NVR4XXX-4KS2L_MultiLang_V4.000.0000001.0.R

Release Notes

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Legal Information

Copyright

Trademarks




, , , and are the trademarks or registered trademarks of Dahua.

All other company names and trademarks mentioned herein are the properties of their respective owners.

Disclaimer

- These release notes are for reference only, and the actual product shall prevail.
- Succeeding products and release notes are subject to change without notice.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1.1 Overview

Item	Description
Product model	NVR4XXX-4KS2/L Series
Version	V4.000.0000001.0
Software package information	DH_NVR4XXX-4KS2L_MultiLang_V4.000.0000001.0.R.191129.zip
Onvif Version	2.4.1
OS requirement	None
Release date	11/29/2019

1.2 New Features

Feature	Description
SMD function	① Support configuring SMD functions on IP cameras, such as enable switch, sensitivity and effective target. ② Support SMD alarm event, reusing MD alarm configuration. ③ Support filtered query and playback for human and vehicle. ④ Support displaying SMD rectangle on human and vehicle in live view. ⑤ Support displaying SMD rectangle on human and vehicle in playback. ⑥ Search and export SMD events. ⑦ Modified SMD playback start point to start from 10s ahead of the recorded video.
Security	① You can set security options to strengthen device security and use the device in a much safer way. ② Security Status, Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information about the security status of the device ③ System Service ,You can set NVR basic information such as basic services, 802.1x and HTTPS ④ Attack Defense ⑤ CA Certificate ⑥ Audio/Video Encryption ⑦ Security Warning

1.3 Fixed Bugs

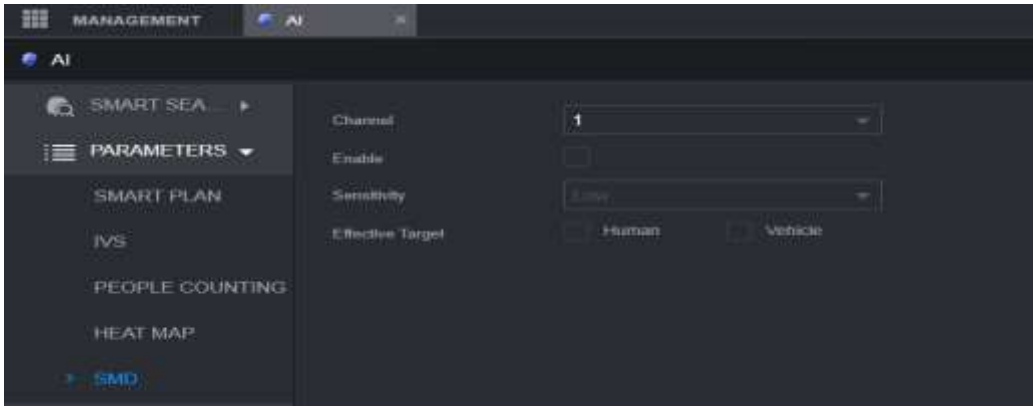
None.

1.4 Instructions for New Features

1.4.1 SMD Function

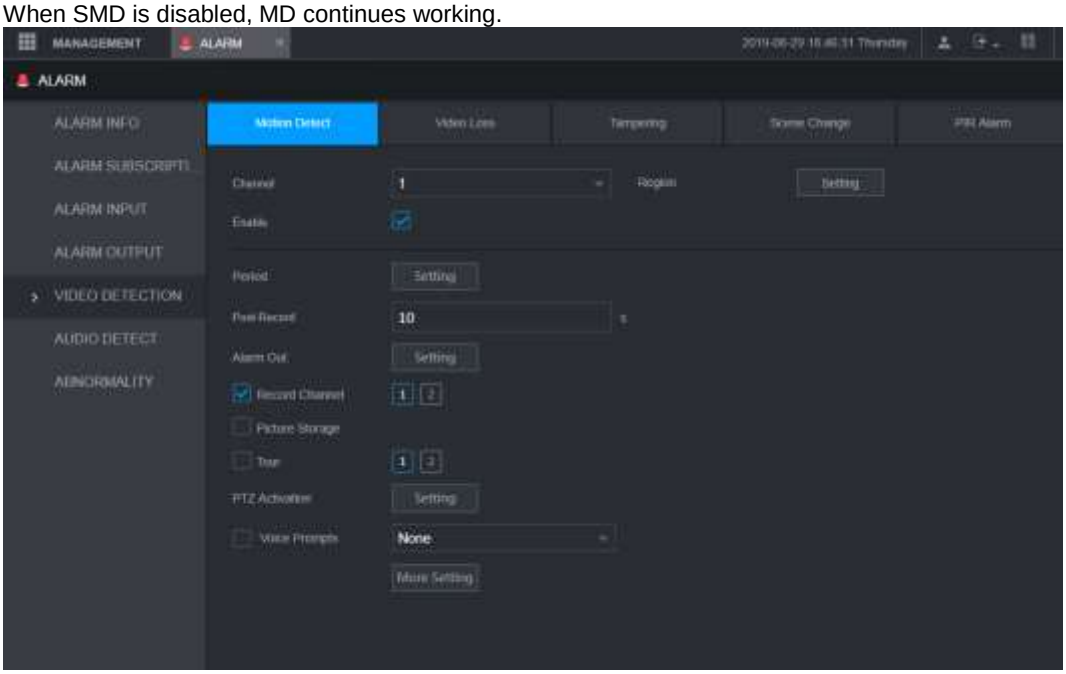
MD (motion detection) has a problem of false alarms, the change of brightness, shaking of leaves or the device, or a rain will trigger a motion detection alarm. Based on the MD function, SMD (Small Motion Detection) is aimed to improve the practical value of motion detection by intelligently analyzing and distinguishing human and vehicle in videos. Alarm event will be triggered only when human or vehicle is detected.

SMD Configuration: Includes enable switch, sensitivity and effective target.



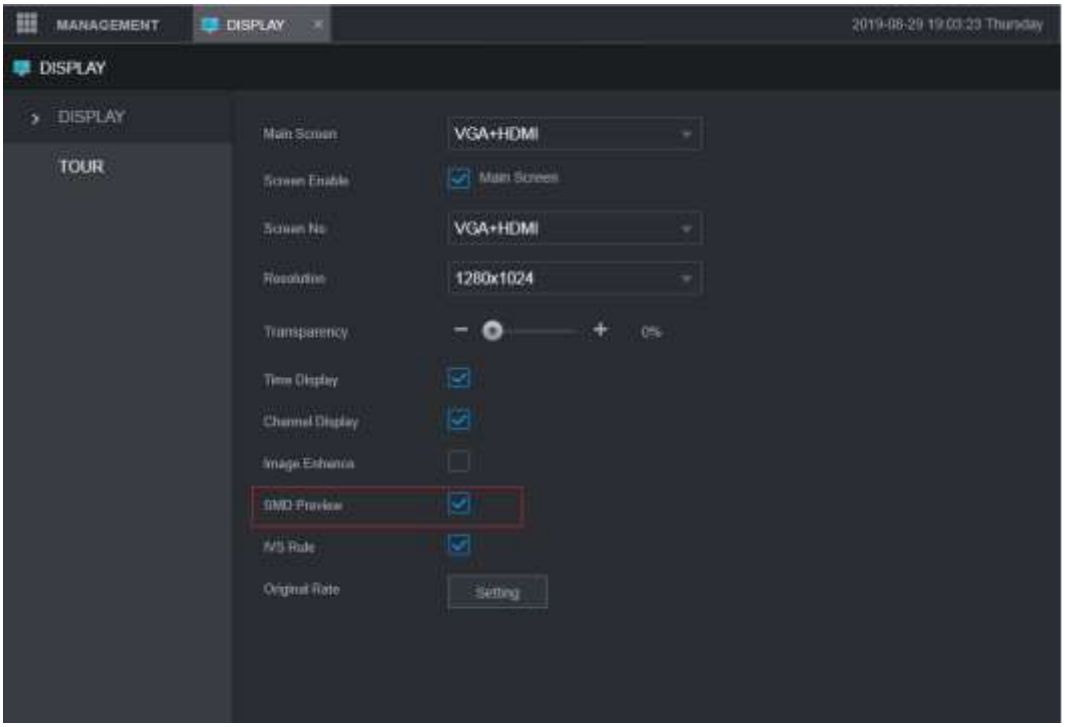
SMD alarm configuration

- SMD reuses alarm configuration of MD.
- When SMD is enabled, MD will be enabled synchronously and its alarm configuration will be applied to SMD.
- When MD is disabled, SMD will be disabled synchronously.
- When SMD is disabled, MD continues working.

