WISENET

White paper

Network Hardening Guide

(IP Camera)

2020. 5. 8.

V3.0

Hanwha Techwin

Contents

Revision History

Version	Revision Date	Revision Details	Note
v1.0	Jun. 13th 2017	- v1.0 released	
v2.0	Jan. 16th 2018	- Non Plug-in HTML5 web viewer added in default level - 'Using SNMP securely' changed to Protective level from secure level (Default setting changed to off) - 'Disabling unused SNMP' removed - STW format backup removed from camera web viewer backup (Table 4) - SVNP protocol removed from 'Disabling unused multicast'	
V3.0	May. 8th 2020	-Add individual device authentication (device / user authentication) -Added SUNAPI / ONVIF deactivation in factory reset state -Secure Boot added -Using a secure communication protocol (HTTP) Change from protection level to secure level -Safe use of SNMP Change from protection level to secure level -Unused SNMP disable protection level added -Changed from secure level to protection level . Disable unused Link-Local IPv4 address . Disable unused UPnP search . Disable unused Bonjour -Changed the HTTP authentication (only Digest authentication) item to Use secure communication protocol (HTTP) and added it to the protection level. -Added use of the latest version of TLS -Added use of safe Cipher Suites -Add secure communication protocol (RTSP) -Add storage encryption / backup encryption	

1. Introduction

In the video surveillance market, a paradox is emerging that network surveillance devices developed to protect customers' property and personal information in recent years are used as a means of seizing personal information. Network surveillance device processes and manages video data that can be used as sensitive personal information. Since it is based on the network, remote access is possible from anywhere in the world where the network is connected. Because of this nature, network surveillance device is subject to ongoing cyber attacks.

Hanwha Techwin has been continuously making efforts to strengthen cyber security with a careful consideration of customers' property and personal information. We hope that this guide will help you understand and safely use the security features implemented in Hanwha Techwin product.

2. Definition of Security Levels

WISENET

This guide defines cyber security levels according to the following criteria, each level assuming the previous level is achieved.

- The default level is the level of security that users can achieve with the functionality provided by the device, without any extra settings.
- The protective level means the level of security that can be achieved with the default settings that initial purchased products have or in the state immediately after the factory initialization.
- The secure level is a level of security that user can achieve by disabling unnecessary features or services that product provided.
- The very secure level means the level of security that can be achieved by combining the security features provided by products with additional external security solutions.

< Table 1 >

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Default Level	Force complex password settings	Default	-
	Remove initial password	Default	-
	Restriction of input in case of consecutive password failure	Default	-
	Remote service (Telnet, SSH) not used	Default	-
	Encrypt preference information	Default	-
	Firmware encryption and secure update	Default	-
	Watermarking and encryption of extracted video formats	Default	-
	Keep log on initialization	Default	-
	HTML5 streaming based NonPlug-in web viewer	Default	-
	Individual device authentication (device / user authentication)	Default	-
	Disable SUNAPI / ONVIF at factory reset	Default	-
	Secure Boot	Default	-

2. Definition of Security Levels

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Protective Level	Performing factory reset	-	-
	Disable guest login	Not set	-
	Disable allow unauthenticated RTSP connections	Not set	-
	Disable unused multicast	Disabled	-
	Disable unused DDNS	Off	-
	Disable unused QoS	Not set	-
	Disable unused FTP	Not set	-
	Disable unused SNMP	Disabled	-
	Disable unused Link-Local IPv4 address	Disabled	-
	Disable unused UPnP search	Disabled	-
	Disable unused Bonjour	Disabled	-
	Use the latest version of TLS	TLS 1.2 / 1.3	-
	Using Safe Cipher Suites	Secure Cipher Suites	-
	Disable unused audio input	unused	-
Secure Level	Check if the latest version of firmware is used	-	-
	Updating to the latest version of firmware	-	-
	Setting the correct date / time	Initial value	change
	Using a secure communication protocol (HTTP)	HTTP + HTTPS	HTTPS
	Using a secure communication protocol (RTSP)	HTTPS + Wisenet / ONVIF	HTTPS + RTSP
	HTTPS (use your own certificate)	HTTP	HTTPS (use your own certificate)
	HTTPS (using public certificate)	HTTP	HTTPS (using public certificate)
	Changing the default port	Initial value	change
	IP filtering	Not set	Set
	Sending E-mail using TLS	Disabled	Activation
	Using SNMP securely	Not set	SNMP v3
	Create additional user accounts	-	-
	Check the log	-	-
	Encryption of stored data (LUKS encryption)	Not set	Set
	Backup data encryption (ZIP file encryption)	Not set	Set
Very Secure Level	802.1 X Certificate-based access control	Not use	Use

- *If the initial setting value is set to 'Default', it means that it is provided as default, not as a user-selectable option. If it is a dash, it means that there is no user-selectable option and it is the activity to check / execute.*

3. Default Level

Hanwha Techwin develops products to ensure safety from cyber security threats even with basic functions and initial settings.

< Table 2>

Security Policy	Features for Cyber Security	Brief Description
Password policy	Force complex password settings	Character input request with password complexity of at least 8 characters (2 or 3 types)
	No initial password	Password setting required for the first web UI login
Access control	Restriction of input when consecutive password input fails	Block password input attacks from unauthorized persons when logging in to the web UI
	Disable SUNAPI / ONVIF at factory reset	Prevention of video leakage
Remote access control security	Remote service (Telnet, SSH) not used	Remove all services that can access the system remotely
Security of setting information backup	Encrypt preference information	Protect backed up configuration information
Firmware security	Firmware encryption and secure update	Prevent exposure and analysis of important information of firmware
		Prevent forgery of firmware and injection of malicious code
Protect extracted video	Watermarking and encryption of extracted video formats	Guaranteed confidentiality and integrity of extracted video format and source authentication
Log protection	Keep log on initialization	Protection against malicious log deletion from intruders
HTML5 streaming standard	HTML5 streaming based NonPlug-in web viewer	Provide optimal video service without Plug-in (ActiveX, Silverlight, NPAPI)
Individual device authentication	Device and mutual authentication (server authentication / client authentication)	Reliable device identification during encrypted communication using device certificates
Physical protection	Secure Boot	Firmware forgery prevention

3.1. Forced complex password setting

Hanwha Techwin products require min. 8 character password. Depending on the length of the password, three (8 to 9 characters) or two (10 or more) combination of letters (upper/lower case, numbers and special characters). Up to 15 characters for NVR/DVR/IP camera and up to 31 characters for VMS. This enforcement helps to reduce the possibility of unauthorized password hijacking by preventing the weak password setting due to user's carelessness.

3.2. No initial password

If a user uses the initial password or can not change the manufacture's default password, it could cause a serious security vulnerability that would allow unauthorized access. To prevent any security vulnerability that may occur due to user's mistake, all Hanwha Techwin products have no initial password and designed to set user's own password when accessing the UI of the product for the first time.

3.3. Input limit for consecutive password failures

Hackers systematically check all possible passwords and passphrases until the correct one is found. If this attack is allowed, the password will out some time. Hanwha Techwin devices block brute-force attack by not allowing 5 times or more login attempt within 30 seconds to improve its security. Also, existing connection of authorized user's is maintained to prevent denial-of-service while password input is blocked.

3.4. Remote service (Telnet, SSH) not used

Daemons that support remote services such as Telnet on a network device can give manufacturers the advantage of conveniently providing A / S to their customers, but if there are manufacturers with hackers or malicious intentions, It can be a factor that can cause dangerous security incidents. Accordingly, Hanwha Techwin's products gave up the convenience of A / S and adopted a policy to boldly eliminate these risks to improve the security level.

3.5. Preference information encryption

If you use the Backup function, you can download the binary file containing the current device's environment setting information to your PC, and restore the backed up environment setting information through the Restore function.

- Excludes the following items from environment setting information
  : Excluding configuration information such as IP & Port, DDNS, IP filtering, HTTPS, 802.1x, QoS, SNMP, Auto IP configure in the network menu

If you use these functions, you can set the same environment for all devices with the same model name with only one device setting. Since the binary file containing the backed up configuration information contains important information of the user's device environment, Hanwha Techwin stores the configuration information using a secure encryption algorithm when back up.

- Settings (IP camera)
  : System → Upgrade / Reboot → Settings Backup & Restore

3.6. Firmware encryption and secure update

Hanwha Techwin's products provide encrypted firmware through the homepage of Hanwha Techwin when providing firmware for adding functions / improving bugs and updating security. In addition, when the firmware is updated, the forged firmware is identified and the integrity can be verified and the update can be completed after verifying the integrity. This prevents hackers from analyzing important information contained in the firmware, and after injecting malicious code through forgery of the firmware, it can take control of the device and prevent it from being used as another attacking bot. The firmware contains a lot of important information that can be exploited by hackers. Hanwha Techwin's products distribute firmware with confidentiality and integrity for the security and secure update of these firmware.

3.7. Watermarking and encryption of extracted video formats

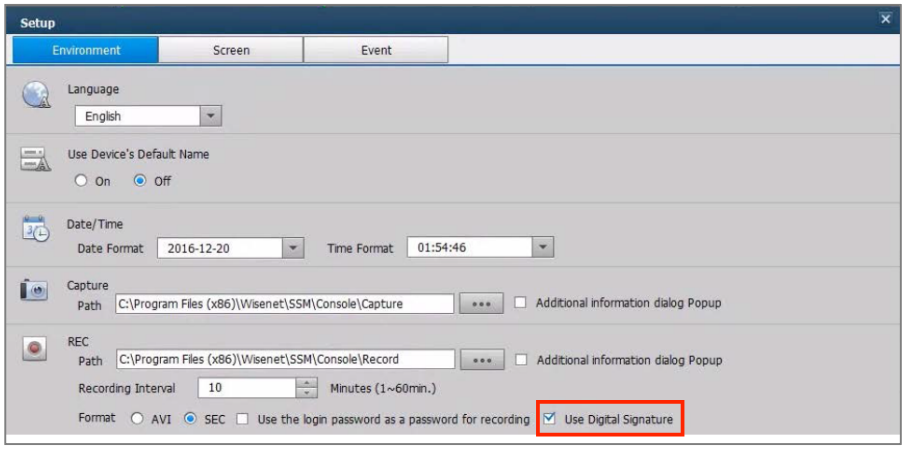
Video files extracted in SEC file format using Hanwha Techwin's NVR / VMS are prevented from being tampered with because they cannot be opened with general editing software. Basically, the player required for playback is automatically extracted from the SEC file, so there is no need to install the player separately, and the user can simply play the video file by double-clicking the SEC file.

