

Network Camera Security Guide

0

January 2018

www.hikvision.com

About This Document

This Guide includes instructions for using and managing the product safely.

User Manual

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

ALL RIGHTS RESERVED.

Any and all information, including, amongst others, wording, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to as "Hikvision"). This user manual (hereinafter referred to as "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 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.

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	1
2.	Security Function Configurations	1
	2.1 Identity Authorization	1
	2.1.1 Creating a strong password	1
	2.1.2 Activating a Camera by Setting a Strong Password	2
	2.1.3 Illegal Login Lock	5
	2.1.4 Resetting 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 Checking the latest firmware version	19
	2.7.2 Upgrading to the Latest Firmware	20
	2.8 Management Security	21
3.	Conclusion	22

1 Abstract

Various types of security attacks on 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 these threats 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 needs.

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 passwords pose a critical threat to user accounts and should not be used.

2.1.1 Creating a strong password

How to set a strong password?

- A general strong password rule for Hikvision devices:
- (1) Valid character range [8-16].
- (2) You can use a combination of numbers, lowercase, uppercase and special character 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 original phrase;
- (4) Use numbers rather 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 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.
- (5) Does not include anything in the dictionary and is not just using dictionary words with numbers replacing letters.

2.1.2 Activating a 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 and upper 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.

Run the SADP software from the disk included with product 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										0 _ D >
Total numbe	r of online devices: 9							Export	Refresh	Activate the Device
I ID	• Device Type	Security	IPv4 Address	Port	Software Version I	Pv4 Gateway	HTTP Po	nt Device Ser	ial No.	
001	\$10-1020000 J	Active	10.16.6.20	8000	VL10649 (005 1	10.16.6.254	80	25.4080	0.012253461204	
002	05-698305-A	Active	10.16.6.21	8000	VL106491008	10.16.6.254	80	21,000	ALCOUNTRY OF	4
003	DS-K2802N-AI	Active	10.16.6.213	8000	V52386810102-	10.16.6.254	N/A	01-42402	ADDALOTY	
004	D5-18408-6425	Active	10.16.6.179	8000	VL038-04 180-	10.16.6.254	N/A	21 1000	>	The device is not activated.
005	DS-18408-CLEWS	Active	10.16.6.127	8000	\$228wid 1871.	10.16.6.254	N/A	25.256		The device is not activated.
006	UNICHINE DEVICE THE	Active	10.16.6.250	B000	VLADurit 2002.	10.16.6.254	80	204110	Cultar01400718	
~	007		2025PW0	4	Inactive	е		192.168	3.1.64	
009	Di-LINDBN-DH/K2DW	^{Acti} Se	lect in	activ	ve device	0.16.6.254	80	11-1010	5.045.420004200	You can modify the network parameters after the device activation. Activate Now
						-			nfirm	New Password:
					F	oass	woi	rd.		Confirm Password: Enable Hik-Connect
										Activate
4									*	

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 the process.

2.1.2.2 Activation via Client Software

Run the client software from the disk included with product 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.



ie <u>S</u> ystem ⊻iew <u>T</u> ool <u>H</u> elp			💩 iVMS-4200		admin 🕁	16:25:04	,
🔡 Control Panel 🖉 De	vice Management						
Server 🗃 Group							
Organization	Device for Manag	gement (0)					
Encoding Device	Add Device	Modify D	elete Remote C VC	A Alloca Activate	Refresh All	Filter	
Add New Device Type	Nickname 🔺	IP	Device Serial No.		Security	Net Status	HDD Statu
	Online Device (3))	Refresh Every 1	55			•
			Refresh Every 1	5s Reset Password	Activate	Filter	•
	Online Device (3)	t 🕹 Add All	Modify Netinfo	Reset Password	Server Port	Start time	, Ac
	Online Device (3) Add to Clien IP 192.168.1.64	t Add All Device Type	Modify Netinfo Firmware Version XX Vx.x.xbuild xxxxx	Reset Password Security (x Inactive	Server Port	Start time 2015-03-20 16:13:4	7 NC
Encoding device: DVR/DVS/NVS/FC/IPD/VMS-4200 PC/VNF/WVB-4200 EncodeCard	Online Device (3)	t 🕹 Add All	Modify Netinfo Firmware Version XX Vx.x.xbuild xxxxx Vx.x.xbuild xxxxx	Reset Password Isecurity Inactive xx Active	Server Port	Start time	7 Nc 1 Nc

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 complete, 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 Passwor	d: ••••••
	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).

