

About this Documentation

This document introduces the security functions of Hikvision intrusion alarm host products to users and guides how to use and manage the alarm host securely. Although this document provides a general security overview, users should select appropriate security settings according to actual situations. The method of introducing and configuring the alarm host security functions in this document is based on version 1.3.2 as an example. Alarm host devices of other versions can refer to this document, but you should pay attention to the differences between different versions.

Hikvision reserves the right to update this document. Please visit the company website (<https://www.hikvision.com/en/>) for the latest version.

Copyright Disclaimer

©2026 Hangzhou Hikvision Digital Technology Co., Ltd. ALL RIGHTS RESERVED.

This Documentation shall not be reproduced, translated, modified, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademark Acknowledgement:

海康威视, **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.

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 RIGHTS 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 PREVAIL

Contents

1	Product Introduction	1
1.1	Abstract	1
1.2	Safety Notifications.....	1
1.3	Strong Passwords.....	1
1.4	External Sensors.....	3
2	Default protection	4
2.1	Disable SSH.....	4
2.2	Disable UPnP.....	4
2.3	Enabling HTTPS.....	5
2.4	TLS Version.....	6
2.5	SADP.....	6
3	Basic Hardening	7
3.1	Factory Default Settings.....	7
3.2	Upgrade	8
3.3	OTAP Reset Password	10
3.4	Permission Management.....	11
3.5	IP address filtering	12
3.6	Time Synchronization	13
3.6.1	NTP Time Synchronization	13
3.6.2	Manual Time Calibration.....	14
3.7	Authentication Mode.....	15
3.7.1	HTTP(S) Authentication Mode	15
3.7.2	HTTP-to-HTTPS Redirection	15
3.8	Equipment ISUP security.....	16
3.9	IPC Access Security.....	21
3.9.1	Adding IPC.....	21
3.9.2	Scanning and Adding IPC within the Local Area Network	22
3.9.3	Adding Hikvision IPC based on HTTPS.....	23
3.9.4	Adding Hikvision IPC using the SDKS protocol	24

3.10	Intercom.....	26
3.10.1	SIP over TLS.....	26
3.10.2	SDES-SRTP	26
3.11	User Lock Configuration	27
3.12	Serial Port Authentication Service	28
3.13	REST button	29
3.14	User Password Expiration Reminder	30
3.14.1	Password is permanently valid.....	30
3.14.2	Password customizing is valid.....	31
3.15	User name support modification	33
3.16	Backup	33
3.17	Email upload.....	34
3.17.1	hMailServer.....	34
3.17.2	Outlook.....	39
3.17.3	Test Verification	43
3.18	FTP Upload.....	46
4	Reinforced expansion.....	48
4.1	Wireless IEEE802.1X.....	48
4.1.1	Environment Setup	49
4.2	sys log	50
4.3	Weak Password Management	51
4.4	Certificate Management	51
4.4.1	Certificate Operations.....	52
4.4.2	Certificate Interlock Alarm	54
4.5	Security Management.....	55

1 Product Introduction

1.1 Abstract

Cybersecurity attacks have become a serious threat to network devices and user data. To defend against these threats, Hikvision alarm hosts adopt a security-by-default approach, integrating cybersecurity best practices into each device, while also allowing end users to make cybersecurity configuration changes to reduce risks in their specific environments.

1.2 Safety Notifications

Hikvision is committed to network security research and provides users with industry-leading network security technologies. This security guide will be updated regularly to demonstrate the latest network security best practices to you.

You can access Hikvision Cybersecurity Center for more cybersecurity information: <https://www.hikvision.com/en/support/cybersecurity/>. If you have any feedback regarding Hikvision cybersecurity, please send an email to HSRCC@hikvision.com.

1.3 Strong Passwords

Passwords are a critical component for securing network devices. To prevent unauthorized access to the system, strong and unique passwords must be created, and best practices for password management must be followed. This section provides guidance on setting up and maintaining secure passwords in accordance with international standards.

How to create a strong password?

A strong password is the first critical line of protection. Please follow the best practices below to ensure your password security:

- Use at least 8 characters. Longer passwords or passphrases are more secure because they are harder to guess.
- Must contain at least three of the following character types: digits, uppercase letters, lowercase letters, and special characters.

- Please do not include in your password: your account username, "123", "admin", four consecutive ascending or descending numbers, or four consecutive repeated characters.
- Do not use passwords that are commonly found in password leak lists, such as "lqaz2wsx", "p@ssword", or similar high-risk choices.

The Password Phrase Method:

A password phrase is a memorable and hard-to-guess sentence or phrase. Here are some tips for creating a strong and easy-to-remember password phrase:

- Select a phrase that includes a number.
- Take only the first letter of each word.
- Keep the original case of each letter, consistent with the writing in the phrase.
- Use actual numbers whenever possible. Use "2" instead of "two" or "to", and use "4" instead of "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 above password generation syntax, the generated password is:
"MftNYwla3ita!"

Password security recommendations

- Avoid using dictionary words in any language.
- Do not use consecutive or repeated characters.
- Change passwords regularly.
- Do not let the browser (e.g., Internet Explorer) save passwords.
- Do not enter passwords on untrusted computers.
- Do not share your password or send passwords by email.
- Do not reply to emails requesting personal information. (Hikvision will never request your personal information via email).
- Keep software updated and be cautious with email attachments and links.

1.4 External Sensors

The alarm control panel can connect to various types of detectors. The sensor types are as follows:

1. **Passive Infrared Detector:** Utilizes the characteristics of temperature difference between the human body and the environment and movement, through an infrared lens, to concentrate scattered infrared rays into regions and deliver them to an infrared receiver (without actively emitting infrared rays), achieving alarm functions through signal processing.
2. **Microwave detection:** When microwave signals encounter a moving object and reflect, the Doppler effect occurs, causing a slight frequency shift between the reflected microwave signal and the transmitted signal. At this point, an alarm can be considered to have been triggered.
3. **Active infrared detector:** An active infrared detector works by emitting an infrared beam and setting up a receiver on the opposite side. When a person or object blocks the beam, the receiver detects the change in signal, which triggers an alarm.
4. **Flooding:** High-precision water sensors are used to collect water immersion data. After analysis and judgment by a microprocessor, alarm information is output.
5. **Temperature and humidity sensor:** Uses a high-precision sensor probe to measure temperature and humidity in the air/medium.
6. **Smoke detector:** Achieves fire prevention by detecting smoke concentration and is subject to CCCF fire certification control.
7. **Gas detector:** A detector that responds to the concentration of methane and other flammable gases.
8. **Glass breakage:** By collecting ultra-low-frequency sound waves generated when the glass is struck but not broken and high-frequency sound waves generated after the glass breaks, a determination is made whether glass breakage has occurred.
9. **Door magnet:** Determine whether the door is open by detecting the change in the reed switch status signal through the magnetic attraction structure.
10. **Vibration sensor:** Determines whether to trigger an alarm by collecting signals such as vibrations and displacements generated when an intruder engages in destructive activities.

2 Default protection

Hikvision devices follow the default security principles. Some security functions or alarm host configurations are enabled by default, providing the device with basic security protection and serving as the foundation for other security reinforcement measures.

2.1 Disable SSH

Web interface configuration path: Maintenance and Security > Maintenance > Device Debugging

The SSH protocol is a network protocol used for remote device operation and maintenance. According to the security principle of minimizing the attack surface, SSH should remain disabled when not needed. By default, SSH is **disabled** on Hikvision alarm host devices.

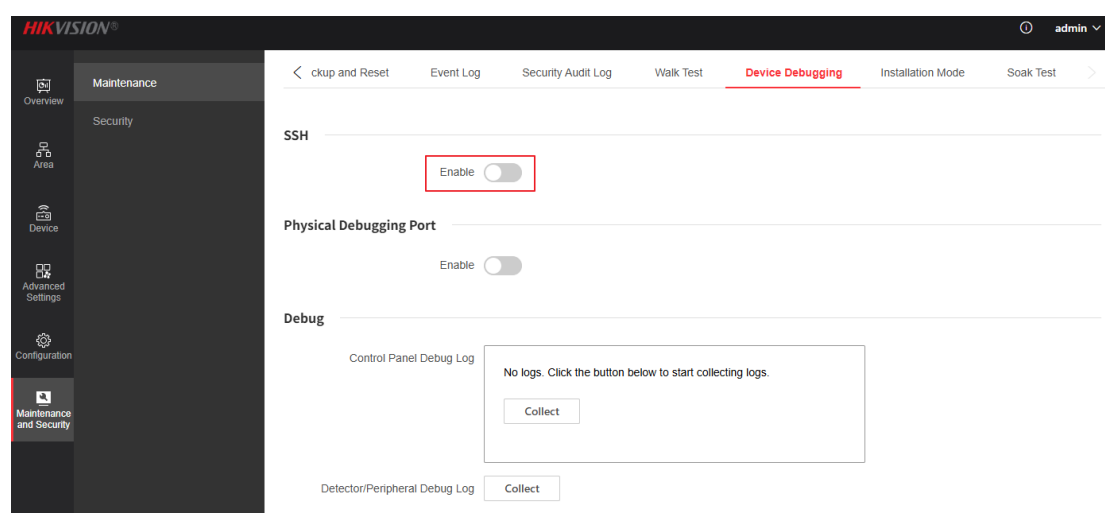


Figure 1 Disable SSH

2.2 Disable UPnP™

Web interface configuration path: Configuration > Network Service > NAT

UPnP™ allows devices to automatically discover other network devices on the network and establish functional network services for data sharing and communication. The UPnP™ feature can be used to quickly connect devices to the wide area network (WAN) through the router, without the need for port mapping. Although UPnP™ provides convenience, it should not be used unless necessary, as it allows any device on the internal network to open ports on the router to communicate outward with the Internet. UPnP™ is

disabled by default. If this feature is not used, ensure that its status is set to off.

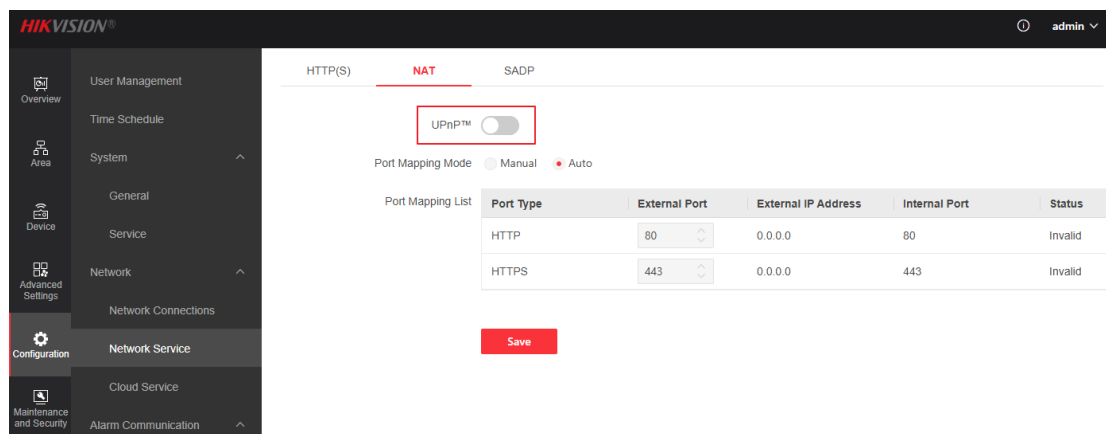


Figure 2 Disable UPnPTM

2.3 Enabling HTTPS

Web interface configuration path: Configuration > Network > Network Service > HTTP(S)

HTTPS is a protocol that adds a TLS/SSL layer on top of HTTP to encrypt communications and ensure the confidentiality of data exchanged between clients and servers. Hikvision alarm host devices have HTTPS **enabled** by default.

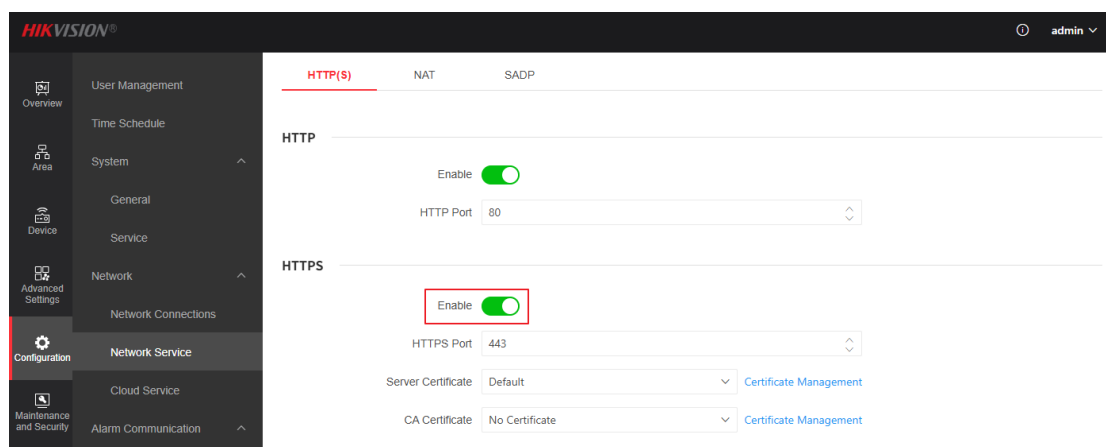


Figure 3 HTTPS Enabled

- HTTP default port: 80;
- HTTP service, enabled by default
- HTTPS default port: 443
- HTTPS service, enabled by default
- HTTP redirection is enabled by default, meaning that entering the device IP address in the browser will redirect to HTTPS
- HTTP and HTTPS services can be closed.

- 1) If your browser has accessed an HTTPS web service, after the HTTPS service is turned off, the browser's default behavior is to open HTTPS. In this case, accessing the web will fail. You need to clear the cache or use incognito mode to access the HTTP web service.
- 2) If you have modified the HTTPS port, similarly, you need to enter `https://{IP}:{new port}` into the address bar to access the HTTPS service (the browser's default behavior is `https://{IP}:443`).
- 3) Turning the HTTP/HTTPS service on/off, changing the HTTP/HTTPS port, or switching certificates will restart the Web service, log out all users, and require re-login for normal access.

2.4 TLS Version

Web interface configuration path: Maintenance and Security > Security > TLS

TLS (Transport Layer Security) is mainly used to provide confidentiality and data integrity between two communicating applications. The protocol is effective for Hikvision alarm host devices' HTTP(S). For the highest level of security and compatibility, it is recommended to disable TLS 1.1 and TLS 1.2 and use **TLS 1.3**. Hikvision alarm hosts have TLS 1.3 enabled by default.

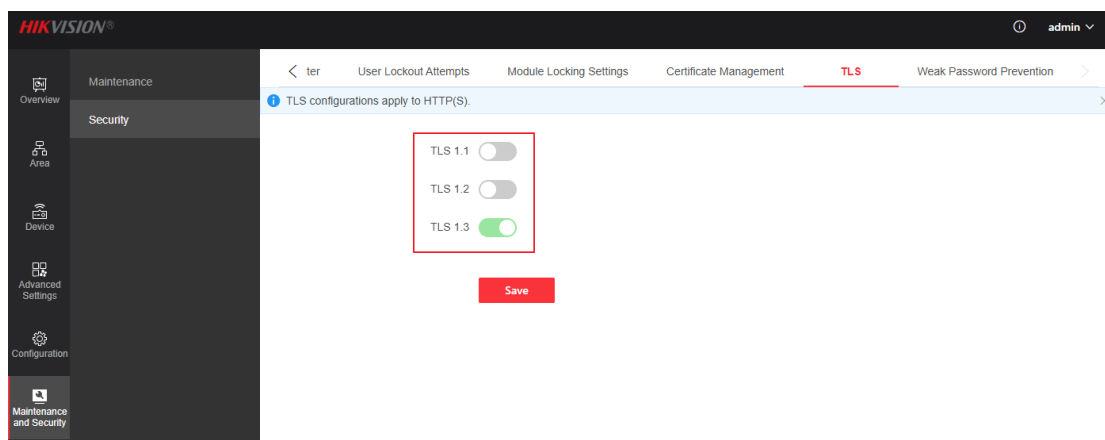


Figure 4 TLS Configuration

2.5 SADP

Web interface configuration path: Configuration > Network > Network Service > SADP

SADP (Search Active Device Protocol) is a protocol for searching Hikvision devices on the same local area network. By default, the SADP function is enabled and supports both protocol versions 3.0 and 3.1.1. Version 3.1.1 is the more secure version. If you want the device to be discoverable but not allow any other operations, you can configure it to Discover Only mode.

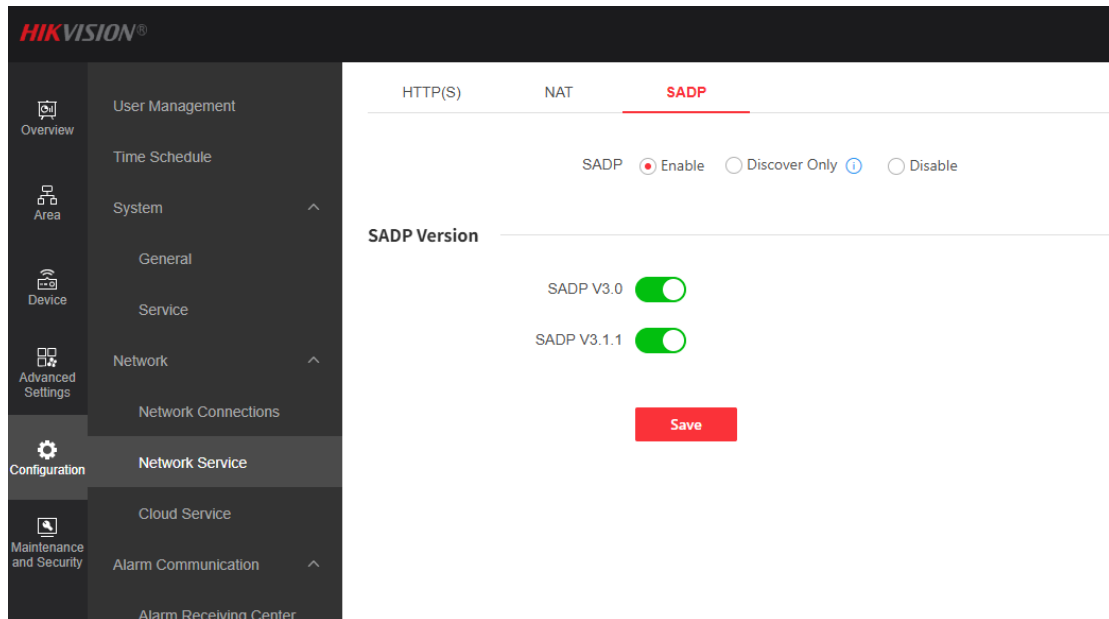


Figure 5 SADP Configuration

3 Basic Hardening

Basic hardenings the minimum recommended level of protection for Hikvision intrusion alarm host. These hardening measures can be directly configured on Hikvision intrusion alarm host without relying on other third-party network infrastructure, platform management systems, devices, or applications.

3.1 Factory Default Settings

Web interface configuration path: Maintenance and Security > Maintenance > Backup and Reset > Reset Options

Resetting the device to factory defaults restores it to a known and clean state, which is crucial for the secure use of the device. Before starting to configure the device, make sure it is in the factory default state. When you need to clear user data or decommission the device, you can reset the device to its original factory state or directly choose to erase all data.

- **Restore Defaults (Reset):** All settings will be cleared except for time zone, user information, Ethernet, WiFi, cloud service, registered detectors, and peripheral parameters.
- **Factory Data Reset (Factory Reset):** All functions and parameters will be restored to factory settings.

- **Erasing all data (Erase):** All data on the device will be permanently erased, and the device will be restarted.

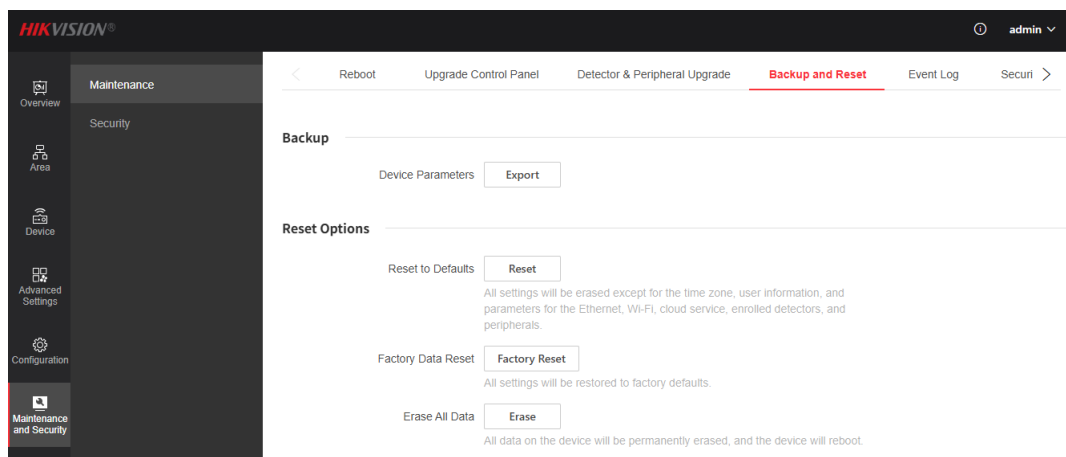


Figure 6 Device Reset

3.2 Upgrade

Web interface configuration path: Maintenance and Security >Maintenance > Upgrade Control Panel and Maintenance and Security >Maintenance > Detector & Peripheral Upgrade

There are two methods to check for updates with the upgrade package: one is manual detection, and the other is automatic detection.

