



White Paper

# Wisenet7

## Next level Cybersecurity

24<sup>th</sup> 03, 2021

## 1. Background and Introduction

## 2. Technology and Feature

### 2.1. Hardware Security

2.1.1. Secure Boot

2.1.2. Secure Storage

2.1.3. Secure OS

2.1.4. Secure JTAG

### 2.2. End-to-End Protection

2.2.1. Device Certificate (Pre-installed)

2.2.2. Mutual Authentication

2.2.3. Verify Chain of Trust

2.2.4. Verify Firmware Forgery

2.2.5. Encrypt Video Image (when at rest and backup)

### 2.3. Secure by Default/Design

2.3.1. Raise the level of security settings

2.3.2. Apply the latest version of TLS protocol

## 3. Security in depth

## 4. Conclusion


Concerns about the ability of hackers to access live images or retrieve recorded images captured by video surveillance cameras located in security sensitive areas have been around for a while. Many manufacturers of professional level cameras have responded to the threat by introducing device network set-up protocols which do not allow for a default password, or one that has consecutive letters or numbers, to be used. However, hackers are likely to continue to look at other ways to gain access to data, including via a camera's 'back door'.

Regardless of whether it is for criminal or malicious purposes, or just seen as a challenge by amateur hackers, it is essential that end-users' confidential data is kept secure. This applies just as much to the many thousands of small businesses that entrust video surveillance solutions to protect their assets, people and property, as it is for high security and mission critical end-users, such as airports, banks, local authorities, government, military and emergency services.

Amid this environment, Hanwha Techwin has been working continuously to strengthen the security level of its products. And in 2020, robust security functions and technologies are implemented to the products equipped with Wisenet7, Hanwha Techwin's own developed SoC (System on Chip).

First, the introduction Hardware security technology has overcome the limitations of security enabled by Software security technology. Secure Storage provides a space for secure data, and based on this, it enables the expansion of Hardware security functions such as Secure Boot, Secure OS, and Secure JTAG.

Second, the ultimate goal of end-to-end protection is to prevent unauthorized users from intercepting or falsifying sensitive information by intervening in the middle of communication, or accessing the device to falsify or tamper with sensitive information. To do this, identification and authentication between devices are required, and access control and authorization based on authentication and protection of system and data through encryption logic are also required.



Third, it is very important that product design specifications and configuration options must consider the security as a top priority. Sometimes implementing the high-level of security functions can degrade performance and backward compatibility of the products, but given the importance of security and the trends in the ecosystem of the industry or society, it is inevitable.

Some of these features and technologies are new and have been developed specifically to combat cyber-attacks whilst others, which were originally intended simply to make chipsets more efficient, are also able to contribute to camera security.

This document is designed to help users better understand Hanwha Techwin's next level cybersecurity technologies implemented to products equipped with Wisenet7.

### 2.1. Hardware Security

Employing hardware security technology is very important in improving the security level of a product, as hardware security technology can better protect vulnerabilities than software-based approaches. Cybercriminals find it hard to alter trusted software ("root of trust") that stems from a secured hardware. Starting with Wisenet7 products, Hanwha Techwin applies four major hardware security technologies as follows:

#### 2.1.1. Secure Boot

Starting with Wisenet7, Hanwha Techwin has implemented Secure Boot.

Secure boot is a mechanism that verifies the integrity of the software running on the camera during boot up, ensuring that the software is not forged from external malicious code or malware.

