

WISENET



White Paper

Cyber Security

Securing Video Surveillance Devices to
Close Network Vulnerabilities

Introduction

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.

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 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. 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).

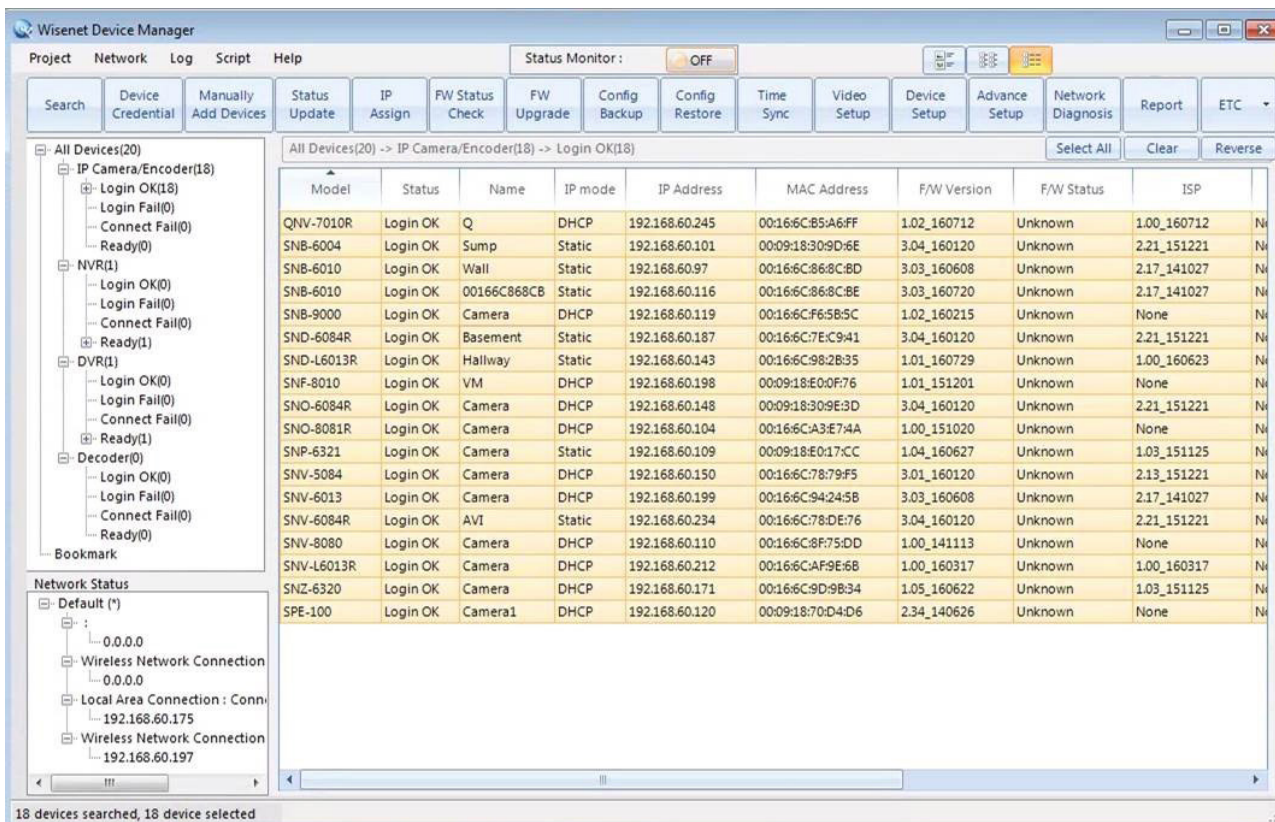


Figure 1

Passwords

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.

1. Change Defaults

Far too often, installers and/or end users fail or forget to take the simple step of changing default passwords for IP devices, including cameras, encoders, NVRs and DVRs when they are deployed. This is critical because default passwords can be easily located online or in user manuals, leaving devices unsecured and highly vulnerable to hacking. Therefore, changing defaults is perhaps the single most important step in securing devices.

