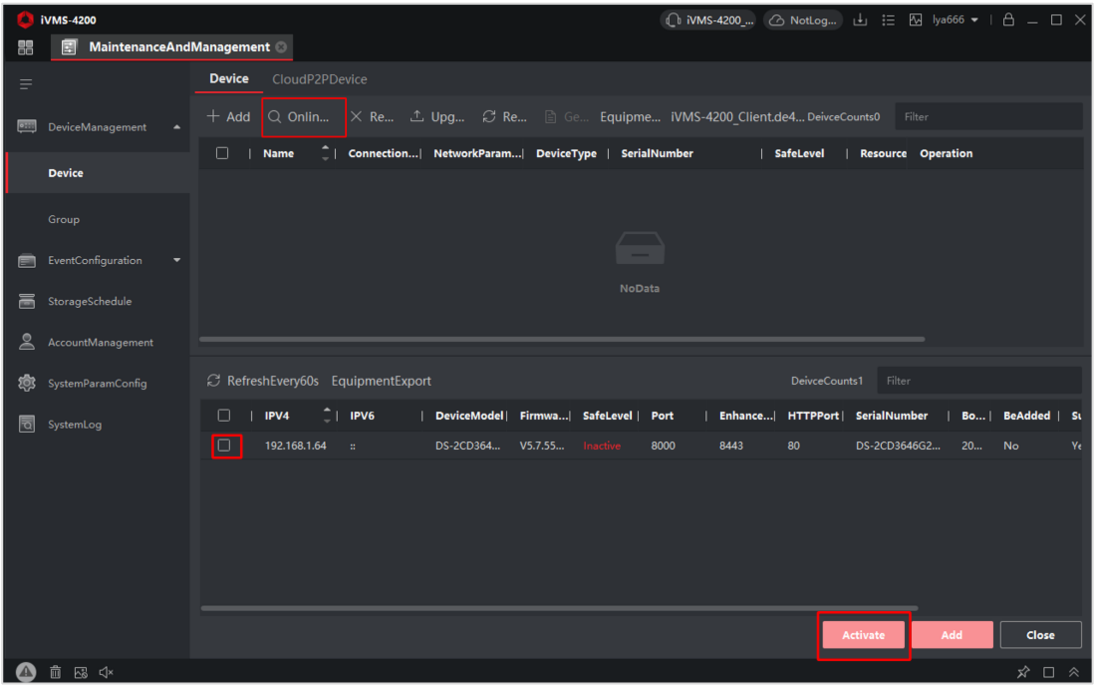


Figure 4 Activation via iVMS-4200

2. Click “**Device Management**” to enter the Device Management interface as shown in the figure below. Then click “**OnlineDevice**” to find devices.



□	IPV4	IPV6	DeviceModel	Firmwa...	SafeLevel	Port	Enhance...	HTTPPort	SerialNumber	Bo...	BeAdded	Su
□	192.168.1.64	::	DS-2CD364...	V5.7.55...	Inactive	8000	8443	80	DS-2CD3646G2...	20...	No	Ye

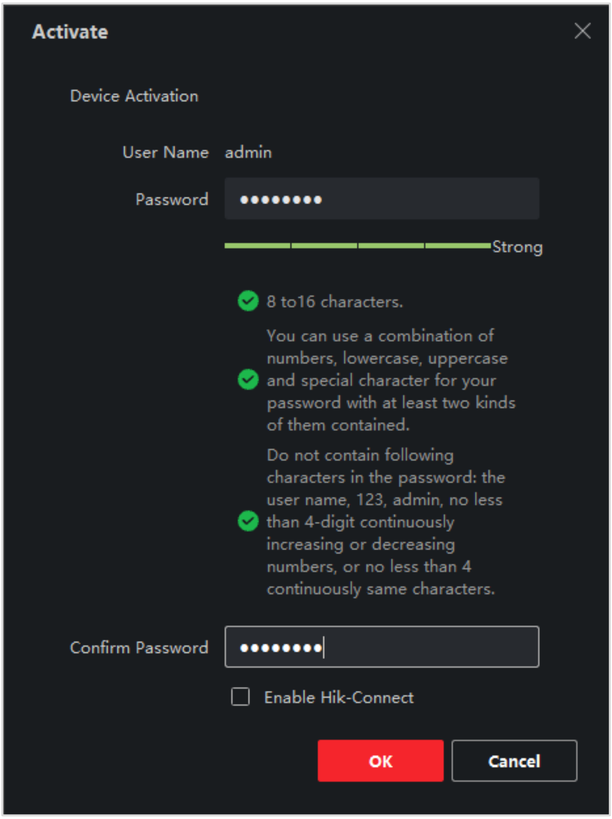
Figure 5 Activation via iVMS-4200

3. Check the device status in the device list, and select your inactive device.

4. Click “**Activate**” to enter the Activate interface.

5. Create a strong password and enter it into the password field, and then confirm it.

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters) to increase the security of your product.



Activate

Device Activation

User Name admin

Password ●●●●●●●●

Strong

✓ 8 to16 characters.

✓ You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

✓ Do not contain following characters in the password: the user name, 123, admin, no less than 4-digit continuously increasing or decreasing numbers, or no less than 4 continuously same characters.

Confirm Password ●●●●●●●●

□ Enable Hik-Connect

Figure 6 Activation via iVMS-4200

6. Click “**OK**” button to complete the activation process.

2.2 Time Synchronization

From a security perspective, accurate date and time settings are essential for secure video recording and system logging. You can synchronize the device time using either an NTP server or manually by navigating to:

- **Configuration > Common Settings > Time Settings**

  or

- **Configuration > System > System Settings > Time Settings**.

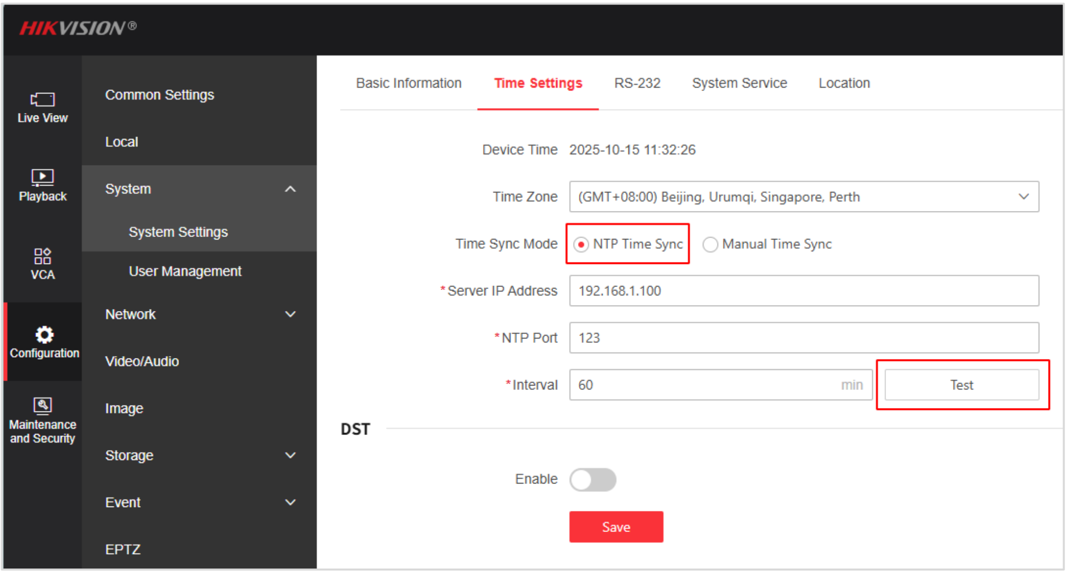
Before you configure time, ensure that all time calibration sources, if already configured, are consistent and accurate.

2.2.1 NTP Time Synchronization

For accurate and reliable time settings, use a Network Time Protocol (NTP) server to synchronize your device’s clock. Before configuring NTP synchronization, ensure you have the necessary NTP server details or have set up an NTP server on your network. Please note that the NTP server and your device must be on the same network.

Steps:

1. Go to **Time Settings** page, select your time zone, and choose “**NTP Time Sync**”.
2. Enter the NTP server’s IP address or domain name, port, and synchronization interval.
3. Click “**Test**” to check connectivity. If successful, click “**Save**”.



Device Time 2025-10-15 11:32:26

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

Time Sync Mode ● NTP Time Sync ○ Manual Time Sync

*Server IP Address 192.168.1.100

*NTP Port 123

*Interval 60 min

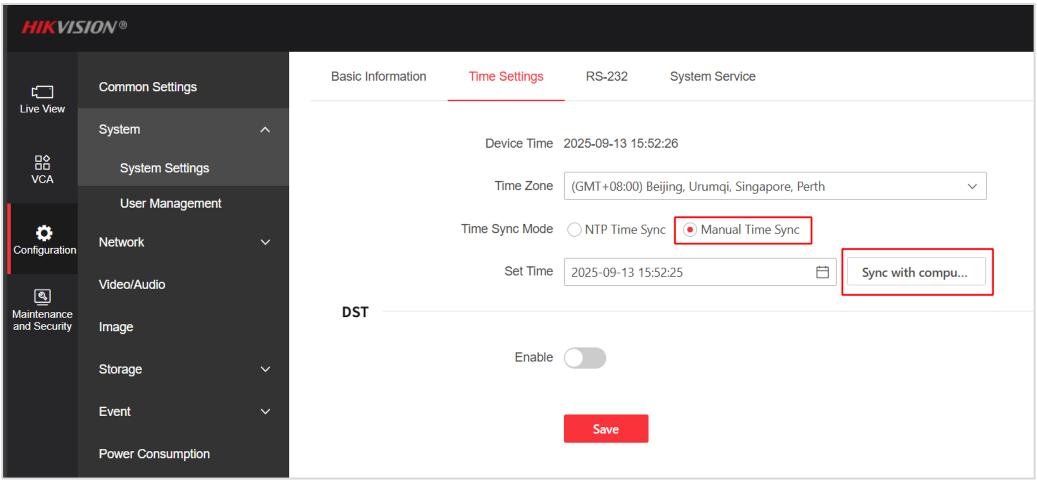
Figure 7 NTP Time Synchronization

2.2.2 Manual Time Synchronization

If no NTP server is available, you can configure the time manually or sync it with your local computer.

Steps:

1. Go to the **Time Settings** page, select your time zone, and then choose “**Manual Time Sync**”.
2. Set the date and time manually or click “**Sync with computer time**” to match your local computer.
3. Click “**Save**” to apply the settings.



Device Time 2025-09-13 15:52:26

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

Time Sync Mode ○ NTP Time Sync ● Manual Time Sync

Set Time 2025-09-13 15:52:25

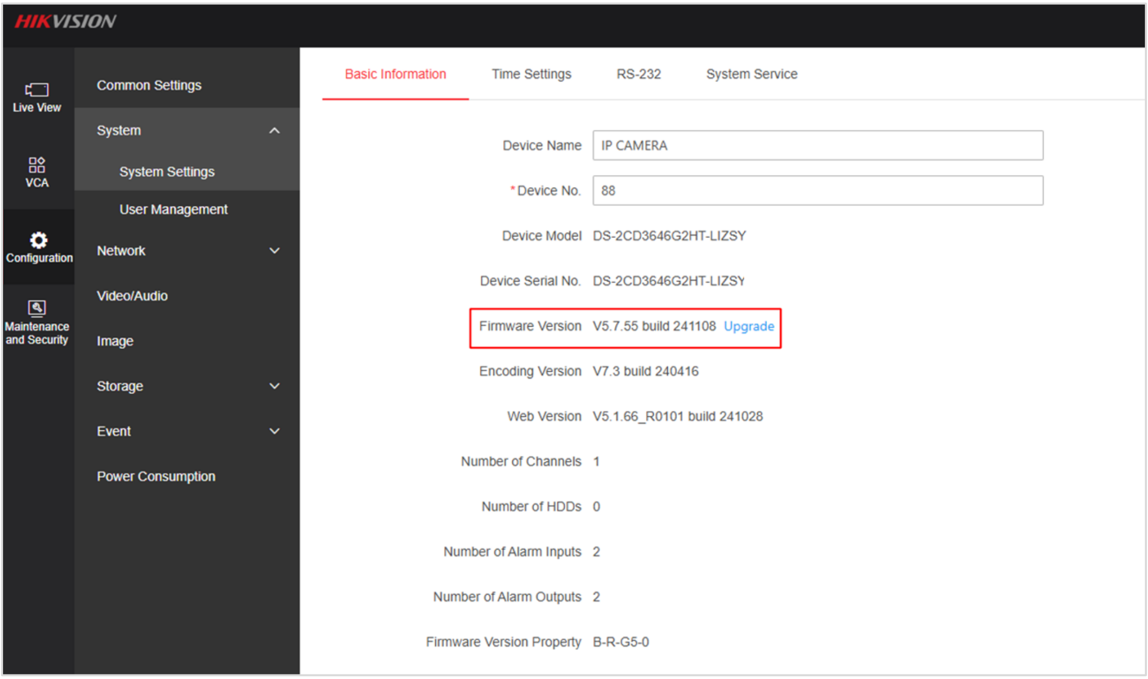
Figure 8 Manual Time Synchronization

2.3 System Upgrade

Firmware is the software that enables and controls the functions of your network device. To ensure you have the latest security updates and bug-fixes, always use the most recent firmware version.

2.3.1 Check the Current Firmware

To check your current firmware version, go to: **Configuration > System > System Settings > Basic Information**.



Device Name: IP CAMERA
*Device No.: 88
Device Model: DS-2CD3646G2HT-LIZSY
Device Serial No.: DS-2CD3646G2HT-LIZSY
Firmware Version: V5.7.55 build 241108
Encoding Version: V7.3 build 240416
Web Version: V5.1.66_R0101 build 241028
Number of Channels: 1
Number of HDDs: 0
Number of Alarm Inputs: 2
Number of Alarm Outputs: 2
Firmware Version Property: B-R-G5-0

Figure 9 Check Current Firmware

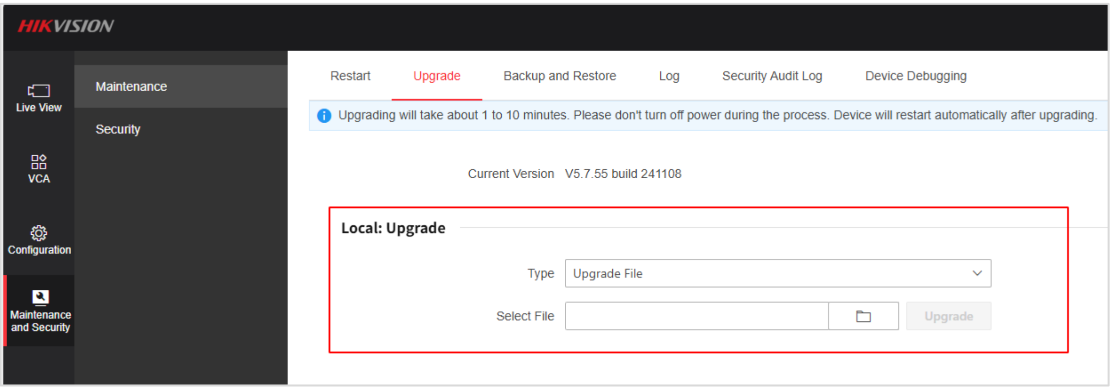
2.3.2 Upgrade the Device to the Latest Firmware Version

You can download the latest firmware package from the official Hikvision firmware website.

Steps:

1. Go to: **Maintenance and Security** > **Maintenance** > **Upgrade**.
2. Choose your upgrade method:
   - Upgrade File: Select the exact path to the upgrade package.
   - Upgrade Directory: Select the directory containing the upgrade package.
3. Click **Folder** 📁 icon to select the upgrade file and then click "**Upgrade**" to start.