There are two operation buttons for manual detection of updates, one on the host upgrade interface and the other on the child device upgrade interface. The functions of the two operation buttons are the same, and they will both perform a real-time query of the latest version of the host and all child devices, and refresh the query results in real time.

The auto-detection update configuration has two switches, one in the host upgrade interface and the other in the child device upgrade interface, both of which are closed by default. The functions of the two switches are the same. When auto-detection update is enabled, it will immediately check the latest version of the host and all sub-devices once, and then automatically check the latest version every 24 hours. Re-entering this interface or manually refreshing this interface will refresh the query results.

Upgrade is allowed only after the query list displays upgradeable information.

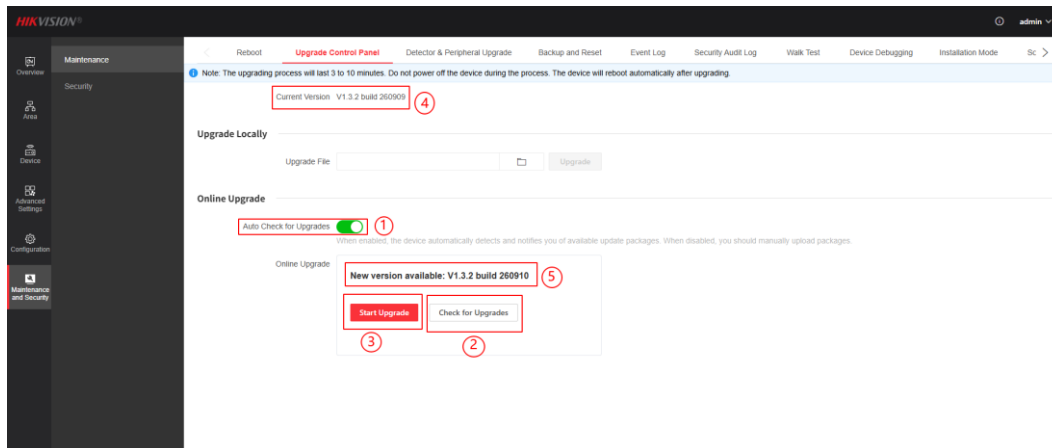


Figure 7 Host upgrade

Labeling instructions:

- 1: Automatic update detection switch
- 2: Manual check for update button
- 3: Upgrade button
- 4: Current Version
- 5: Upgradable to the latest version

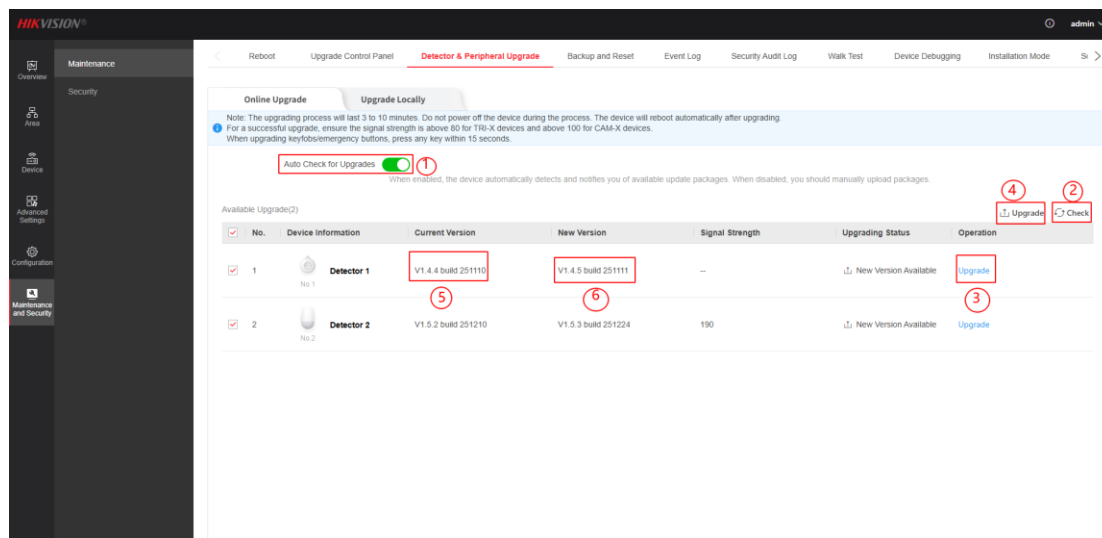


Figure 8 Child device upgrade

Labeling instructions:

- 1: Automatic update detection switch
- 2: Manual check for update button
- 3: Upgrade button
- 4: Batch Upgrade Button
- 5: Current Version
- 6: Upgradable to the latest version

3.3 OTAP Reset Password

Password reset requires the use of Sdp. Before enabling "Find Only" mode, password reset follows the Sdp protocol. After switching to "Find Only" mode, Sdp resets the password using the Otap protocol.

Step 1: Switch SADP to discovery mode only via the web

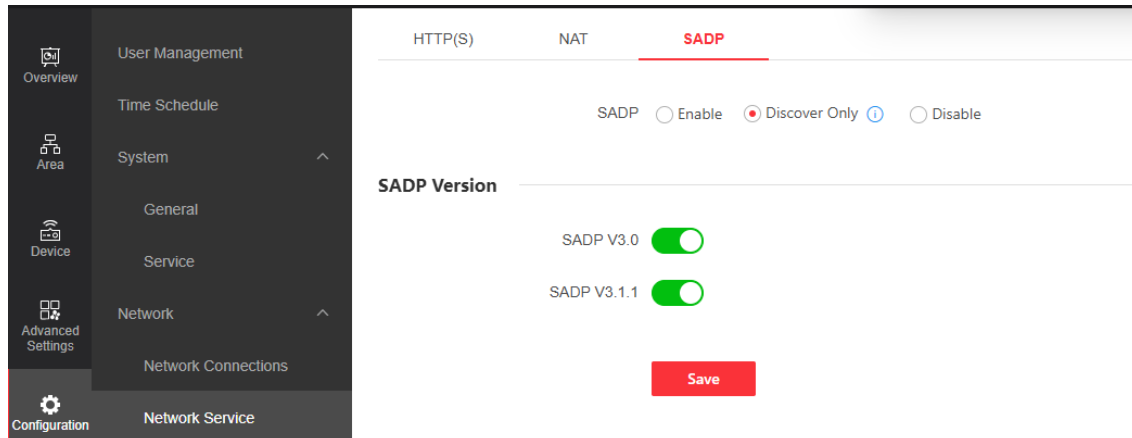


Figure 9 SADP

Step2: Open the sadp demo

1. Scanning device
2. Selected device
- 3&4. Export the device code, the C:\QrCodes\DeviceKey.xml file, to Hikvision technical service, Hikvision technical service will go to the device password reset website to obtain the reset code (8-digit string)
5. Enter a new password and reset code

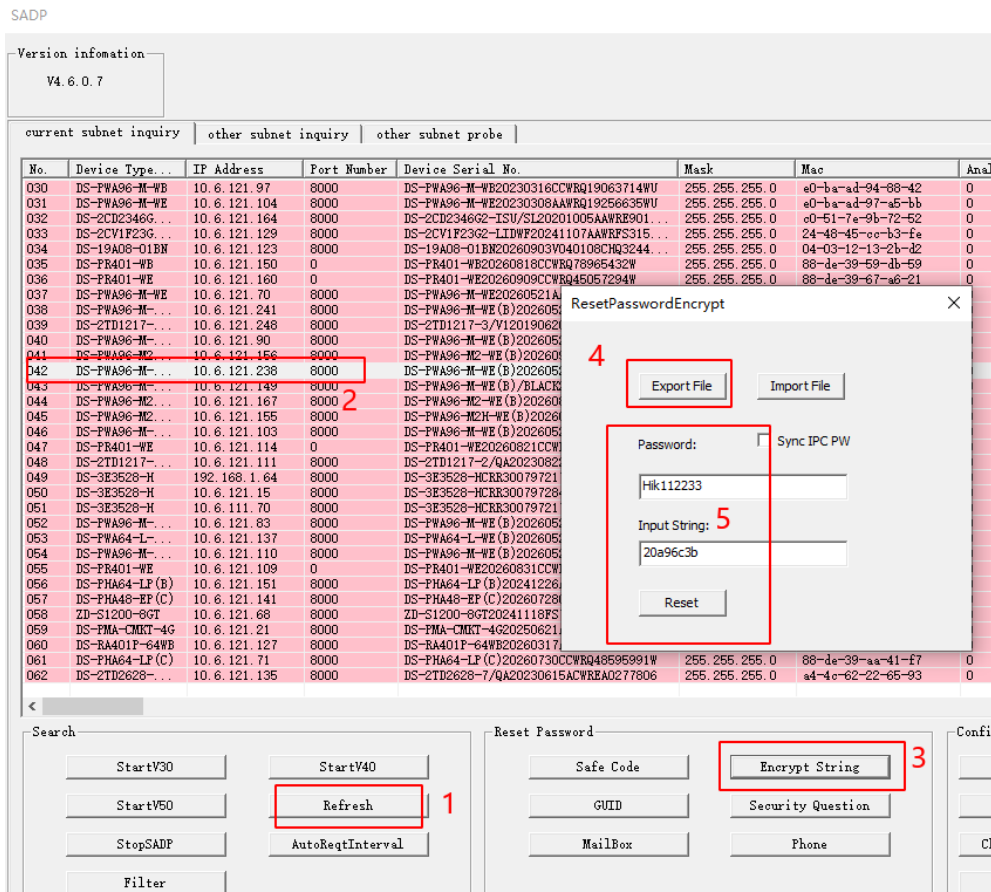


Figure 10 SADP Demo

3.4 Permission Management

Web interface configuration path: Configuration > User Management > User Management

Hikvision alarm host supports permission configuration functions, allowing you to determine whether users can access the corresponding resource objects.

Based on the permissions assigned to the user, Hikvision alarm host supports three levels of users: Cloud Administrator, Cloud Installer, and (Cloud, Local) Operator. Cloud Administrators and Cloud Installers can add, edit, or delete others, and assign permissions to different users.

To add a new user, go to the user management interface and click "Add." In the pop-up "Add User" interface, the administrator can assign permissions to the new user. For existing users, the administrator can find the user in the user management interface, click the edit icon to the right of the username, and then edit their permissions. We strongly recommend assigning permissions based on business relevance and the principle of least privilege, as this maximizes security.

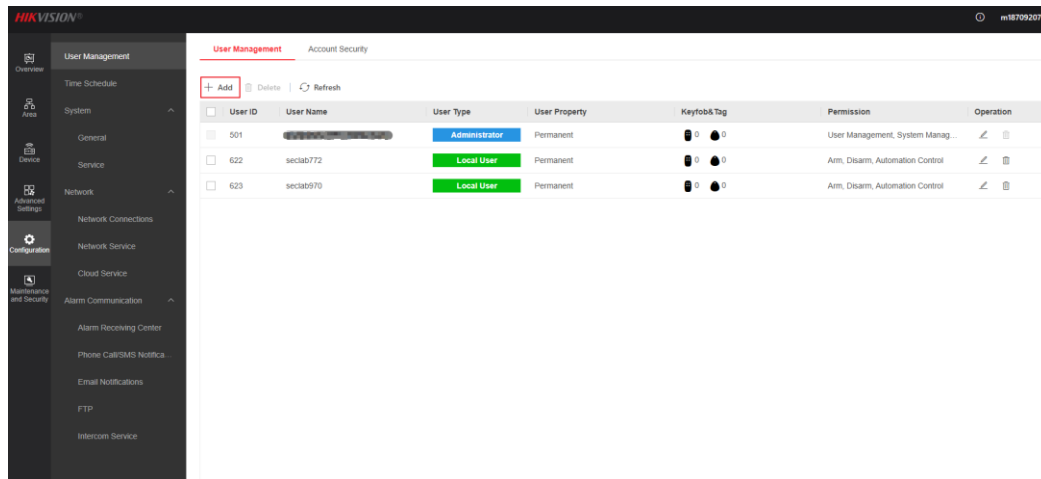


Figure 11 Add User

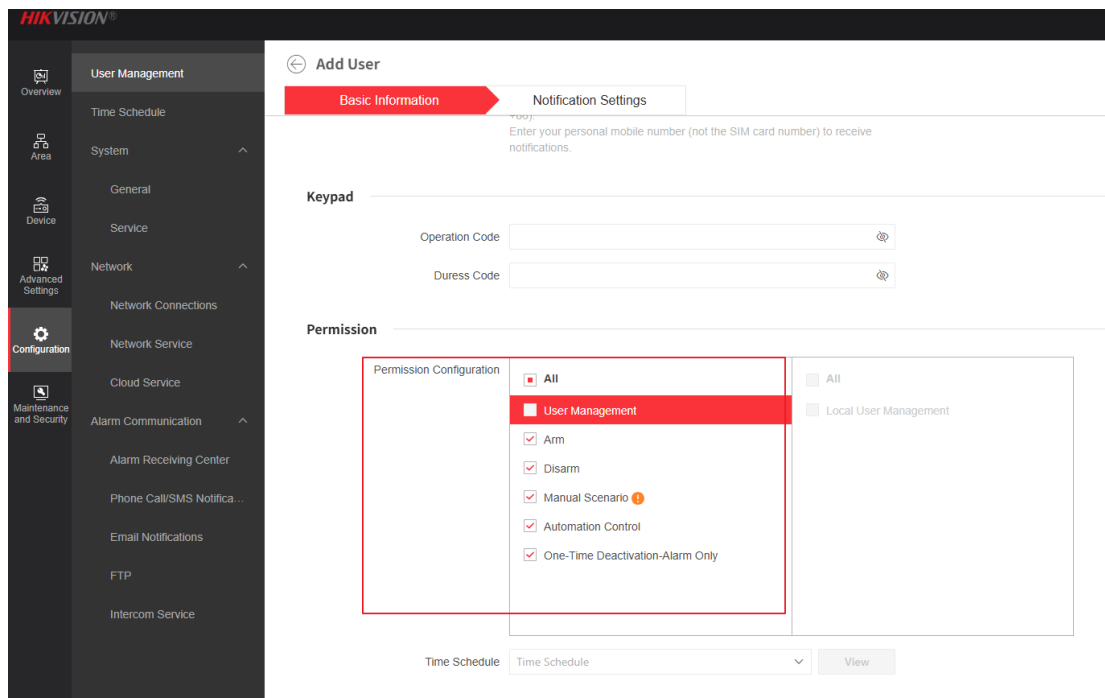


Figure 12 User Permission

3.5 IP address filtering

Web interface configuration path: Maintenance and Security > Security > IP Address Filter

IP address filtering is an access control measure that can prevent unauthorized system access to the alarm host device. After enabling this function, you can allow or prohibit specific IP addresses from accessing the device according to your actual needs.

Configuration steps: Enter the IP address filtering settings interface, click the "Enable" button to activate this function, and select the filtering method: blacklist or whitelist

- **Blocklist:** All IP addresses in the list cannot access the alarm host
- **Allowlist:** Only IP addresses in the list can access the alarm host; all other addresses are strictly denied

Warning: When using the "Allowlist" mode, you must first add the administrator's IP address. Otherwise, it may result in the administrator being unable to access the device and being locked out by their own security policies. When using the "Blocklist" mode, it is forbidden to add the administrator's IP to the list and save it.

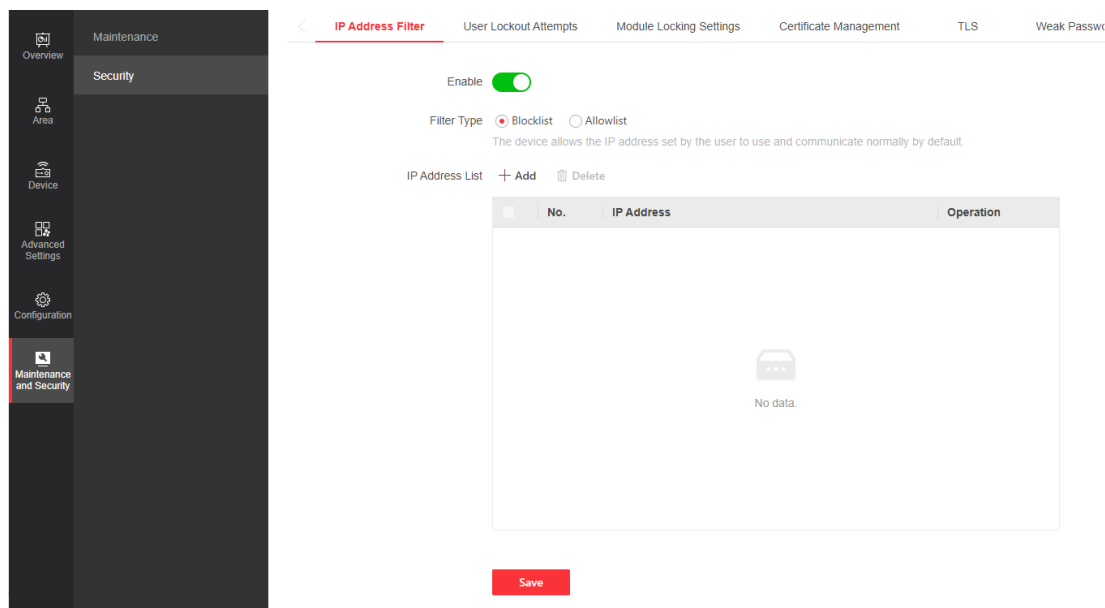


Figure 13 IP Address Filter

Note: This control measure works best in network environments where devices are assigned static IP addresses.

3.6 Time Synchronization

Web interface configuration path: Configuration > System > General > Time Settings

From a security perspective, setting the correct date and time is critical for alarms and logging. The device time can be set through NTP synchronization or manually adjusted.

Before configuring, ensure that all time calibration sources (if configured) are consistent and accurate.

3.6.1 NTP Time Synchronization

To achieve accurate and reliable time synchronization, you can use an NTP server. Before configuring NTP time synchronization, you need to obtain NTP server information or set up an NTP server in your network. If your alarm host can access the Internet, you can use a public NTP server. You can search for an NTP server that is geographically close

to you using a search engine.

Access the time settings interface, select the appropriate time zone, and then select **"NTP"**. Enter the server IP address (i.e., the IP address or domain name of the NTP server), NTP port, and synchronization interval, and you can also select the date and time format. After completing the selection, click **"Save"**

The screenshot shows the HIKVISION web interface with the 'Time Settings' tab selected. The left sidebar contains navigation options: Overview, Area, Device, Advanced Settings, Configuration (highlighted), Maintenance and Security. The main content area has three tabs: Basic Information, Time Settings (active), and Control Panel Options. Under 'Time Settings', the 'Device Time' is 09/10/2026 16:12:59. The 'Time Zone' is set to '(GMT+00:00) Dublin, Edinburgh, London'. The 'Time Synchronization Mode' is set to 'NTP' (radio button selected). The 'Server Address' is 'time.windows.com', the 'NTP Port' is '123', and the 'Interval' is '60' minutes. The 'Date Format' is 'MM/dd/yyyy hh:mm:ss'. A 'DST' section at the bottom has a 'DST' toggle switch. A red 'Save' button is at the bottom right.

Figure 14 NTP Time Synchronization

3.6.2 Manual Time Calibration

Enter the time settings interface, select the appropriate time zone, and then select **"Manual."** You can manually set the date and time, or click **"Sync. with computer time"** to synchronize with the local computer time. After completing the selection, click **"Save."**

The screenshot shows the HIKVISION web interface with the 'Time Settings' tab selected. The left sidebar is the same as in Figure 14. The main content area shows the 'Time Settings' tab with 'Device Time' at 09/10/2026 08:30:39. The 'Time Zone' is '(GMT+00:00) Dublin, Edinburgh, London'. The 'Time Synchronization Mode' is set to 'Manual' (radio button selected). The 'Set Time' is '09/10/2026 16:30:10' with a calendar icon and a 'Sync. with computer time' button. The 'Date Format' is 'MM/dd/yyyy hh:mm:ss'. A 'DST' section at the bottom has a 'DST' toggle switch. A red 'Save' button is at the bottom right.

Figure 15 Manual Time Synchronization

3.7 Authentication Mode

3.7.1 HTTP(S) Authentication Mode

Web interface configuration path: Configuration > Network > Network Service > HTTP(S)

To achieve the highest level of HTTP(S) authentication security, it is strongly recommended to use the digest authentication mode with the SHA256 algorithm. The alarm host device defaults to using the SHA256 algorithm and also supports configuration to the MD5, MD5/SHA256 algorithm.

