WISENET

White paper

Network Hardening Guide

2018. 1. 16. (v2.0)

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'	

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

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.

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Default Level	Forced complex password setting	Default	-
	No initial password	Default	-
	Input limit for consecutive password failures	Default	-
	HTTP Authentication (Digest only)	Default	-
	No Backdoor (Telnet, SSH)	Default	-
	Preference information encryption	Default	-
	Firmware encryption	Default	-
	Watermark & encryption of extracted video	Default	-
	Maintained logs after factory reset	Default	-
	HTML5 non plug-in web viewer	Default	-
Protective Level	Perform Factory Reset	-	-
	Disabling guest login	Disabled	Disabled
	Disabling unauthenticated RTSP connections	Disabled	Disabled
	Disabling unused multicast	Disabled	Disabled
	Disabling unused DDNS	Off	Off
	Disabling unused QoS	Not set	Not set
	Disabling unused FTP	Disabled	Disabled
	Disabling unused audio input	Disabled	Disabled
	Using SNMP securely	Disabled	Disabled

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Secure Level	Firmware version checking and updating	-	-
	Setting the correct date & time	-	-
	HTTPS (Hanwha Techwin certificate)	Initial value	Change
	HTTPS (authenticated certificate)	HTTP	HTTPS (own certificate)
	Changing the default port	HTTP	HTTPS (authenticated certificate)
	IP Filtering	Initial value	Change
	Sending E-mail using TLS	Not set	Set
	Disabling unused Link-Local IPv4 address	Not use	Use
	Disabling unused UPnP	use	Not use
	Disabling unused Bonjour	use	Not use
	Creating additional user accounts	use	Not use
	Checking the log	-	-
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 1 >

Security Policy	Features for Cyber Security	Brief Description
Password policy	Forced complex password setting	Three or more combinations of uppercase and lowercase letters, numbers, and special characters for 8 letters long (2 combinations for 10 letters)
	No initial password	Password setting required for the first web UI login
	Input limit for consecutive password failures	Block password random input to web UI
User authentication	HTTP Authentication (Digest only)	Protect user password during HTTP comm.
Remote access control	No Backdoor (Telnet, SSH)	Remove all services that can access the system remotely
Preference information	Preference info. encryption	Protect backed up configuration Info.
Firmware	Firmware encryption	Protect critical info. from the firmware and prevents malware injection into the firmware
Extracted video	Watermark & encryption of extracted video	Ensure confidentiality and integrity of extracted video and authenticate origin
Log	Maintained logs after factory reset	Prevent malicious log deletion from intruders
HTML 5 Streaming	HTML5 non plug-in web viewer	Optimal video streaming without plug-in (Active X, Silverlight, NPAPI)

3.1. Forced complex password setting

Hanwha Techwin products require min. 8 character password. Depending on the length of the password, two (8 to 9 characters) or three (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. HTTP authentication (Digest only)

Since Hanwha Techwin NVR/IP camera provides the digest authentication HTTP mode by default, user password can be protected during information transmission / reception between server and client over HTTP. If clear text, base64 encoding, or basic authentication HTTP mode is used, an unauthorized person can get the password by packet monitoring on the network.

If it is need to protect user ID and video/data as well as user password, security level can be improved the by setting HTTPS mode (Refer to Table 3).

< Table 2 >

Option	Corresponding level	Initial value
HTTP (Do not use secure connection)	Default level	○
HTTPS (Secure connection mode using a unique certificate)	Secure level	X
HTTPS (Secure connection mode using the public certificate)	Secure level	X

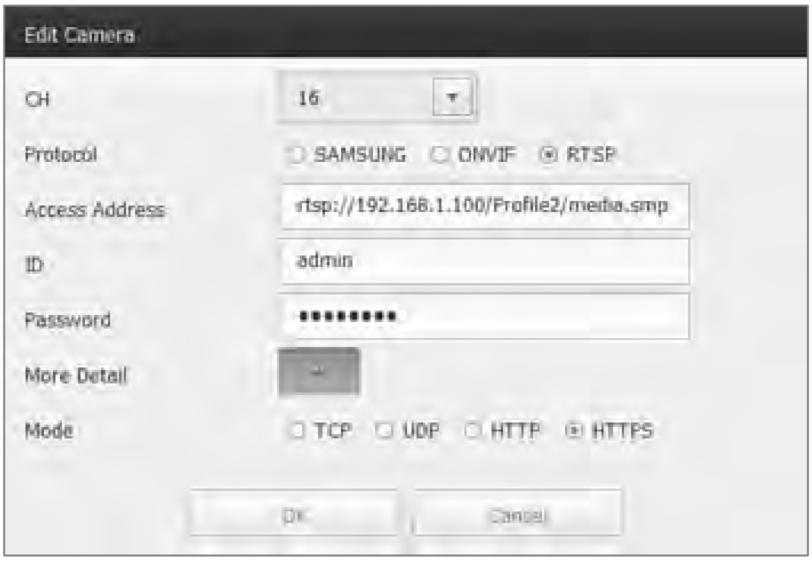
< Table 3 >

Mode	Password Protection	Video/Data Protection	User ID Protection	Use/Not use
HTTP (Basic)	X	X	X	Not use
HTTP (Digest)	○	X	X	Use (Default)
HTTPS	○	○*	○	Use

* HTTPS mode protects only the data transmitted in the HTTP protocol like user authentication. To protect the video streaming transmitted by the RTSP protocol, the client terminal needs to perform additional setup task of tunneling RTSP to HTTPS.

For example, if you want to protect the video transmitted from IP camera to NVR with HTTPS, first set the mode of IP camera to HTTPS through camera web viewer. IP camera web viewer does not have a part to set RTSP over HTTPS mode, so it is necessary to connect the camera to the NVR and set the corresponding mode through the NVR or web viewer as follows.