If you want to extract video files for legal evidence or privacy purposes, you can select the SEC file format and set a password to extract it. Watermarking and encryption are applied to the extracted SEC file to ensure that the video is tampered with and ensure confidentiality. If extracted as a SEC file from VMS (SSM), the digital signature function is additionally supported to support the video. It is possible to confirm that it was extracted from SSM.

< Table 3 >

Device	Extraction location	Backup file format	Watermarking /Encryption	Digital Signature	Player
Camera	Webviewer	AVI	X	X	general video player
NVR	Set	NVR	X	X	Only playable on set
		SEC	O	X	Backup viewer
	Webviewer	SEC[1]	O	X	Backup viewer
		AVI	X	X	general video player
VMS(SSM)	-	SEC	O	O	Backup viewer
		AVI	X	X	general video player

• SSM console setup → Environment → REC → Format



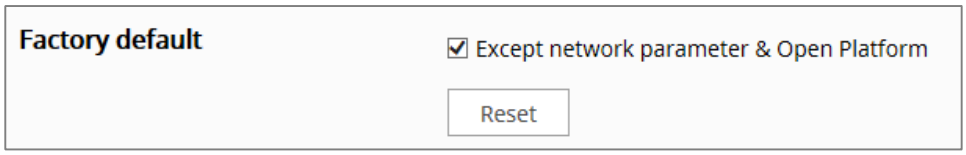
[1] Non-Plug-in web viewer is not supported when extracting SEC file of NVR web viewer

3.8. Maintained logs after factory reset

It is very important for network or security administrators to check the log to analyze the intrusion path or to understand the incident when someone intrudes or attempts to break into a network device.

However, because intruders are aware of the logs of these network devices, they want to delete logs so that they do not leave their marks or traces. Hanwha Techwin's product is developed to retain log files from being erased by device initialization (factory reset) to prevent such malicious intent.

- Settings (IP camera) : System → Upgrade / Reboot → Factory Reset



3.9. HTML5 non plug-in web viewer

Most video surveillance devices provide web viewer video streaming service using the plug-in (ActiveX, Silverlight, NPAPI) installed into a web browser. However, such plug-in have high possibility of security vulnerabilities and exposures. Recently, malicious code infections are frequently caused by the security vulnerabilities in effect. As a result, the most of browsers have blocked plug-in installation and execution, and standardization is underway to provide services through HTML5 (HTML latest standards), which can provide media service without plug-in.

In response to this trend and security requirements, Hanwha Techwin has strengthened security and user convenience by providing HTML5 web viewer service that can provide optimal video service without plug-in.

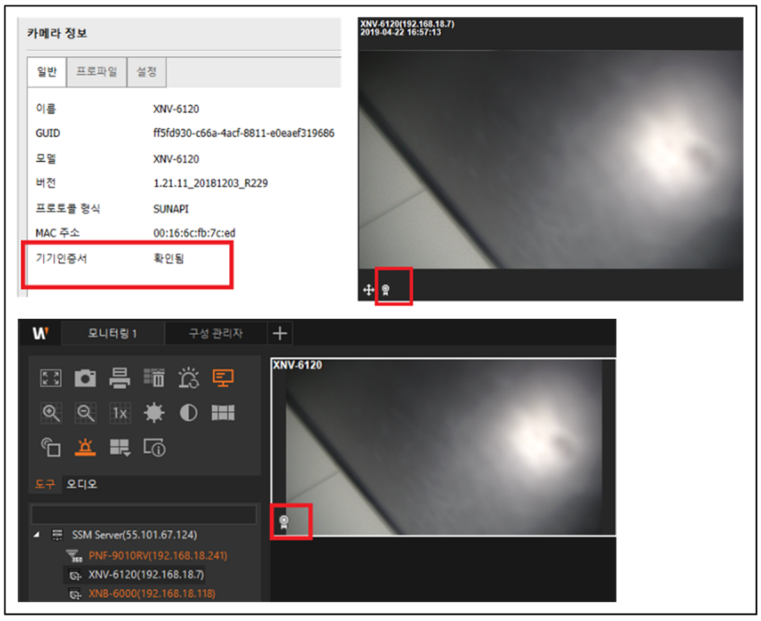
3.10. Individual device authentication (Device/mutual authentication (server authentication/client authentication))

Network devices provided by Hanwha Techwin are equipped with device identification and mutual authentication functions using device certificates for encrypted communication. Through this, it is possible to check whether it is a reliable device manufactured by Hanwha Techwin, and security can be strengthened by preventing hackers from eavesdropping on or manipulating secure communication through man-in-the-middle attacks.

The device certificate injection uses THALES HSM equipment to generate a certificate / private key for each device and injects it into each device during manufacturing. The generated certificate is digitally signed by the Private Root CA, so you can prove that it was issued by Hanwha Techwin.

Using this certificate, you can perform secure communication without a security warning in a web browser, and you can confirm this in products that implement device / mutual authentication as shown below.

• Device authentication (SSM): registration → device selection → camera information → general → device authentication 'verified' information confirmation



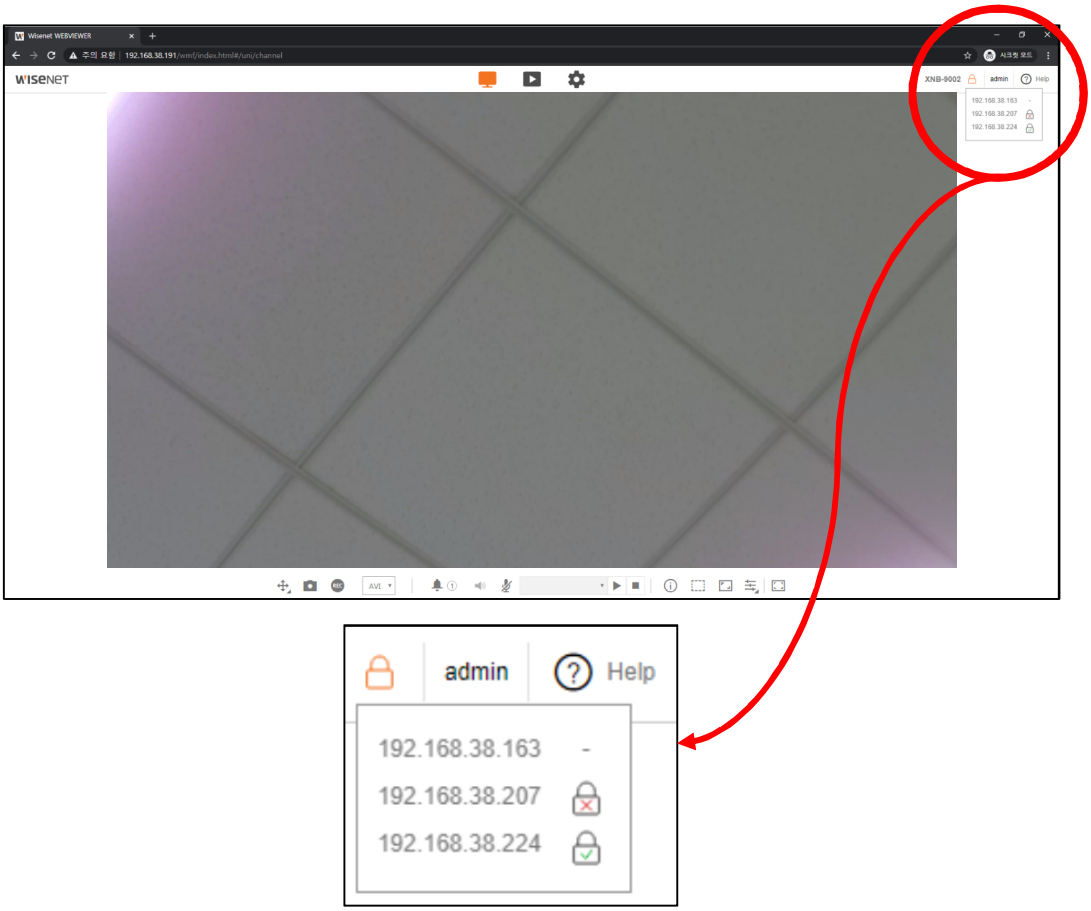
- Mutual authentication (camera)

  : Live screen → Select mutual authentication icon → Check authentication status

  ① Not applicable: without icon – mark

  ② Mutual authentication success: Success icon

  ③ Mutual authentication failure: failure icon



You can check the installation guide of Hanwha Techwin's Private Root CA certificate on our website.

- Hanwha Techwin Private Root CA pre-installation guide

  (https://www.hanwha-security.com/en/technical-guides/cybersecurit/)

3.11. Disable SUNAPI / ONVIF at factory reset

To prevent the leakage of video image information through SUNAPI / ONVIF, Hanwha Techwin restricts access to SUNAPI / ONVIF until a password is set.

