

NVR Network Hardening Guide

05.2023

V1.1

Contents

- 1. Introduction**
- 2. Definition of Security Levels**
- 3. Default Level**
- 4. Protective Level**
- 5. Secure Level**
- 6. Very Secure Level**

Revision History

Version	Revision Date	Revision Details	Note
V1.0	July. 24 th 2020	V1.0 Released	
V1.1	May. 24 th 2023	Modify the web viewer UI for each feature	

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 Vision 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 Vision 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.

< 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	-
	Input limit for consecutive password failures	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 authentication)	Default	-
Protective Level	Performing factory reset	-	-
	Disable unused multicast	Disable	-
	Disable unused DDNS	Off	-
	Disable unused SNMP	Disable	-
	Disable audio function	unused	-

2. Definition of Security Levels

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
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 (using private certificate)	HTTP	HTTPS(using private certificate)
	HTTPS (using public certificate)	HTTP	HTTPS((using public certificate)
	Changing the default port	Initial value	Change
	IP filtering	Not set	Set
	Using SNMP securely	Not set	SNMP v3
	Changing the administrator account/creating additional user accounts	-	Change/Set
	Restriction settings	-	Set
	Check the log	-	-
Very Secure Level	802.1X 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 Vision 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 when logging in to the initial access UI (Including Install Wizard)
Access control	Restriction of input when consecutive password input fails	Block password input attacks from unauthorized persons when logging in to the web UI
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

3. Default Level

3.1. Forced complex password setting

Hanwha Vision 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 Vision 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 Vision 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 Vision '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 Back up(Export) function, you can download the file containing the current device's environment setting information to your PC, and restore the backed up environment setting information through the Import function.

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 file containing the backed up configuration information contains important information of the user's device environment, Hanwha Vision stores the configuration information using a secure encryption algorithm when back up.

3. Default Level

3.6. Firmware encryption and secure update

Hanwha Vision's products provide encrypted firmware through the homepage of Hanwha Vision 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 Vision'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

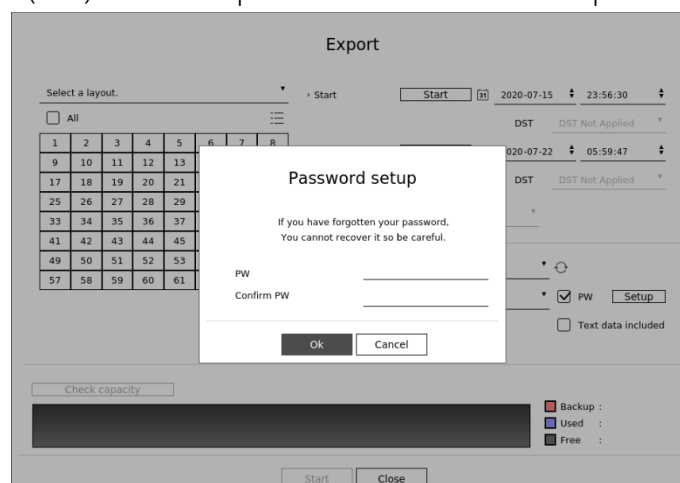
Video files extracted in SEC file format using Hanwha Vision's NVR cannot be opened with general playback/editing software. This prevents indiscriminate exposure of the video, and also enables detection of video tampering by applying watermarking. By default, the player required for playback is automatically extracted from the SEC file, so there is no need to install a separate player, and the user can simply play the video file by double-clicking the SEC file. In addition, the SEC file format can check whether the video file has been tampered with for legal evidence or privacy purposes and ensure confidentiality.

< Table 3 >

Device	Extraction location	Backup file format	Watermarking/ Encryption	Digital Signature	Player
NVR	Set	NVR	X	X	Only playable on set
		SEC	O	X	Backup viewer
	Webviewer	AVI	X	X	general video player

- Setup(NVR SET)

: Search → Select Export → Enter channel/time information → Device settings → Set storage type (SEC) → Check password checkbox → Set password



3. Default Level

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 Vision's product is developed to retain log files from being erased by device initialization (factory reset) to prevent such malicious intent.

