WISENET

White paper

Cyber Security

Securing Video Surveillance Devices to Close Network Vulnerabilities

2017.1.26.

Hanwha Techwin

Contents

Contents

1. Introduction

WISENET

We live in an increasingly connected world, where more and more devices and systems are networked and shared with other systems. Convenience is a main driver behind this trend, as people have come to expect the ability to connect to and control devices and systems anywhere, anytime.

However, there is a downside to the unprecedented level of convenience provided by the growing number of networked devices, namely increased security risk. Because each device is an endpoint for networks, they introduce the potential to become entry points for hackers and others with malicious intents. In fact, in many of the most high-profile data breaches that have occurred recently, hackers were able to access corporate networks through POS, *HVAC and other networked systems that failed to provide an adequate level of security to prevent these types of breaches.

*HVAC: Heating, Ventilation and Air Conditioning

While IP-based video surveillance and other solutions have grown in popularity to become the accepted standard for new deployments and upgrades, security systems are no exception. A hacker does not discriminate among networked devices whether it performs a critical function like security or not. As such, video surveillance cameras and other devices are among the lengthy list of potential network entry points that are continually being probed for vulnerabilities that can be exploited. Therefore, it is essential that organizations take the necessary measures to ensure the highest level of security for their networks and IP cameras, encoders, NVRs and DVRs. There are a number of best practices that should be undertaken to strengthen device security to prevent unauthorized access and protect end users video surveillance systems and their overall network.

Hanwha Techwin is not only aware of these best practices but has built a number of technologies and capabilities into its products to make it easier for organizations to take these important steps toward improving network security.

1. Introduction

These items should be reviewed by the owner of security systems, IT personnel, and Systems Integrators installing systems to determine the level of security needed while balancing the ease of use, with acceptable risks.

This guide will show snapshots from network cameras where applicable. Most settings can be configured in batch for multiple cameras using the Wisenet Device Manager Software (Figure 1).

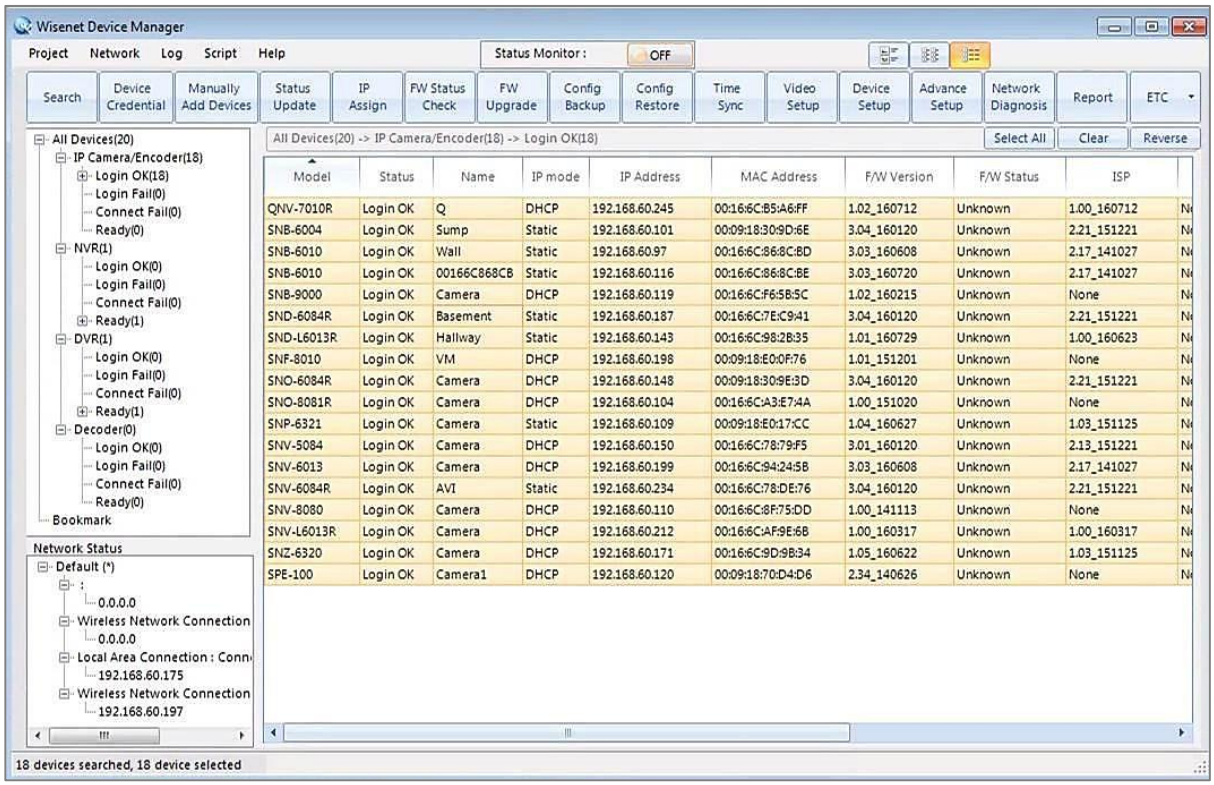


Figure 1. Wisenet Device Manager screen

2. Password

WISENET

From checking email to unlocking smartphones or logging in to computers, passwords are an integral part of our everyday lives. So it seems intuitive enough that people would recognize the importance of creating strong passwords to protect their devices and networks, but in reality that isn't always the case. These best practices will help ensure the highest level of password security.