Basic > User >

Hanwha passwords require a minimum of 8 characters and 2/3 categories of characters, depending on length. In addition, 4 or more consecutive or repeated characters are not allowed, and special characters are permitted. Passwords have a maximum length of 15 characters (Figure 2).

Administrator password change

Current password

New password

Confirm new password

. If the password is 8 to 9 letters long, then it should be a combination of at least three types upper/lower case alphabets, 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.

. User name should be different from password.

. The following special characters are available for use. ~`!@#\$%^*()_-=|{}[].?,/

. Don't use 4 or more characters consecutive together. (examples : 1234, abcd)

. Don't use 4 or more characters repeated. (examples : !!!!!, 1111, aaaa)

Figure 2

2. Avoid Common Mistakes

Simply changing the password is not enough. As a result of the seemingly endless number of functions that require authorization, there are two mistakes many people make with passwords for the sake of convenience, and all too often people make both when creating passwords.

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.

For example, Hanwha devices require passwords that are at least eight characters long, contain at least three character sets from uppercase, lowercase, numbers and symbols. Passwords longer than 10 characters require only two character sets. In addition, passwords cannot repeat the same character more than three times or have more than three sequential characters.

3. Utilize Multiple Credentials

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. For starters, this prevents the admin password from being constantly transmitted over the network in an effort to prevent it from being intercepted. Second, 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. Finally, unique credentials make analyzing logs much easier and more informative.

Hanwha cameras and recorders allow many user/user groups to be created with various permissions and user levels, as shown in Figure 3.

Basic > User >

Current users						
	Use	Name	Password	Audio-In	Alarm output	Profile
<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	manage	••••••••	<input type="checkbox"/>	<input type="checkbox"/>	All ▾