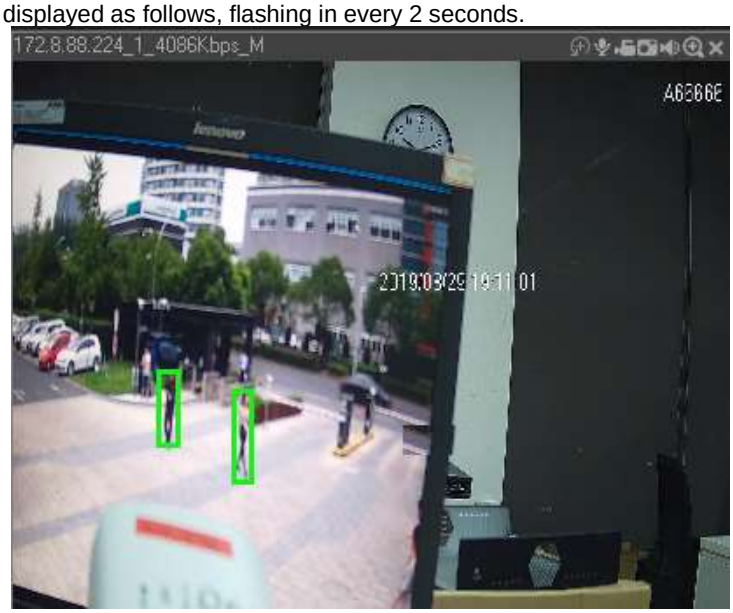


SMD rectangle displayed on human and vehicle

You can enable **SMD Preview** on **Display** interface to display SDM rectangle on human and vehicle.

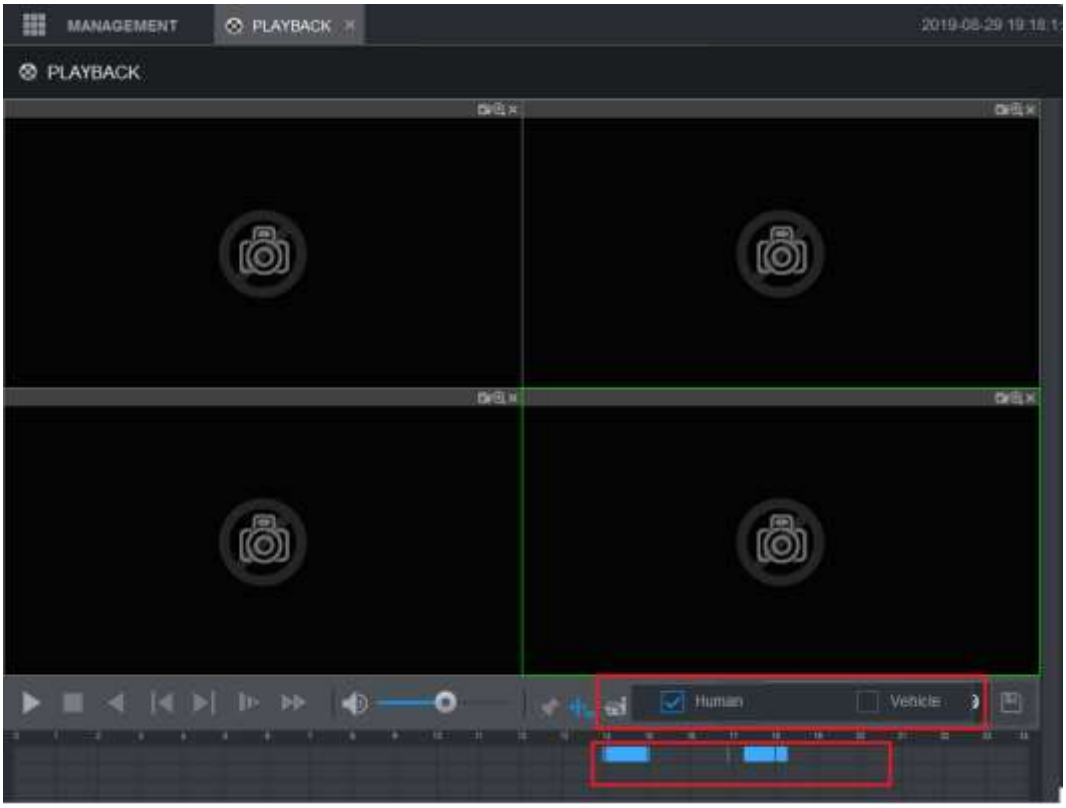


SMD rectangles are displayed as follows, flashing in every 2 seconds.



Filtered query and playback for human and vehicle

- Query files are displayed in the color of blue.
- Enable switch reuses the switch of smart rules.
- Video playback by filtered result.

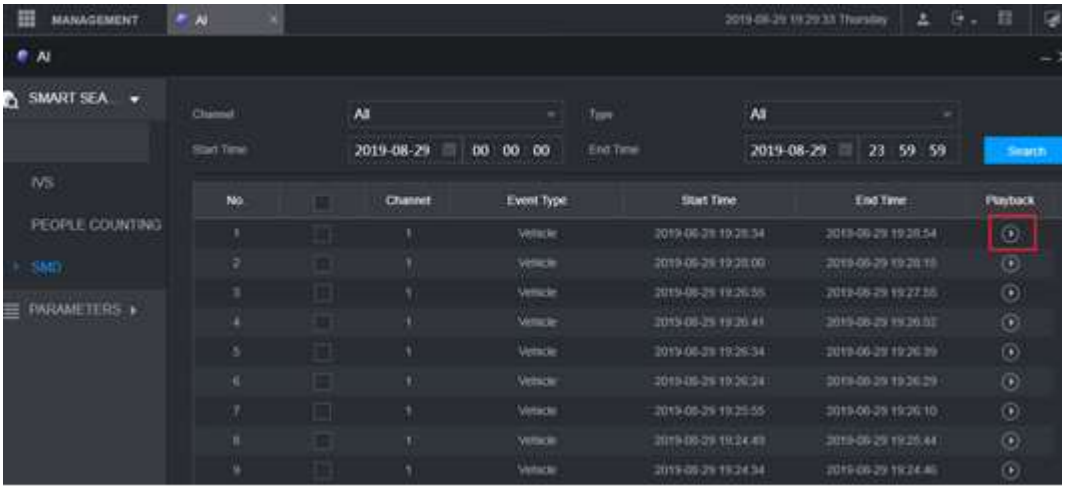


SMD search on AI interface

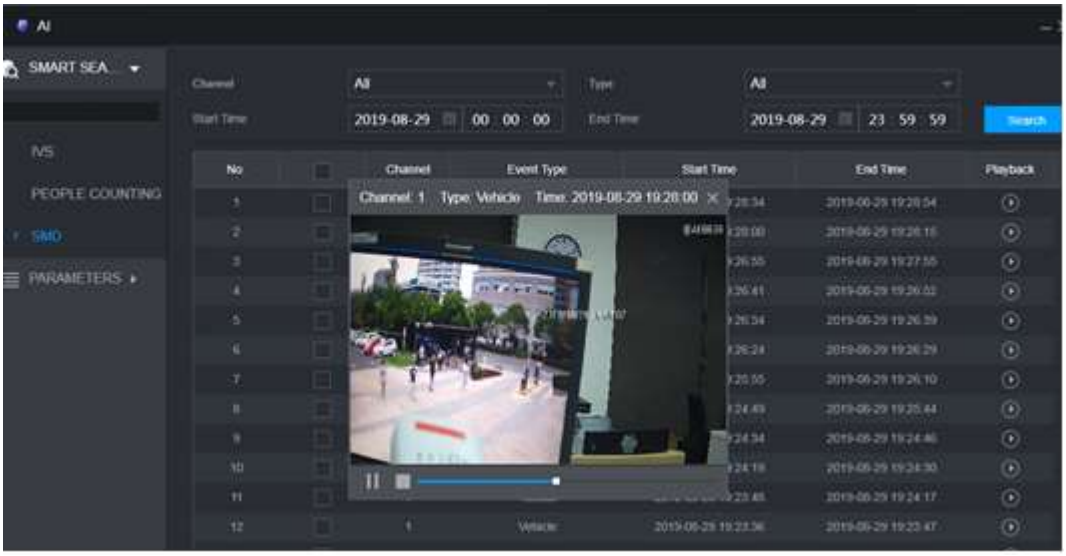
You can search for SDM event on the **AI** interface by time, channel, human and vehicle.

SMD playback on AI interface

You can directly play videos in **Playback** column from start time to end time by filtered results.



Cilck , and then a player will be prompted to play video.



1.4.2 Security

You can set security options to strengthen device security and use the device in a much safer way.

Security Status

Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information about the security status of the device.

Detecting User and Service

Green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

- Login authentication: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.
- User Status: When one of device users or Onvif users uses weak password, the icon will be in orange to warn risk. You can click **Details** to optimize or ignore the risk warning.