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 Vision has strengthened security and user convenience by providing HTML5 web viewer service that can provide optimal video service without plug-in.

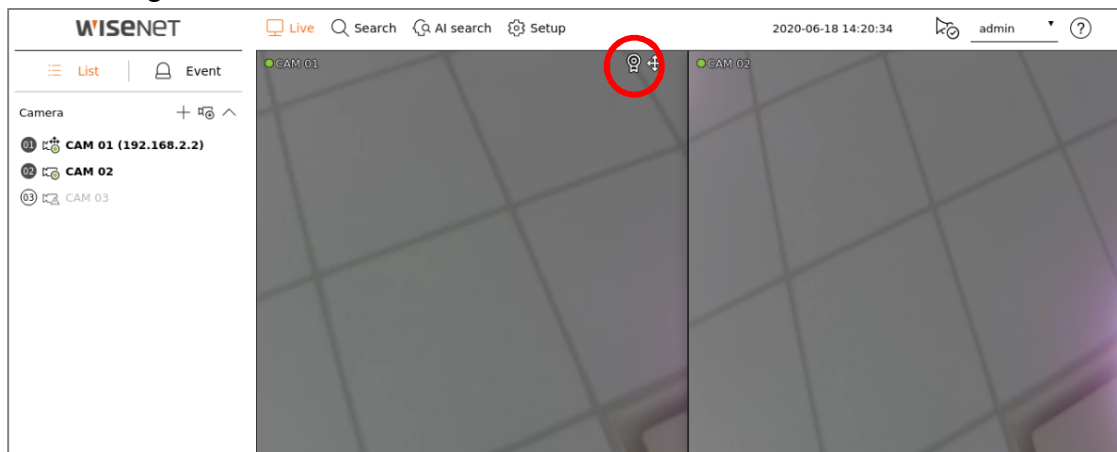
3. Default Level

3.10. Individual device authentication

(Device/mutual authentication (server authentication/client authentication))

The network devices provided by Hanwha Vision are equipped with device identification and mutual authentication functions using device certificates during encrypted communication. This allows you to verify whether the device is a trusted device manufactured by Hanwha Vision and enhances security by preventing hackers from arbitrarily overhearing or manipulating security communications through man-in-the-middle attacks. In other words, when connected to a camera manufactured by Hanwha Vision, the storage device performs encrypted communication with the camera and verifies the device as a trusted device as follows.

- device authentication(NVR) – Available in sets
: After connecting the set, check the device certificate icon on the Live screen



In addition, we have distributed/guided the "Hanwha Vision's Private Root CA certificate pre-installation guide" to apply device authentication to web viewer (web browser) connections instead of connections between our devices.

The installation guide can be found on our homepage.

- Hanwha Vision Private Root CA Certificate Pre-installation Guide

(<https://www.hanwhavision.com/ko/support/cybersecurity/>)

4. Protective Level

Hanwha Vision 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 unused multicast	Prevent malicious attacks by minimizing services that are initially activated
	Disable unused DDNS	
	Disable unused SNMP	
	Disable unused audio input	

4. Protective Level

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 Vision product can achieve the protective level of security with the initial state alone.

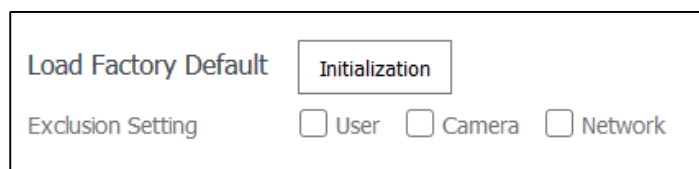
- Setup(NVR)

1) System → System Management → Settings

2) Uncheck User/Camera/Network

(If you check the corresponding function, the setting value of the item is maintained and the system setting is initialized)

