WISENET

White Paper:
Network Hardening Guide

Hanwha
Techwin America

hanwhasecurity.com

Contents

Introduction

In the video surveillance market, a paradox has emerged where network surveillance devices developed to protect customers' property and personal information in recent years are used as a means of seizing sensitive personal and corporate information. Network surveillance devices process and manage video data that can be used as sensitive personal information. Since it is placed on the network, remote access is possible from anywhere in the world where the network is connected. Because of this nature, network surveillance device are subject to ongoing cyber-attacks in an attempt to penetrate the local network.

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 products.

It is important to note that the configuration changes described and shown in this document refer to the web viewer user interface. The Wisenet Device Manager can be used to push configuration changes in bulk to IP cameras allowing for a quick and consistent configuration of key security settings.

In the following guide, directions and screenshots will be given for Hanwha Techwin IP cameras. Many of the configuration items also apply to NVR products, with slight changes to menu location.

This guide defines cyber security levels according to the following criteria, each level building on and assuming the previous level has been implemented.

- The product design level is the level of security that users can achieve with the cyber security product design provided by the device, without any 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 as well as keeping it up to date and reviewing system logs.
- The very secure level means the level of security that can be achieved by combining the security features provided with additional external security solutions.

< Table 1 >

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Product Design 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	
	Configuration file encryption	Default	
	Firmware encryption	Default	
	Watermark & encryption of extracted video	Default	
	Maintained logs after factory reset	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
Secure Level	Checking the version of firmware and updating	-	
	Setting the correct date & time	Initial value	Change
	HTTPS (Hanwha Techwin certificate)	HTTP	HTTPS (own certificate)
	HTTPS (authenticated certificate)	HTTP	HTTPS (authenticated certificate)
	Changing the default port	Initial value	Change
	IP Filtering	Not set	Set
	Sending E-mail using TLS	Not use	Use
	Disabling unused Link-Local IPv4 address	Use	Not use
	Disabling unused UPnP	Use	Not use
	Disabling unused Bonjour	Use	Not use
	Using SNMP securely	SNMP v2c	SNMP v3
	Disabling unused SNMP	SNMP v2c	Not use
	Creating additional user accounts	-	
	Checking the log	-	
Very Secure Level	802.1 X Certificate-based access control	Not use	Use

Product Design Level

Hanwha Techwin develops products to ensure safety from cyber security threats by design, even with many default settings.

< Table 2 >

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 character length (2 combinations for 10 character length).
	No initial password	Password setting required for the first web viewer login
	Input limit for consecutive password failures	Block password guessing attempts
User authentication	HTTP Authentication (Digest only)	Protect user password during HTTP communications
Remote access control	No Backdoor (Telnet, SSH)	Remove all services that can access the system remotely
Preference information	Configuration file encryption	Protect backed up configuration information
Firmware	Firmware encryption	Protect critical information 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

Forced Complex Password Setting

Hanwha Techwin products require a minimum 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) are required. The policy limits the use of 4 or more repeated or sequential characters (aaaaa, abcde, qwerty, 12345). All standard keyboard special characters are allowed to ensure a complex password. A maximum password length of 15 characters is supported for NVR/DVR/IP camera and up to 31 characters for VMS. This enforcement helps to reduce the possibility of unauthorized password hijacking, guessing, or cracking by preventing the use of a weak password due to a user's carelessness.

Product Design Level

No initial password

If a user uses the initial password or cannot change the manufacturer'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 a user's mistake, all Hanwha Techwin products have no initial password and are designed to force setting the user's own password when accessing the UI of the product for the first time.

Input Limit for Consecutive Password Failures

Hackers systematically check common passwords and/or all possible passwords until the correct one is found. If this type of attack is allowed, the password will eventually be discovered given enough time. Hanwha Techwin devices prevent brute-force attack by blocking 5 or more authentication requests that occur within 30 seconds to improve its security. Existing connections of authorized users are maintained to prevent a denial-of-service from occurring while authentication requests are blocked. This temporary block will greatly increase the time required to guess the password, usually leading the hacker to choose a better target.

HTTP Authentication (Digest only)

Since Hanwha Techwin NVR/IP cameras provides digest authentication HTTP mode by default, user names & passwords are protected during information transmission / reception between server and client over HTTP. If clear text, base64 encoding, or basic authentication HTTP mode were to be allowed, the password can be easily discovered by packet monitoring the network.
If the transmitted video needs to be encrypted in addition to the password, the security level can be improved the configuring HTTPS mode (Refer to Table 3).

< Table 3 >

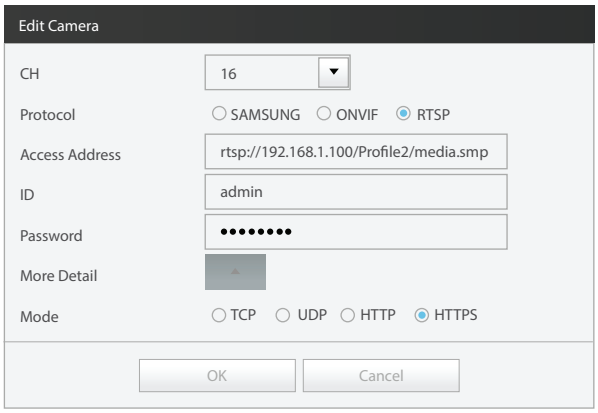
Option	Corresponding Level	Initial value
HTTP (Do not secure connection)	Default level	√
HTTPS (Secure connection mode using a unique certificate)	Secure level	X
HTTPS (Secure connection mode using a public certificate)	Secure level	X

< Table 4 >

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

* HTTPS mode protects only the data transmitted in the HTTP protocol such as user authentication and API commands. To protect the video streaming transmitted by the RTSP protocol, additional setup must be done to perform tunneling of RTSP over 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 configuration 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 as follows:

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



No Backdoor (Telnet, SSH)

If a network device supports remote services such as telnet, it is advantageous for the manufacturer to easily provide customer service. These services allow direct root access to the device, useful for troubleshoot and diagnostics. 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 eliminated these risks in consideration of the safety of customer information, not service convenience.

Configuration File 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). The administrator is then able to restore this configuration information that was backed up through the restore function.
By using these functions, the administrator 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 contains important information of the user's device environment, Hanwha Techwin uses a secure encryption algorithm to save the configuration information when backing it up.

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

Firmware Encryption

Manufacturers provide firmware for feature additions, bug fixes, and security improvements on their official website. This firmware controls how the product operates. If the file is tampered with, malicious software could be introduced.
Hanwha Techwin's firmware is encrypted to protect important internal information and prevent malware introduction such as a backdoor, so users can safely upgrade with the latest firmware. If a firmware is not encrypted, the file system, database structure, & underlying programming code can be examined and exploited.

Watermark & Encryption of Backup Video

Video files that have been backed-up in SEC format using Hanwha Techwin NVR and VMS cannot be opened with normal playback / editing software, so file forgery can be prevented.

• SEC file player is included automatically during the backup process.

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 backup SEC file to ensure that the video is tamper-proof and confidential. If the SSM VMS was used for backup, the digital signature function is also supported and provides additional cryptographic functions to quickly ensure the authenticity and integrity of the file.