- In NVR web viewer, Device → Camera → Cam Registration → Select a channel → Edit Camera



Edit Camera

CH: 16

Protocol: ○ SAMSUNG ○ ONVIF ● RTSP

Access Address: rtsp://192.168.1.100/Profile2/media.smp

ID: admin

Password: ●●●●●●●●●

More Detail

Mode: ○ TCP ○ UDP ○ HTTP ● HTTPS

3.5. No backdoor (Telnet, SSH)

If a network device supports remote services such as telnet, it is advantageous for the manufacturer to easily provide the customer service. However, if there is a hacker or a malicious intentional manufacturer, this can be a factor that causes the most dangerous security incidents.

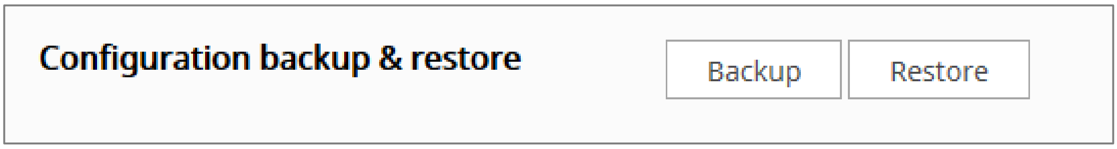
Hanwha Techwin has improved security by eliminating these risks in consideration of the safety of customer information, not service convenience.

3.6. Preference information encryption

The backup function allows you to save a binary file containing the configuration information of the current device (except IP & Port, DDNS, IP filtering, HTTPS, 802.1x, QoS, SNMP). It is able ton restore the configuration information that was backed up through the Restore function.

By using these functions, user can set the same configuration 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 uses the secure encryption algorithm to save the configuration information when backing it up.

- In camera web viewer, System → Upgrade / Reboot → Configuration backup & restore



3.7. Firmware encryption

Manufacturers provide firmware for product additions / bugs and security improvements on their official website. This firmware contains more important information than people usually think.

Hanwha Techwin's firmware is encrypted to protect important internal information and prevent malware infiltration like backdoor, so user can safely upgrade with the latest firmware.

3.8. Watermark & encryption of extracted video

Video files extracted by SEC format using Hanwha Techwin NVR and SSM(VMS) can not be opened with normal playback / editing software, so file forgery can be prevented.

- SEC file player is included automatically when extracting the SEC file.

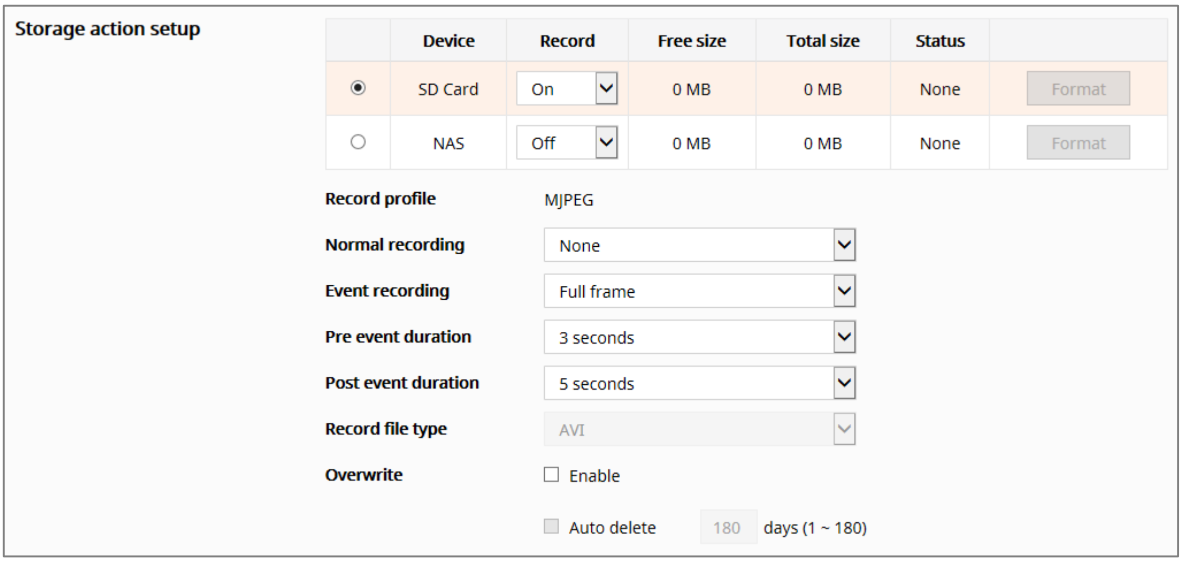
If you want to extract a video file for legal or privacy protection needed, you can extract it in SEC format with password setting. Watermarking and encryption are applied to the extracted SEC file to ensure that the video is tamper-proof and confidential. If the SEC file is extracted from the SSM(VMS), the digital signature function is additionally supported and also it is possible to technically confirm that it was extracted from Hanwha Techwin's SSM.

< Table 4 >

Device	Method	Backup Format	Watermarking /Encryption	Digital Signature	Player
Camera	Web viewer	AVI	X	X	general video player
NVR	Set	NVR	X	X	Only playable on set
		SEC	O	X	Backup viewer
	Web viewer	SEC	O	X	Backup viewer
		AVI	X	X	general video player
VMS(SSM)	-	SEC	O	O	Backup viewer
		AVI	X	X	general video player

3. Default Level

- IP camera setup → Event → Storage → Storage action setup → Select a Device



Storage action setup

	Device	Record	Free size	Total size	Status	
●	SD Card	On	0 MB	0 MB	None	Format
○	NAS	Off	0 MB	0 MB	None	Format