If devices such as camera and recorder have an initial password, user should not use the initial password and set own password as the initial password is widely open through user manual or internet. Hanwha Techwin does not provide an initial password and all devices are designed to set password at its initial use.

However, just password change is not enough. Because many people make two mistakes very often for there convenience while setting password.

The first is using the same password for everything. The danger here is that if someone can decipher the password for, say, your email account, they then have access to everything you've password-protected, opening up the potential for theft, identity theft and much more. The second – and most risky – mistake people make in order to more easily remember their passwords is using names, birthdates and/or words that can be found in the dictionary.

Hacking has become a highly organized and sophisticated practice that employs powerful tools, such as technologies that quickly and automatically cycle through possible combinations of words to decipher passwords. These tools have been fairly successful with easily remembered passwords that are so convenient for users. Additionally, with so much personal information available online, passwords that use names, birthdays or other significant dates can also be effortlessly cracked. Thus, it is imperative to use strong passwords that are much more difficult to break. There are a number of best practices that should be followed to accomplish this using a combination of letters, numbers and other symbols.

2. Password

While not required, it is also a good practice to use different passwords for each device or using the same password only for some – not all – of the devices, clients and systems on the network. Creating a unique username instead of using the admin account for the VMS and other clients to connect to is highly recommended. This prevents the admin password from being constantly transmitted over the network in an effort to prevent it from being intercepted.

Hanwha Techwin products require 8 to 15 letters long password. If the password is 8 to 9 letters long, it should be a combination of at least three types upper/lower case alphabet, numbers and special characters. If the password is 10 to 15 letters long, then it should be a combination of at least two types upper/lower case alphabets, numbers and special characters. In addition, consecutive or repeated text string is not available for password.

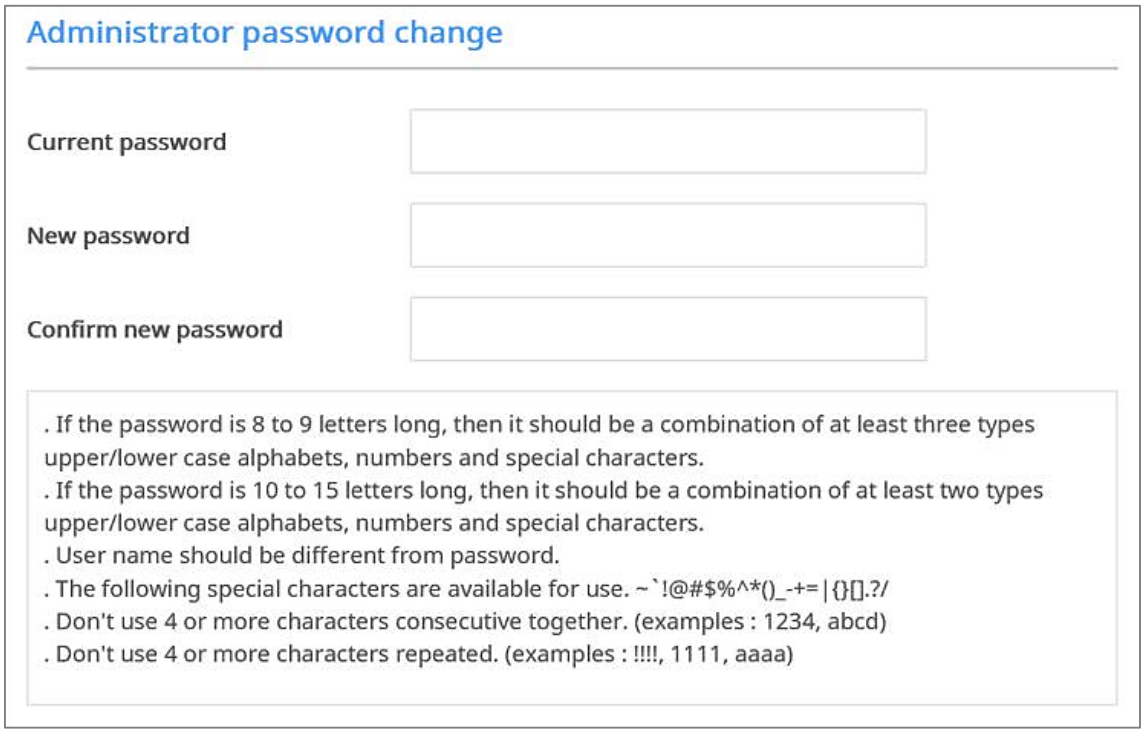


Figure 2. Camera Password Configuration

3. Authority Separation

Limiting the authorization associated with this unique account will also limit a hacker's access. Therefore, should an account be compromised, the impact will not affect the entire camera, including its settings. Also, unique credentials make analyzing logs much easier and more informative. Hanwha Techwin cameras and recorders allow many user/user groups to be created with various permissions and user levels.