Note: The upgrade process typically takes 1 to 10 minutes. Do not disconnect the device's power during the upgrade. The device will automatically reboot when the upgrade is complete.



Upgrading will take about 1 to 10 minutes. Please don't turn off power during the process. Device will restart automatically after upgrading.

Current Version V5.7.55 build 241108

Type Upgrade File

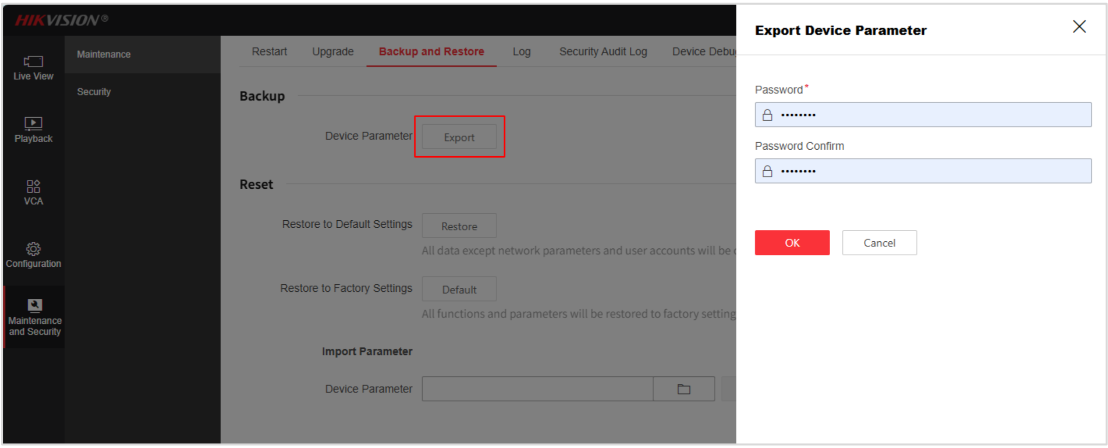
Figure 10 Local Upgrade

2.4 Backup

Backing up device’s parameters is essential for quickly restoring device to its last stable state in case of failure.

Steps:

1. Go to **Maintenance and Security** > **Maintenance** > **Backup and Restore**.
2. Click “**Export**” and then enter the password for this backup file.



All data except network parameters and user accounts will be r

All functions and parameters will be restored to factory setting

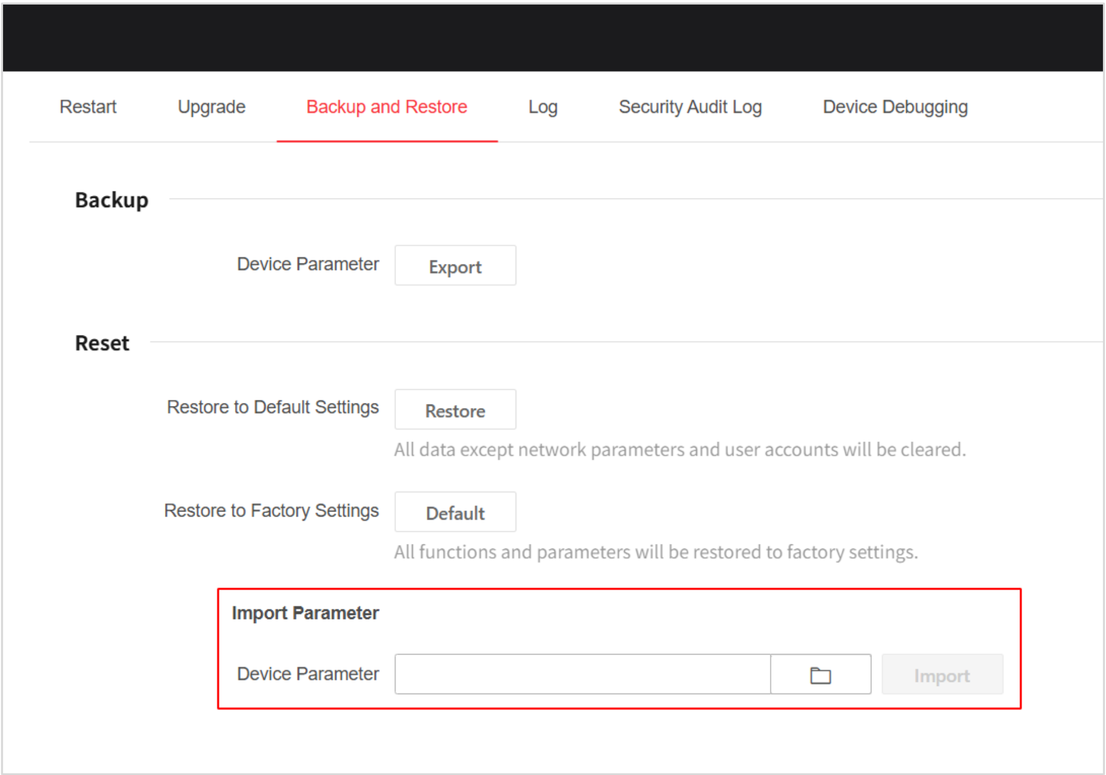
Figure 11 Backup

3. Click “**OK**”, and then the configuration backup file will be automatically downloaded.

You can restore the device to its backup state by importing the backup file into the Import Parameter area below.

Steps:

Click the **Folder** icon, select the backup file, click the “**Import**” button, enter the password you previously set for the backup file, and then click “**OK**” to start the import.



Restart | Upgrade | Backup and Restore | Log | Security Audit Log | Device Debugging

Backup

Device Parameter: Export

Reset

Restore to Default Settings: Restore

All data except network parameters and user accounts will be cleared.

Restore to Factory Settings: Default

All functions and parameters will be restored to factory settings.

Import Parameter

Device Parameter: Import

Figure 12 Backup

2.5 System Restore

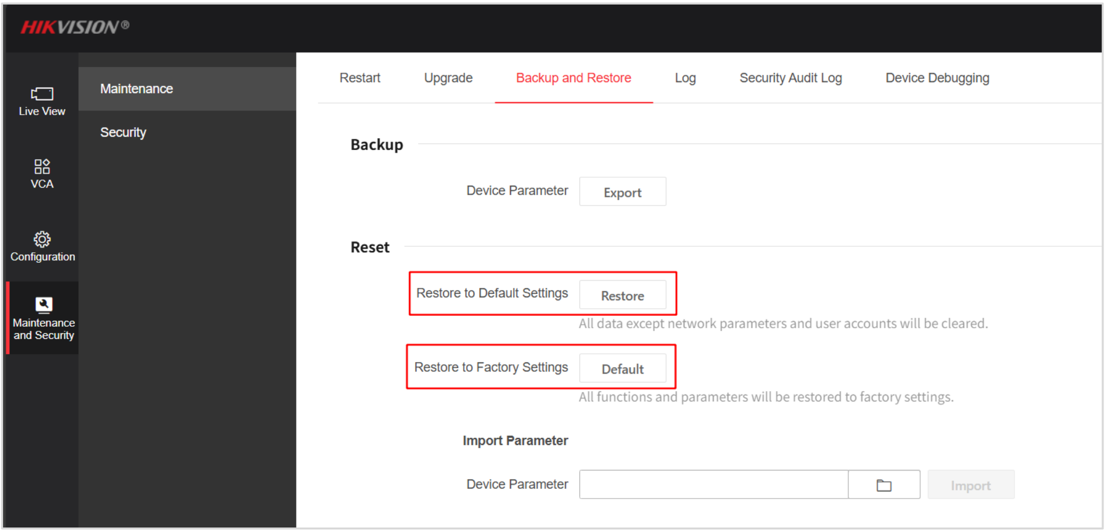
Resetting the device to its factory defaults can return it to a known, clean state, which is essential for the secure use of the device. Before you start configuring the device, be sure it is in a factory-default state. You should also restore the device to its original factory state whenever you must erase user data or retire the equipment.

Warning: Restoring the system will erase configurations, logs, and data depending on the option selected. Always perform a full backup and verify its integrity before proceeding.

Steps:

Go to **Maintenance and Security > Maintenance > Backup and Restore**.

- **Restore to Default Settings**: Clears all data except network parameters and user accounts.
- **Restore to Factory Settings**: Resets all functions and parameters to factory defaults.



All data except network parameters and user accounts will be cleared.

All functions and parameters will be restored to factory settings.

Figure 13 System Restore

Note: After restoring to factory settings, the device’s IP address will also revert to its factory default value (e.g., 192.168.1.64). Please be aware of this change before proceeding.

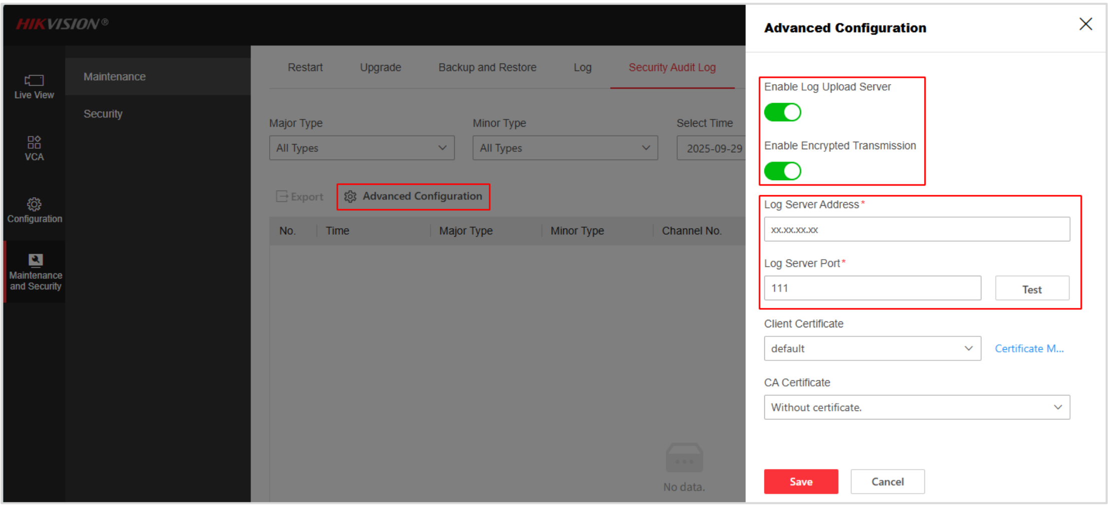
2.6 Remote Syslog

Hikvision network cameras support sending logs to a remote syslog server, which can better preserve the logs and facilitate centralized auditing. The syslog standard is based on RFC 3164. Be sure to set up a remote syslog server that support RFC 3164 beforehand.

Steps:

1. Go to **Maintenance and Security** > **Maintenance** > **Security Audit Log.**

2. Click “**Advanced Configuration**”, enable the **Log Upload Server**, and set the log server parameters. Enabling **Encrypted Transmission** is also recommended so that the data sent by the device to the log server will be encrypted for transmission.



Major Type: All Types

Minor Type: All Types

Select Time: 2025-09-29

Enable Log Upload Server: on

Enable Encrypted Transmission: on

Log Server Address*: xx.xx.xx.xx

Log Server Port*: 111

Client Certificate: default

CA Certificate: Without certificate.

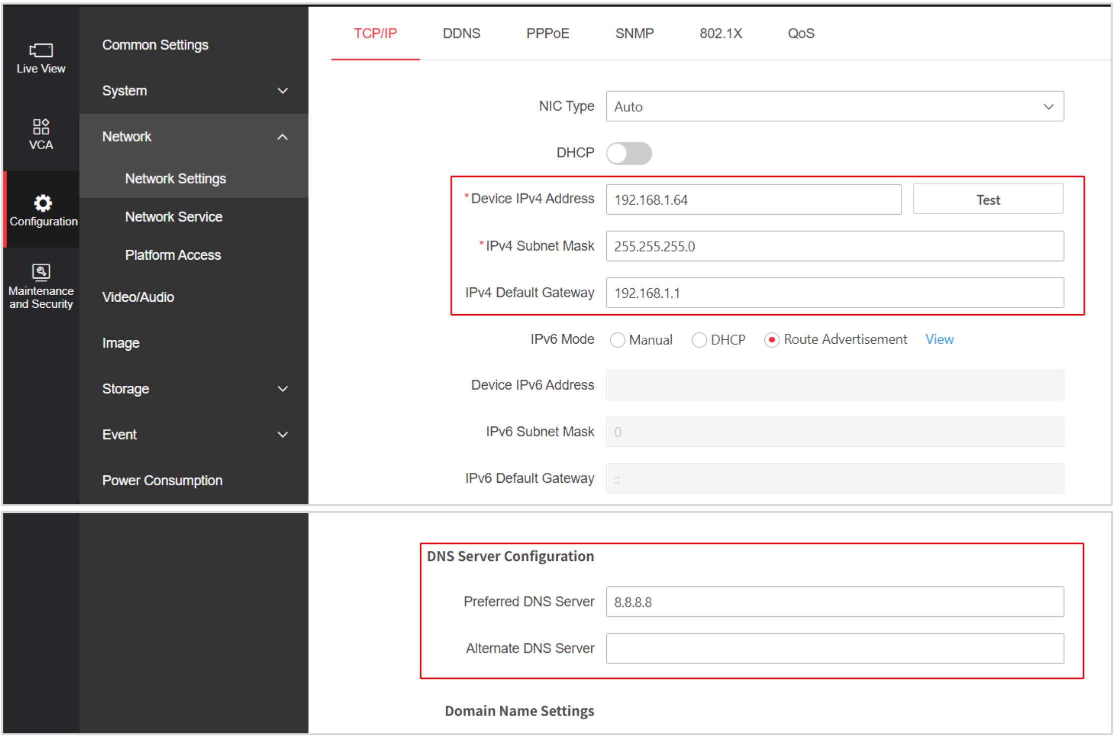
Figure 14 Remote Syslog

3. Click “**Save**” to apply the settings.

2.7 Configure Basic Network Settings

Steps:

1. Go to **Configuration** > **Network** > **Network Settings** > **TCP/IP**.
2. Enter the required network parameters: **IPv4 Address**, **Subnet Mask**, **Default Gateway** and **DNS Sever**.
3. When finished, click "**Save**" to apply the network settings.



NIC Type: Auto

DHCP

*Device IPv4 Address: 192.168.1.64

*IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 192.168.1.1

IPv6 Mode: ○ Manual ○ DHCP ● Route Advertisement

Device IPv6 Address:

IPv6 Subnet Mask: 0

IPv6 Default Gateway: ::

DNS Server Configuration

Preferred DNS Server: 8.8.8.8

Alternate DNS Server:

Domain Name Settings

Figure 15 Configure Basic Network Settings

2.8 Disable DDNS

Hikvision network devices support Dynamic Domain Name System (DDNS), which allows remote access by mapping a dynamic IP address to a fixed domain name. While DDNS can be convenient, it also introduces security risks by exposing your device to the internet, making it easier for the attackers to find and target your system. This function is disabled by default. If you do not need DDNS service, ensure it remains disabled.

Steps:

1. Go to **Configuration** > **Network** > **Network Settings** > **DDNS**.
2. Ensure the "**Enable**" switch is turned **off**.