Figure 1 Security status

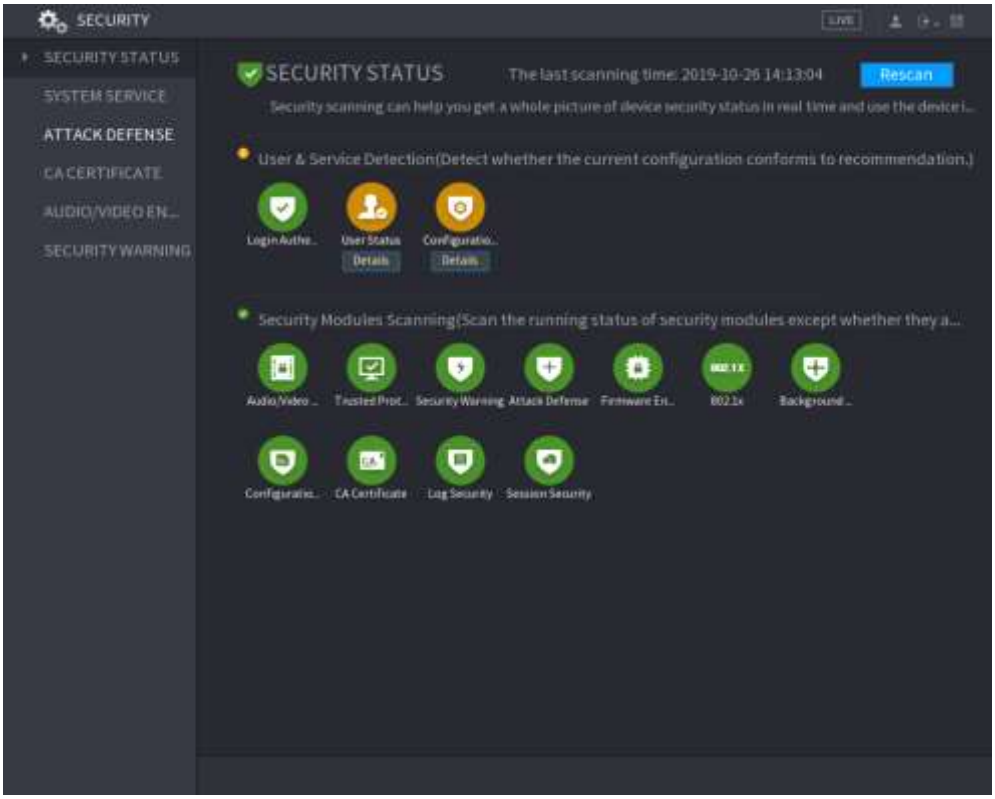
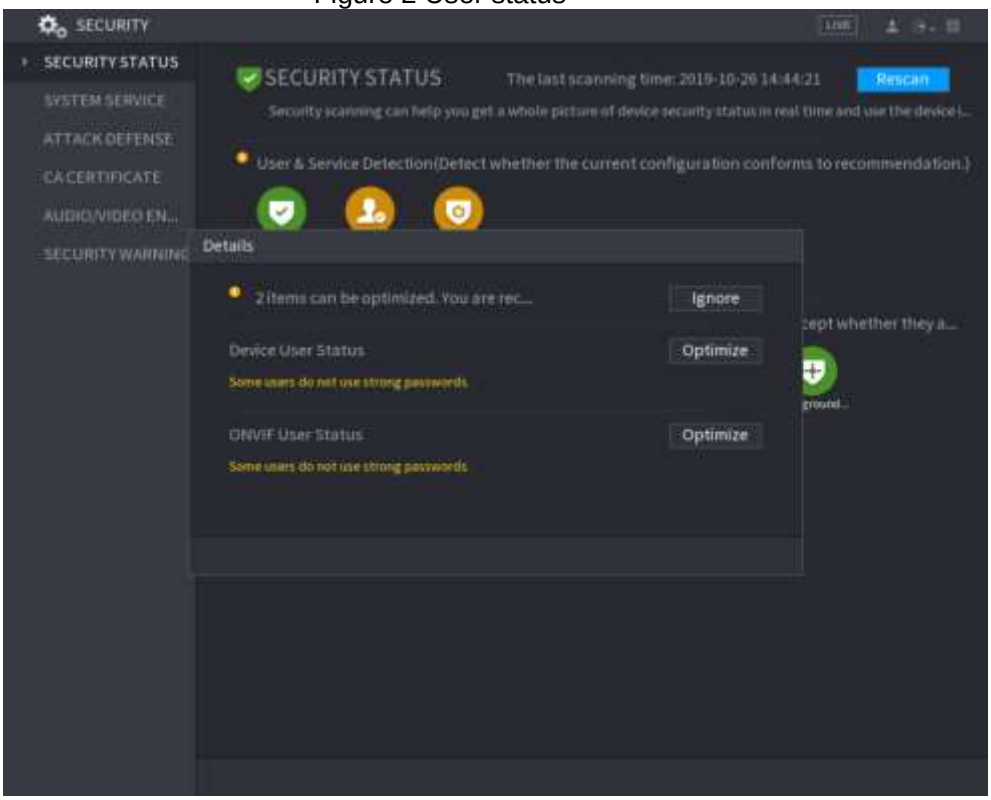
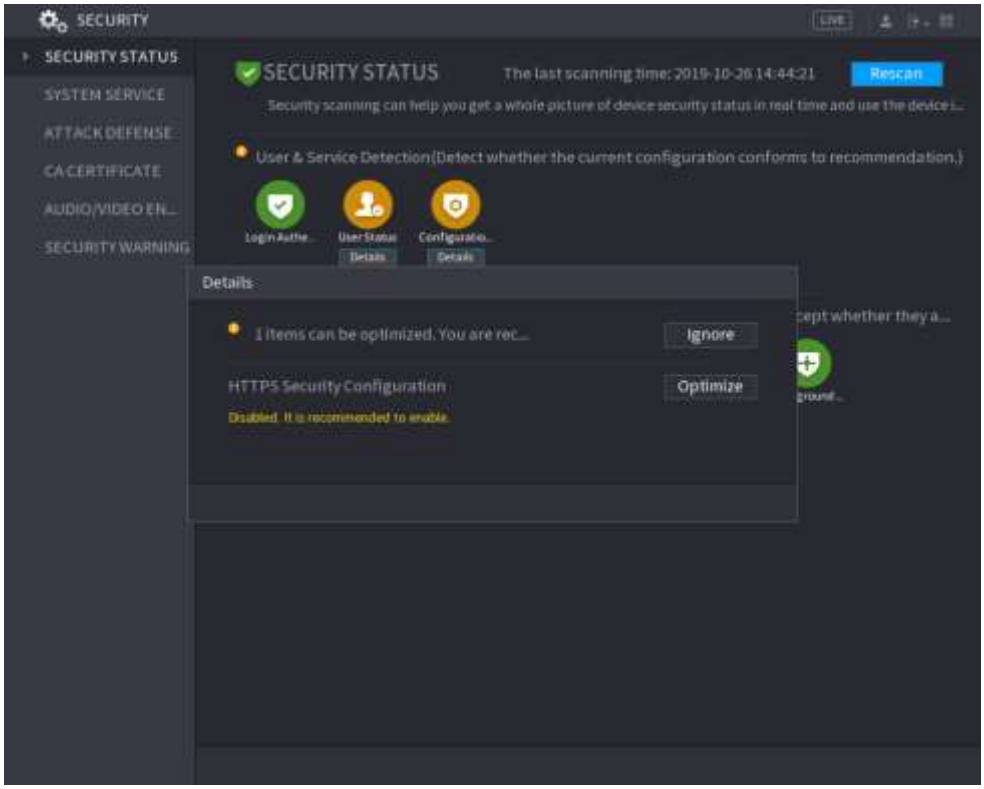


Figure 2 User status



- Configuration Security: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description. See Figure 3.

Figure 3 Configuration security



Scanning Security Modules

This area shows the running status of security modules. For details about the security modules, move mouse pointer on the icon to see the on-screen instructions.

Scanning Security Status

You can click **Rescan** to scan security status.

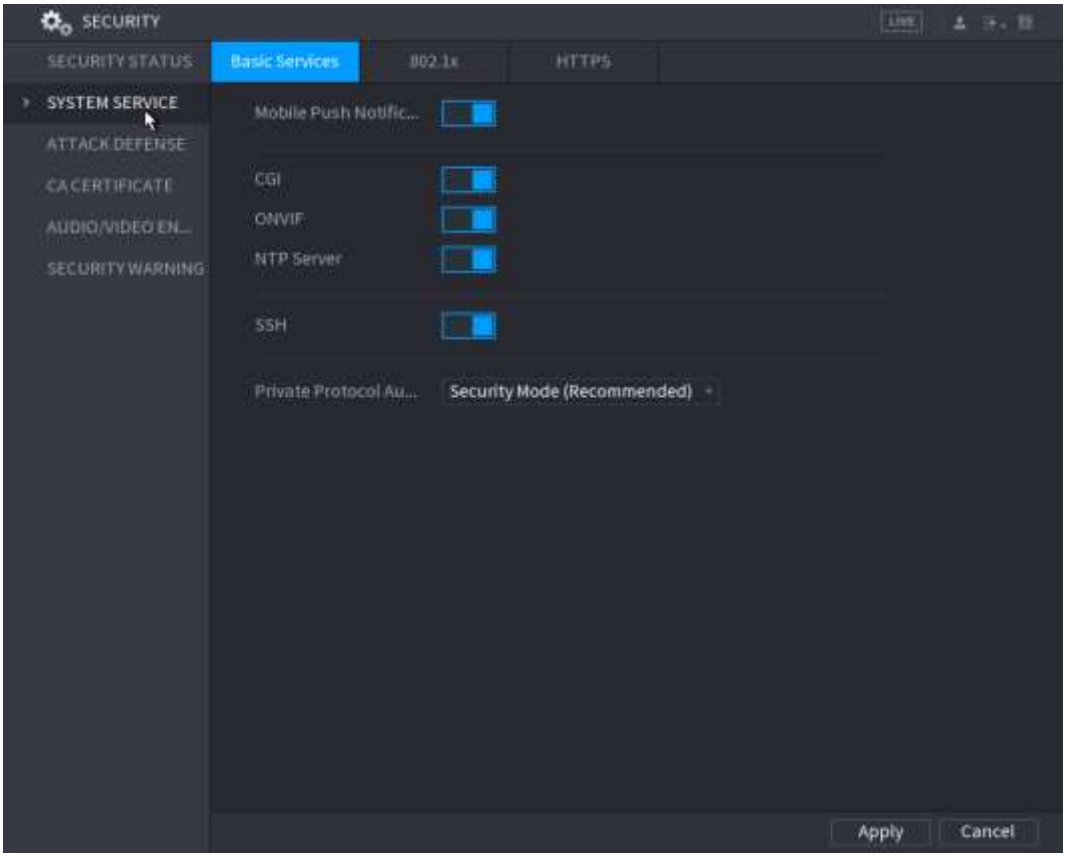
System Service

You can set NVR basic information such as basic services, 802.1x and HTTPS.