3) Initialization button click



Load Factory Default Initialization

Exclusion Setting ☐ User ☐ Camera ☐ Network

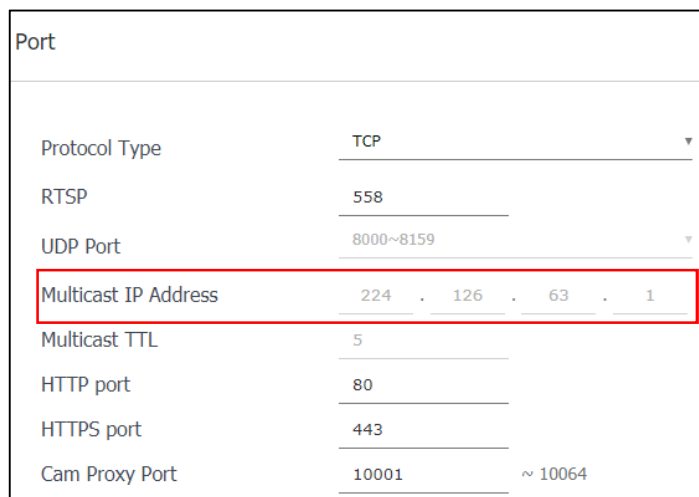
4.2 Disabling unused multicast

As a function to specify the use of multicast, you can set the RTSP protocol. The default setting for this service is disabled. If you don't need that service, we recommend keeping it disabled for added security.

- Setup(NVR)

1) Setup → Network → Port → Multicast IP Address

2) Maintained Multicast IP Address disable



Port	
Protocol Type	TCP
RTSP	558
UDP Port	8000~8159
Multicast IP Address	224 . 126 . 63 . 1
Multicast TTL	5
HTTP port	80
HTTPS port	443
Cam Proxy Port	10001 ~ 10064

4. Protective Level


4.3. Disabling unused DDNS

If your storage device is directly connected to a DHCP-enabled cable modem, xDSL modem, or PPPoE modem, the IP address will change every time you try to connect to your ISP. In this case, the user is not aware of the changed IP address, but by pre-registering the ID of the product through the DDNS function, the user can easily access the changed IP address. In addition, the Quick Connect (UPnP) function is a service that automatically discovers and connects to the device. If you think the DDNS and Quick Connect (UPnP) services are unnecessary, you can uncheck the settings for the service features for added security.

DDNS & P2P

Wisenet DDNS & P2P

☐ Enable ⓘ



Product ID

DDNS -

P2P -

☐ Quick connect(UPnP)

Public DDNS

DDNS Site

Off

▼

Host name

User name

Password

4. Protective Level

4.4. Disable unused SNMP

Hanwha Vision'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.

- Setup(NVR Webviewer)

1) Network → SNMP

2) Disable SNMP v1, v2c and v3

SNMP

☐ Enable SNMP v1

☐ Enable SNMP v2c

☐ Enable SNMP v3

☐ Enable SNMP traps

Read community

Write community

Password

IP address

Password

0000

4.5. Disable audio function

The audio use function is a function that allows you to input sound into the video. If you feel that the service is unnecessary, you should turn off the service function to enhance security. Since the audio use function can be set individually for each channel recording file, it is necessary to select and disable each recording file that has already been set.

- Setup(NVR Webviewer)

1) Setup → Record → Record Settings

2) After selecting each set recording file, select Disable Audio

3) Click OK button

Record setup

Total bitrate (limit/max) 120.0 / 120 Mbps

Apply to other channels

CH	Camera name	IP address	Continuous recording ▼	Event recording ▼	Continuous recording		Limit	Pre	Event	Post	Audio ▼
					Full frame	I-frame					
1	CAM 01	192.168.200.101	Full ▼	Full ▼	0.7 M (30.0)	0.4 M (0.5)	15 M	5 s	▼	30 sec ▼	Off ▼
2	CAM 02		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼
3	CAM 03		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼
4	CAM 04		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼
5	CAM 05		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼
6	CAM 06		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼
7	CAM 07		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼
8	CAM 08		Full ▼	Full ▼			15 M	5 s	▼	30 sec ▼	Off ▼