< Table 5 >

Device	Method	Backup Format	Watermarking / Encryption	Digital Signature	Player
Camera	Web Viewer	STW	X	X	SD card player
		AVI*	X	X	General video player
NVR	Set	NVR	X	X	Only playable on set
		SEC*	√	X	Backup viewer
	Web Viewer	SEC*	√	X	Backup viewer
		AVI	X	X	General video player
Camera/ NVR via SSM	-	SEC*	√	√	Backup viewer
		AVI	X	X	General video player
Camera/NVR via SmartViewer	-	SEC*	√	X	Backup viewer
		AVI	X	X	General video player

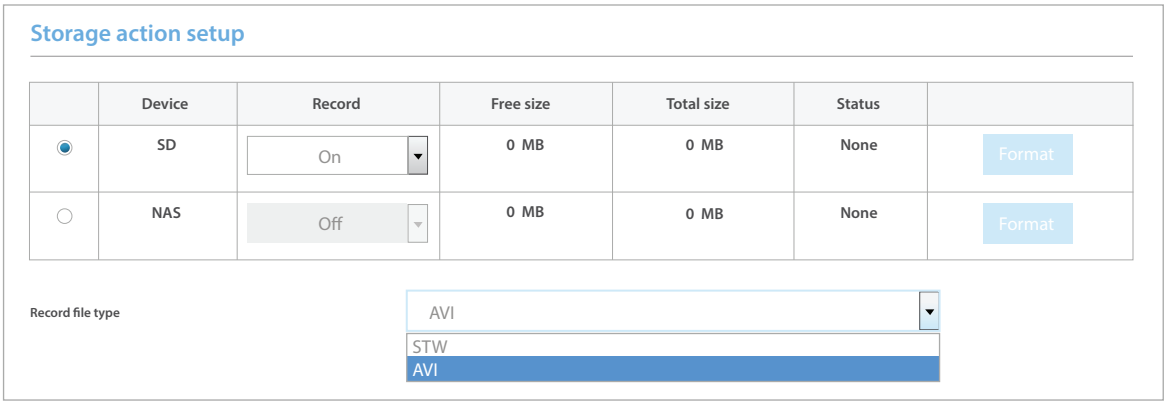
* Indicates default backup format.

Comparison of Digital Signature & Watermarking

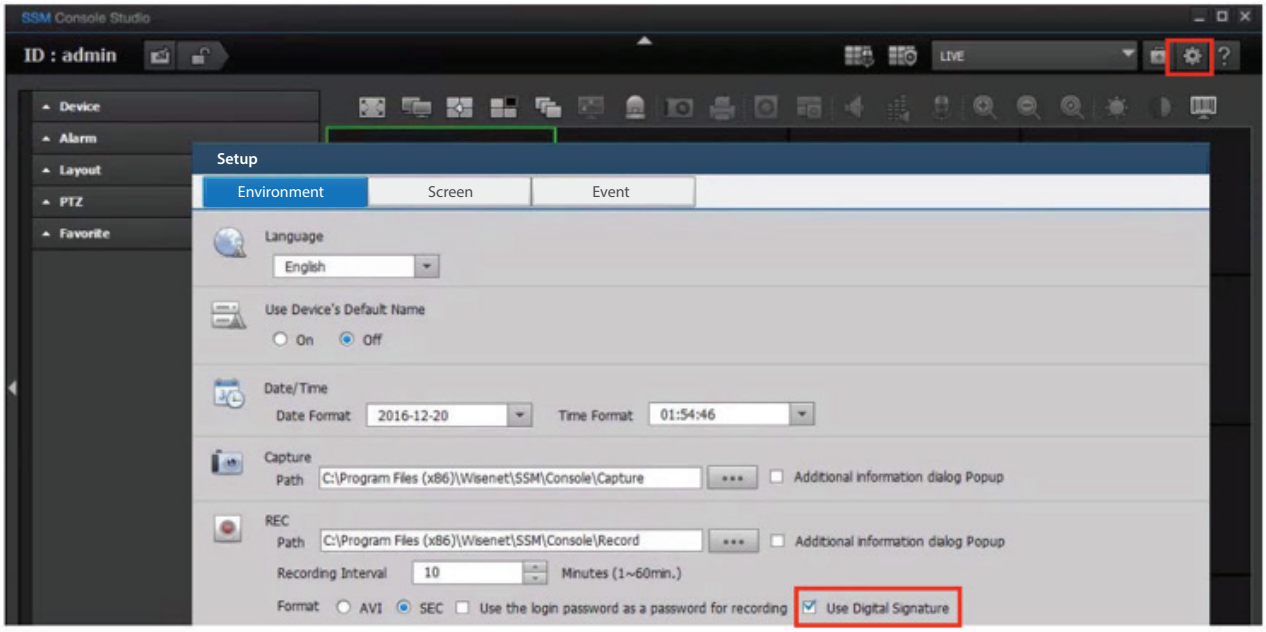
< Table 6 >

Digital Signature	Watermark
Can verify entire backup file data	Can verify each frame of backup file
Can verify video and audio data as well as header information	Can verify forged video or audio data, not header information tampering
Can verify in case an entire frame is removed	Cannot verify if an entire frame is removed
Cannot check the date/time of forged frame	Can check if the date / time of a frame is forged
Can verify entire file at once	Must playback entire file to determine forged frame
Supported by SSM	Supported by SmartViewer, SSM, NVR, DVR

• IP camera setup → Event → Storage → Storage action setup → Record file type



• SSM console setup → Environment → REC → Format



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 a trace. Hanwha Techwin's product is developed to retain log files from being erased by device power cycle or initialization (factory reset) to prevent such malicious intent. These logs can easily be downloaded individually or in bulk for forensic investigation. Most products have a System log, Event log, & an Access log.

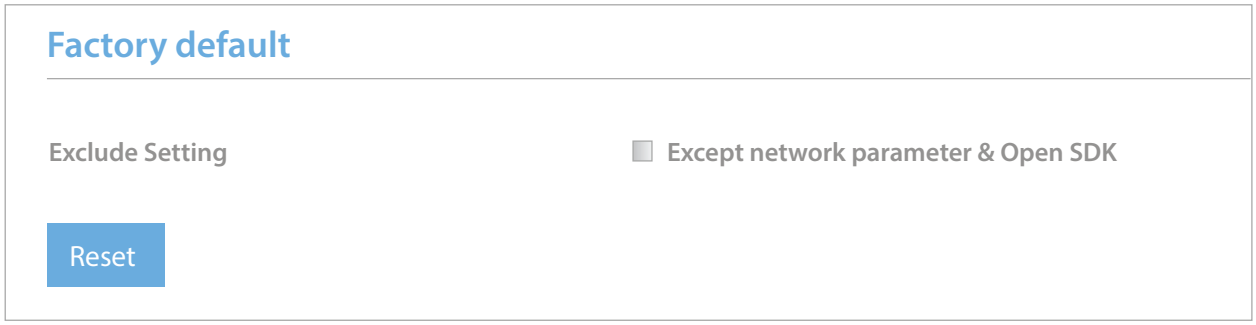
Protective Level

Perform Factory Default

If the device you want to set up is not in the initial state, it is recommended to perform a factory reset of the device to initialize the device's settings. If a device is thought to have been compromised or accessed by unauthorized individuals, it is recommended to factory default the device. Hanwha Techwin products can achieve the protective level of security with the initial state alone. The factory default can be executed through the Web Viewer, Wisenet Device Manager, or with hardware button.

To perform a factory default through Web Viewer:

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



* To factory default using the hardware button, press and hold the button for 5 seconds while device is powered on and fully booted up.

Disabling Guest Login

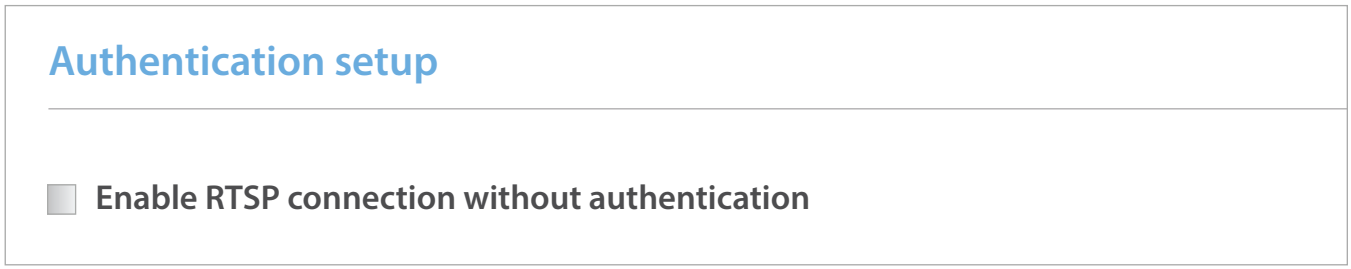
Hanwha Techwin cameras provide a guest login function. This guest account is limited because it allows only minimal privileges, but if the guest login is enabled, video streams may be exposed to unauthorized users. If guest access is not needed, guest login must be disabled. Guest login uses a username and password of guest.