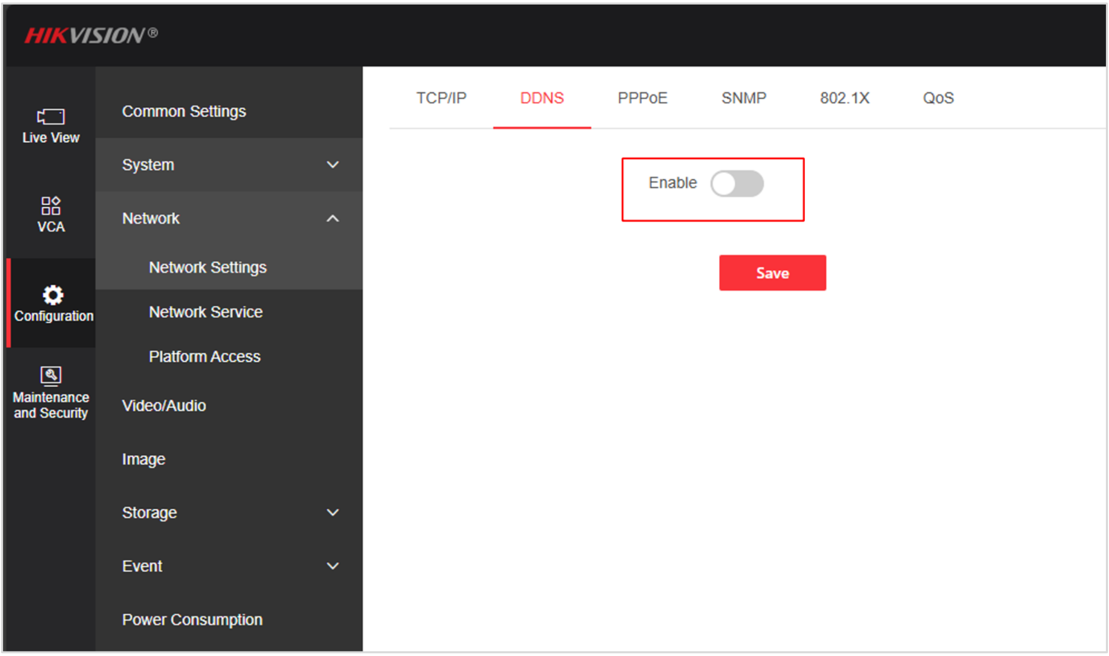


Figure 16 Disable DDNS

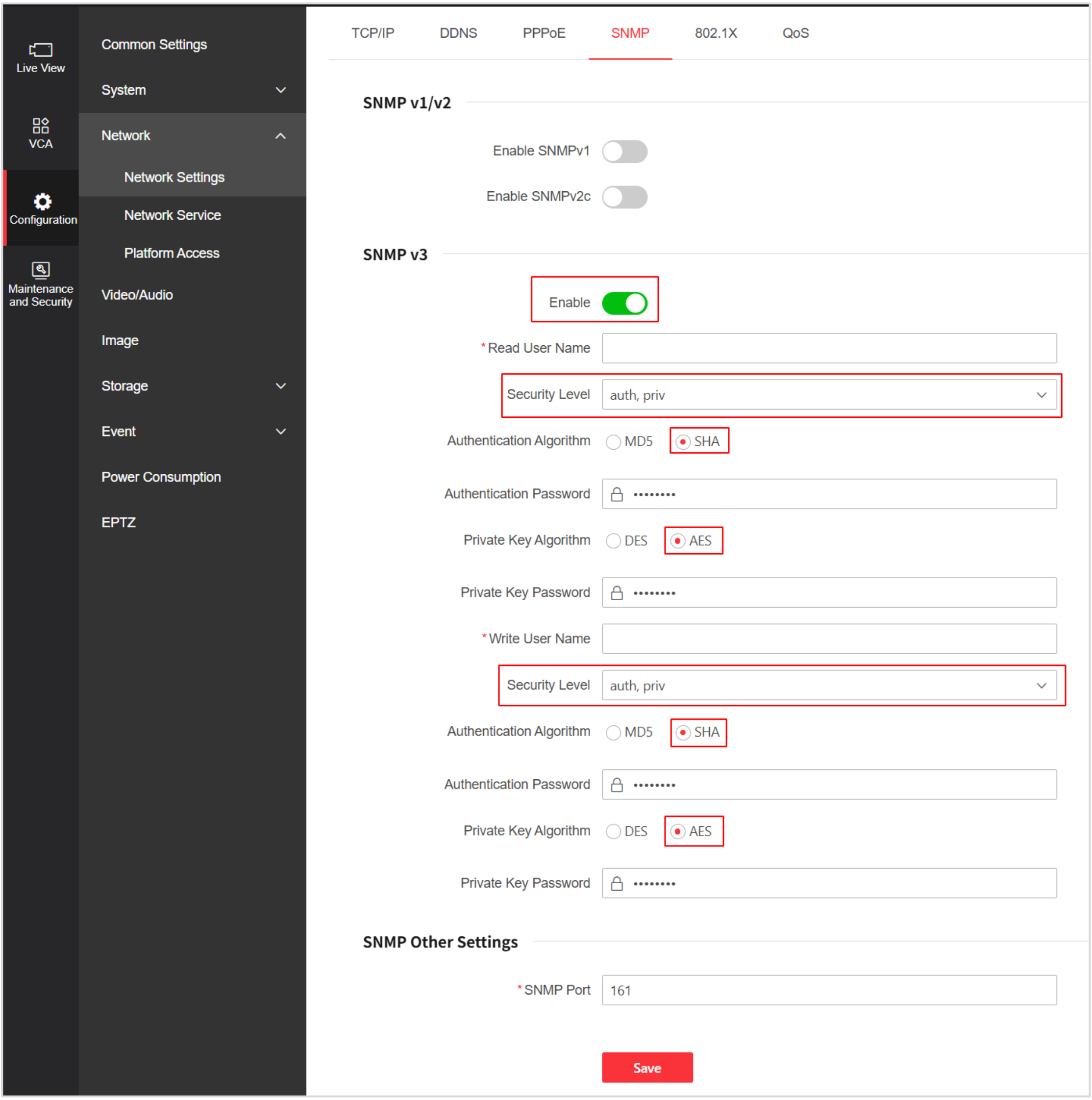
2.9 Choose SNMPv3

According to the principle of minimizing network exposure in cybersecurity, SNMP service is disabled by default. Keep disabled when not in use.

If SNMP is required, always enable the SNMPv3, which offers significantly stronger security than SNMPv1 or SNMPv2c. SNMPv3 supports authentication and encryption, helping protect management data from interception, spoofing, and tampering. Earlier versions transmit data in plain text, making them vulnerable to compromise.

Steps:

1. Go to **Configuration > Network > Network Settings > SNMP**.
2. Ensure that “Enable SNMPv1” and “Enable SNMPv2c” are turned **off**, and turn on the “**Enable**” switch of SNMPv3.
3. Configure the **SNMPv3** settings. For maximum security, select the security level as "**auth**, **priv**", use **SHA** as the authentication algorithm, **AES** as the private key algorithm, and set strong passwords.



SNMP v1/v2

Enable SNMPv1 ○

Enable SNMPv2c ○

SNMP v3

Enable ●

*Read User Name

Security Level: auth, priv

Authentication Algorithm: ○ MD5 ● SHA

Authentication Password: ••••••••

Private Key Algorithm: ○ DES ● AES

Private Key Password: ••••••••

*Write User Name

Security Level: auth, priv

Authentication Algorithm: ○ MD5 ● SHA

Authentication Password: ••••••••

Private Key Algorithm: ○ DES ● AES

Private Key Password: ••••••••

SNMP Other Settings

*SNMP Port: 161

Figure 17 Choose SNMPv3

4. Click “**Save**” to apply the settings.

Note: Depending on your device’s firmware version, a reboot may be required for the changes to take effect.

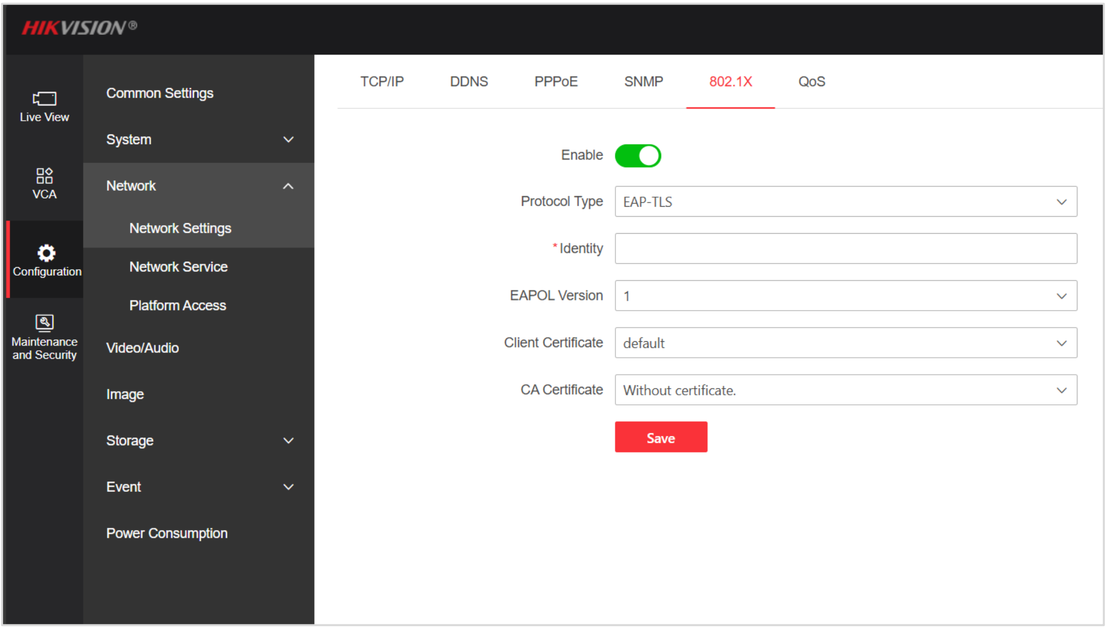
2.10 IEEE 802.1X

Hikvision network devices support IEEE 802.1X port-based network access control, utilizing EAP-TLS as the authentication method. This feature ensures that only authorized devices can connect to the network by validating their certificates.

This function is disabled by default. If you need to use it, enter the 802.1X configuration page to set it. For enhanced security, we strongly recommend selecting **EAP-TLS** as the protocol type. For optimal security, we recommend authenticating your device with a client certificate that has been signed by a certificate authority (CA) that is trusted by both the device and the authentication server.

Steps:

1. Go to **Configuration > Network > Network Settings > 802.1X**.
2. Turn on the “**Enable**” switch.
3. Choose **EAP-TLS** as protocol type, then enter the Identity field (Length should be no more than 32) and pick the certificates. Regarding the configuration of the certificate, you can refer to the ***Section 2.12***.
4. Click “**Save**”.



Enable: on
Protocol Type: EAP-TLS
* Identity:
EAPOL Version: 1
Client Certificate: default
CA Certificate: Without certificate.

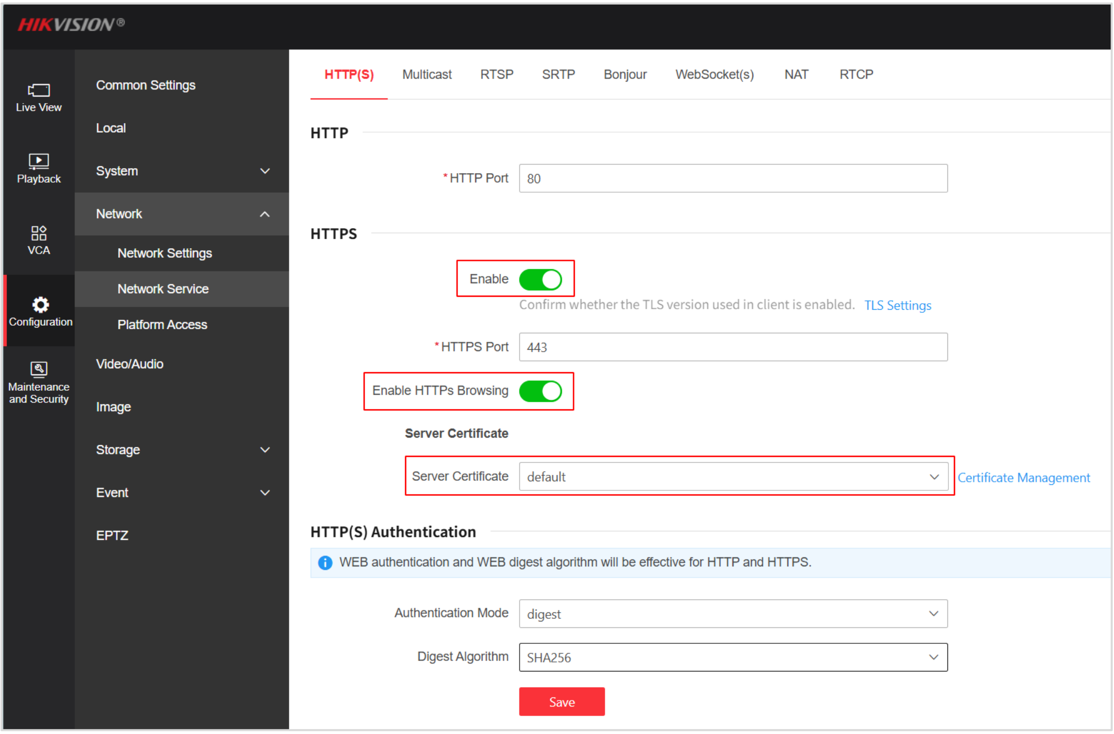
Figure 18 IEEE 802.1X

2.11 HTTPS and HTTPS Browsing

HTTPS can provide confidentiality and integrity when a website and its associated web server are communicating. HTTPS is enabled by default. Moreover, on Hikvision network devices you can enable HTTPS Browsing (also known as HTTPS Redirection) so that every access to the device’s web interface is automatically redirected to HTTPS, ensuring that all communication is encrypted.

Steps:

1. Go to **Configuration** > **Network** > **Network Service** > **HTTP(S)**.
2. Ensure the “**Enable**” switch is on and turn on the “**Enable HTTPS Browsing**” switch.
3. Select the appropriate server certificate. Regarding the configuration of the certificate, you can refer to the ***Section 2.12***.
4. Click the “**Save**” button to save the settings.



HTTP

*HTTP Port: 80

HTTPS

Enable: On

Confirm whether the TLS version used in client is enabled.

*HTTPS Port: 443

Enable HTTPs Browsing: On

Server Certificate

Server Certificate: default

HTTP(S) Authentication

WEB authentication and WEB digest algorithm will be effective for HTTP and HTTPS.

Authentication Mode: digest

Digest Algorithm: SHA256

Figure 19 Enable HTTPS

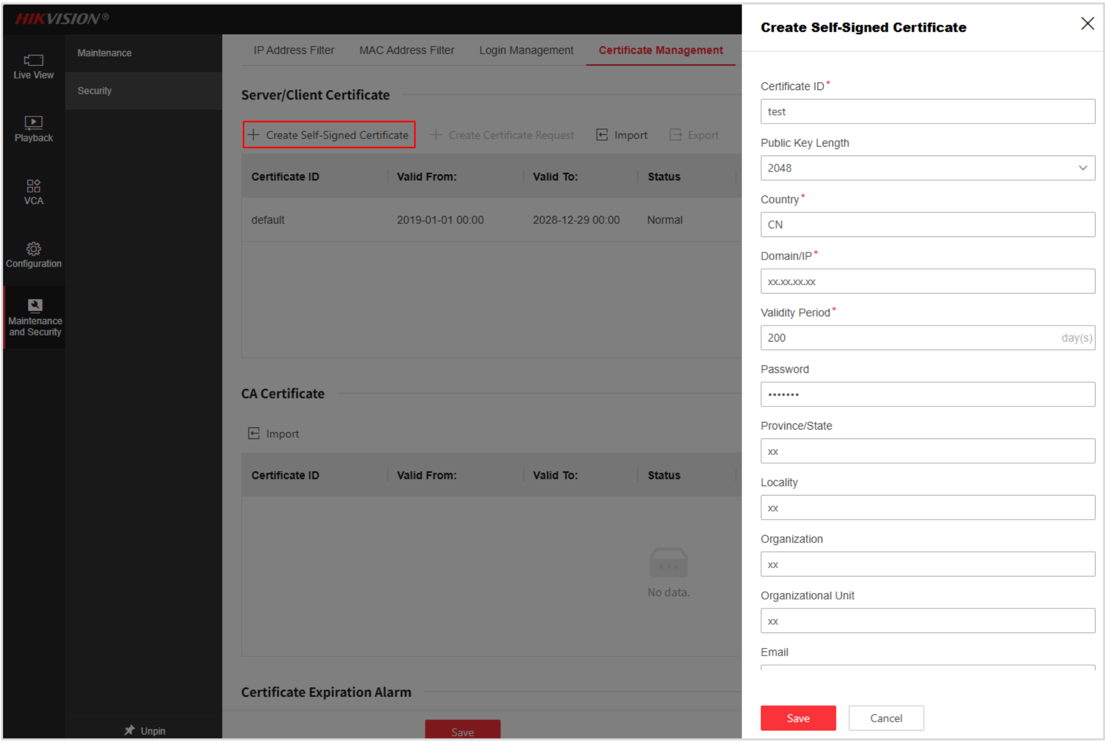
2.12 Certificate Management

When the device is activated, a default certificate will be automatically generated. Also, you can create and use your own certificate.