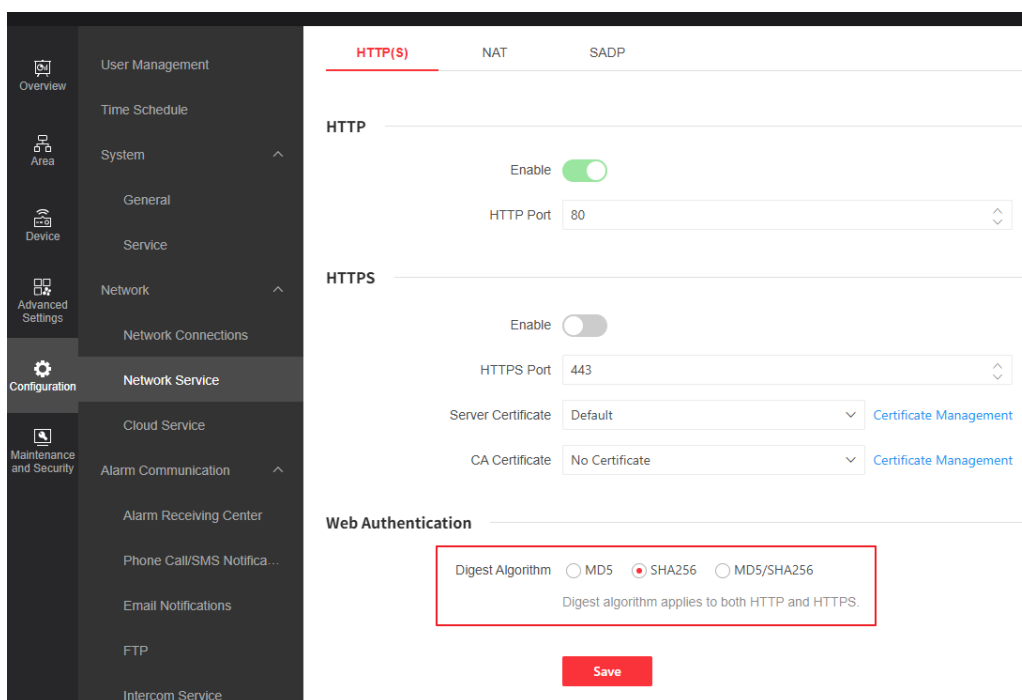


Figure 16 HTTP(S) Configuration

Note: Please ensure that the client you are using supports the SHA256 algorithm, otherwise it may cause connection issues.

3.7.2 HTTP-to-HTTPS Redirection

Web interface configuration path: Configuration > Network > Network Service > HTTP(S)

It is displayed only when the HTTP service is turned off. Redirect to HTTPS Automatically switch.

- 1) Disabling Redirect to HTTPS Automatically will close the HTTP port (default 80);
- 2) Enable Redirect to HTTPS Automatically, the HTTP port (default 80) retains the redirection function, and all other requests will be rejected

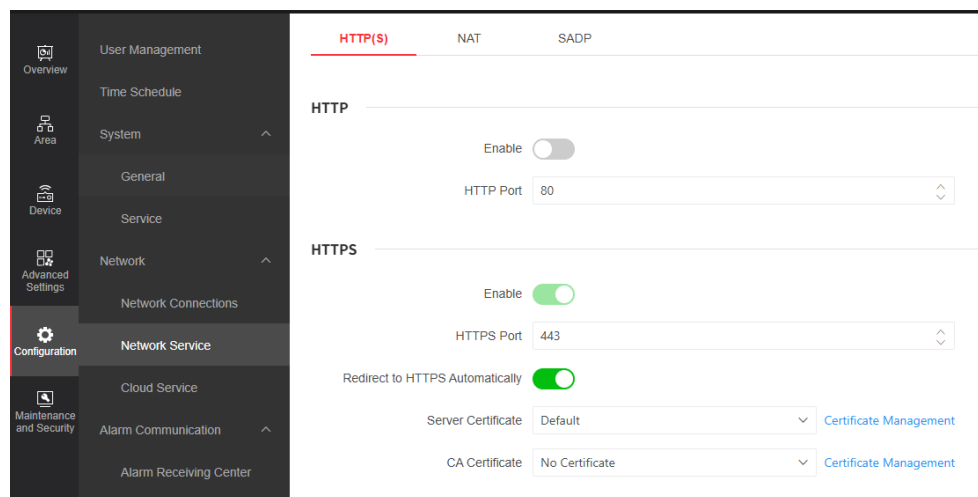


Figure 17 Redirect to HTTPS Automatically Configuration

3.8 Equipment ISUP security

Web interface configuration path: Configuration > Alarm Communication > Alarm Receiving Center, select ISUP protocol 788 for Protocol.

Pre-resources:

demo version: HCISUPSDKV2.5.2.152.

certificate path: client certificate: \\lib64\Cert\client\client-cert.pem.

client certificate key: \\lib64\Cert\client\client-key.pem.

server ca certificate: \\lib64\Cert\root\root-cert.pem.

Device side:

step1: Import client certificate and key.

Step 2: Import CA certificate.

Step 3: Configuration of ISUP parameters and differences from the old version: tls port default 7661 and Bind certificate

Alarm Receiving Center 1 2

Enable ☒

Registration Status ✓ Online

Connection Type ☐ Serial Port ☒ IP

Protocol Type ISUP

TLS ☒

Client Certificate isupc [Certificate Management](#)

CA Certificate isupca [Certificate Management](#)

Periodic Test ☐

Transmission Mode ☒ TCP ☐ UDP

Communication Channel

Network Type	Enable
Ethernet	☒
Wi-Fi	☒
Cellular	☒

Network Switching Report ☐

ISUP Protocol Version ☒ v5.0

Server Address Type ☒ IP ☐ Domain Name

* Server Address 10.6.121.118

* Port 7661

* Device ID 6666

* Password *****

Figure 18 ISUP Configuration

demo configuration:

step1: start service.

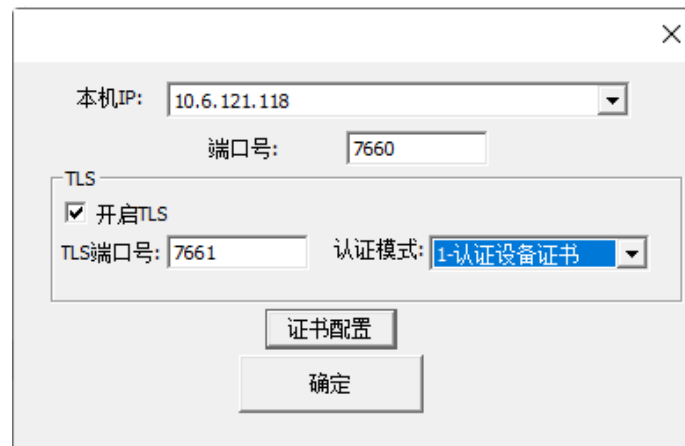


Figure 19 ISUP Demo step1

Step 2: Wait for device registration.



Figure 20 ISUP Demo step2

step3: Configure local settings.

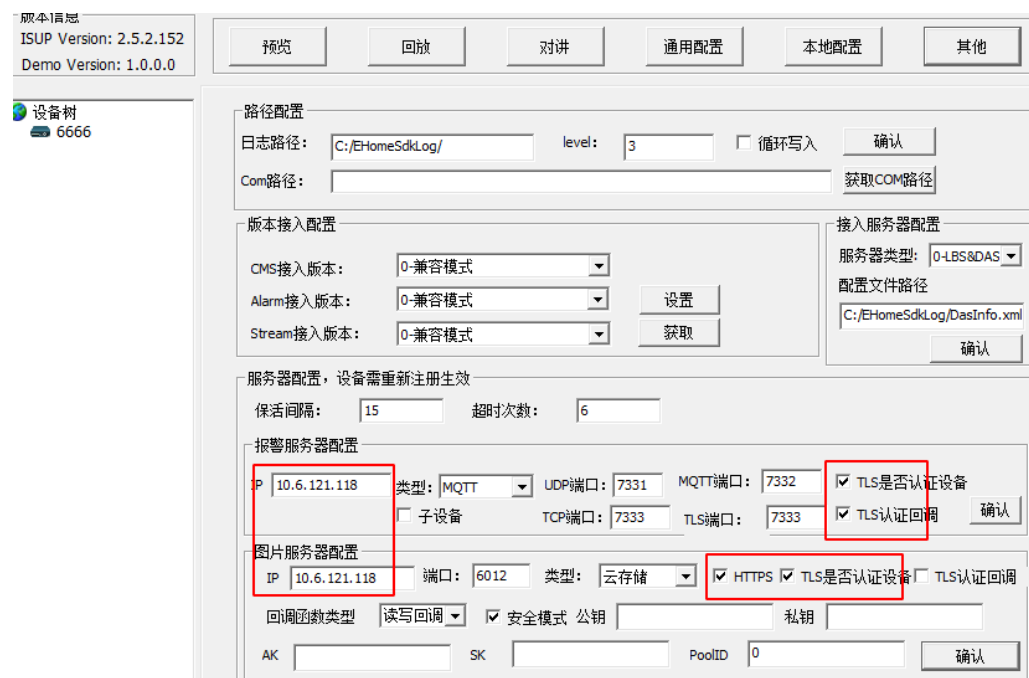


Figure 21 ISUP Demo step3

Step 4: Set up registration information.



Figure 22 ISUP Demo step4

step5: Modify the cloud storage certificate.

PUT /ISAPI/System/PictureServer?format=json

```
{
  "PictureServerInformation": {
    "pictureServerType": "cloudStorage",
    "addressingFormatType": "ipaddress",
    "ipv4Address": "10.6.121.118",
    "portNo": 6012,
    "underlyingProtocol": "https",
    "cloudStorage": {
      "cloudManageHttpPort": 6012,
      "cloudTransDataPort": 6012,
      "cloudCmdPort": 6012,
      "cloudHeartBeatPort": 0,
      "cloudStorageHttpPort": 0,
      "cloudUsername": "",
      "cloudPassword": "",
      "cloudPoolId": 1,
      "cloudProtocolVersion": "V2.0",

```

```
"cloudAccessKey": "6666",
"cloudSecretKey": "oXNoOgopK+hDf+6EI0HtFE4bhR6CEOAC6lxkMTZE7uc="},
"linkEncrypt": {
"verifyMode": 3,
"devCertID": "isupc",
"serverCertID": "isupca"}}
}
```

During the isup registration process, release the ehome message. Print “dbgCtrl 1:1:hint” to obtain this message. After copying, modify it to the actual certificate ID imported:
 "devCertID": "isupc", "serverCertID": "isupca"

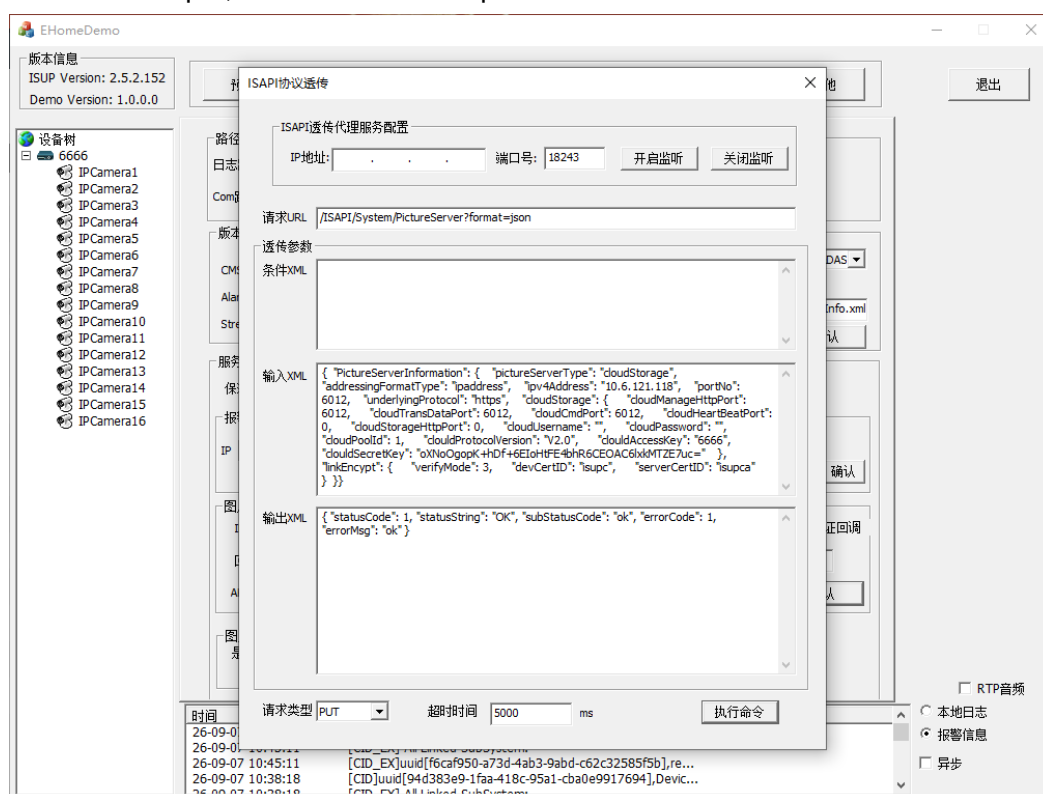


Figure 23 ISUP Demo step5

Step 6: Registration successful, view alarm information.



Figure 24 ISUP Demo step6

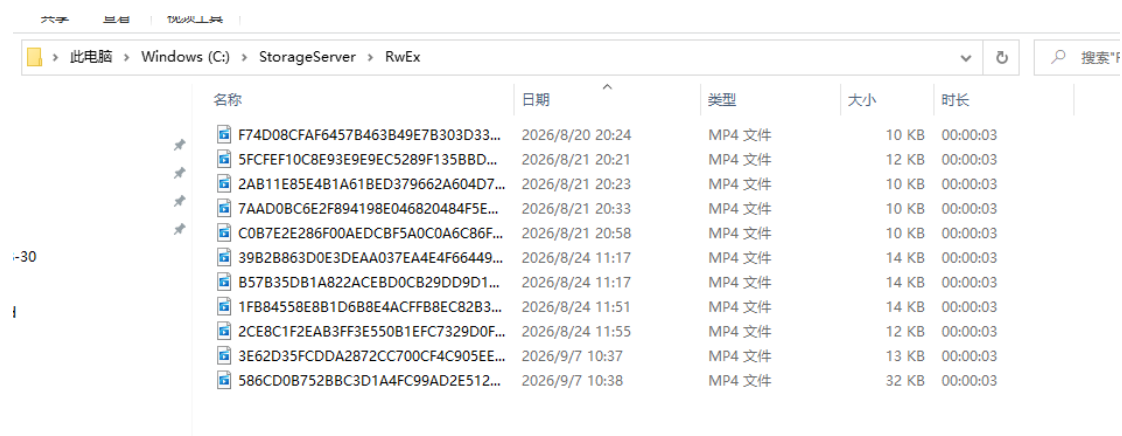


Figure 25 ISUP Demo Alarm Info

3.9 IPC Access Security

3.9.1 Adding IPC

Add Hikvision IPC by manually entering the IP address and port via the SDKS or ISAPI protocol through the entry shown in the figure.

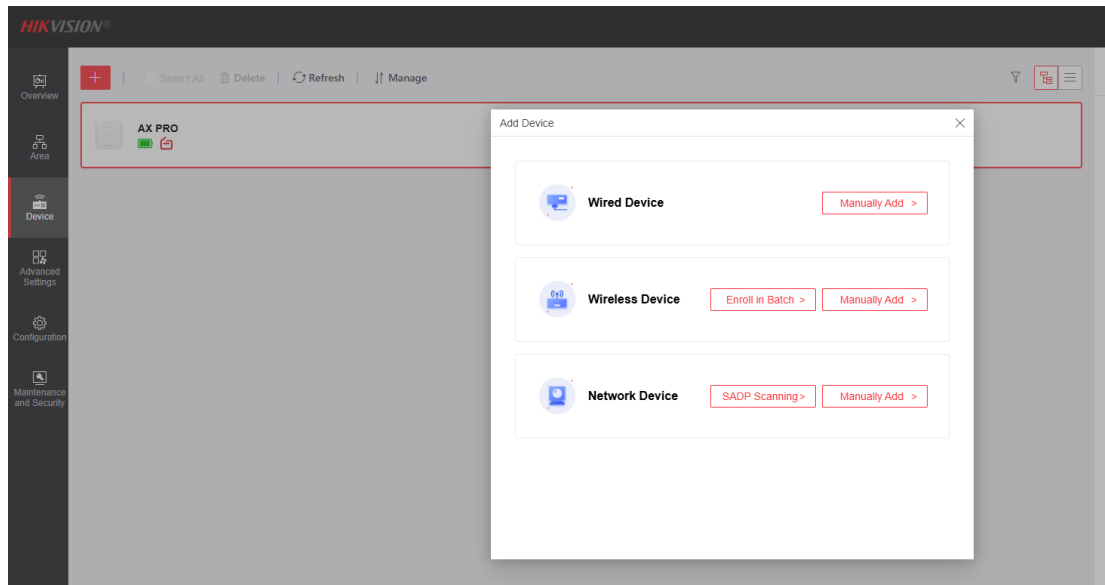


Figure 26 Manually add HIKVISION IPC entry

3.9.2 Scanning and Adding IPC within the Local Area Network

Supports displaying Hikvision IPCs scanned in the local network through the entry shown in the figure, and manually adding Hikvision IPCs via SDKS protocol or ISAPI protocol with port settings.

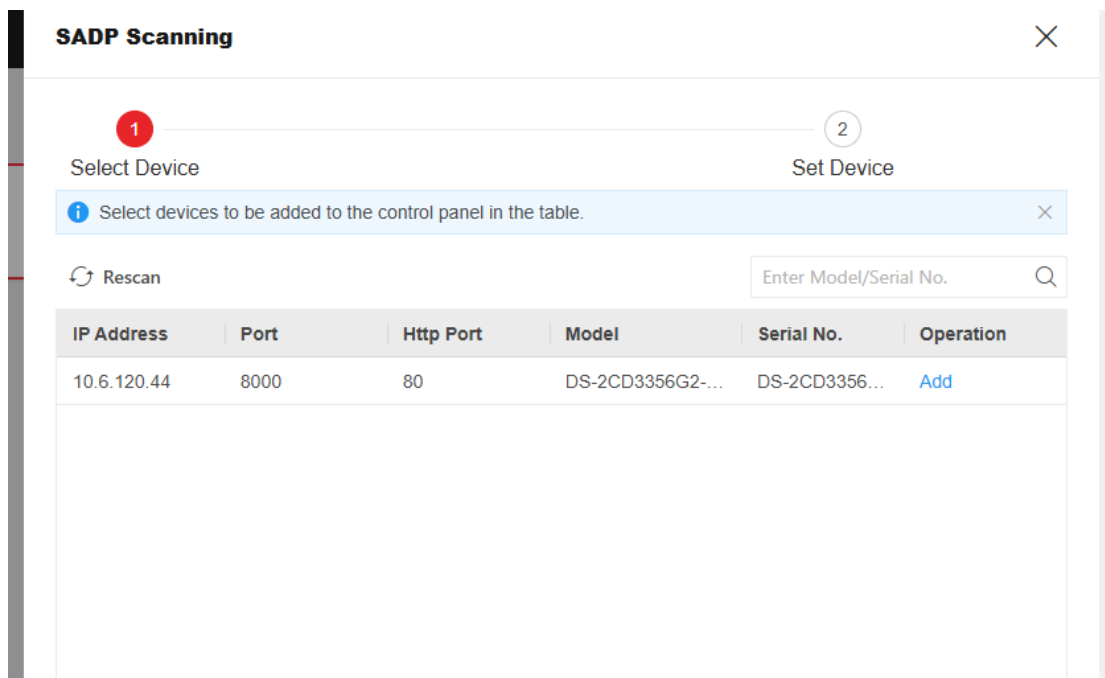


Figure 27 SADP scanning Hikvision IPC

3.9.3 Adding Hikvision IPC based on HTTPS

Under the premise that the Hikvision IPC enables HTTPS port support for login, the alarm host can achieve encrypted communication and encrypted video stream transmission through the following configuration:

(1) Encrypted communication: In the manual addition interface, select the “**HIKVISION ISAPI**” protocol, enter the corresponding IP address, fill in the Port according to the IPC HTTPS port (default is 443), and enter the username and password.

(2) Encrypted video stream transmission: Select Transport Protocol (video stream transmission method).

Figure 28 Manually add Hikvision IPC configuration interface based on HTTPS

SADP Scanning
✕

1
Select Device

2

2
Set Device

Protocol Type

☐ HIKVISION SDK
 ☒ HIKVISION ISAPI
 ☐ ONVIF

Transport Protocol

☐ Auto
 ☐ TCP
 ☒ RTSP Over HTTPS

Port*

443

User Name*

Password*

🔍

Previous

Save

Cancel

Figure 29 HIKVISION IPC configuration interface for adding devices via HTTPS SADP scan

3.9.4 Adding Hikvision IPC using the SDKS protocol

Under the premise that the Hikvision IPC enables SDK and adds service support for login, the alarm host can achieve encrypted communication and encrypted stream transmission through the following configuration:

(1) Encrypted communication: In the manual addition interface, select the “**HIKVISION SDK**” protocol, enter the corresponding IP address, fill in the Port according to the IPC SDK added service port (default is 8443), and input the username and password.

(2) Encrypted stream transmission: Select Transport Protocol (stream transmission method).

Figure 30 Manually adding Hikvision IPC configuration interface based on SDKS

Figure 31 Hikvision IPC configuration interface for adding devices via SDKS SADP scan

3.10 Intercom

3.10.1 SIP over TLS

Web configuration interface path: Configuration > Intercom Service > Intercom Parameters > TLS

After enabling the **"TLS"** switch, enable SIPS (SIP Secure, RFC 5630): SIP over TLS, which carries SIP signaling over TLS, providing transport-layer encryption and integrity protection for VoIP signaling (registration REGISTER, call control INVITE/200 OK/BYE, etc.), preventing signaling from being eavesdropped or tampered with, including sensitive information such as registration credentials, numbers, and call status. "CA Certificate" is used to select the CA certificate the device uses to verify the identity of the SIP server. When the device has imported the CA certificate corresponding to the CA that issued the SIP server certificate, this option can be selected to verify the SIP server certificate. "Client Certificate" is used to select the client certificate the device presents to the SIP server for the server to authenticate the device. When the device has imported a client certificate issued by a CA trusted by the SIP server, this option can be selected.