	Activation			User Name
				Password
A And	User Name	admin		
	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.] 🕑 • Strong	Login
	Confirm	•••••	ОК	

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

The illegal login lock is used to limit the number of user login attempts. Login attempts from the IP address are rejected for 30 mins if the 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 the 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	
Q E	Local System System Settings Maintenance		IP Address Filter gal Login Lock Save	Security Service		
	Security User Management		Care			
© <u>0</u> :	Network Video/Audio					
	Image Event Storage					
		Fig. 2-5 Enab	le Illegal Login L	lock		

2.1.4 Resetting password by Security Question

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

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

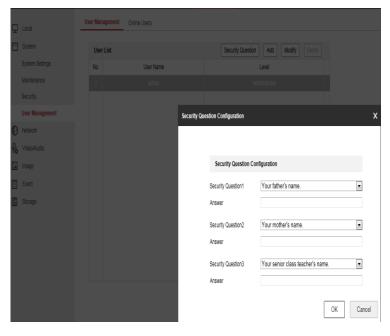


Fig. 2-6 Security Question

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 the 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 that you select "digest" mode.

НІК	VISION	Live View	Playback	Picture	Configuration
Ωı	Local	Authentication	IP Address Filter	Security Service	
— (System	RTSP Authentic	ation digest		~
S	System Settings	WEB Authentica	tion digest		~
N	Maintenance				
S	Security	🗎 S	ave		
L	User Management				
© 1	Network				
<u>Q</u> . \	Video/Audio				
1	Image				
Ē 6	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	VISION	Live View	Playback	Picture	Configuration	
Ţ	Local	User Manageme	online Users			
	System	User List			Secu	rity Question Add Modify Delete
	System Settings	No.	User N	lame		Level
	Maintenance	1	adm	iin		Administrator
	Security					
	User Management					
Ð	Network					
Q.	Video/Audio					
1	Image					
圁	Event					
	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 a 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.

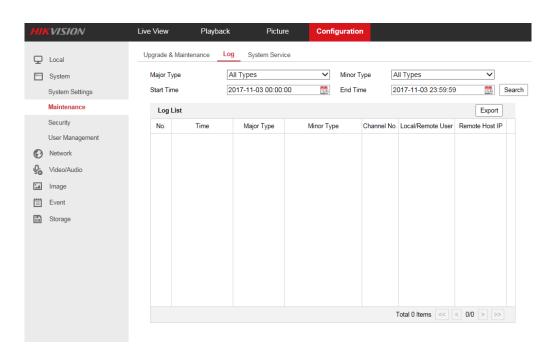


Fig. 2-11 Log

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	ation Meth	hod		Oreate	Self-signed	l Certificat	te
				Signed	l certificate i	s availabl	e, Start the installation directly.
				Oreate	the certifica	te reques	t first and continue the installation.
Create	Self-sigr	ned Certific	ate	Create			
	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" then click "Save".

Create the authorized certificate: Select "Create the certificate request first and continue the installation" as the Installation Method. Click the "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/IP=1	Delete
Property	<pre>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</pre>	^ ~	

Fig. 2-13 Installed Certificate

Note:

1. The security notification (Fig. 2-16) will be shown in the 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 certificate authority (CA).

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 vet 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 dose this webpage.
Solution Continue to this website (not recommended).