Figure 3

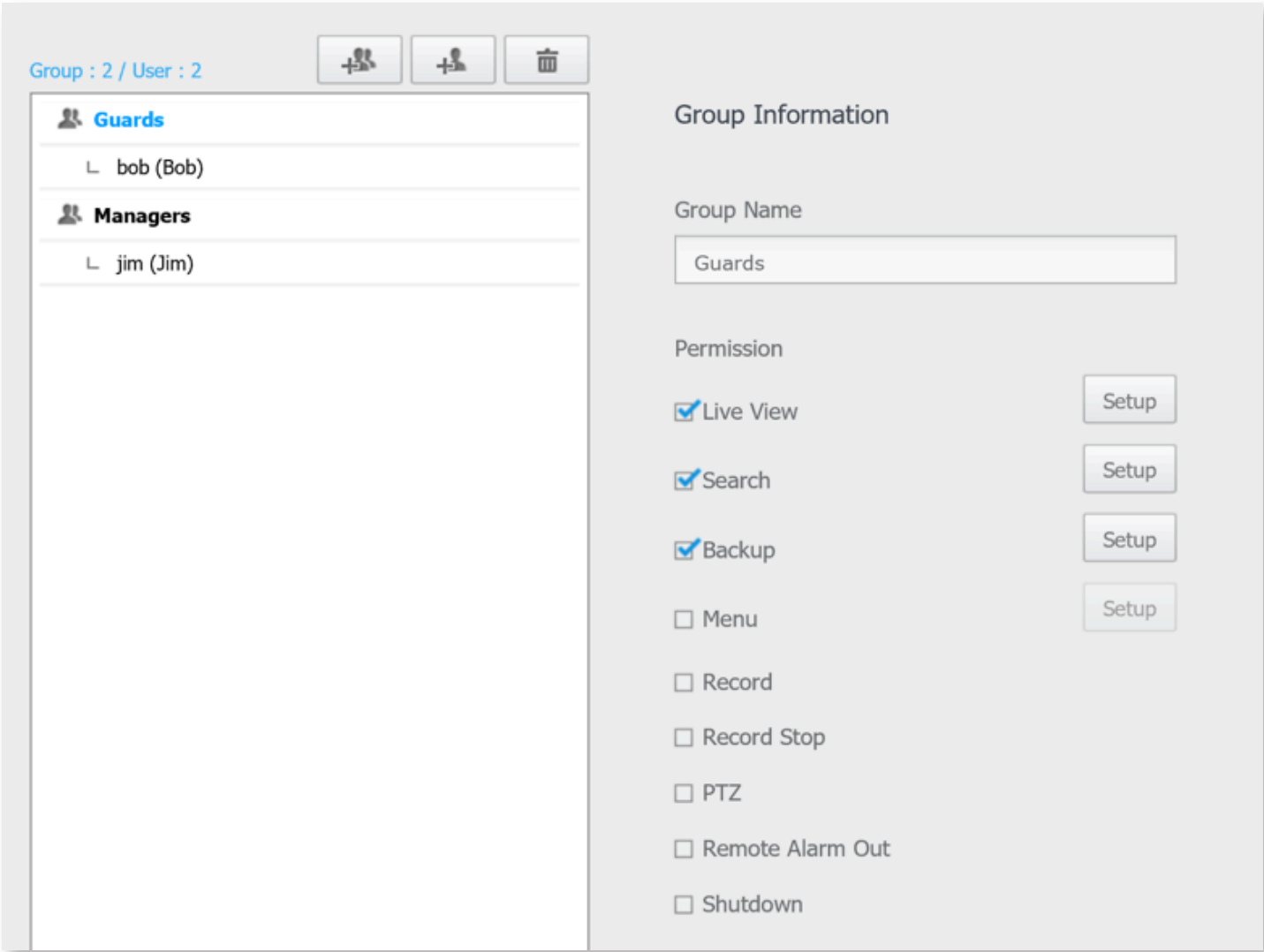


Figure 4

Guest Access

Hanwha 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.

Basic > User

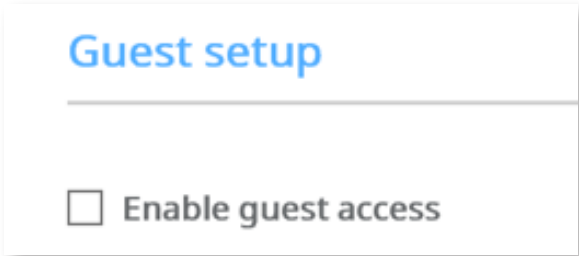


Figure 5

Least Privilege Principle

Another best practice is to limit what features a user has access to such as audio, PTZ, alarm I/O. 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. Configuration options are shown in the camera & recorder screenshots in Figure 4.

Authentication and Encryption

Because user authentication requires sending usernames and passwords over the network, even the strongest passwords can be easily stolen during that transfer. Therefore, it is imperative to choose the most secure authentication and encryption methods available.

Digest vs. Clear Text Authentication

Traditionally, usernames and passwords are sent over networks using clear text and base64 encoding, which provides open access to these credentials to anyone who is monitoring the network to intercept and view traffic, allowing them to access a device.

A second, less common tactic is using digest authentication to encrypt 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.

While all Hanwha products support digest passwords, 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.

SSL Encryption

One excellent method for ensuring user credentials and data itself are sent to their intended destinations and kept secure is to employ SSL encryption. 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 6).



Network > HTTPS

Secure connection system

☐

HTTP (Do not use secure connection)

☒

HTTPS (Secure connection mode using a unique certificate)

☐

HTTPS (Secure connection mode using the public certificate)

Install a public certificate

Name for the certificate

Certificate file

Browse

Key file

Browse

Install

Delete

Cancel

Apply

Figure 6

Avoid the Cloud

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.

Network Setup and Configuration

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 (Figure 7).