3.1. Least Privilege Principle

Use the principle of least privilege, providing the user with the minimum features needed to perform their necessary functions. If they need to access the setup menu once a year, provide an alternate user login through the web interface instead of allowing their VMS account full access, or better yet, have a higher level user perform this non-routine task. This will help to prevent "drive-by" configuration changes, and keeps the high-level credentials off the network as much as possible.

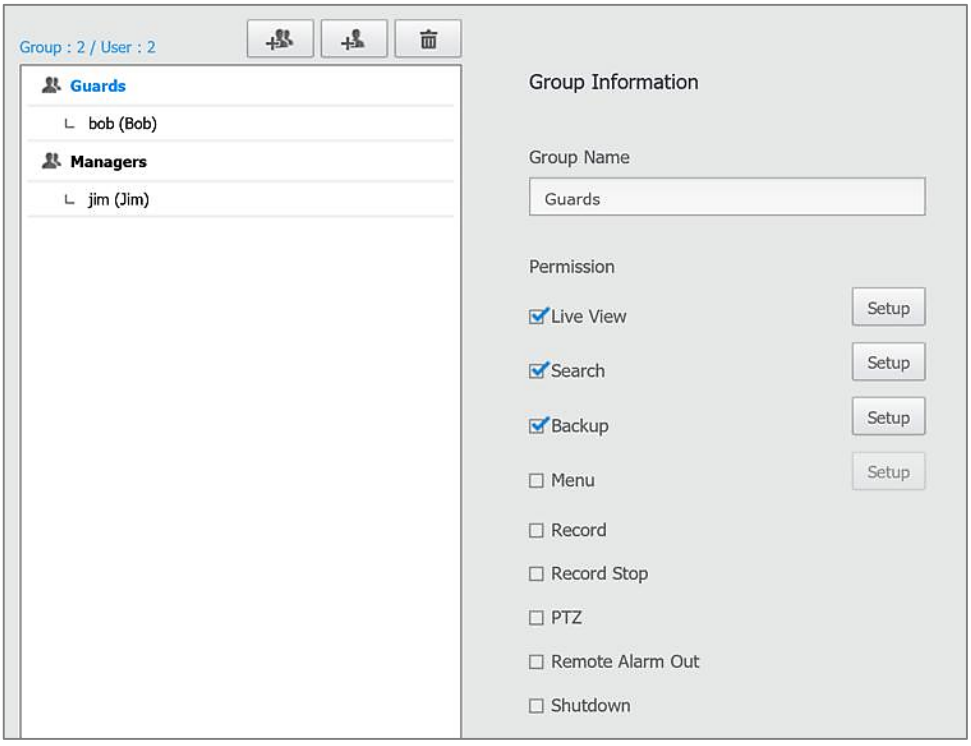


Figure 3. SSM User Authority Configuration

3.2. Guest Access

Hanwha Techwin cameras provide a separate guest login feature with the username and password “guest.” This account has limited privileges and is inactive by default, so it must be specifically turned on in the setup menu. This is ideal for limited access uses, but should remain disabled when not needed.

4. Authentication and Encryption

4.1. Digest vs. Clear Text Authentication

Usernames and passwords are sent over networks using clear text, base64 encoding and basic authentication of HTTP protocols which allows open access to these credentials to anyone who is monitoring the network to intercept and view traffic, allowing them to access a device.

While digest authentication encrypts data using a hash function, which is then compared to the hashed credentials on the device. As a result, digest authentication strengthens security by not sending actual usernames and passwords over the network.

Hanwha Techwin products support digest passwords and doesn't provide basic authentication. However, the same cannot be said for every client that connects to a device. Therefore, it is important to determine their capabilities to ensure that all clients a) work, and b) do not revert to clear text or base64 passwords.

4.2. SSL Encryption

SSL is an excellent method for ensuring user credentials and data itself are sent to their intended destinations. This simple, cost-effective method further enhances the security of a device.