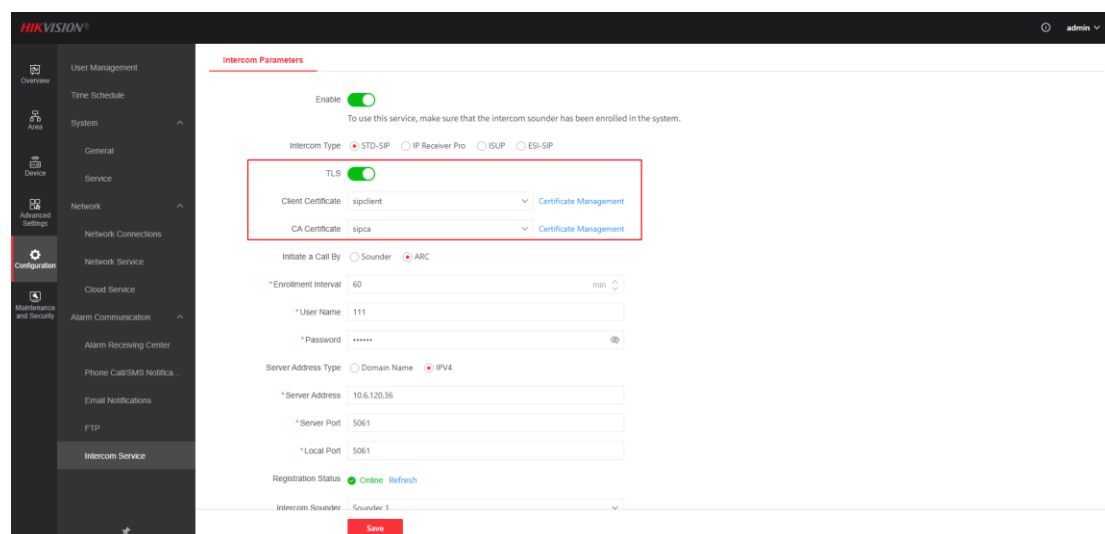


Figure 32 SIP over TLS

3.10.2 SDES-SRTP

Switch configuration: SDES-SRTP relies on SIP over TLS. When SIP over TLS is enabled, SDES-SRTP is automatically enabled; when SIP over TLS is disabled, SDES-SRTP is automatically disabled.

After enabling the **"TLS"** switch, enable SDES-SRTP: Use SDES (Session Description extensions, RFC 4568) to negotiate SRTP (Secure RTP, RFC 3711) media encryption keys,

encrypt and authenticate RTP audio streams to prevent voice media from being eavesdropped, tampered with, or injected. SDES does not introduce additional signaling interactions; encryption keys are inlined in the SDP message body as a=crypto attributes and transmitted via SIP signaling. The caller announces the encryption suite and master key in the SDP of the INVITE message according to priority, and the called party returns the selected suite and its own master key in the 200 OK. Both parties derive SRTP session keys separately. Key material is transmitted throughout the SIPS (TLS) encrypted signaling channel, and keys are not exposed on the network. Mandatory encryption: The device carries a=encryption: mandatory in the 200 OK to indicate that media encryption is mandatory. Endpoints that do not support SRTP cannot establish calls and will not accept downgraded negotiations from the peer.

3.11 User Lock Configuration

Web interface configuration path: Maintenance and Security > Security > User Lockout Attempts

User locking is a security protection mechanism, mainly used to prevent malicious login attempts such as brute-force password cracking, thereby enhancing device security. This feature is enabled by default and cannot be disabled. It locks the user account automatically after multiple consecutive failed login attempts and prohibits the user from logging in again for a specified period of time.

The following parameters can be set manually:

- **Retry Times Before Auto-lock:** Refers to the number of consecutive incorrect password entries by a user after which the system will automatically lock the account.
- **Locking Time:** refers to the time period that must elapse after an account is locked before it is automatically unlocked. During this period, login operations cannot be performed.

Note: This feature is a global security policy and applies to administrator accounts as well.

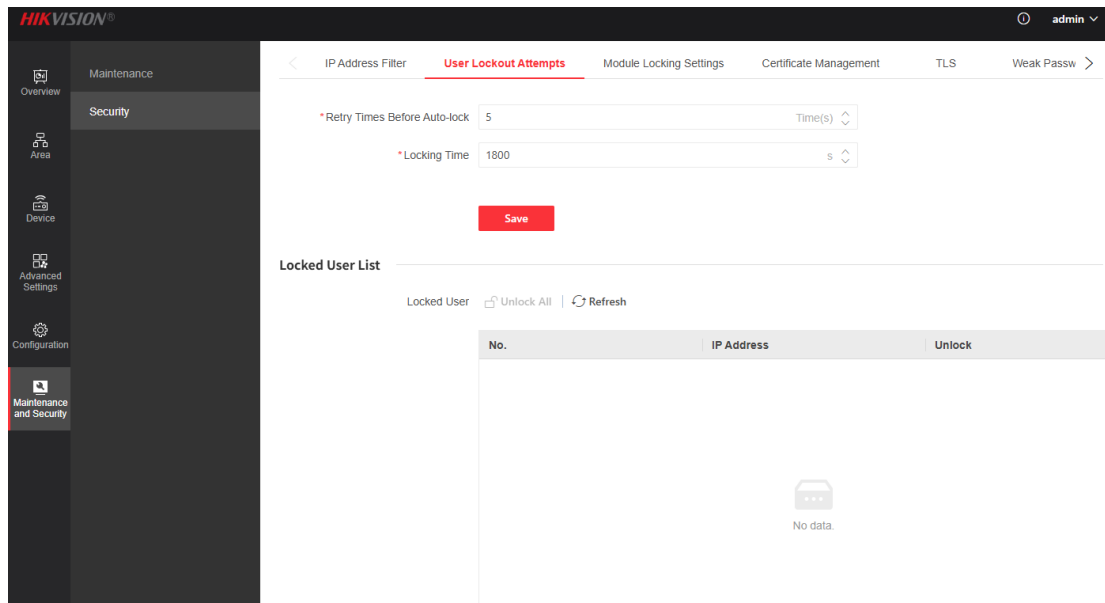


Figure 33 User Lockout Attempts

3.12 Serial Port Authentication Service

Web configuration interface path: Maintenance and Security > Maintenance > Device Debugging > Physical Debugging Port

The physical debugging port (Physical Debugging Port) is used to output device operation print information and supports serial port command interaction. It serves as a channel for on-site device diagnosis, while also preventing attackers from obtaining sensitive information such as kernel prints and shell access through it. This switch is used to control the enabling/disabling of the host's physical debugging port.

- **Default disabled:** No print output and no command interaction via the serial port. It can only be used after user authentication is completed through the serial port authentication service. It remains disabled by default upon leaving the factory, reducing the physical layer attack surface.
- **Enable:** The serial port directly outputs printing and allows command interaction without requiring the serial port service to perform user authentication. This state is convenient for on-site debugging, but it increases the physical attack surface and reduces device security. It should only be temporarily enabled when debugging is required.

When switching the switch, a confirmation prompt pops up on the page: "To ensure device security, please disable the physical debugging port after debugging is complete. Reboot the device to apply the changes. Continue?" After clicking Confirm, the device will automatically restart after a delay of approximately 5 seconds, and the configuration will

take effect after the restart; clicking Cancel will make no changes. This operation requires the logged-in user to have configuration permissions and to enter the login password for secondary authentication; consecutive incorrect passwords will trigger source IP locking to prevent online brute-force attacks. Operation logs are written and the device is restarted.

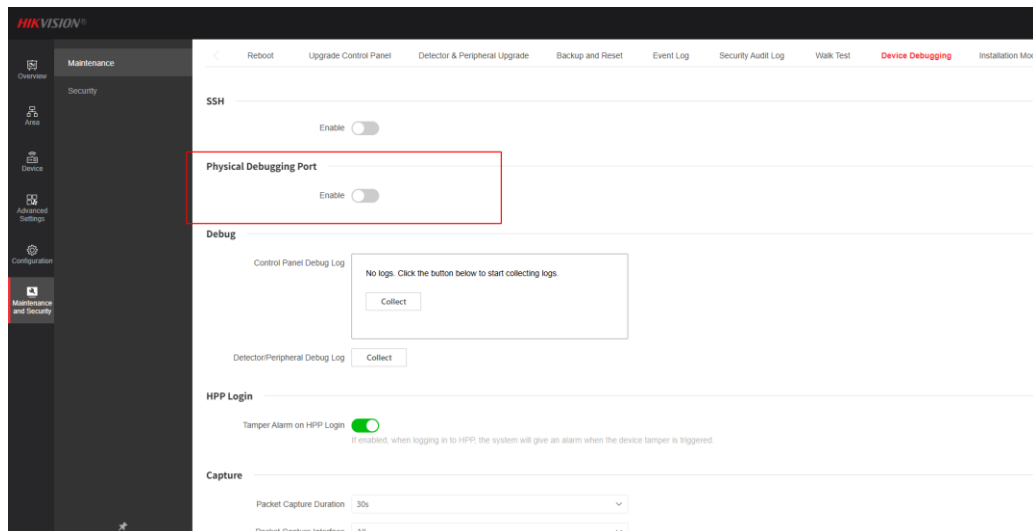


Figure 34 Physical Debugging Port Button

3.13 REST button

Web configuration interface path: Configuration > General > Control Panel Options

Disable Reset Button is used to configure the physical reset button (Reset Button) function switch, which is disabled by default.

- **Disabled:** Allows users to restore the device to factory settings via the reset button.
- **Enable:** Disable the reset button function to prevent device parameters from being lost due to accidental touches or unauthorized operations, thereby enhancing device security.

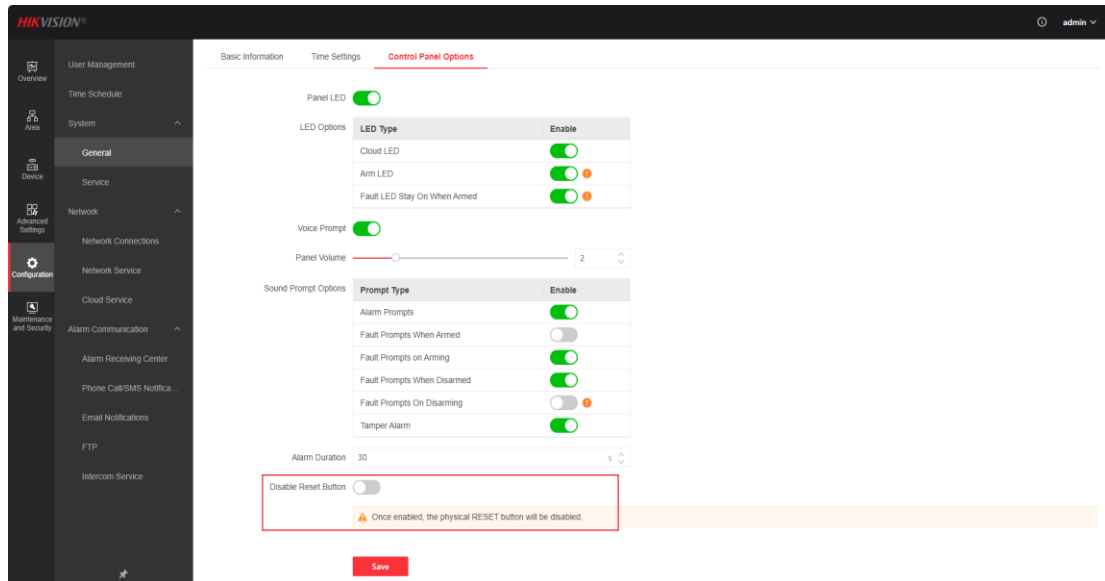


Figure 35 Disable Reset Button

3.14 User Password Expiration Reminder

Web configuration interface path: Configuration > User Management > Account Security

Password validity period configuration is used to set the number of valid days for a password, supporting two configurations: permanently valid and custom validity. The default is permanent validity. This configuration applies only to locally activated users and does not include cloud users.

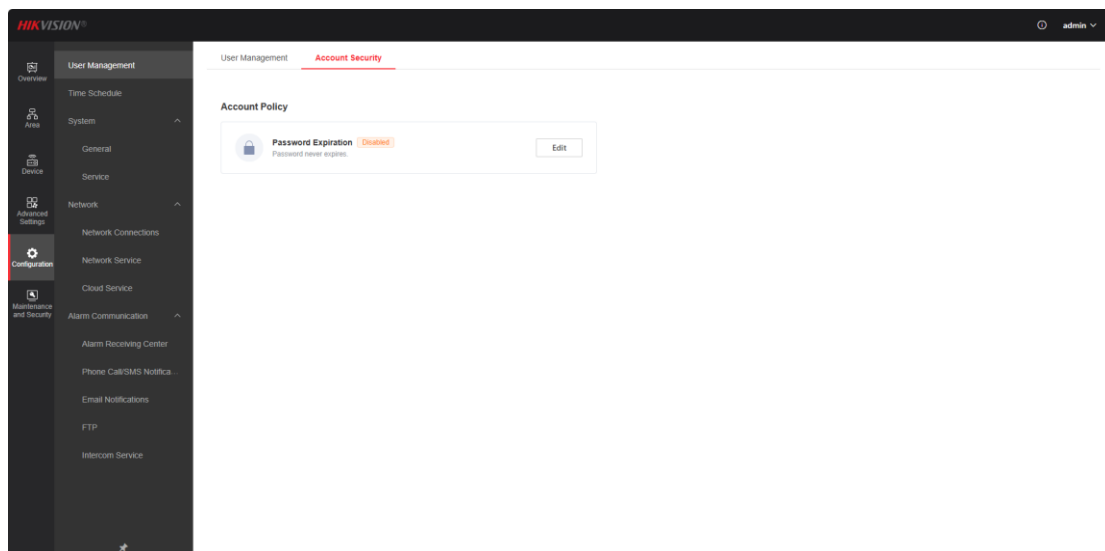


Figure 36 Password Expiration

3.14.1 Password is permanently valid

A permanent password will reduce account security and increase the risk of being

cracked. It is recommended to set a custom validity period and a reasonable expiration time, and regularly update passwords to reduce the risk of hacking.

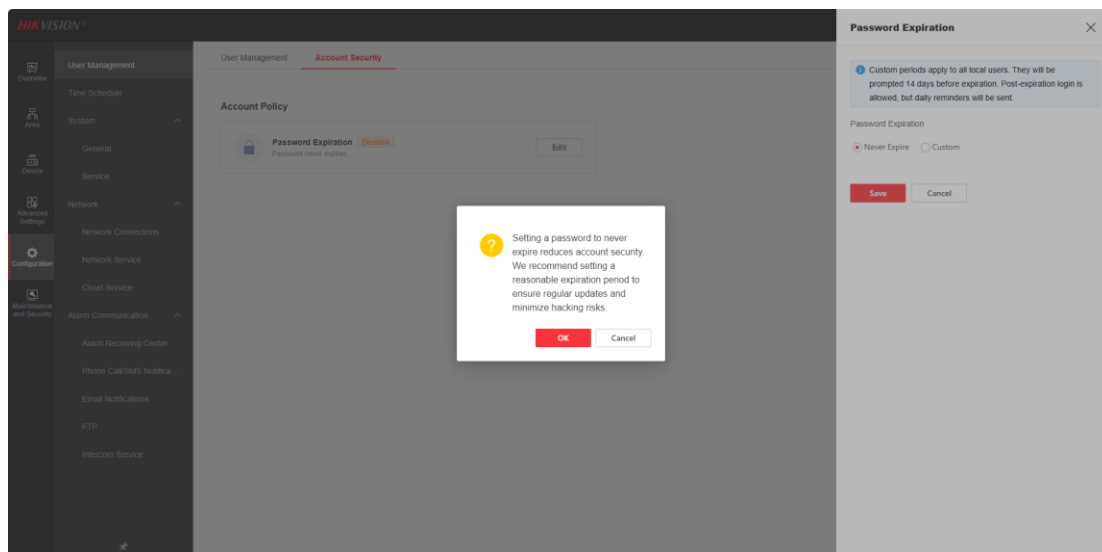


Figure 37 Password Never Expire

3.14.2 Password customizing is valid

The time range for the validity of a custom password configuration is 30-1200 days, defaulting to 180 days.

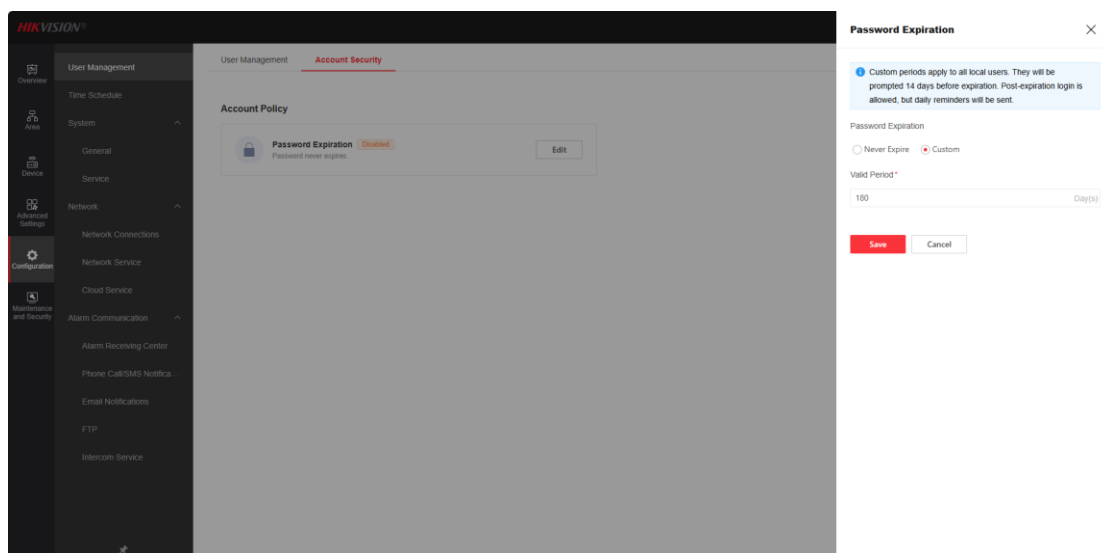


Figure 38 Password Custom

If the remaining valid days of the password are 14 days or less, a pop-up window will appear during user login to the Web, reminding the user of the remaining valid days and guiding the user to change the password.

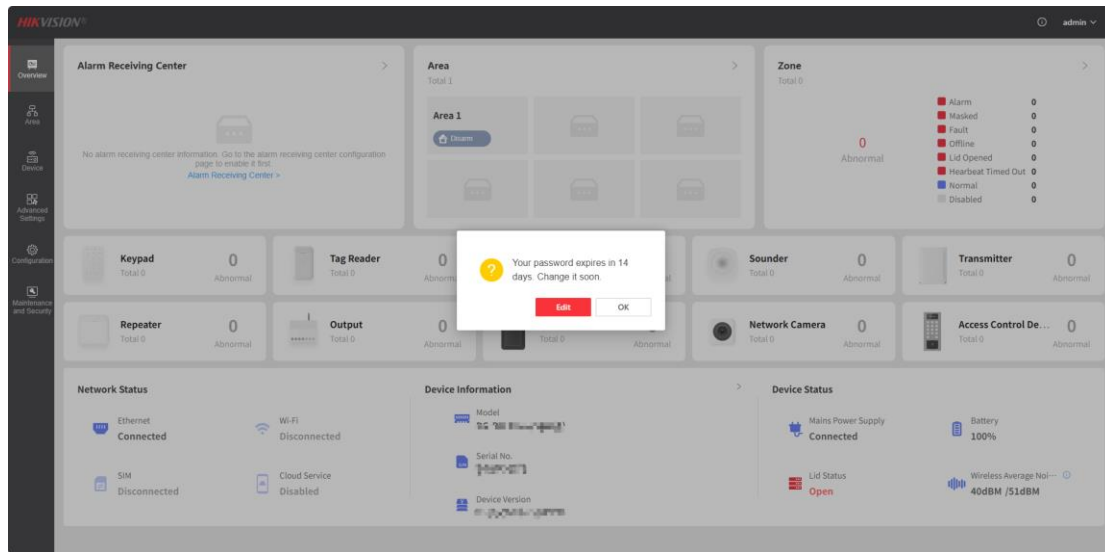


Figure 39 Password remaining valid days 14 days or less

After the password expires, a pop-up window reminds the user that the password has expired during the Web login process and guides the user to change the password.