Basic Services

Step 1 Select **Main Menu** > **SECURITY** > **SYSTEM SERVICE** > **Basic Services**.
The **Basic Services** interface is displayed. See Figure 0.

Figure 0 Basic services interface



Step 2 Select **Basic Services** and configure parameters.

There might be safety risk when **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** is enabled.

Table 1 Basic service parameters

Parameter	Description
Mobile Push Notifications	After enabling this function, the alarm triggered by the NVR can be pushed to a mobile phone. This function is enabled by default.
CGI	If this function is enabled, the remote devices can be added through the CGI protocol. This function is enable by default.
ONVIF	If this function is enabled, the remote devices can be added through the ONVIF protocol. This function is enabled by default.
NTP Server	After enabling this function, a NTP server can be used to synchronize the device. This function is enabled by default.
SSH	After enabling this function, you can use SSH service. This function is disabled by default.
Private Protocol Authentication Mode	● Security Mode (Recommended): Uses Digest access authentication when connecting to NVR. ● Compatible Mode: Select this mode when the client does not support Digest access authentication.

Step 3 Click **Apply** to complete the settings.

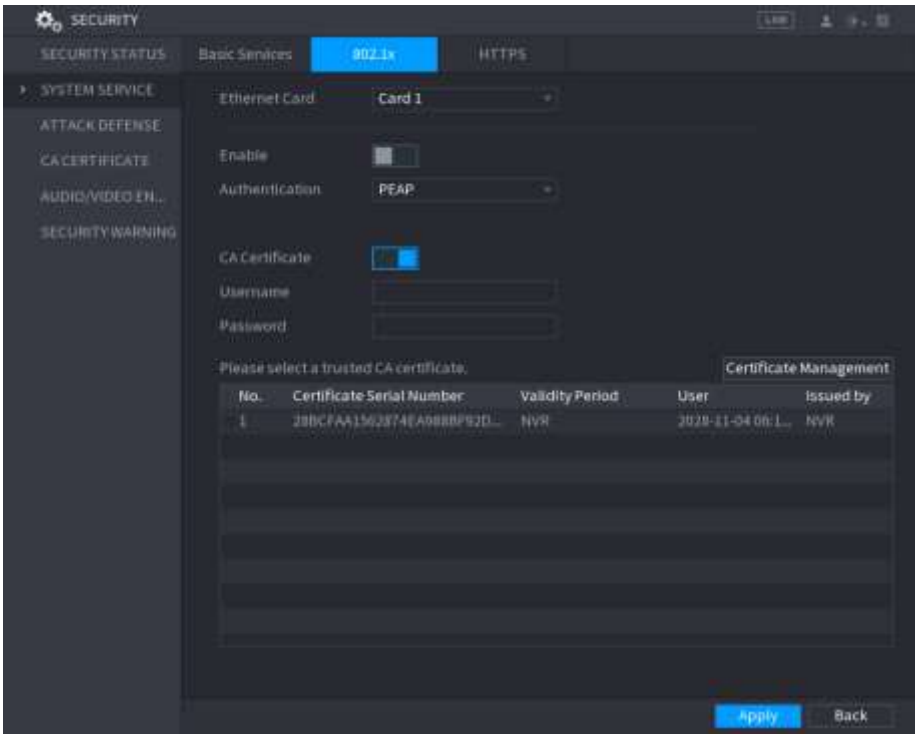
802.1x

The device needs to pass 802.1x certification to enter the LAN.

Step 1 Select **Main Menu** > **SECURITY** > **SYSTEM SERVICE** > **802.1x**.

The **802.1x** interface is displayed. See Figure .

Figure 5 802.1x interface



Step 2 Select the Ethernet card you want to certify.

Step 3 Select **Enable** and configure parameters. See Table .

Table 2 802.1x parameters

Parameter	Description
Authentication	• PEAP: protected EAP protocol. • TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click **Browse** to import CA certificate from flash drive. For details about importing and creating a certificate, see CA Certificate.
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

Step 4 Click **Apply** to complete the settings.

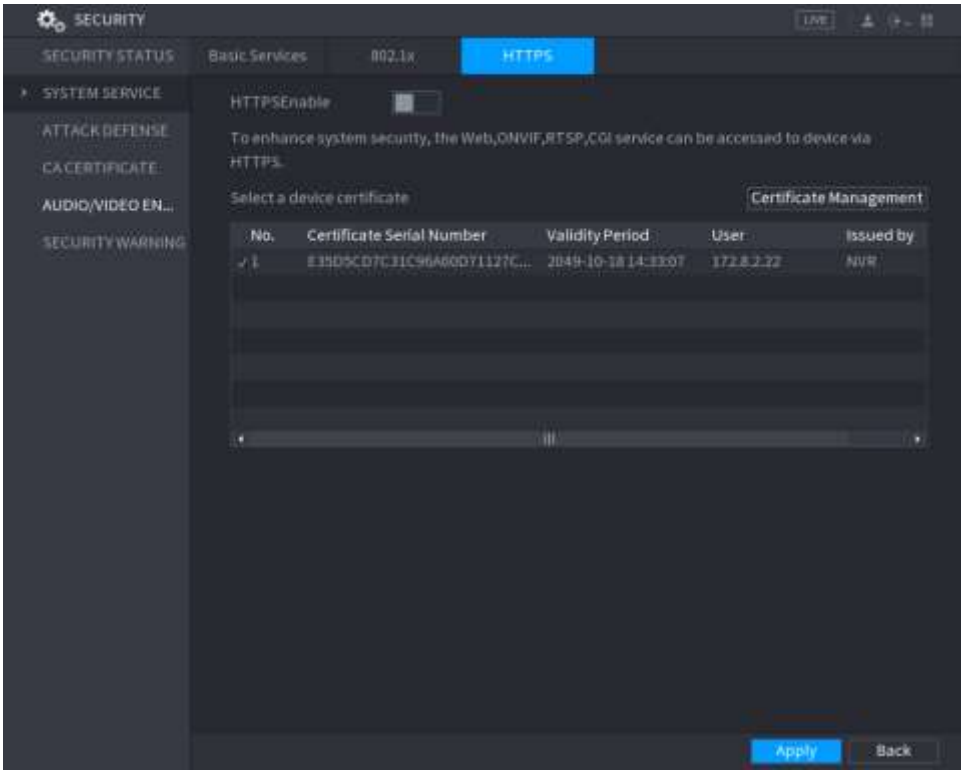
HTTPS

We recommend that you enable HTTPS function to enhance system security.

Step 1 Select **Main Menu** > **SECURITY** > **SYSTEM SERVICE** > **HTTPS**.

The **HTTPS** interface is displayed. SeeFigure .

Figure 6 HTTPS interface



Step 2 Select **HTTPSEnable** to enable HTTPS function.

Step 3 Click **Certificate Management** to create or import a HTTPS certificate from USB drive.

For details about importing or creating a CA certificate, see CA Certificate.

Step 4 Select a HTTPS certificate.

Step 5 Click **Apply** to complete the settings.

