



White paper

Network Hardening Guide

(NVR)

2020. 7. 24

V1.0



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	

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 Secure by Design, which means the level of security that users can achieve with the functionality provided by the device, without any extra settings.
- The protective level means Secure by Default, which 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
Default Level	Force complex password settings	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
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
	Create user group/user	-	Set
	Permission 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

The devices provided by Hanwha Techwin are developed with Secure by Design, so you can be assured of the security from cyber threats with only the functions provided by the device itself.

< 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)
Access control	Input limit for consecutive password failures	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 authentication	Reliable device identification during encrypted communication using device certificates

3.1. Forced complex password setting

Hanwha Techwin products require min. 8 character password. Depending on the length of the password, 3 (8 to 9 characters) or 2 (10 or more) types of characters are required. This forced setting helps to prevent vulnerable password setting due to user's carelessness, thereby reducing the possibility of password stealing from unauthorized persons.

3.2. 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.

3.3. Remote service (Telnet, SSH) not used

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

3.4. 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 Techwin stores the configuration information using a secure encryption algorithm when back up.

3.5. Firmware encryption and secure update

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

3.6. Watermarking and encryption of extracted video formats

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

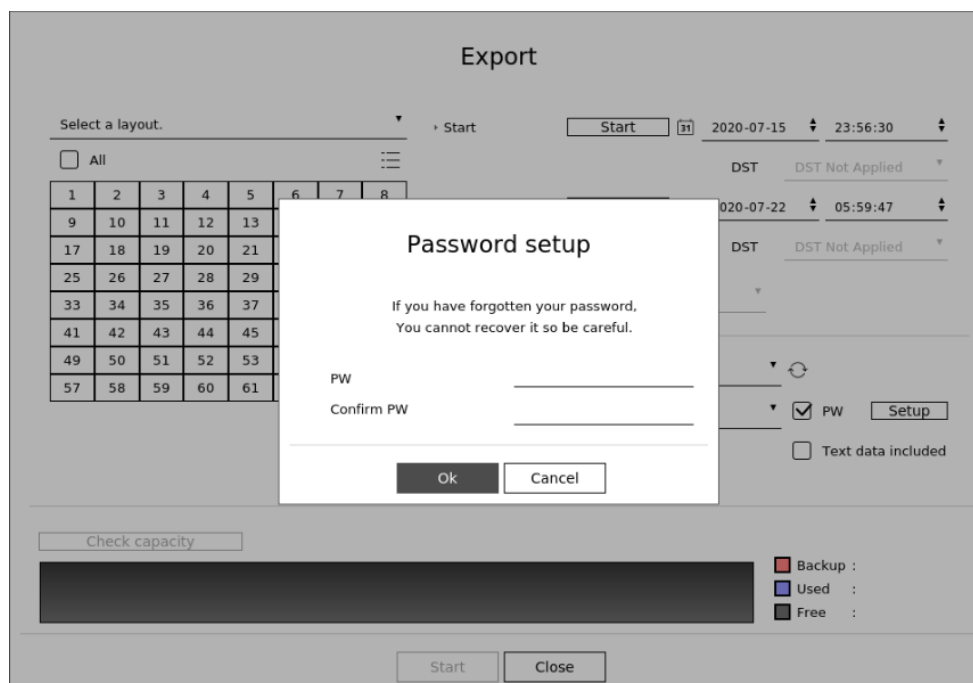
The SEC file format can ensure that video files are tampered with for legal evidence or privacy purposes, and ensure confidentiality, and can help prevent inadvertent leakage/exposure.

