

# Network Camera Security Guide

00

۲

۲

January 2018

www.hikvision.com

### About This Document

This Guide shows users how to configure a Hikvision IPC system with a high level of

cybersecurity protection.

### **User Manual**

COPYRIGHT ©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

#### ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

### **About this Manual**

This Manual is applicable to iVMS-4200 Client Software.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (<u>http://overseas.hikvision.com/en/</u>).

Please use this user manual under the guidance of professionals.

### **Trademarks Acknowledgement**

**HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

### **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 THE APPLICABLE LAW. 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.

3

# Contents

1Abstract	1
2Security Function Configurations	1
2.1 Identity Authorization	1
2.1.1 Create a strong password	1
2.1.2 Activate Camera by Setting a Strong Password	2
2.1.3 Illegal Login Lock	5
2.1.4 Reset password by Security Question	6
2.1.5 Authentication	7
2.2 Authorization Management	7
2.2.1 User Management	7
2.3 Log	9
2.4 Encryption	9
2.4.1 HTTPS	9
2.5 Port and Service Security	11
2.5.1 SNMP	11
2.5.2 Disable UPnP	12
2.5.3 Port Forwarding	13
2.5.4 QoS	13
2.5.5 Hik-Connect	14
2.6 Security Management	15
2.6.1 IP Address Filter	15
2.6.2 802.1x	16
2.6.3 Encryption of Device Parameters Exporting/Importing .	17
2.6.4 Default	17
2.6.5 Time Synchronization	18
2.7 Firmware upgrade	19
2.7.1 Check the latest firmware version	19
2.7.2 Upgrade Latest Firmware	20
2.8 Management Security	21
3 Conclusion	22

# **1** Abstract

Various types of security attacks in the Internet have become a severe threat for network devices and users' privacy. Hikvision network cameras 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 removing 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 Function Configurations

# 2.1 Identity Authorization

Account usernames and passwords are important data, used to identify and authenticate users. Default passwords and weak password pose a critical threat to user accounts and should not be used.

# 2.1.1 Create a strong password

How to set a strong password?

- A general strong password rule for Hikvision devices:
- (1) Valid password range [8-16].
- (2) You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

'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 original phrase;
- (4) Use number with higher priority than letter, 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 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 send your passwords to anyone in email.
- (4) Consider using a password manager so you don't have to remember the password.
- (5) Does not include anything in the dictionary and is not just using dictionary words with numbers replacing letters.

### 2.1.2 Activate Camera by Setting a Strong Password

Users are required to activate the camera first by setting a strong password for it before they can use the camera. We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product and to protect your privacy information or data.

Activation via web browser, SADP, and client software are all supported.

Note: The rules of password levels are:

Strong password: it uses at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.

Medium password: It is a combination of the following categories: numbers and symbols, lower case letters and symbols, upper case letters and symbols, lower case letters.

Weak password: It is a combination of number and lower case letters or numbers and upper case letters.

Risk password:

It is no longer than 8 characters.

It includes only one category of characters.

It is the same or the reverse of user name.

To protect your privacy and to increase the security of your product, we highly recommend you to use strong password.

### 2.1.2.1 Activation via SADP Software

SADP software is used for detecting the online device, activating the camera, and

resetting the password.

Get the SADP software from the disk included in the product package or from the official website, and install the SADP by following the prompts. Run the SADP software to search for devices on the LAN. The device status, such as device model, IP address, security status, and serial number, can be displayed in the software (Fig. 2-1).