Figure 7

VLANs

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.

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 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 8).

Network > IP Filtering

Filtering type

Filtering type
☒ Deny
☐ Allow

IPv4

	Use	IP	Prefix	Filtering range
<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	192.168.0.1	24	192.168.0.0 ~ 192.168.0.255

Add
Delete

IPv6

	Use	IP	Prefix	Filtering range
--	-----	----	--------	-----------------

Add
Delete

Figure 8

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.

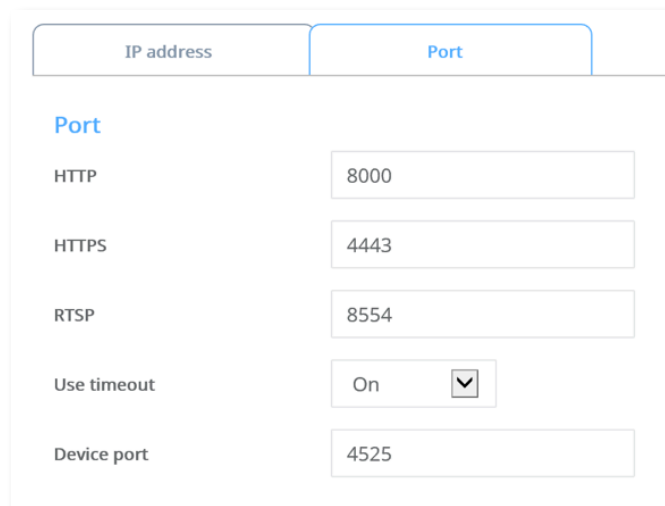
Ports and Services

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.

Change Default Ports

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 (Figure 9).

Basic > IP & Port > Port



IP address	Port
Port	
HTTP	8000
HTTPS	4443
RTSP	8554
Use timeout	On <input type="checkbox"/>
Device port	4525

Figure 9

Disable Unused Ports, Services and Protocols

Because many security devices are full-blown computers, running on modern operating systems, Hanwha 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 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 (Figure 10).

Network > Auto IP Configure

Link-Local IPv4 address

Auto configure

☐

IP address

169.254.11.161

Subnet mask

255.255.0.0

UPnP discovery

☐

Friendly name

WISENET-QNV-7010R-00166CB5A6FF

Bonjour

☐

Friendly name

WISENET-QNV-7010R-00166CB5A6FF

Figure 10

Network > DDNS

☒ Samsung DDNS

Server name

www.samsungipolis.com

Product ID

Test123

×

☐ Quick connect

Figure 11

SNMP

SNMP is an excellent tool for a network administrator to manage the devices on their network. Given the access SNMP can provide to networks, it is important to change the default community strings, using hard-to-guess, mixed-case alphanumeric entries. Unfortunately, SNMP v1 and v2c send the community strings in clear text, which could allow unauthorized access. IP filtering can be applied to increase security. If SSL encryption is enabled, SNMP v3 can encrypt the data, which is highly recommended. However, if SNMP is not used for device management, it is recommended to disable the protocol.

One challenge that contributes to the risk of hacking is that typically SNMP v1 or v2 is always enabled and cannot be disabled through the menu of a camera. Hanwha devices support SNMP versions 1, 2c and 3, however, all versions cannot be disabled through the user interface. In order to fully disable SNMP on Hanwha cameras, the following commands are used:

<http://IPADDRESS/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version1=False>

<http://IPADDRESS/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version2=False>

SNMP v2c is enabled by default on Hanwha IP cameras, with a Read Community of “public” and a Write Community of “write”. SNMP traps can be enabled for Authentication Failure & Network Connection to a specific Community string & IP address. SNMP v3 requires a password (Figure 12).