Record profile MJPEG

Normal recording None

Event recording Full frame

Pre event duration 3 seconds

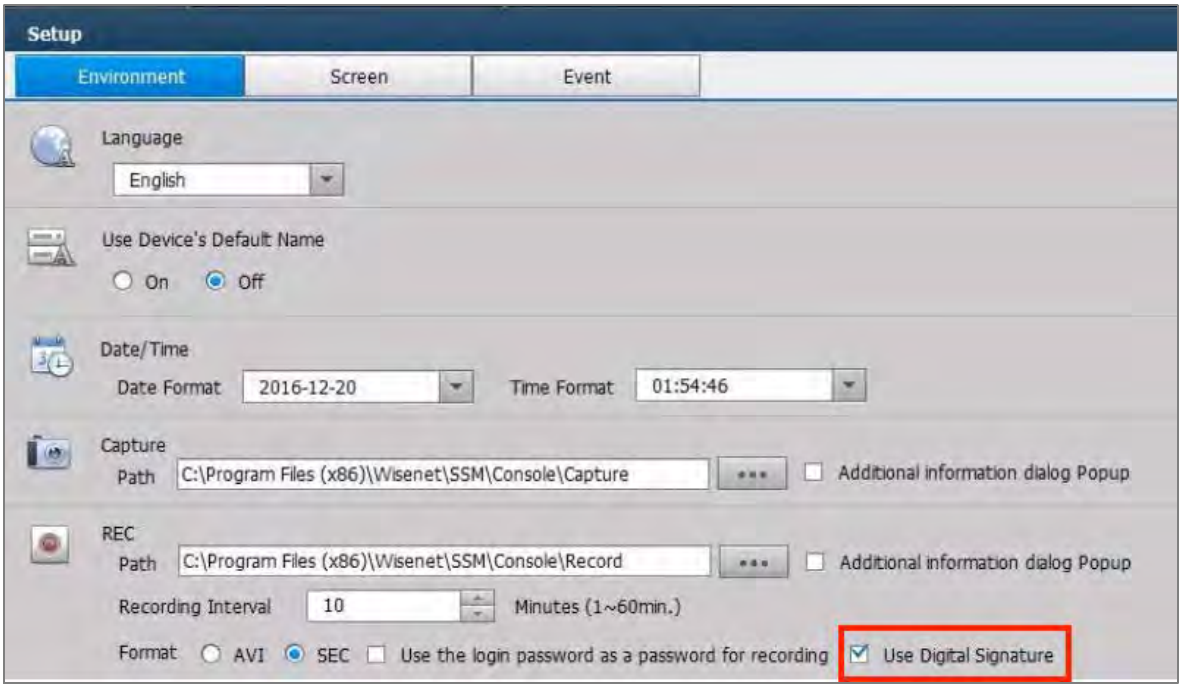
Post event duration 5 seconds

Record file type AVI

Overwrite □ Enable

□ Auto delete 180 days (1 ~ 180)

- SSM console setup → Environment → REC → Format



Language
English

Use Device's Default Name
○ On ● Off

Date/Time
Date Format 2016-12-20 Time Format 01:54:46

Capture
Path C:\Program Files (x86)\Wisenet\SSM\Console\Capture ••• □ Additional information dialog Popup

REC
Path C:\Program Files (x86)\Wisenet\SSM\Console\Record ••• □ Additional information dialog Popup

Recording Interval 10 Minutes (1~60min.)

Format ○ AVI ● SEC □ Use the login password as a password for recording ☑ Use Digital Signature

3.9. 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.

3.10. HTML5 non plug-in web viewer

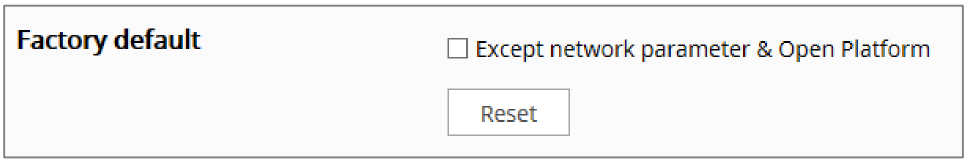
Most video surveillance devices provide web viewer video streaming service using the plug-in (ActiveX, Silverlight, NPAPI) installed into a web browser. However, such plug-in have high possibility of security vulnerabilities and exposures. Recently, malicious code infections are frequently caused by 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.

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'.



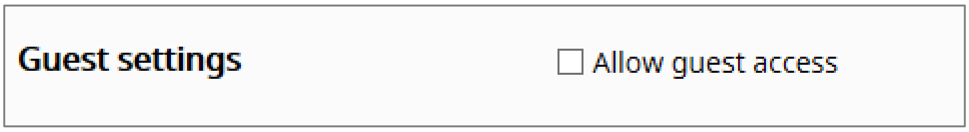
Factory default

□ Except network parameter & Open Platform

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



Guest settings

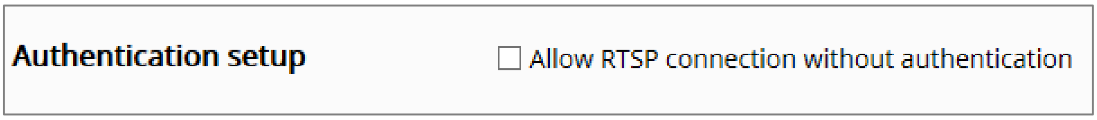
□ Allow guest access

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'



Authentication setup □ Allow RTSP connection without authentication

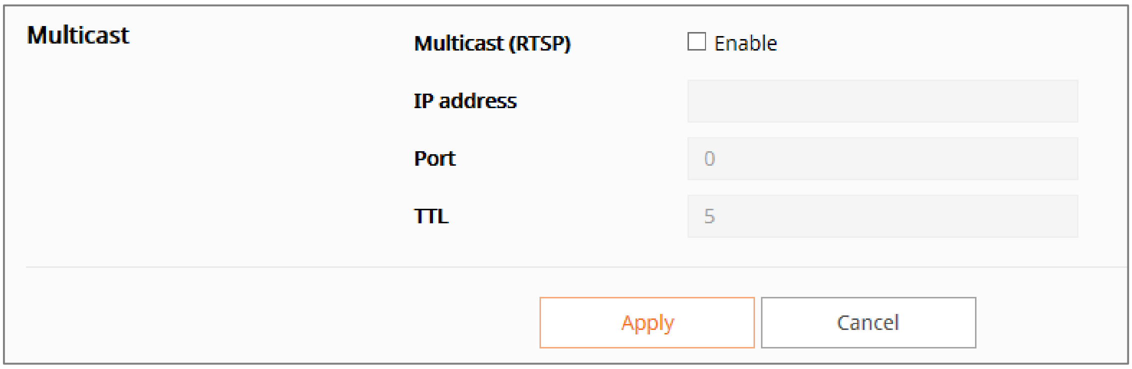
4.4 Disabling unused multicast

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'.