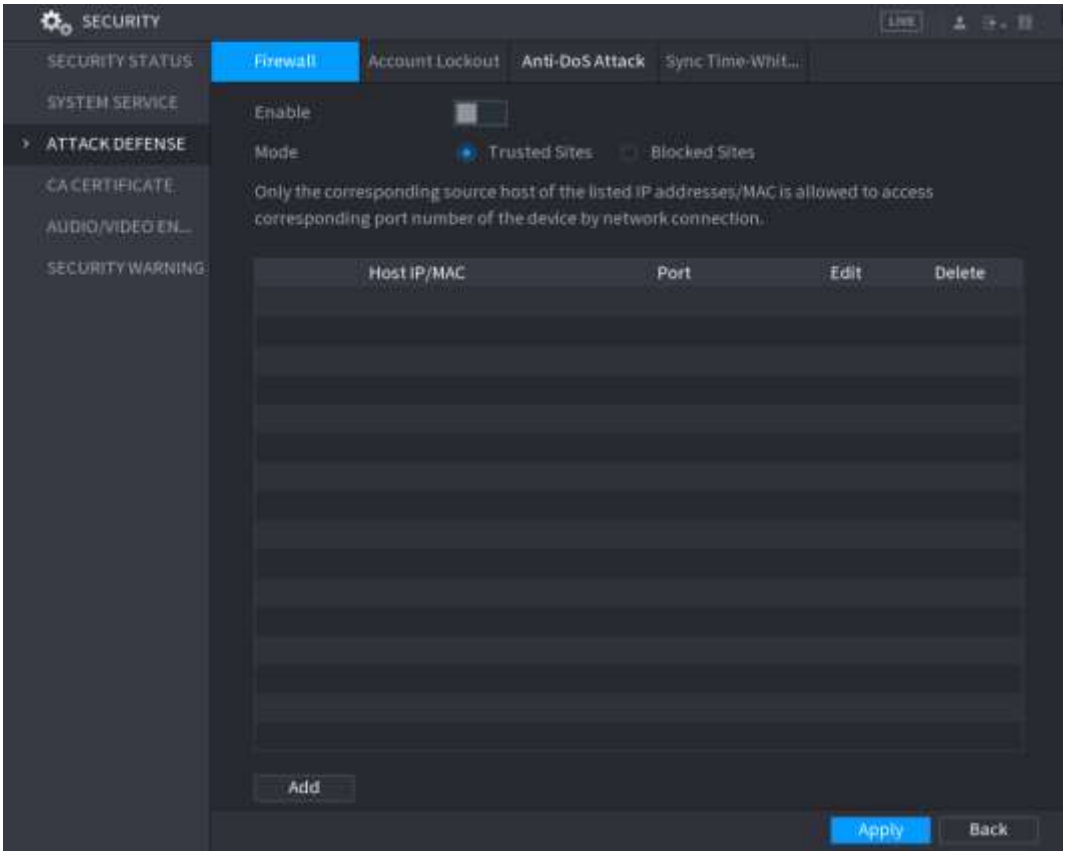
Attack Defense

Firewall

Step 1 Select **Main Menu** > **SECURITY** > **ATTACK DEFENSE** > **Firewall**.

The **HTTPS** interface is displayed. See Figure .

Figure 7 Firewall interface



Step 2 Select **Enable** to enable firewall.

Step 3 Configure the parameters. See Table ..

Table 3 Firewall parameters

Parameter	Description
Mode	Mode can be configured when Type is Network Access. ● If Trusted Sites is enabled, you can visit device port successfully with IP/MAC hosts in Trusted Sites. ● If Blocked Sites is enabled, you cannot visit device port with IP/MAC hosts in Blocked Sites.
Add	When Type is Network Access, you can configure IP Address, IP Segment and MAC Address.
Type	You can select IP address, IP segment and MAC address.
IP Address	Enter IP Address, Start Port and End Port that is allowed or forbidden. When Type is IP Address, they can be configured. Start Port and End Port can be configured only in Network Access Type.
Start Port	
End Port	
Start Address/End Address	Enter Start Address and End Address of IP Segment. When Type is IP Segment, they can be configured.
MAC Address	Enter MAC Address that is allowed or forbidden When Type is MAC Address, it can be configured.

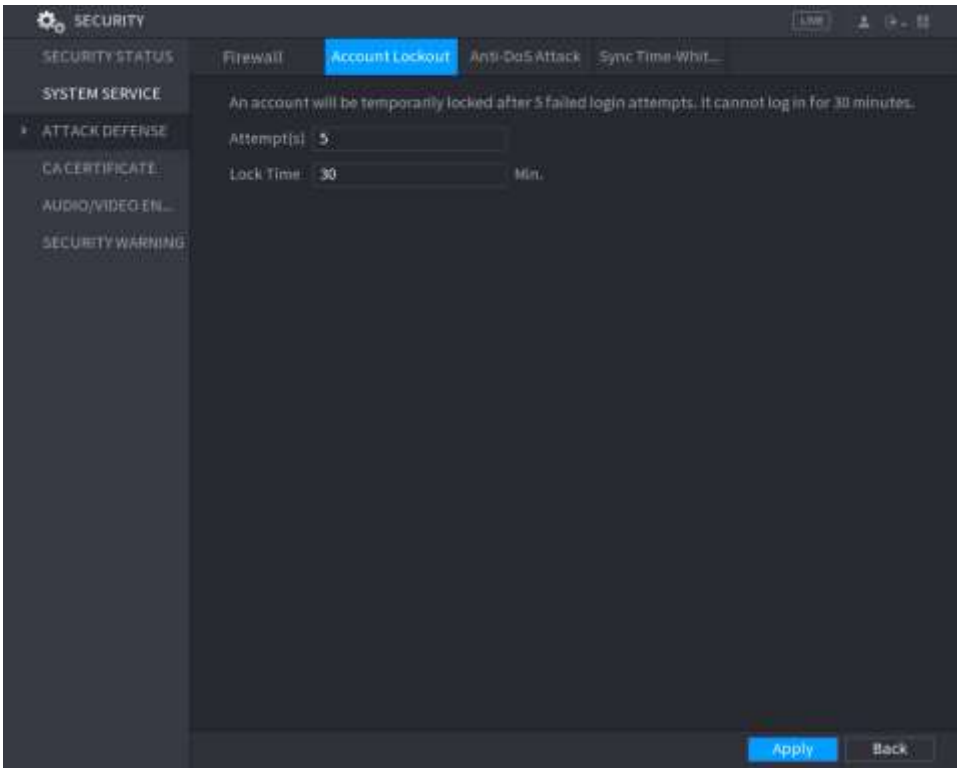
Step 4 Click **Apply** to complete the settings.

Account Lockout

Step 1 Select **Main Menu** > **SECURITY** > **ATTACK DEFENSE** > **Account Lockout**.

The **Account Lockout** interface is displayed. See Figure .

Figure 8 Account Lockout



Step 2 Set parameters. See Table .

Table 4 Account lockout parameters

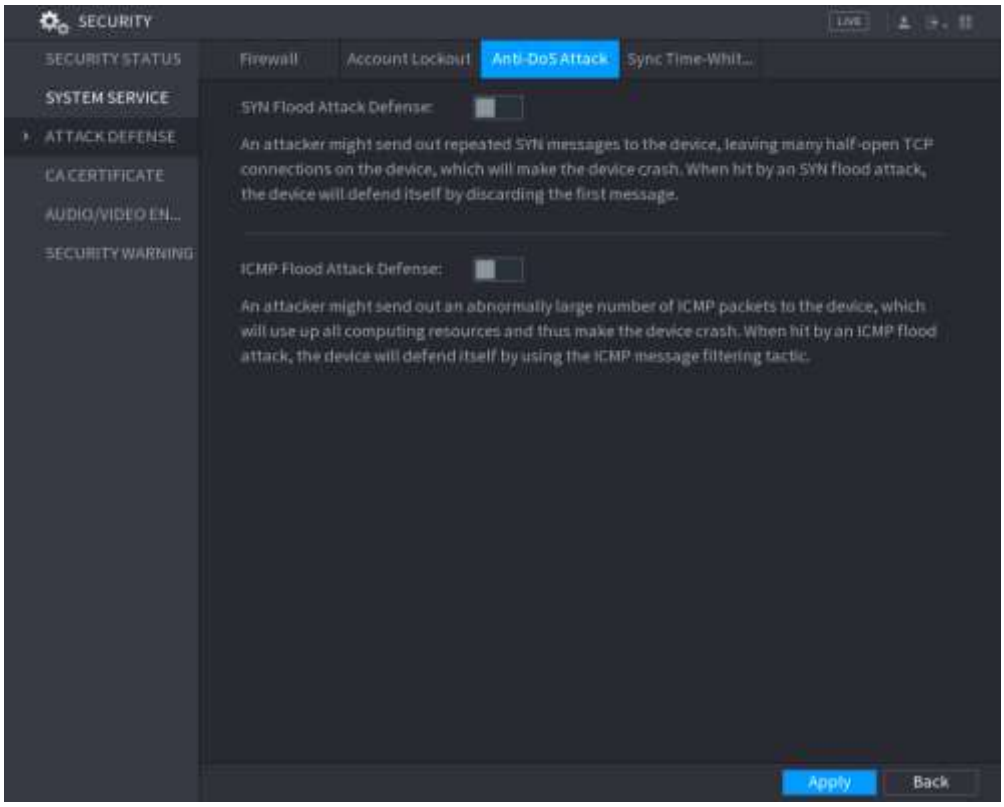
Parameter	Description
Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number. Value range: 5–30. Default value: 5.
Lock Time	Set how long the account is locked for. Value range: 5–120 minuites. Default value: 30 minutes.

Step 3 Click **Apply** to complete the settings.

Anti-Dos Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against Dos attack. See Figure .