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

Disabling Unauthenticated RTSP Connections

Hanwha Techwin cameras provide a function that allows RTSP connections 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.

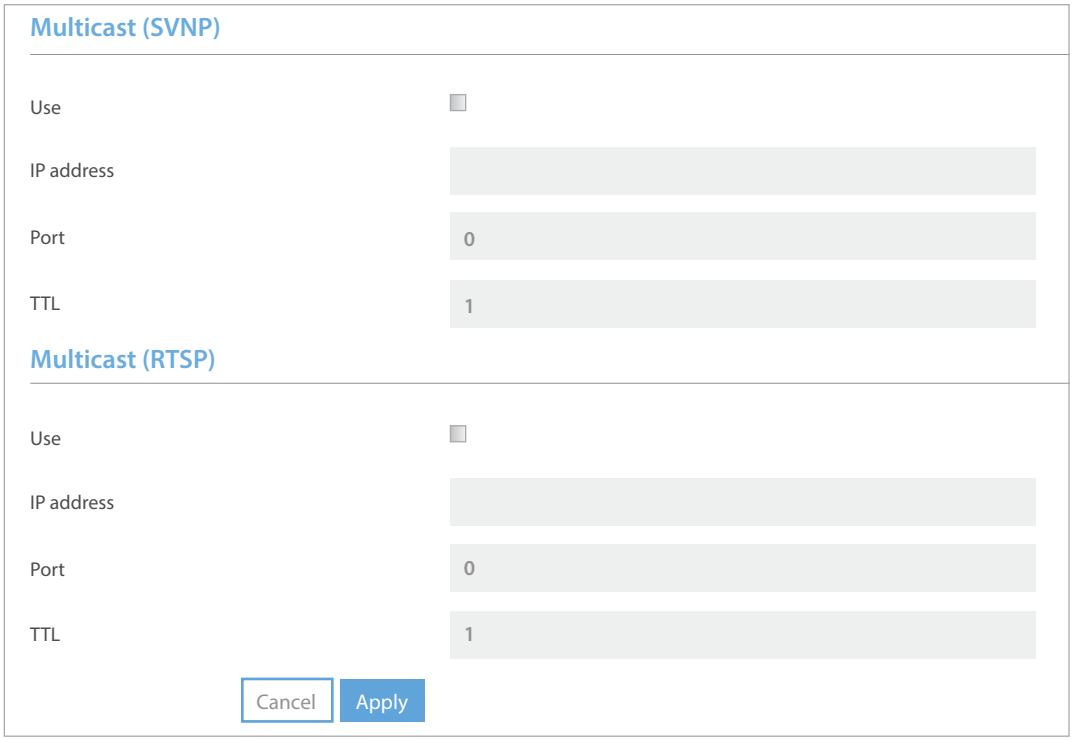
1) IP camera setup → Basic → User → Authentication setup
2) Uncheck 'Enable RTSP connection without authentication'



Disabling Unused Multicast

Hanwha Techwin cameras are able to multicast video stream using the SVNP and RTSP protocols. If these services are unnecessary, make sure to deselect the service features for added security.

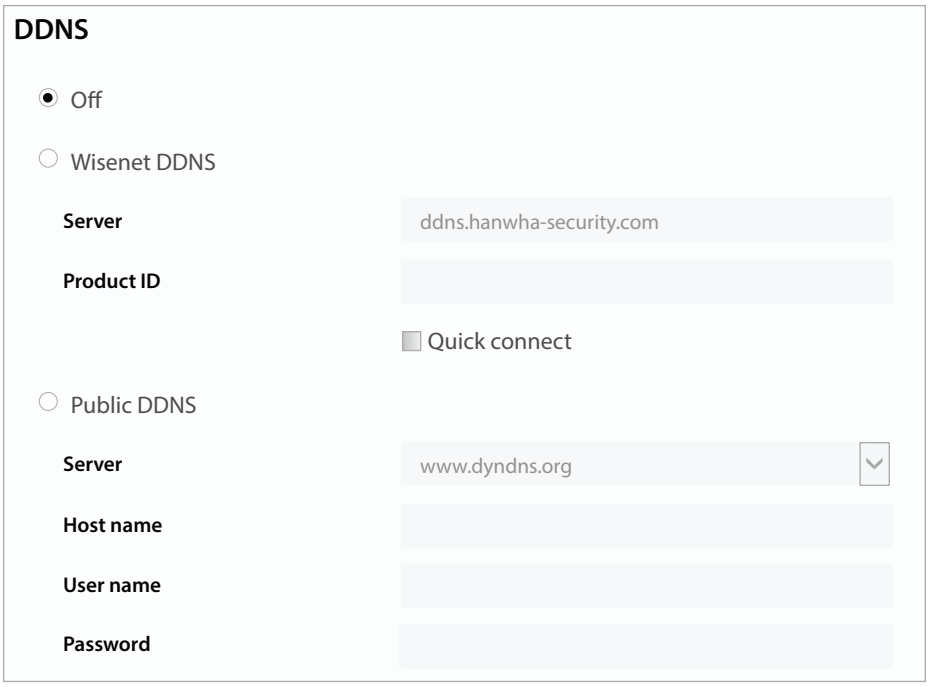
1) IP camera setup → Network → Video Profile
2) Uncheck 'Use' box of Multicast SVNP, RTSP.
3) Click 'Apply'.
4) Repeat for all other video profiles.



Disabling Unused DDNS

If your device is connected to the internet, the global IP address may occasionally change. In this case, the user will not know when the IP address changes and will not be able to view video. The DDNS function provides a fixed, user selected name to access the device, while keeping track of the current IP address and port. If the service is not being utilized, make sure to disable the service for added security.

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



Disabling Unused QoS

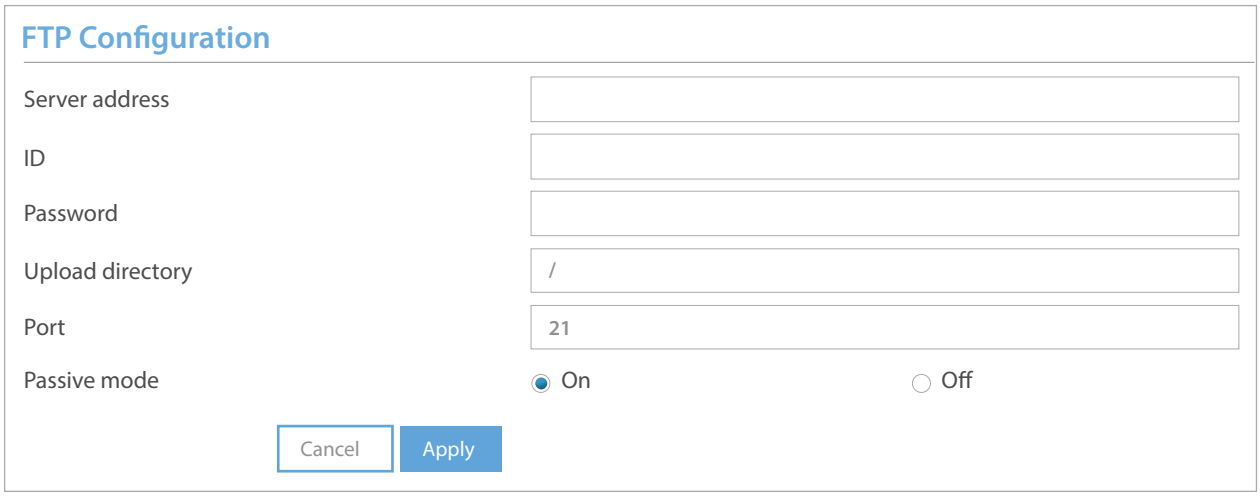
QoS (Quality of Service) is a function to set a priority level to guarantee the quality of video transmission to specific IP addresses. If you think the service is unnecessary, make sure to disable the service for added security.