Multicast

Multicast (RTSP) □ Enable

IP address

Port 0

TTL 5

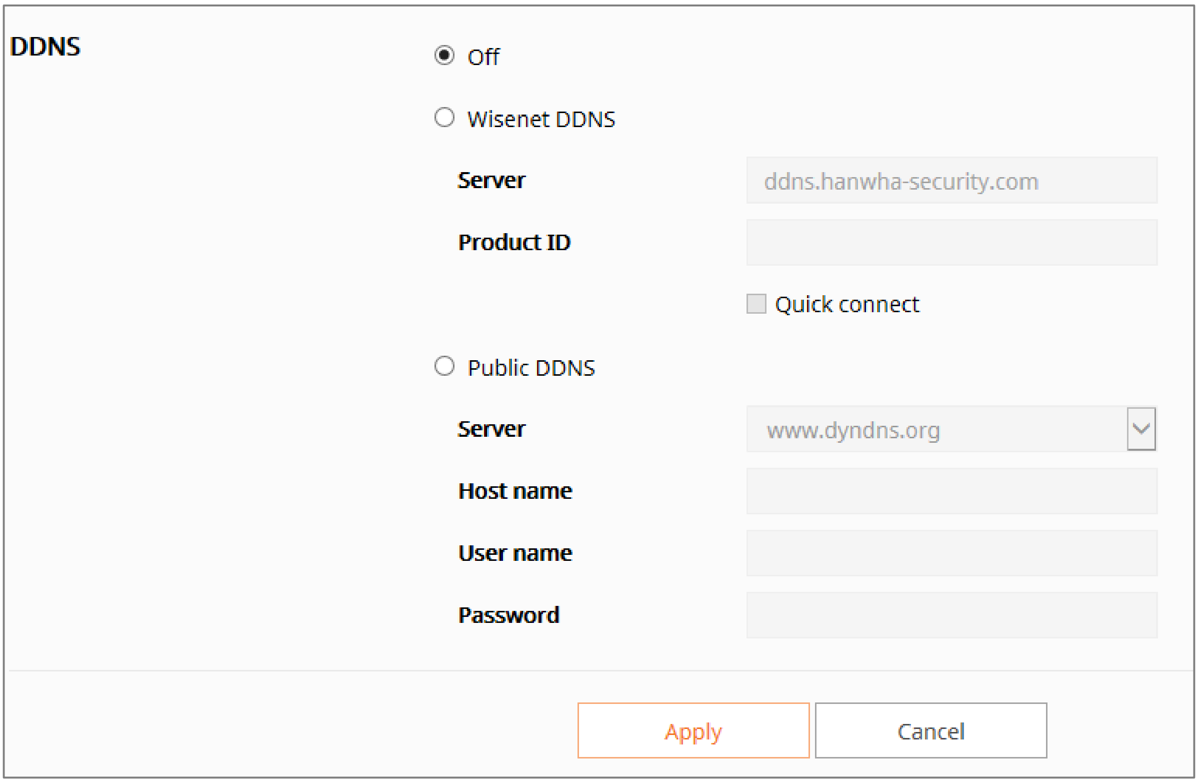
4.5. Disabling unused DDNS

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'.



DDNS

● Off

○ Wisenet DDNS

Server: ddns.hanwha-security.com

Product ID:

□ Quick connect

○ Public DDNS

Server: www.dyndns.org

Host name:

User name:

Password:

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. 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'.

4.9. Using SNMP securely

SNMP can be used to manage network devices conveniently. However, SNMP v1 and v2c are vulnerable because they use plain text community strings. Therefore, in order to use SNMP securely, it is recommended to use SNMP v3 only. By default, SNMP is disabled in Hanwha Techwin devices for security. If you want to use SNMP v3, HTTPS setting is a prerequisite. If HTTPS (Use own certificate) is already set in the previous section, 1) ~ 2) of the following procedure can be omitted.

1) IP camera setup → Network → HTTPS → Secure connection system
2) Chose 'HTTPS (Secure connection mode using a unique certificate)' and Click 'Apply'.
3) Network → SNMP
4) Uncheck SNMP v1 and v2c then check SNMP v3 and set password

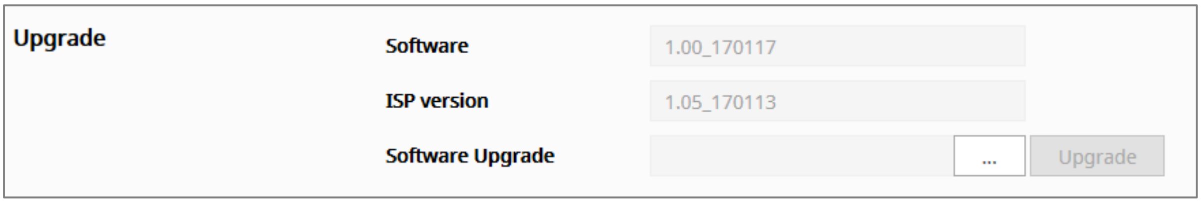
5.1. Checking the version of firmware and updating

It is able to check and download the latest firmware version of the products you use through the website of Hanhwa Techwin.

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

Through the web browser of product, you can check the current firmware version and the distribution date. Please check the firmware version of your current product and always update to the latest version.