Figure 9 Anti-Dos attack interface



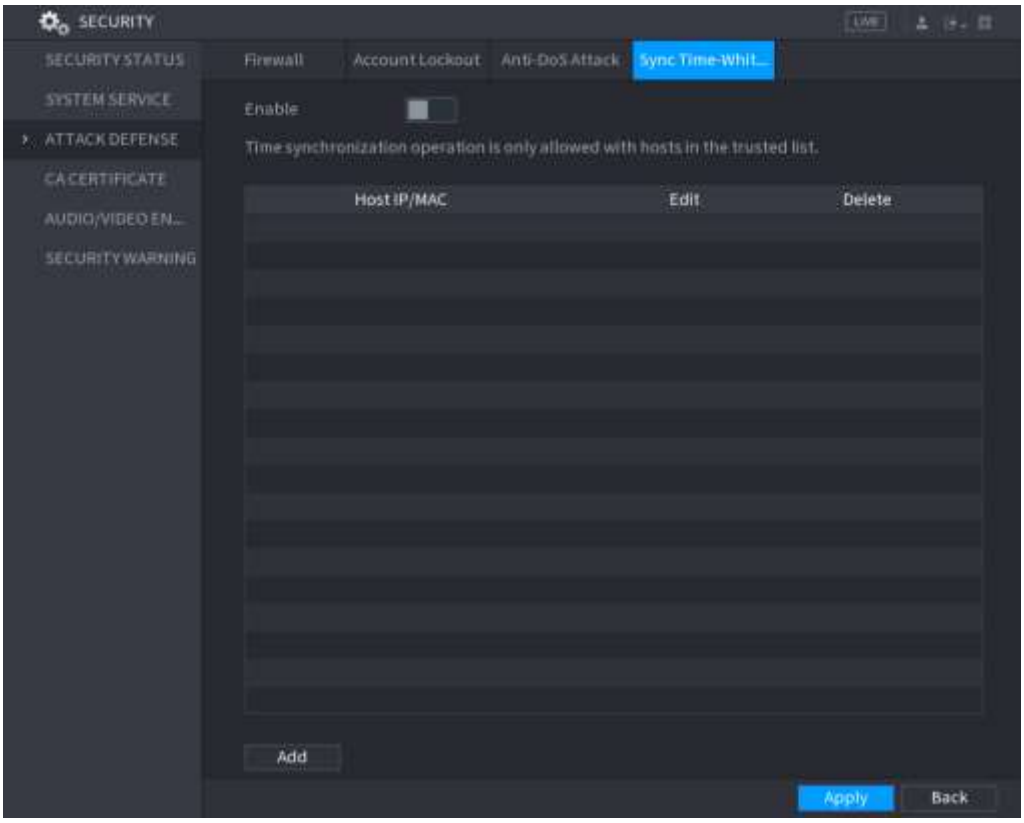
Sync Time-Whitelist

The synchronization is only allowed with hosts in the trusted list.

Step 1 Select **Main Menu** > **SECURITY** > **ATTACK DEFENSE** > **Sync Time-Whitelist**.

The **Sync Time-Whitelist** interface is displayed. See Figure .

Figure 10 Sync Time-Whitelist



Step 2 Select **Enable** to enable **Sync Time-Whitelist** function.

Step 3 Configure the parameters. See Table .

Table 5 Sync Time-Whitelist parameters

Parameter	Description
Add	You can add trusted hosts for time synchronization.
Type	Select IP address or IP segment for hosts to be added.
IP Address	Input the IP address of a trusted host. When Type is IP Address, it can be configured
Start Address	Input the start IP address of trusted hosts. When Type is IP Segment, it can be configured
End Address	Input the end IP address of trusted hosts. When Type is IP Segment, it can be configured

Step 4 Click **Apply** to complete the settings.

CA Certificate

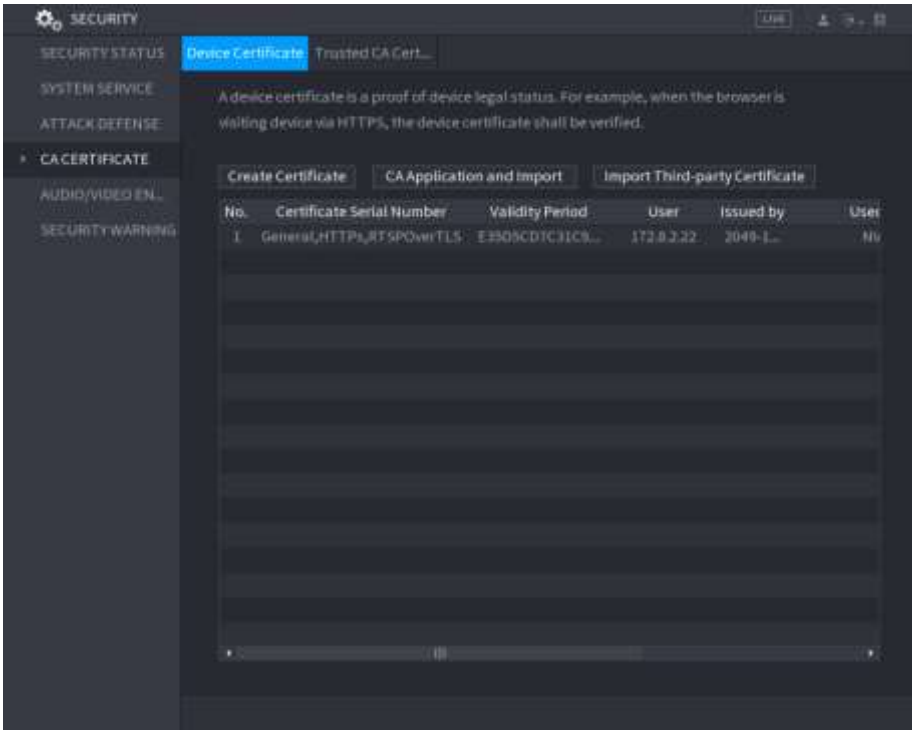
You can create or import device certificate and install trusted CA Certificate.

Device Certificate

Create Certificate

1. Select **Main Menu** > **SECURITY** > **CA CERTIFICATE** > **Device Certificate**.
   The **Device Certificate** interface is displayed. See Figure .

Figure 11 Device Certificate



2. Configure parameters. See Table .

Table 6 Creating Certificate

Parameter	Description
County	This parameter is user defined.

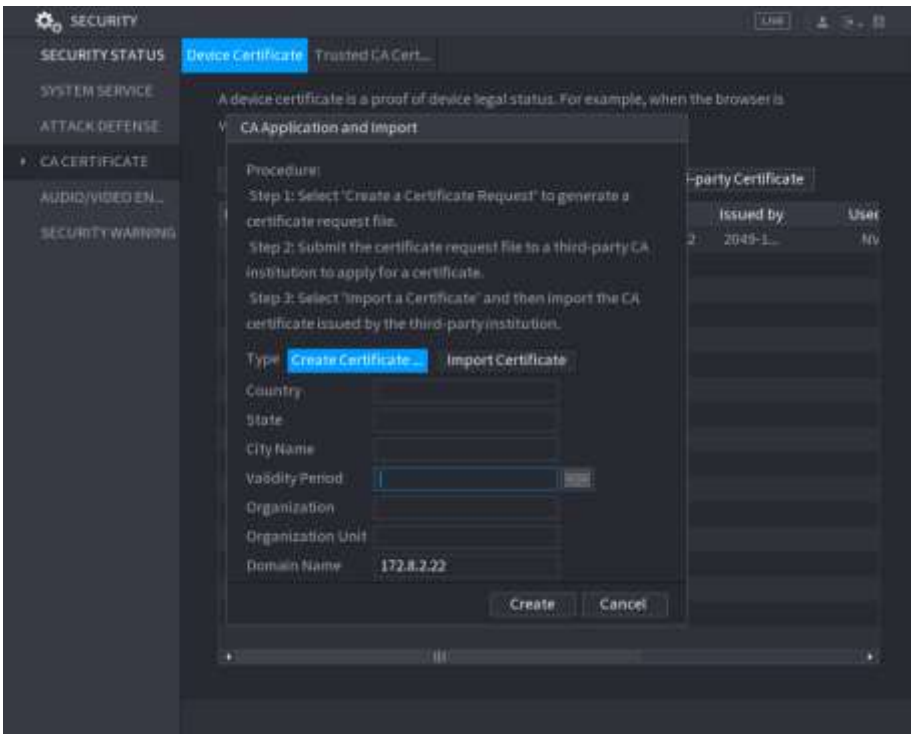
Parameter	Description
State	This parameter is user defined.
City Name	This parameter is user defined.
Valid Period	Input a valid period for the certificate.
Organization	This parameter is user defined.
Organization Unit	This parameter is user defined.
Domain Name	Input the IP address of the certificate.

3. Click **Create**.

CA Application and Import

Follow the on-screen instructions to finish CA application and import. See Figure ..

Figure 12 CA application and import



Import Third-Party Certificate

Step 1 Select **Import Third-party Certificate**.

Step 2 Configure Parameters. See Table .

Table 7 Importing third-party certificate

Parameter	Description
Path	Click **Browse** to find the third-party certificate path on the USB drive.
Private Key	Click **Browse** to find the third-party certificate private key on the USB drive.
Private Key Password	Input the private key password.

Step 3 Click **Create**.