2.12.1 Create Self-signed Certificate

Steps:

1. Go to **Maintenance and Security > Security > Certificate Management**.
2. Click “**Create Self-signed Certificate**” button.
3. Enter the Certificate ID, Public Key Length, Country, Domain/IP, Validity Period and other information. Here, we strongly recommend setting the public key length to **the highest value** supported by the system (2048 in this case).
4. Click "**Save**", and then the self-signed certificate will be successfully created.



Server/Client Certificate

Certificate ID	Valid From:	Valid To:	Status
default	2019-01-01 00:00	2028-12-29 00:00	Normal

CA Certificate

Certificate ID	Valid From:	Valid To:	Status

Certificate Expiration Alarm

Create Self-Signed Certificate

Certificate ID*: test
Public Key Length: 2048
Country*: CN
Domain/IP*: xx.xx.xx.xx
Validity Period*: 200 day(s)
Password: •••••••
Province/State: xx
Locality: xx
Organization: xx
Organizational Unit: xx
Email:

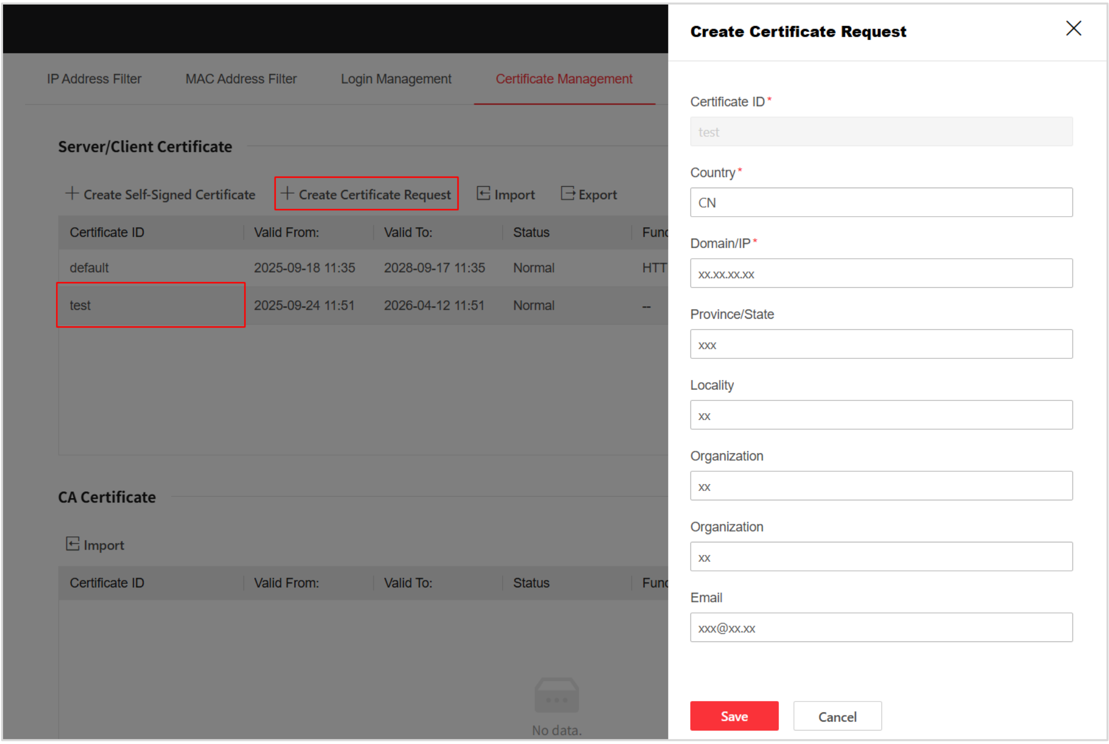
Figure 20 Create Self-signed Certificate

Note: Since the self-signed certificate is not very secure, the browser will recognize it as "certificate prompt", which is normal. If you have higher security requirements, it is recommended to use the third-party CA organization to sign the certificate.

2.12.2 Create CA Certificate

Steps:

1. Select the certificate that you wish to use for CA certification and then click "**Create Certificate Request**" button to create a certificate request.
2. Fill in the required information in the popup window and click "**Save**".



Server/Client Certificate

+ Create Self-Signed Certificate
+ Create Certificate Request
Import
Export

Certificate ID	Valid From:	Valid To:	Status	Func
default	2025-09-18 11:35	2028-09-17 11:35	Normal	HTT
test	2025-09-24 11:51	2026-04-12 11:51	Normal	--

CA Certificate

Certificate ID	Valid From:	Valid To:	Status	Func

Create Certificate Request

Certificate ID *: test

Country *: CN

Domain/IP *: xx.xx.xx.xx

Province/State: xxx

Locality: xx

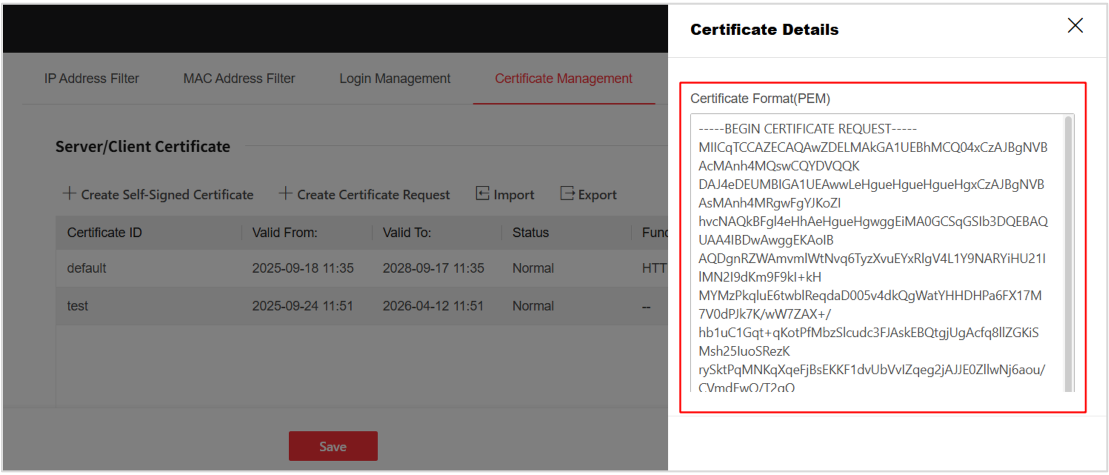
Organization: xx

Organization: xx

Email: xxx@xx.xx

Figure 21 Create Certificate Request

3. Then you will see a Certificate Details page. Copy this PEM-formatted CSR content into a plain text file, then save it with a `.csr` file extension (e.g., `request.csr`).



Server/Client Certificate

+ Create Self-Signed Certificate
+ Create Certificate Request
Import
Export

Certificate ID	Valid From:	Valid To:	Status	Func
default	2025-09-18 11:35	2028-09-17 11:35	Normal	HTT
test	2025-09-24 11:51	2026-04-12 11:51	Normal	--

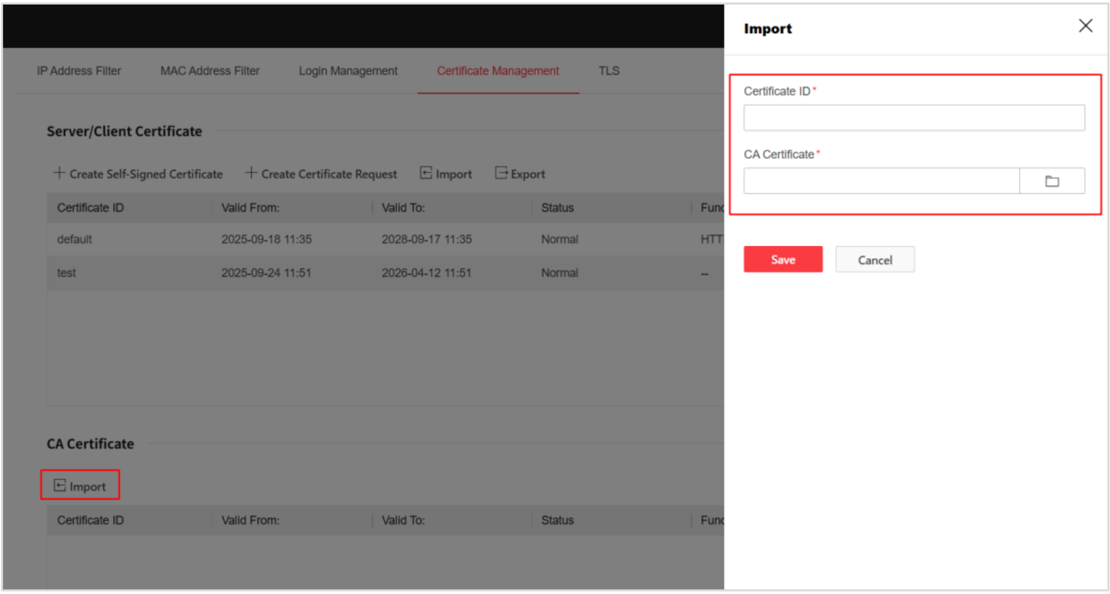
Certificate Details

Certificate Format(PEM)

```
-----BEGIN CERTIFICATE REQUEST-----
MIICqTCCAZECAQAwZDELMAkGA1UEBhMCQ04xCzAJBgNVB
AcMAnh4MQswCQYDVQQK
DAJ4eDEUMBIGA1UEAwwLeHgueHgueHgueHgxCzAJBgNVB
AsMAnh4MRgwFgYJKoZI
hvcNAQkBFgl4eHhAeHgueHgwggEiMA0GCSqGSIb3DQEBAQ
UAA4IBDwAwggEKAoIB
AQDgnRZWAmvmlWtNvq6TyzXvuEYxRlgV4L1Y9NARYiHU21I
lMN2I9dKm9F9kI+kH
MYMzPkqluE6twblReqdaD005v4dkQgWatYHHDHPa6FX17M
7V0dPJk7K/wW7ZAX+/
hb1uC1Gqt+qKotPfMbzSlcudc3FJAskEBQtgjUgAcfq8llZGKiS
Msh25luoSRezK
rySktPqMNKqXqeFjBsEKKF1dvUbVvIZqeg2jAJJE0ZllwNj6aou/
CVmdFwO/T2qO
```

Figure 22 Create Certificate Request

4. Submit the generated CSR file to a third-party certification authority. Once you receive the issued certificate (usually in `.crt` or `.pem` format) from the CA, import it into your device by clicking "**Import**".



Server/Client Certificate

+ Create Self-Signed Certificate
+ Create Certificate Request
Import
Export

Certificate ID	Valid From:	Valid To:	Status	Func
default	2025-09-18 11:35	2028-09-17 11:35	Normal	HTT
test	2025-09-24 11:51	2026-04-12 11:51	Normal	--

CA Certificate

Certificate ID	Valid From:	Valid To:	Status	Func

Import

Certificate ID*

CA Certificate*

Figure 23 Import CA certificate

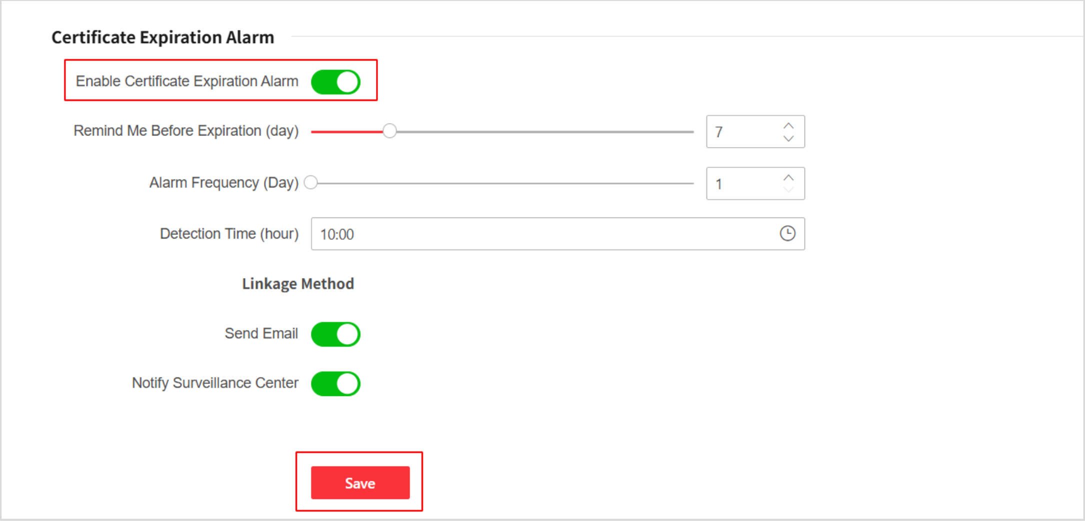
5. Upload the CA certificate you received and click the “**Save**”.

2.13 Certificate Expiration Alarm

Certificates have a validity period. If expired, they may disrupt encrypted communication and authentication processes, thereby creating security vulnerabilities. Hikvision devices support the certificate expiration alarm mechanism, which can alert users in advance to update certificates and avoid service interruptions.

Steps:

1. Go to **Maintenance and Security > Security > Certificate Management**.
2. Turn on the “**Enable Certificate Expiration Alarm**” switch.
3. Set corresponding parameters and choose your preferred notification method.