< 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

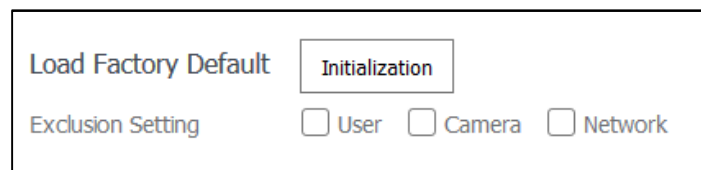


3.7. Maintained logs after factory reset

It is a very important function for network administrators and security administrators to be able to analyze the route of intrusion or understand the cause of an accident by checking the log when someone attempts or breaks into a network device. However, since hackers know the log function of these network devices, they try to forcibly delete the recorded logs when invading, so as not to leave their traces. Hanwha Techwin's devices do not allow such malicious log deletion or log initialization through device initialization. That is, even if factory initialization is executed as follows, the log stored in the storage device is never initialized.

- Setup(NVR)

: System Environment → System Management → Settings → Reset

A screenshot of a web-based settings interface for a factory reset. It features a light gray background with a white rectangular area containing the controls. On the left, the text 'Load Factory Default' is displayed in blue. To its right is a button labeled 'Initialization' in black text on a light gray background. Below 'Load Factory Default' is the text 'Exclusion Setting' in blue. To the right of 'Exclusion Setting' are three unchecked checkboxes labeled 'User', 'Camera', and 'Network' in blue.

3.8. HTML5 non plug-in web viewer

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

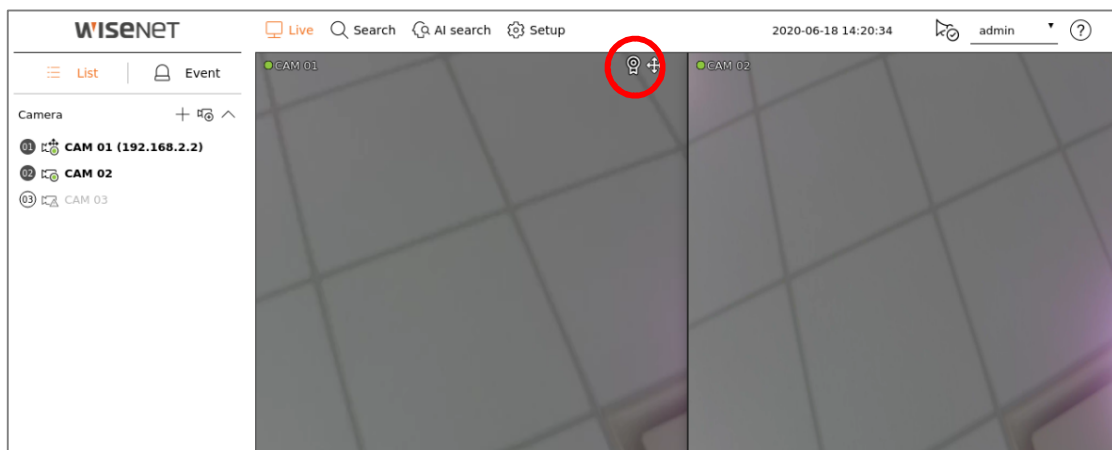
In response to this trend and security requirements, Hanwha Techwin has strengthened security and user convenience by providing HTML5 web viewer service that can provide optimal video service without plug-in.

3.9. Individual device authentication

Network devices provided by Hanwha Techwin are equipped with a device identification function using a device certificate for encrypted communication. Through this, it is possible to check whether it is a reliable device manufactured by Hanwha Techwin, and it is possible to enhance security by preventing hackers from eavesdropping on or manipulating secure communication through man-in-the-middle attacks. In other words, when connecting with a camera manufactured by Hanwha Techwin, the storage device performs encrypted communication with the camera, performs verification on the device as shown below, and proves that it is a trusted device.

- device authentication(NVR) – Available in sets

: After connecting the set, check the device certificate icon on the Live screen



In addition, "Hanwha Techwin's Private Root CA Certificate Pre-Installation Guide" is distributed/guided so that device authentication can be applied to the web viewer (web browser) connection rather than the connection between our equipment.

