HIKVISION

Network Video Recorder Security Guide

January 2018

www.hikvision.com

About This Document

This Guide shows users how to configure a Hikvision NVR system with a high level of cybersecurity protection.

User Manual

Trademarks Acknowledgement

Contact Information

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China

Tel: +86-571-8807-5998

Fax: +86-571-8993-5635

Email: overseasbusiness@hikvision.com; sales@hikvision.com

Technical Support: support@hikvision.com

HSRC (Hikvision Security Response Center) Email: HSRC@hikvision.com

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS TO THE APPLICABLE LAWS. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Contents

1. Abstract

Various types of security attacks in the Internet have become a severe threat for network devices and users' privacy. Hikvision network video recorders have integrated a variety of reliable security features to defend against without the owner even knowing their device has been compromised. Hikvision has added a number of cybersecurity protections and removed many features by default. This allows the user to open specified security functions according to their need.

Note: This document provides a general security overview; users should choose the appropriate security settings that apply to their actual situation.

2. Security configuration

2.1 Security deployment

Hikvision's high-end and mid-range NVRs have two network adapters, they are equipped with one or two LAN ports and POE ports. In Multi-Address mode, users can set one LAN port to connect to the local area network and another LAN port to the wide area network. Two network environments are isolated to some extent which enhances security. Users are expected to deploy the NVR in a data center or similar room with the appropriate physical protections.

2.2 Identity authentication

2.2.1 Setting a strong password

How to set a strong password?

A general strong password rule for Hikvision devices:

(1) Valid characters range [8-16].

(2) You can use a combination of numbers, lowercase, uppercase and special characters for your password using at least two of the above.

'Passphrases' are easy to remember but hard to crack. Here's a simple way to set a 'Passphrase'.

(1) Choose a phrase with number in it;

(2) Only use the first letter of a word;
(3) Letters should follow the case sensitivity of the original phrase;
(4) Use numbers rather than letters, for example, use '2' to replace 'to', use 4 to replace 'for';
(5) Don't delete punctuation.

Let's take the phrase below as an example:

'**My flight to New York will leave at three in the afternoon!** ' .

'Phrase password' should be '**MftNYwla3ita!** '.

Some tips for a strong password：

(1) Don't use sequential letters or numbers like 'cdef', '12345';
(2) Don't allow web browser to remember password on public computers;
(3) Don't email your passwords to anyone.
(4) Consider using a password manager so you don't have to remember the password.

2.2.2 Activating devices with strong password

Hikvision devices require the user to set a password before activation as shown in the picture below. In order to protect your data and privacy, we highly suggest you set a strong password according to the password rules.

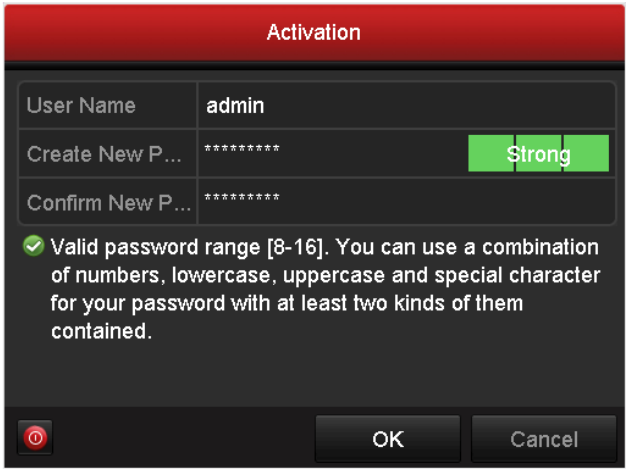

Fig. 2-1 Activation

2.2.3 Using GUID or security questions to reset a password

After the NVR is activated, the user is asked to export one GUID file which can be used to reset the password.

Fig. 2-2 GUID Attention

In addition, the user can set security questions and answer these to reset the password.