Network > SNMP

The screenshot displays the 'SNMP v1,v2c' configuration section. It includes checkboxes for 'Enable SNMP v1' (unchecked) and 'Enable SNMP v2c' (checked). Below these are text input fields for 'Read community' (containing 'public') and 'Write community' (containing 'write'). The 'SNMP v3 (Only operates when the SSL/TLS is authenticated.)' section has an unchecked 'Enable SNMP v3' checkbox and a 'Password' text field. The 'SNMP Trap' section features an unchecked 'Enable SNMP Trap' checkbox, a 'Community' text field, an 'IP address' text field, and two unchecked checkboxes for 'Authentication failure' and 'Network connection'.

Figure 12

RTSP

Many VMS stream video using the RTSP protocol. Hanwha 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 cameras, this function can easily be enabled from within the camera's user interface during deployment if required. It is recommended to require authentication for all video stream. 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.

Basic > User

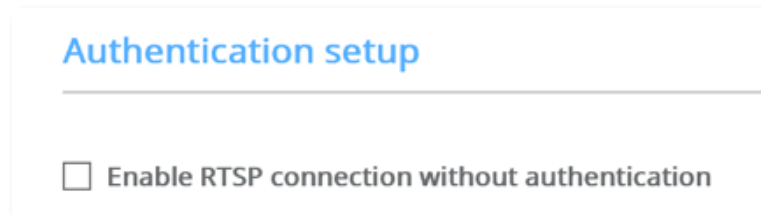


Figure 13

Identifying and Thwarting Attacks

Two of the most common methods of attacks used by hackers are 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 cameras include two methods that have proven highly effective in achieving this goal.

User Account Blocking

Denial of Service (DoS) attacks involves flooding a device with commands more rapidly than it can process them, overwhelming the device to the point where it can no longer serve up valid requests. To protect against DoS attacks, if a Hanwha camera receives too many unauthenticated requests, those connections are blocked while authenticated connections are allowed to continue as normal (Figure 14).



Figure 14

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 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.

Physical Access to Devices

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.

Device Placement

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.

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 (Figure 15).

Event > Storage

Storage action setup

	Device	Record	Free size	Total size	Status	
<input checked="" type="radio"/>	SD	On <input type="button" value="v"/>	0 MB	0 MB	None	<input type="button" value="Format"/>
<input type="radio"/>	NAS	Off <input type="button" value="v"/>	0 MB	0 MB	None	<input type="button" value="Format"/>

Record profile

H.264

Normal

None

Event

Full frame

Pre event duration

3 seconds

Post event duration

5 seconds

Record file type

STW

NAS connection setup

IP address

ID

Password

Default folder

Figure 15

Hanwha cameras can detect a physical network layer disconnection, and start recording on the edge, if power is still available.

Event > Network disconnection detection

Network disconnection

Enable

☒ On☐ Off

Event action setup

Record

☒

Alarm output1

Off

Activation time

☒ Always☐ Only scheduled time

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 16).

Network > 802.1x

IEEE 802.1x setting

IEEE 802.1x

☒ Use

EAP type

EAP-TLS

EAPOL version

1

ID

admin8021x

Password

.....

Certificates

CA certificates

Install

Delete

Not available

Browse

Client certificate

Install

Delete

Not available

Browse

Client private Key

Install

Delete

Not available

Browse

Figure 16

Tampering Detection

A common method for disrupting video is to physically block or obscure a camera’s lens, such as using a bag or spray paint, or by changing the direction in which a box or bullet camera is pointed. Tampering Detection generates an alert when a rapid change to the field of view occurs to identify potential issues, often before an incident occurs with a camera that is not functioning properly. All Hanwha IP cameras include tampering detection, without lowering the frame rate. Additionally, recognizable settings (such as name, SNMP) can be used to help identify if a device has been defaulted or compromised to gain access. In cases where the settings can’t be verified, restore to a known good configuration or reset it to default settings. Configuration includes sensitivity setting (Figure 17).