Certificate Expiration Alarm

Enable Certificate Expiration Alarm: ●

Remind Me Before Expiration (day): 7

Alarm Frequency (Day): 1

Detection Time (hour): 10:00

Linkage Method

Send Email: ●

Notify Surveillance Center: ●

Figure 24 Certificate Expiration Alarm

4. Click "**Save**".

2.14 HTTP(S) Authentication

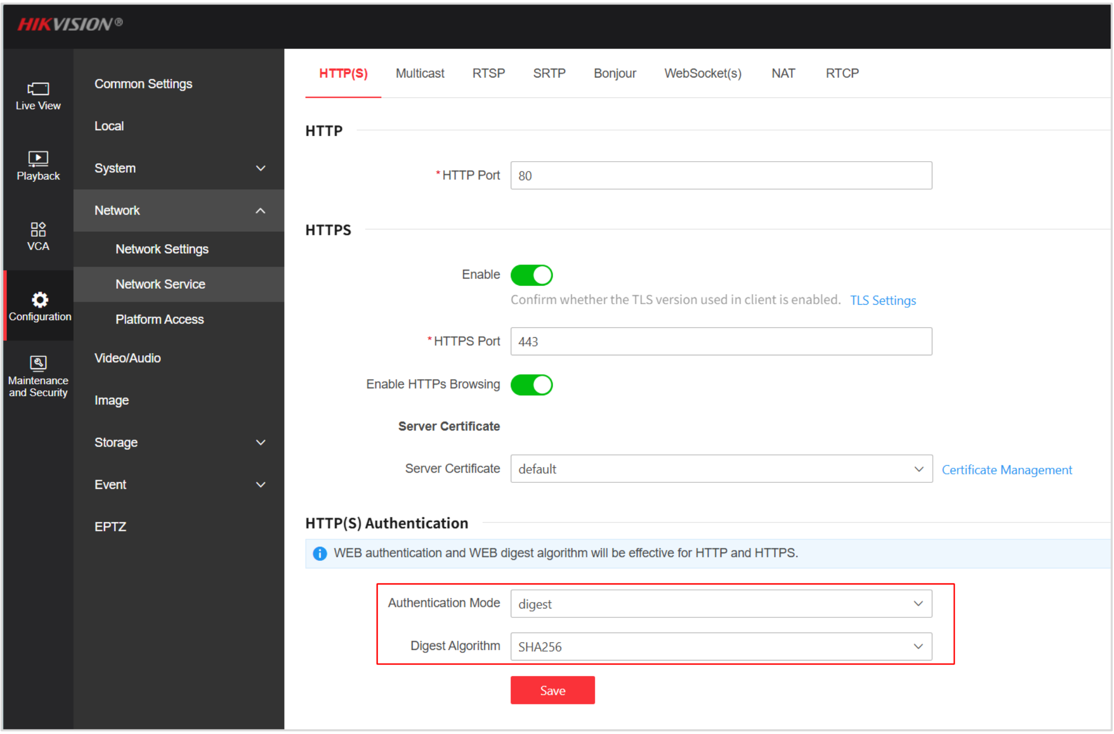
For authentication, Hikvision network devices support:

- Two authentication modes: **digest** and **digest/basic.**
- Three digest algorithm options: **MD5**, **SHA256** and **MD5/SHA256**.

For the highest level of security, we strongly recommend using the **digest** authentication mode with the **SHA256** algorithm.

Steps:

1. Go to **Configuration** > **Network** > **Network Service** > **HTTP(S)**.
2. Select "**digest**" as the authentication mode and "**SHA256**" as the digest algorithm.
3. Click “**Save**” to apply the settings.



HTTP

*HTTP Port 80

HTTPS

Enable

Confirm whether the TLS version used in client is enabled.

*HTTPS Port 443

Enable HTTPs Browsing

Server Certificate

Server Certificate default

HTTP(S) Authentication

WEB authentication and WEB digest algorithm will be effective for HTTP and HTTPS.

Authentication Mode digest

Digest Algorithm SHA256

Figure 25 HTTP(S) Authentication Mode

Note: If you experience connection issues when using SHA256, you may revert to the default settings, which use MD5 as the digest algorithm.

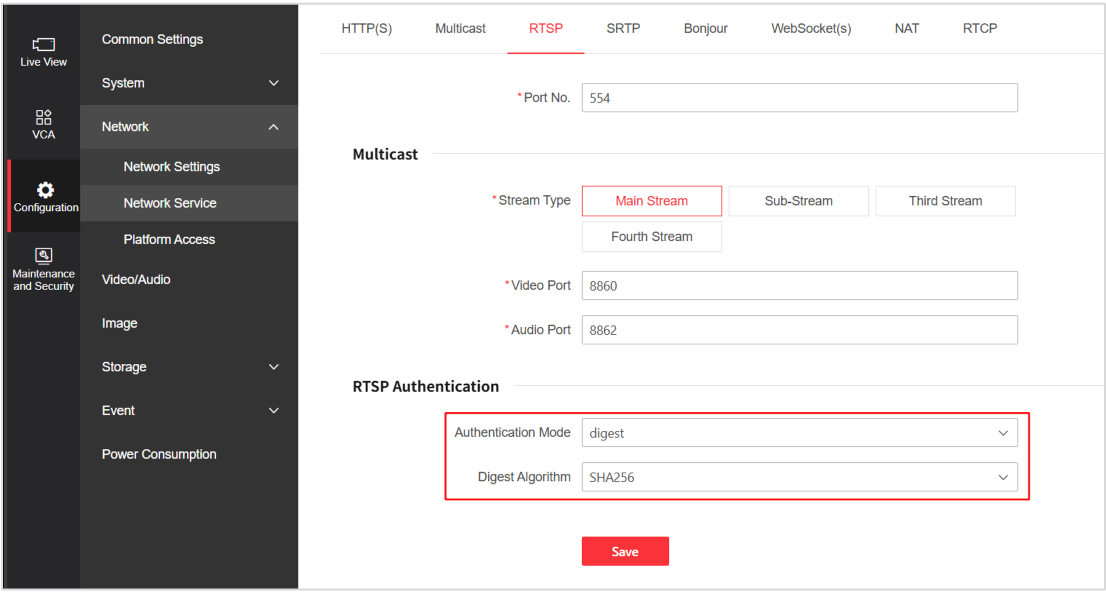
2.15 RTSP Authentication

For the highest level of security, we strongly recommend using the **digest** authentication mode with the **SHA256** algorithm.

Steps:

1. Go to **Configuration > Network > Network Service > RTSP**.
2. Select "**digest**" as the authentication mode and "**SHA256**" as the digest algorithm.

3. Click “**Save**” to apply the settings.



*Port No. 554

Multicast

*Stream Type: Main Stream | Sub-Stream | Third Stream | Fourth Stream

*Video Port 8860

*Audio Port 8862

RTSP Authentication

Authentication Mode: digest

Digest Algorithm: SHA256

Figure 26 RTSP Authentication Mode

Note: If you experience connection issues when using SHA256, you may revert to the default settings, which use MD5 as the digest algorithm.

2.16 ONVIF

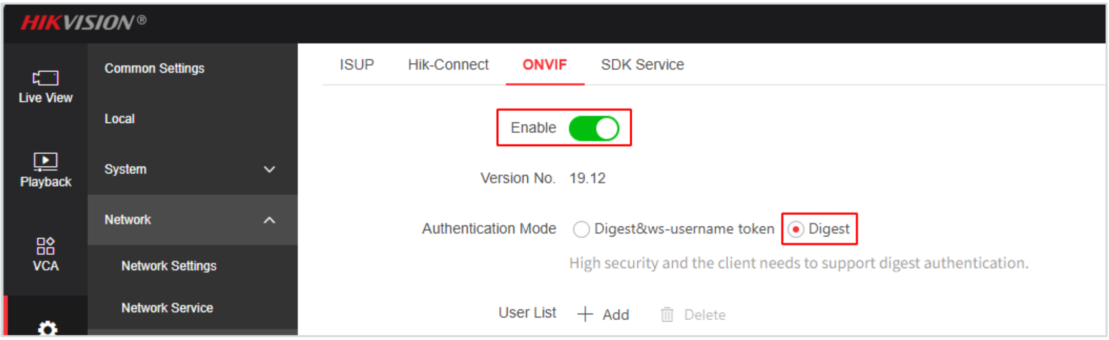
Hikvision network cameras support the ONVIF (Open Network Video Interface Forum) protocol, which enables interoperability between network video devices and third-party video management systems (VMS). This protocol is disabled by default to minimize potential exposure on the network.

Enable ONVIF only if you need to integrate the device with a third-party VMS or software that requires it.

For authentication security, we strongly recommend using **digest** authentication, as it transmits a hashed version of the credentials instead of plain text. This helps prevent interception and replay attacks, especially when used over a secure HTTPS connection. This is more secure than WS-Username Token authentication, which can expose credentials in plain text.

Steps:

1. Go to **Configuration > Network > Platform Access > ONVIF**.
2. Select Digest as the authentication mode.
3. Click “**Save**” to apply the settings.



Enable ●

Version No. 19.12

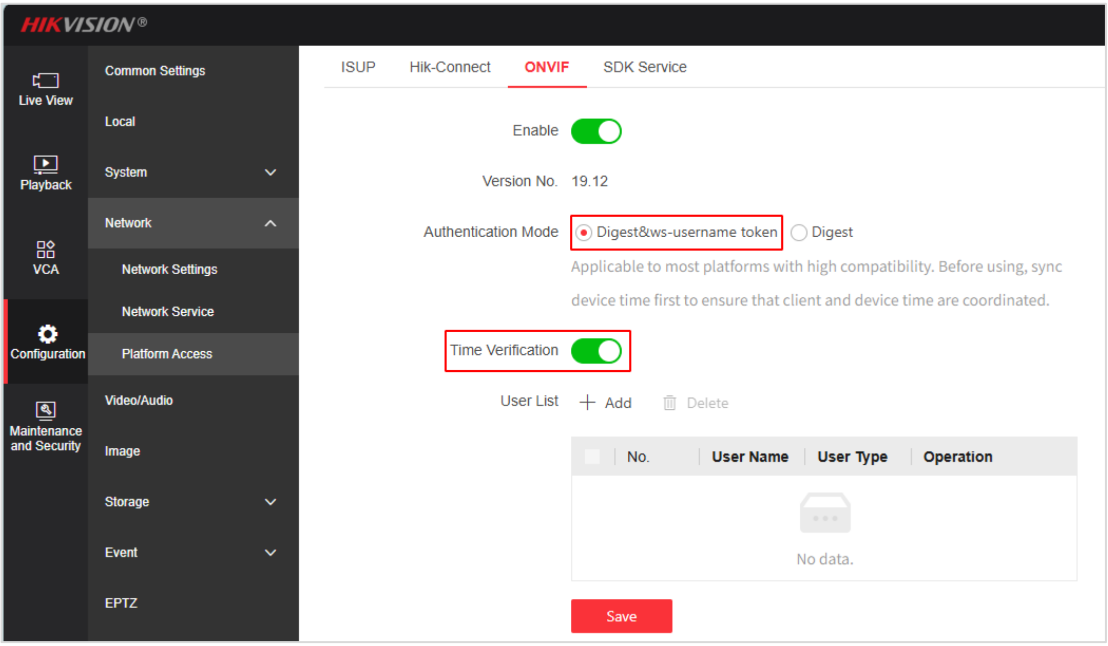
Authentication Mode ○ Digest&ws-username token ● Digest

High security and the client needs to support digest authentication.

User List

Figure 27 ONVIF Configuration

If you select the “digest&ws-username token” authentication mode, be sure to enable the **“Time Verification”** function. This helps prevent replay attacks and enhances security.



Enable ●

Version No. 19.12

Authentication Mode ● Digest&ws-username token ○ Digest

Applicable to most platforms with high compatibility. Before using, sync device time first to ensure that client and device time are coordinated.

Time Verification ●

User List

□	No.	User Name	User Type	Operation
No data.				

Figure 28 ONVIF Configuration

2.17 Enhanced SDK Service and Security Mode

Enabling the SDK service allows the camera to be accessed through client software. For improved security, the Enhanced SDK Service uses the TLS protocol to protect data during transmission. By default, Hikvision network cameras have the Enhanced SDK Service and Security Mode enabled. We strongly recommend using this configuration for optimal security.

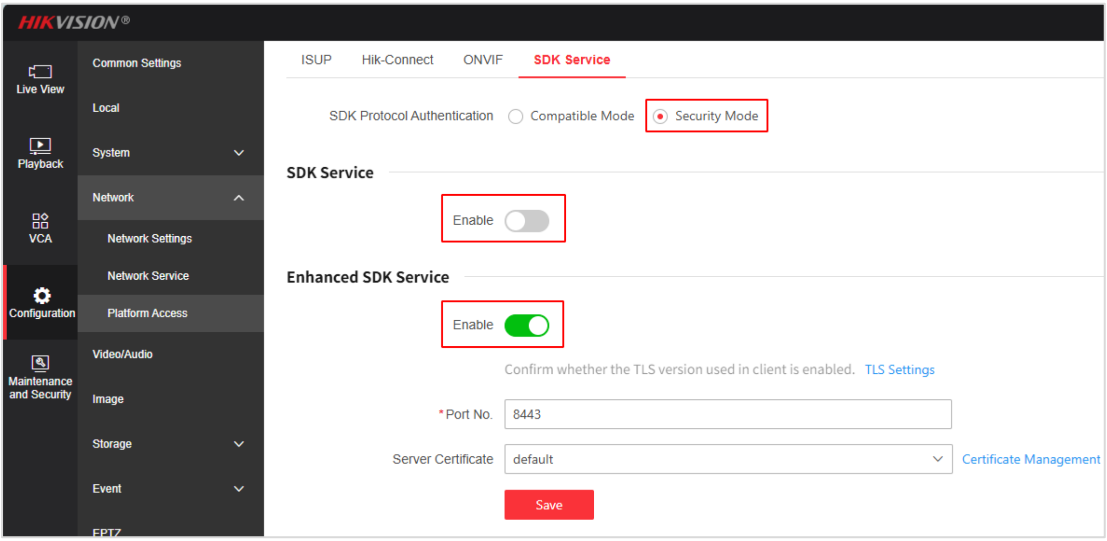
Steps:

1. Go to **Configuration > Network > Platform Access > SDK Service**.
2. Set SDK Protocol Authentication to **Security Mode**.

3. Ensure the **Enhanced SDK Service** is enabled (the switch is **on**). Confirm the port number and select the appropriate server certificate if needed.

4. Ensure the **SDK Service** is disabled (the switch is **off**).

5. Click “**Save**” to apply the settings.



SDK Protocol Authentication ○ Compatible Mode ● Security Mode

SDK Service

Enable ○

Enhanced SDK Service

Enable ●

Confirm whether the TLS version used in client is enabled. TLS Settings

*Port No. 8443

Server Certificate default

Certificate Management

Figure 29 SDK Service Configuration

2.18 TLS Version

Transport Layer Security Protocol (TLS) provides confidentiality and data integrity between communication applications. Hikvision network cameras support TLS 1.1, TLS 1.2 and TLS 1.3, with TLS 1.2 and TLS 1.3 enabled by default.

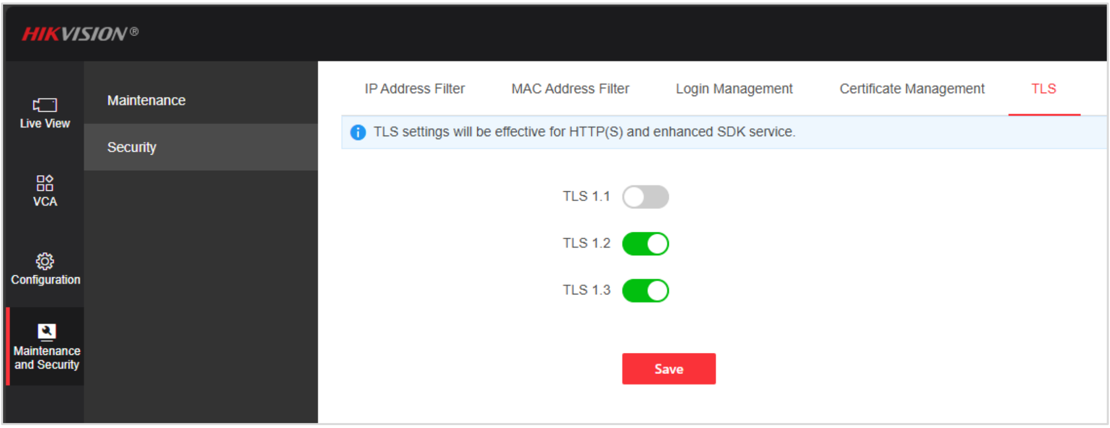
Because TLS 1.1 and earlier versions have known security vulnerabilities (such as the BEAST attack), it is recommended to disable TLS 1.1 and use TLS 1.3 (which offers enhanced security features like forward secrecy) or TLS 1.2 (with strong encryption suites).

Steps:

1. Go to **Maintenance and Security > Security > TLS**.

2. Ensure **TLS 1.2** and **TLS 1.3** are enabled and TLS 1.1 is disabled.

3. Click “**Save**” to apply the settings.



TLS settings will be effective for HTTP(S) and enhanced SDK service.