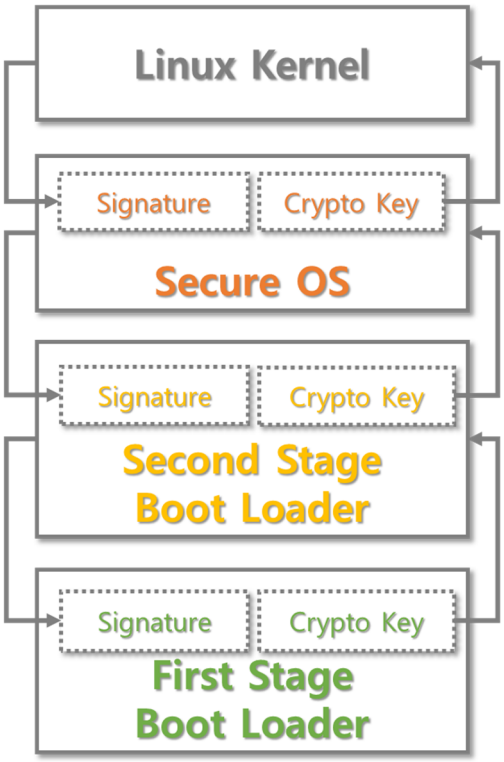
3.12. Secure Boot

Hanwha Techwin strives to strengthen security by providing devices equipped with its own WN7 chip. WN7 has a built-in Secure Boot function.

Secure Boot is a security technology that prevents the forged / modulated boot image from being executed by verifying the digital signature of each boot image loaded at boot time.

Previously, if only the firmware image was encrypted once, the WN7 verifies the boot image step by step and the first stage passes the verification before the next stage boot image is loaded.

The verification method loads the authentication signature when the boot image is created, and verifies the corresponding signature when the product is booted, and proceeds to boot if there is no abnormality in the verification result.



4. Protective Level

Hanwha Techwin devices are safe for basic security even with the initial settings immediately after purchase or factory reset.

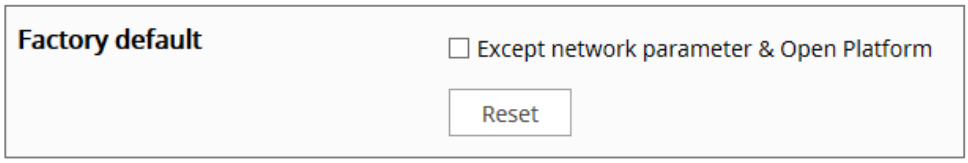
< Table 4>

Security Policy	Features for Cyber Security	Brief Description
Service protection	Factory reset	Initialize existing information stored in the device
	Disable guest login	Video protection from unauthorized users
	Disable allow unauthenticated RTSP connections	RTSP video protection from unauthorized users
	Disable unused multicast	Prevent malicious attacks by minimizing services that are initially activated
	Disable unused DDNS	
	Disable unused QoS	
	Disable unused FTP	
	Disable unused SNMP	
	Disable unused Link-Local IPv4 address	
	Disable unused UPnP search	
	Disable unused Bonjour	
	Disable unused audio input	
cryptography	Using a secure communication protocol (HTTPS)	Protection of personal information and video transmitted and received on the web viewer
	Use the latest version of TLS	Use the latest version that is safe for security
	Safe use of Cipher Suites	Use secure cryptographic algorithms

4.1. Perform Factory Reset

If the device you want to set up is not in the initial state, it is need to perform a factory reset of the device to initialize the device's settings. Hanwha Techwin product can achieve the protective level of security with the initial state alone.

1) System → Upgrade/Reboot → Factory default
2) Uncheck 'Except network parameter & Open SDK'.
3) Click 'Reset'.



4.2. Disabling guest login

Hanwha Techwin camera provides guest login function. This guest account is limited because it allows only minimal privileges, but if guest login is enabled, video streams may be exposed to unauthorized users, so if guest access is not needed, guest login must be disabled.

- IP camera web viewer → Basic → User → Guest setup

4.3 Disabling unauthenticated RTSP connections

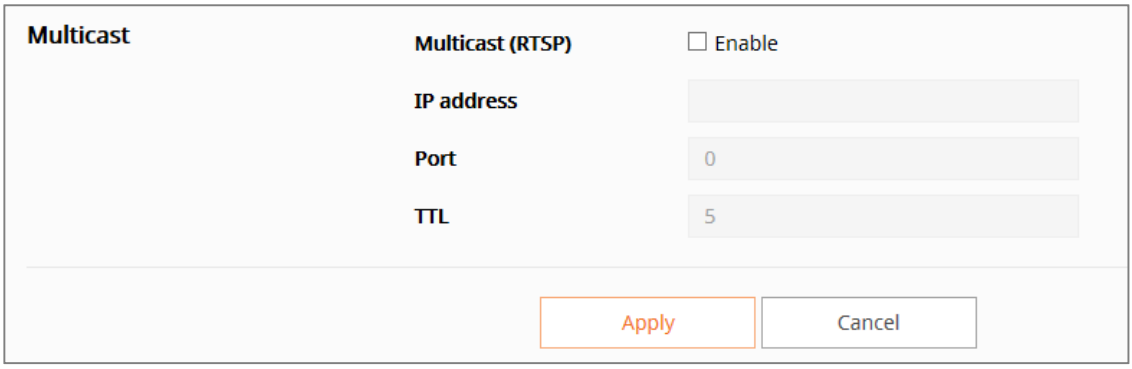
Hanwha Techwin camera provides a function that allows RTSP connection without authentication. This feature is useful for providing an RTSP video stream for public purposes, but if you want to protect the RTSP video stream from unauthorized users, you must disable the RTSP connection without authentication feature.

1) IP camera setup → Basic → User → Authentication setup
2) Uncheck 'Enable RTSP connection without authentication'

4.4 Disabling unused multicast

It is able to set multicast for SVNP and RTSP protocols. If these services are unnecessary, make sure to deselect the service features for added security.

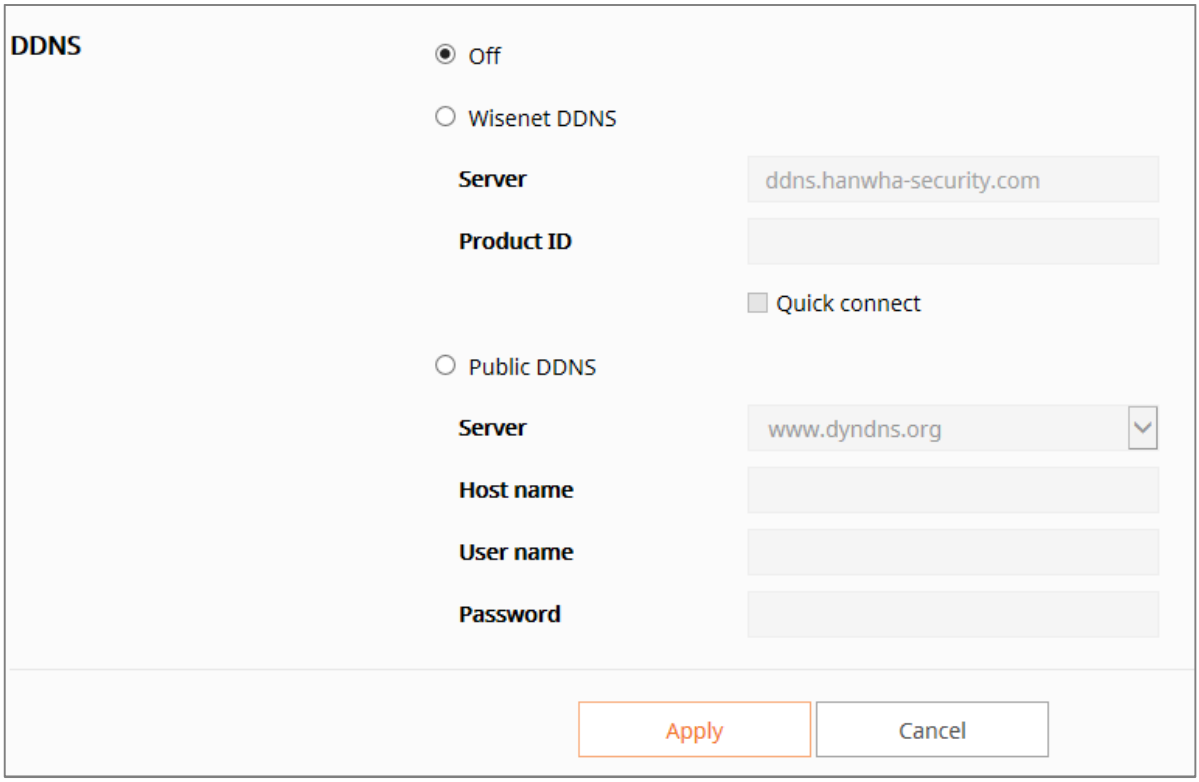
1) IP camera setup → Network → Video profile
2) Uncheck 'Use' box of Multicast RTSP.
3) Click 'Apply'.



4.5. Disabling unused DDNS

If your camera is connected directly to a DHCP-based cable modem, DSL modem, or PPPoE modem, the IP address will change each time you try to connect to your ISP. In this case, the user can not know the changed IP address. If the ID of the product is pre-registered through the DDNS function, the changed IP address can be easily accessed. If you think the service is unnecessary, make sure to deselect the service feature for added security.

1) IP camera setup → Network → DDNS
2) Check 'Off' for DDNS.
3) Click 'Apply'.



4.6. Disabling unused QoS

QoS(Quality of Service) is a function to set the priority to guarantee the quality of video transmission for specific IP. If you think the service is unnecessary, make sure to deselect the service feature for added security.

1) IP camera setup → Network → QoS
2) Chose listed IP for QoS then delete.
3) Click 'Apply'.

4.7. Disabling unused FTP

The FTP function is for transferring the images shot by the camera through the FTP server set up when an alarm or event occurs. If you think the service is unnecessary, make sure to deselect the service feature for added security.