	SADP										© _ □ ×
То	al num	ber of online devices: 9							Export	Refresh	Activate the Device
	ID	•   Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP	Port   Device S	erial No.	
	001	\$10-10200000 J	Active	10.16.6.20	8000	VL10bald 1006.	10.16.6.254	80	25.428	#3-3#125580#13CH	
	002	05-098305-A	Active	10.16.6.21	8000	VL10544 (008.	10.16.6.254	80	21.000	IS ADDRESSO	4
	003	25-429029-AI	Active	10.16.6.213	8000	V5.2.06689.0012-	10.16.6.254	N/A	01-4248	DR-ADDISALDONA	
	004	25-18488-6425	Active	10.16.6.179	8000	VL0306-M 100-	10.16.6.254	N/A	21-1010	>	The device is not activated
	005	DS-15808-018945	Active	10.16.6.127	8000	\$2,2 (build 1877).	10.16.6.254	N/A	25.256		The device is not activated.
	006	UNICHIN DEVICE TIME	Active	10.16.6.250	8000	VLADuAL 2012.	10.16.6.254	80	20.411	000000000000000000000000000000000000000	
-	•	007 🛛		2025790	14	Inacti	ve		192.16	8.1.64	
	009	D5-185085-046/K2DW	<sup>Acti</sup> Se	lect in	activ	ve devid	e.10.16.6.254	80	11.000	n er connect	You can modify the network parameters after the device activation. Activate Now
Input and confirm									New Password:		
	password.							Confirm Password: •••••••			
											Activate

Fig. 2-1 SADP software interface

Click to select the device to be activated. The status of the device is shown on the right side of the window. Enter the password in the password field and click **Activate** to start activation.

### 2.1.2.2 Activation via Client Software

Get the client software from the disk included in the product package or from the official website, and install the software by following the prompts. Run the client software to search for devices on the LAN in the **Device Management** interface. The device status, such as device model, IP address, Security status, serial number, can be displayed in the software.



<u>F</u> ile <u>S</u> ystem <u>V</u> iew <u>T</u> ool <u>H</u> elp			iVMS-4200		admin 💮 🕻	20 🛗 16:25:04 🔒	- = ×
📲 Control Panel 🔷 De	vice Management						
Server 🗃 Group							
Organization	Device for Manag	jement (0)					
Encoding Device	Add Device	Modify Delete	Remote C VCA Alloca	Activate	Refresh All	Filter	
Add New Device Type	Nickname 🔺	IP Devic	e Serial No.	S	ecurity	Net Status	HDD Statu
							+
	Online Device (3		Refresh Every 15s				
	4 Add to Clien	t 🛟 Add All 🛛	Iodify Netinfo Reset	Password	Activate	Filter	
	IP	Device Type	Firmware Version	Security   S	erver Port	Start time	AC
Encoding device:	10.16.1.222	XX-XXXXXXXX-XX	Vx.x.xbuild xxxxxx	Active 8	000	2015-03-20 10:13:47	NC
DVR/DVS/NVR/IPC/IPD/iVMS-4200 PCNVR/iVMS-4200 EncodeCard	192.0.0.64	XX-XXXXXX-XXX	Vx.x.xbuild xxxxxx	Active 80	000	2015-03-20 07:53:43	Nc +
Server	•					)	Þ
🔟 🤚 🖼 🍁 Motion Detection Ala	rm					,	

Fig. 2-2 Device Management

Select an inactive device and click the **Activate** button to pop up the Activation interface. Create a password and enter it into the password field, retype the password to confirm. Click the **OK** button to start the activation. When compelte, the security status for that device will be changed to **Active**.

	Activation ×
User Name:	admin
Password:	•••••
	Strong
	Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.
Confirm New Passwo	rd: ••••••
	Ok Cancel

Fig. 2-3 Activation via client software

### 2.1.2.3 Activation via Web Browser

Set the IP address of the PC and network camera to be on the same subnet. Enter the IP address of the network camera into the address bar of the web browser, and click **Enter** to enter the activation interface (Fig. 2-6).

A				
	Activation			User Name
				Password
	User Name	admin		
	Password	•••••	Strong	Login
		Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.		
	Confirm	•••••	]	
			OK	

Fig. 2-4 Activation via Web Browser

If there are two or more devices on the network, the IP addresses of devices should be configured to avoid IP address confliction.