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

- Hanwha Techwin Private Root CA pre-installation guide

[\(https://www.hanwha-security.com/ko/technical-guides/cybersecurit/\)](https://www.hanwha-security.com/ko/technical-guides/cybersecurit/)

4. Protective Level

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

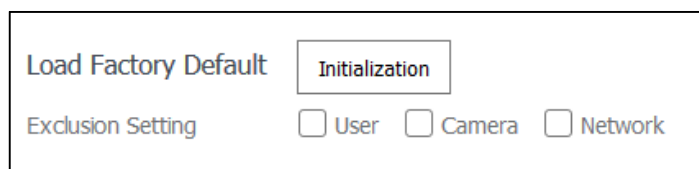
< Table 4 >

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 audio function	

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.

- Setup(NVR)
 - 1) System Environment → System Management → Settings → initialization Setting
 - 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

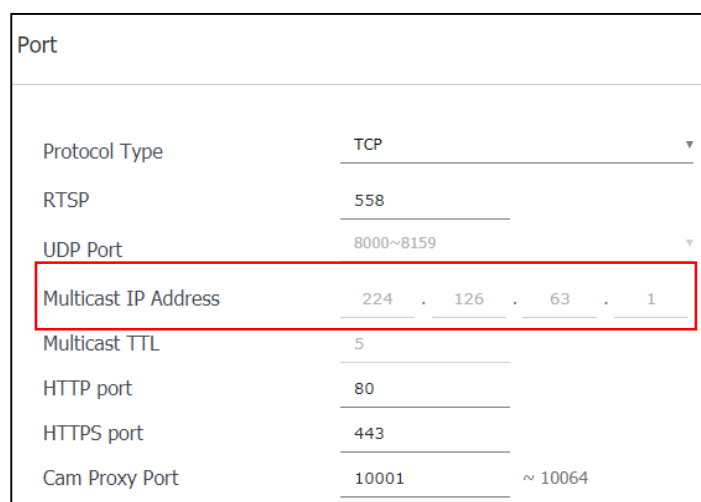


Load Factory Default	Initialization
Exclusion Setting	<input type="checkbox"/> User <input type="checkbox"/> Camera <input type="checkbox"/> Network

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

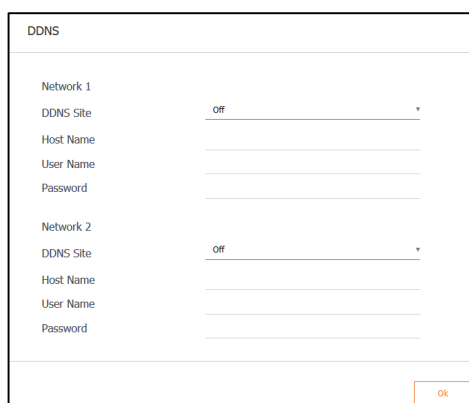


Port	
Protocol Type	TCP
RTSP	558
UDP Port	8000~8159
Multicast IP Address	224 . 126 . 63 . 1
Multicast TTL	5
HTTP port	80
HTTPS port	443
Cam Proxy Port	10001 ~ 10064

4.3. Disabling unused DDNS

If the storage device is directly connected to a DHCP-type cable modem, DSL modem or PPPoE modem, the IP address changes each time you try to connect to the ISP. In this case, the user does not know the changed IP address, but it is easy to access the changed IP address by pre-registering the product ID through the DDNS function. If you feel that the service is unnecessary, make sure to deselect the setting of the service function for security.

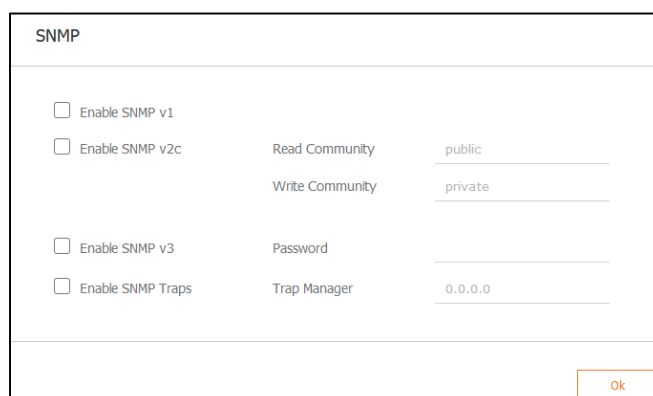
- Setup(NVR)
 - 1) Network → DDNS → Select Disabled
 - 2) Click OK button