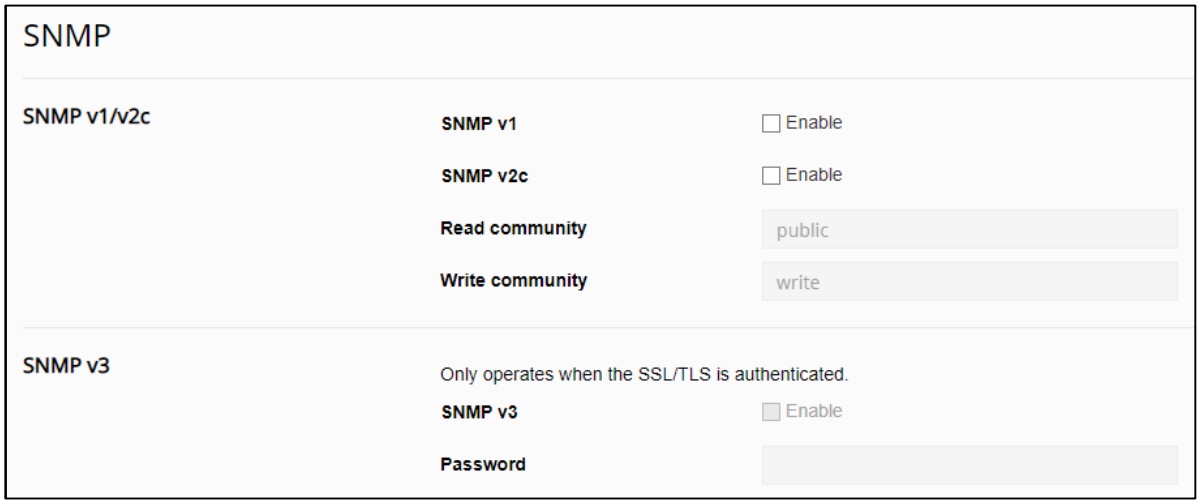
1) IP camera setup → Event → FTP/E-mail → FTP Configuration
2) Remove server address, ID and password.
3) Click 'Apply'.

4.8. Disable unused SNMP

Hanwha Techwin's devices support SNMP v1, v2c and v3 functions simultaneously. If you think the SNMP service is unnecessary, uncheck the setting of the service function to enhance security.

1) Network → SNMP

2) Deselect SNMP v1, v2c and v3



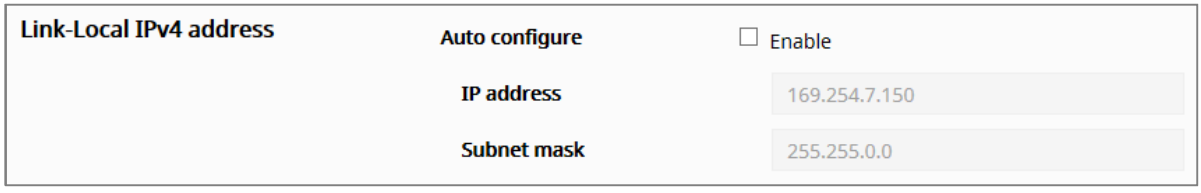
4.9. Disable unused Link-Local IPv4 address

The link-local IPv4 address auto-configuration function is set to 169.254.xxx.xxx for the camera in a link-local network (meaning a network connected to one link, such as a camera and a host connected to the same switch) that do not receive the same IP as a DHCP server. This function assigns IP. If you think the service is unnecessary, uncheck the setting of the service function to enhance security.

1) Network → Auto IP Settings → Link-Local IPv4 Address

2) Deselect automatic setting

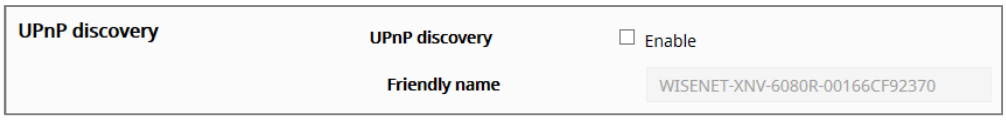
3) Click the Apply button



4.10. Disable unused UPnP search

The UPnP search function is a function that automatically searches for cameras from clients and operating systems that support the UPnP protocol. If you think the service is unnecessary, uncheck the setting of the service function to enhance security.

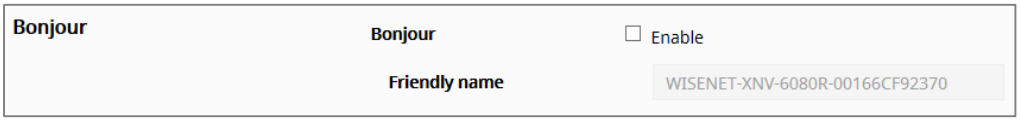
1) Network → Auto IP setting → UPnP discovery
2) Uncheck UPnP discovery
3) Click the Apply button



4.11. Disable unused Bonjour

Bonjour is a feature that automatically searches for cameras from clients and operating systems that support the Bonjour protocol. If you think the service is unnecessary, uncheck the setting of the service function to enhance security.

1) Network → Auto IP Settings → Bonjour
2) Deselect Bonjour Settings
3) Click the Apply button



4.12. Use the latest version of TLS

TLS is used to establish a secure and encrypted communication channel between client-server developed based on the SSL protocol. TLS currently has four versions, 1.0, 1.1, 1.2, and 1.3, but the initial version of TLS, TLS 1.0 / 1.1, is vulnerable to various attacks such as POODLE[2] and BEAST[3].

Hanwha Techwin provides TLS 1.2 / 1.3 as the initial setting, and if necessary, adds a specific TLS version. However, it is necessary for users to deselect TLS 1.0 / 1.2 in order to use the product safely.

[2] POODLE Vulnerability: An abbreviation of Padding Oracle On Downgraded Legacy Encryption, a protocol downgrade vulnerability that allows the use of outdated encryption techniques.
[3] BEAST Vulnerability: Short for Browser Exploit Against SSL / TLS, a vulnerability that can decrypt HTTPS cookies in an end-user browser and hijack an effective target session.

4.13. Safe use of Cipher Suites

Through the Cipher Suites of the TLS handshake, the final verification between the client and the server will be conducted on the method of certificate verification and asymmetric key exchange, symmetric key encryption and operation, and message authentication used in TLS. The structure is as follows.

Hanwha Techwin provides Cipher Suites based on TLS 1.2 / 1.3 as follows.

■ TLS 1.2 Cipher Suites

TLS_RSA_WITH_NULL_MD5	0x00,0x01	Compatible	NULL-MD5
TLS_RSA_WITH_NULL_SHA	0x00,0x02	Compatible	NULL-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	0x00,0x2F	Compatible	AES128-SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	0x00,0x32	Compatible	DHE-DSS-AES128-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x00,0x33	Compatible	DHE-RSA-AES128-SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA	0x00,0x34	Compatible	ADH-AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	0x00,0x35	Compatible	AES256-SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	0x00,0x38	Compatible	DHE-DSS-AES256-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x00,0x39	Compatible	DHE-RSA-AES256-SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA	0x00,0x3A	Compatible	ADH-AES256-SHA
TLS_RSA_WITH_NULL_SHA256	0x00,0x3B	Compatible	NULL-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	0x00,0x3C	Secure/Compatible	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	0x00,0x3D	Secure/Compatible	AES256-SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x00,0x40	Secure/Compatible	DHE-DSS-AES128-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x00,0x67	Secure/Compatible	DHE-RSA-AES128-SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x00,0x6A	Secure/Compatible	DHE-DSS-AES256-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x00,0x6B	Secure/Compatible	DHE-RSA-AES256-SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256	0x00,0x6C	Secure/Compatible	ADH-AES128-SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256	0x00,0x6D	Secure/Compatible	ADH-AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	0X00, 0x9C	Secure/Compatible	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	0X00, 0x9D	Secure/Compatible	AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00, 0x9F	Secure/Compatible	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	0x00,0xBD	Compatible	DHE-DSS-CAMELLIA128-SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00,0xC0	Compatible	CAMELLIA256-SHA256
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	0x00,0xC3	Compatible	DHE-DSS-CAMELLIA256-SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00,0xC4	Compatible	DHE-RSA-CAMELLIA256-SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0XC0, 0x09	Secure/Compatible	ECDHE-ECDSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0XC0, 0x0A	Secure/Compatible	ECDHE-ECDSA-AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0XC0, 0x13	Secure/Compatible	ECDHE-RSA-AES128-SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0XC0, 0x14	Secure/Compatible	ECDHE-RSA-AES256-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0XC0, 0x2C	Secure/Compatible	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0XC0, 0x23	Secure/Compatible	ECDHE-ECDSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0XC0, 0x24	Secure/Compatible	ECDHE-ECDSA-AES256-SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0XC0, 0x27	Secure/Compatible	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0XC0, 0x28	Secure/Compatible	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0XC0, 0x2B	Secure/Compatible	ECDHE-ECDSA-AES128-GCM-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0XC0, 0x2C	Secure/Compatible	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0XC0, 0x2F	Secure/Compatible	ECDHE-RSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0XC0, 0x30	Secure/Compatible	ECDHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_CCM_8	0XC0, 0xA3	Secure/Compatible	DHE-RSA-AES256-CCM8
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0XCC, 0xA8	Secure/Compatible	ECDHE-RSA-CHACHA20-POLY1305
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0XCC, 0xA9	Secure/Compatible	ECDHE-ECDSA-CHACHA20-POLY1305