Built-in certificates allow SSL encryption to be up and running in seconds. SSL certificate can also be purchased from a commercial Certificate Authority or issued by corporate entities for even further security to avoid a certificate security message upon access. While SSL security is a great way to harden your communications channel in a potentially insecure network or cloud, determine which channels need to be encrypted and is supported. This includes camera to NVR/VMS and VMS to client. SSL encryption should also be used when sending e-mail notifications using the SMTP protocol to prevent credentials from being sent in clear text. Make sure that your SMTP server supports SSL/TLS and verify what port is used.

Configuration options allow the selection of a unique (built-in) or public certificate, and the installation & naming of a certificate and key file. When the HTTPS options are changed, the camera will reboot, and then only allow encrypted HTTPS communications to take place over the HTTPS port (refer to Figure 4).

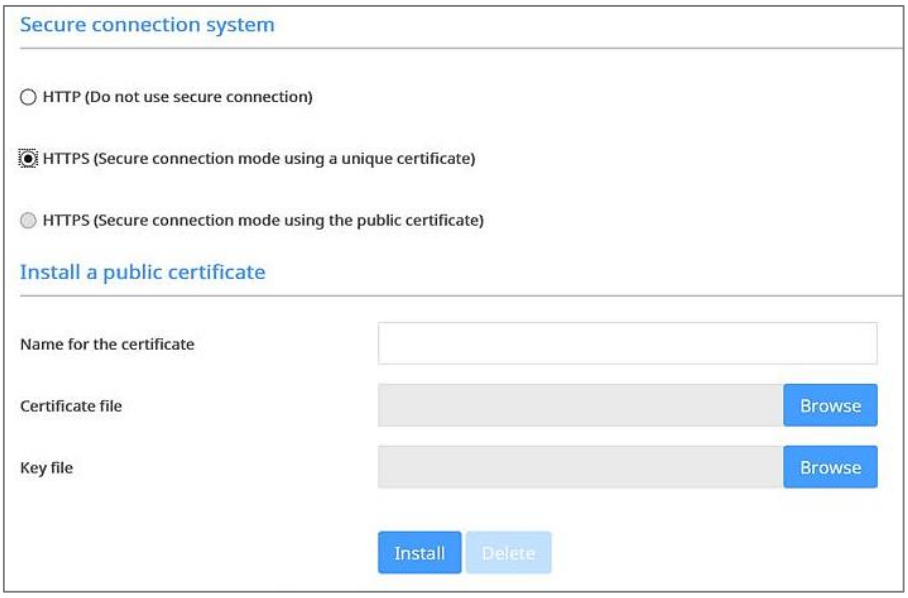


Figure 4. SSL Encryption Configuration

4.3. Minimum Use of Cloud Storage

Using a cloud service to record or view your system not only requires large amounts of bandwidth, but also can introduce a security problem. When the cloud connects to a device, it sends login information. If this information was captured or a man-in-the-middle attack (MITM) used, the credentials could be decrypted or replayed, allowing unauthorized access. In addition, not all cloud services support SSL encryption or even digest authentication.

5. Network Setup and Configuration

5.1. Physical Network Segregation

One common and effective technique to increase the safety of a security network is to physically separate the cameras and recorders from the corporate network. This prevents attackers from gaining access due to the lack of access. Many NVRs have multiple network interfaces, allowing them to record from one, and provide workstation access on the other. This technique reduces the number of externally exposed devices, which need increased security controls.

5.2. VLAN

The use of Virtual LANs (VLANs) is recommended to keep a security network separate from the corporate network when a separate network is not employed. VLANs operate on the network switches and segregate the traffic commonly based on switch ports. This allows firewalls to protect security devices away from other devices on the network. If access is needed to specific devices, firewall rules can be created or a device can be added to the VLAN.

5.3. IP Filtering

IP Filtering is a method to explicitly specify who is allowed to access a network device or conversely, who is denied access to the device. An IP address or range/subnet can be specified. This can ensure only the correct people, based upon their PC's IP addresses have access to the device, and a drive-by attempt from the local network or the Internet is denied access. Hanwha Techwin devices allow the entry of IPv4 and IPv6 IP addresses & prefixes for denying or allowing access. The range to be filtered will be shown to validate the IP and prefix before confirming and applying. Make sure to verify this before applying, otherwise you could be denied access. Up to 10 entries can be added each for IPv4 and IPv6 (Figure 5).