5. Secure Level

Hanwha Vision 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(HTTPS)	Protection of personal information and video transmitted and received on the web viewer
-	Using a secure communication protocol (RTSP)	Protection of video transmitted through RTSP
-	HTTPS (using private certificate)	Secure connection between device and client through certificate
-	HTTPS (using 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
Service protection	Using SNMP securely	Clear all SNMP initial values for enhanced security
-	Changing the administrator account/ Creating additional user accounts	Change the admin account and use it, For frequently used functions, security is enhanced by creating a user account with minimal privileges when necessary.
-	Restriction settings	Prevent information disclosure by granting access to functions
Log	Check the log	Analysis of unauthorized access records

5. Secure Level

5.1. Checking the version of firmware and updating

Through the Hanwha Vision homepage (www.hanwhavision.com), Users can check the latest firmware version of the product. The current firmware version, MAC address, UWA version, and open source notice of the product can be found in the product information as shown in the figure below. To ensure that the firmware version of your product is always up to date and to upgrade the software, download the firmware of your product from Hanwha Vision's website and click the Upgrade button to proceed with the upgrade.

- www.hanwhavision.com → Product → Detail page of product → Firmware
- Setup(NVR Web viewer)
 - 1) Setup → System → System management → Product Information
 - 2) Check the current S/W version.
 - 3) Offline upgrade → Click 'Browse' and open the latest firmware
 - 4) Click 'Upgrade'

Product information		Settings	
Model	XRN-820S		
Software version	5.30.32_230222124325		
MAC address 1	E4:30:22:64:8E:FC		
MAC address 2	E4:30:22:64:8E:FD		
UWA Version	3.40.09		
Open Source Announcement			
Offline upgrade	<input type="text"/>	Browse	Upgrade
Online upgrade	<input type="text"/>	Upgrade	Refresh
Auto FW update	<input checked="" type="radio"/> Enable update notification <input type="radio"/> Auto updates <input type="radio"/> Disable update notification Apply		
Auto update schedule	<input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly 00 : 00 v		
Device name	XRN-820S	Apply	

5. Secure Level

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.

- Setup(NVR Web viewer)

1) Setup → System → Date/Time/Language

2) Set the time zone for your location, which is based on Universal Time (GMT).

(The Use Daylight Saving Time (DST) option appears only when you select a region that uses DST in its time zone, and you select it if it applies. If selected and applied, it will be set to one hour ahead of your region's standard time)

3) Select Edit to set the time to be applied to the system

4) Set the time synchronization

5) Click the OK button for the system time settings

Date/Time/Language

System time

2023-05-22 13:39:33

Modify☐

Date

31

2023

5

22

YYYY-MM-DD

Time

13

37

31

PM

24 Hours

Standard Time Zone

GMT+09:00, Seoul, Irkutsk, Osaka, Sapporo, Tokyo

Time sync

Setup

DST

Enable☐

Start time

Mar

Last

Sunday

1H

End time

Oct

Last

Sunday

1H

Language

English

Holiday

2023

Apr. to Jun.

Apr

May

Jun

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1	30	1	2	3	4	5	6	28	29	30	31	1	2	3
2	3	4	5	6	7	8	7	8	9	10	11	12	13	4	5	6	7	8	9	10
9	10	11	12	13	14	15	14	15	16	17	18	19	20	11	12	13	14	15	16	17
16	17	18	19	20	21	22	21	22	23	24	25	26	27	18	19	20	21	22	23	24
23	24	25	26	27	28	29	28	29	30	31	1	2	3	25	26	27	28	29	30	1
30	1	2	3	4	5	6	4	5	6	7	8	9	10	2	3	4	5	6	7	8

© 2023 Hanwha Vision Co., Ltd. All rights reserved.

18

5. Secure Level

5.3. Using a secure communication protocol (HTTPS)

Hanwha Vision's NVR provides HTTP+HTTPS mode between server and client as the initial setting. Both HTTP/HTTPS apply digest authentication method, so user passwords can be protected during communication, and important information transmitted and received through HTTPS mode is protected by encrypted communication.

5.4. Using a secure communication protocol (RTSP)

In addition to HTTPS mode, video streams transmitted over RTSP must also be secured. Securing video over RTSP requires additional configuration on the client side to tunnel RTSP to HTTPS. For example, if you want to secure video streaming from an IP camera to an NVR with HTTPS, first set the IP camera to HTTPS mode on the IP camera's web viewer, then connect the camera to the NVR and set the RTSP protocol and HTTPS streaming method through the Set UI or NVR's web viewer.