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

Disabling Unused FTP

The FTP function is used for transferring images to a file server on a periodic timer schedule or when an alarm or event occurs. If you think the service is unnecessary, make sure to disable the service for added security.

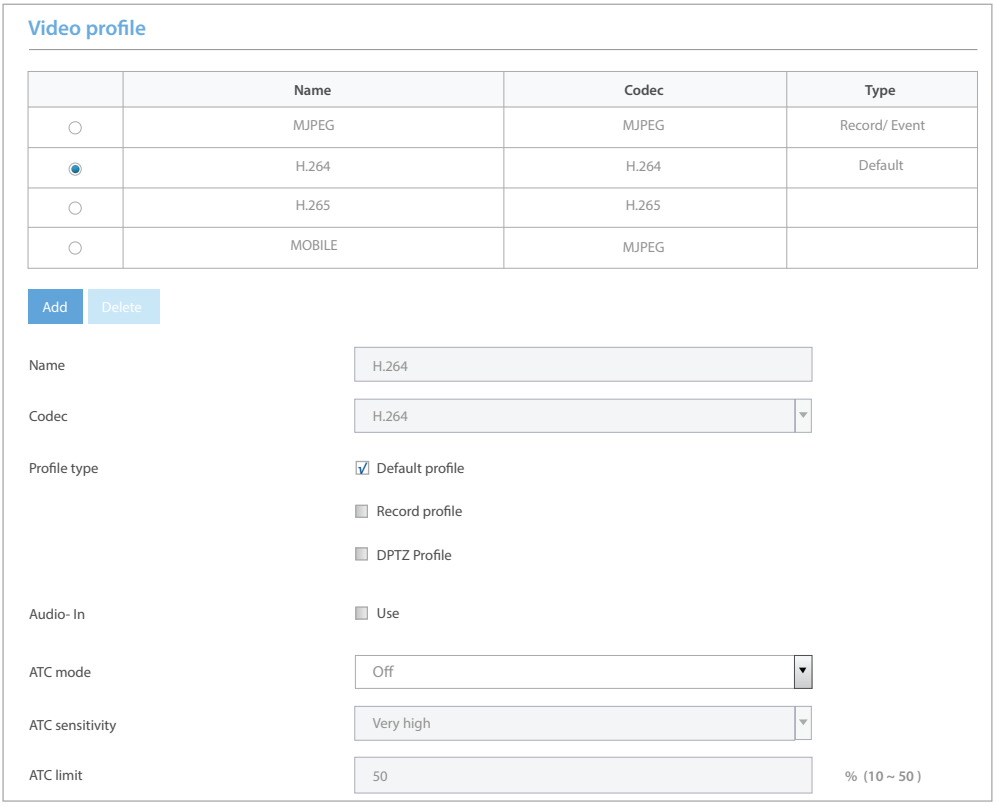
1) IP camera setup → Event → FTP/E-mail → FTP Configuration
2) Remove server address, ID and password.
3) Click 'Apply'.



Disabling Unused Audio Input

Audio Input is a function that allows you to input sound into the video stream from a line input, microphone input, or built-in microphone, depending on camera model. Using the audio input function may be illegal in certain states or installation locations where privacy is expected. The Audio Input function can be enabled or disabled for each user account, which can provide a way of restricting access to this function. If you think the feature is unnecessary, make sure to disable it for added security. The audio input function is set individually for each video profile, so it is necessary to select each profile and then disable the function.

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



Secure Level

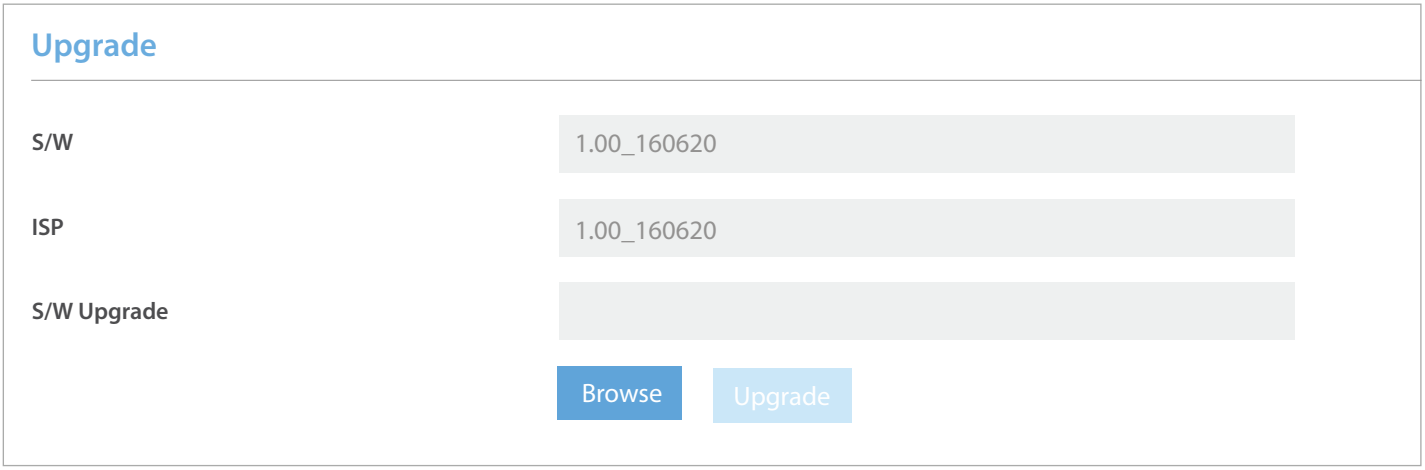
Checking the Version of Firmware and Updating

It is essential to update the firmware of any network-connected device to ensure you are operating with the latest features and security fixes. The firmware addresses issues that may have arisen after release of the product. The firmware is able to enhance and upgrade core components such as the webserver, database, etc. As the firmware upgrade takes a few minutes to process, it is recommended to perform it at a low risk time. Ensure the device has stable power while upgrading. All configuration is kept during the upgrade, and you can upgrade directly to the latest version in most cases. Please check the release notes included with the firmware download for any warnings. You can easily check and download the latest firmware of the products you use through the Hanhwa Techwin website.

- www.hanwha-security.com → Product → Product Page → Firmware

Through the web viewer, 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 select the latest firmware .IMG file
4) Click 'Upgrade'



The Wisenet Device Manager can automate the process of checking for new firmware, downloading firmware, unzipping files, and upgrading the devices. To speed up deployment, the Device Manager is capable of upgrading 16 devices at one time, and queuing up the remaining devices, if desired.