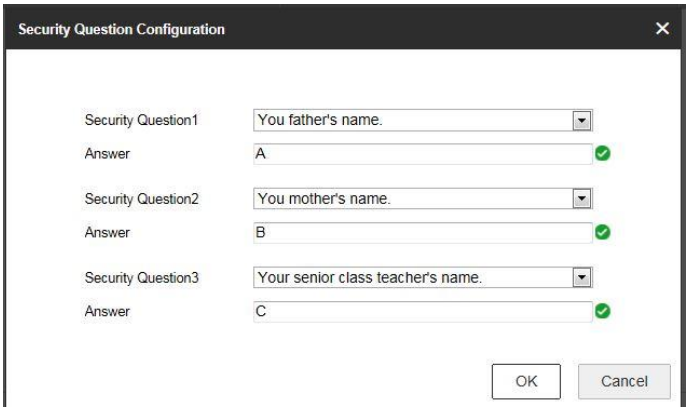

Fig. 2-3 Security Question Configuration

Enter the password reset interface by clicking “Forget Password”.

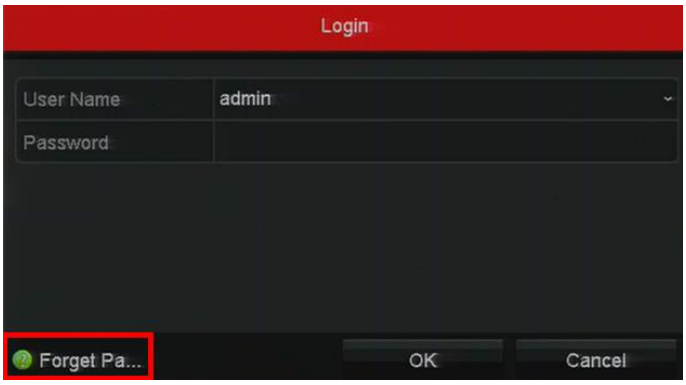

Fig. 2-4 Forget Password

If there are more than 7 failed login attempts with the GUID or security questions, the user will be forbidden for resetting the password for one minute.

After the admin password is changed or the GUID file has been used, the GUID file will expire.

2.2.4 Choosing a secure authentication method

Both RTSP and WEB support two authentication methods: ‘digest’ and ‘digest/basic’. Please select ‘digest’ as the method which is more secure. In the process of 'digest' authentication, the digest value of the password is transmitted, thus preventing the

leak of the password in the plaintext.

2.3 User Management

The Hikvision NVR supports 3 levels of user accounts: Admin, Operator & User. We highly recommend that each user account is created with a strong password using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters, in order to reduce the likelihood of the password being hacked. We also recommend that passwords are reset regularly, especially for high security systems.

The Admin user should check the other accounts regularly and delete them if they're no longer used in system.

When the admin user inputs the wrong password more than 7 times (or 5 times for operator/user), the account will lock to protect against a 'brute force' password attack.

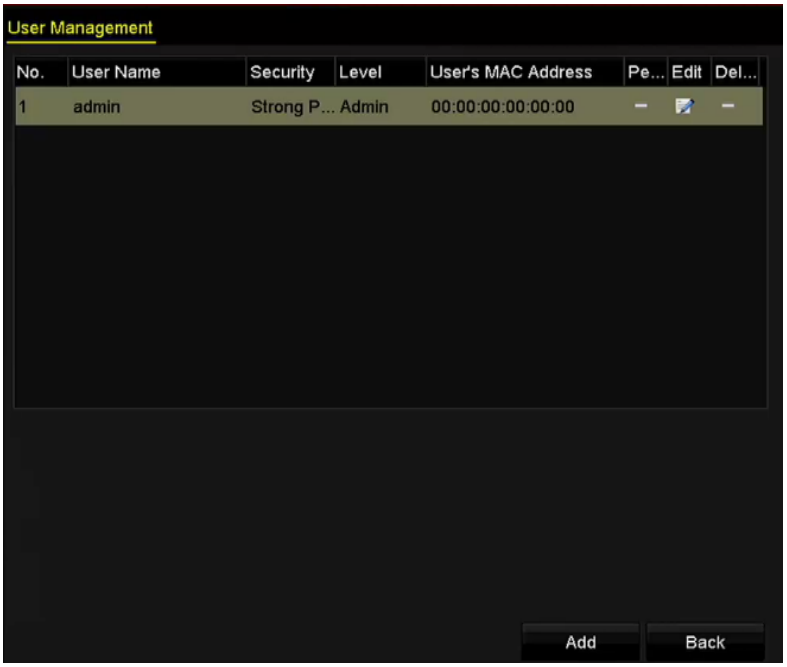

Fig. 2-5 User Management

The Admin user can assign different permissions for all users.