- Settings (NVR Web Viewer)
 - 1) Setup → Camera → Camera setup → Select camera → Manual registration
 - 2) Protocol: RTSP
 - 3) Details → Streaming mode: HTTPS

The screenshot shows the 'Channel setup' interface of an NVR web viewer. It features a table with columns: CH, Camera name, IP address, Model, Protocol, and Video. The table lists 8 channels, each with a camera name (CAM 01 to CAM 08), an IP address (192.168.200.101 for CAM 01), a model (XNV-9082R), and a protocol (Wisenet). A 'Manual registration' dialog box is open over the table, allowing for manual configuration of a camera. The dialog includes fields for CH (1), Protocol (RTSP selected), URL (rtsp://), ID (admin), Password, and Streaming mode (HTTPS selected). The dialog also has 'Ok' and 'Cancel' buttons.

CH	Camera name	IP address	Model	Protocol	Video
1	CAM 01	192.168.200.101	XNV-9082R	Wisenet	On
2	CAM 02				
3	CAM 03				
4	CAM 04				
5	CAM 05				
6	CAM 06				
7	CAM 07				
8	CAM 08				

Manual registration

CH: 1

Protocol: ☐ Wisenet ☐ ONVIF ☒ RTSP

URL: rtsp://

ID: admin

Password:

Details: ^

Streaming mode: ☐ TCP ☐ UDP ☐ HTTP ☒ HTTPS

Ok Cancel

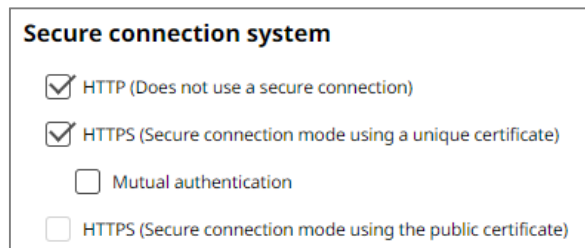
5. Secure Level

5.5. HTTPS (using private certificate)

The initial secure connection method supports both HTTP and HTTPS. HTTPS (Use own certificate) is a feature that enables secure connection between the device and the client using the own certificate provided by Hanwha Vision. When HTTPS (Use own certificate) is selected, the device's own certificate is used in the secure connection mode, and the user does not need to register a separate certificate.

- Settings (NVR Web Viewer)

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



Secure connection system


- ☒ HTTP (Does not use a secure connection)
- ☒ HTTPS (Secure connection mode using a unique certificate)
- ☐ Mutual authentication
- ☐ HTTPS (Secure connection mode using the public certificate)

5.6. HTTPS (using public certificate)

This feature allows users to register their own public certificate to enable secure connection between the device and the client without using their own certificate provided by Hanwha Vision. If you register a public certificate and private key through public certificate installation, you can select HTTPS (using a public certificate), and the registered public certificate and private key will be used in secure connection mode.

- Settings (NVR Web Viewer)

- 1) Setup → Network → HTTPS → Install a public certificate
- 2) Enter a certificate name and specify the public certificate to use for the certificate file
- 3) Specify the private key to be used in the key file and click the Install button
- 4) Select HTTPS (Use public certificate) and click Apply button



Install a public certificate

Name for the certificate

Certificate file

Key file

- ※ HTTPS (Use public certificate) can be selected only if there is a registered public certificate.
- ※ If you want to delete the registered public certificate and private key, click the Delete button. You can delete a public certificate only when you connect to HTTP (Disable secure connection) or HTTPS (Use own certificate).

5. Secure Level

5.7. Changing the default port

To prevent scanning or attacks through the default ports of network devices, it is generally safer to have users redirect ports rather than use well-known ports. Consider changing the commonly provided default port number to a higher port number. For example, changing the HTTP web service port accessible through a web browser to 8000 instead of 80 can protect web service access from simple scanning programs or attacks that involve typing the address directly into the web browser.