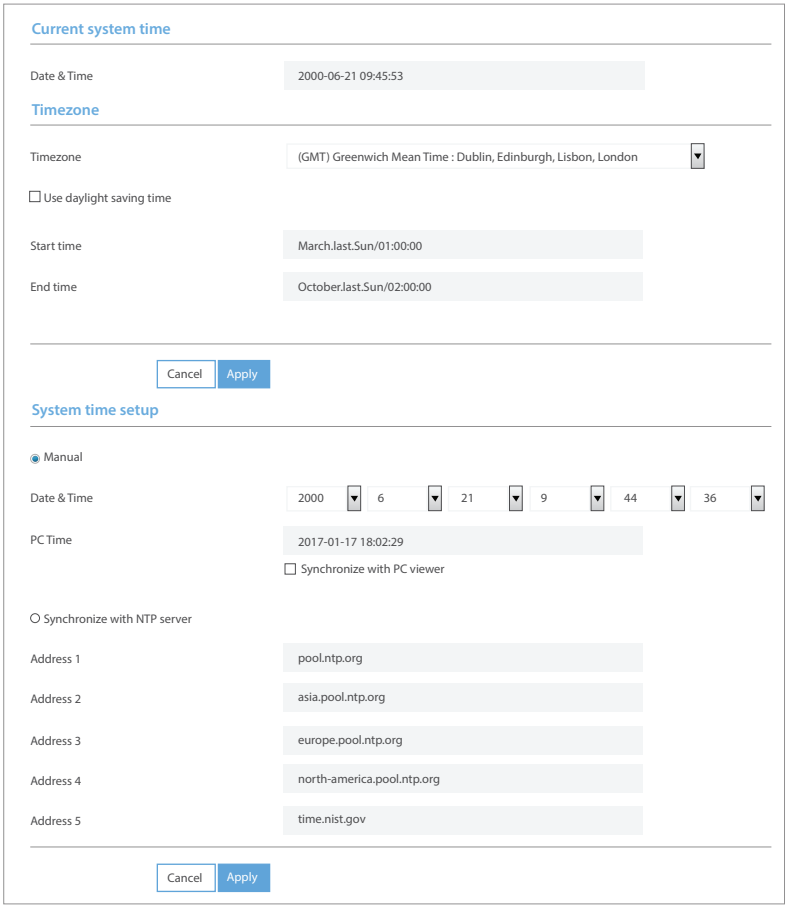
Setting the Correct Date & Time

The built-in clock keep the date and time up to date. It is important to check that the clock is correct when deploying a device. The clock is used to record logs and for recording video. If the clock is incorrect, forensic investigation in case of a network breach will be very difficult. Furthermore, the video evidence may not be admissible in court if the clock is not accurate. Finally, many other services rely on an accurate clock and may fail to work properly if the clock is not set correctly, including HTTPS, ONVIF, SNMP v3, and 802.1x.

The NTP protocol can be used to ensure that over time the clock does not drift and stays accurate. All Hanwha Techwin NVRs feature an NTP server for cameras to sync to when enabled.

To check if the current system clock is set properly, the user has three methods:

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



HTTPS (Hanwha Techwin certificate)

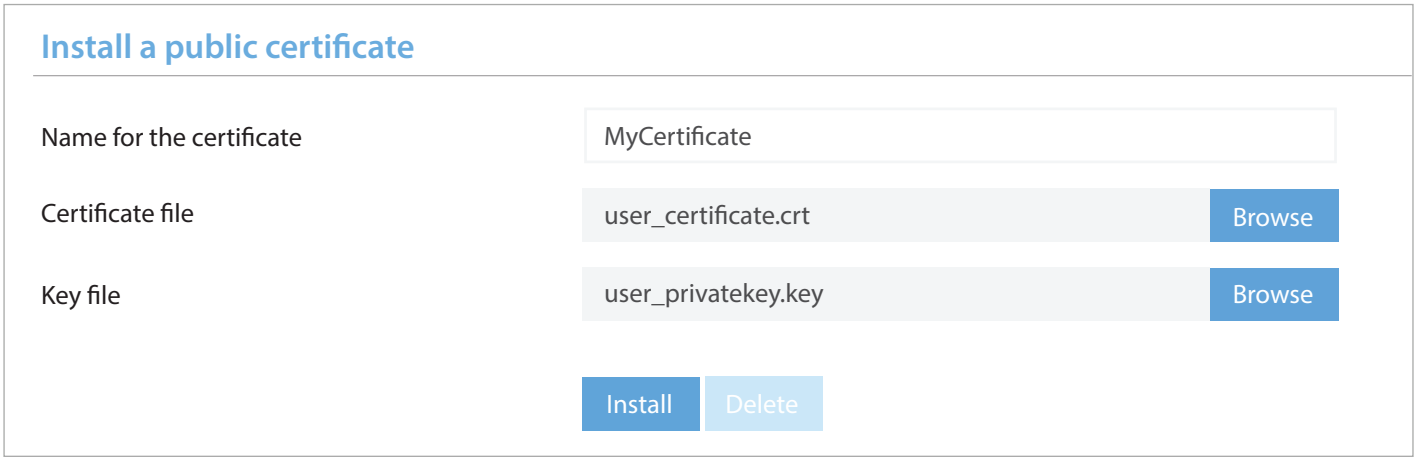
HTTPS (Hanwha Techwin certificate) is a function that enables a secure connection between the device and client using a certificate provided by Hanwha Techwin. If you select 'HTTPS (Secure connection mode using a unique certificate)', the device's built-in certificate will be used in secure connection mode and you do not need to purchase and install a separate certificate. Once enabled, communications will occur over the HTTPS port.

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

HTTPS (authenticated certificate)

HTTPS (authenticated certificate) is a function that allows ther user to register their own authorized certificate to secure the 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 the device will be used in secure connection mode.

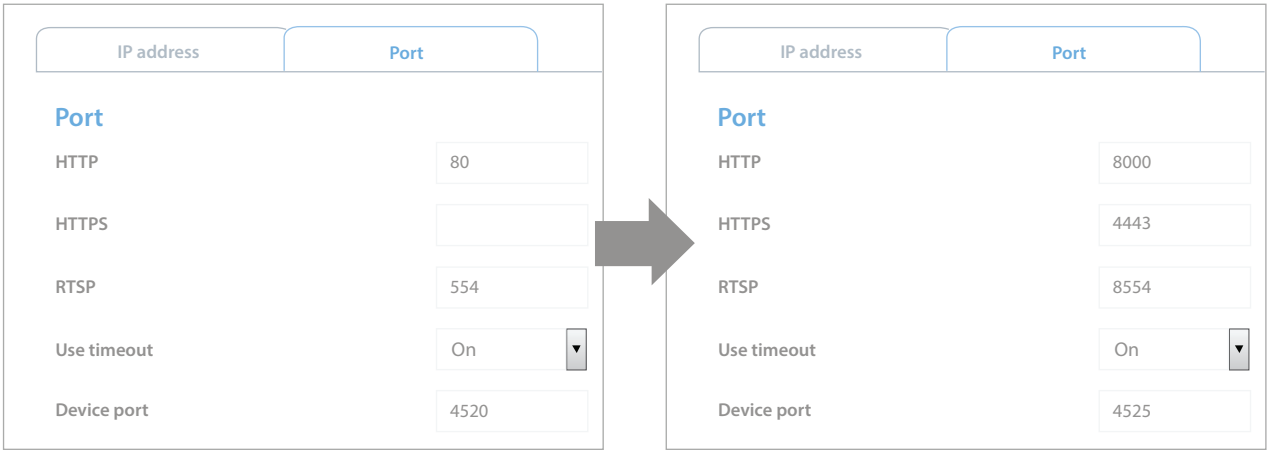
1) IP camera setup → Network → HTTPS → Install a public certificate
2) Input a name for the certificate and open the certificate file and key file.
3) Click 'Install' then choose HTTPS (Secure connection mode using the public certificate)
4) Click 'Apply'.



Changing the Default Port

In order to better avoid scans or attacks through the well-know default port of a network device, it is recommended to change the port. Commonly higher port numbers will be used, such as 8000+ or 10000+. For example, if you change the HTTP web service port to 8000 rather than 80, you can protect your web server from attacks from simple scanning programs or attempt to enter addresses directly into a web browser.