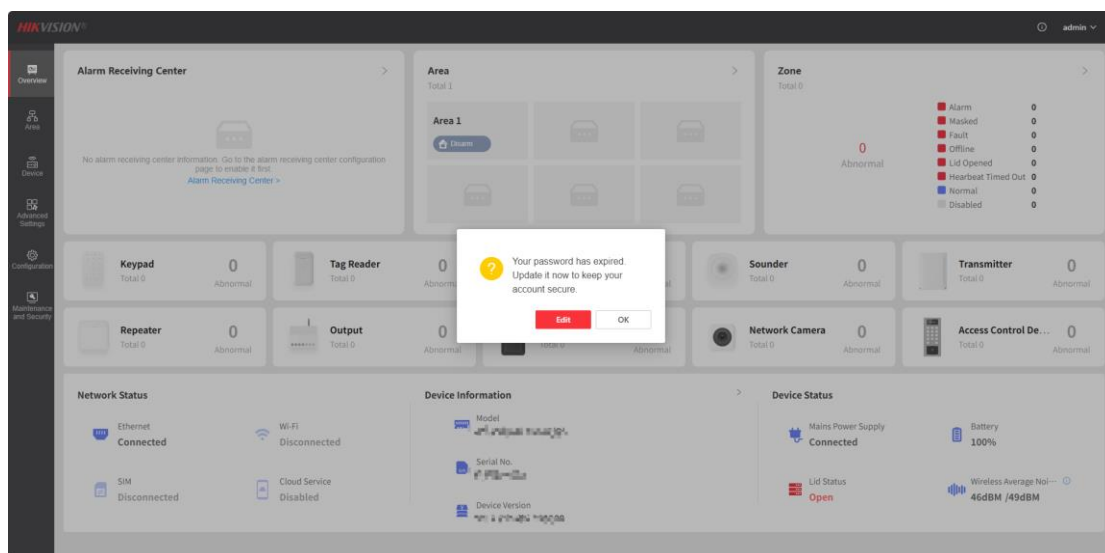


Figure 40 Password Expired

If the remaining validity period of the password is 14 days or less, or after it has expired, the remaining validity period of the password can be refreshed using the following methods:

- The user logs into the Web and follows the pop-up prompt guidance or enters the user management configuration to modify the user password and refresh the remaining valid days of the current user password.
- Local administrator logs in to the Web to modify the password validity period, refresh the remaining valid days of passwords for all local users.
 - Modify the password validity period to permanent.
 - Modify custom valid days.

Note: If the remaining valid days of the password are 14 days or less or after expiration, if the user does not change the password or does not modify the password validity period, it will not affect normal use. However, a pop-up reminder will appear every time the user logs in to the Web.

3.15 User name support modification

Web configuration interface path: Configuration > User Management > Default User

Basic Information > User Name

The default admin user of the device supports modifying the default username. When modifying, the user password must be entered for secondary authentication. The default admin user is the preferred target for attackers to guess. Allowing renaming can effectively increase the cost of brute-force attacks and dictionary attacks, thereby enhancing device security.

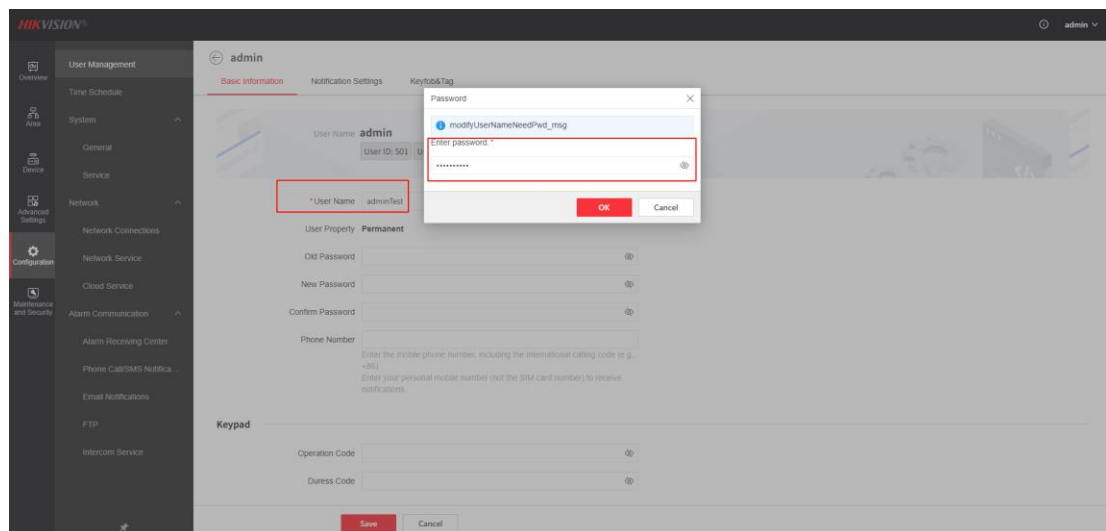


Figure 41 Default User Name Change

3.16 Backup

Web interface configuration path: Maintenance and Security > Maintenance > Backup and Reset

Regularly backing up device parameters is crucial for quickly restoring the device to its original state in case of a failure.

When performing a backup, enter the Backup and Restore interface and click the **"Export"** button in the backup module. Create and enter an encryption password, then export the current device parameter file. Specify a save path and store the device parameter file on your local computer for future use.

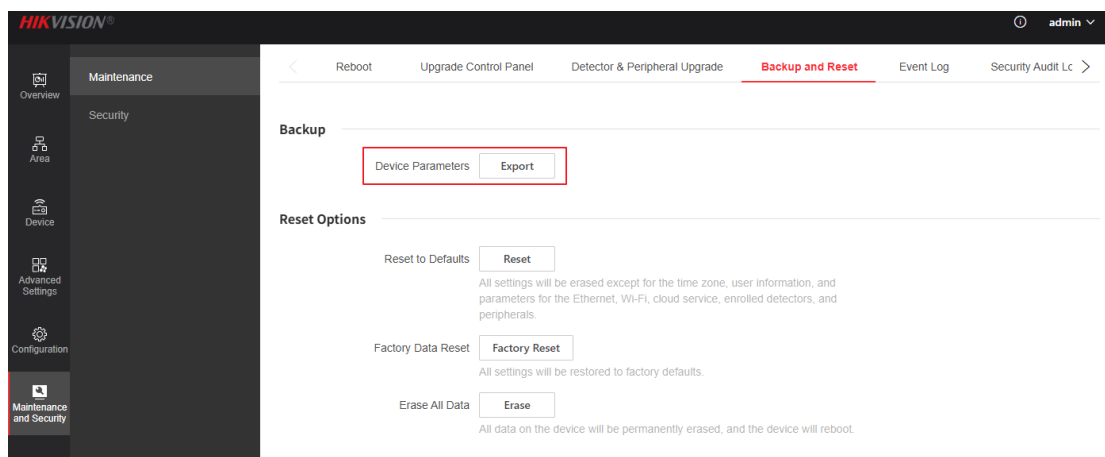


Figure 42 Backup

3.17 Email upload

Web interface configuration path: Configuration > Email Notifications

Select TLS, Client Certificate and select the certificates imported in Certificate Management. Server Authentication is enabled or disabled depending on whether the email server requires mandatory authentication login. If enabled, enter the email address and password of the email sender.

Local testing uses hMailServer + Outlook.

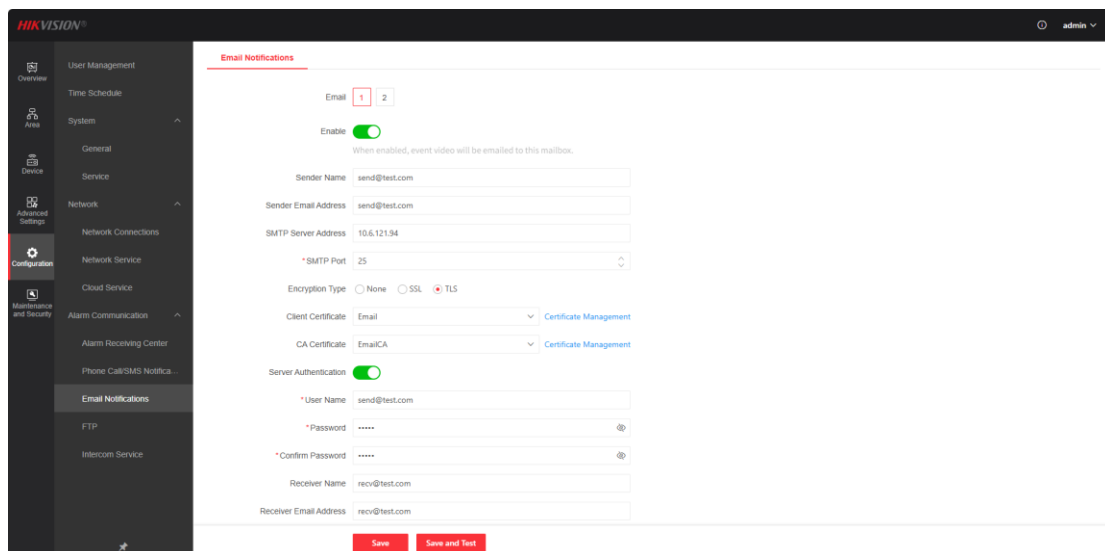


Figure 43 Email Notifications

3.17.1 hMailServer

1. Download and Installation

Official website download address <https://www.hmailserver.com/download>.

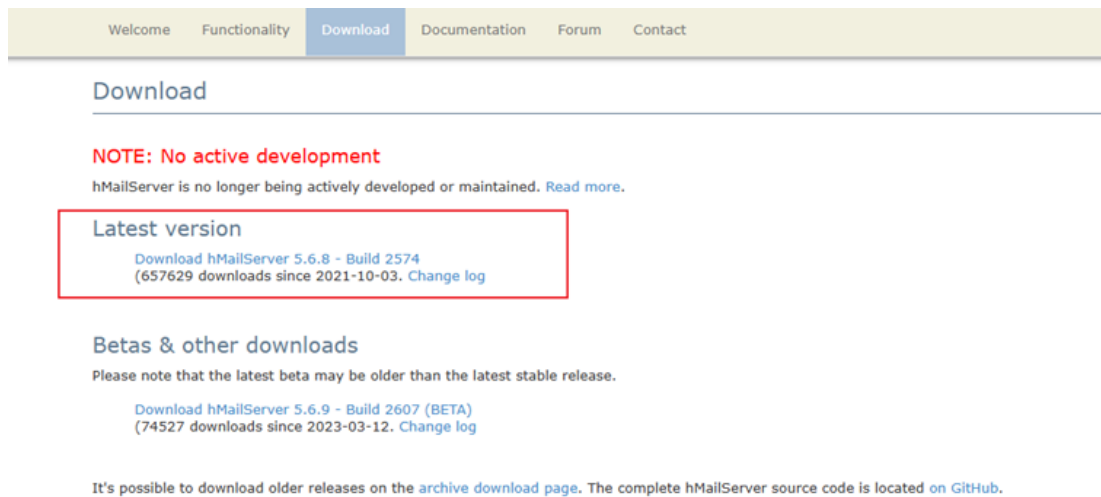


Figure 44 hMailServer download

After the download is complete, run the exe file to install directly. During the installation process, you can choose a custom installation directory and set a default password when setting the server password. This password will be required for subsequent runs.

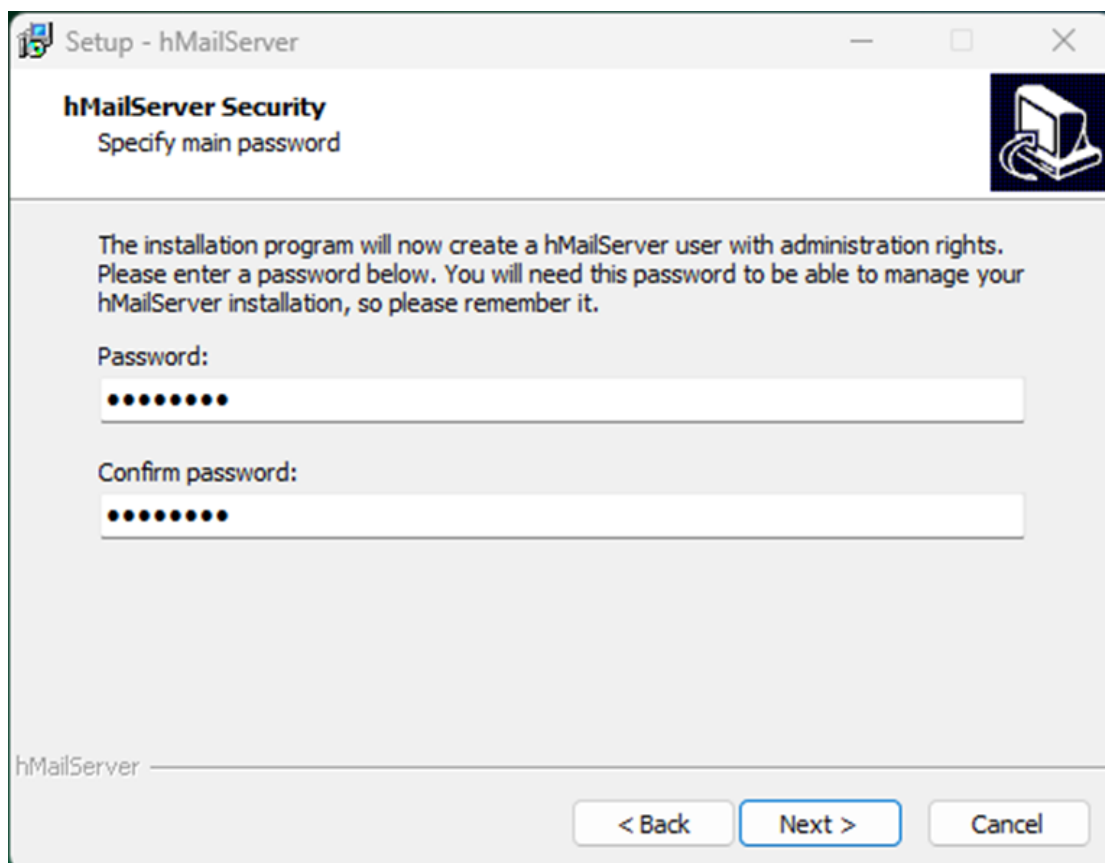


Figure 45 hMailServer Password

2. Operation and Settings

After the installation is completed, run hMailAdmin.exe in the Bin folder under the installation directory as an administrator. After launching, click Connect and enter the

default password set during installation to complete the software startup.

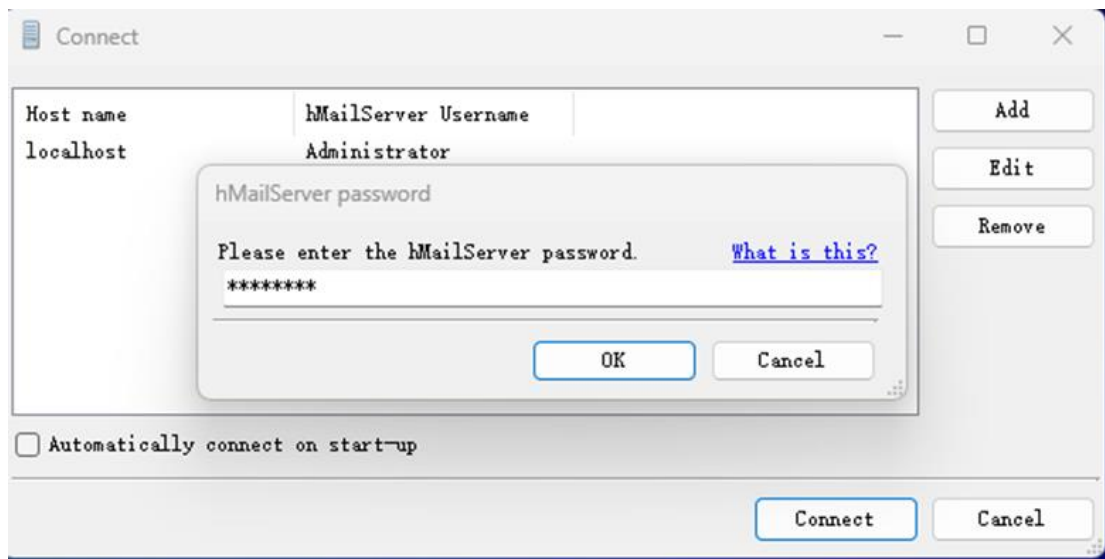


Figure 46 hMailServer Connect

2.1. Add a domain name and account

2.1.1. Domain name addition

Click Add domain to add a domain or Domains > Add

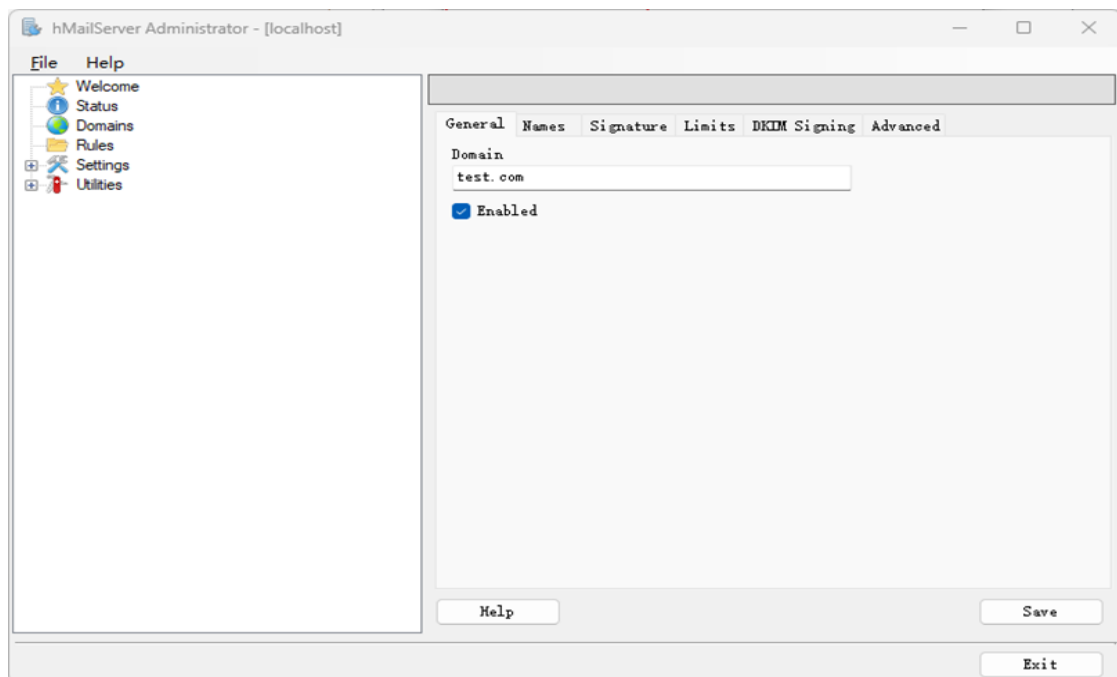


Figure 47 Domain Add

2.1.2. Account addition

Domain > test.com > Accounts > Add.

Add two accounts separately for sending and receiving emails, the sending email account send@test.com, the receiving email account recv@test.com, or you can also add

one account for both sending and receiving. A password needs to be set when adding an account, which will be used by the email client later.

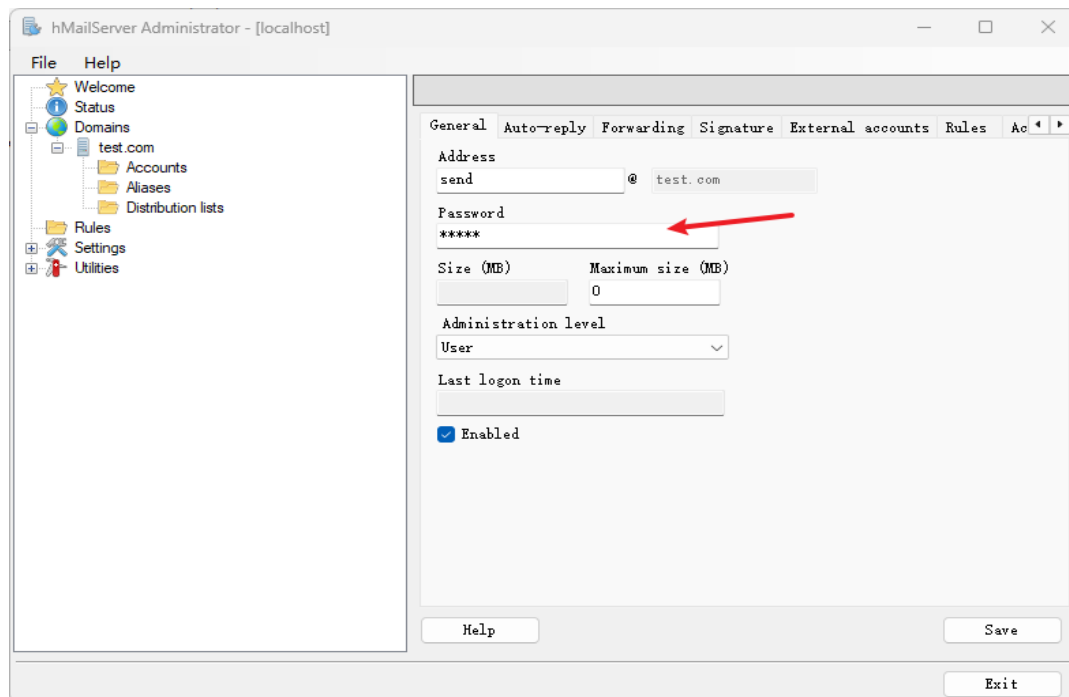


Figure 48 Accounts Add

2.2. Advanced Configuration

2.2.1. Add SSL certificate

Settings > Advanced > SSL certificates > Add, import the server certificate and private key. The certificate can be issued by an authority or self-signed using openssl.