4.4. Disable unused SNMP

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

- Setup(NVR)
 - 1) Network → SNMP
 - 2) Disable SNMP v1, v2c and v3



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)
 - 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) 147.2 / 150.0 Mbps						Apply to CH		
CH ▶	Normal recording▶	Event▶	Frame		Limit	Event		Audio▶
			FULL	I-frame		Pre▶	Post▶	
1	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
2	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
3	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
4	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
5	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
6	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
7	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
8	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
9	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
10	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
11	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
12	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
13	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
14	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
15	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
16	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
17	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
18	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off

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

< Table 5 >

Security Policy	Features for Cyber Security	Brief Description
-	Check and update the latest version firmware	Make sure you are using the latest version of the firmware and update if it is a security-poor 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
-	Create user group/user	Frequently used functions increase security by creating a user account with the least privilege.
-	Permission settings	Prevent information disclosure by granting access to functions
Log	Check the log	Analysis of unauthorized access records

5.1. Check and update the latest version firmware

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

In the figure below, if the customer is using the PRN-6410DB4 model, the latest firmware version currently deployed is 3.04.64_200515152334.

Also, you can check the MAC address, RAID version, and open source notice information. For software upgrade, download and upgrade the firmware of the product from the Hanwha Techwin website.

Please check that the firmware version of the product is always up to date.

- www.hanwha-security.com → Product introduction → Product detail page → Firmware download
- Setup(NVR)
 - 1) Setups → System Environment → System Management → System Information → S/W Upgrade
 - 2) Check the current S/W version of the product
 - 3) Click the search button to select the latest firmware downloaded
 - 4) Click the Upgrade button

The screenshot displays the 'System information' section of a web interface. It contains a table with the following data:

Model Name	PRN-6410DB4
Software Version	3.04.64_200515152334
MAC Address 1	00:09:18:E1:A1:92
MAC Address 2	00:09:18:E1:A1:93
MAC Address 3	00:09:18:E1:A1:91
RAID Version	2.0.5.7063

Below the table is a button labeled 'Open Source Announcement'.

The 'S/W Upgrade' section includes a text input field, a 'Browse' button, and an 'Upgrade' button.

The 'Server Upgrade' section includes a text input field, an 'Upgrade' button with a circular arrow icon, and a checkbox labeled 'Enable online upgrade' which is checked. An 'Apply' button is located to the right of the checkbox.

The 'Device Name' section shows a text input field containing 'PRN-6410DB4'.

The 'Power Control' section has two buttons: 'Shutdown' and 'Restart'.

An 'Ok' button is located at the bottom right of the interface.

5.2. Setting the correct date & time

The date & time function is a prerequisite for checking the exact time information of the log when analyzing information such as the system log output from the device. Therefore, setting the current system time correctly is a very important security activity. If the current system time is not set properly, the user can set the time to be applied to the system.

- Setup(NVR)
 - 1) Setup → System Environment → Move Date/Time/Language
 - 2) Set the time zone of the area where you live, which is the standard time (GMT)
(The option to use daylight saving time (DST) is displayed only when you select a region that uses daylight saving time in the time zone and selects if the function is applied. If selected and applied, it is set to one hour ahead of the local time.)
 - 3) Select Modify to set the time to be applied to the system
 - 4) Time synchronization setting
 - 5) Click the OK button of the system time setting

Date/Time/Language

System Time

2020-06-04 15:15:46

Modify

☐

Date

2020

6

4

YYYY-MM-DD

Time

15

15

42

PM

24 Hour

Time zone

GMT

Time Sync.