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'



Upgrade

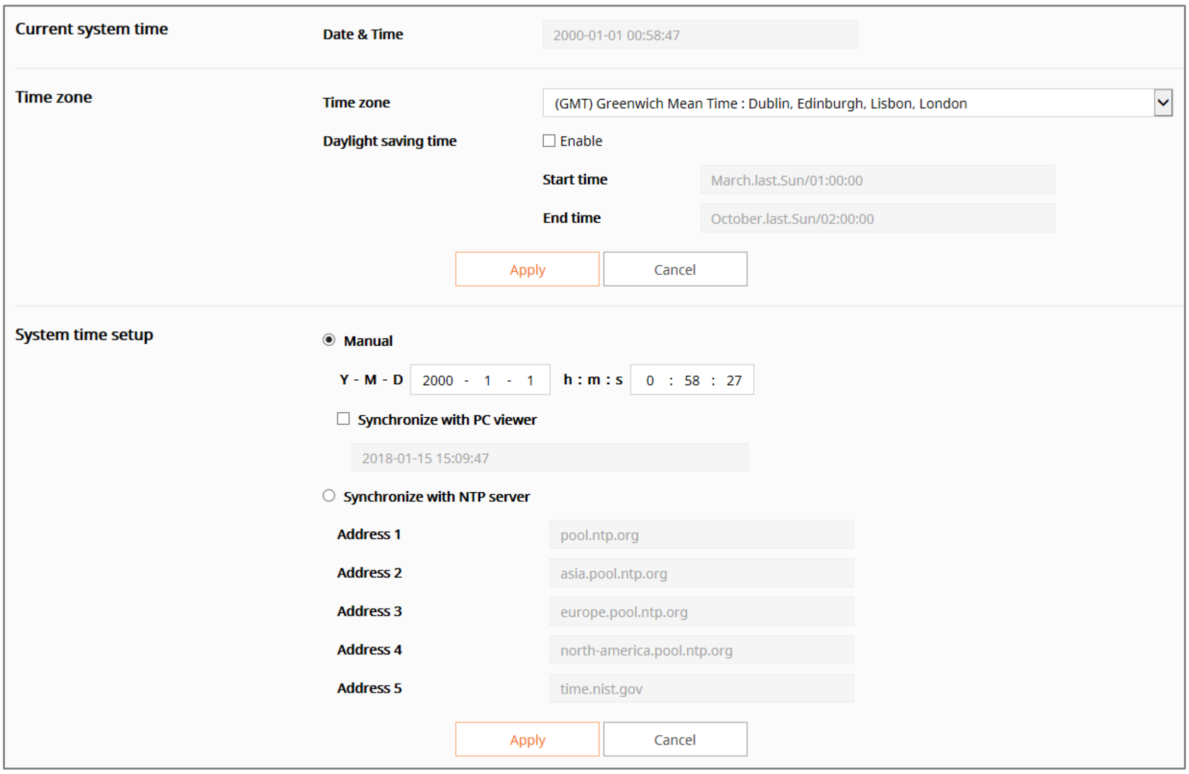
Software	1.00_170117
ISP version	1.05_170113
Software Upgrade	

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.



Current system time — Date & Time: 2000-01-01 00:58:47

Time zone — Time zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight saving time: □ Enable

Start time: March.last.Sun/01:00:00

End time: October.last.Sun/02:00:00

System time setup

● Manual

Y - M - D: 2000 - 1 - 1 h : m : s: 0 : 58 : 27

□ Synchronize with PC viewer

2018-01-15 15:09:47

○ Synchronize with NTP server

Address 1: pool.ntp.org

Address 2: asia.pool.ntp.org

Address 3: europe.pool.ntp.org

Address 4: north-america.pool.ntp.org

Address 5: time.nist.gov

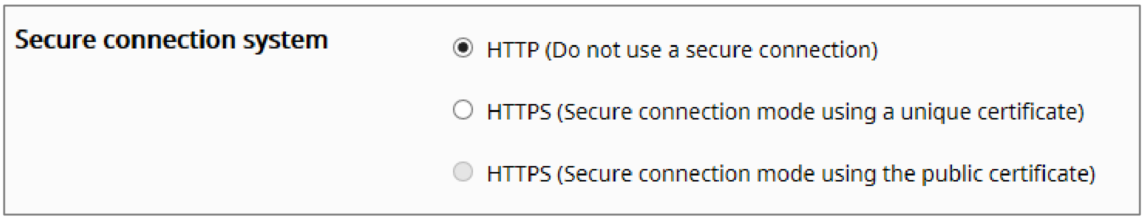
5.3. HTTPS (Hanwha Techwin certificate)

It is a function that enables secure connection between the device and client using the certificate provided by Hanwha Techwin. If you select 'HTTPS (Secure connection mode using a unique certificate)', the device's built-in 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’.



Secure connection system

● HTTP (Do not use a secure connection)

○ HTTPS (Secure connection mode using a unique certificate)

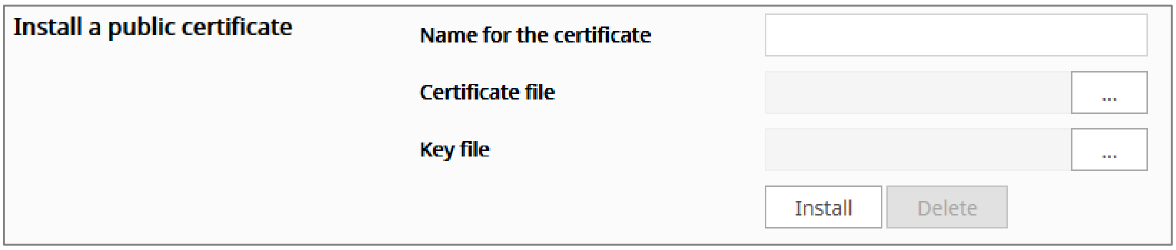
○ HTTPS (Secure connection mode using the public certificate)

5.4. 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).*



Install a public certificate

Name for the certificate	
Certificate file	...
Key file	...