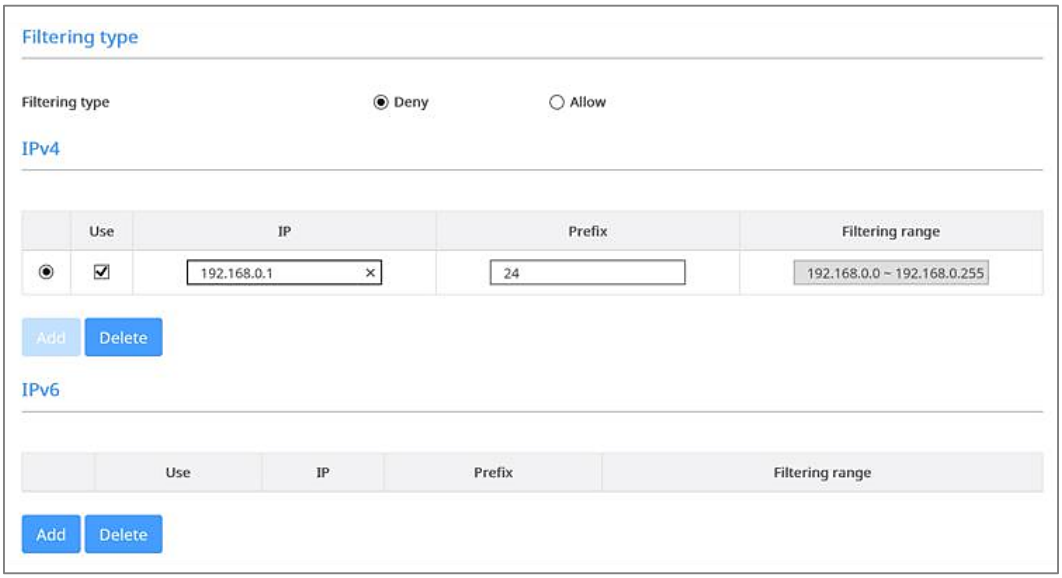


Figure 5. IP Filtering Configuration

5.4. VPN

The best practice for connecting remote locations, such as multiple office, or remote workers is to use a VPN solution. This creates a secure, encrypted channel eliminating the chance of information leakage, such as usernames and passwords. A VPN solution can involve dedicated hardware such as a VPN router, and/or a software VPN running on a client PC.

5.5. Change Default Ports

In today's connected world, many devices are connected to the Internet (whether intentionally or unintentionally), and there are numerous services employed by hackers to perform scans, looking for these devices.

One simple way to help hinder these scanners, as well as script-kiddies, drive-by attacks and inadvertent access is to change the ports of networked devices from their well-known defaults readily available online to higher port numbers of your choosing. Especially important is the HTTP web port, which for most devices defaults to port 80 to allow access via a web browser. Changing this port to 8000, for example, requires an extra step when entering the address in a web browser, often protecting from a simple scanner or someone manually typing an address in to a web browser.

5.6. Disable Unused Ports, Services, Protocols

Because many security devices are full-blown computers, running on modern operating systems, Hanwha Techwin has taken the approach of using custom-developed, stripped-down Linux operating systems, where any unused service has been removed or disabled. Many other manufacturers leave these services available for debugging or due to lack of a strong security awareness and/or posture. A number of recent incidents where other manufacturers' devices have been hacked involved attackers entering a device via telnet, which provides full

command line access to all files and services. Windows-based recording platforms have a host of services running in addition to requiring constant security updates and patches, requiring time, tracking, and Internet access.

Hanwha Techwin devices utilize a variety of protocols that provide useful functions. However, it is recommended that any services not needed for an application be disabled. This could include multicast, Dynamic DNS (DDNS), Quality of Service (QoS), Bonjour, Universal Plug and Play (UPnP) discovery & port forwarding, link local address, File Transfer Protocol (FTP), Network Attached Storage (NAS) and email notifications. As mentioned earlier, implementing unique credentials and restricting privileges for FTP, NAS and email are also excellent ways to further enhance security. Auto IP Configure protocols are enabled by default, whereas other services listed are all disabled.

5.7. RTSP

Many VMS stream video using the RTSP protocol. Hanwha Techwin cameras provide an option to allow RTSP video connections without requiring authentication. This can be useful when sending streams over the Internet for public viewing to ensure the credentials are not exposed or for 3rd party integration when authentication is not supported. For Hanwha Techwin cameras, this function can easily be enabled from within the camera's user interface during deployment if required. However, it is recommended to require authentication for all video stream in terms of security. If public viewing is needed, 3rd party services can ingest the authenticated stream and provide public access via another portal isolating the camera from direct public access. Hanwha Techwin cameras do not open passwords over RTSP protocol by supporting digest authentication as well as HTTP protocol by default.

Three of the most common methods of attacks used by hackers are brute-force, Denial of Service (DoS) and buffer overflow. Each of these has proven effective in attacks and must therefore be properly addressed to protect devices and networks from unauthorized access. Hanwha Techwin cameras include two methods that have proven highly effective in achieving this goal.

6.1. User Account Blocking

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.

Figure 6. Password Input Block

6.2. Buffer Overflow Protection

Another common attack vector is for hackers to pass carefully crafted commands to a device in an attempt to disclose information or send commands directly to other underlying services, such as databases or file systems. Often these commands exploit a weakness in the parser or database or break the interface, allowing commands to be sent directly to the database server, operating system or file system. Hanwha Techwin devices filter commands before passing them to a web server or database, preventing attacks based on buffer overflows and direct hacking by making the underlying core services inaccessible to hackers.

