

Product Security Hardening Guide

V2.0.0

DAHUA TECHNOLOGY CO., LTD.



Legal Statement

Copyright Statement

© 2017 Zhejiang Dahua Technology Co., Ltd. All rights reserved. Without the prior written permission of Zhejiang Dahua Technology Co., Ltd. (hereinafter referred to as Dahua), no one can copy, transmit, distribute or store any content of this document in any form. Products described in this document may contain software copyrighted by Dahua or some other third person. Unless approved by the related obligee, no one can copy, distribute, modify, extract, decompile, disassemble, decode, reverse engineer, lease, transfer or sub-license the above-mentioned software in any form which may lead to property infringement.

Trademark Statement

alhua alhua alhua HDCVI are trademarks or

registered trademarks owned by Zhejiang Dahua Technology Co., Ltd.

- HDMI logo, HDMI and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC. This product has been authorized by HDMI Licensing LLC to use HDMI technology.
- VGA is the trademark of IBM.
- Windows logo and Windows are trademarks or registered trademarks of Microsoft.
- Other trademarks and company names mentioned are the properties of their respective owners.

Disclaimer

- Within the scope allowed by applicable laws, in any case, this company won't compensate any special, contingent, indirect and secondary damages resulting from relevant contents and products described in this document, nor compensate any losses in profits, data, reputation, document loss or expected savings.
- Products described in this document are provided "as is". Unless required by applicable laws, this company doesn't provide any express or implicit guarantees for all contents in the document, including but not limited to guarantees for marketability, quality satisfaction, application to specific purpose and non-infringement of third-party rights.
- The security technologies, capability and characteristics described in this document shall be subject to the specific product model, software version, software platform and the implementation of specific solution. It does not provide any expressed or implied guarantee that all the products or solutions of Dahua provide all the security technologies, capability and



characteristics described in this document.

Export Control Compliance Statement

 Dahua abides by applicable export control laws and regulations, and implements export, re-export and transfer requirements of hardware, software and technology. Regarding products described in this manual, please fully understand and strictly conform to applicable export control laws and regulations at home and abroad.

About This Document

- If the PDF document obtained cannot be opened, please upgrade the reading tool to the latest version or use other mainstream reading tools.
- The company reserves the right to modify any information in this document at any time. The modified contents will be added to the new version of this document without prior notice. There may be slight difference in part of the product functions before and after the update.
- This document may contain technical inaccuracies, discrepancies with the product function and operation or typographical errors. All subject to the final interpretation of the company.



Table of Contents

LEGAL STATEMENT	I
1.PREFACE	1
1.1 Acronym	1
1.2 Overview	1
2 Security Level	3
2.1 Security Level Introduction	
2.2 Level 1 Protection	4
2.2.1 Factory Default Setting	4
2.2.2 Password Management	4
2.2.3 Set Reset Password Info	6
2.2.4 Use Latest Firmware or Client	
2.2.5 System Time Calibration	9
2.2.6 Function Minimization	10
2.2.7 Set Account Locking rules	11
2.2.8 Check Log	
2.2.9 Check Online User	13
2.3 Level Two Protection	13
2.3 Level Two Protection	13
2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Managemen	13
 2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Managemen 2.3.3 Enable HTTPS Service 	13
 2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Managemen 2.3.3 Enable HTTPS Service 2.3.4 Audio Video Transmission Encryp 	13 13 t
 2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Managemen 2.3.3 Enable HTTPS Service 2.3.4 Audio Video Transmission Encryp 2.3.5 Black and White List Configuration 	13 13 13 14 14 16 tion
 2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Management 2.3.3 Enable HTTPS Service 2.3.4 Audio Video Transmission Encrypt 2.3.5 Black and White List Configuration 2.3.6 Limit Max Concurrency of Login 	13 13 t
 2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Managemen 2.3.3 Enable HTTPS Service 2.3.4 Audio Video Transmission Encryp 2.3.5 Black and White List Configuration 2.3.6 Limit Max Concurrency of Login 2.3.7 Backup Config Data 	13 13 13 14 14 16 16 10 10 21 1 22 22 23
 2.3 Level Two Protection 2.3.1 Port Management 2.3.2 Hierarchical Account Managemen 2.3.3 Enable HTTPS Service 2.3.4 Audio Video Transmission Encryp 2.3.5 Black and White List Configuration 2.3.6 Limit Max Concurrency of Login 2.3.7 Backup Config Data 2.3.8 Automatic Network Resume 	13 13 14 14 16 tion
 2.3 Level Two Protection	13 13 14 14 16 tion 21 1 22 22 22 22 23 23 23 24 24
 2.3 Level Two Protection	13 13 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 2.3 Level Two Protection	13 13 13 14 14 16 tion 21 1 22 22 22 22 23 23 23 24 24
 2.3 Level Two Protection	13 13 14 14 16 tion 21 1 22 22 22 23 23 23 23 24 24 25 25
 2.3 Level Two Protection	13 13 13 14 14 16 tion 21 22 22 22 23 23 23 24 25 27
 2.3 Level Two Protection	13 13 14 14 16 tion 21 1 22 22 23 23 23 23 23 24 24 25 25 27 28
 2.3 Level Two Protection	13 13 13 14 16 tion 21 1 22 22 23 23 23 24 24 25 25 27 28 29 29