Setup

DST

Enable

☐

Start

Mar

Last

Sunday

1H

End

Oct

Last

Sunday

1H

Language

한국어

Holiday

2020

Apr~Jun

Apr

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

May

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

Jun

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

Ok

5.3. Using a secure communication protocol (HTTP)

Hanwha Techwin's NVR provides HTTP+HTTPS mode between the server and client as the initial setting. Digest authentication method is applied to both HTTP/HTTPS, so user password can be protected during communication. Video data and user passwords transmitted and received via HTTPS mode can be protected through encrypted communication.

5.4. Using a secure communication protocol (RTSP)

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

- Setup (NVR Web Viewer)

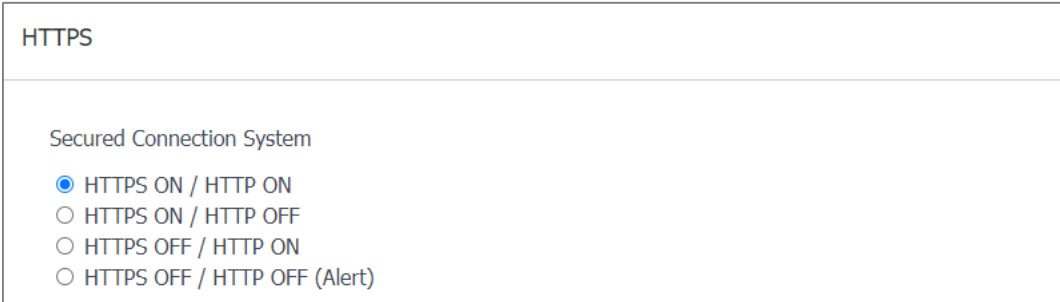
: Device → Camera → Camera Registration → Channel Selection → Camera Modification

Edit Camera	
CH	1
Protocol	<input type="radio"/> Wisenet <input type="radio"/> ONVIF <input checked="" type="radio"/> RTSP
Access Address	rtsp://192.168.1.123:443/stream1
ID	admin
Password	
More Detail	
Mode	<input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
<div>Ok Cancel</div>	

5.5. HTTPS (Private certificate)

The initial secure access method supports HTTP and HTTPS simultaneously. HTTPS (using self-signed certificate) is a function that enables secure connection between the device and the client using its private certificate provided by Hanwha Techwin. If you select HTTPS (secure connection mode using private certificate), the device's private certificate will be used in secure connection mode, and you do not need to register a separate certificate.

- Setup(NVR)
 - 1) Network → HTTPS → Secure connection method
 - 2) Select HTTPS (secure connection mode using private certificate)
 - 3) Click the Apply button



The screenshot shows a web interface for configuring HTTPS. At the top, the title 'HTTPS' is displayed. Below it, the section 'Secured Connection System' contains four radio button options: 'HTTPS ON / HTTP ON' (which is selected), 'HTTPS ON / HTTP OFF', 'HTTPS OFF / HTTP ON', and 'HTTPS OFF / HTTP OFF (Alert)'.

5.6. HTTPS (Public certificate)

This is a function that enables users to securely connect their devices and clients by directly registering their public certificate without using the certificate provided by Hanwha Techwin. Registering a public certificate and private key through the installation of a public certificate makes it possible to select HTTPS (secure access mode using public certificate) and the registered public certificate and private key will be used in the secure access mode.

- Setup(NVR)
 - 1) Network → HTTPS → Install public certificate
 - 2) After entering the certificate name, specify the public certificate to be used in the certificate file.
 - 3) Specify the private key to be used for the key file and click the install button
 - 4) Select HTTPS (secure connection mode using a public certificate) and click the Apply button

Install Public Certificate

Certificate File

Browse

Install

Delete

Key File

Browse

Install

Delete

- ※ HTTPS (secure connection mode using a public certificate) can be selected only if there is a public certificate registered.
- ※ If you want to delete the registered public certificate and private key, click the Delete button. Deletion of a public certificate is possible only when connecting via HTTP (not using secure access) or HTTPS (secure access mode using private certificate).