Permissions can be divided into 3 parts:

- Local Configuration
- Remote Configuration
- Camera Configuration

Local Configuration

• Local Log Search: Searching and viewing logs and system information of NVR.

• Local Parameter Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.

- Local Camera Management: The adding, deleting and editing of IP cameras.
- Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- Local Shutdown Reboot: Shutting down or rebooting the NVR.

Remote Configuration

- Remote Log Search: Remotely viewing logs that are saved on the NVR.
- Remote Parameter Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Remote Camera Management: Remote adding, deleting and editing of the IP cameras.
- Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.
- Remote Video Output Control: Sending remote button control signal.
- Two-Way Audio: Realizing two-way radio between the remote client and the NVR.
- Remote Alarm Control: Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.
- Remote Advanced Operation: Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- Remote Shutdown/Reboot: Remotely shutting down or rebooting the NVR.

Camera Configuration

- Remote Live View: Remotely viewing live video of the selected camera(s).
- Local Manual Operation: Locally starting/stopping manual recording and alarm output of the selected camera(s).
- Remote Manual Operation: Remotely starting/stopping manual recording and alarm output of the selected camera(s).
- Local Playback: Locally playing back recorded files of the selected camera(s).
- Remote Playback: Remotely playing back recorded files of the selected camera(s).
- Local PTZ Control: Locally controlling PTZ movement of the selected camera(s).
- Remote PTZ Control: Remotely controlling PTZ movement of the selected camera(s).
- Local Video Export: Locally exporting recorded files of the selected camera(s).

2.4 System logs

The operation, alarm, exception and information of the NVR can be stored in the log files, which can be viewed and exported at any time. Log information includes Number, Time, Major Type, Minor Type, Channel Number, Local/Remote User and Remote Host IP. Users can set various search parameters, including the Major Type, Minor Type, Start Time and End Time. The log is saved sequentially in a binary file format. When log files are full, new logs will overwrite the oldest log. Logs cannot be modified or

deleted.

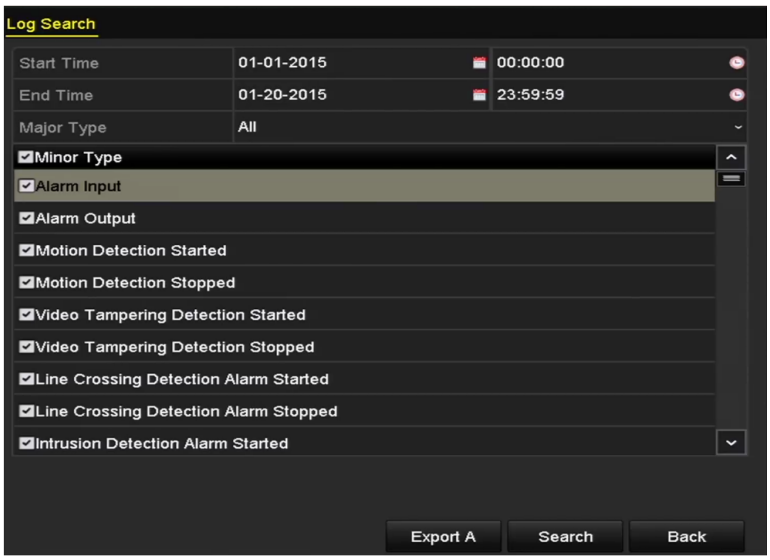

Fig. 2-6 System Log

2.5 Port and service

In order to decrease the risk of network attack, the NVR only opens specified ports by default. Users should only open ports and services that are necessary.

2.5.1 SNMP

You can use the SNMP protocol to obtain the device status and parameter information. Please ensure the SNMP status is off if it's not used.