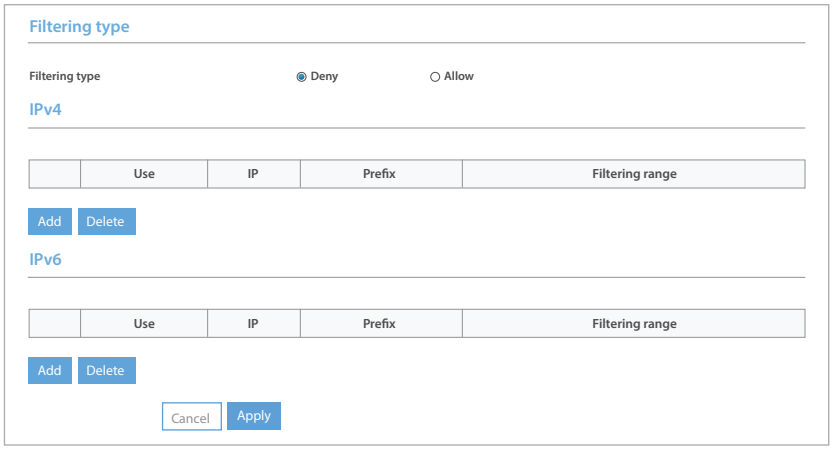
1) IP camera setup → Basic → IP & Port → Port
2) Change the HTTP and HTTPS port number to high number from 80 and 443
3) Change the RTSP port number to high number from 554.
4) Change the device port number from 4520.
5) Click 'Apply'.



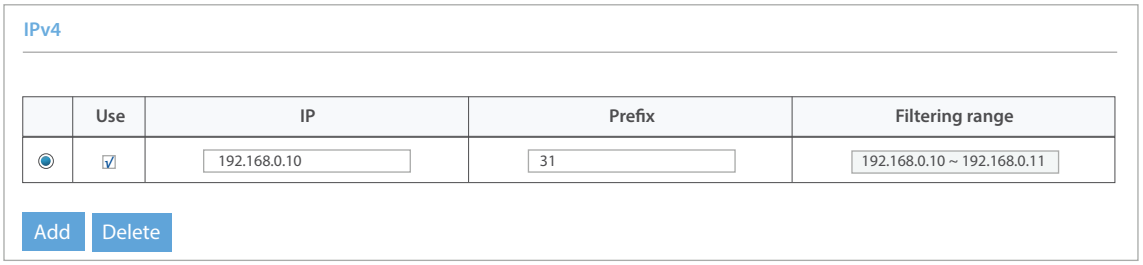
IP Filtering

Hanwha Techwin products support the creation of IP lists to allow or deny access from specific IP address. This can be used to restrict access only to the security department, or to prevent access from the WAN router or wireless pool of IP addresses, for example.

1) IP camera setup → Network → IP filtering → Filtering type



3) Click 'Add' then an IP address to allow or deny access.
When IP address and prefix is input, the filtering IP address range will be displayed.

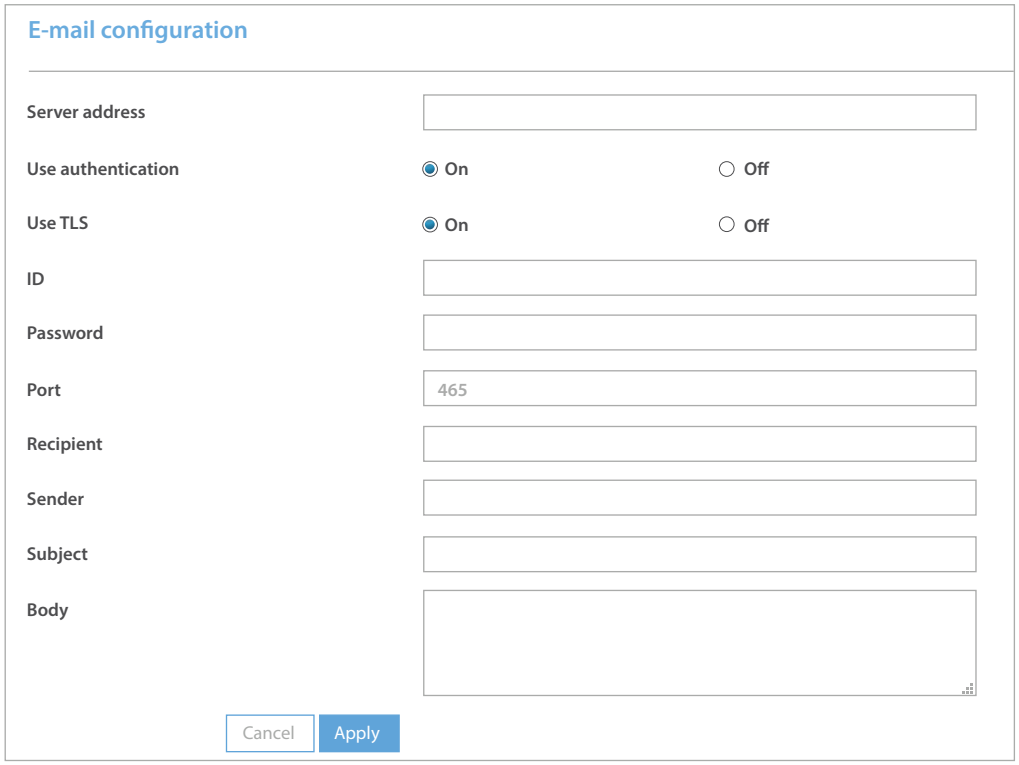


4) Click 'Apply'.
* The IP address of PC currently in use to setup cannot be added for deny filtering. PC IP address must be added to allow filtering.

Sending E-mail using TLS

Hanwha Techwin cameras support e-mail transmission of images taken when an alarm or event occurs. When using this function, the TLS mode enables secure e-mail transmission from camera to mail server to prevent user credentials from being disclosed from repetitive image transfers.

1) IP camera setup → Event → FTP/E-mail → E-mail configuration
2) Enter the E-mail server address.
3) Choose 'on' for 'Use authentication' and 'Use TLS'.
4) Enter the user account ID and password to connect to the E-mail server.
5) The default value for an E-mail server port is 25, or 465 with TLS. Some E-mail servers may use other ports.
6) Enter the E-mail recipient address in the Recipient field and the E-mail sender address in the Sender field.
7) Enter the E-mail subject and contents (Body) and click the 'Apply'. When sending an E-mail, the alarm and event images are delivered as attachments.



Disabling Unused Link-Local IPv4 Address

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

1) IP camera setup → Network → Auto IP configure → Link-Local IPv4 address
2) Uncheck 'Auto configure'.
3) Click 'Apply'.

Disabling Unused UPnP

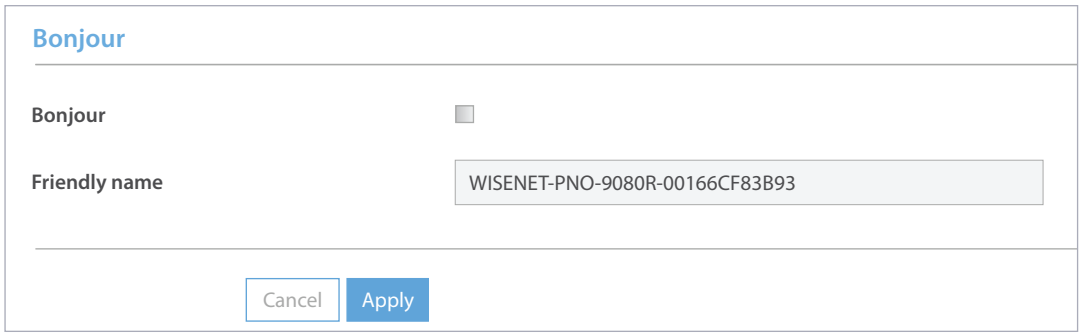
The UPnP discovery function supports automatic UPnP protocol search for clients and operating systems. While it allows easy display and access to devices from a graphical interface in the Operating System, it can allow unauthorized individuals to obtain information about the device. Note that UPnP discovery is separate from UPnP Automatic Port Forwarding. 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'.