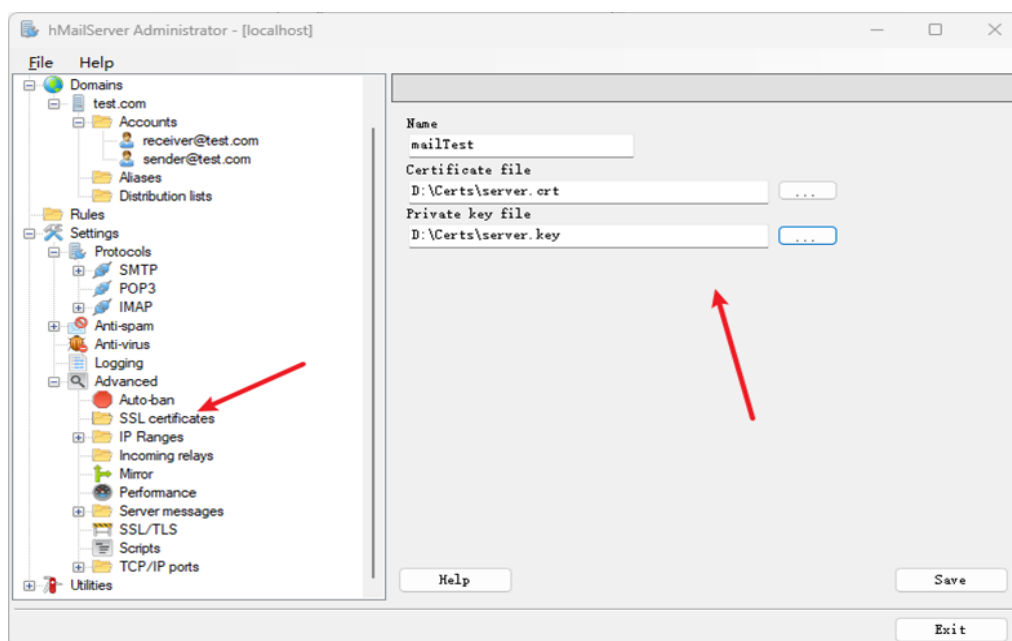


Figure 49 Certificates Add

2.2.2. IP Ranges

Settings > Advanced > IP Ranges > Add, add the local IP. Deselect Require SSL/TLS for authentication.

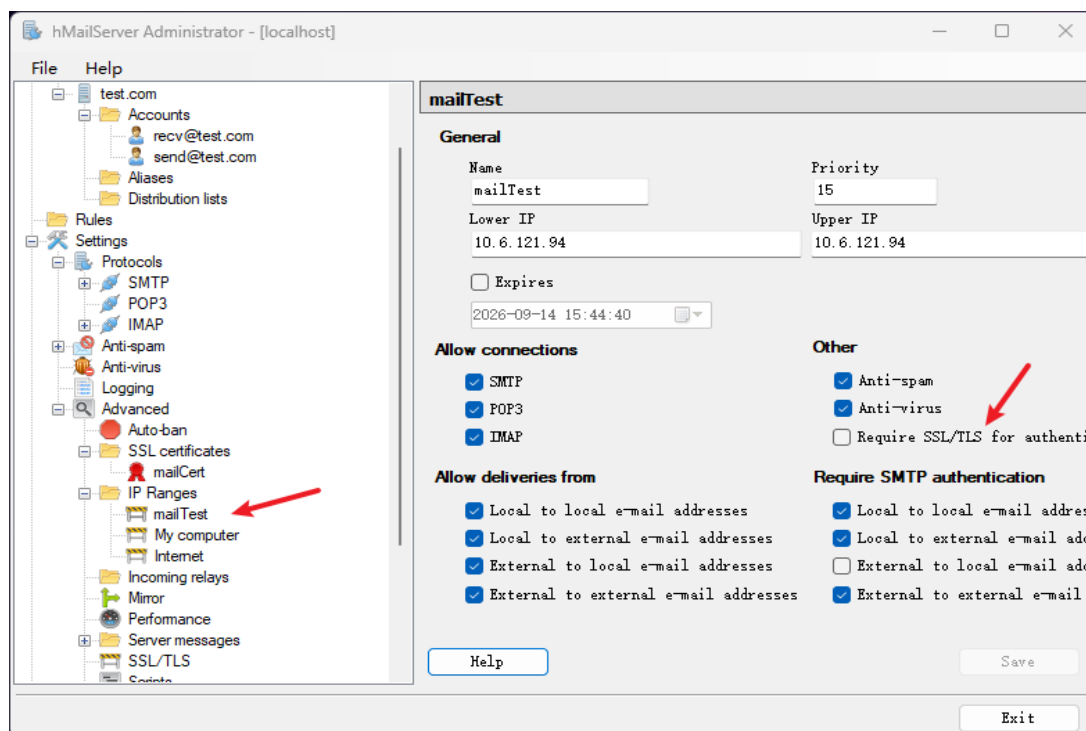


Figure 50 IP Range Add

2.2.3. SSL/TLS version settings

Settings > Advanced > SSL/TLS

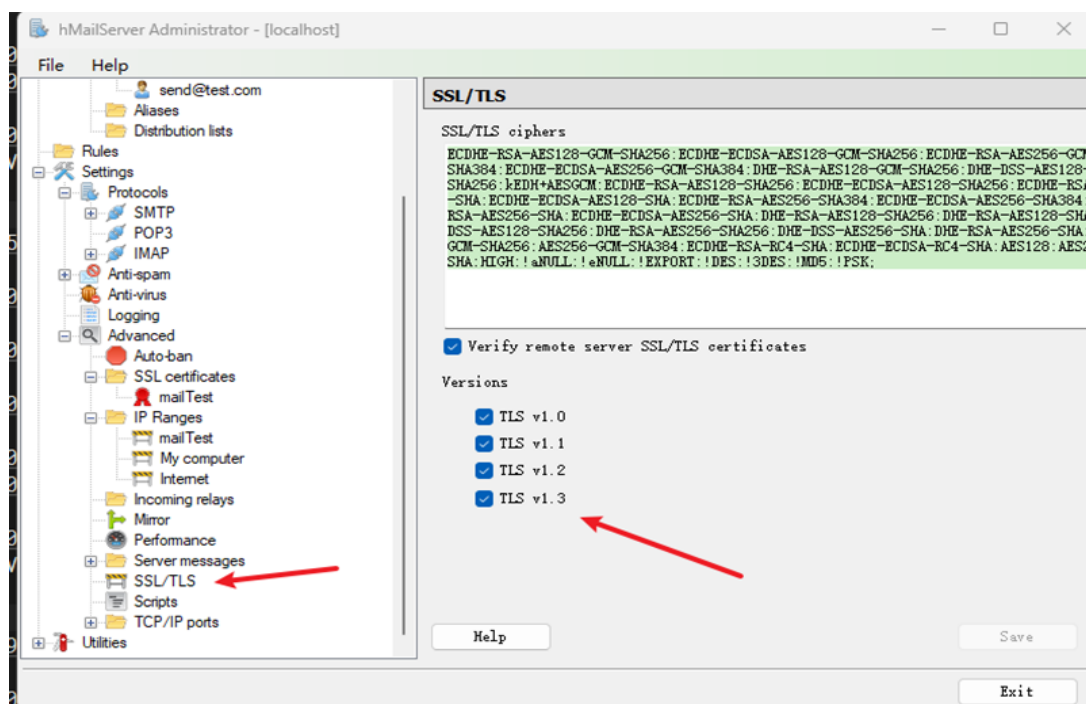


Figure 51 SSL/TLS Version Settings

2.2.4. TCP/IP ports

Settings > Advanced > TCP/IP Ports> Add, add the local IP and communication port, set the communication port to 25, select None for Connection security, and select other types during subsequent testing and verification.

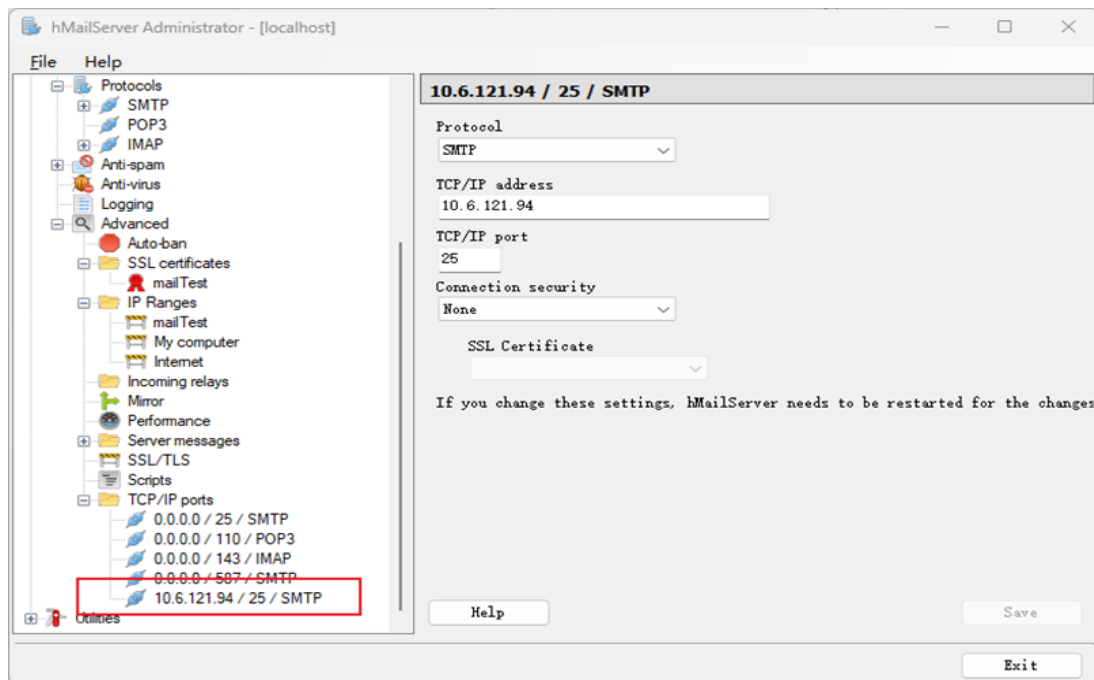


Figure 52 TCP/IP Ports Add

3.17.2 Outlook

After the email server is set up, an email client needs to be installed to receive emails. Outlook is selected here.

1. Add an email account

When starting Outlook for the first time, directly select manual setup or other server types, or in the already opened Outlook, select File > Add Account.

自动帐户设置
手动设置帐户，或连接至其他服务器类型。

☐ 电子邮件帐户(A)

您的姓名(Y):
示例: Ellen Adams

电子邮件地址(E):
示例: ellen@contoso.com

密码(P):
重新键入密码(T):
键入您的 Internet 服务提供商提供的密码。

☒ 手动设置或其他服务器类型(M)

< 上一步(B) 下一页(N) > 取消

Figure 53 Manual Setup

2. Select Service

Service selection POP or IMAP.

选择服务

☐ Outlook.com 或 Exchange ActiveSync 兼容的服务(A)
连接到 Outlook.com 等服务以访问电子邮件、日历、联系人和任务

☒ POP 或 IMAP(P)
连接到 POP 或 IMAP 电子邮件帐户

< 上一步(B) 下一页(N) > 取消

Figure 54 Select Service

3. Account Settings

添加帐户

POP 和 IMAP 帐户设置
输入帐户的邮件服务器设置。

用户信息

您的姓名(Y): send@test.com

电子邮件地址(E): send@test.com

服务器信息

帐户类型(A): POP3

接收邮件服务器(I): 10.6.121.94

发送邮件服务器(SMTP)(O): 10.6.121.94

登录信息

用户名(U): send@test.com

密码(P): *****

☒ 记住密码(R)

☐ 要求使用安全密码验证(SPA)进行登录(Q)

测试帐户设置
建议您测试您的帐户以确保条目正确无误。

测试帐户设置(T)...

☒ 单击“下一步”时自动测试帐户设置(S)

将新邮件传递到:

☒ 新的 Outlook 数据文件(W)

☐ 现有 Outlook 数据文件(X)

浏览(S)

其他设置(M)...

< 上一步(B) 下一页(N) > 取消

Figure 55 Account Settings

- Enter the email account name send@test.com and the corresponding password created in hMailServer in the user information and login information.
- Select POP3 as the account type in the server information, and enter the IP address of the machine running hMailServer for both the sending and receiving servers.

After filling it out, click on Other Settings, where you need to fill in the sending server and advanced information in Other Settings.

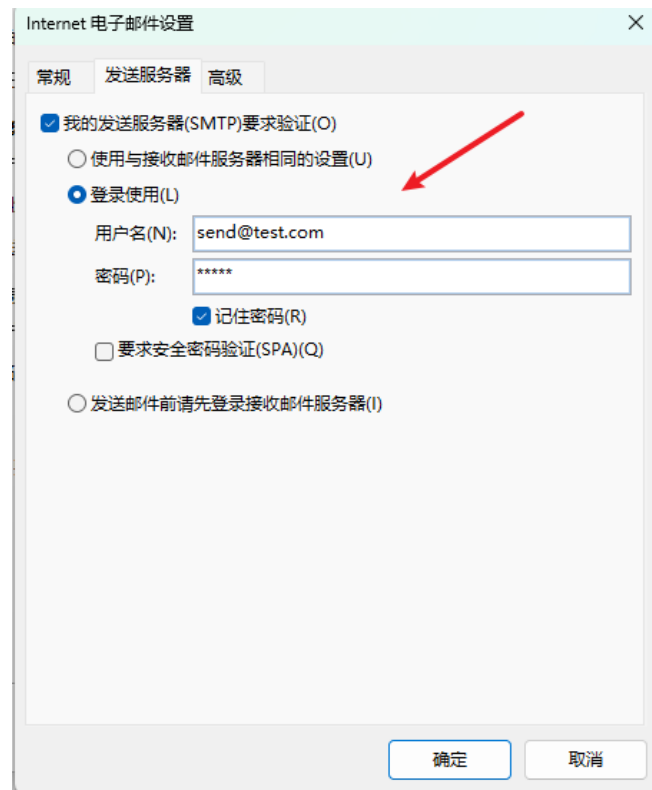


Figure 56 Sending Server

Enter the email sending account and the corresponding password information in the sending server.

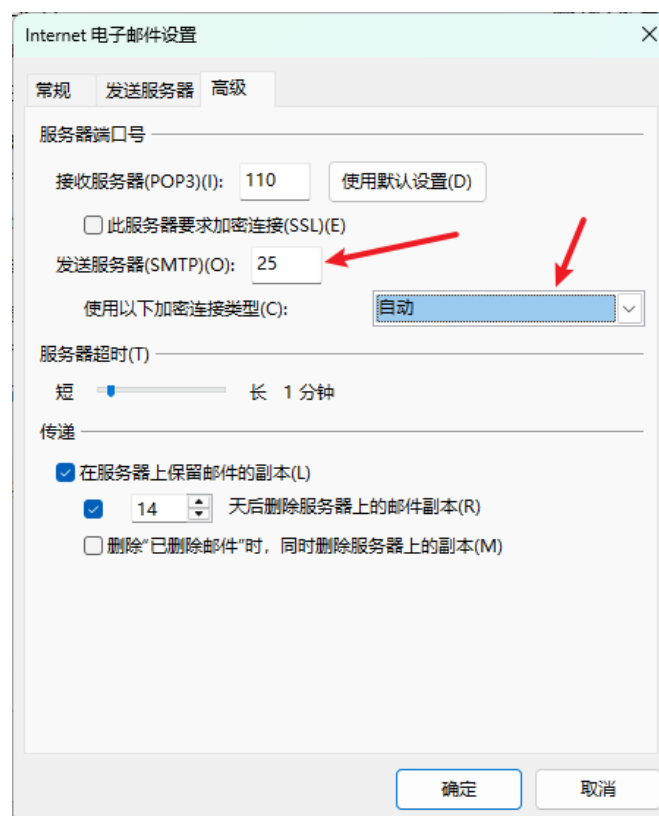


Figure 57 Advanced Configuration

Select automatic encryption type, set the sending server port to default 25 (ensure it matches the TCP/IP ports in hMailServer is consistent with the ports configured in it)

After completing other settings, click “OK” to return to the account settings interface, then click “Next” to enter the account test.



Figure 58 Account Test

After the account test is completed, click “Close”. The account has been successfully added. The steps to add the email account recv@test.com are the same as above and are not repeated here.

3.17.3 Test Verification

In hMailServer, when adding a new IP in TCP/IP ports, select STARTTLS (Required) for Connection security, Select the imported SSL certificate and save it.

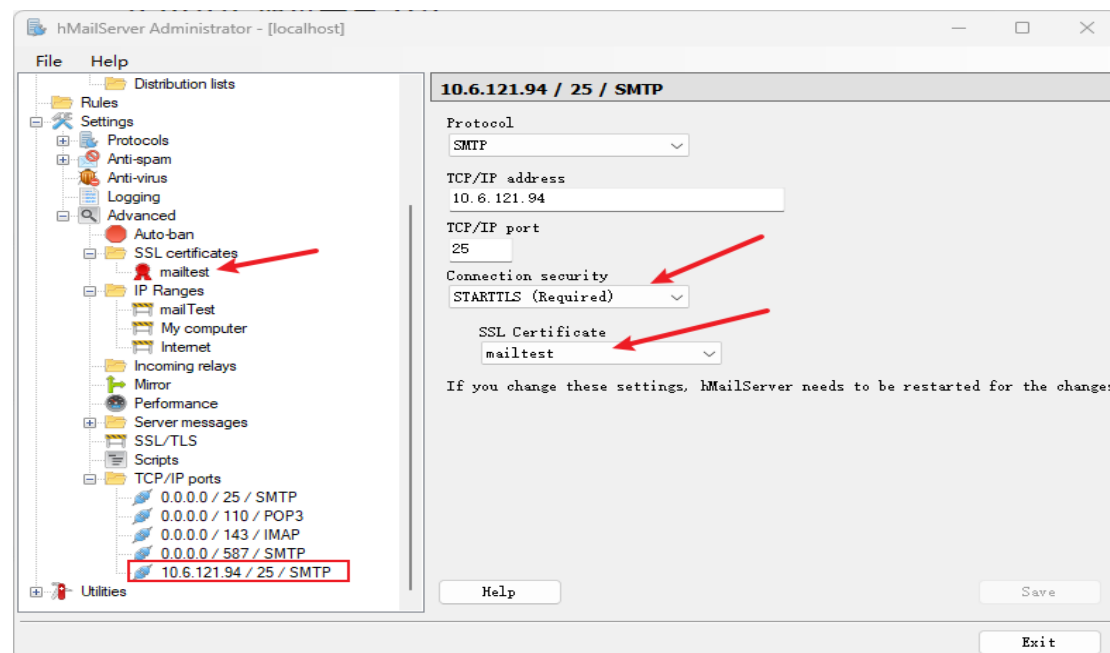


Figure 59 Connection Security STARTTLS Required

The Web email configuration is shown in the figure

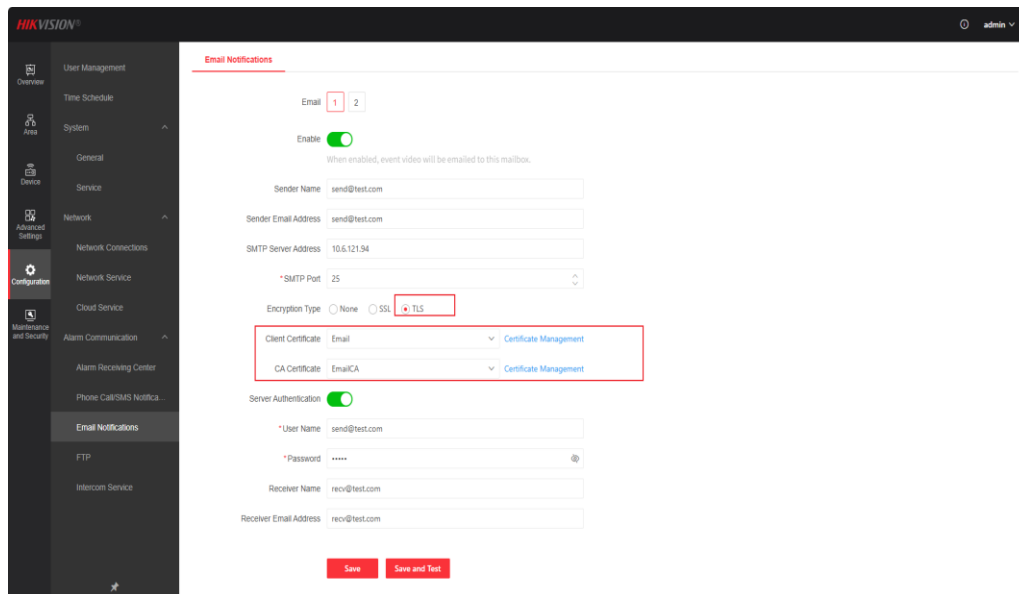


Figure 60 Email TLS Settings

- Sender Name, Sender Email Address fill in the email account name send@test.com.
- SMTP Server Address should be filled with the IP of the machine where hMailServer is running.
- Fill in the SMTP Port with the configuration in hMailServer, default 25.
- Enter the User Name as send@test.com, and enter the corresponding password for Password.
- Receiver Name, Receiver Email Address fill in the email account name recv@test.com.
- Select the client and CA certificates imported in the certificate management under Client Certificate and CA Certificate.

Note: The CA certificate must match the server certificate imported in hMailServer.

hMailServer configuration is complete, the host Web mailbox settings are complete, click Save and Test, the test email result is as follows.