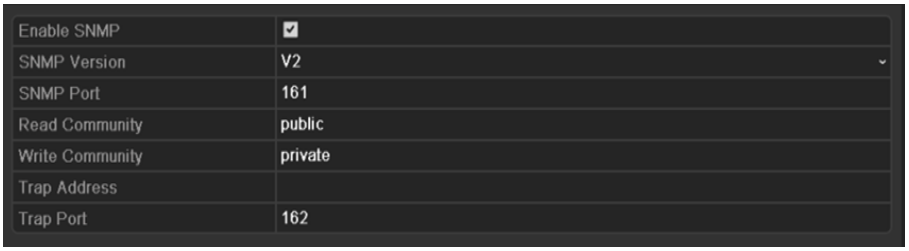

Fig. 2-7 SNMP

2.5.2 UPnP™

Universal Plug and Play (UPnP™) can permit the device to seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, and communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port

mapping. UPnP is closed by default, please ensure the UPnP™ status is set to off if it's not used.

NOTE: While UPnP™ adds convenience, it should not be used unless needed as it allows any device on your internal network to open ports on your router to communicate outbound to the Internet.

If you want to enable the UPnP™ function of the device, you must enable UPnP™ on the gateway router to which your device is connected. When the network working mode of the device is set as multi-address, the default route of the device should be in the same network segment as that of the LAN IP address of the router. You can refer to the User Manual for more detailed operation instructions.

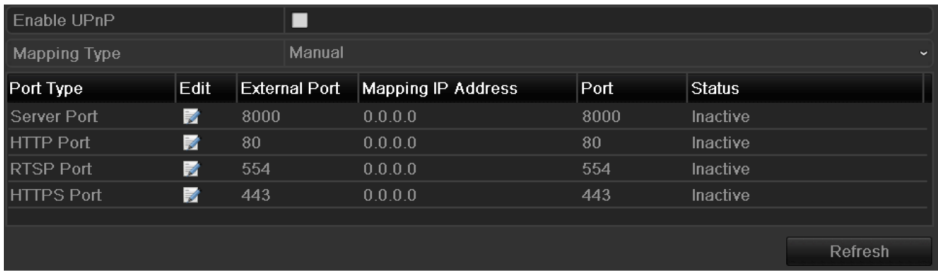

Fig. 2-8 UPnP

2.5.3 Port forwarding

Port forwarding can be configured when a device needs access to the Internet from behind a firewall. The following security best practices should be followed to reduce the risk of cyberattack against your Internet-facing device.

1. Minimize the number of ports that are accessible via the Internet. Configure port forwarding only when it is necessary. For example, forwarding port 443 when encrypted web services are needed.
2. Ensure that the all accounts are set with very strong passwords. This is extremely important when a device is 'Internet-facing'.
3. Avoid the use of general ports but use a custom port instead. For example, port 80 is generally used in HTTP. It's recommended to use a custom port for a specific service. The custom port shall follow TCP/IP port definition (1-65535).

2.5.4 Hik-Connect

HIK Cloud P2P provides the mobile phone application and the service platform page to access and manage your connected NVR, which enables you to gain convenient remote access to the surveillance system.

The Stream Encryption Function encrypts the video stream sent from NVR and the user needs to input a verification code for live view or playback.

Fig. 2-9 Hik-Connect

2.6 Video data protection

You can lock the recorded video files or set the HDD property to Read-only to protect the video files from being overwritten.

The video files can be backed up to various devices, such as USB devices (USB flash drives, USB HDDs, USB writers), SATA writer and e-SATA HDD. Please backup your video regularly if the HDD is full.

2.6.1 Locking/unlocking video files

Users can enter the "backup" interface, select the channel to be searched, and set the search conditions which include video type, file type, start and stop time, find the video files to be protected and lock or unlock them. The configuration interface is shown below. Please check the user manual for specific steps.