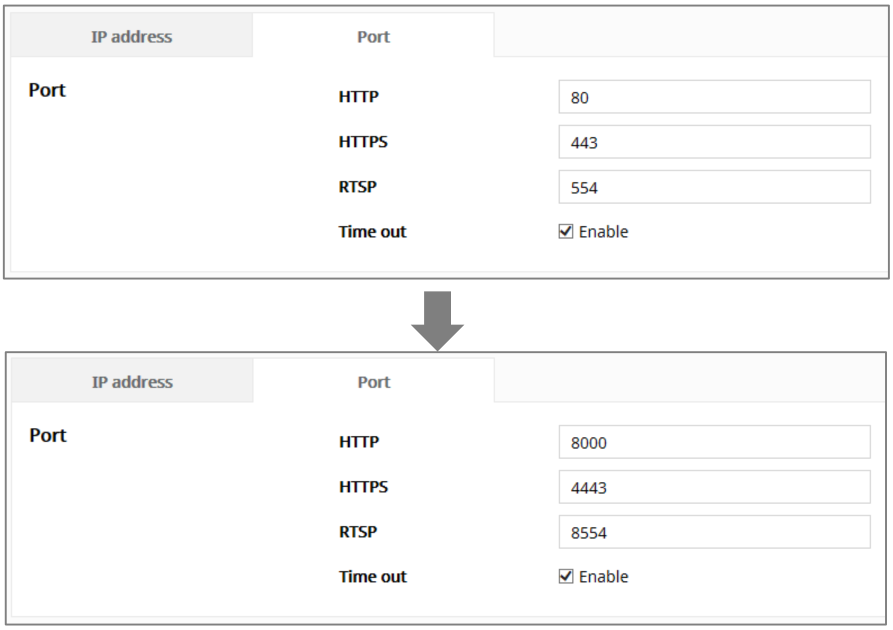
5.5. Changing the default port

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’.



Port

HTTP	80
HTTPS	443
RTSP	554
Time out	☑ Enable

Port

HTTP	8000
HTTPS	4443
RTSP	8554
Time out	☑ Enable

- *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.*

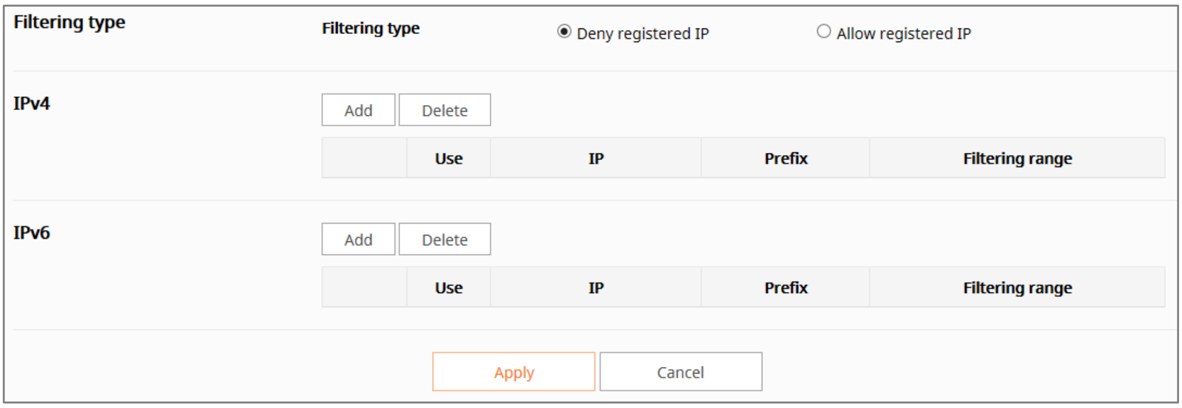
5.6. IP Filtering

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.


Filtering type

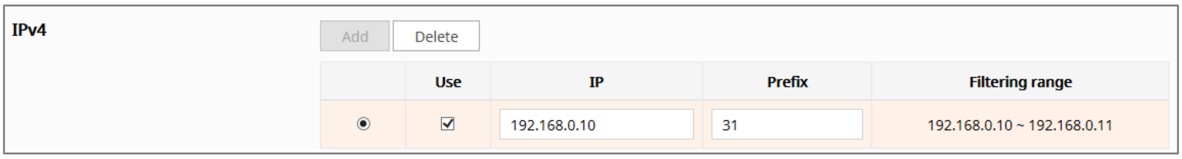
Filtering type ● Deny registered IP ○ Allow registered IP

IPv4

	Use	IP	Prefix	Filtering range

IPv6

	Use	IP	Prefix	Filtering range



IPv4

	Use	IP	Prefix	Filtering range
●	☑	192.168.0.10	31	192.168.0.10 ~ 192.168.0.11

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.*

5.7. 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’.

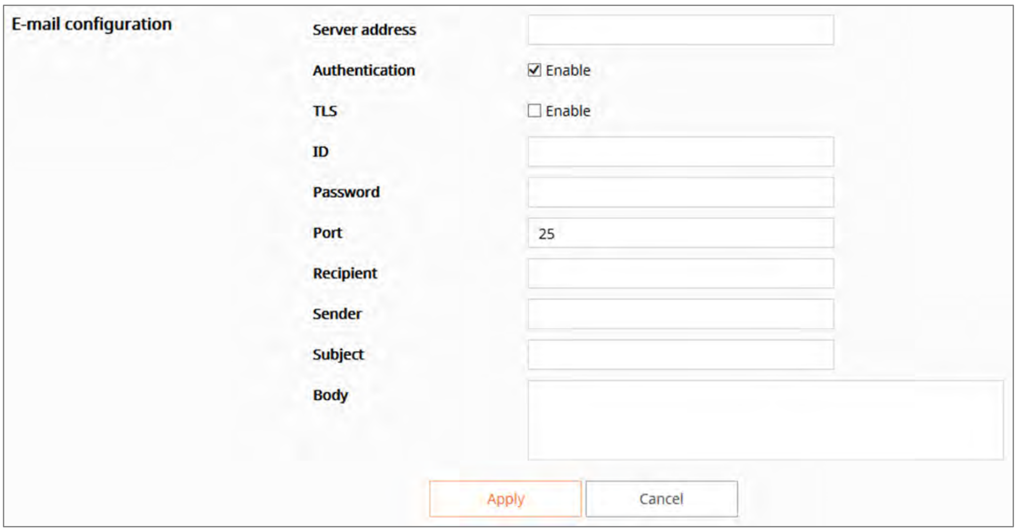
4) Enter the user account ID and password to connect to the email server.