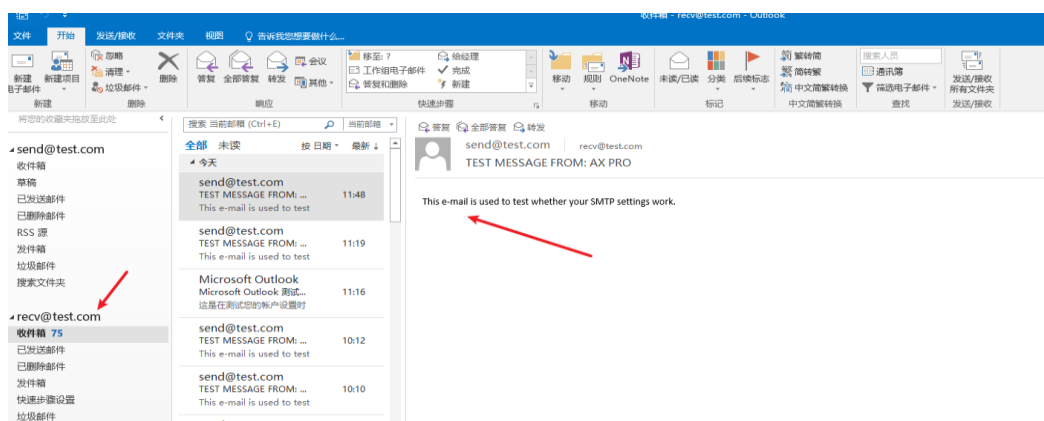


Figure 61 Test Email

The webmail encryption types also support None and SSL:

- When selecting None, in hMailServer, under TCP/IP ports, add a new IP and select None for Connection security, then save.
- When selecting SSL, in hMailServer's TCP/IP ports, add a new IP and select SSL/TLS for Connection security, then save.

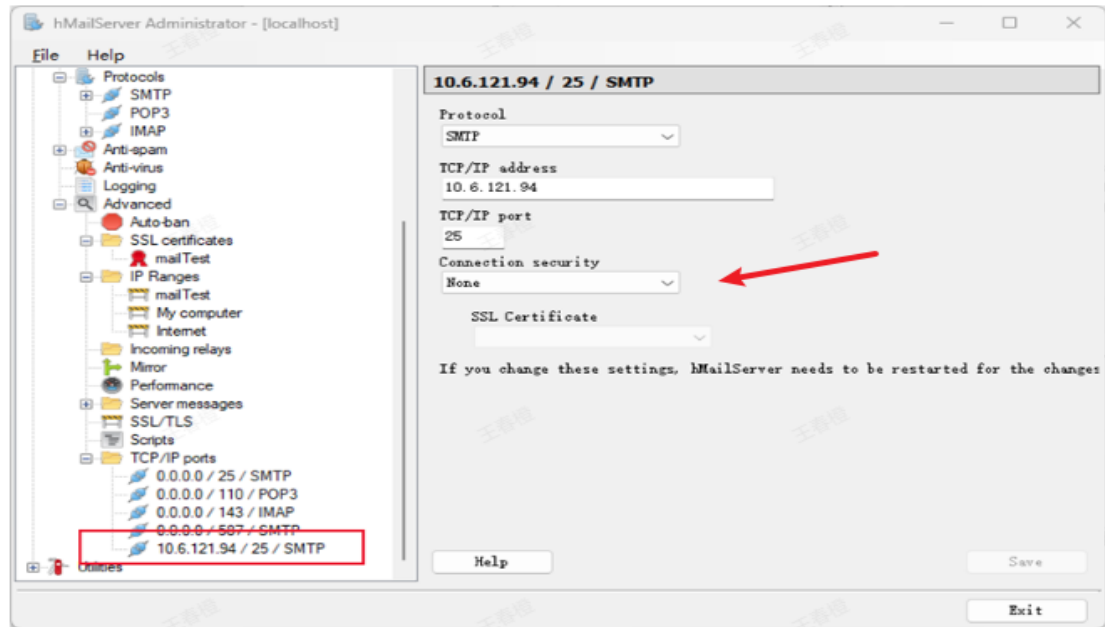


Figure 62 Connection Security None

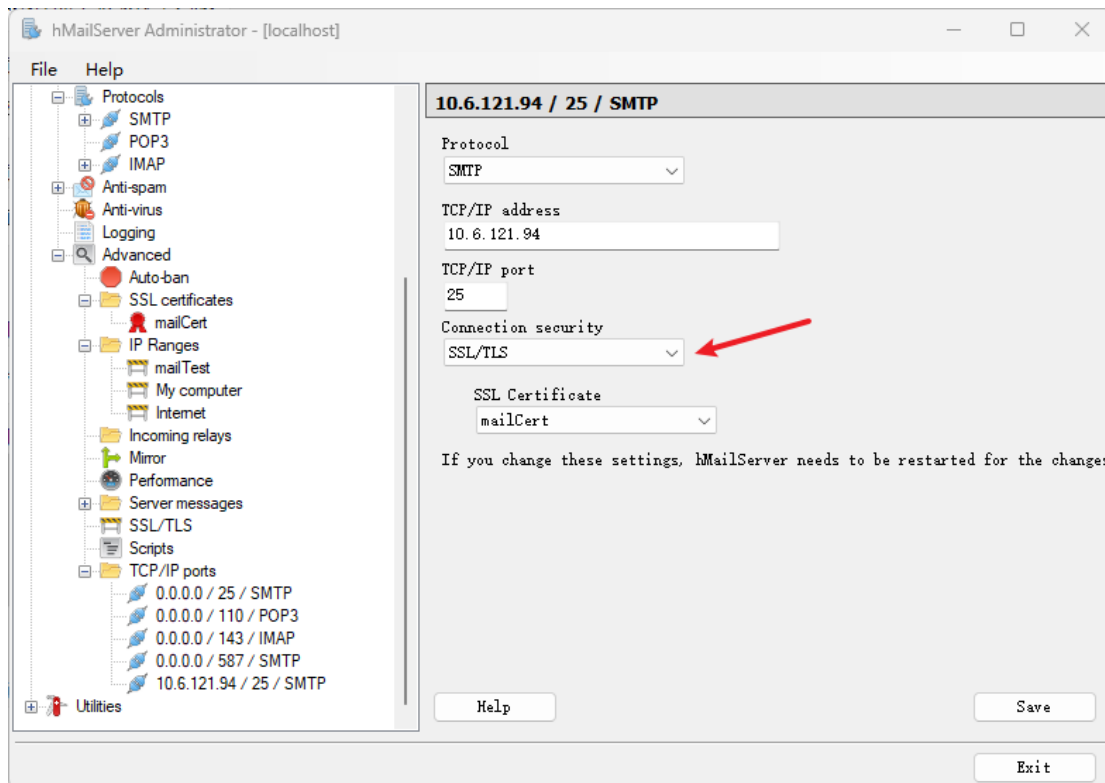


Figure 63 Connection Security SSL/TLS

3.18 FTP Upload

Web interface configuration path: Configuration > FTP.

To ensure the security of image or video uploads, select **FTPS** for FTP upload configuration. Select the FTPS protocol, After importing the Client Certificate and CA Certificate through the certificate management interface, you can select the corresponding certificates here, and configure the server IP and port. For security reasons, it is not recommended to enable anonymous configuration. Also, enter the username and password, as well as the file storage path.

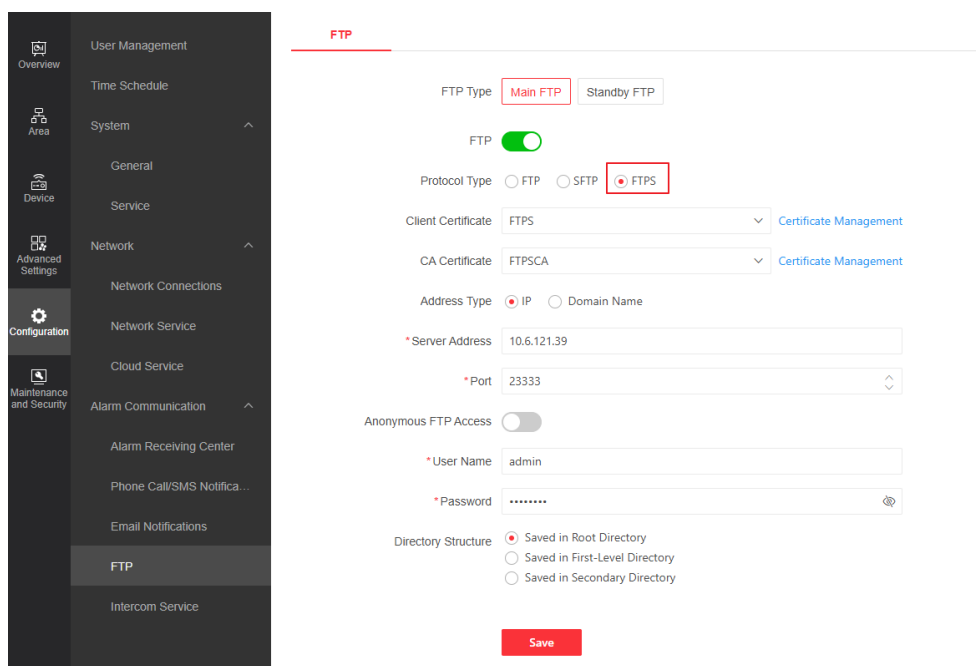


Figure 64 FTPS

It is recommended to use FileZilla for the FTPS server software. The download link is:

<https://filezilla-project.org/download.php?type=server>.

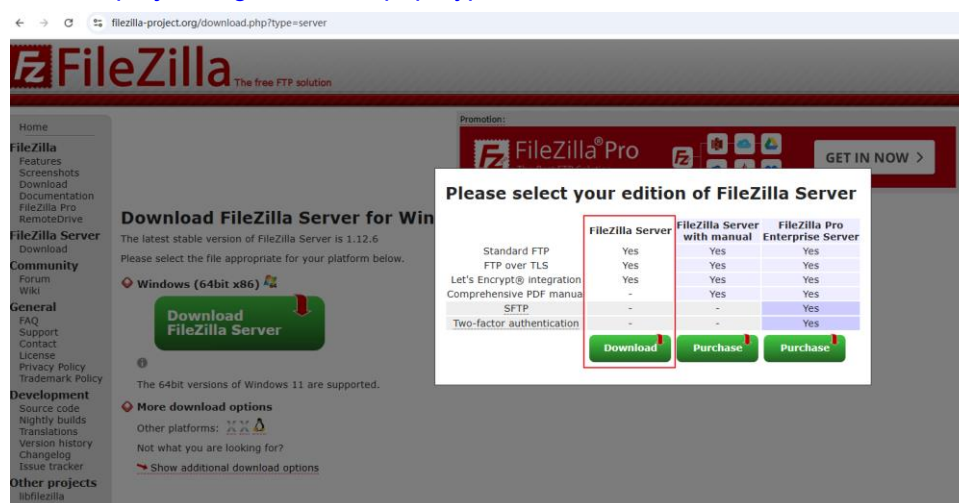


Figure 65 FileZilla Download

Install after downloading; the installation process is omitted.

Then set up the FTPS test environment:

1. First configure the listening port and protocol type: as follows

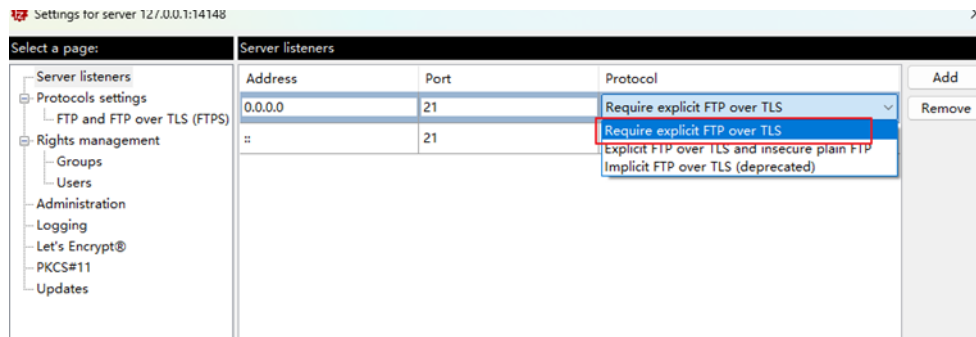


Figure 66 FileZilla port Configuration

2. Configuration certificate related:

Select the "Provide a X.509 certificate and private key" option in the red box under TLS authentication, which allows importing the public and private keys. Click Edit to copy the server's public and private keys into the fields, then click Apply to take effect.

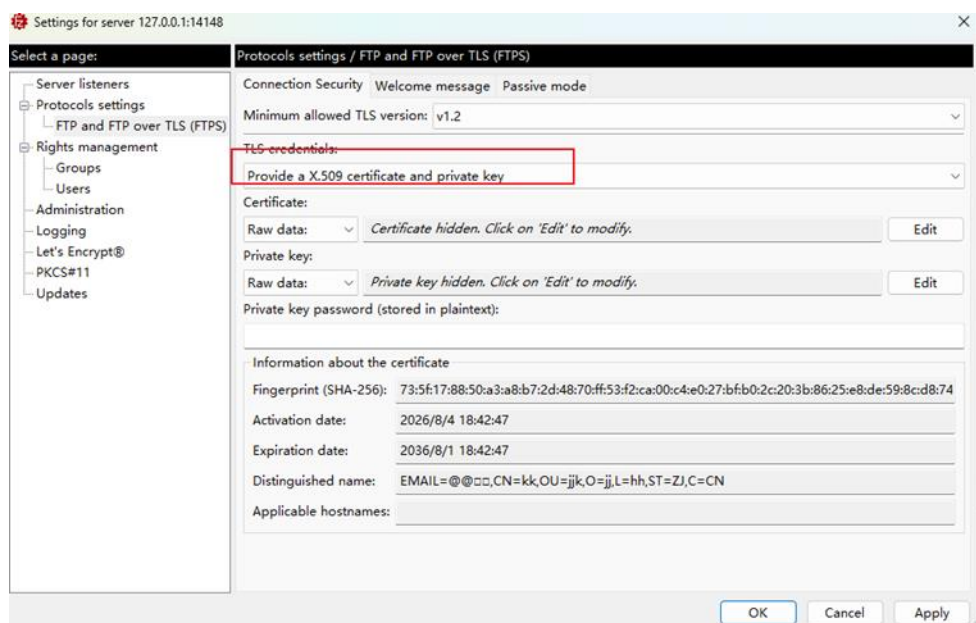


Figure 67 FileZilla TLS Configuration

3. Create user:

Click add, enable user configuration, then select "require a password to log in" for authentication method. If configured with other authentication methods, it will report that the user does not exist. Then configure Virtual path and Native path, and click apply.

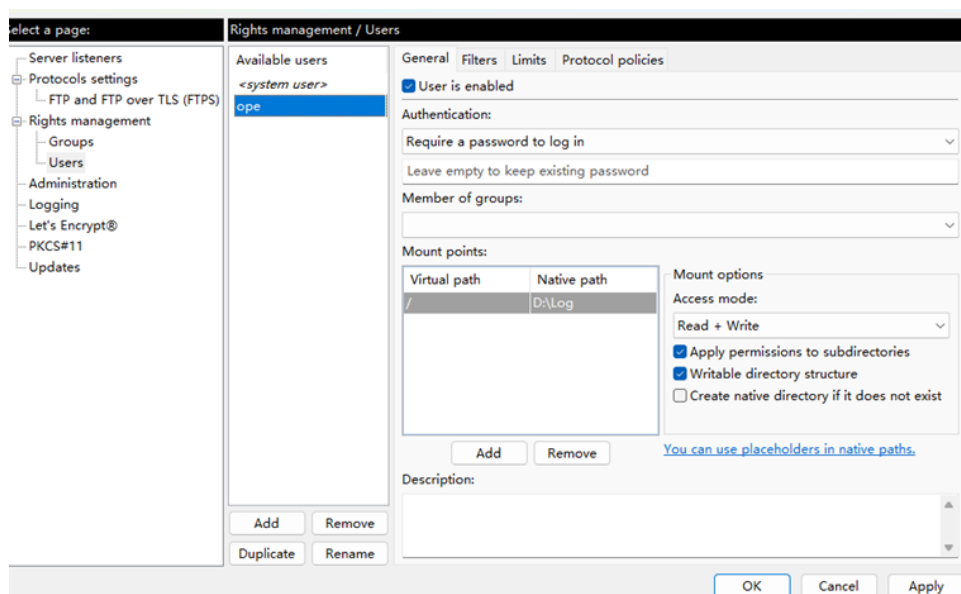


Figure 68 FileZilla USER Configuration

Expected result: If the pircam detector or the associated IPC of the zone generates an alarm, an alarm video will be generated, and the alarm video will be uploaded to the configured path.

4 Reinforced expansion

4.1 Wireless IEEE802.1X

Web configuration interface path: Configuration->Network Connections->Wi-Fi

If the main unit is in hotspot mode, click the reset button to switch the main unit to WiFi mode.

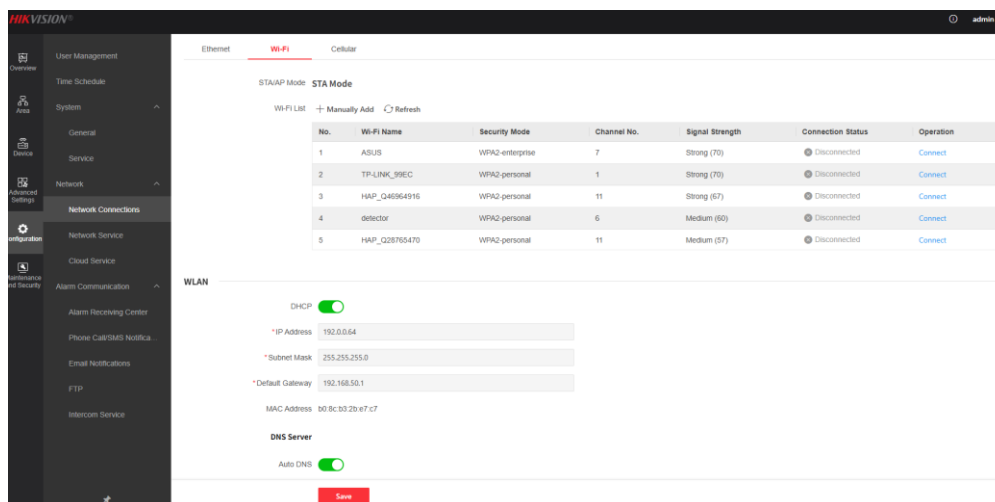


Figure 69 Wi-Fi Configure

Select a Wi-Fi that supports IEEE802.1X authentication, set Authentication to EAP-TLS, and enter the correct username, EAPoL version, client certificate, and CA certificate.

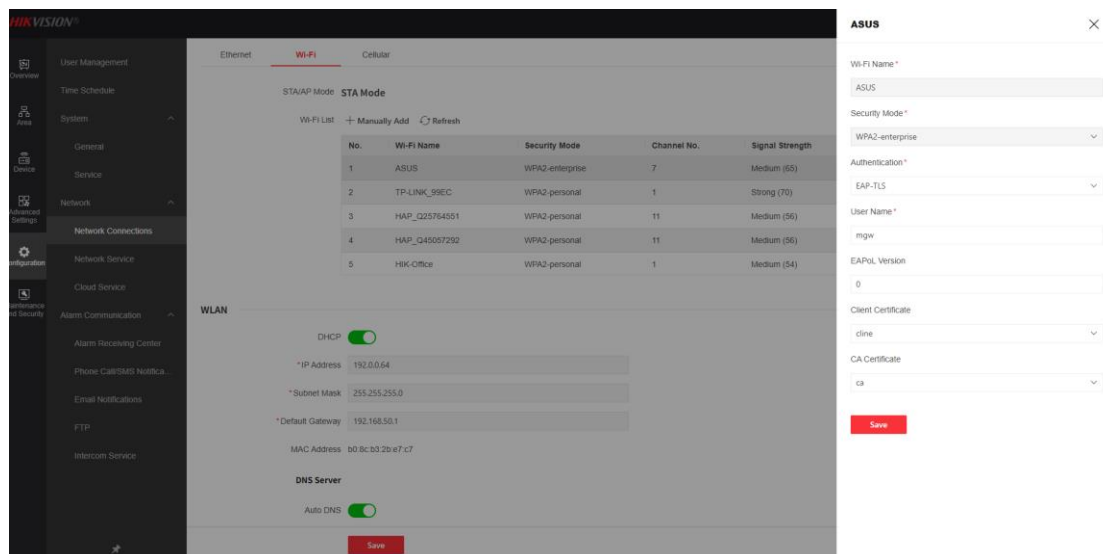


Figure 70 Wi-Fi Connect

4.1.1 Environment Setup

The router needs to support the WPA2-Enterprise authentication method. This article uses the TUF-AX3000 as an example

- Set the authentication mode: Network Map -> Authentication Method -> Set to WPA2-Enterprise.
- Set the RADIUS server address: Wireless Network --> RADIUS Settings --> Set the server address, server port (default 1812), and online password (same as the server settings).

RADIUS server configuration: The RADIUS server is used for authentication with EAP-TLS. This article uses FreeRADIUS as an example to deploy RADIUS.

- Download the installation package: <https://sourceforge.net/projects/radiusport>, the installation path in this article is D:\freeradius-3.2.10, replace the subsequent path with your own secure path.
- Set client information: Open the D:\freeradius-3.2.10\etc\raddb\clients.conf file, and append the router's address at the end of the file.

```
client my_ap {
    ipaddr = 10.6.121.143 # 你的 AP 的 IP 地址
    secret = Hik12345 # 设置一个强密码，并在 AP 上配置相同的密码
}
```

Figure 71 clients.conf

- Set user information: User information needs to be modified in the D:\freeradius-3.2.10\etc\raddb\mods-config\files\authorize file, with the following users already present by default:

```
iketestuser    EAP-IKEv2-IDType := KEY_ID,  EAP-IKEv2-Secret := "testpw"

bob            Digest-HA1 := "12af60467a33e8518da5c68bbff12b11"

mgw            Cleartext-Password := "tttt"
               Reply-Message := "success"

pwduser        Cleartext-Password := "testpwduser"
```

Figure 72 authorize

- Certificate: The certificate exists in D:\freeradius-3.2.10\etc\raddb\certs, which has already been generated by default. The private key needs to be encrypted using openssl before it can be imported into the alarm host.