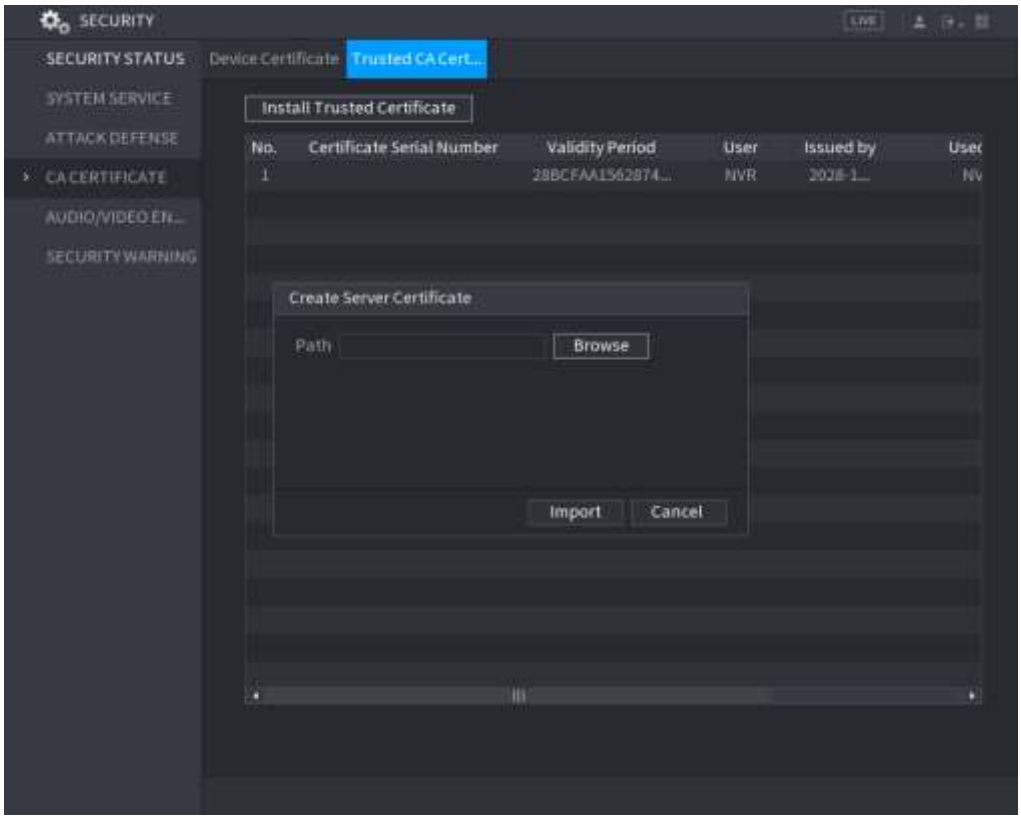
Trusted CA Certificate

Step 1 Select **Main Menu** > **SECURITY** > **CA CERTIFICATE** > **Trusted CA Certificate**.

Step 2 Click **Install Trusted Certificate**.

The **Create Server Certificate** is displayed. See Figure ..

Figure 13 Creating server certificate



Step 3 Click **Browse** to select the certificate that you want to install.

Step 4 Click **Import.**

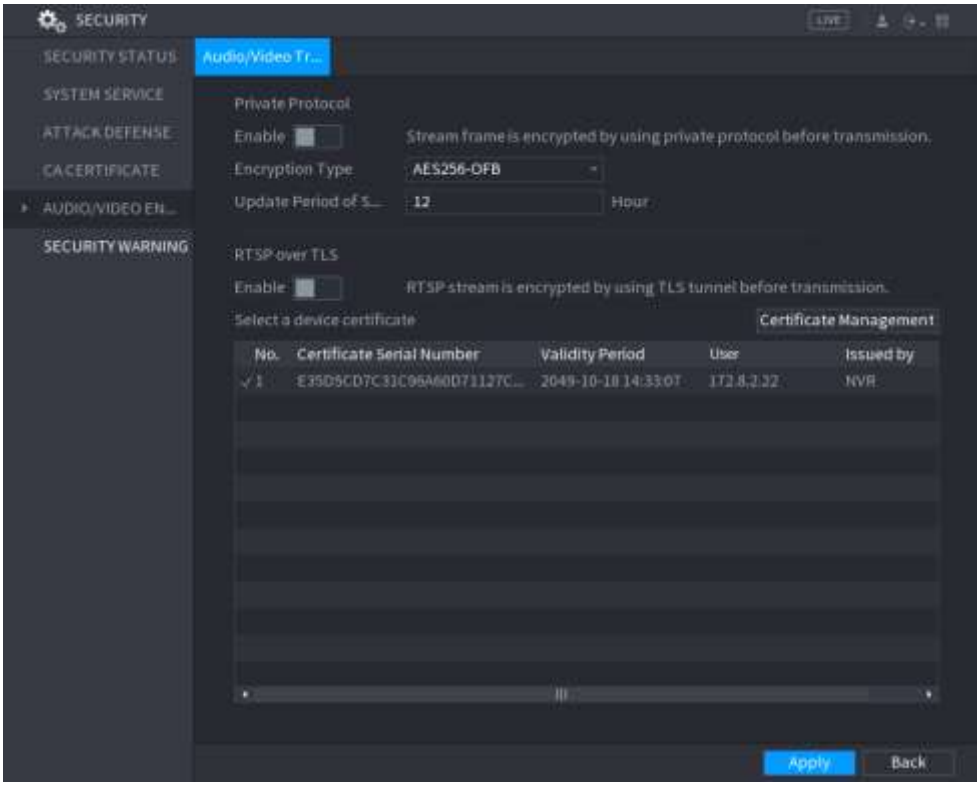
Audio/Video Encryption

The device supports audio and video encryption during data transmission.

Step 1 Select **Main Menu** > **SECURITY** > **AUDIO/VIDEO ENCRYPTION** > **Audio/Video Transmission**.

The **Audio/Video Transmission** interface is displayed. See Figure

Figure 14 Audio and video transmission



Step 2 Configure parameters. See Table .

Table 8 Audio and video transmission parameters

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety vulnerability if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "Device Certificate".

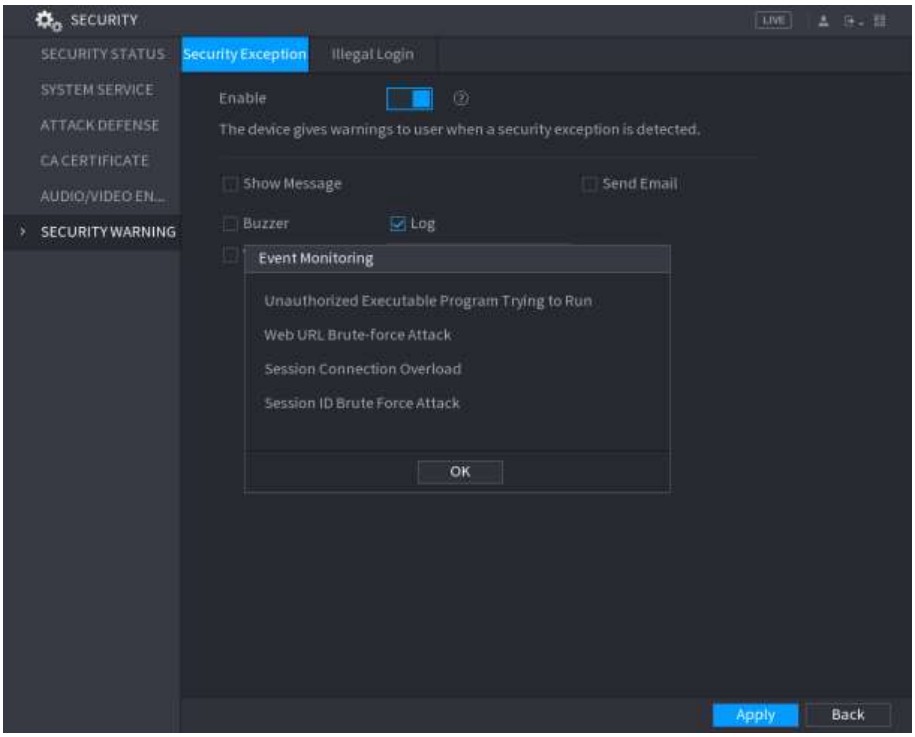
Step 3 Click **Apply** to complete the settings.

Security Warning

Security Exception

Step 1 Select **Main Menu** > **SECURITY** > **SECURITY WARNING** > **Security Exception**.
The **Security Exception** interface is displayed. See Figure 5.

Figure 15 Security Exception



Step 2 Select **Enable** and configure parameters. See Table .