# 2.1.3 Illegal Login Lock

It is used to limit the user login attempts. Login attempt from the IP address is rejected for 30 mins if admin user performs 7 failed user name/password attempts (5 times for the operator/user). Notifications are shown when the IP address is rejected by camera. The illegal login lock defends against brute-force password attacks. It's highly recommended that this feature is enabled. (Fig. 2-5).



HI	KVISION	Live View	Playback	Picture	Configuration	
Ç E	Local System System Settings Maintenance	Authentication	IP Address Filter gal Login Lock Save	Security Service		
¢ •	User Management Network Video/Audio Image Event Storage					

Fig. 2-5 Enable Illegal Login Lock

# 2.1.4 Reset password by Security Question

The security question is used to reset the admin password via client software or web browser.

The user can set a list of **Security Questions** in **User Management**.

		User Manag	ement Online Users					
8		User Li	st		Security Question	n Add Modify Delete		
		No.	User Name			Level		
	User Management			Security Qu	estion Configuration			x
θ								
Q.								
E					Security Question Co	onfiguration		
Ë					Security Question1	Your father's name.	[	•
٥					Answer			
					Security Question2	Your mother's name.		•
					Answer			-
					Security Question3	Your senior class teacher's name.		•
					Answer			
							ОК	Cancel

Fig. 2-6 Security Question

In the login interface, you may click **Forget Password** and answer all 3 security questions to reset the password.





Fig. 2-7 Forget Password

Note: 1. The PC used to reset password and the camera should be on the same IP address segment of the same LAN.

2. Only the administrator is able to reset a password.

### 2.1.5 Authentication

RTSP Authentication and WEB Authentication support "digest" and "digest/basic" authentication modes. If there are no compatibility requirements of "basic" authentication, it's recommended to select "digest" mode.

HIKVISION	Live View	Playback	Picture	Configuration
Local	Authentication	IP Address Filter	Security Service	
System	RTSP Authenti	cation digest		$\checkmark$
System Settings	WEB Authentic	ation digest		~
Maintenance				
Security		Save		
User Management				
Network				
Video/Audio				
🔝 Image				
Event				
🖺 Storage				

Fig. 2-8 Authentication Modes

# 2.2 Authorization Management

### 2.2.1 User Management

Three levels of users are supported: Administrator (admin), Operator, and User. The admin user can add, delete or modify user accounts, and grant them different permissions.



#### Enter the User Management interface: Configuration > System > User Management

HII	<b>KVISION</b>	Live View	Playback	Picture	Configuration	
Ţ	Local	User Managem	ent Online Users			
····	System	User List			Sec	curity Question Add Modify Delete
	System Settings	No.	User N	lame		Level
	Maintenance	1	adn	nin		Administrator
	Security					
	User Management					
G	Network					
<u>Q.</u>	Video/Audio					
1	Image					
圁	Event					
B	Storage					

#### Fig. 2-9 User Management

The interface for adding a user account is shown in Fig. 2-12. The Administrator is able to check or uncheck the permissions for the new user.

Add user		×
User Name		
Level	Operator 🗸	
Admin Password		
Password		
	Valid password range [8-16]. You can use a combination of numbers,	
	lowercase, uppercase and special character for your password with at	
	least two kinds of them contained.	
Confirm		
Select All		
Remote: Parameters S	Settings	
Remote: Log Search /	Interrogate Wor	
Remote: Upgrade / Fo	rmat	
Remote: Two-way Aud	dio	
Remote: Shutdown / R	Reboot	
Remote: Notify Surveil	llance Center /	
Remote: Video Output	Control	
Remote: Serial Port C	ontrol	
Remote: Live View		
Remote: Manual Reco	nd	
Remote: PTZ Control	~	
Remote: Playback		
	OK Cancel	

Fig. 2-10 Adding a user account

# 2.3 Log

The log files are stored on an SD card. Log information includes number, Time, Major Type, Minor Type, channel number, Local/Remote User and Remote Host IP. Users can set query various search parameters, including the Major Type, Minor Type, Start Time and End Time. The log files can be exported in text format or Excel format. 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. 2-11 Log

# 2.4 Encryption

# 2.4.1 HTTPS

HTTPS is a transmission encryption protocol based on SSL/TLS and HTTP. It improves the security of WEB access. If a certificate is already installed, the detailed information of the certificate will be shown. Check "Enable" to enable HTTPS (Fig. 2-14).