4.2 sys log

Web interface configuration path: Maintenance and Security->Maintenance->Security

Audit Log

1. Configure syslog service parameters.

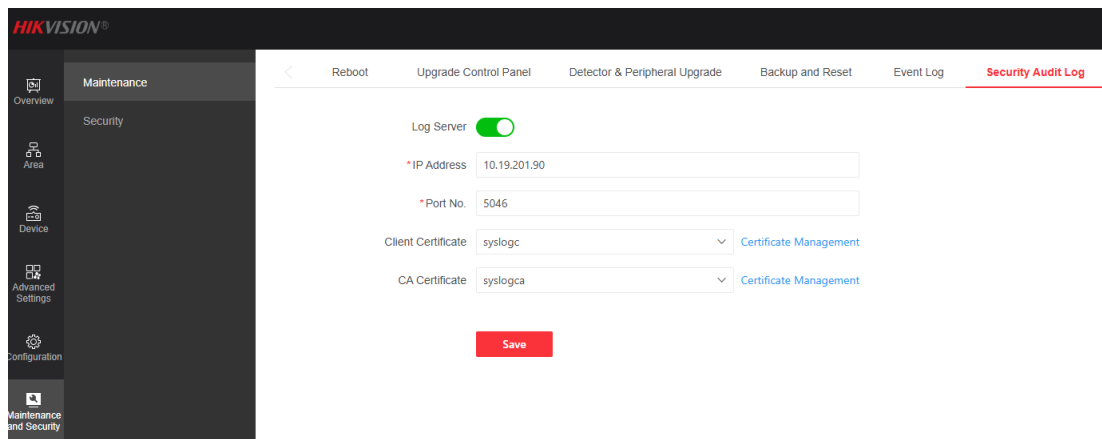


Figure 73 security Audit Log Configuration

2. View platform logs.

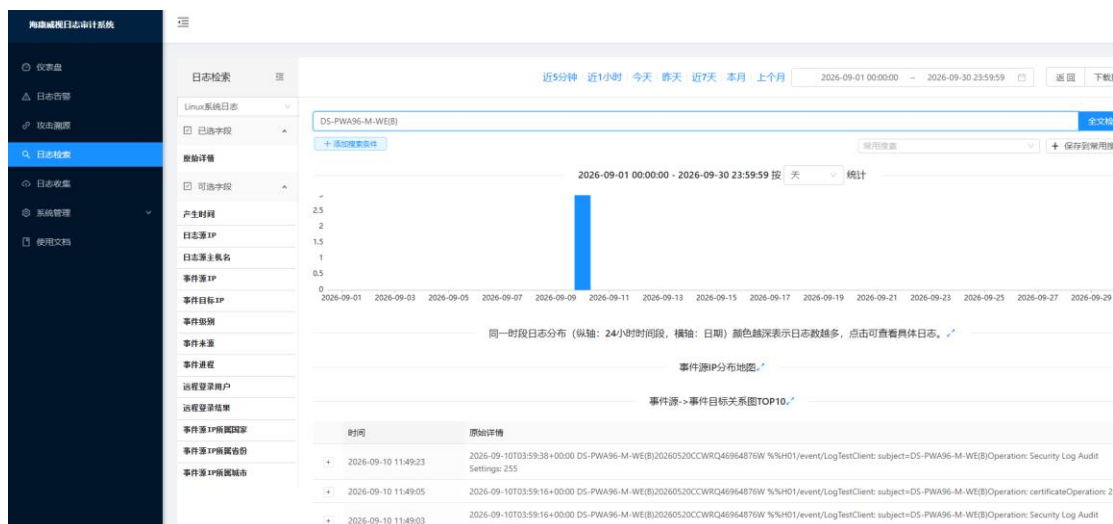


Figure 74 security Audit Log Configuration

4.3 Weak Password Management

Web interface configuration path: Maintenance and Security -> Security -> Weak Password Prevention

The weak passwords can be configured. Passwords in the weak password list cannot be set as user passwords when adding users, thus ensuring user security.

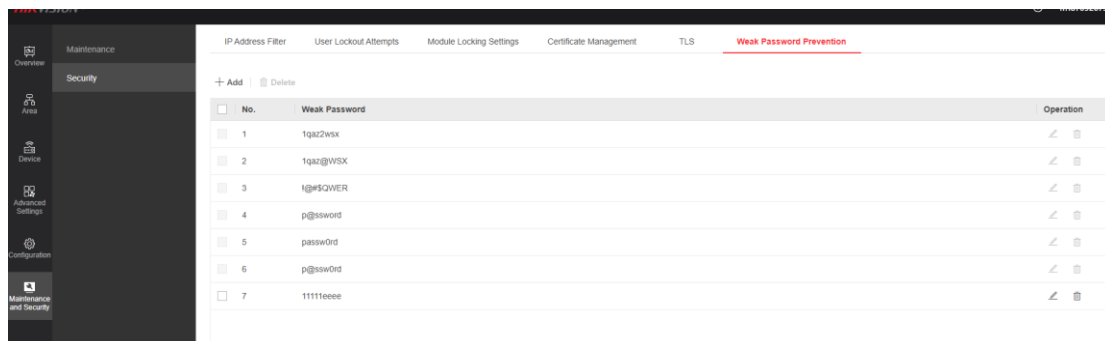


Figure 75 Weak Password Management

4.4 Certificate Management

Web configuration interface path: Maintenance and Security > Security > Certificate Management

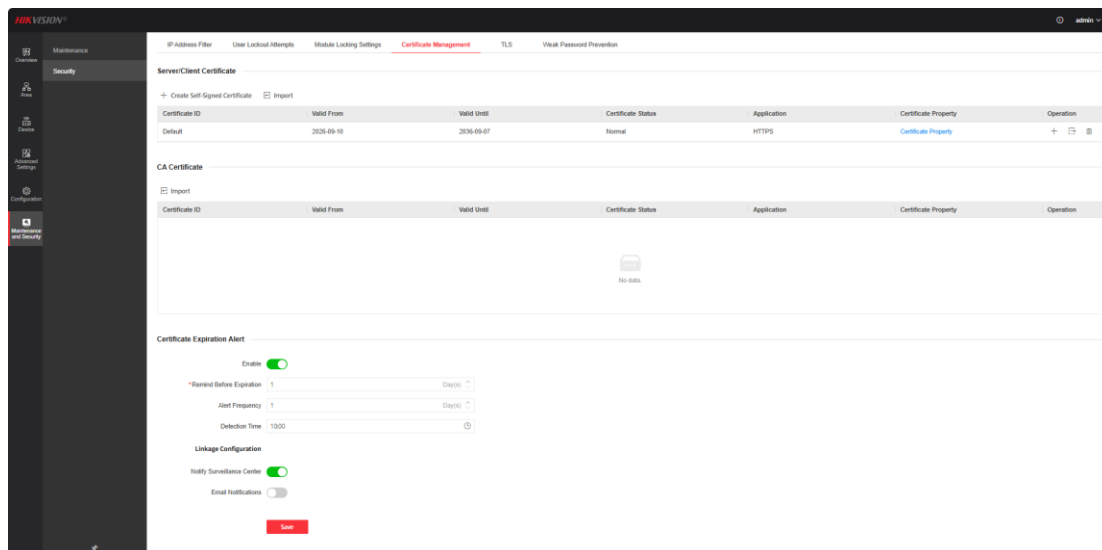


Figure 76 Certificate Management

4.4.1 Certificate Operations

- Click the “**Create Self-Signed Certificate**” button and enter valid certificate information to create a Self-Signed Certificate.

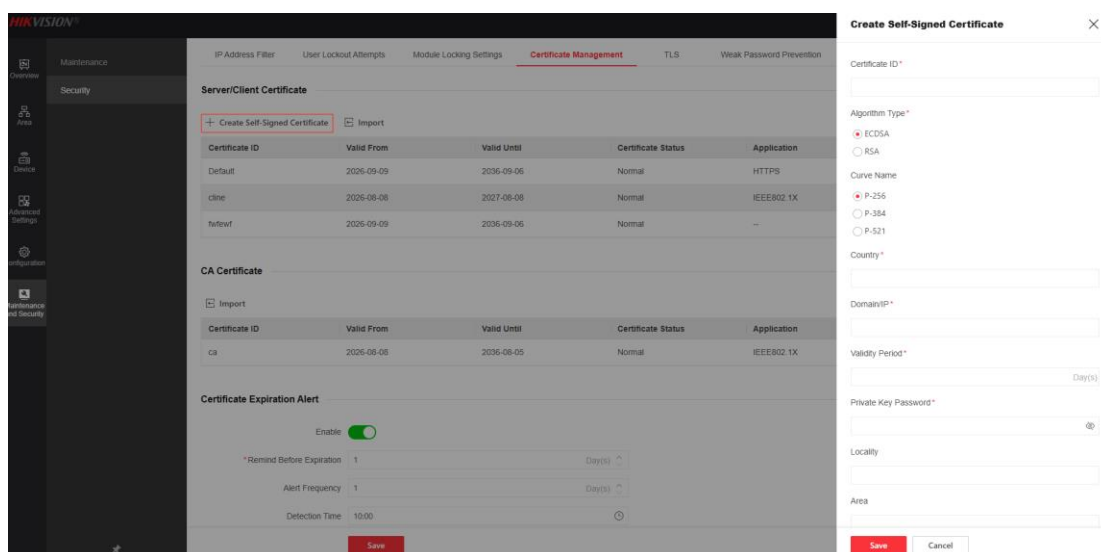


Figure 77 Create Self-Signed Certificate

- Click the “**Import**” button under the Server/Client Certificate page to import the Server/Client Certificate. If a private key file is imported, the private key file must be encrypted before import, and the corresponding password must be entered.

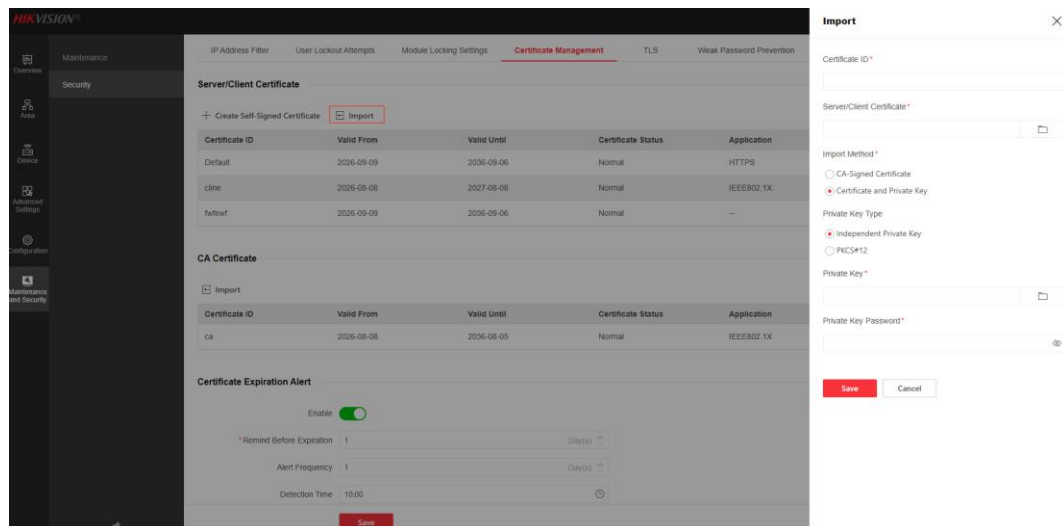


Figure 78 Import Server/Client Certificate

- Click the **“Export”** button in the certificate-related row to export the Server/Client Certificate.

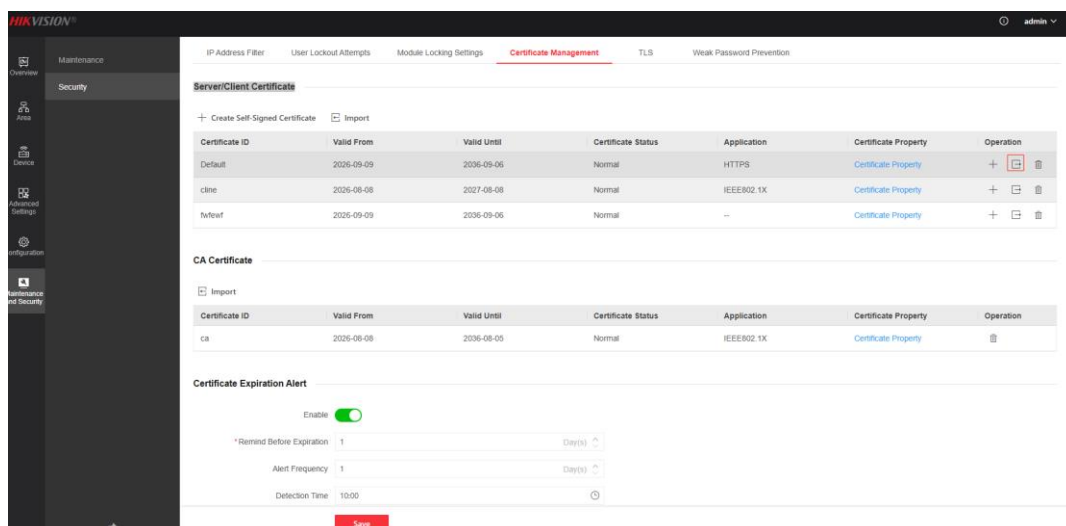


Figure 79 Export Server/Client Certificate

- Click the **“Import”** button on the CA Certificate page to import the CA Certificate.

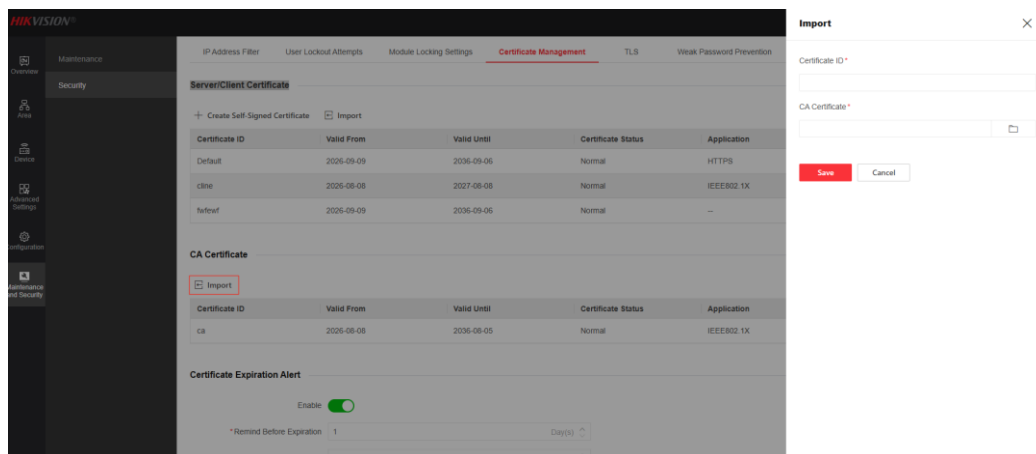


Figure 80 Import CA Certificate

- Click the “Delete” button in the row of the certificate to delete the relevant certificate. If the certificate is bound to services in the Application column, it must be unbound before deletion.

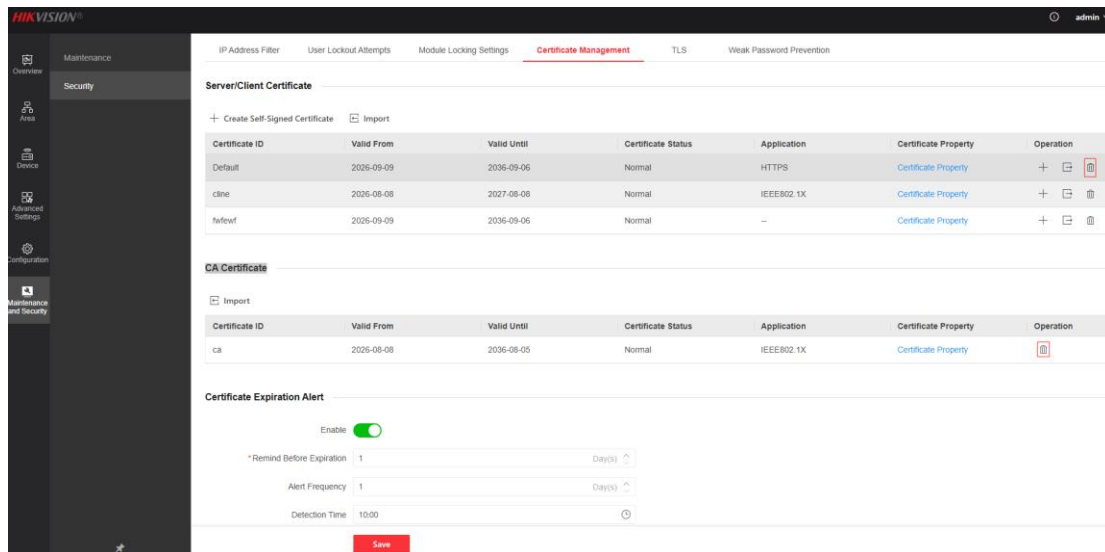


Figure 81 Delete Certificate

- Certificate binding, refer to the certificate binding function on each service page.

4.4.2 Certificate Interlock Alarm

Support Interlock of the host alarm when the certificate is abnormal, close to expiration, or has expired.

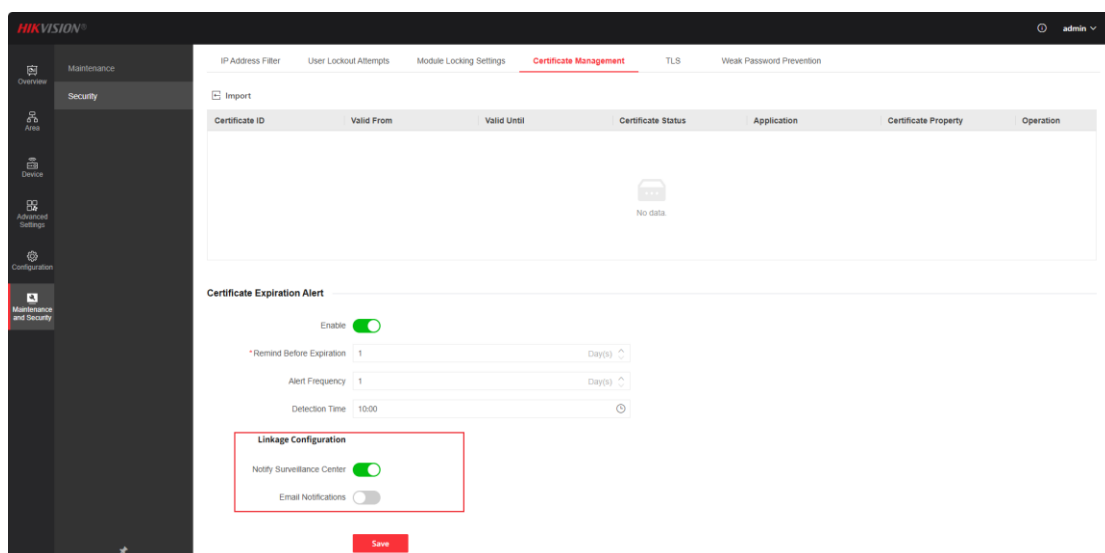


Figure 82 Certificate Linkage Configuration

- After Notify Surveillance Center is enabled, the host records certificate expiration warnings, expired certificate anomalies, and pushes CID reports. This configuration is

enabled by default.

- When Email Notifications are enabled, the system sends emails to the linked email address to alert the user when a certificate is abnormal, nearing expiration, or has expired. This configuration is disabled by default. The email format is as follows:

Subject:

Device Name: Cert Expiring Soon/Cert Expired/Cert Abnormal

Main text:

CERT ID: xxx

STATUS: Expiring Soon, xxx day(s) remaining /Expired xxx day(s)/Abnormal

AFFECTED FUNCTION: HTTPS/WebSocketS/SDK_OVER_TLS/SRTP/securitylog/
IEEE802.1X/WPA/SIP/ISUP_OVER_TLS/OTAP_OVER_TLS/EMAIL/FTPS/EZVIZ/DDNS/
OTA_UPGRADE/DC09

HOST NAME: xxx

HOST S/N: xxx

4.5 Security Management

The safety functions provided by the equipment itself enhance its inherent safety capabilities, but effective management of the equipment's use and configuration is essential to fully utilize these security features. The following are some basic requirements for managing the security of the alarm host:

(1) Follow basic information system security principles when configuring the alarm host, including the principle of least privilege, the principle of separation of duties, the principle of security isolation, etc.

(2) Develop safety regulations, processes, operating procedures, and record forms related to the use of the alarm host to standardize operations and record all activities.

(3) Regularly perform security scans, configuration verification, and penetration testing to evaluate the security level of all devices on the network, identify potential security risks, assess these risks, and develop remediation plans.

(4) Implement improvements based on the safety assessment results and remediation plan, and monitor the effectiveness of these improvements.

(5) 7×24-hour continuous monitoring of network anomalies and threat information, including the availability status of systems and networks, malware detection, and intrusion detection.

(6) Regularly conduct security audits of network information systems, optimize the configuration of security devices and the devices themselves based on audit findings, and

further enhance device security.

(7) Establish a network security emergency response mechanism, develop contingency plans and procedures, and regularly conduct emergency drills to verify and improve the current response mechanisms and plans.

(8) Provide comprehensive safety awareness training and assess the professional skills of personnel managing various equipment and alarm host users.