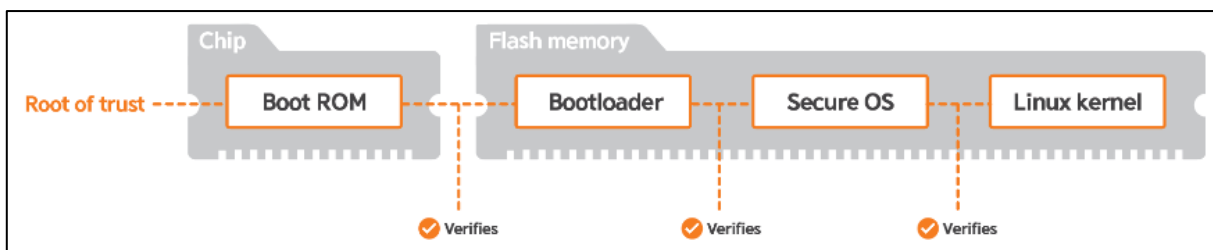


Image 1. Secure Boot in Wisenet7 Products

#### 2.1.2. Secure Storage

Wisenet7 also supports an independently secure hardware module called HTPM (Hanwha Trusted Platform Module). HTPM consists of crypto-processor (a dedicated microcontroller designed to secure operation), random number generator, Secure Storage, Secure OS, etc.

Secure Storage area of HTPM consists of OTPROM (One Time Programmable Read-Only Memory) and EEPROM (Electrically Erasable Programmable Read-Only Memory) and stores important information in the camera. Important information constituting the root of trust is programmed into the OTPROM during the manufacturing process, and important operational information is securely stored in the EEPROM.

### 2.1.3. Secure OS

A separate Secure OS must be used to securely process important information stored in the Secure Storage.

There is no way to access the Secure OS from outside the camera. To access the Secure OS or Secure Storage, you must use a separate API through the Linux OS. The Secure OS provides independent encryption and decryption functions, reducing the task load on the main OS as well as providing another layer of protection and separation. Applications used in the Secure OS are verified to prevent forgery and alteration.

### 2.1.4. Secure JTAG

Most electronics and IoT (Internet of Things) devices have a physical debug and test connector, known as JTAG, designed for use during manufacturing, QA, and service. The best way to prevent unauthorized access through these interfaces is to disable them. However, this would also block tracking the cause of failures that may occur on the chip or board during the product development or production phases.

To prevent above issue, a secret key-based authentication mechanism has been implemented in Wisenet7 that enables the use of JTAG securely while achieving a high level of security. Only the manufacturer has the corresponding authentication key which allows an access to only system related information not the customers' personal information. And in case of product failure, the cause can only be analyzed by local access using the authentication key owned by manufacturer, not remote, so there is no need to worry about access from unauthorized users.

## 2.2. End-to-End Protection

In addition to access control based on traditional passwords, it is possible to upgrade the level of secure communication using a device certificate inserted for device authentication between devices. This prevents unauthorized users from eavesdropping or tampering during communications. Also, by introducing digital signature and encryption functions, End-to-End data security can be enhanced during data storage and backup, as well as in firmware update and boot up.

### 2.2.1. Device Certificate (Pre-installed)

Hanwha uses Thales HSM equipment to generate certificates / private keys for each Wisenet7 device and programs each device during the manufacturing process. When you create a certificate, it is digitally signed by our private Root CA, so you can prove it was issued by Hanwha. With this certificate, you can perform secure communications without a security alarm in your web browser. Using your web browser, one can easily view the certificate to verify its' origin and authenticity.

### 2.2.2. Mutual Authentication

Performing mutual authentication for secure communications is a good way to enhance the confidentiality, integrity, and authenticity of communications security. Hanwha Techwin Wisenet7 products support Client Authentication for Mutual Authentication between our cameras and client devices in HTTPS (HTTP over TLS, RTSP over HTTPS) communication.

In general, Mutual Authentication can be performed either by a user or by a device. Hanwha Techwin has implemented Mutual Authentication performed between devices manufactured by Hanwha Techwin.

Authentication of the camera acting as a server in Mutual Authentication is called Server Authentication, and authentication of client devices (NVR, VMS, client workstation) is called

Client Authentication. Server Authentication is performed on the client, and Client Authentication is performed on the server. Client Authentication is provided as an option on the premise of Server Authentication, thus providing Mutual Authentication by authenticating clients in a comprehensive sense.

### 2.2.3. Verify Chain of Trust

The Root CA certificate exists to guarantee the Root of Trust in the camera, and the chain of certificate is verified using the Root CA certificate. There are two types of Root CA certificate in Wisenet7 products. One is the Root CA certificate for Device Certificate, and the other is the Root CA certificate for Open Platform Applications.