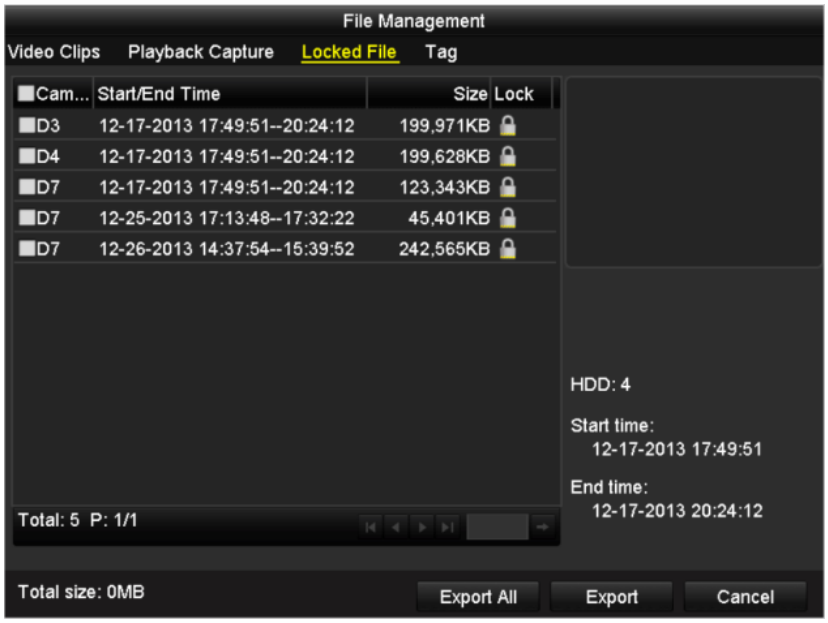

Fig. 2-10 Lock Files

2.6.2 HDD read-only

The HDD can be configured for redundancy, read-only or read/write (R/W). Before setting the HDD, please set the storage mode to Group (refer to step1-4 of Chapter Setting HDD Groups).

A HDD can be set to read-only to prevent important recorded files from being overwritten when the HDD becomes full in overwrite recording mode.

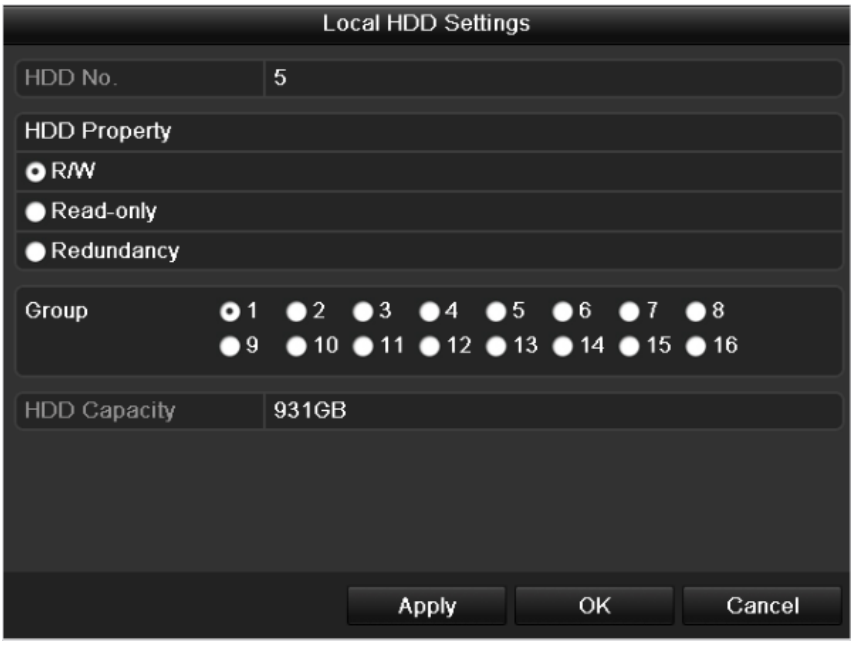

Fig. 2-11 HDD read-only Setting

2.6.3 Backup

The NVR supports file backups, event video backup, video clip backup, and image backup. Users should backup important data regularly. You can refer to the User Manual for more detailed operation guide.