6.3. Device Placement and Physical Access

Cameras should be installed so they cannot be easily reached, misdirected, or unplugged, preferably with an appropriate housing so that physical access cannot be gained. Network and power cabling should run through conduit or behind/through walls and ceilings so that the cables cannot be unplugged or intercepted. Consider vandal dome models for best physical security.

Physical access to any security of network device is paramount. With physical access, most devices can be defaulted, allowing new settings to be configured potentially by unauthorized individuals. As per the Defense in Depth security model, it is critical that network devices be installed behind lock-and-key, preferable with access control and/or video security monitoring. This provides multiple layers of security, not relying on a single mechanism.

6.4. Ensure Continued Recording

During a break in, a thief will often steal or destroy a recorder or server in an attempt to destroy video evidence. One method to combat this is to use SD cards recording in each of your cameras. While the recording retention period will be shorter, it will provide redundant recording capabilities. SD card recording can also be used in case of NVR/VMS failure, and intentional or accidental network disruption, permitting the camera still has power.

Configuration options include enable/disable SD card functions, continuous/event recording on full/I-Frame/none, pre& post event recording duration, record file type (AVI/STW), overwrite, auto delete/duration, normal recording schedule, & SD card file system. Any profile/codec can be selected for recording. An SD card can be reformatted if necessary, however a blank SD card that is inserted will be auto-configured. A NAS can also be configured instead of an SD card, or as a primary recording device with an SD card as an optional failover backup recording media. NAS recording has the same configuration options with addition of IP address, user ID, password, and default folder.

6.5. 802.1x Certificate-Based Access Control

In many buildings, network jacks may be accessible, or a camera could be unplugged or a cable tampered with to gain access to the Ethernet network infrastructure. The 802.1x standard provides port-based network access control that requires an identifying certificate to be installed on each connected device to gain access to the protected network. Thus, should an attacker plug an unauthorized device into the network, it will be denied access.

The Wisenet Device Manager can be used to easily enable 802.1x as well as deploy certificates from a centralized location without the need to make configurations on each cameras' interface. Configuration options include selection of EAP type, EAPOL version, user ID & password, and certificate/key installation.

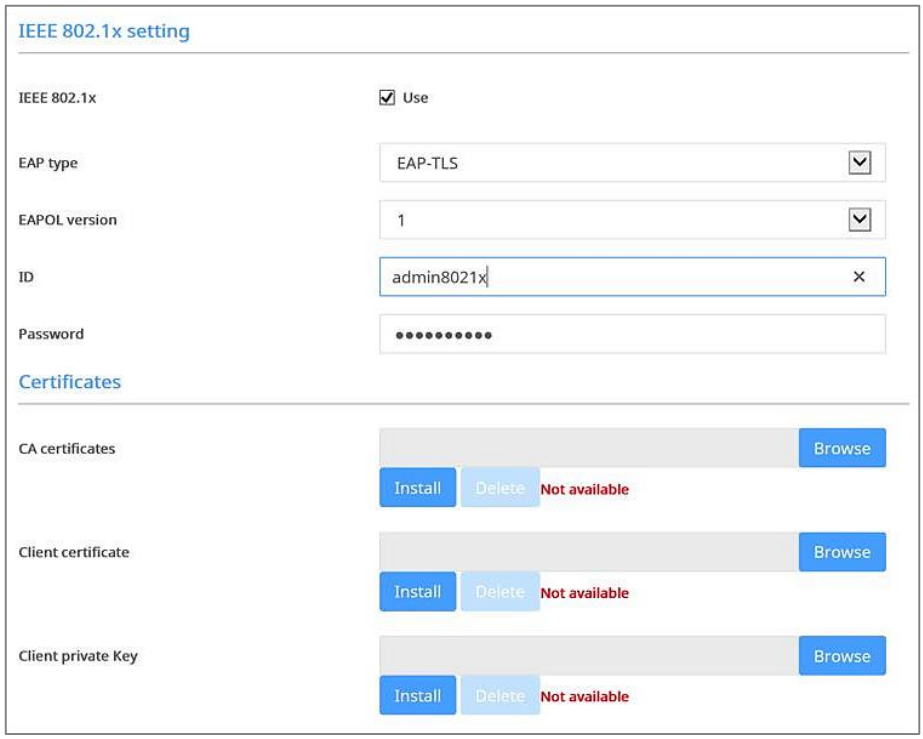


Figure 7. Certificates Installation Screen

6.6. Power

A UPS can ensure that your network devices stay powered and prevent damage from surges during power failures, managed shutdowns, brownouts, and inadvertent or malicious disconnection. If a UPS is connected to the network for management, make sure that it is properly secured and security updates are installed. There have been cases of attackers gaining access to a secure network through ancillary devices such as a UPS that was connected to a LAN or Internet for monitoring. Many IP cameras can also have dual power sources – PoE & low voltage 12vDC/24vAC depending on model, for redundant power in case the PoE power budget is exceeded. Most network switches can have a priority specified to indicate what type of device (phones, cameras, WAP, etc.), or which ports are more important in a power shortage.