- Settings (NVR Web Viewer)

- 1) Setup → Network → IP & 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 558.

- 4) Click 'Apply'.

IP address	Port
Protocol type	TCP ▼
RTSP port	558
UDP Port	8000~8159 ▼
Multicast IP address	224 126 63 1
Multicast TTL	5
HTTP port	80
HTTPS port	443
Cam Proxy Port	10001 ~ 10008

IP address	Port
Protocol type	TCP ▼
RTSP port	8558
UDP Port	8000~8159 ▼
Multicast IP address	224 126 63 1
Multicast TTL	5
HTTP port	8000
HTTPS port	4443
Cam Proxy Port	10001 ~ 10008

- *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. Secure Level

5.8. IP Filtering

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

- Settings (NVR Web Viewer)

1) Setup → Network → IP filtering

2) Select a filtering type

- Deny registered IP: Block access from IPs registered with the filtering
- Allow registered IP: Allow access only to IPs registered for filtering

3) Input the IP Address

IP filtering

IPv4 IPv6

Filtering type ☒ Deny registered IP ☐ Allow registered IP Delete

No.	Enable	IP address	Prefix	Filtering range
1	On			
2	On			
3	On			
4	On			
5	On			
6	On			
7	On			
8	On			
9	On			
10	On			

4) Enter the IP addresses and prefixes you want to restrict or allow, and the Filtering range item on the right displays the range of IP addresses blocked or allowed.

Filtering type ☒ Deny registered IP ☐ Allow registered IP Delete

No.	Enable	IP address	Prefix	Filtering range
1	On	192.138.13.10	31	192.138.13.10 ~ 192.138.13.11

5) Click Apply button after completing the settings

- If you select Allow in IP Filtering and Enable IPv6, you need to register both IPv4 and IPv6 addresses of the PC you are setting up. The IP of the PC you are setting up cannot be registered as restricted, but must be registered as allowed, and only the IPs you set up can be accessed after that.

5. Secure Level

5.9. Using SNMP securely

SNMP provides a convenient way to manage network devices. By default, Hanwha Vision has all options unchecked for enhanced security. To use SNMP securely, it is recommended to set it to SNMP v3 only.

SNMP v1 and v2c are insecure because SNMP functions are provided through the default community string by default, but users can change the community string to use them. If you use SNMP v1 and v2c, we recommend that you change the community string to use it.

- Settings (NVR Web Viewer)

- 1) Setup → Network → SNMP
- 2) Uncheck use of SNMP v1 and SNMP v2c
- 3) Select SNMP v3 use and set password

SNMP		
<input type="checkbox"/> Enable SNMP v1		
<input type="checkbox"/> Enable SNMP v2c	Read community	<input type="text"/>
	Write community	<input type="text"/>
<input type="checkbox"/> Enable SNMP v3	Password	<input type="text" value="Password"/>
<input type="checkbox"/> Enable SNMP traps	IP address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

5. Secure Level

5.10. Changing the administrator account & Creating additional user accounts

Accessing and using the device with only the initial administrator account of "admin" can result in a security vulnerability where the administrator password is continuously transmitted over the network, exposing sensitive credentials to someone who is continuously monitoring the network for malicious purposes. For this reason, it is best to change the administrator account.

Additionally, administrators can grant users administrator privileges, including frequently used settings functions, which can be vulnerable and should be minimized to only those users who really need them.

- Settings (NVR Web Viewer)

- 1) Setup → System → User → Administrator → Change ID/Password
- 2) Click 'Apply'.

The screenshot shows the 'Administrator' tab in the NVR Web Viewer settings. It includes a link to the password setting guide, fields for ID (admin), Current PW, New PW, and Confirm new password. There is also a 'Show password' checkbox.

- 1) Setup → System → User → Add to Group/User
- 2) Set permissions for the user group

The first screenshot shows the 'User' tab with a list of users (user1, user2) and a 'Group information' section. The second screenshot shows the 'User information' section for 'user1', including fields for Group, Name, ID, Password, Confirm PW, and Viewer status. A 'Success' message is visible next to the password field.