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.



E-mail configuration

Server address	
Authentication	☑ Enable
TLS	□ Enable
ID	
Password	
Port	25
Recipient	
Sender	
Subject	
Body	

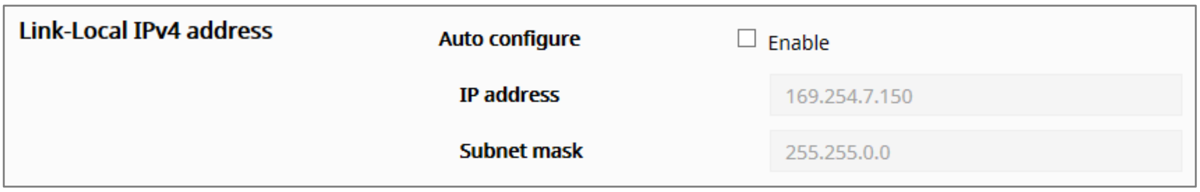
5.8. Disabling unused Link-Local IPv4 address

The Link-Local IPv4 address auto-configuration function assigns the IP address of 169.254.xxx.xxx to the camera like a DHCP server in a link-local network (meaning a network connected by one link like the camera and host connected to the same switch) where no IP is assigned. If you think the service is unnecessary, make sure to deselect the service feature for added security.

1) IP camera setup → Network → Auto IP configure → Link-Local IPv4 address

2) Uncheck ‘Auto configure’.

3) Click ‘Apply’.



Link-Local IPv4 address	Auto configure	□ Enable
	IP address	169.254.7.150
	Subnet mask	255.255.0.0

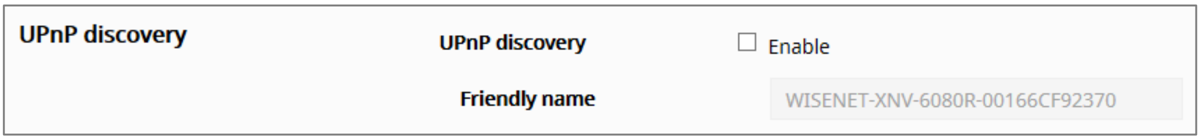
5.9. Disabling unused UPnP

The UPnP discovery is a function that supports automatic UPnP protocol search for clients and operating systems. If you think the service is unnecessary, you may want to opt out of setting up the service.

1) IP camera setup → Auto IP configure → UPnP discovery

2) Uncheck ‘UPnP discovery’.

3) Click ‘Apply’.



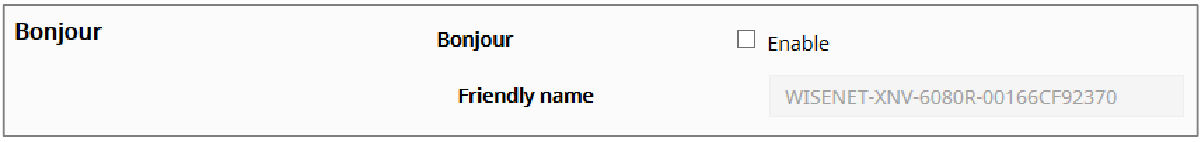
UPnP discovery	UPnP discovery	□ Enable
	Friendly name	WISENET-XNV-6080R-00166CF92370

5.10. Disabling unused Bonjour

The Bonjour is a function that allows the client and operating system that supports the Bonjour protocol to automatically search for cameras. If you think the service is unnecessary, make sure to deselect the service feature for added security.

1) IP camera setup → Auto IP configure → Bonjour

2) Uncheck 'Bonjour and click 'Apply'.



Bonjour

Bonjour	☐ Enable
Friendly name	WISENET-XNV-6080R-00166CF92370

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.

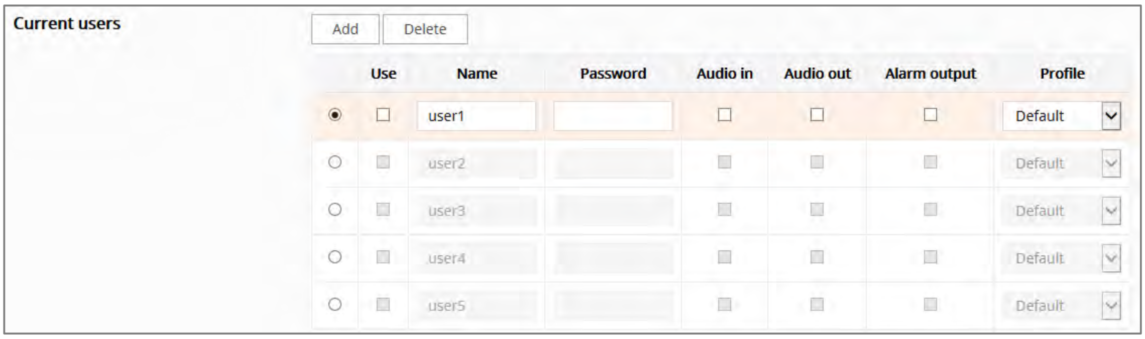
1) IP camera setup → Basic → User → Current users

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'.