Event > Tampering Detection

Tampering detection

Enable

☒ On☐ Off

Sensitivity

-

50

+

Event action setup

FTP

☒

E-mail

☐

Record

☒

Alarm output1

Off

▼

Activation time

☒ Always

☐ Only scheduled time

Figure 17

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.

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 recognizes the critical role each of these plays in creating a strong overall strategy to lock down devices and protect networks from hackers.

Check Device Logs

Because Hanwha 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 Wisenet Device Manager can be used to easily download logs from multiple devices at once (Figure 18).

System > Log

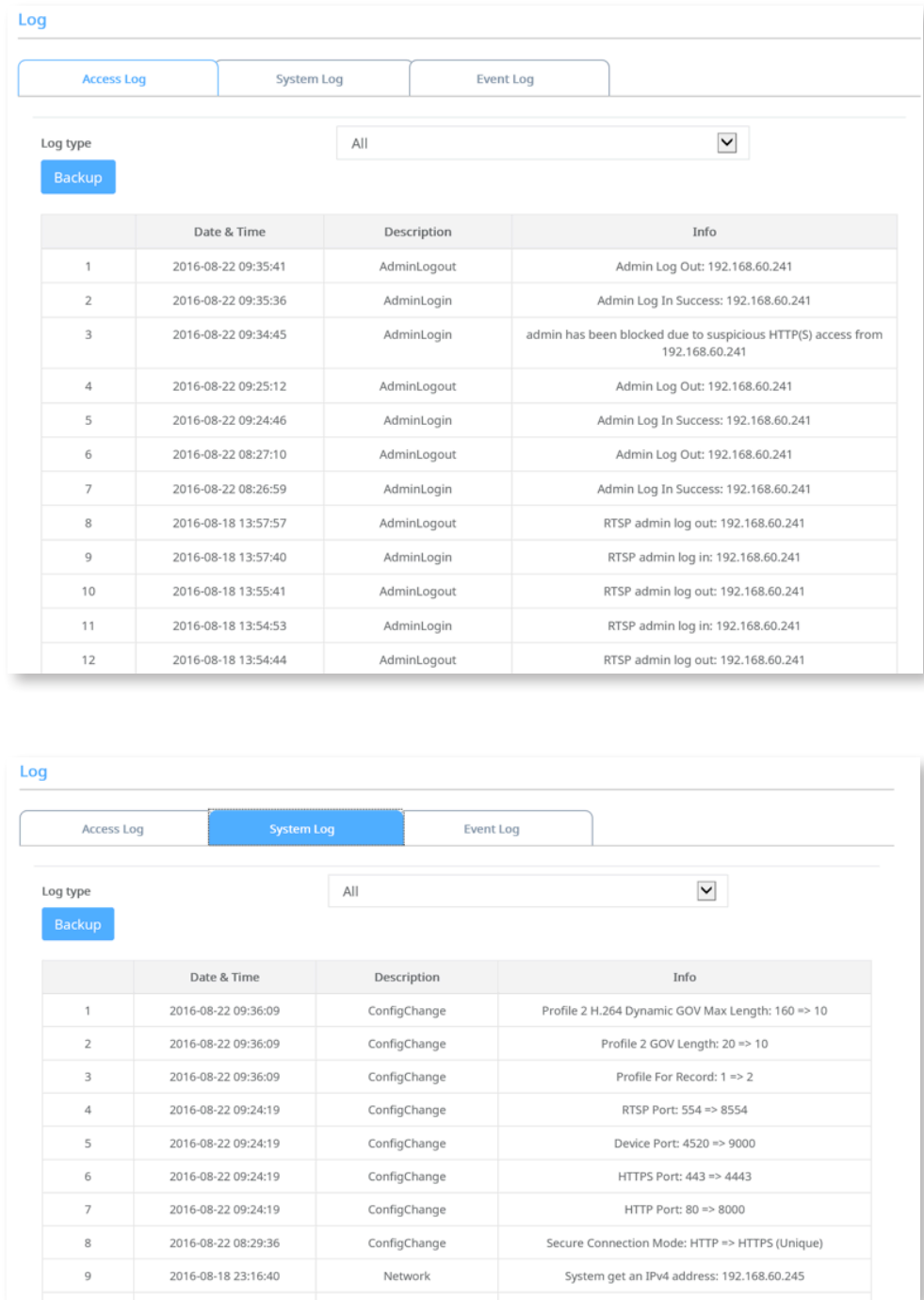


Figure 18

If settings cannot be verified, a factory default may be in order to ensure known good settings are in place. For Hanwha 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 (Figure 19 and 20).

System > Upgrade / Reboot