The Root CA certificate for Device Certificate is used when installing the device certificate on the camera or performing client authentication using a client (PC, NVR) device certificate. The former serves to prevent the installation of any certificate without the manufacturer's permission by verifying the certificate chain when the device certificate is installed on the camera. The latter serves as a reminder that it is a trusted device manufactured by Hanwha by verifying the certificate chain of client devices.

The Root CA Certificate for Open Platform Applications prevents unauthorized applications from being installed by verifying the certificate chain that each different signing key and certificate used to sign Wisenet7 Open Platform Application is generated and distributed by Hanwha. This ensures that only secure, authorized, and non-tampered software is running on the camera. This ensures that malicious software does not have access to the camera or network.



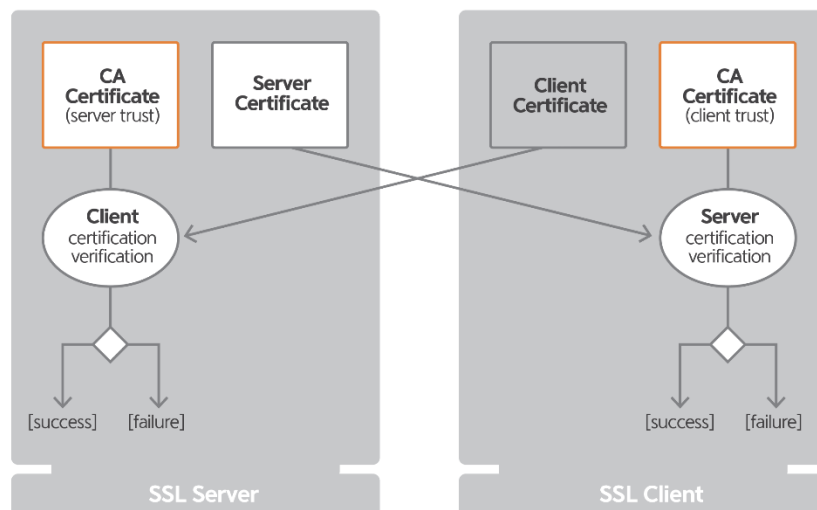


Image 2. Chain of Trust Concept

#### 2.2.4. Verify Firmware Forgery

Hanwha Techwin's Signed Firmware technology is a secure way to update firmware. By including a digital signature in the firmware and verifying the signature value upon update, you can trust that the firmware has not been forged or tampered.

The digital signature of the firmware is generated with a private key through a key server securely managed by Hanwha Techwin, and the public key that verifies the digital signature is safely stored in the Wisenet7's Secure Storage area (HTPM).

Using digital signatures is a better way to improve security than using simple hashes, CRC checksums, etc. to verify firmware integrity. This is because the hash or checksum of a tampered firmware can be easily recalculated.

#### 2.2.5. Encrypt Video Image (when at rest and backup)

Video images generated from the camera must be treated as important user data. Therefore, not only must secure communication be used when transmitting video images, but also security mechanisms must be applied when storing images on an external storage medium and when backing up video from the camera to a PC/VMS/NVR.

Wisenet7 products support file system encryption when recording to an SD Card.

By encrypting the file system itself rather than individual encryption for each file, there is no load required for separate decryption during video transmission and playback. In addition, AES encryption is performed using the password set by the user as an encryption key, so that even if the SD card is stolen, the stored video can be safely protected.

Wisenet7 products support Video Encryption at backup. They protect the video by encrypting the ZIP file when backing up the video saved in the camera or manually recording the live video on the PC.