TLS 1.1 ○

TLS 1.2 ●

TLS 1.3 ●

Figure 30 TLS Version

2.19 Secure Real-time Transport Protocol

Hikvision network cameras support Secure Real-time Transport Protocol (SRTP). If your video management system is compatible, we highly recommend enabling SRTP to replace unencrypted RTP video streaming.

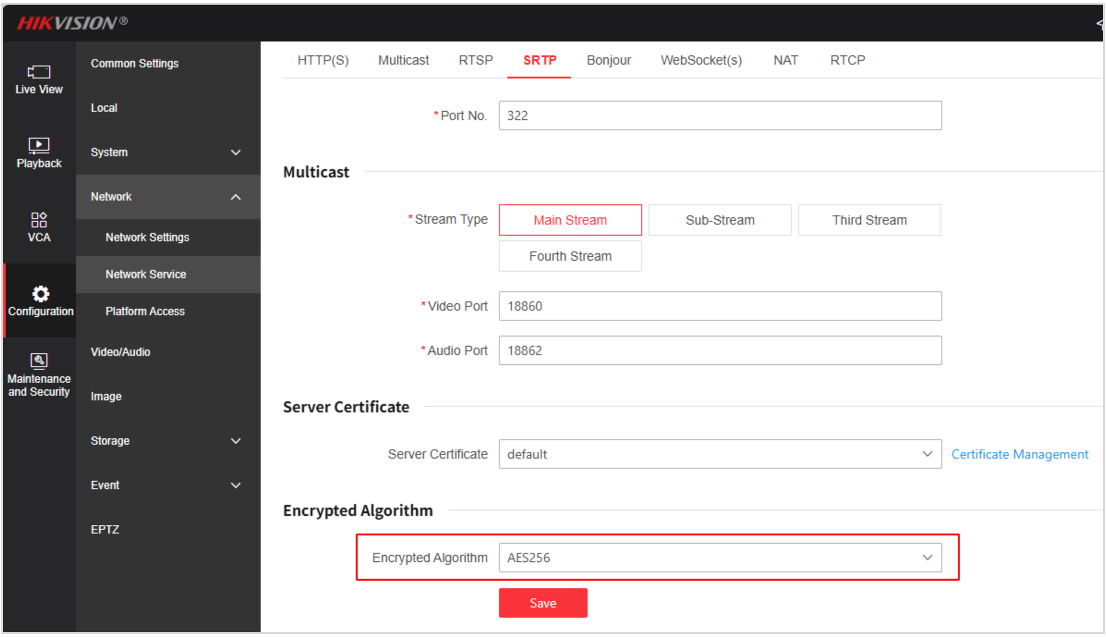
In addition, note that longer encryption keys provide stronger security. By default, the device uses **AES256** for encryption.

Steps:

1. Go to **Configuration > Network > Network Service > SRTP**.

2. Select the appropriate Server Certificate and set encryption algorithm to **AES256**. Regarding the configuration of the certificate, you can refer to the ***Section 2.12***.

3. Click “**Save**” to apply the settings.



*Port No. 322

Multicast

*Stream Type: Main Stream

*Video Port 18860

*Audio Port 18862

Server Certificate

Server Certificate: default

Encrypted Algorithm

Encrypted Algorithm: AES256

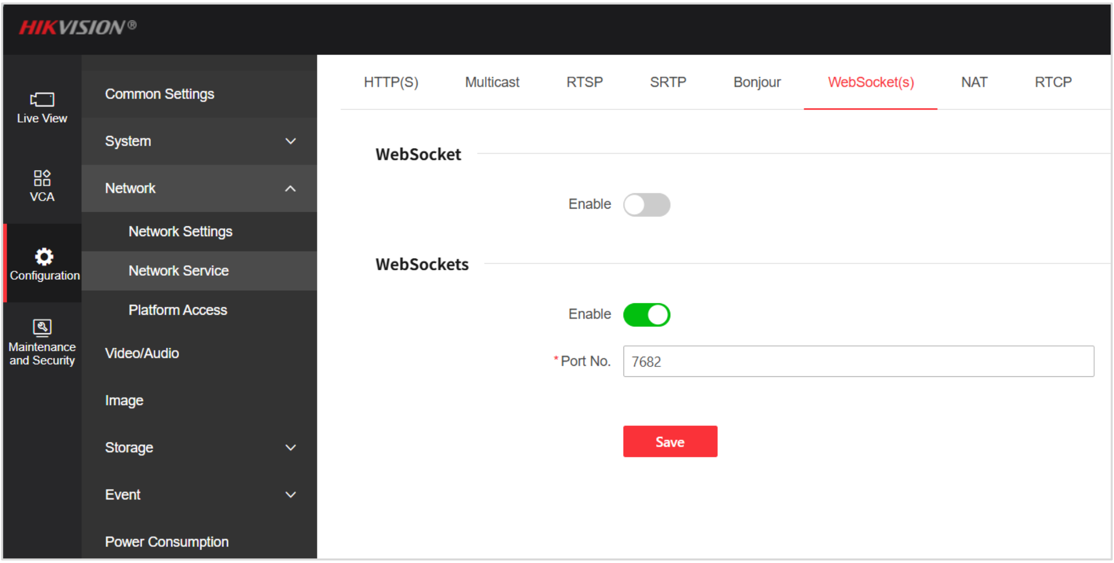
Figure 31 SRTP Configuration

2.20 Enable WebSockets

If the Web Plug-In is not installed, you can enable the WebSocket(s) service so that the camera's video stream can be transmitted over WebSocket(s) and viewed in a web browser. When HTTPS is enabled, enabling the **WebSockets** feature can encrypt the video stream transmitted via WebSockets.

Steps:

1. Go to **Configuration > Network > Network Service > WebSocket(s)**.
2. Enable the **Websockets** function and enter the required port number. At the same time, disable the insecure WebSocket service.



WebSocket

Enable ○

WebSockets

Enable ●

* Port No. 7682

Figure 32 Enable WebSockets

3. Click "**Save**" to apply the settings.

Note: After enabling WebSockets, you must access the device using HTTPS. Otherwise, the live view feature will not work. For example, if your device's IP address is 192.168.1.64, enter `https://192.168.1.64` in your web browser. This ensures that video is transmitted securely and can be viewed properly.

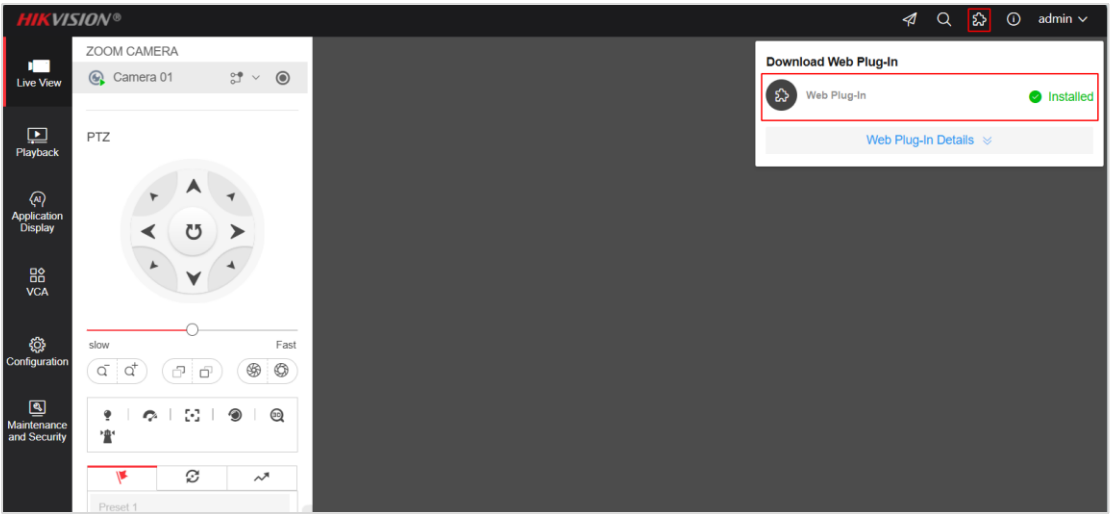
However, when a Web Plug-In is installed, video data is no longer transmitted via the WebSocket(s) protocol. For the configuration of encrypted video transmission in this scenario, please refer to the next section.

2.21 Encrypted Transmission (Plug-In Enabled)

Certain web browsers may restrict the display of the device function (e.g., Live View) and therefore require a plug-in to work. Installing a plug-in can ensure normal display. When a Web Plug-In is installed, video data is no longer transmitted via the WebSockets protocol. In this scenario, setting Protocol Type to **HTTP** can make video stream transmitted via RTP-over-HTTPS, which is an encrypted transport.

Steps:

1. Click the **Plug-In** button at the top of the configuration page to check whether Web Plug-In is installed.



Download Web Plug-In

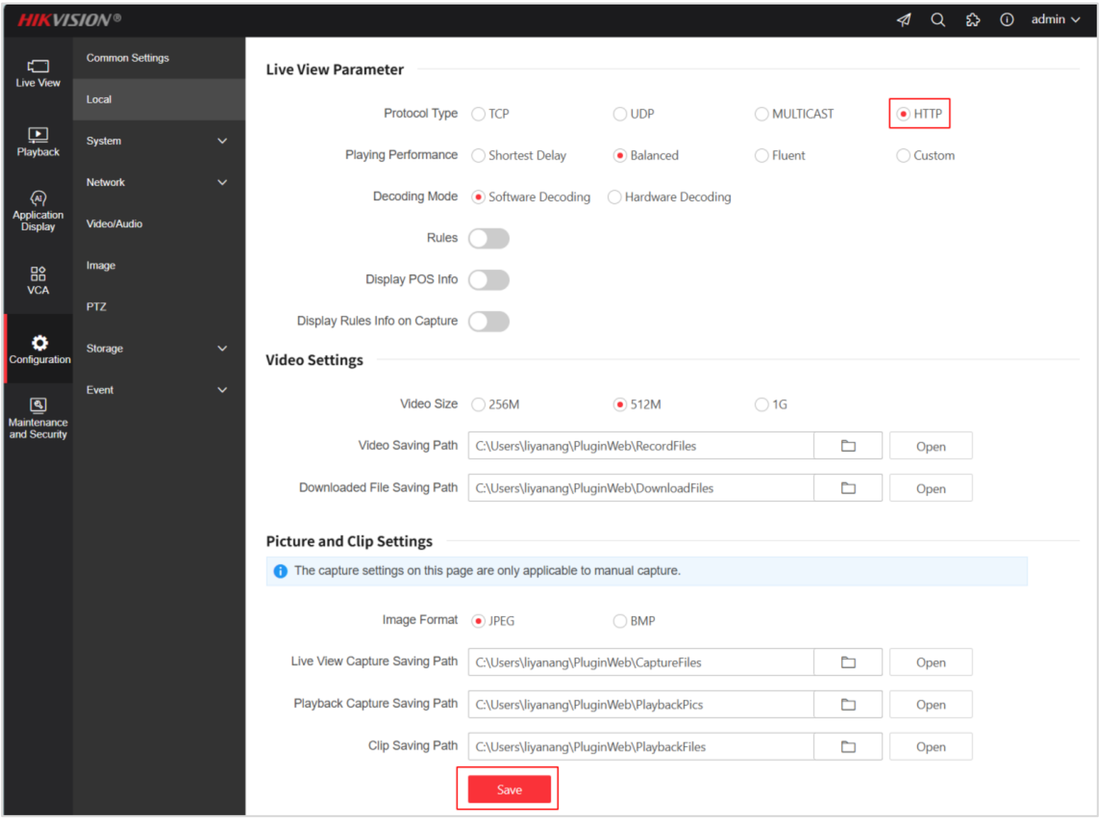
Web Plug-In ● Installed

Web Plug-In Details

Figure 33 Check Plug-In

2. If installed, go to **Configuration > Local**. Set **Protocol Type** to **HTTP**.

3. Click “**Save**” to apply the settings.



Live View Parameter

Protocol Type ○ TCP ○ UDP ○ MULTICAST ● HTTP

Playing Performance ○ Shortest Delay ● Balanced ○ Fluent ○ Custom

Decoding Mode ● Software Decoding ○ Hardware Decoding

Rules

Display POS Info

Display Rules Info on Capture

Video Settings

Video Size ○ 256M ● 512M ○ 1G

Video Saving Path C:\Users\liyanang\PluginWeb\RecordFiles Open

Downloaded File Saving Path C:\Users\liyanang\PluginWeb\DownloadFiles Open

Picture and Clip Settings

The capture settings on this page are only applicable to manual capture.

Image Format ● JPEG ○ BMP

Live View Capture Saving Path C:\Users\liyanang\PluginWeb\CaptureFiles Open

Playback Capture Saving Path C:\Users\liyanang\PluginWeb\PlaybackPics Open

Clip Saving Path C:\Users\liyanang\PluginWeb\PlaybackFiles Open

Save

Figure 34 Set Protocol Type

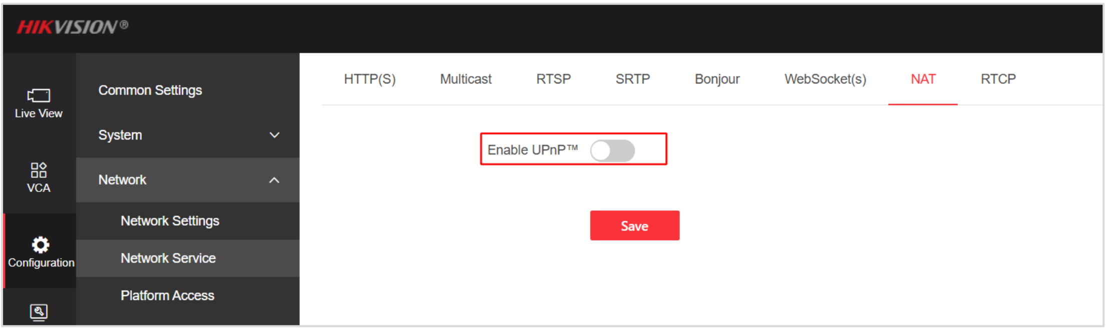
Note: After setting, you must access the device using HTTPS. Otherwise, the video data will not be encrypted. For example, if your device’s IP address is 192.168.1.64, enter https://192.168.1.64 in your web browser.

2.22 Disable UPnP™

Universal Plug and Play (UPnP™) is a networking protocol that enables automatic port forwarding on routers, allowing devices within a local network to seamlessly communicate with external services. This function is disabled by default; if your device does not rely on cloud-based or remote services (e.g., hosted video monitoring), it is recommended to disable UPnP™ to reduce potential security risks.

Steps:

1. Go to **Configuration > Network > Network Service > NAT**.
2. Ensure the "**Enable UPnP™**" switch is in the **off** position.
3. Click "**Save**" to apply the settings.



Enable UPnP™ ○

Figure 35 Disable UPnP™

2.23 Disable SSH

Secure SHell (SSH) is a network protocol that provides secure command-line remote access and device management over unsecured networks.

SSH is disabled by default on Hikvision devices. While SSH can be useful for advanced configuration and troubleshooting, it should remain disabled unless specifically required, as enabling it can increase security risk.

Steps:

1. Go to **Maintenance and Security > Maintenance > Device Debugging > SSH Settings**.
2. Ensure the "**Enable**" switch is in the **off** position.
3. Click "**Save**" to apply the settings.