SNMP	FTP	Email	Platfor	m Access	HTTPS	QoS	Wi-Fi			
🗌 En	able									
Inst	all Certifi	icate								
Install	Installation Method				Create Self-signed Certificate     Signed certificate is available, Start the installation directly.					
Create	Self-sigr	ned Certific	ate	<ul> <li>Create</li> <li>Create</li> </ul>	the certifica	te reques	t first and continue the installation.			
	<b>B</b> :	Save								

Fig. 2-12 Enable HTTPS

Three installation methods are available, "Create Self-signed Certificate", "Signed Certificate is available, Start the installation directly" and "Create the Certificate request first and continue the installation".

Create Self-signed Certificate: Select "Create Self-signed Certificate" as the Installation Method and click the "Create" button to enter the certificate creation interface. Enter the country, host name/IP, validity and other information. Click "OK" to save the settings.

Install a Signed Certificate: Select "Signed Certificate is available", Start the installation directly as the Installation Method and click "Browse" to select a signed certificate. Click "Install" and click "Save".

Create the authorized certificate: Select "Create the certificate request first and continue the installation" as the Installation Method. Click "Create" button to create the certificate request. Fill in the required information in the popup window. Download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed valid certificate, import the certificate to the device.

Once a certificate is installed you will see the certificate information as shown in (Fig.2-15).

Certificate Details		
Installed Certificate	C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IF	Delete
Property	Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=192.168.1.64, EM=com.cn Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=192.168.1.64, EM=com.cn Validity: 2016-11-10 11:20:11 ~ 2019-11-10 11:20:11	<

Fig. 2-13 Installed Certificate

Note:

1. The security notification (Fig. 2-16) will be shown in browser when a user accesses the device via HTTPS with a self-signed certificate installed. This is because the

certificate is not issued by a trusted CA.

8	There is a problem with this website's security certificate.
	The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website has expired or is not yet valid.
	The security certificate presented by this website was issued for a different website's address.
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
	We recommend that you close this webpage and do not continue to this website.
	Click here to close this webpage.
[	Continue to this website (not recommended).

Fig. 2-14 Security Notification of Self-signed Certificate

2. It's recommended to install certificates issued by Certification authority (CA) to improve the security of web access. Generally a CA charges for issuing a digital certificate.

# 2.5 Port and Service Security

Only necessary services and ports are enabled by default to minimize the possibility of attacks and reduce security risks. The supported services and protocols, such as ONVIF, CGI, UPnP, QoS, Multicast, Platform Access, SNMP are disabled by default. Users should only enable the required services and protocols that are necessary to their environment.

# 2.5.1 SNMP

The device supports SNMP v1, SNMP v2 and SNMP. You can set the SNMP function to get camera status, parameters and alarm related information, and manage the camera remotely when it is connected to the network. If SNMP is not required, please disable it. SNMP v3 is highly recommended to replace SNMP v1 or SNMP v2.