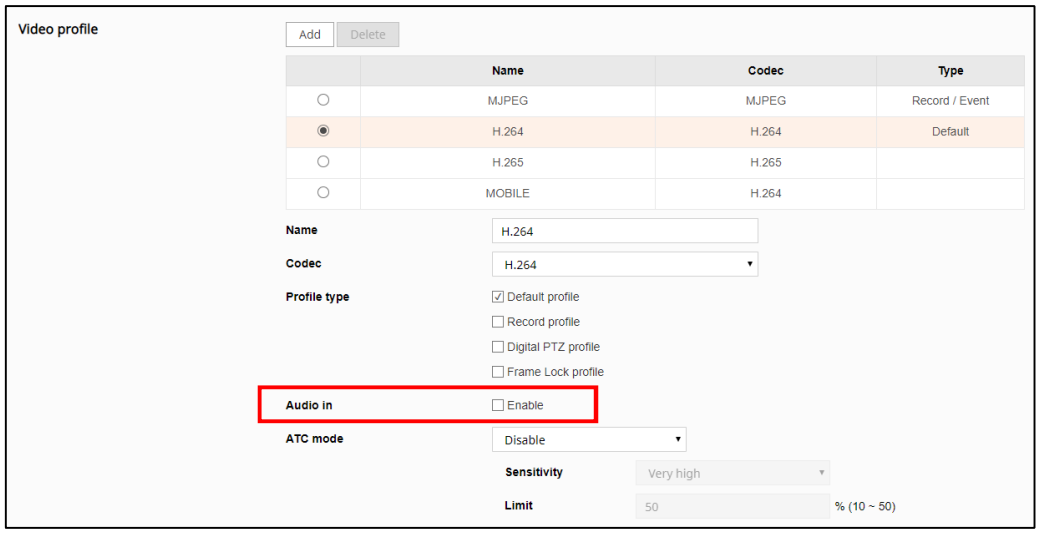
■ TLS 1.3 Cipher Suites

TLS_AES_128_GCM_SHA256	0x13,0x01	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	0x13,0x02	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_CCM_SHA256	0x13,0x04	TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256	0x13,0x05	TLS_AES_128_CCM_8_SHA256

4.14. Disabling unused audio input

Audio-In is a function that allows you to input sound into the video. If you think the service is unnecessary, make sure to deselect the service feature for added security. Audio Input (Audio-In) function can be set individually for each video profile, so it is necessary to select each profile than set up.

1) IP camera setup → Video Profile
2) Chose video profiles and uncheck 'Audio-In'.
3) Click 'Apply'.



5. Secure Level

Hanwha Techwin can be attacked from outside if unnecessary services or ports that are not actually used are open, so users can improve security by disabling functions or services that they do not need.

< Table 5 >

Security Policy	Features for Cyber Security	Brief Description
-	Check and update the latest version firmware	Make sure you are using the latest version of firmware and update if it is a Vulnerable firmware
-	Setting the correct date / time	Set accurate date and time for log analysis
-	Using a secure communication protocol (RTSP)	Protection of video transmitted through RTSP
-	HTTPS (with own certificate)	Secure connection between device and client through certificate
-	HTTPS (with public certificate)	
-	Change default port	Preventing web service access attacks through port changes
Access control	IP filtering	Prevent access attacks through specific IP access permission / deny
-	E-mail transmission using TLS	Secure email transmission using TLS
Service protection	Using SNMP securely	Clear all SNMP initial values for enhanced security
-	Create additional user accounts	Frequently used functions increase security by creating a user account with the least privilege.
Log	Check log	Analysis of unauthorized access records
Protect stored data	Encryption of stored data (LUKS encryption)	Protection of stored data
Protect backup data	Backup data encryption (ZIP file encryption)	Protection of backup data

5.1. Checking the version of firmware and updating

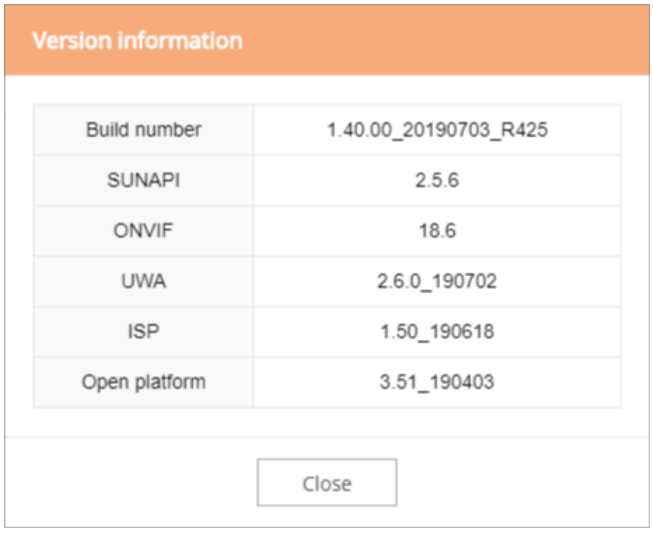
Through the Hanwha Techwin website (www.hanwha-security.com), you can check the latest firmware version of products used by customers.

In the figure below, if the customer uses the XNO-8080R model, the latest firmware version currently deployed is 1.40.00, and if you click the Info button, you can see that it is the version released on July 3, 19.

In addition, you can check the version information related to SUNAPI, ONVIF, UWA, ISP, Open platform. To upgrade the software, download the firmware for the product from the Hanwha Techwin website, and click the Upgrade button to upgrade. Please check that the firmware version of the product you are using is always up to date.

- www.hanwha-security.com → Product → Detail page of product → Firmware

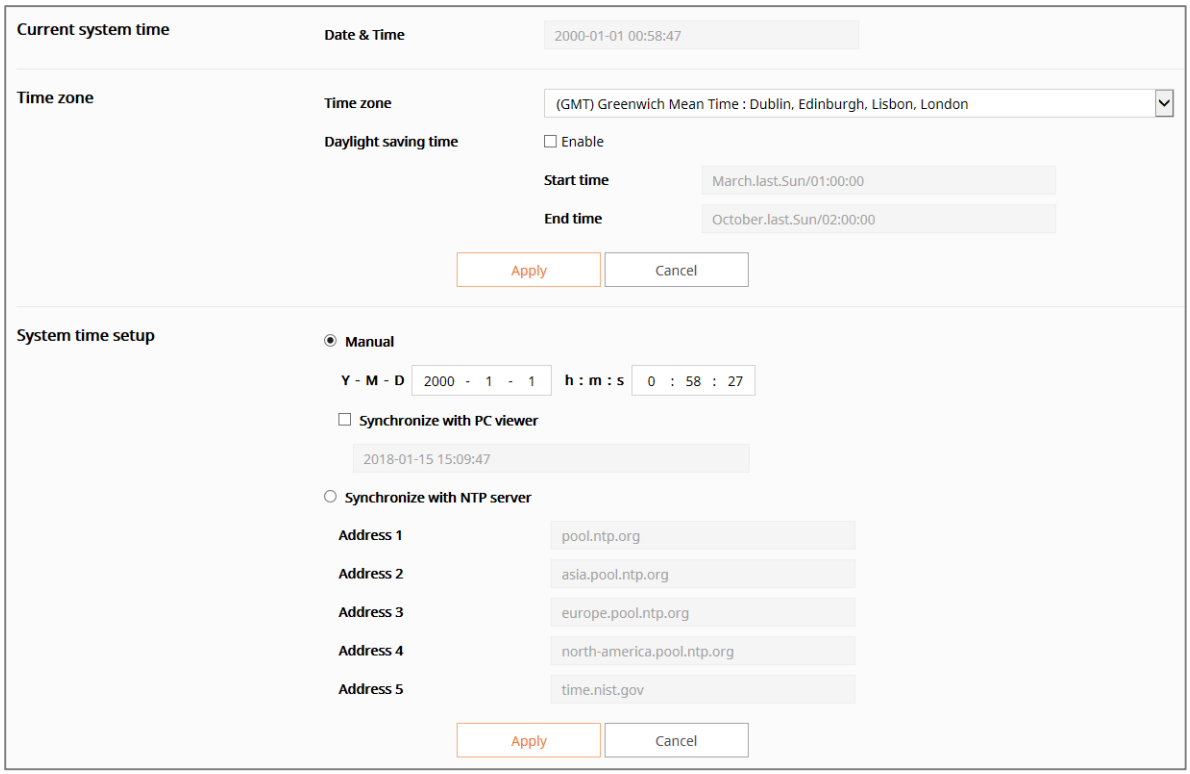
1) System → Upgrade/Reboot → Upgrade
2) Check the current S/W and ISP version.
3) Click 'Browse' and open the latest firmware
4) Click 'Upgrade'



5.2. Setting the correct date & time

Date & Time setup is a precondition for checking the accurate time information of log when analyzing information such as system log from device. It is very important to set correct time of current system. If the current system time is not set properly, the user can set the system time by one of three methods below.

1) IP camera setup → Basic → Date & Time
2) Chose your time zone and check 'Use daylight saving time' if needed.
3) Click 'Apply' of Time zone setup.
4) Set the system time by on of below methods.
   - Manual: Set the current time manually
   - Synchronize with PC viewer: Set the current time by the time of your PC
   - Synchronize with NTP server: Synchronized with the time of the NTP server
5) Click 'Apply' of System time setup.



5.3. Using a secure communication protocol (HTTP)

Hanwha Techwin's IP cameras and NVR devices provide HTTP + HTTPS mode between the server and client as the initial setting. However, since the HTTPS setting mode is a mode set on the web viewer, video data, user passwords and IDs transmitted and received on the web viewer can be protected. In addition, if the user changes to HTTP mode, the Digest authentication method is applied, so the user password can be protected.