5.7. Changing the default port

The network device's default port, or well-known port, can easily be exposed to scans or malicious attacks. Therefore, it is safe for users to re-use the port.

Change the default port number that is usually provided to a higher port number. For example, if you change the HTTP web service port accessible through a web browser to 8000 instead of 80, you can protect access to the web service from a simple scan program or an attack that directly enters an address into the web browser.

- Setup(NVR)

- 1) Setting → Network → Interface → Port
- 2) Change the HTTP port and HTTPS port settings from 80 and 443 to higher ports, respectively.
- 3) Change the RTSP port setting from 558 to a higher port
- 4) Click OK button

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

→

Port

Protocol Type	TCP
RTSP	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 ~ 10064

※ When the port is reassigned, connection problems may occur with the connected camera or VMS, so it is also necessary to change the settings of the connected equipment. If the problem is not resolved, please restore to the default port.

5.8. IP Filtering

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

- Setup(NVR)

1) Setup → Network → IP Filtering

2) Select a filtering type

(Deny: Block access of IP registered in filtering / Allow: Allow access only to IPs registered for filtering)

IP filtering

Filtering Type ☒ Deny ☐ Allow

IP4 ▼ Delete

	Use▶	IP Address	Prefix	Filtering Range
<input type="checkbox"/>	On	<input type="text"/>		
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			
<input type="checkbox"/>	On			

3) Enter the IP to be allowed or denied.

After entering the IP address and Prefix, the filtering range item on the right shows the range of blocked or allowed IP addresses.

IP4 ▼ Delete

	Use▶	IP Address	Prefix	Filtering Range
<input checked="" type="checkbox"/>	On	192.168.0.10	31	192.168.0.10 ~ 192.168.0.11

4) Click the OK button after completing the settings

※ If you select Permit in IP Filtering and set IPv6 to Enabled, You must register both the IPv4 and IPv6 addresses of the PC you are setting up. The IP of the PC currently being set cannot be registered due to rejection, but must be registered with permission. After that, only the set IPs can be accessed.

5.9. Using SNMP securely

SNMP provides the ability to conveniently manage network devices. By default, Hanwha Techwin is deselected to enhance security. In order to use SNMP safely, it is recommended to set it only with SNMP v3.

SNMP v1 and v2c are vulnerable to security because SNMP function is provided through Default community string by default, so it is recommended to change and use community string.

- Setup(NVR)
 - 1) Setup → Network → SNMP
 - 2) Uncheck Enable SNMP v1 and SNMP v2c
 - 3) Select SNMP v3 and set password

SNMP		
<input type="checkbox"/> Enable SNMP v1		
<input type="checkbox"/> Enable SNMP v2c	Read Community	<u>public</u>
	Write Community	<u>private</u>
<input type="checkbox"/> Enable SNMP v3	Password	<u></u>
<input type="checkbox"/> Enable SNMP Traps	Trap Manager	<u>0.0.0.0</u>

5.10. Create user group/user

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.

- Setup(NVR)
- 1) Setup → System Environment → User → User
 - 2) Add user account after adding user group
 - 3) Setting permissions for user groups

The image displays two screenshots of the WISENET user management interface. The top screenshot shows the 'Group Information' page for 'Group : 1 / User : 1'. It features a large empty box on the left for group details and a list of permissions on the right, each with a checkbox and a 'Setup' button. The permissions listed are: Live View, Search, Backup, Menu, Record, Record stop, PTZ, Remote alarm out, and Shutdown. The bottom screenshot shows the 'User Information' page for the same group. It includes fields for Name, ID, Password, and Confirm PW. There is a 'View password' checkbox and two radio buttons: 'Not Use' (selected) and 'Use'.

5.11. Permission Setup

When using the device, you can set access rights for functions/networks and logins. The function and network access restrictions can be set whether all users are allowed to use without authentication, or only authorized users after password authentication. However, if access rights for each function are set only for a specific channel in the Live, Search, and Backup functions, the function for which the permission is set can be used only for that channel.