	ни	VISION	Live View		Playba	ack Pict	ure	Config	juration	
	₽	Local	SNMP	FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
	<b>—</b>	System	SNI	/IP v1/v2						
	Ð	Network	🗆 En:	able SNN	1P∨1					
		Basic Settings	🖂 En	able SNN	1P v2c					
		Advanced Settings	Read S	SNMP Co	mmunity	public				
1	<u>Q.</u>	Video/Audio	Write S	NMP Co	mmunity	private				
	1	Image	Trap A	ddress						
	圁	Event	Trap P	ort		162				
	B	Storage	Trap C	ommunit	y	public				
			SNI	/IP v3						
			En:	able SNN	1Pv3					
			Read U	JserNam	8					
			Securit	y Level		no auth, no priv		$\sim$		
			Authen	tication A	Algorithm	MD5 SHA				
			Authen	tication F	assword	•••••				
			Private	-key Algo	prithm	DES AES				
			Private	-key pas	sword	•••••				
			Write U	JserNam	Ð					
			Securit	y Level		no auth, no priv		$\checkmark$		
			Authen	tication A	Algorithm	MD5 SHA				
			Authen	tication F	assword	•••••				
			Private	-key Algo	prithm	DES AES				
			Private	-key pas	sword	•••••				
			SNM	IP Other	Settings					
			SNMP	Port		161				
						_				
				- 🗎 S	Save					

Fig. 2-15 SNMP Configuration

# 2.5.2 Disable UPnP

Universal Plug and Play (UPnP<sup>™</sup>) is a networking protocol that provides compatibility between networking equipment, software and hardware devices. UPnP<sup>™</sup> is disabled by default. If the device is not connected to hosted video services, UPnP<sup>™</sup> should not be enabled.



# 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 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 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 QoS

QoS (Quality of Service) is a mechanism that prioritizes network traffic for specified applications. It can help solve the network delay and network congestion by configuring the priority of data transmissions. Generally, QoS is not needed in non-time-based application system. If QoS is not supported by network infrastructure, set "Video/Audio DSCP", "Event/Alar DSCP" and "Management DSCP" to "0".



HIKVISION	Live View	Playback	Picture	Configuration	
🖵 Local	SNMP FT	P Email Platf	orm Access HTTPS	QoS 802.1x	Integration Protocol
System	Video/Audio	DSCP 0			
Network	Event/Alarm	DSCP 0			
Basic Settings	Managemen	t DSCP 0			
Advanced Setting	s				
Video/Audio	E	Save			
Image					
Event					
Storage					



### 2.5.5 Hik-Connect

Platform access provides you an option to manage devices via the Hik-Connect platform. If access to Hik-Connect is not needed, please disable it.

HIKVISION	Live View	Playba	ack Pictu	ire	Configu	ration	
Local	SNMP FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
System	Enable						
Network	Platform Acces	s Mode	Hik-Connect		~		
Basic Settings	Server IP		dev.hik-connect.co	om	[	Custom	
Advanced Settings	Register Status	3	Offline		$\checkmark$		
Q. Video/Audio	Verification Co	de					
Image			6 to 12 letters (a to z numbers (0 to 9), cas are recommended to	:, A to Z) or se sensitive o use a	e. You		
Event			combination of no les or numbers.	ss than 8 le	etters		
Storage			Create a verificat	tion code.			
		Save					

Fig. 2-18 Disable Hik-Connect

When a user enables platform access and selects Hik-Connect mode, they will create a verification code or change the verification code for the camera. The verification code should be more than 8 (preferably more than 12) characters composed of upper case letters, lower case letters numbers and special characters.

	W Enable				
Network	Platform Access Mode	Hik-Connect			
	Server IP		Custom		
Advanced Settings	Register Status				
	Venfication Code		Note		×
		6 to 12 vetters (a to 2. A to 2) numbers (0 to 9), case sense are recommended to use a combination of no less than 8 or trumbers.	To enable Hik-Connect s verification code.	ervice, you need to create a verification	code or change the
Storage	📑 Save	C Create a vertication code	Verification Code	6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.	
			Confirm Verification Code		
			The Hik-Connect service Service" and "Privacy Pc	will require internet access. Please rea bicy" before enabling the service.	d the " <u>Terms of</u> K Cancel

Fig. 2-19 Create verification code for Hik-Connect

# 2.6 Security Management

# 2.6.1 IP Address Filter

The IP Address Filter prevents unauthorized clients from accessing a device. Click the **Enable IP Address Filter** checkbox to activate this feature.