Table 8 Security exception parameters

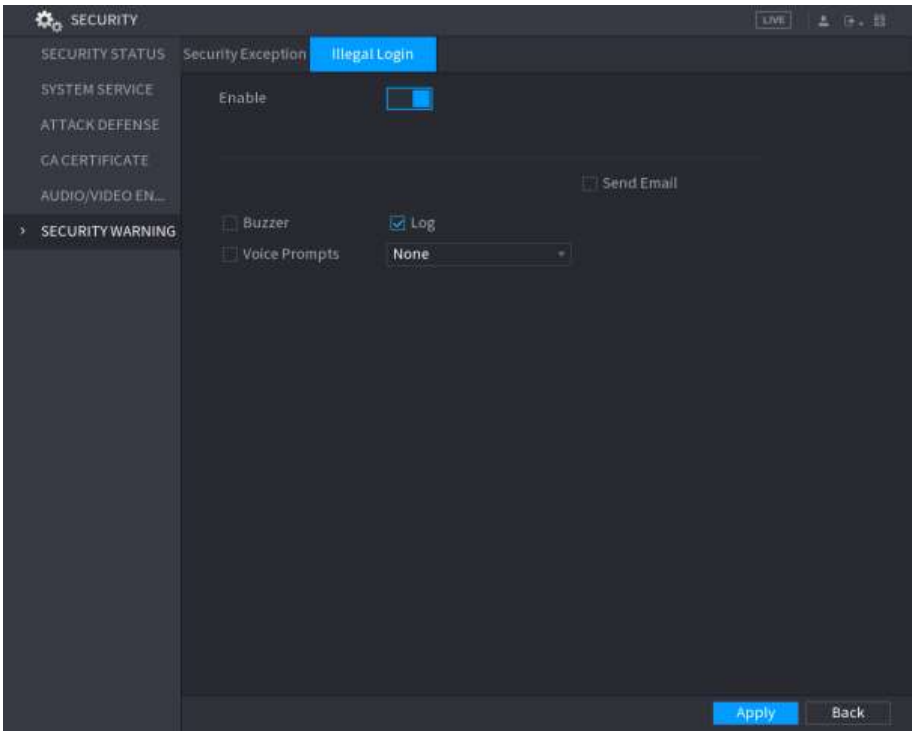
Parameter	Description
Alarm Out	The alarm device (such as lights, sirens, etc.) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.
Latch	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Buzzer	Select the check box to activate the buzzer when an alarm occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. System plays the audio file when the alarm occurs. See "File Manage" to add audio file first.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm occurs.
Send Email	Select the check box. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user. You need to set the email first. For details, see " Email".
⑦	Security Event monitoring explanation. It indicates the type of attacks that can trigger security exception. ● Unauthorized executable program trying to run ● Web URL brute-force attack ● Session connection overload ● Seesion ID brute-force attack

Step 3 Click **Apply** to complete the settings.

Illegal Login

Step 1 Select **Main Menu** > **SECURITY** > **SECURITY WARNING** > **Illegal Login**. The **Illegal Login** interface is displayed. See Figure ..

Figure 16 Illegal login



Step 2 Select **Enable** and configure parameters. See Table .

Table 9 Illegal login parameters

Parameter	Description
Alarm Out	The alarm device (such as lights, sirens) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.
Latch	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds to 300 seconds.
Buzzer	Select the check box to activate the buzzer when an alarm occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. System plays the audio file when the alarm occurs. See " File Manage" to add audio file first.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm occurs.
Send Email	Select the check box. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user. You need to set the email first. For details, see "错误!未找到引用源。".

Click , and then you can visit the web of a remote device to complete normal operations.

1.5 Compatibility

None

1.6 Software Environment

Model	Version
DH-IPC-HFW1230SP-0280B-S2	2.6.01.05.08459: DH_IPC-HX1XXX-Eos4_Eng_P_V2.680.0000000.2.R.190410.zip
DH-IPC-HDBW1831RP-S-0400B	2.6.01.05.06116: DH_IPC-HX2(1)XXX-Sag_EngSpnFrn_PN_V2.622.0000000.18.R.190109.zip
DH-IPC-HFW2230SP-S-0280B-S2	2.6.01.05.10817: DH_IPC-HX2XXX-Mole_MultiLang_PN_V2.800.0000000.1.R.190723.zip
DH-IPC-HFW2231TP-ZAS-27135-S2	2.6.01.05.10817: DH_IPC-HX2XXX-Mole_MultiLang_PN_V2.800.0000000.1.R.190723.zip
DH-IPC-HFW2431TP-ZAS-27135-S2	2.6.01.05.10817: DH_IPC-HX2XXX-Mole_MultiLang_PN_V2.800.0000000.1.R.190723.zip
DH-IPC-HDBW2531RP-ZAS-27135-S2	2.6.01.05.13292: DH_IPC-HX25(8)XX-Mole_MultiLang_PN_V2.800.0000000.4.R.190918.zip
DH-IPC-HFW2831TP-ZAS-27135-S2	2.6.02.05.00694: DH_IPC-HX25(8)XX-Mole_MultiLang_PN_V2.800.0000000.6.R.191023.zip
DH-IPC-HFW3241TP-ZAS-27135	DH_IPC-HX5(4)(3)XXX-Leo_MultiLang_PN_Stream3_V2.800.0000000.3.R.190830.zip
DH-IPC-HFW3441TP-ZAS-27135	DH_IPC-HX5(4)(3)XXX-Leo_MultiLang_PN_Stream3_V2.800.0000000.3.R.190830.zip
DH-IPC-HFW3541TP-ZAS-27135	DH_IPC-HX5(4)(3)XXX-Leo_MultiLang_PN_Stream3_V2.800.0000000.3.R.190830.zip
DH-IPC-HFW5431EP-ZE-27135	2.6.01.05.10487: DH_IPC-HX5X3X-Rhea_MultiLang_PN_Stream3_V2.800.0000008.0.R.190619.zip
DH-IPC-HFW5241EP-ZE-27135	2.6.01.05.10979: DH_IPC-HX5XXX-Volt_MultiLang_PN_Stream3_V2.800.0000000.1.R.190706.zip

Model	Version
DH-IPC-HFW5442EP-ZE-2712	2.6.01.05.10979: DH_IPC-HX5XXX-Volt_MultiLang_PN_Stream3_V2.800.0000000.1.R.190706.zip
DH-IPC-HFW5541EP-ZE-27135	2.6.01.05.10979: DH_IPC-HX5XXX-Volt_MultiLang_PN_Stream3_V2.800.0000000.1.R.190706.zip
DH-SD6CE230U-HNI	2.6.01.05.00664: DH_SD-Yin-Demeter_Internal_PN_Stream3_Intelligent_V2.640.0000000.0.R.180502.zip
DH-SD5A425XA-HNR	2.6.01.05.11696:DH_SD-Prometheus_MultiLang_PN_Stream3_V2.800.0000000.15.R.190802.zip
DH-SD6CE230U-HNI	2.1.01.01.12843:DH_SD-Eos_Eng_P_Stream3_V2.622.0000000.5.R.171228.zip 2.1.01.02.11710:General_SD6CEXXX-HN-R-MAIN_MCU_V2.400.0000000.0.R.170912.zip
DH-SD5A425XA-HNR	DH_SD-Eos-Civil_MultiLang_PN_Stream3_V2.800.0000000.5.R.190827.zip
DH-SD6CE230U-HNI	2.1.01.01.12842: DH_SD-Eos_Chn_PN_Stream3_V2.622.0000000.5.R.171228.z2.1.01.02.11644: General_SD6A9XXX-HN-MAIN_MCU_V2.300.0000000.4.R.170814.zip
DH-SD49225T-HN-S2	2.6.01.05.05052: General_SD-Mao-Rhea_MultiLang_PN_Stream3_IVS_V2.623.0000000.7.R.181124.zip
DH-SD49225XA-HNR	2.6.01.05.12351: DH_SD-Prometheus_MultiLang_PN_Stream3_V2.800.0000000.17.R.190819.zip
PTZ1C203UE-GN	DH_SD-Eos-Civil_MultiLang_PN_Stream3_V2.800.0000000.5.R.190827.zip
VTO2202F-P	DH_VTO2202F_MultiLang_PN_SIP_V4.400.0000000.2.R.20190919.zip
VTO2111D-WP-S1	General_VTO2111D_Eng_P_16M_SIP_V4.300.0000000.6.R.20190320.zip
VTO1210C-X-S1	General_VTOXXX_Eng_P_16M_SIP_V4.300.0000000.1.R.20190305.zip
NKB3000	General_NKB5000_All_V3.211.10SA000.1.R.181204.BIN
NKB1000	General_NKB1000_ChnEng_V2.620.0000000.0.R.20180115.zip
SmartPss	General_SMARTPSS-Win32_ChnEng_IS_V2.003.0000000.0.R.190802.zip
DSS PRO/DSS Express	General_DSS-PRO_Win64_IS_V7.002.0000002.1.R.20190418.exe
NET SDK	General_NetSDK_Chn_Win32_IS_V3.051.0000005.1.R.190910.7z

Model	Version
PlaySDK	General_PlaySDK_Chn_Windows32_IS_V3.041.0000000.0.R.190123.zip
DMSS/IOS/plus	V4.70
Player	General_Player_EngChn_MAC_V3.44.0.R.170724.zip
ConfigTool	General_ConfigTool_ChnEng_V4.011.0000003.5.R.20190722.zip
DiskManager	General_DiskManager_Chn_WIN32_V2.02.1.R.170417.zip

1.7 Pending Issues

None.

1.8 Update Guide

None.

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com