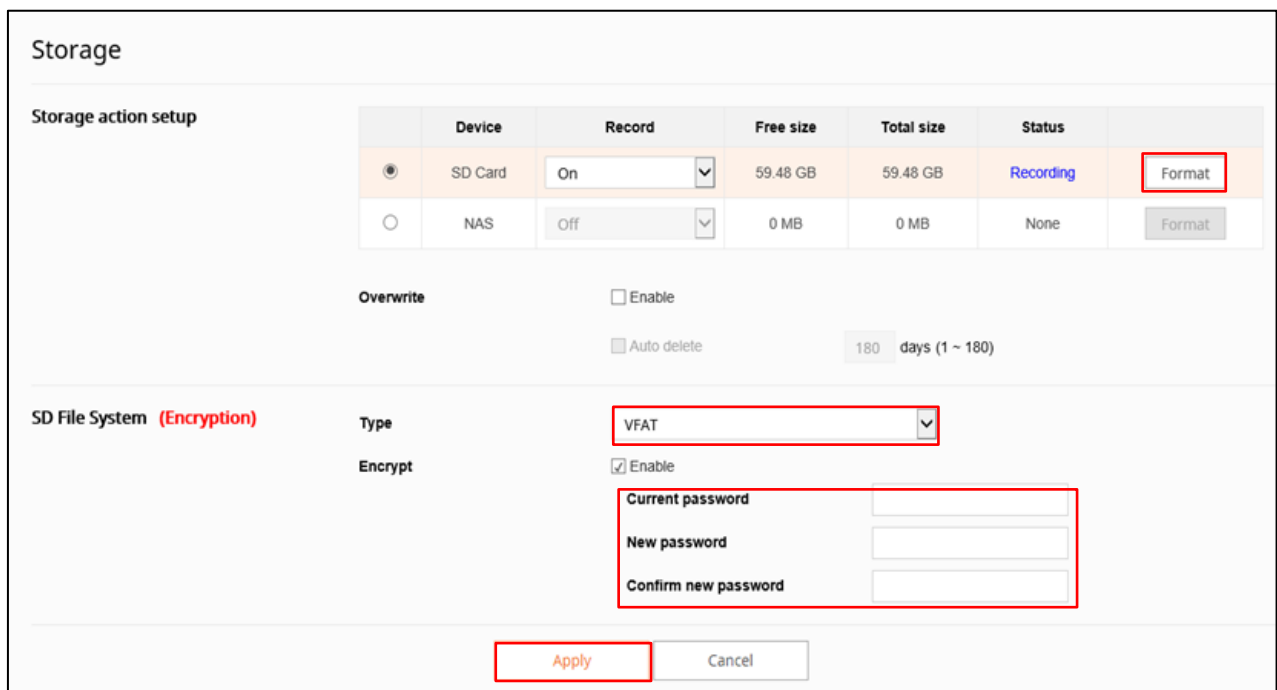


Image 3. UI on SD Card Encryption

## 2.3. Secure by Default/Design

When developing products, manufacturers need to keep in mind security standards to ensure the confidentiality, integrity, and authenticity of the system and user sensitive data. It is necessary to reflect these security standards from the product design stage, which is called “Secure by design”.

“Secure by default” means that the default configuration settings are the most secure settings possible, which are not necessarily the most user-friendly and backward compatibility settings. Therefore, the user must analyze the security risk according to the setting change suitable for usability and compatibility in each secure by default setting.

### 2.3.1. Raise the level of security settings

Wisenet7 products provide enhanced security out of the box at factory default settings. By default, the HTTPS mode is enabled, and unnecessary initial services are disabled, including SNMP (Simple Network Management Protocol), Link-Local address, UPnP discovery, and Bonjour. In addition, the SUNAPI & ONVIF protocols are disabled by default until a user password is configured. All Hanwha Techwin products ship without a default password. During initial installation, the user must set a complex password using the Wisenet Device manager utility before viewing video or making other configuration changes. The password is securely transmitted using encryption.

### 2.3.2. Apply the latest version of TLS protocol

Wisenet7 products support the latest TLS version 1.3. By default, only safe TLS versions (1.2, 1.3) are enabled for communications. TLS 1.2 is still secure and although it has faults, it is widely adopted and is currently the standard for IoT devices.

Additional options for specific TLS versions (1.0, 1.1) and HTTP communications are available when needed such as backward compatibility but not recommend.

The most noticeable differences in the TLS 1.3 version include Faster performance and Enhanced security.