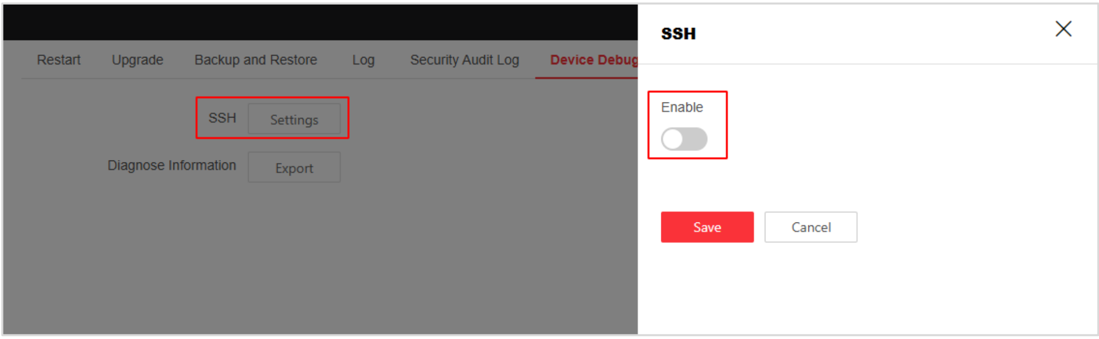


Figure 36 Disable SSH

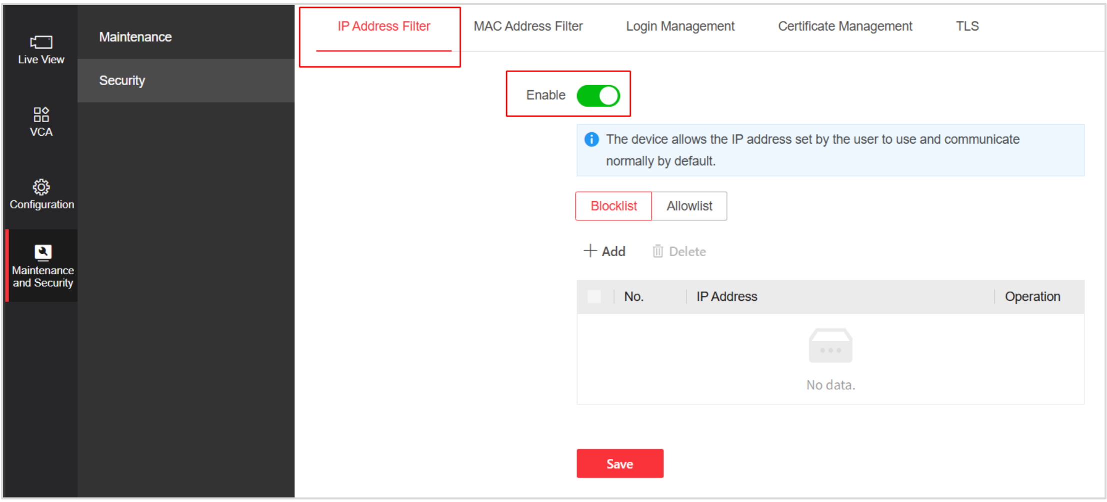
Note: For devices without this configuration interface, SSH is disabled by default.

2.24 Set IP Address Filter

Enabling IP address filtering restricts device access to only authorized users, helping to prevent unauthorized access. If you want to use this function, you can configure it by following steps.

Steps:

1. Go to **Maintenance and Security > Security > IP Address Filter**.



The device allows the IP address set by the user to use and communicate normally by default.

Figure 37 Set IP Address Filter

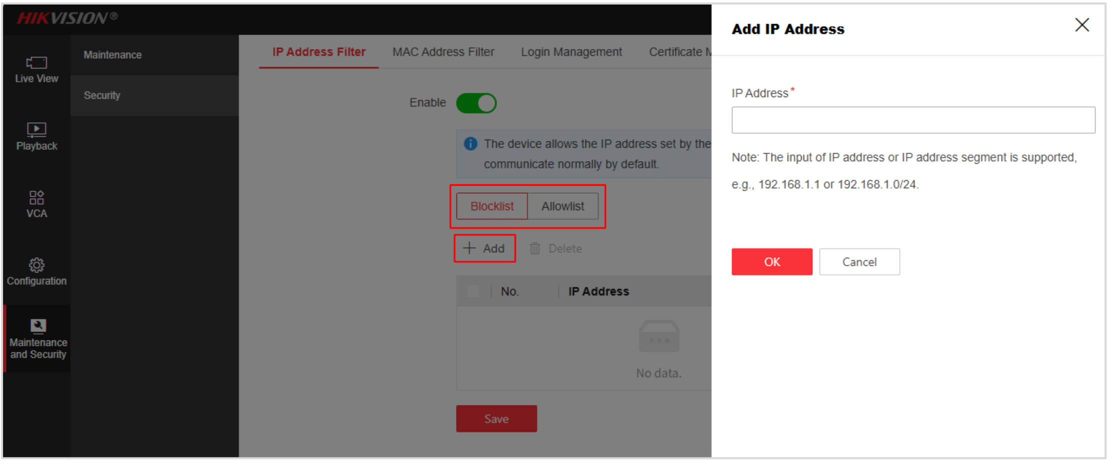
2. Turn on the “**Enable**” switch.

3. Choose the filter type:

- **Blocklist**: IP address on this list cannot access the device.
- **Allowlist**: Only IP addresses on this list can access the device.

Warning: For the “Allowlist” mode, it is critical to add the administrator device’s IP address first! If this is not done, it may cause the administrator to lose access to the device, effectively locking themselves out.

4. Based on your security strategy, select either Blocklist or Allowlist. Click "**Add**", enter the IP address you want to filter in the pop-up window, and click “**OK**”.



The device allows the IP address set by the communicate normally by default.

Note: The input of IP address or IP address segment is supported, e.g., 192.168.1.1 or 192.168.1.0/24.

Figure 38 Set IP Address Filter

5. Click “**Save**” to apply the settings.

2.25 Set MAC Address Filter

MAC address filtering is a network security feature that helps control which devices can connect to your system. By specifying allowed or blocked MAC addresses, you can enhance access control and reduce unauthorized connection. If you want to use this function, you can configure it by following steps.

Steps:

1. Go to **Maintenance and Security > Security > MAC Address Filter**.

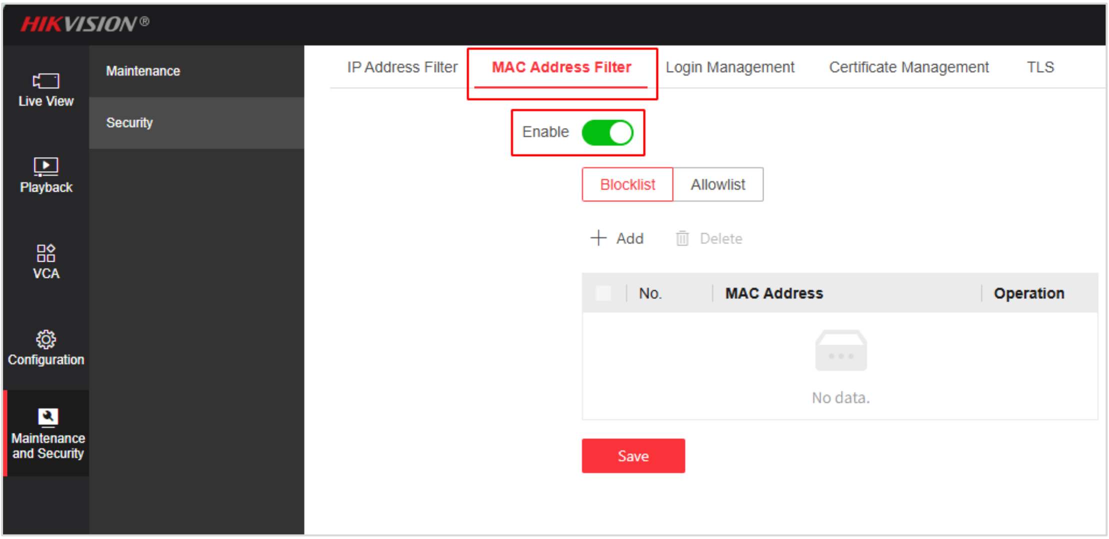


Figure 39 Set Mac Address Filter

2. Turn on the “**Enable**” switch**.**

3. Choose the filter type:

- **Blocklist**: Devices with MAC addresses on this list will be denied access.
- **Allowlist**: Only devices with MAC addresses on this list will be permitted access.

Warning: For the “Allowlist” mode, it is critical to add the administrator device’s MAC address first! If this is not done, it may cause the administrator to lose access to the device, effectively locking themselves out.

4. Based on your filtering strategy, select either Blocklist or Allowlist. Click the “**Add**”, enter the MAC address you want to filter in the pop-up window, and click “**OK**”.

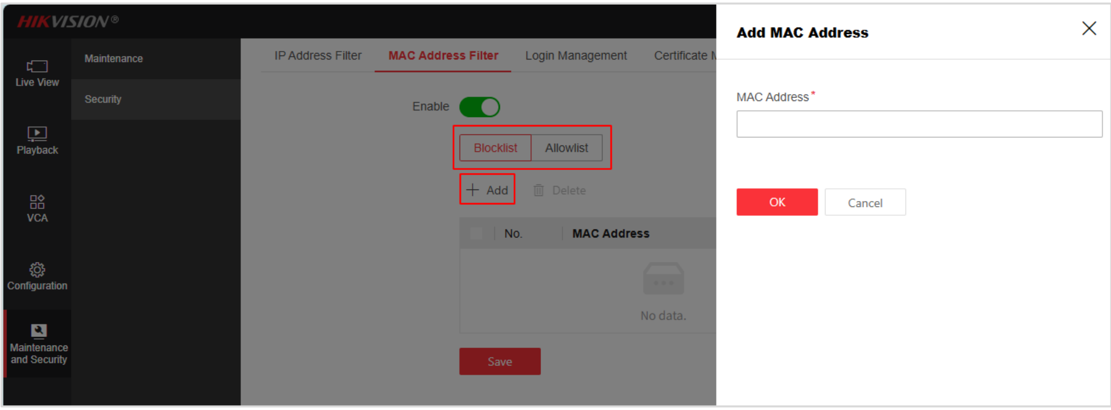


Figure 40 Set Mac Address Filter

5. Click “**Save**” to apply the settings.

Note: The MAC address must be entered in the standard 48-bit format (colon-separated or dash-separated), such as `00:1A:2B:3C:4D:5E` or `00-1A-2B-3C-4D-5F`.

2.26 Account Security Settings

Security Question and Reserved Email are two methods that support you to reset your password when you forget it. These recovery methods can be set up during device activation or configured later through the account settings.

Steps:

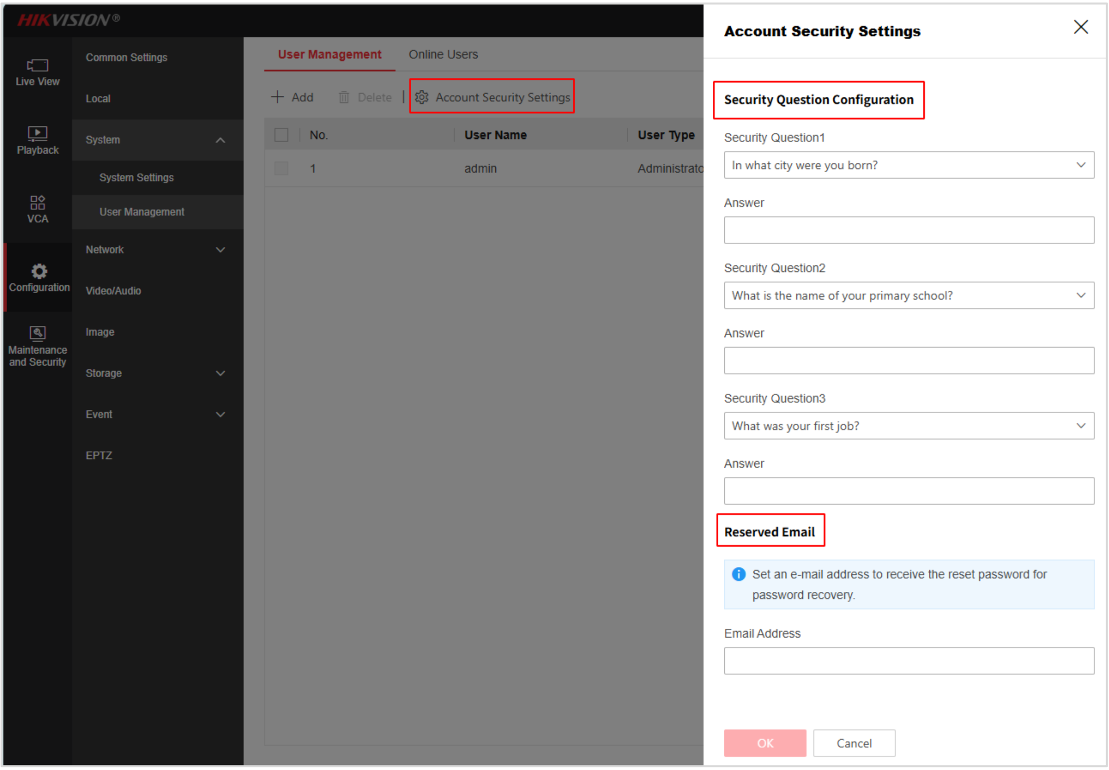
1. Go to **Configuration > System > User Management > User Management**.

2. Select the user account you want to configure, then click “**Account Security Settings**” at the top of the page.

3. Choose the **security questions** and provide corresponding answers. Be sure to remember the answers. It will be required if you use this method to reset your password.

4. Enter a **reserved email address**. This is a pre-designated administrator or system recovery email used for password reset or verification purposes. Do not use a personal or unverified address. This email will be used to receive a verification code during password recovery.

5. Click “**OK**” to save your settings.



Account Security Settings

Security Question Configuration

Security Question1: In what city were you born?

Answer

Security Question2: What is the name of your primary school?

Answer

Security Question3: What was your first job?

Answer

Reserved Email

Set an e-mail address to receive the reset password for password recovery.

Email Address

Figure 41 Account Security Settings

2.27 User Access Control

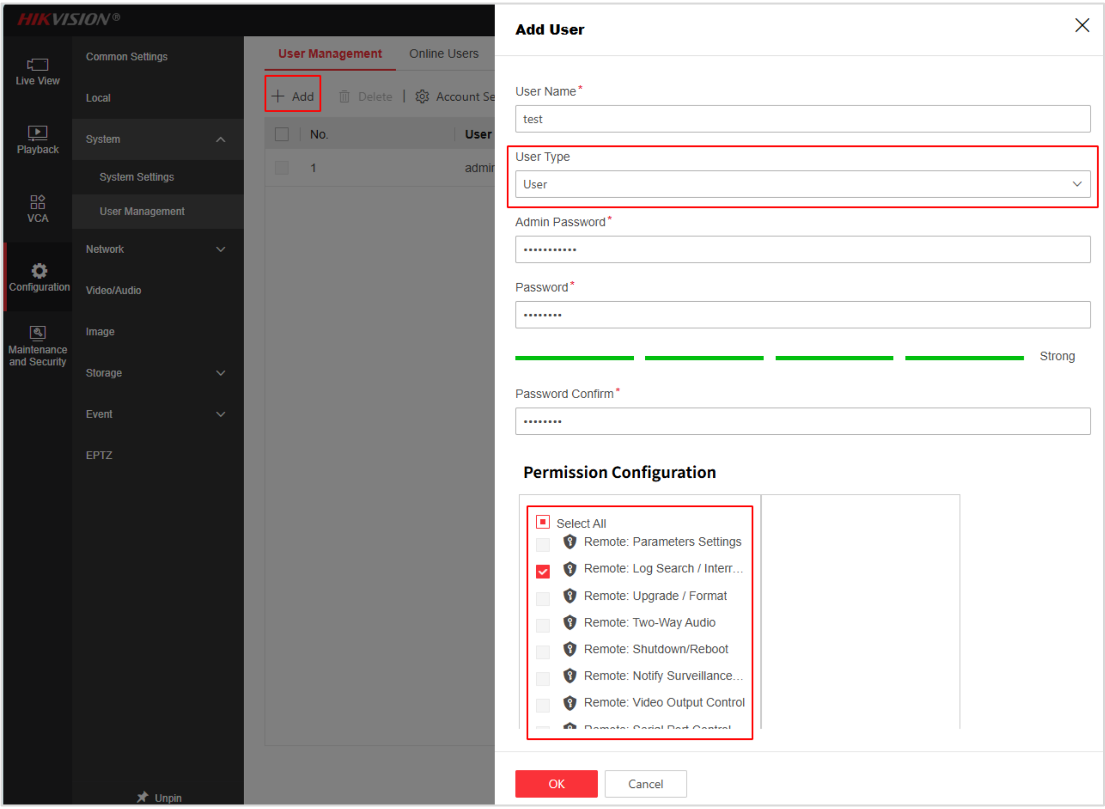
2.27.1 Set Permission Level for Users’ Roles

Hikvision network devices support three user roles: **Admin**, **Operator**, and **User**. The **Admin** account has full control, including the ability to create, modify, or delete other user accounts and assign specific permissions. When adding or editing a user, you can define their permission level to control what actions they are allowed to perform on the device.