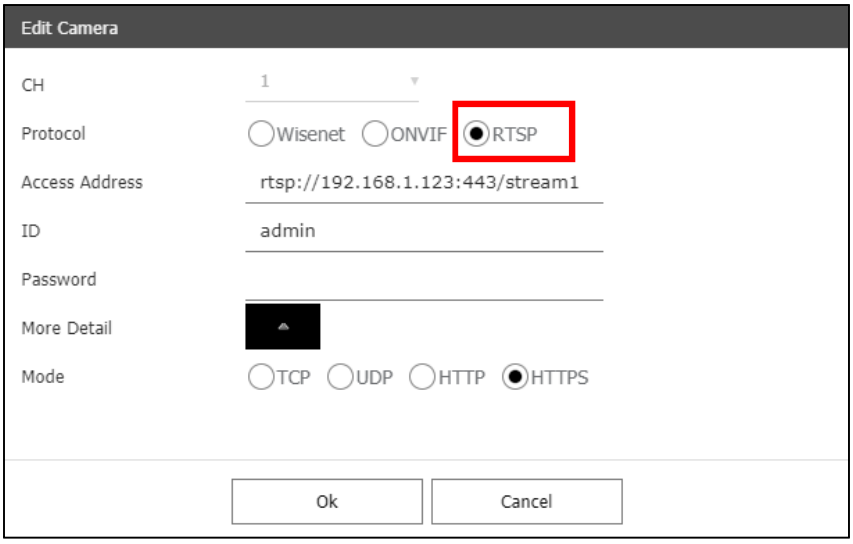
< Table 6>

Connection mode	User password protection	Video data protection	Use
HTTP (Digest authentication)	○	X	HTTPS simultaneous support
HTTPS	○	○*	Use (initial setting)

5.4. Using a secure communication protocol (RTSP)

In addition to HTTPS mode, video streaming via RTSP must also be secured. In order to protect the video through RTSP, additional setup is required to tunnel RTSP to HTTPS at the client end. For example, if you want to protect the video transmitted from the IP camera to the NVR with HTTPS, first set the HTTPS mode in the IP camera's web viewer. After connecting the camera to the NVR, set it to RTSP mode through Set UI or the NVR's web viewer.

• Settings (NVR Web Viewer): Device → Camera → Camera Registration → Channel Selection → Camera Modification

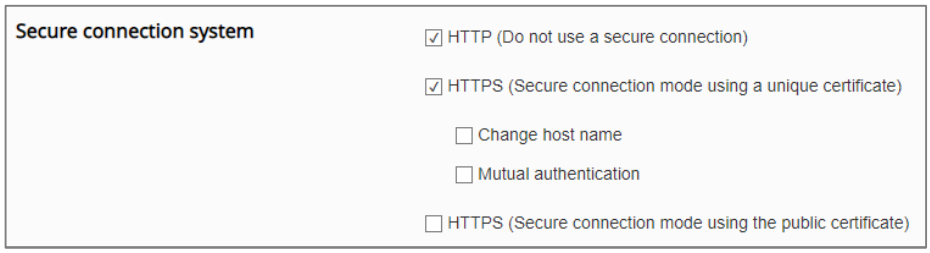


5.5. HTTPS (Hanwha Techwin certificate)

The initial secure access method supports HTTP and HTTPS simultaneously.

HTTPS (Hanhwa Techwin certificate) is a function that enables secure connection between a device and a client using its own certificate provided by Hanwha Techwin. If you select HTTPS (secure connection mode using your own certificate), the device's own certificate will be used in secure connection mode, and you do not need to register a separate certificate.

1) IP camera setup → Network → HTTPS → Secure connection system
2) Chose 'HTTPS (Secure connection mode using a unique certificate)'
3) Click 'Apply'.

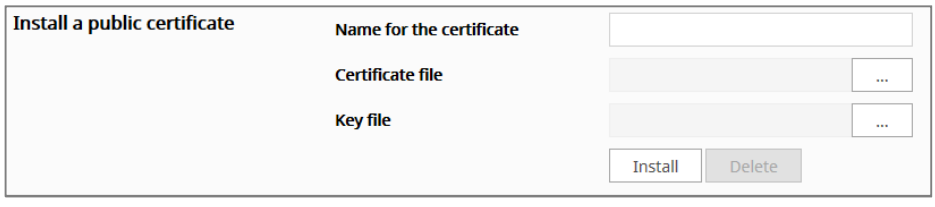


5.6. HTTPS (authenticated certificate)

It is a function that allows the user to register own authorized certificate directly to secure connection between the device and the client. By registering the public certificate and the private key, it is possible to select 'HTTPS (Secure connection mode using the public)' and it will be used in secure connection mode.

1) IP camera setup → Network → HTTPS → Install a public certificate
2) Input a name for the certificate and open the certificate file and key file.
4) Click 'Install' then choose HTTPS (Secure connection mode using the public certificate)
5) Click 'Apply'.

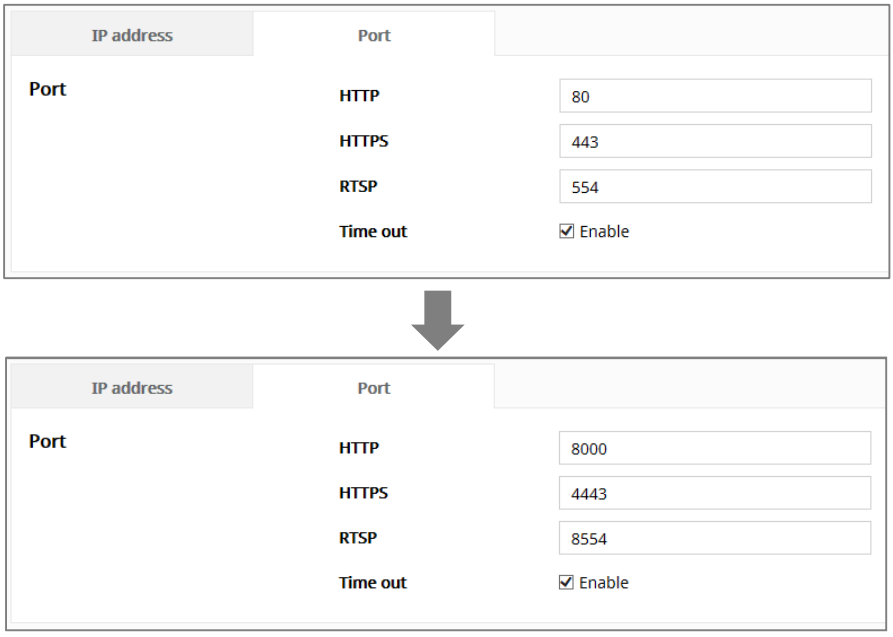
- *If you want to delete the registered certificate and private key, click the Delete button. You can delete the certificate only when you connect with HTTP (Do not use secure connection) or HTTPS (Secure connection mode using a unique certificate).*



5.7. Changing the default port

In order to avoid scan or attack through the default port of a network device, it is safe that user's own port rather than well-known default port. Normally, change the default port number to a higher port number. For example, if you change the HTTP web service port to 8000 rather than 80, you can protect your web service access from attacks that attempt to enter addresses directly into a simple scanning program or web browser.

1) IP camera setup → Basic → IP & Port → Port
2) Change the HTTP and HTTPS port number to high number from 80 and 443
3) Change the RTSP port number to high number from 554.
4) Change the device port number to high number from 4520.
5) Click 'Apply'.

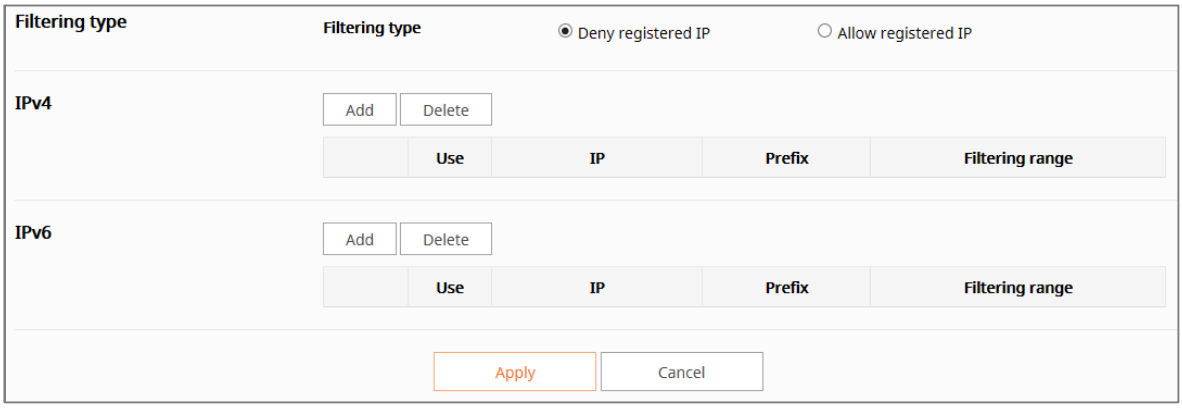


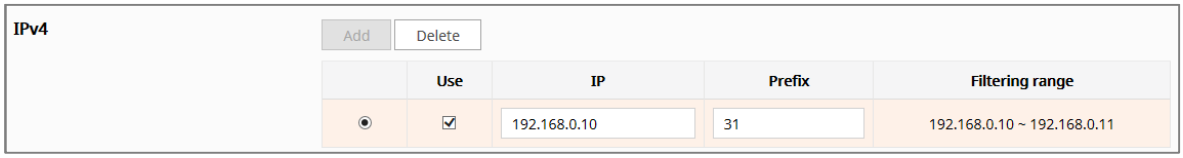
- *When port number is reassigned, it may cause communication problem if there is a connected recording device or VMS. If not resolved, return to the default port, please.*

5.8. IP Filtering

Hanwha Techwin products support the creation of IP lists to allow or deny access from specific IP address.

1) IP camera setup → Network → IP filtering → Filtering type
2) Select a filtering type
3) Click 'Add' then input an IP address to allow or deny access.
   When IP address or prefix is input filtering IP address range will be displayed.





4) Click 'Apply'.