### 2.3.3. Provide Secure Cipher Suites

Previously, some weak cipher suites are provided for compatibility in TLS mode. but, Wisenet7 products provide initially security-enhanced cipher suites and then they provide option to apply weak cipher suites for compatibility.

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken (i.e. cracked). The larger the key size the stronger the cipher. Weak ciphers are generally known as encryption/ decryption algorithms that use key sizes that are less than 128 bits (i.e., 16 bytes ... 8 bits in a byte) in length.

To understand the ramifications of insufficient key length in an encryption scheme, a little background is needed in basic cryptography. Cryptography is the process of converting ordinary information (i.e., plaintext) into a scrambled unintelligible mess (i.e., cipher text). This conversion process is called encryption. The second process of cryptography is called decryption which takes the cipher text and recreates the plaintext. These processes (encryption/decryption) are controlled by a 'key.' The key is a secret that is shared between the two communicating parties. The key is used to cipher the plaintext and to decipher the cipher text.

Secure communications revolve around four basic components. These four components are: the encryption/decryption algorithm to use on the data to be exchanged, the encryption/decryption algorithm to use for the shared key exchange, the authentication type and the message authentication code. And, if more than one of these four elements is used, it could be classified as a weak cipher suite.

HTTPS

---

**TLS settings**

|                    |  |
|--------------------|--|
| <b>Cipher mode</b> | <input checked="" type="radio"/> Secure cipher suites only |
|                    | <input type="radio"/> All compatible cipher suites         |
| <b>Version</b>     | <input type="checkbox"/> TLSv1_0                           |
|                    | <input type="checkbox"/> TLSv1_1                           |
|                    | <input checked="" type="checkbox"/> TLSv1_2                |
|                    | <input checked="" type="checkbox"/> TLSv1_3                |

Image 4. TLS Setting option

To further strengthen the cybersecurity of the camera, it is recommended to use multiple layers of security. This ensures that if one layer is breached, other layers are still present to protect your network and devices. It is recommended to have collaboration between IT, video security, the system integrator, and the end user to determine the system requirements as well as the responsibilities of each group. The following is a list of cybersecurity related features that can be implemented in your network devices to enhance your network security, including cameras, switches, etc.

- Create user-level accounts with least privileges required
- Disable guest / non-authenticated RTSP access
- Change passwords regularly & do not share passwords with other systems
- Update system clock/NTP, DST, time zone
- Enable 802.1x certificate-based access control
- Enable Multicast only if needed
- Enable DDNS only if needed
- Enable Bonjour only if needed
- Enable UPnP only if needed
- Enable link-local address only if needed
- Enable FTP only if needed
- Use SNMP v3 when SNMP is needed
- Use secure SMTP when e-mail is needed
- Enable QoS only if needed
- Enable VLANs on network
- Ensure camera is out of reach, cables are protected
- Change default ports from well-known ports to high ports
- Enable IP Filtering

- Ensure cameras are on a separate network from corporate/production network/Internet
- Enable SD card recording as a backup in case of VMS or network disruption
- Document configuration and create an export/backup
- Save a snapshot of camera view
- Place a recognizable setting to indicate tampering/defaulting
- Utilize VPN or secure cloud for remote access
- Use proprietary video file format for SD recording and exporting video
- Ensure all network switches, NVRs/VMS, & PoE midspans/injectors are protected by a UPS
- Enable tampering, defocus detection analytics
- Enable network disconnect detection if using low voltage power
- Check device logs regularly

Wisenet7 offers end-to-end cybersecurity with the industry's highest levels of cybersecurity policy with Secure boot/OS/storage, a signed firmware/open platform app, Secure JTAG and more. Hanwha Techwin established its own device certificate issuing system to embed certificates into the product not only in the development progress but also in the manufacturing progress. With the next-level cybersecurity features of Wisenet7, users can now build the surveillance solution that has never been safer before.



# WISENET

Hanwha Techwin Co.,Ltd.

13488 Hanwha Techwin R&D Center,

6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do

TEL 1588.5772

<http://hanwha-security.com>

Copyright © 2021 Hanwha Techwin. All rights reserved.