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

2. It's recommended you install certificates issued by a 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, and 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 retrieve the camera status, parameters and alarm related information, and manage the camera remotely when it is connected to the network. SNMP is disabled by default. If SNMP is not required, it should not be enabled. SNMP v3 is highly recommended to replace SNMP v1 or SNMP v2.



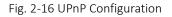
	IKVISION	Live View		Playba	ick Pict	ure	Config	juration	
ç	2 Local	SNMP	FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
E	System	SNN	/IP v1/v2						
¢	Network		able SNN						
	Basic Settings		able SNN						
	Advanced Settings	Read S	SNMP Co	mmunity	public				
Q	Video/Audio	Write S	NMP Co	mmunity	private				
4	Image	Trap A	ddress						
Ċ	Event	Trap P	ort		162				
	Storage	Trap C	ommunit	у	public				
		SNM	/IP v3						
		🗀 Ena	able SNN	1Pv3					
		Read L	JserNam	e					
		Securit	y Level		no auth, no priv		\sim		
		Authen	tication A	Algorithm	MD5 SHA				
		Authen	tication F	Password	•••••				
		Private	-key Algo	orithm	DES AES				
		Private	-key pas	sword	•••••				
		Write U	JserNam	е					
		Securit	y Level		no auth, no priv		\sim		
		Authen	itication A	Algorithm	MD5 SHA				
				Password	•••••				
			-key Algo		DES AES				
		Private	-key pas	sword	•••••				
		SNM	IP Other	Settings					
		SNMP	Port		161				
			8	Save					

Fig. 2-15 SNMP Configuration

2.5.2 Disable UPnP[™]

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

HIKVISIO N	Live View F	'layback Pio	ture Configuration	on	
Local	TCP/IP DDNS	PPPoE Port NA	T		
System	Friendly Name	HIKVISION DS-	2CD2755FWD-IZ		
Basic Settings	Port Mapping M	ode Auto	\checkmark		
Advanced Settings	Port Type	External Port	External IP Address	Internal Port	Status
Uideo/Audio	HTTP	80	0.0.0.0	80	Not Valid
Image	RTSP	554	0.0.0.0	554	Not Valid
Event	Server Port	8000	0.0.0.0	8000	Not Valid
Storage					
	🗎 Save				



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 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 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 a non-time-based application system. If QoS is not supported by the network infrastructure, set "Video/Audio DSCP", "Event/Alar DSCP" and "Management DSCP" to "0".



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

Fig. 2-17 QoS Configuration

2.5.5 Hik-Connect

Platform access provides you an option to manage devices via the Hik-Connect platform. Hik-Connect is disabled by default. If access to Hik-Connect is not needed, it should not be enabled.

HIKVISIO N	Live View	Playba	ack Pictu	re	Configu	uration	
🖵 Local	SNMP FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
🗂 System	🗌 Enable						
Network	Platform Acces	s Mode	Hik-Connect		\checkmark		
Basic Settings	Server IP		dev.hik-connect.co	om		Custom	
Advanced Settings	Register Status	6	Offline		\sim		
Uideo/Audio	Verification Co	de					
Image			6 to 12 letters (a to z numbers (0 to 9), cas are recommended to	se sensitiv	e. You		
Event			combination of no less or numbers.		etters		
Storage			Create a verificat	tion code.			
	8	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.

] Local] System	V Enable				
	Platform Access Mode	Hik-Connect			
	Server IP		Custom		
Advanced Settings	Register Status				
	Verification Code		Note		×
			To enable Hik-Connect s verification code.	ervice, you need to create a verification code	e or change the
Storage			Verification Code		
	🖹 Sale			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		
				will require internet access. Please read the <u>blics</u> before enabling the service.	"Terms of Cancel

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

By default, during transmission, the video stream is encrypted.

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 on the 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.



HIKVISIO N	Live View	Playback	Picture	Configuration	
Local		P Address Filter	Security Service		
System Settings Maintenance		Filter Type Forbidd	len	~	Add Modify Delete
Security User Managem Network Image Image Event Storage	nt No.	IP IP Save			Add Modify Delete

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.