It is recommended to assign roles according to the principle of least privilege, granting each user only the access necessary for their responsibilities. Limiting user permissions reduces the risk of unauthorized configuration changes or compromise of critical device settings.

Steps:

1. Go to **Configuration > System > User Management > User Management**.
2. Click “**Add**” to create a new user.
3. Enter the “**User Name**”, select the “**User Type**” and set the “**Password**”.
4. Enable or disable specific permissions based on the access you want to grant.



Add User

User Name*
test

User Type
User

Admin Password*
•••••••••••

Password*
••••••••

Strong

Password Confirm*
••••••••

Permission Configuration

□ Select All
□ Remote: Parameters Settings
☑ Remote: Log Search / Interr...
□ Remote: Upgrade / Format
□ Remote: Two-Way Audio
□ Remote: Shutdown/Reboot
□ Remote: Notify Surveillance...
□ Remote: Video Output Control

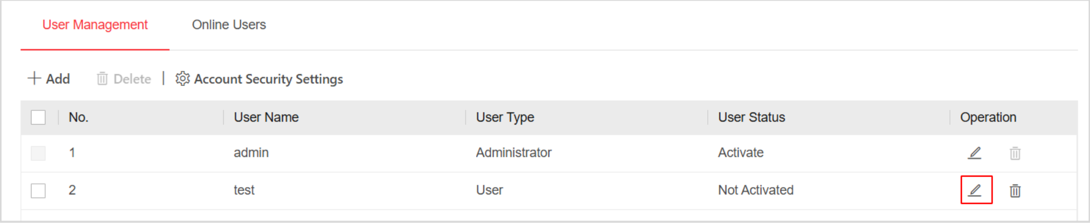
OK Cancel

Figure 42 Add New User

5. Click “**OK**” to save the new user account.

To modify an existing user’s permissions, you can:

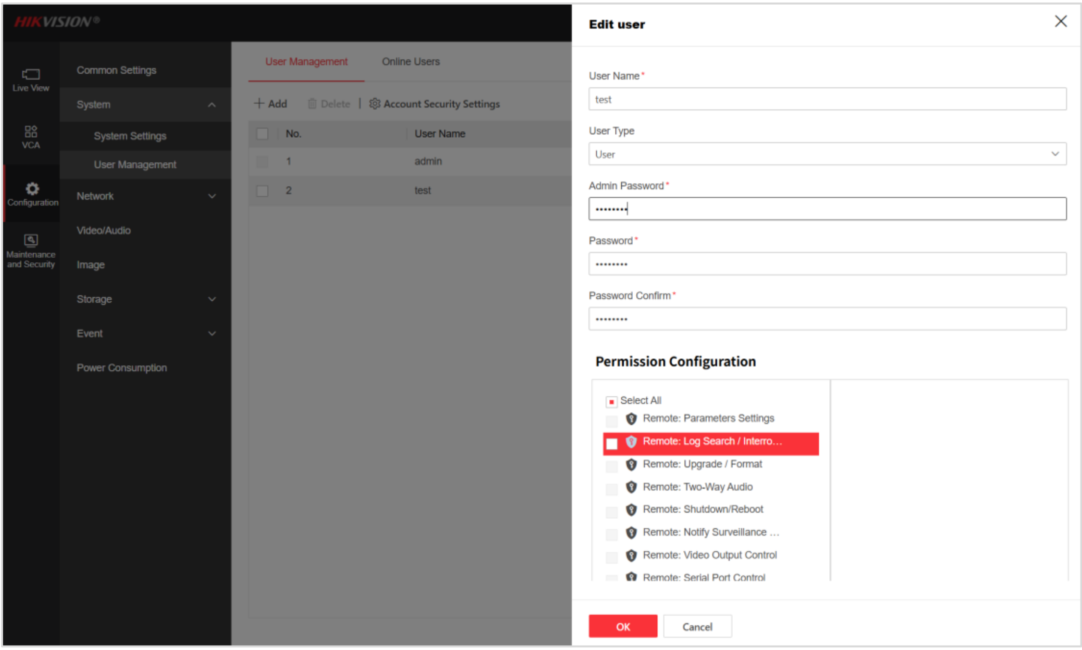
1. Click the **Modify** ✎ icon located behind the corresponding user account.



□	No.	User Name	User Type	User Status	Operation
□	1	admin	Administrator	Activate	✎ 🗑
□	2	test	User	Not Activated	✎ 🗑

Figure 43 Modify user’s permissions

2. Modify the permissions as needed, then click “**OK**” to apply the changes.



User Name*: test

User Type: User

Admin Password*: ••••••••

Password*: ••••••••

Password Confirm*: ••••••••

Figure 44 Modify User’s Permissions

2.27.2 Remove Inactive User Accounts

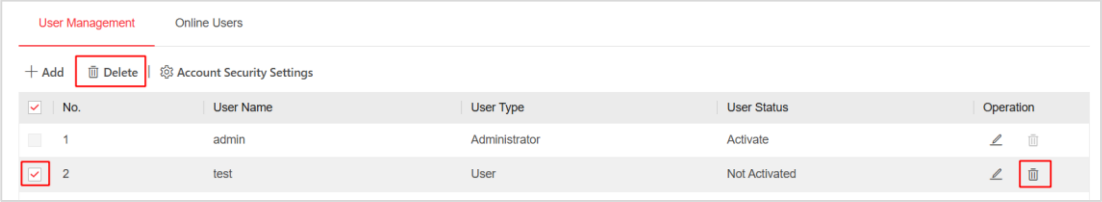
To maintain system security, it is important to regularly remove user accounts that are no longer in use. Inactive accounts can pose a security risk if left unmanaged.

Steps:

1. Locate the user account you wish to remove in **Configuration > System > User Management > User Management**.

2. Select the account and click “**Delete**” button or **Delete** 🗑 icon located behind the corresponding user account.

3. Confirm the deletion to complete the process.



☑	No.	User Name	User Type	User Status	Operation
□	1	admin	Administrator	Activate	✎ 🗑
☑	2	test	User	Not Activated	✎ 🗑

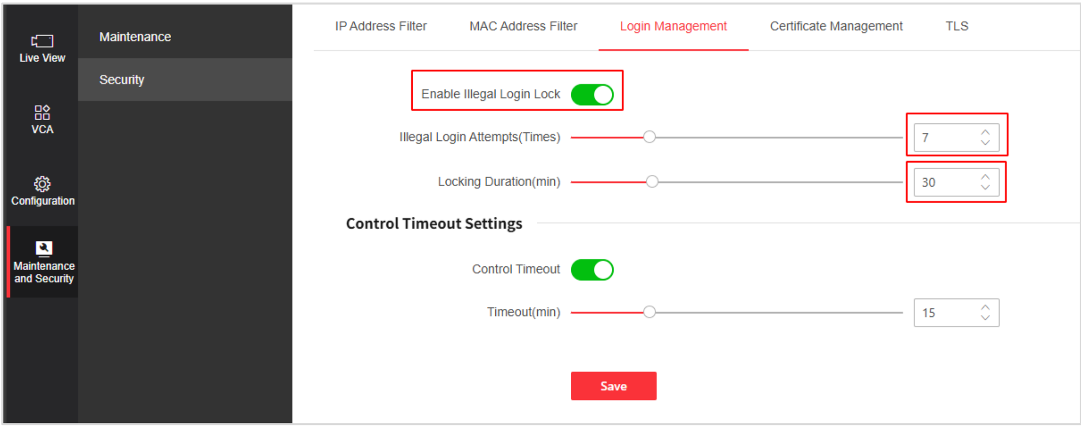
Figure 45 Delete inactive accounts

2.28 Enable Illegal Login Lock

Hikvision network devices include a security feature that automatically blocks an IP address from logging into a specific user account after repeated failed login attempts for that account. This helps protect against brute-force attacks by temporarily locking out suspicious sources. This function is enabled by default.

Steps:

1. Go to **Maintenance and Security > Security > Login Management**.



Enable Illegal Login Lock

Illegal Login Attempts(Times) 7

Locking Duration(min) 30

Control Timeout Settings

Control Timeout

Timeout(min) 15

Figure 46 Lock Illegal Login IP Address

2. Ensure the "**Enable Illegal Login Lock**" switch is **on**.

3. Set the number of allowed failed login attempts and define the lockout duration as needed.

4. Click "**Save**" to apply the settings.

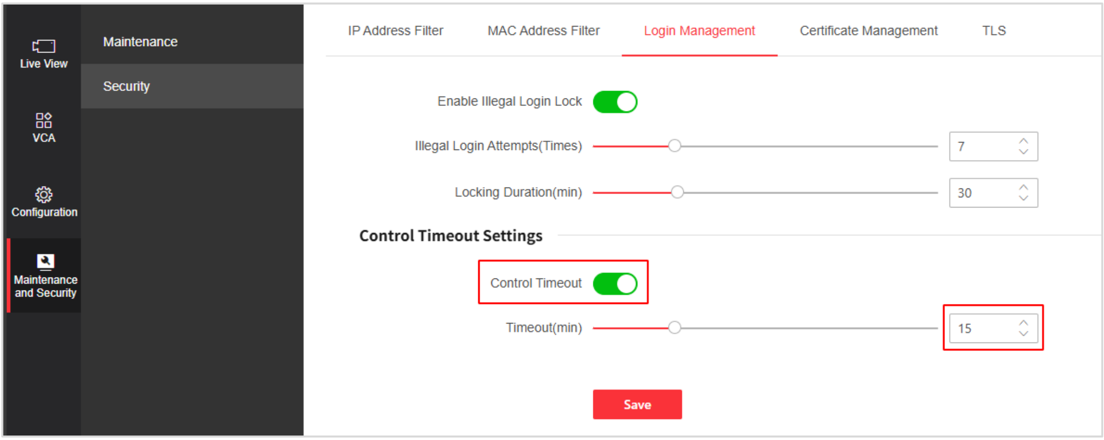
Note: By default, the IP address will be blocked after **7 failed attempts**, and the blocking duration is **30 minutes**. For stronger protection, it is recommended to reduce the number of allowed attempts and increase the lockouts duration.

2.29 Enable Control Timeout Setting

The control timeout feature automatically logs out a user after a period of inactivity, helping to prevent unauthorized access. Once enabled, the system will log out users who have not interacted with the device for a specified duration. By default, this feature is enabled and the system will log out after 15 minutes if no operation is performed. You can also configure the timeout value as needed.

Steps:

1. Go to **Maintenance and Security > Security > Login Management**.



Enable Illegal Login Lock ●

Illegal Login Attempts(Times) 7

Locking Duration(min) 30

Control Timeout Settings

Control Timeout ●

Timeout(min) 15

Save

Figure 47 Control Timeout Settings

2. Ensure the “**Control Timeout**” switch is **on**.

3. Set the desired timeout duration. For enhanced security, shorter timeouts are recommended.

4. Click “**Save**” to apply the changes.

Note: User actively viewing live video or playback will not be logged out automatically.

2.30 Sustaining System Security

Securing network devices is an ongoing process that requires vigilance, regular updates, and adherence to best practices. By following the recommendations and configuration steps outlined in this guide, users can significantly reduce cybersecurity risks and strengthen the overall security posture of their Hikvision network devices.

Remember, every network environment is unique. It is important to assess your organization’s specific requirements and adjust security settings accordingly. Stay informed about the latest security advisories and firmware updates from Hikvision, and review your security configurations periodically to ensure continued protection.

For further information, technical support, or updates to this guide, please visit the official Hikvision website: https://www.hikvision.com.

3 Appendix

A. Set Your PC and Device to the Same LAN

Here we use a Windows 11 PC and a device whose factory IP is 192.168.1.64 as an example. The steps to configure the PC's IP address are as follows.

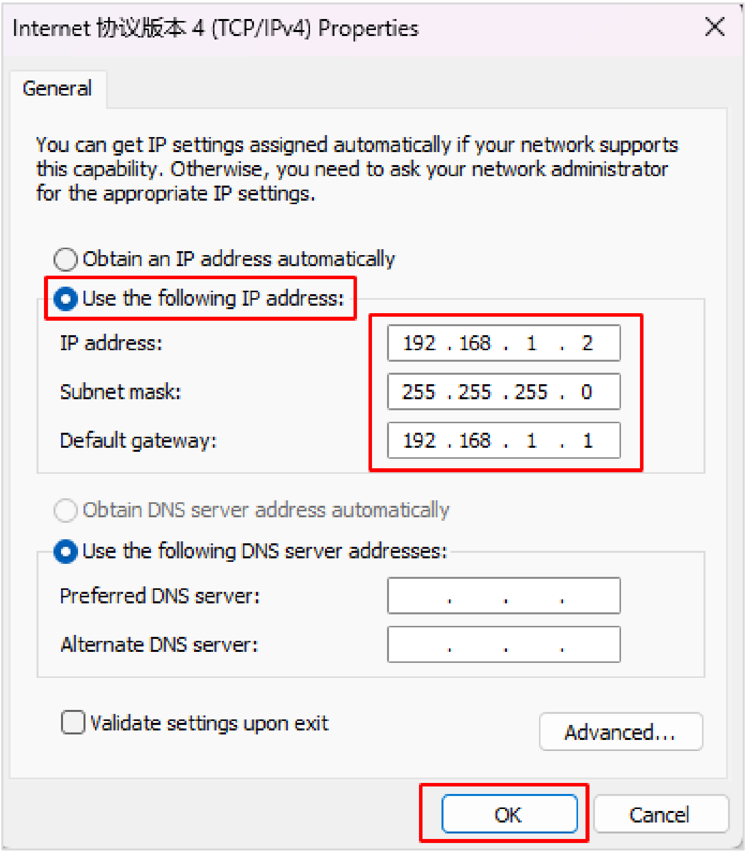
Steps:

1. Connect the device directly to the PC using an network cable and power it on.

2. On your PC, open **Control Panel > Network and Internet > Network and Sharing Center**.

3. Click **Change adapter settings**, locate the network interface that is physically connected to the device – it is normally the **Ethernet** adapter.

4. Right-click that adapter, click **Properties**, then double-click I**nternet Protocol Version 4 (TCP/IPv4)**. Fill in the **IP address**, **Subnet mask** and **Default gateway** fields.



Internet 协议版本 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 48 Internet Protocol Version 4 (TCP/IPv4)

- **IP address:** If device's default IP is 192.168.1.64, set PC's IP to any address from 192.168.1.2 to 192.168.1.253 (excluding 192.168.1.64). Example: 192.168.1.2.
- **Subnet mask:** It is recommended to use the same subnet mask as the device.
- **Default gateway:** This field can be left empty.

5. Click **OK** to apply the settings.

Note: It is recommended that you record the original network settings before making any changes. If you later no longer need this PC to communicate with the device, restore the previous configuration as appropriate; otherwise, the altered settings may interfere with the computer’s normal network connectivity.