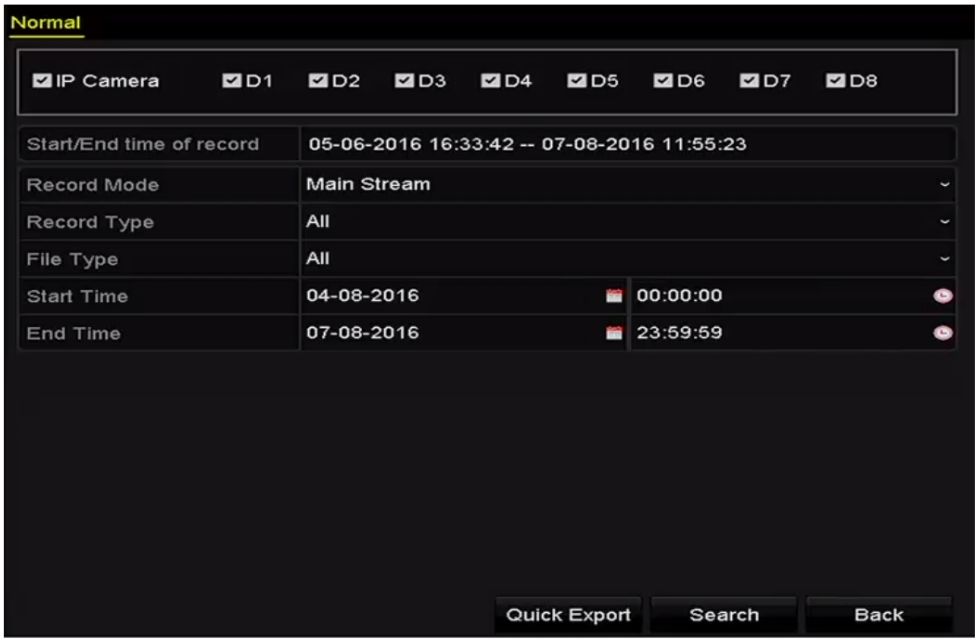

Fig. 2-12 Backup

2.7 Secure management

2.7.1 NTP

A Network Time Protocol (NTP) Server can be configured on your NVR to ensure the accuracy of system date/time. You can refer to User Manual for detailed operation instructions.

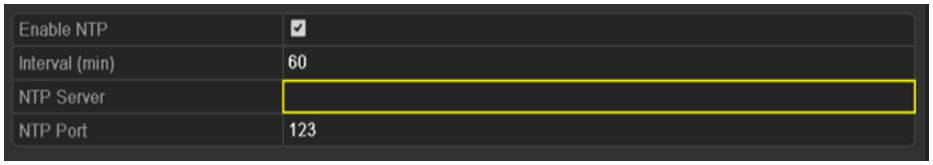

Fig. 2-13 NTP Setting

2.7.2 Exporting/importing configuration file

The configuration files of the NVR can be exported to a local device for backup and the configuration files of one NVR can be imported to multiple NVR devices if they are to

be configured with the same parameters. The NVR's device parameters will be encrypted by a custom encryption key that is created by the user during the export process. The same encryption key is required when the user imports the configuration file.