HIK	VISION	Live View F		Playba	ck Pic	Picture C		guration	
-	ocal	SNMP	FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol
_	iystem letwork	Protoc	ol		EAP-MD5		~		
1	asic Settings		_ version		1		~		
A	dvanced Settings	User N	lame						
<u>Q.</u> V	ídeo/Audio	Passw							
🔝 In	nage	Confirm	n						
ËE	vent	_			_				
🖺 S	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 tara	Vogiste & Bantineror	Log Types Deals		
E total	Report.			
System Settings	Rature	Report To Hold B		
Mannance Decide	Celset			
Constant of the second se	Pendore	Result all the parameters, succed the IP ap	ramiters and user efformation, to the Sofield Indirest	
6 mm	Detail	Terror al parameters to setail settings.		
Pa sometate	Information Export			
GT THE	Deve a Paranymen		File Encryption Configuration	×
📋 Fort	Depuse interna	Downoad the tog, spream information and		
Di mene	Physic Config. File		Input the encryption password.(1 to 16 characters)	
	Device Pacameters			
	Side .		Contres	
	Uppraite			
	Firman (a)			
	Table Note: The upgrading pr	ocesa will be 1 to 10 minutes, prese don't	OK Cancel	

Fig. 2-22 Exporting Device Parameters

It's recommended to set a strong password for the file and store 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)



HIKVISION	Live View Playback Picture Configuration
🖵 Local	Upgrade & Maintenance Log System Service
System System	Reboot
Maintenance	Reboot Reboot the device.
Security User Management	Restore Reset all the parameters, except the IP parameters and user information, to the default settings. Default Restore all parameters to default settings.
Video/Audio	Information Export
Image	Device Parameters Diagnose Informa Download the log, system information and hardware information.
Storage	Import Config. File Device Parameters Browse Import
	Status
	Upgrade Firmware 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 Pla	yback Picture	Configuration
🖵 Local	Basic Information Tir	ne Settings DST R	IS-232 About
System	Time Zone	(GMT+08:00) Beijin	g, Urumqi, 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	2017-11-03T13:51:2	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 Checking the latest firmware version

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



HIKVISION	Live View	Playback	Picture	Configuration
Local	Basic Inform	nation Time Settings	DST RS-232	
System	Device Na	IP CAM	ERA	
System Sett	ings Device No	. 88		
Maintenance	Model	DS-2CE)2085FWD-I	
Security	Serial No.	DS-2CE	2085FWD-I20161	109AAWR676584421
User Manage	ement Firmware	Version V5.4.4 k	ouild 161013	
Network	Encoding	Version V7.3 bu	ild 161013	
Video/Audio	Web Vers	V4.0.1 I	ouild 161013	
Image	Plugin Ver	v3.0.6.*	10	
📋 Event	Number o	f Channels 1		
Storage	Number o	f HDDs 0		
	Number o	f Alarm Input 0		
	Number o	f Alarm Output 0		

Fig. 2-25 Firmware Version

2.7.2 Upgrading to the Latest Firmware

The steps to upgrade to the latest 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 the Firmware Directory is selected, the correct firmware in the directory is recognized automatically to start upgrading.

Note: The upgrade 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.



н	KVISION	Live View Playb	ack	Picture	Configuration		
Ţ	Local	Upgrade & Maintenance	Log	System Service			
	System	Reboot					
	System Settings	Reboot	Reboo	ot the device.			
	Maintenance	Default					
	Security	Restore	Reset	all the parameters exce	pt the IP parameters and us	ser information to the de	fault settings
	User Management	Default		re all parameters to defa			aut settings.
Ð	Network	Delaut	110310	re all parameters to dela	uit oottingo.		
<u>Q.</u>	Video/Audio	Export					
1	Image	Device Parameters					
Ë	Event	Import Config. File					
B	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. 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 settings 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 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>.