6.7. Network Administration

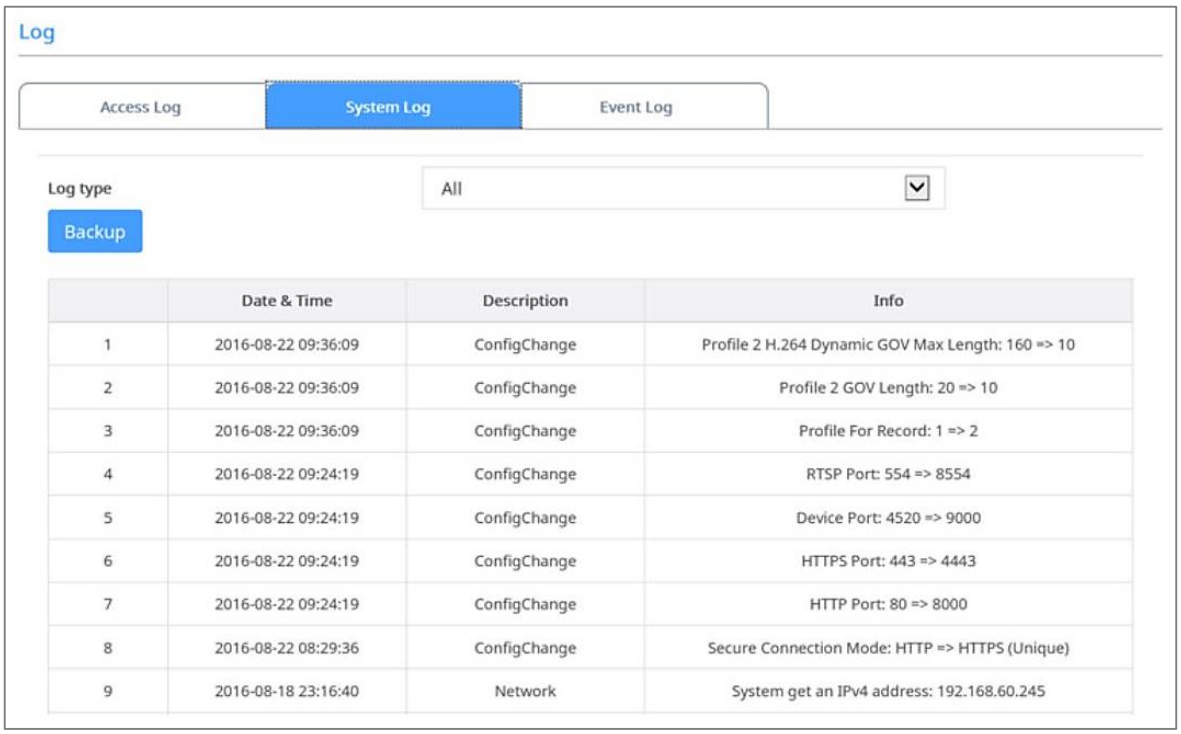
Beyond deployment, there are a number of tasks network administrators must continually undertake to ensure the ongoing security of their cameras and other devices. Among the most critical are reviewing all changes, developing and ensuring consistent and approved configurations, performing software updates and ensuring software complies with organizational security standards. As outlined here, Hanwha Techwin recognizes the critical role each of these plays in creating a strong overall strategy to lock down devices and protect networks from hackers.

6.8. Check Device Logs

Because Hanwha Techwin cameras log all changes made to device settings, it is important to check the logs to determine what changes have been made and who made them. To enable easy rollback, most log entries include both prior and new settings, and logs are retained during a factory default. The retained logs can be utilized for route analysis and trace back incase trespassing.

The Wisenet Device Manager can be used to easily download logs from multiple devices at once.

If settings cannot be verified, a factory default may be in order to ensure known good settings are in place. For Hanwha Techwin cameras, this can be done simply by holding the Factory Default button for five seconds while the camera is powered on. After defaulting the camera, it is important to configure the IP address and change the default admin password. A factory default can be executed while retaining all “IP & Port” and “Network” menu settings.