Select the type of IP Address Filter in the drop-down list, Forbidden or Allowed

- Allowed mode indicates that only IP addresses in IP Address Filter List are able to access the device. The maximum number of IP addresses that can be added to this list, is 48.
- Forbidden mode indicates that all IP addresses on the IP Address Filter List are forbidden to access the device. The maximum number of IP addresses that can be added to this list, is 48.



HI	KVISION	Live View	Playback	Picture	Configuration		
Ţ	Local	Authentication	IP Address Filter	Security Service			
	System System Settings	IP Address F	Iter Type Forbidd	len	~	_	
	Maintenance	IP Addres	s Filter				Add Modify Delete
	User Management	No.	IP				
Ð	Network						
Q.	Video/Audio						
1	Image						
Ë	Event						
8	Storage						
		E	Save				

Fig. 2-20 IP Address Filter

### 2.6.2 802.1x

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X. A user can configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

HI	<b>KVISION</b>	Live View	Playba	ck Pict	ture	Config	juration	
Ţ	Local	SNMP FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
	System	Enable IE	EE 802.1X	EAD MOS				
Ð	Network	Protocol		EAP-MD5		<b>~</b>		
	Basic Settings	EAPOL version	n	1		~		
	Advanced Settings	User Name						
<u>Q.</u>	Video/Audio	Password						
<u>**</u>	Image	Confirm						
圁	Event			_				
5	Storage		Save					

Fig. 2-21 802.1x Configuration

# 2.6.3 Encryption of Device Parameters Exporting/Importing

Device parameters can be exported by entering a password that is created by a user while exporting the device parameters file. The file doesn't include admin password information. A user needs to enter the password of the device parameters file while importing the file into a device.

Q ues	lippide & Mantenance	Lig Type Deals		
E total	Report			
Autom Settings	Refare 1	Subset To David		
Manifesterory	Output:			
and the second sec	Persona a l	Repet all the parameters, socied the 17 par	randers and user effectively. In the Soluri sellings,	
(3 hours	Detail	Renter al parameters to setal technol.		
Co sometade	Information Export			
Gi zwa	Device Parameters		File Encryption Configuration	×
E feet	Depune Homa	Doested the log, system information and		
D more	Inport Canfig. File		Inc. I the providing opposite (1 to 16 characters)	
	Caulos Paconesin			
	200.0		Confirm	
	Upprate			
	Formane in			
	Dates Note: The upgrading as	ocean will be 1 to 10 minutes, prese don't	OK Carce	A

Fig. 2-22 Exporting Device Parameters

It's recommended to set a strong password for the file and keep the file safely.

# 2.6.4 Default

If you are unsure about the configurations of a device, you can restore the device to make it recover to a known state.

There are two ways of restoring the device, **Restore** and **Default**.

- Restore: Reset all the parameters, except the IP parameters and user information, to the default settings.
- > **Default**: Restore all the parameters to the factory default.

Enter the Maintenance interface: **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**. (Fig. 2-27)



<b>HIKVISION</b>	Live View Playback Picture Configuration
🖵 Local	Upgrade & Maintenance Log System Service
System	Reboot
System Settings	Reboot Reboot the device.
Maintenance	Default
Security User Management	Restore Reset all the parameters, except the IP parameters and user information, to the default settings.
Network	Default Restore all parameters to default settings.
Video/Audio	Information Export
🖬 Image	Device Parameters
Event	Diagnose Informa Download the log, system information and hardware information.
Storage	Import Config. File
	Device Parameters Browse Import
	Status
	Upgrade
	Firmware V Browse Upgrade
	Status
	Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

Fig. 2-23 Default

# 2.6.5 Time Synchronization

Time zone configuration and two time synchronization methods are supported.