If the user has no input for the set time, the log-in access is automatically logged out. In addition, you can set whether to manually enter the ID when logging in, or to select the ID list without entering the ID.

- Setup(NVR)

1) Setup → System Environment → User → Permission Setup

2) Restricted Access/Restriction on Network Access/Auto Logout/Manual Input of ID Settings

Permission Setup

Restricted Access

☒ All

☒ Live View
☒ Remote alarm out

☒ PTZ
☒ Search

☒ Record
☒ Backup

☒ Record stop
☒ Shutdown

Restriction on Network Access

☐ All Network

☐ Web Viewer

Auto Logout

3 min

Manual Input of ID

☐ On

☒ Off

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.
- Setup(NVR)
 - : System Environment → Log Information → System log/Event log/Backup log

System log			
<div> <div>All CHs ▾ View all ▾</div> <div> <div>Today</div> <div>Q</div> <div>2020 ▾ 6 ▾ 16 ▾</div> </div> </div>			
No. ▾	CH	Log List	Date/Time
24	-	Setup Start (Admin) : IP-192.168.2.70 (WEB)	2020-06-16 10:31:23
23	-	Setup Start (Admin) : IP-192.168.2.70 (WEB)	2020-06-16 10:26:35
22	-	Setup Start (Admin) : IP-192.168.2.70 (WEB)	2020-06-16 10:18:19
21	-	Setup Start (Admin) : IP-192.168.2.70 (WEB)	2020-06-16 10:01:59
20	-	Setup Start (Admin) : IP-192.168.2.70 (WEB)	2020-06-16 09:57:04
19	-	Logout (Admin) : Local	2020-06-16 08:38:14
18	-	Network2 connected	2020-06-16 08:34:53
17	-	Network3 Disconnected	2020-06-16 08:34:51
16	-	Login (Admin) : Local	2020-06-16 08:33:26
15	-	DSP(Display) Start	2020-06-16 08:33:10
<div> <div>< 1 / 3 ></div> <div>Export</div> </div>			

5. Secure Level

Event log

All CHsView all

Today

2020616

No.	CH	Log List	Date/Time
<div><0/0></div> <div>Export</div>			

Backup log

~|

No.	User	Date/Time
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div>< / ></div>		

6. Very Secure Level

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

< Table 7 >

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

6.1. 802.1 X Certificate-based access control

Hanwha Techwin products can configure a more robust network security environment by setting port-based access control for network devices connected to network switches, bridges, and wireless access points (APs).

802.1x supported for Camera, Viewer, and iSCSI of Hanwha Techwin NVR uses standard EAP-TLS that requires a certificate.

Network switch (or bridge, wireless AP, etc.) supporting 802.1x, 802.1x authentication server, device-specific certificate and private key are required, and device-specific certificate and private key are installed through the setting page as follows.

- Setup(NVR)

1) Setup → Network → 802.1x

2) Select to Camera or Viewer or iSCSI

3) Set EAPOL version to 1 or 2

4) Enter the client's certificate ID and private key password

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

5) Install the CA public certificate of the authentication server through the public certificate

6) When using port-based access control, install client certificate and private key

※ The installed certificate and private key are used only for TLS communication between the RADIUS server and the client device.

7) Click OK button

The image shows two parts of the NVR's configuration interface. On the left is a summary table for 802.1x settings, and on the right is a detailed configuration window for 'Network 1'.

802.1x		
Network 1 (Camera)	: <input type="checkbox"/> Enable IEEE 802.1x	<input type="button" value="Setup"/>
Network 2 (Viewer)	: <input type="checkbox"/> Enable IEEE 802.1x	<input type="button" value="Setup"/>
Network 3 (iSCSI)	: <input type="checkbox"/> Enable IEEE 802.1x	<input type="button" value="Setup"/>

Network 1

IEEE 802.1x setting (EAPOL using EAP-TLS)

EAPOL Version: 1

ID:

Password:

CA Certificate:

Client Certificate:

Client Private Key:

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>

Copyright © 2020 Hanwha Techwin. All rights reserved