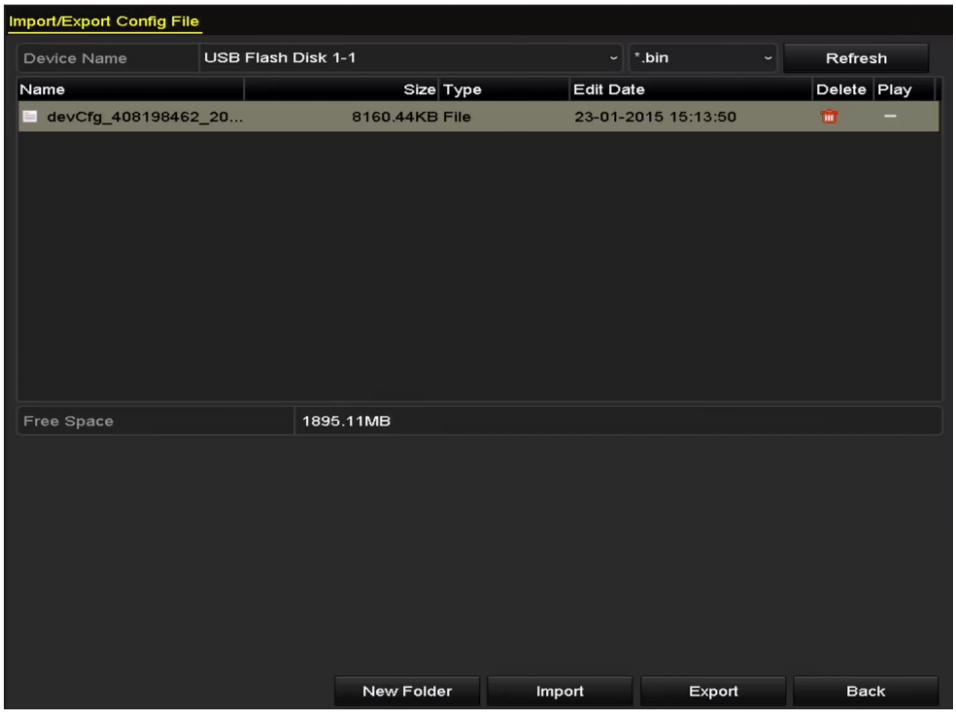

Fig. 2-14 Export Config File

2.7.3 Restoring default settings

If you are unsure of what changes have been made to the device configuration or if you believe that the device has been compromised, you can restore the device to the default settings.

There are three options for default setting:

- Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
- Factory Defaults: Restore all parameters to the factory default settings.
- Restore to Inactive: Restore the device to the inactive status.

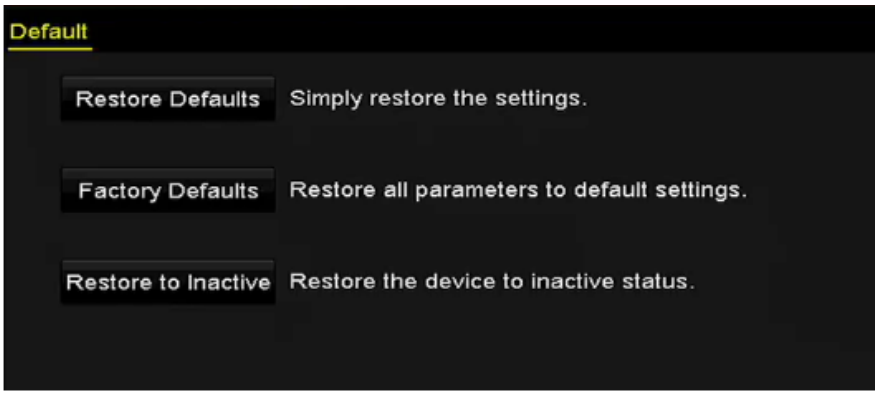

Fig. 2-15 Default

2.8 Upgrading firmware

We highly recommend that all Hikvision devices are regularly updated to the latest firmware to ensure a more stable and secure system.

The NVR supports two upgrade methods: local upgrade and remote upgrade.

The configuration interface is shown below. Please check the user manual for specific steps.

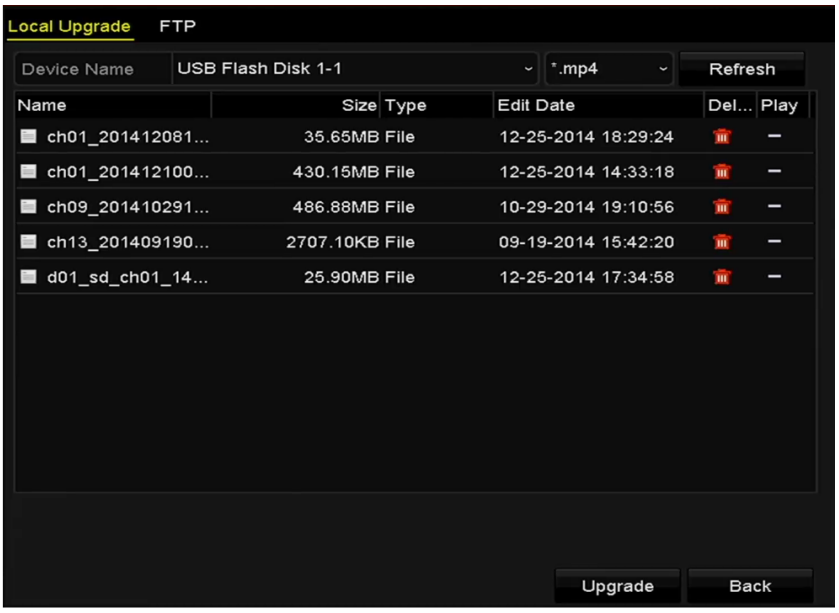

Fig. 2-16 Upgrade

2.9 Communication security

2.9.1 HTTPS

HTTPS provides encrypted authentication between a web client and the web server,

which protects against ‘packet sniffing’ and ‘man-in-the-middle; attacks. You can configure HTTPS remotely with the webpage or iVMS client.