Current users

	Use	Name	Password	Audio in	Audio out	Alarm output	Profile
●	☐	user1		☐	☐	☐	Default
○	☐	user2		☐	☐	☐	Default
○	☐	user3		☐	☐	☐	Default
○	☐	user4		☐	☐	☐	Default
○	☐	user5		☐	☐	☐	Default

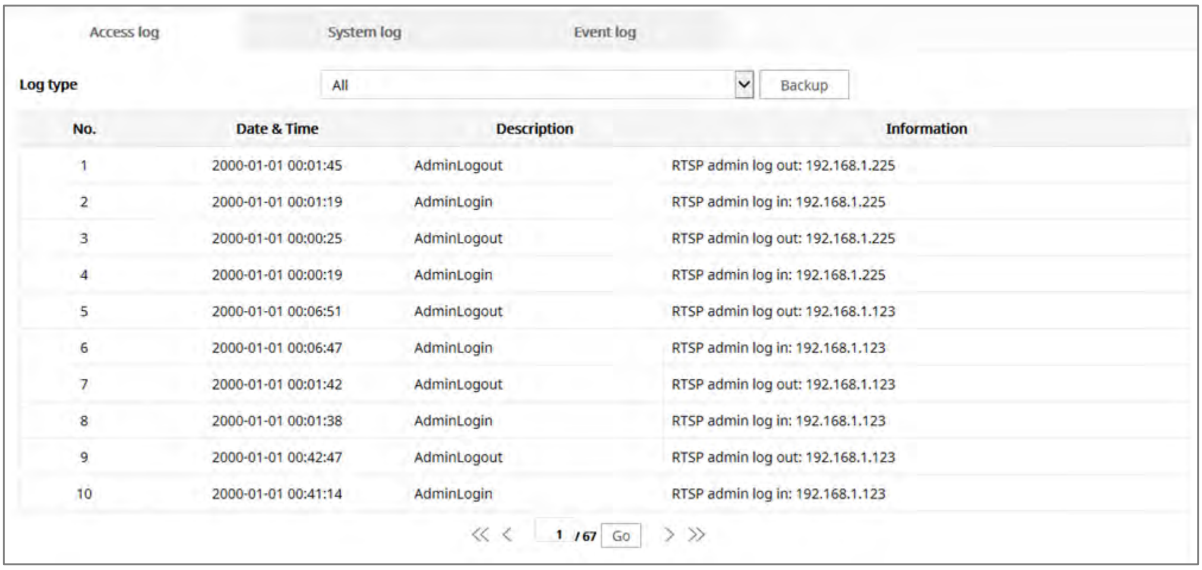
5.12. Checking the log

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



Log type: All

No.	Date & Time	Description	Information
1	2000-01-01 00:01:45	AdminLogout	RTSP admin log out: 192.168.1.225
2	2000-01-01 00:01:19	AdminLogin	RTSP admin log in: 192.168.1.225
3	2000-01-01 00:00:25	AdminLogout	RTSP admin log out: 192.168.1.225
4	2000-01-01 00:00:19	AdminLogin	RTSP admin log in: 192.168.1.225
5	2000-01-01 00:06:51	AdminLogout	RTSP admin log out: 192.168.1.123
6	2000-01-01 00:06:47	AdminLogin	RTSP admin log in: 192.168.1.123
7	2000-01-01 00:01:42	AdminLogout	RTSP admin log out: 192.168.1.123
8	2000-01-01 00:01:38	AdminLogin	RTSP admin log in: 192.168.1.123
9	2000-01-01 00:42:47	AdminLogout	RTSP admin log out: 192.168.1.123
10	2000-01-01 00:41:14	AdminLogin	RTSP admin log in: 192.168.1.123

6. Very Secure Level

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.

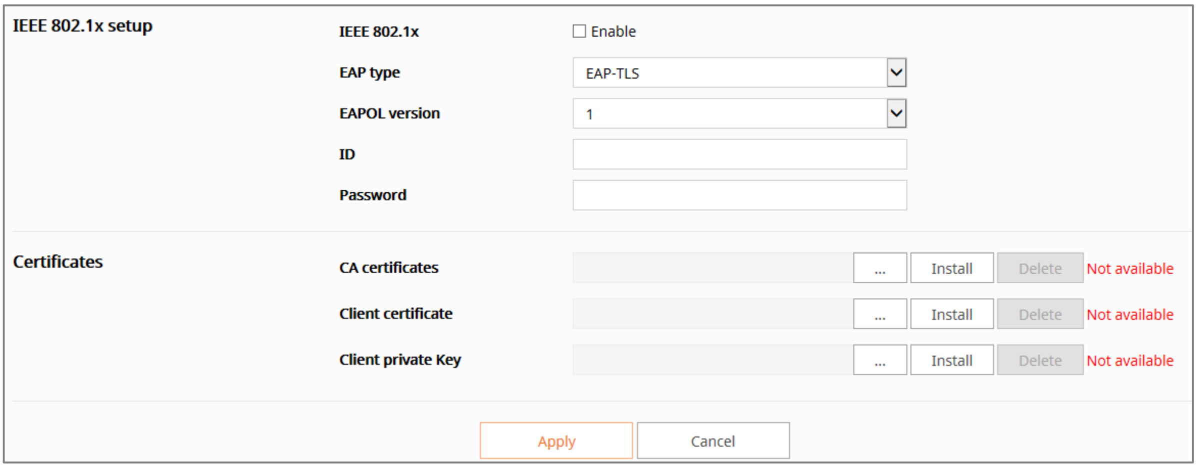
4) Input the ID and password of client certificate.

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’.



IEEE 802.1x setup

IEEE 802.1x: □ Enable

EAP type: EAP-TLS

EAPOL version: 1

ID:

Password:

Certificates

CA certificates: ... Install Delete Not available

Client certificate: ... Install Delete Not available

Client private Key: ... Install Delete Not available

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