Disabling Unused Bonjour

The Bonjour function allows the client and operating system that supports the Bonjour protocol to automatically search for cameras. While it allows easy display and access to devices from a graphical interface in the Operating System, it can allow unauthorized individuals to obtain information about the device. If you think the service is unnecessary, make sure to disable the service for added security.

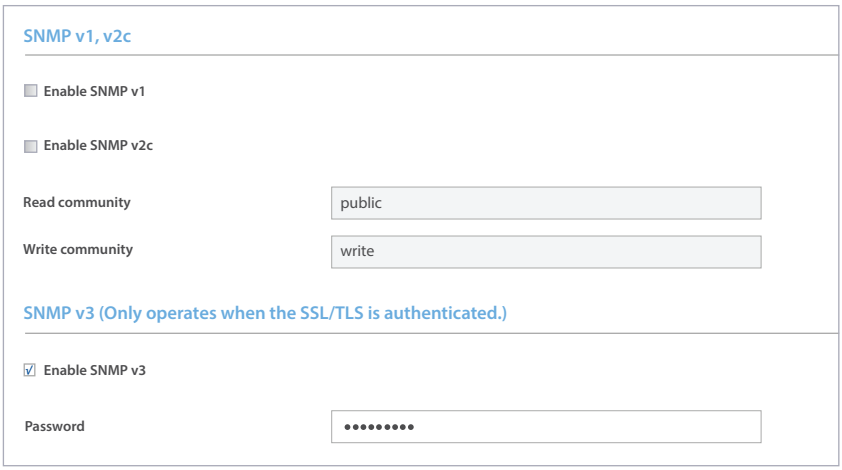
1) IP camera setup → Auto IP configure → Bonjour
2) Uncheck 'Bonjour'.
3) Click 'Apply'.



Using SNMP Securely

SNMP provides the ability to conveniently manage network devices. However, SNMP v1 and v2c are vulnerable because they use clear text strings. If you want to use this function, it is recommended to use the secure SNMP v3 only. SNMP v3 is only available when the camera is running in HTTPS mode.

1) IP camera setup → Network → HTTPS → Secure connection system
2) Choose 'HTTPS (Secure connection mode using a unique certification).'
3) Click 'Apply'.
4) Go to Network → SNMP
5) Disable SNMP v1 and SNMP v2.
6) Enable SNMP v3 and set password

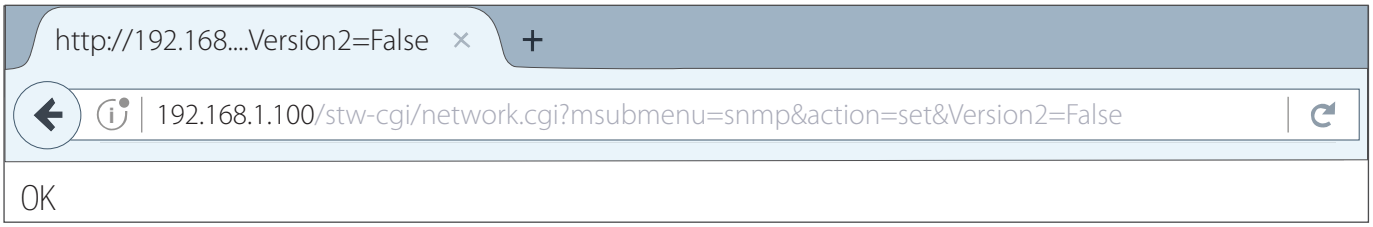


Disabling Unused SNMP

SNMP v1, v2c, and v3 versions can be supported at the same time. Many models do not allow SNMP to be fully disabled through the web viewer interface. To disable all SNMP protocols, utilize the Wisenet Device Manager or send the following commands:

- SNMP v2c Disable
  http://(IP address)/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version2=False

- SNMP v1 Disable
  http://(IP address)/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version1=False

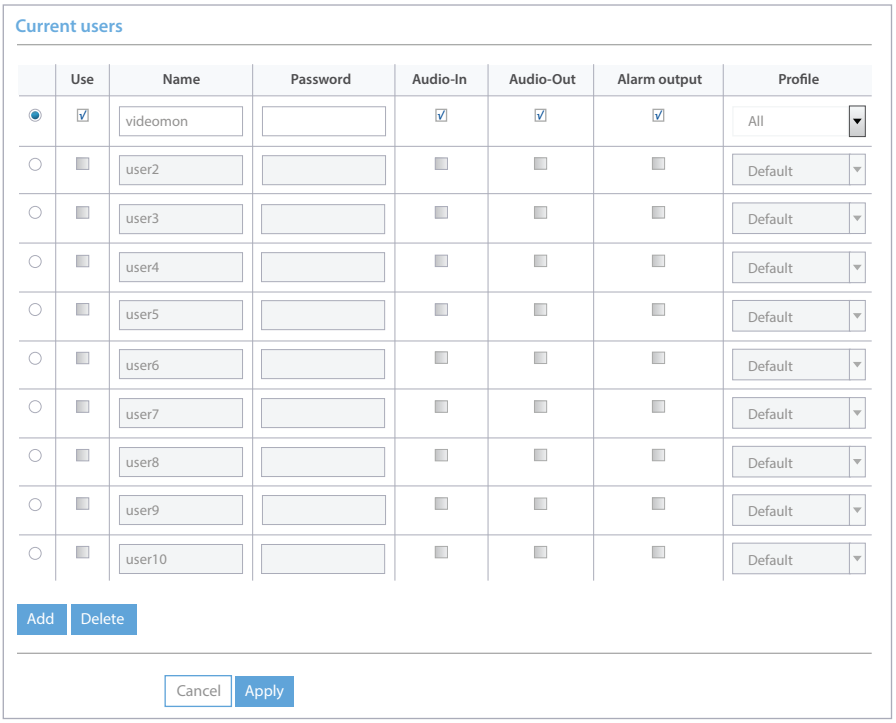


Creating Additional User Accounts

Accessing the device only with an administrator account causes the administrator password to be continuously transmitted over the network. This can lead to a security vulnerability that exposes sensitive information to a person who has malicious purposes. Furthermore, sole reliance on administrator-level access escalates the privileges of all users. Each user should only have the minimal amount of privileges required to perform their job functions to prevent accidental or malicious setting changes. Therefore, you can enhance your security by using the administrator account for configuration only, and 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 a profile then click 'Apply'.

*PTZ/ fisheye cameras will have an additional PTZ option to allow/disable access to move the camera.