- 1) Manual Time Sync. or Sync. with computer time.
- 2) Time synchronization with NTP server. NTP server address, port and interval can be configured.



HIKVISION	Live View Playt	oack Picture	Configuration
🖵 Local	Basic Information Time	e Settings DST RS-232	About
System	Time Zone	(GMT+08:00) Beijing, Uru	mqi, Singapore 🗸
System Settings	NTP		
Maintenance			
Security	Server Address	time.windows.com	
User Management	NTP Port	123	
Network	Interval	1440	minute(s)
Video/Audio		Test	
🔝 Image	Manual Time Sync.		
Event	Manual Time Sync.		
Storage	Device Time	2017-11-03T13:51:27	
	Set Time	2017-11-03T13:51:20	Sync. with computer time
	🖹 Save		

Fig. 2-24 Time Settings

# 2.7 Firmware upgrade

It is highly recommended that users regularly upgrade to the latest firmware to ensure security updates and bug fixes are installed.

# 2.7.1 Check the latest firmware version

Enter the System Settings interface to check the firmware version information: **Configuration > System > System Settings > Basic Information**. (Fig. 2-29)



HIKV	<i>(ISION</i> I	ive View	Playback	Picture	Configuration
Дю	cal _	Basic Information	Time Settings	DST RS-2	32
🛅 Sy	stem	Device Name	IP CA	MERA	
Sy	stem Settings	Device No.	88		
Ma	intenance	Model	DS-20	D2085FWD-I	
Se	curity	Serial No.	DS-20	D2085FWD-I201	61109AAWR676584421
Us	er Management	Firmware Version	V5.4.4	build 161013	
🚱 Ne	etwork	Encoding Version	V7.3 b	ouild 161013	
<u>Q</u> . ∨io	deo/Audio	Web Version	V4.0.1	build 161013	
in Im	age	Plugin Version	V3.0.6	5.10	
l凹 Ev	rent	Number of Chann	els 1		
E St	orage	Number of HDDs	0		
		Number of Alarm	Input 0		
		Number of Alarm	Output 0		
		Number of Addition	output		

Fig. 2-25 Firmware Version

### 2.7.2 Upgrade Latest Firmware

The steps to upgrade firmware are:

- 1) Download the firmware to a computer on the same network as the camera.
- 2) Log into the camera's management interface from the computer with the firmware file and select **firmware** or **firmware directory** to locate the upgrade file.
- 3) Click **Upgrade** to start the upgrade. If Firmware Directory is selected, the correct firmware in the directory is recognized automatically to start upgrading.

Note: The upgrading process will take 1 to 10 minutes. Please do not disconnect power to the camera during this process. The camera reboots automatically after the upgrade.



HII	<b>KVISION</b>	Live View Playb	ack	Picture	Configuration		
Ţ	Local	Upgrade & Maintenance	Log	System Service			
	System	Reboot					
	System Settings	Reboot	Reboot the device.				
	Maintenance	Default					
	Security	Delduit					
	User Management	Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.				
Ð	Network	Default	Resto	re all parameters to defa	ult settings.		
.Q.	Video/Audio	Export					
1	Image	Device Parameters					
₿	Event	Import Config. File					
8	Storage	Device Parameters				Browse	Import
		Status					
		Upgrade					
		Firmware V				Browse	Upgrade
		Status					

Fig. 2-26 Firmware Upgrade

### 2.8 Management Security

Security management is one of the most important elements of product security. All of the technical cybersecurity settings and configurations can't secure a system 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 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 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 have been devoted to the research of network security for many years and will provide users with industry-leading cybersecurity technology.

You can view <u>http://www.hikvision.com/cn/support\_list\_591.html</u> to find more cybersecurity information. If you have any question on cybersecurity, please email to <u>HSRC@hikvision.com</u>.