- *The IP address of pc currently in use to setup cannot be added for deny filtering and only allow filtering is available. If you use IPv6, you must register both the IPv4 and IPv6 addresses.*

5.9. Sending E-mail using TLS

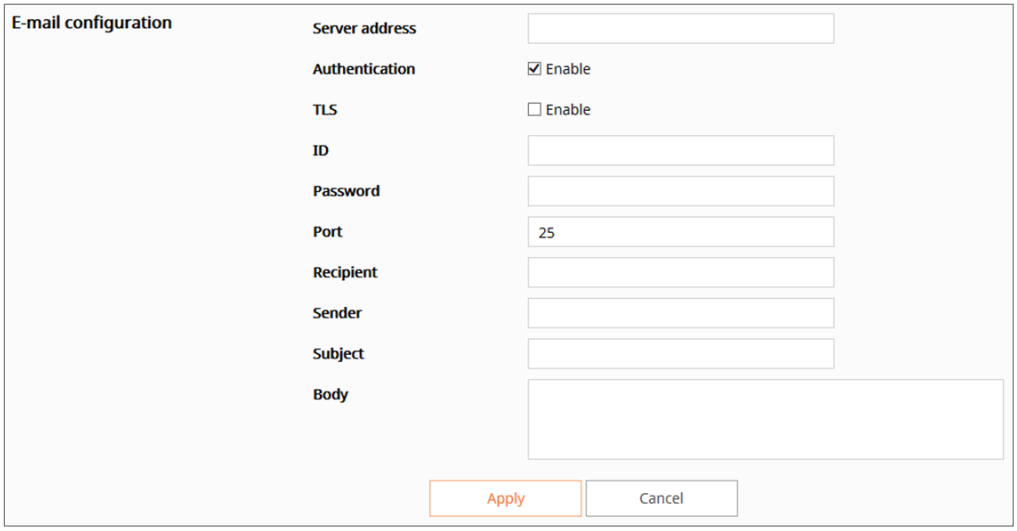
Hanwha Techwin camera supports e-mail transmission of images taken when an alarm or event occurs. When using this function, TLS mode enables secure email transmission from camera to mail server.

1) IP camera setup → Event → FTP/E-mail → E-mail configuration
2) Enter the IP address of the email server to which you want to send alarm and event images.
3) Choose 'on' for 'Use authentication' and 'Use TLS'.
4) Enter the user account ID and password to connect to the email server.
5) The default value for an email server port that does not use TLS is 25, but if you use TLS, the port is set to 465.

6) Enter the email recipient address in the Recipient field and the email sender address in the Sender field.

- *If the sender's address is not correct, the email server may classify the sender's email as spam.*

7) Enter the e-mail subject and contents (Body) and click the 'Apply'. When sending an email, the alarm and event images are delivered as attachments.



5.10. Using SNMP securely

SNMP provides the ability to conveniently manage network devices. By default, Hanwha Techwin is deselected to enhance security. In order to use SNMP safely, it is recommended to set it only with SNMP v3. If you want to use SNMP v3, HTTPS setting is a prerequisite, and if HTTPS (use your own certificate) in the previous section is already set, 1) to 3) of the following steps can be omitted.

SNMP v1 and v2c are vulnerable to security and avoid use because SNMP functions are provided through community strings in plain text.

1) Network → HTTPS → Secure connection method

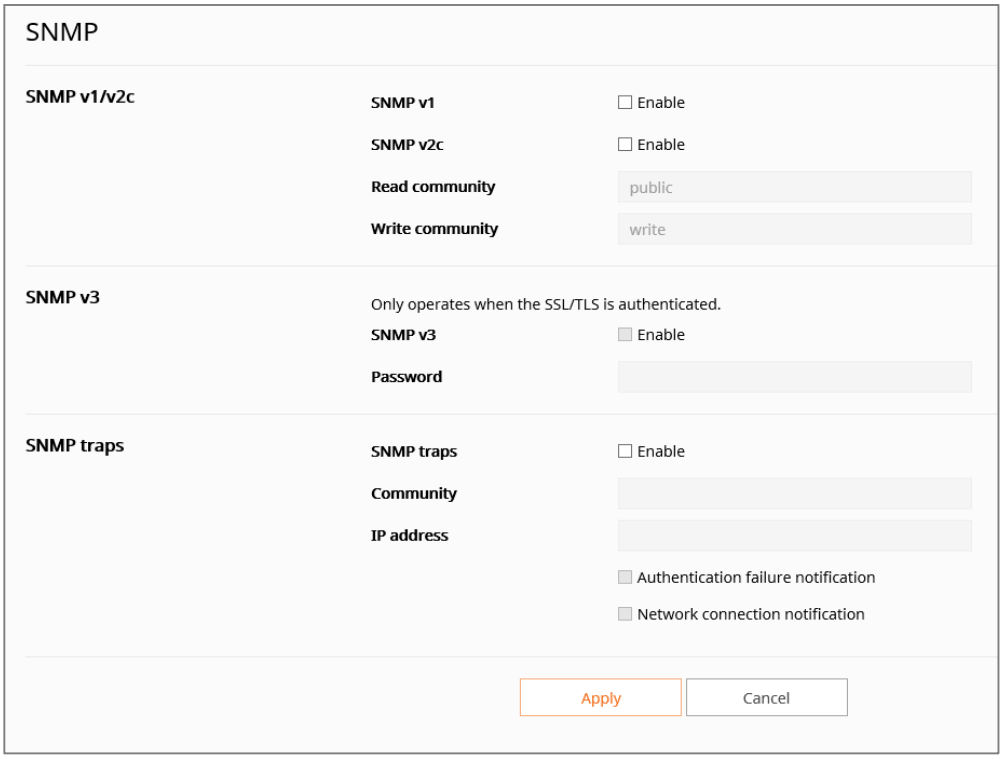
2) Select HTTPS (secure connection mode using its own certificate)

3) Click the Apply button

4) Network → SNMP

5) Uncheck use of SNMP v1 and SNMP v2c

6) Select SNMP v3 use and set password (Select v3 after changing HTTPS mode)

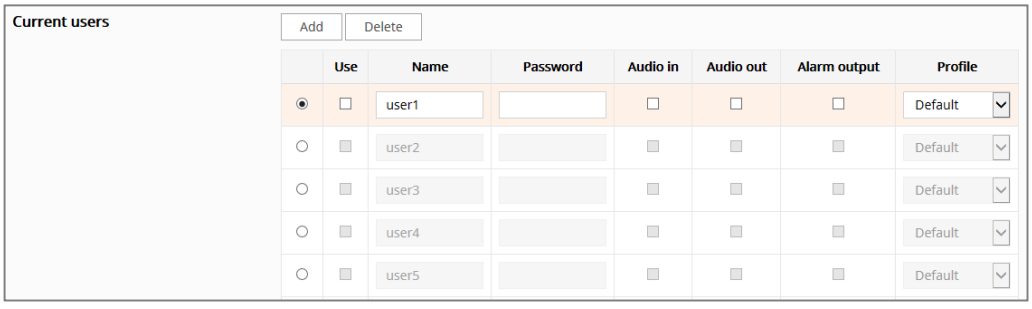


5.11. Creating additional user accounts

Accessing the device only with an administrator account can cause the administrator password to be continuously transmitted over the network, which can lead to a security vulnerability that exposes sensitive information to a person who has malicious purposes.

Therefore, it is able to enhance your security by enabling settings to be performed in your administrator account only, and by adding user accounts with limited privileges, such as frequently used video monitoring features.

1) IP camera setup → Basic → User → Current users
2) When you select the account to add, the setting items are activated.
3) Check 'Use' then input the name and password.
4) Select whether to use audio-in/out and alarm output.
5) Select the profile then click 'Apply'.



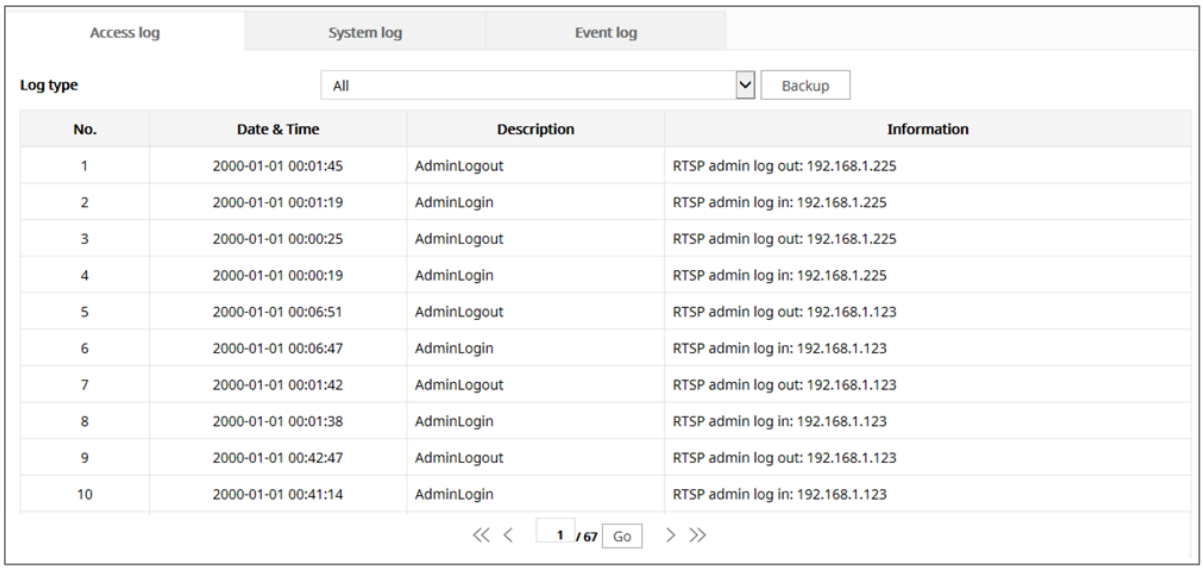
5.12. Checking the log

Administrators can analyze the logs stored in the system to find traces of unauthorized access to the device for malicious purposes. It is able to check various information such as device access, system setting change, event and etc. Also the log can be used as important data to enhance security of network system including device itself. The reason why log data should be checked and analyzed is as follows.