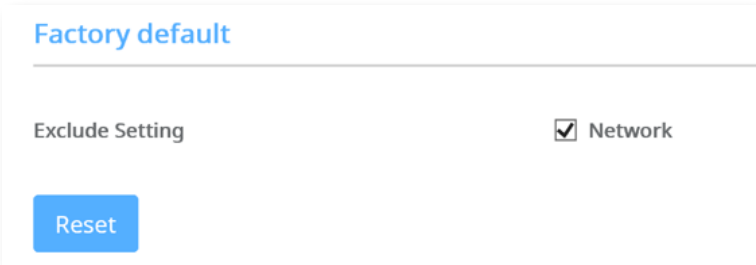


Figure 19

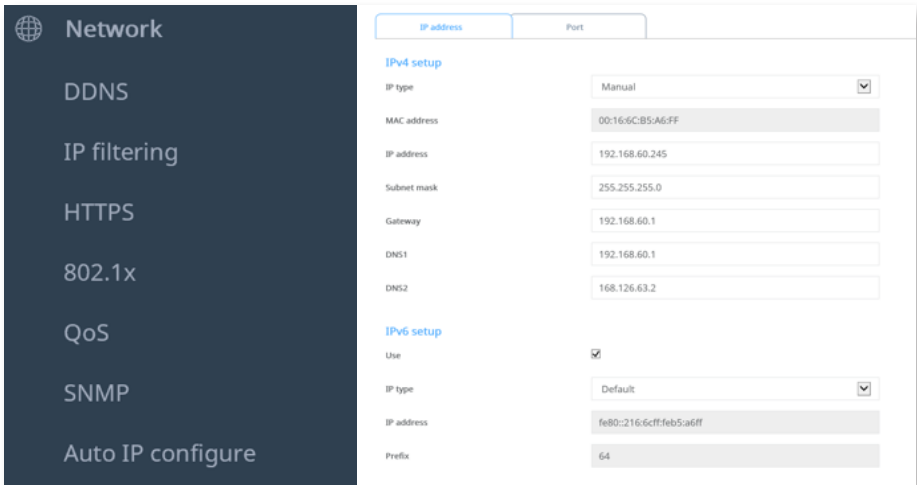


Figure 20

Back Up Configurations

Another critical administrative task is to perform regular backups of all known good configurations, which is beneficial in case of both inadvertent and subversive changes. The Wisenet Device Manager tool allows device configurations to be quickly and easily backed up and restored and can also generate a report containing key settings and information, along with camera snapshots, which are ideal for job completion records. The backup can also be restored as a template to newly installed cameras of the same model ensuring all settings are consistently applied for an easy installation (Figure 21).

System > Upgrade / Reboot

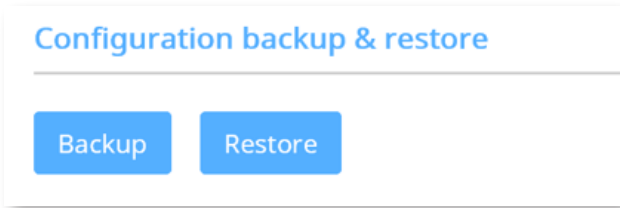


Figure 21

Update Firmware Regularly

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 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 (Figure 22).