5. Secure Level

5.11. Restriction settings

Set Restrictions is a service that allows you to set user access to features or network access. Feature restrictions can set which features to restrict a user's access to, and viewer usage restrictions can restrict a user's remote access.

When you set a check to a feature restriction item, permissions are limited to the checked items set on the Users tab screen. However, you can grant additional feature permissions for specific users. Unchecking a Feature Restrictions item allows access to the checkboxes set on the Users tab screen.

If you set a check to All viewers in Restrict viewer usage, all users will not be able to access the network and the web viewer, and if you set a check to Web viewer, all users will not be able to access the web viewer. The Auto logout setting can increase security by allowing users to be automatically logged out after a period of inactivity on the storage device.

AdministratorUserRestriction settings

Access restriction

☐ Select all

☐ Live channel

☒ Record

☒ Remote alarm output control

☒ Search channel

☒ Stop recording

☒ Shutdown

☒ Export

☒ PTZ control

☒ Manual trigger

Remote access restriction

☐ All viewers

☐ Web viewer

Login

Auto logout

3 minute

▼

ID manual entry

☐ Enable

AdministratorUserRestriction settings

Group : 2 / User : 0

user1

user2

Group information

Name

Permission

☒ Live channel

☐ Search channel

☐ Export

☐ Menu

☐ Record

☐ Stop recording

☐ PTZ control

☐ Remote alarm output control

☐ Shutdown

☐ Manual trigger

Setup

Setup

Setup

Setup

5. Secure Level

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.
- Settings (NVR Web Viewer)

Setup → System → Log → System log/Event log/Export log

System log

Event log

Export log

Search date

2023-05-23 ~ 2023-05-23

Channel

All channels

Log type

All

Search

No.	Description	Date & Time
3	Admin logout (Remote) : IP-192.168.200.254	2023-05-23 10:08:01
2	Admin setup start (Remote) : IP-192.168.200.254 (WEB)	2023-05-23 10:07:45
1	Admin login (Remote) : IP-192.168.200.254	2023-05-23 10:07:41

<

1

/ 1

>

Export

6. Very Secure Level

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

< Table 6 >

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. Very Secure Level

6.1. 802.1 X Certificate-based access control

Setting up port-based access control for network devices connected to network switches, bridges, wireless access points (APs), etc. enables you to configure a stronger network security environment. 802.1x supported by Hanwha Vision cameras uses the standard method EAP-TLS, which requires a certificate. If you want to use this feature, you need a network switch (or bridge, wireless AP, etc.) that supports 802.1x, an 802.1x authentication server, and a device-specific certificate and private key. You can install the certificate from the 'Certificate management' page.

- Settings (NVR Web Viewer)

1) Setup → Network → 802.1x

2) Check Network 1 (Camera) or Network 2 (All)

※ Network 1 (Camera): Set up by connecting directly to the camera/Network 2 (All): Connect to a network using a router

3) Select 1 or 2 for EAPOL version.

4) Input the ID and password of client certificate.

※ If you are using an unencrypted private key file, you do not need to enter it.

5) Select the CA certificate published by the authentication server and the installed client certificate.

※ Client certificate and private key is used for TLS communication between RADIUS server and client device.

7) Click 'Apply'.

The image shows two overlapping windows from the NVR Web Viewer. The background window is titled '802.1x' and contains two sections: 'Network 1 (Camera)' and 'Network 2 (All)'. Each section has a checkbox for 'Enable IEEE 802.1x' and a 'Setup' button. The foreground window is titled 'Network 1' and is titled 'IEEE 802.1x setting (EAPOL using EAPOL-TLS)'. It contains the following fields: 'EAPOL version' with a dropdown menu set to '1', 'ID' with a text input field, and 'Password' with a text input field. Below these are three rows for certificates and keys: 'CA certificates', 'Client certificate', and 'Client private key'. Each row has a text input field followed by 'Browse' and 'Install' buttons. At the bottom of the dialog are 'Ok' and 'Cancel' buttons.



HEAD OFFICE

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, South KOREA

TEL +82.1588.5772 www.Hanwha-Security.com