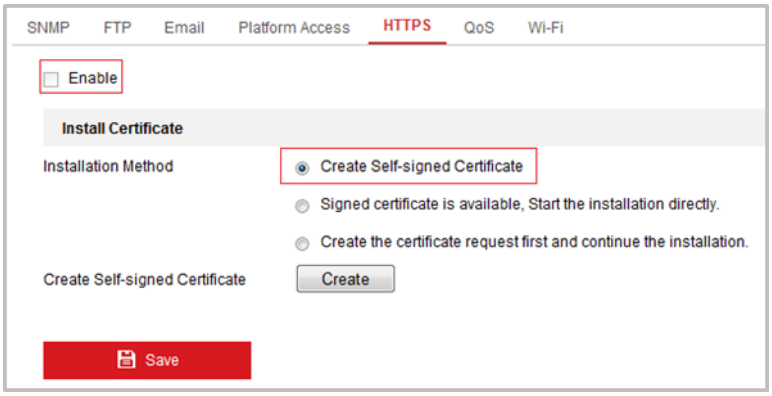

Fig. 2-17 HTTPS

Note：1. All self-signed certificates will initiate a pop-up like the one below, because they are not authorized by a certificate authority (CA), you can click “Continue to this website”.

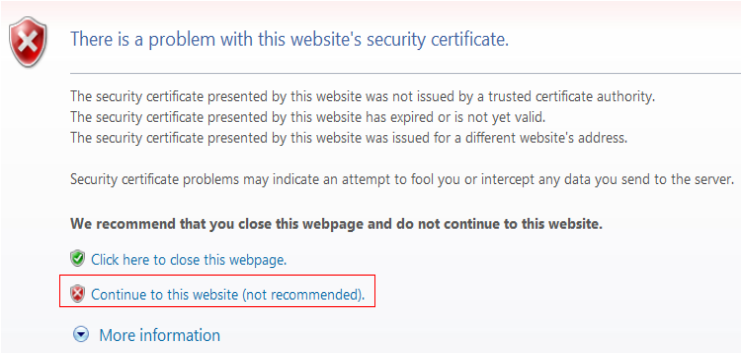

Fig. 2-18 Pop-up for unauthorized Certificate

2． We recommend the use of certificates issued by a certificate authority (CA) to improve the security level of access, and to eliminate the certificate warning that pops up when using a self-signed certificate.

2.10 Management security

Security management is one of the most important elements of product security. None of the technical cybersecurity settings and configurations can secure a system on their own if users are not following cybersecurity best practices. Below, are some general rules for security management:

(1) Develop product security related systems, processes, plans, operating instructions and forms. Document all processes and run table-top exercises or drills to practice what to do in an incident.

(2) Use security scanning tools, configuration verification, and penetration testing to evaluate the security of networks and devices, then identify potential security risks,

assess the risk and prepare a remediation plan.

(3) Compile the corresponding reinforcement proposal and operation guide, according to the results of the product security assessment. And then guide the reinforcement and keep track of the reinforcement effect.

(4) Monitor the security on all networks and devices, 24/7. This monitoring should include, but is not limited to, system and network availability, malware detection, and intrusion detection.

(5) Periodically initiate cybersecurity audits of your network and applications. Adjust the firewall of the video monitoring platform, server, and other network devices and host system security policy according to the results, to protect the security of products further.

(6) It can refer to the emergency response mechanism of the Internet industry, and combine its own emergency process to provide security emergency service for video surveillance system.

(7) Strengthen the security awareness and system security management training for different types of video surveillance staff.

(8) Product security setting should follows the basic principles of information system security: the principle of least privilege, the principle of decentralization and balance, the principle of security isolation, etc.

3. Conclusion

This security guide will be updated regularly to show you the best practices of latest network security.

Hikvision has been devoted to the research of network security for many years and will provide users with industry-leading cybersecurity technology.

You can view http://www.hikvision.com/cn/support_list_591.html to find more cybersecurity information. If you have any question on cybersecurity, please email to HSRC@hikvision.com.