	Date & Time	Description	Info
1	2016-08-22 09:36:09	ConfigChange	Profile 2 H.264 Dynamic GOV Max Length: 160 => 10
2	2016-08-22 09:36:09	ConfigChange	Profile 2 GOV Length: 20 => 10
3	2016-08-22 09:36:09	ConfigChange	Profile For Record: 1 => 2
4	2016-08-22 09:24:19	ConfigChange	RTSP Port: 554 => 8554
5	2016-08-22 09:24:19	ConfigChange	Device Port: 4520 => 9000
6	2016-08-22 09:24:19	ConfigChange	HTTPS Port: 443 => 4443
7	2016-08-22 09:24:19	ConfigChange	HTTP Port: 80 => 8000
8	2016-08-22 08:29:36	ConfigChange	Secure Connection Mode: HTTP => HTTPS (Unique)
9	2016-08-18 23:16:40	Network	System get an IPv4 address: 192.168.60.245

Figure 8. Configuration Change History in System Logs

6.9. Regular Firmware Update

Hackers work tirelessly to identify and exploit vulnerabilities in software, particularly outdated versions that have not been updated to improve security. Once a vulnerability is found, it is often quickly disseminated online, opening the door for multiple individuals to easily access any device running older firmware versions – and by extension the network itself. Software providers recognize this and continually release updates to provide improvements and/or patches that will close those doors and protect users from unauthorized access.

The firmware for every Hanwha Techwin device includes a listing of updates administrators can refer to in order to ensure they are running the most recent version. It is recommended that firmware be up-to-date prior to a system deployment, and that it be regularly updated on an ongoing basis. Many installers opt to update firmware, assign IP addresses and set admin passwords on the bench before deployment.

The Wisenet Device Manager tool can be used to easily check firmware version and up-to-date status for all devices at once, and firmware can be downloaded and installed with just a few simple clicks.

6.10. Encrypted Firmware

Most security device manufacturers offer firmware to allow users to add features, bug fixes and security upgrades. The firmware provided for this improvement can also be targeted by hackers.

The firmware contains important information more than we think. For example, it contains algorithms for identifying user accounts, encryption algorithms and key information used to encrypt sensitive information, operating system files or important web service URLs, and if they are exposed, there also is the possibility of weaknesses exposure that can infiltrate the backdoor into firmware. If the corrupted firmware which including backdoor is distributed, hacker can take control of a device and use it as an outpost for other peripheral system attacks.

Most embedded devices, including network security devices, do not have special safeguards for firmware security. However, Hanwha Techwin distributes encrypted firmware using industry-recommended encryption algorithm for security and secure upgrades. Therefore if new firmware is released, update with latest firmware with confidence.

6.11. Video Formats

Most security equipment support industry standard, open video formats as well as proprietary video formats. On the surface, an open video format may seem ideal because users can simply open the video with their favorite media player. However, security applications demand a format that cannot be edited, altered or tampered with. This is essential, dictating that when video is downloaded, there must be a mechanism to authenticate the video and ensure that it has not been manipulated functions that simply do not exist with open formats.

Hanwha Techwin provides a watermarking function that can check whether the video has been falsified by storing the hash information of the video for each frame when it is stored in SEC format in NVR / VMS. If password is set, it is stored in encrypted SEC format, so your personal information can be protected even if the video file is leaked. The SEC format requires a dedicated player for playback which automatically included during back up. Hanwha Techwin's VMS, SSM supports not only watermarking function but also digital signature, and can sign and verify the video tampering by using hash information of whole video image. Validation of the watermarking and digital signature is possible using the backup viewer.

It is able to backup in AVI file format through the web viewer of the recording devices. Since the video file is an open video format, it can be played by the universal media player. Hanwha Techwin IP cameras can store videos in STW file format and export them via web viewer. It can be played and converted to AVI file format using the standalone SD card player.

6.12. Open Platform Apps

Many Hanwha Techwin cameras allow the installation of third-party applications to enhance their functions, such as providing license plate recognition, retail business intelligence, people counting and more. When running apps on cameras, it is important to know which are installed, as well as the source of the software package.

During installation, Hanwha Techwin cameras inform you of an app's required permissions; be sure to read this information carefully and understand whether data will be sent to any other location. If an app cannot be verified or if its purpose is unknown, stop installation immediately, uninstall the app and obtain it from the trusted partner that provides it. Configuration options include setting auto start, priority level, starting/stopping apps, installing/uninstalling apps, and executing an app webpage.

7. Conclusion

WISENET

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

Therefore, these best practices serve as a conversation starter for organizations that recognize the importance of and are serious about securing their networks. Open and informed dialogue between the end user, their IT department, the installer and systems integrator are the key to finding the best solution to fit an individual organization's security needs.

Hanwha Techwin inspects product security and diagnoses vulnerability from development stage by own security team and specialized institution. Strict policies such as user authentication, database & firmware encryption, backdoor removal and strict password ID and rule are applied to all products for the trustworthy security.

WISENET

Hanwha Techwin Co.,Ltd.

Hanwha Techwin R&D Center, 6, Pangyo-ro 319beon-gil,
Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea

TEL 82.70.7147.8771-8

FAX 82.31.8018.3715

http://hanwha-security.com

Hanwha Techwin