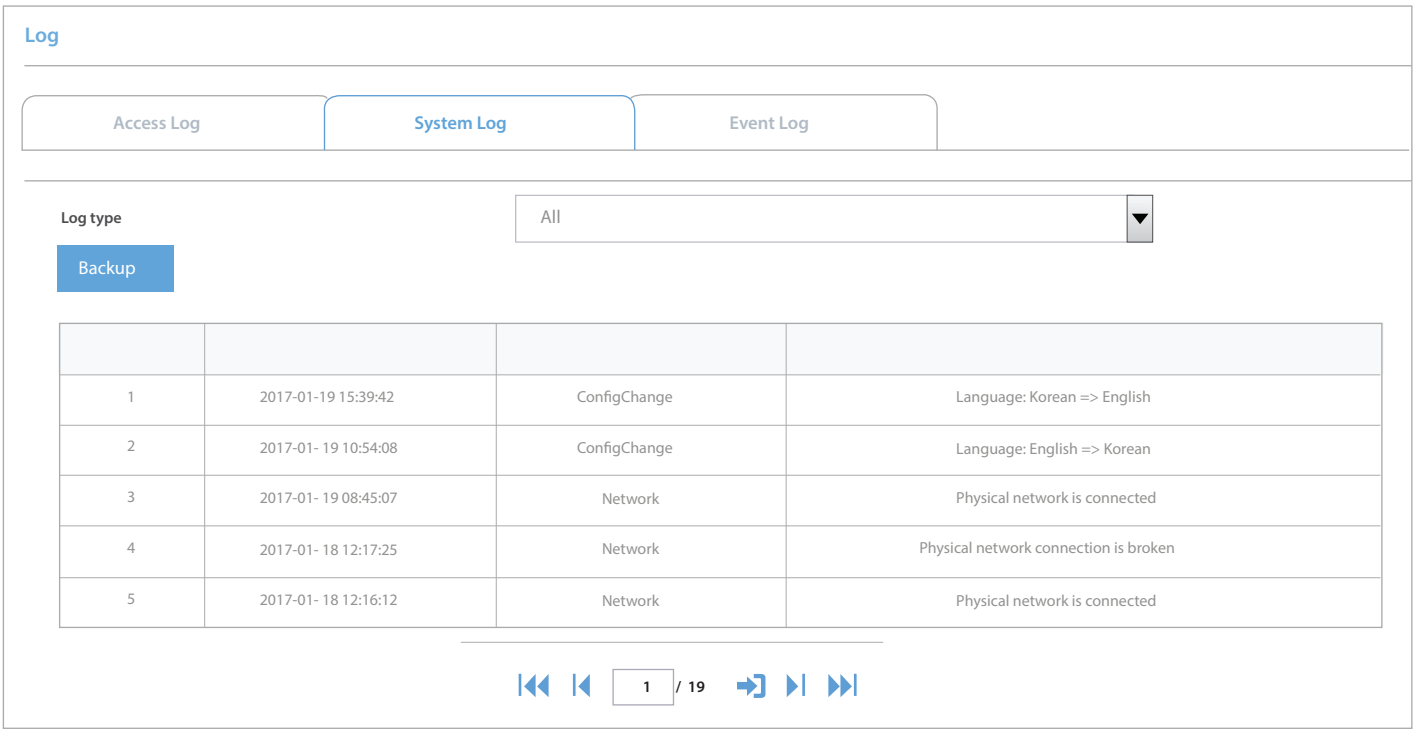
Checking the Log

Administrators can analyze the logs stored in the system to find evidence of unauthorized access and configuration changes to the device for malicious purposes. You can check various information such as device access, system setting change, and event history. The logs serve as important data to enhance the security of a network system. 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



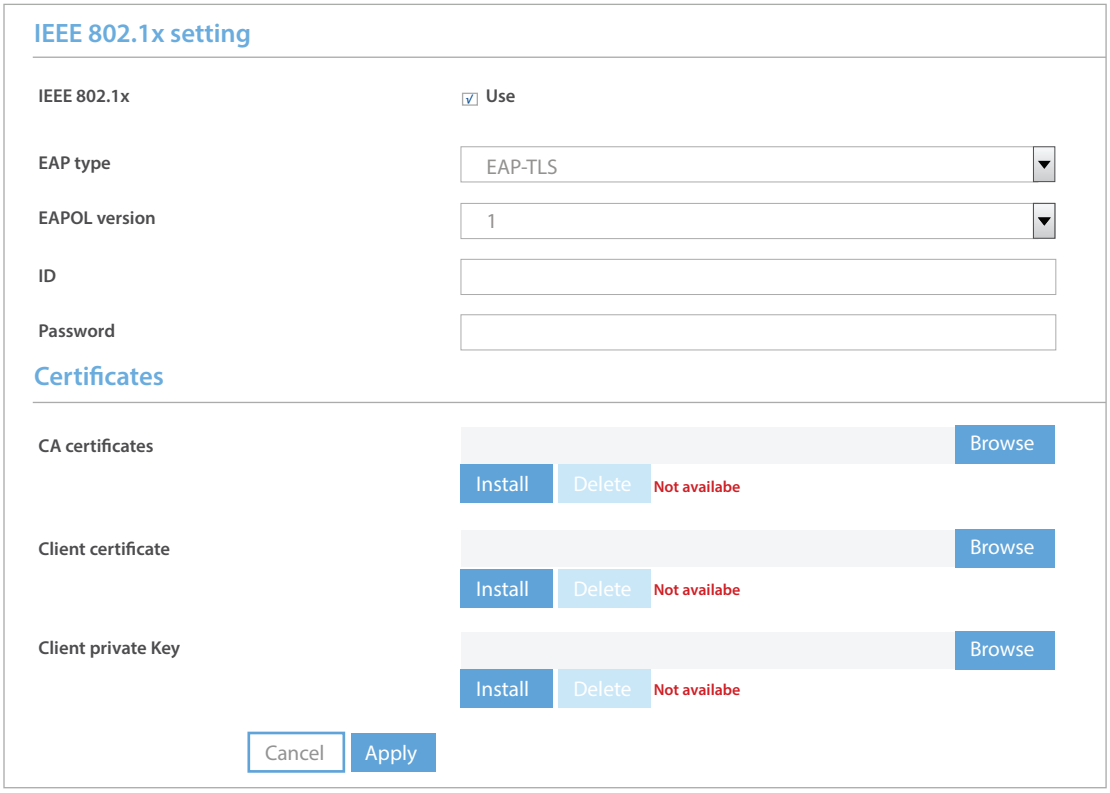
Very Secure Level

802.1 X Certificate-Based Access Control

In many buildings, network jacks may be accessible, or a camera could be unplugged or a cable tampered with to gain access to the Ethernet network infrastructure. The 802.1x standard provides port-based network access control that requires an identifying certificate to be installed on each connected device to gain access to the protected network. Thus, should an attacker plug an unauthorized device into the network, it will be denied access. Setting up port-based access control for network devices, incorporates all devices on the network including network switches, media converters, printers, and wireless access points (APs), providing a more robust network security environment.

Hanwha Techwin products 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, and 802.1s authentication server, device certificates, and private key. 802.1x configuration is typically performed on an isolated network or VLAN before being migrated to the secure network.

1) IP camera setup → Network → 802.1x → IEEE 802.1x setting
2) Check 'Use' and select EAP type.
3) Select 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'.



Summary

The harsh reality in today's connected world is that individuals and groups will continue their attempts to identify and exploit vulnerabilities to breach network security. And while we benefit from the convenience of a growing number of devices accessible via those networks, the reality is that those devices only increase the likelihood of unauthorized network access. Therefore, it is vital that all of these devices are secured to prevent them from becoming an open door for hackers. Employing these best practices not only can prevent networked video devices and systems from serving as entry points, but also ensures the integrity and continued operation of this critical function – ensuring the ongoing safety and security of people and assets. Additionally, many of these steps are also applicable to other devices and systems. Therefore, these best practices serve as a requirement for organizations that recognize the importance of and are serious about securing their networks.

Therefore, these best practices serve as a conversation starter for organizations that recognize the importance of and are serious about securing their networks. Open and informed dialogue between the end user, their IT department, the installer and systems integrator are the key to finding the best solution to fit an individual organization's security needs.
Hanwha Techwin inspects product security and diagnoses vulnerability from development stage by own security team and specialized institution. Strict policies such as user authentication, database & firmware encryption, backdoor removal and strict password ID and rule are applied to all products for the trustworthy security.

WISENET

Hanwha Techwin America
500 Frank W. Burr Blvd. Suite 43 Teaneck, NJ 07666
Toll Free: 877.213.1222
www.hanwhasecurity.com

Hanwha Techwin America