- Any problems that occur in the system (including errors and security flaws) are recorded and become a useful clue.
- It is able to search for errors in the system.
- It can be used to predict potential system problems.
- It can be used as information for recovery in case of trouble.
- It can be used as evidence for infringement.
- Log management is mandated by various laws and guidelines.

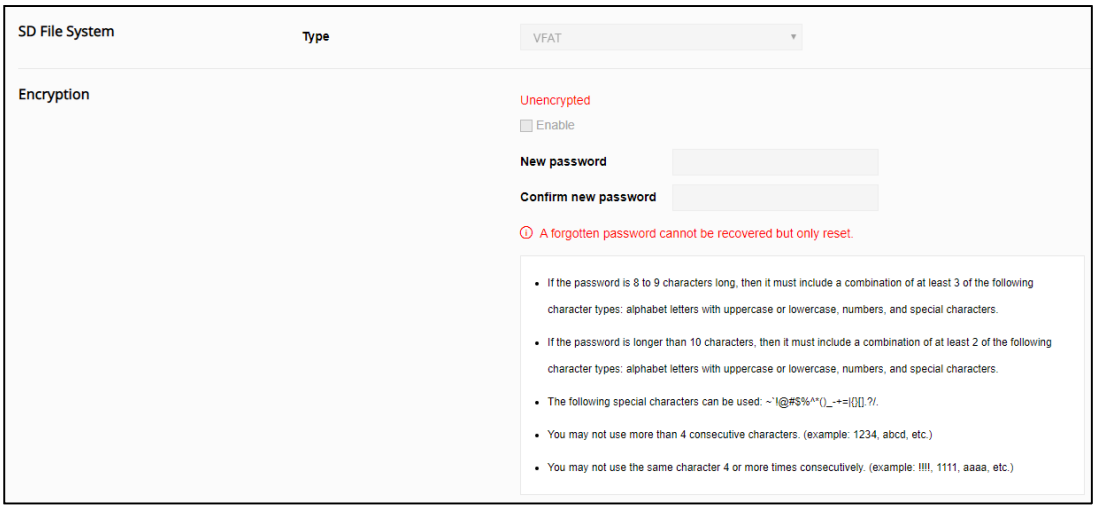
For example, if your password entry fails consecutively, your account may be locked. Access log searches can identify these types of attacks, such as a large number of login failures or account lockouts.

- IP camera setup → System → User → Log



5.13. Encryption of stored data (LUKS encryption)

The data encryption function is a function that encrypts data stored in the SD card so that it cannot be checked even if it is leaked. Since the initial value is inactive, it is used by activating the corresponding setting when saving data to the SD card. Password is required for use. Even when changing the SD card encryption function settings, the set password is required, and if the password is lost, the SD card must be formatted and used again, so it is necessary to securely manage the password.



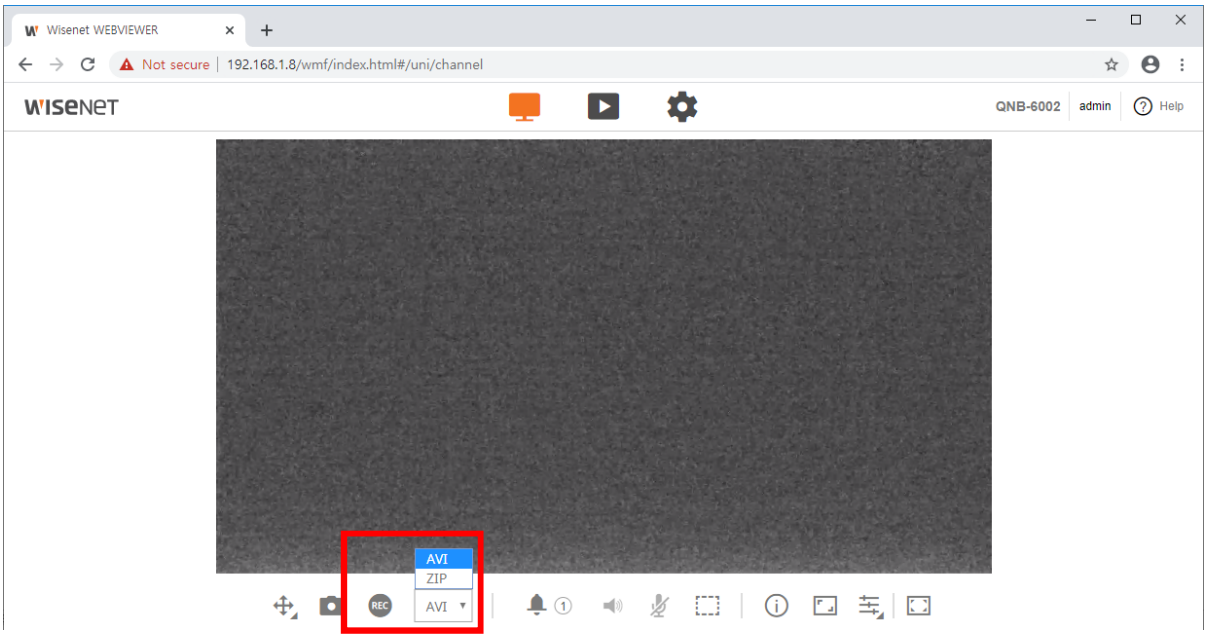
5.14. Backup data encryption (ZIP file encryption)

When extracting data stored on the SD card to the outside or recording live video, the backup file can be set as an AVI or ZIP file. When it is set to AVI, important information may be exposed because it is not encrypted, but if it is set as a ZIP file, it can be encrypted to prevent exposure. When encrypting the ZIP file, a password is required. If the password is not entered, the ZIP file encryption is not applied.

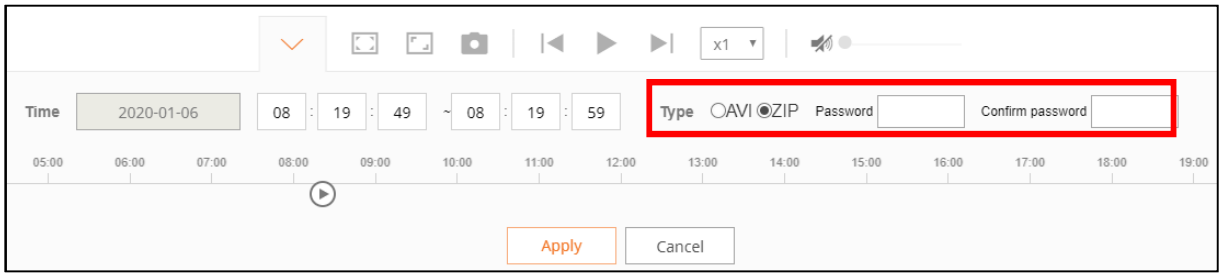
- When recording video on the live screen

5. Secure Level

- When recording video on the live screen



- When backing up video on the Playback screen



6. Very Secure Level

Hanwha Techwin devices can improve security by linking the security functions provided by the devices with external security solutions.

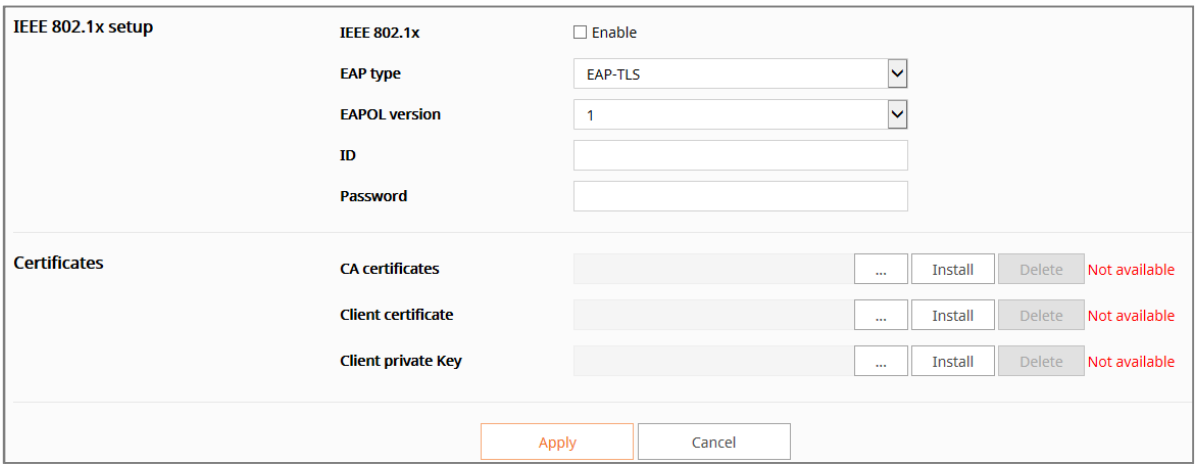
< Table 7 >

Security Policy	Features for Cyber Security	Brief Description
-	802.1 X Certificate-based access control	Enhanced security environment with port-based access control settings

6.1. 802.1 X Certificate-based access control

Setting up port-based access control for network devices, such as network switches, bridges, and wireless access points (APs), allows a more robust network security environment. Hanwha Techwin camera supports 802.1X EAP-LEAP and EAP-TLS which is a standard method that requires certificates. To use this feature, you need a network switch (or bridge, wireless AP, etc.) that supports 802.1X, 802.1X authentication server, device certificate, and private key.

1) IP camera setup → Network → 802.1x → IEEE 802.1x setting
2) Check 'Use' and select 'EAP-TLS' for EAP type.
3) Select 1 or 2 for EAPOL version.
4) Input the ID and password of client certificate.
5) Install a CA certificate.
6) Install a client certificate and private key for port-based access control.
   - *Client certificate and private key is used for TLS communication between RADIUS server and client device.*
7) Click 'Apply'.



WISENET

Hanwha Techwin Co.,Ltd.
Hanwha Techwin R&D Center, 6, Pangyo-ro 319beon-gil,
Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 82.70.7147.8771-8
FAX 82.31.8018.3715
http://hanwha-security.com

Hanwha Techwin