System > Upgrade / Reboot

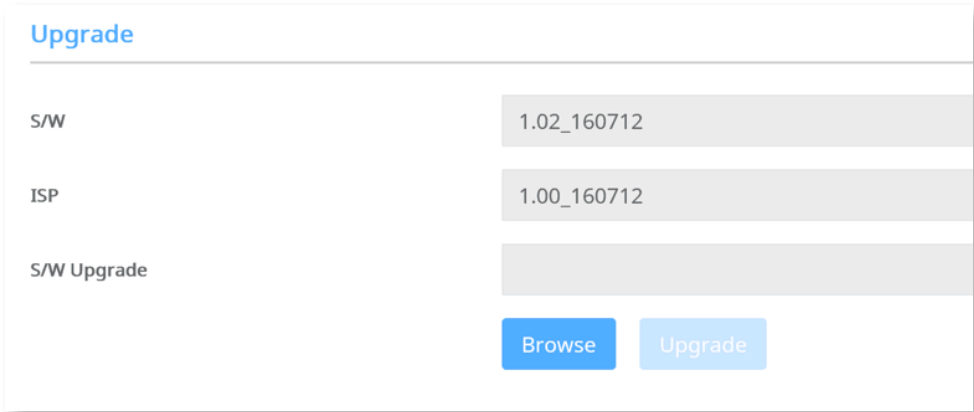


Figure 22

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 video formats provide these critical safeguards, as well as an optional, complex password that ensures video can be used as evidence. The required player is automatically included with any downloaded or archived video with no installation required. Users simply double-click the executable to view the video file. Hanwha IP cameras can store video in the STW file format. Videos can be exported by the web browser, or played back using the standalone SD Card Player. Video exported from a recorder can be saved in the SEC file format with the portable player included (Figure 23).

Event > Storage

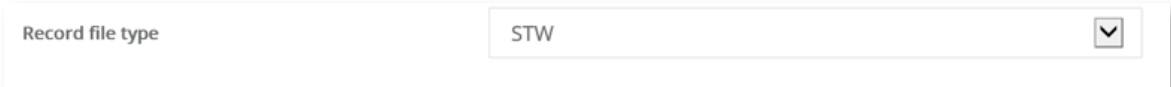


Figure 23

Open Platform Apps

Many Hanwha 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 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 (Figure 24).

System > Open SDK

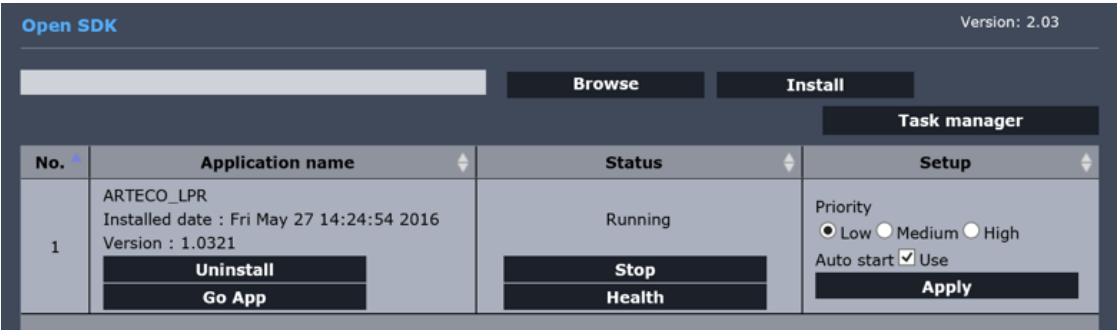


Figure 24

Summary

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

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

WISeNET

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



© 2016 Hanwha Techwin Co., Ltd. All rights reserved.

Under no circumstances, this document shall be reproduced, distributed or changed, partially or wholly, without formal authorization of Hanwha Techwin Co.,Ltd.

I.H-1607