Thermologia	
3.2 Config SNMP Securely	29
3.3 Config AP Hotspot Securely	30
3.4 Config SMTP Securely	30
3.5 Safe Config FTP Function	31
4 INCIDENT RESPONSE	33
4.1 Security Incident Response Mechanism	33
4.2 Security Incident Response Email	



1 Preface

This document mainly introduces security levels and various security hardening items, secure application of some functions and incident response mechanism and contact info.

1.1 Acronym

Abbreviation	Full Name
ARP	Address Resolution Protocol
FTP	File Transfer Protocol
MAC	Media Access Control
SSH	Secure Shell
Onvif	Open Network Video Interface Forum
UPnP	Universal Plug and Play
NTP	Network Time Protocol
DDNS	Dynamic Domain Name System
CGI	Common Gateway Interface
3G	3rd-generation
PPPoE	Point to Point Protocol over Ethernet
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer
НТТР	Hyper Text Transfer Protocol
SMTP	Simple Mail Transfer Protocol

1.2 Overview

With rapid development of IoT network scale and application, continuous increase of audio/video multi-media application, network environment becomes more and more complicated. All kinds of network threats and attacks are emerging, and network security issue raises more and more concern. Network security events occur frequently, including



Trojan virus, ARP spoofing, application and system attack and so on.

In order to achieve the best network security, Dahua minimizes equipment security risks in product design, development and test and avoids network attacks on devices. However, equipment and service security require the response of the entire supply chain and the participation of end users. Therefore, we develop this security hardening guide to help you establish a security management system to ensure normal and safe operation of equipment and systems.



2 Security Level

2.1 Security Level Introduction

The guide formulates three protection levels according to different system scales and security needs. Please refer to Table 2-1 for more details about three protection levels and corresponding security items.

Protection Level	Security Item
Level 1 Protection	Facroty Default setting
	Password Management
	Set reset password info
	Use latest firmware
	Set account lock
	Disable unnecessary function
	Enable HTTPS service
	Audio and video transmission encryption
	System time Calibration
	Disable anonymity login
	Online upgrade
	Check log
	Check online users
	Use latest version of client
	AP hot spot safe application
Level 2 Protection	Port management
	Hierarchical account management
	Limit the max. number of logins
	Configure black and white list
	Backup config data
	Enable RAID backup storage
	Safe config SNMP
Level 3 Protection	Network log
	Enable 802.1x
	Device anti-theft
	Device anti-damage
	Device anti-thunder
Ĩ	
Level 1 protection requ	uires minimum security while level 3 protection requires
Maximum security. Lev	vel 2 protection contains all the security items of level 1
protection and level 3	protection contains all the security items of level 2

Tab		2_1	
Iau	IC.	2-1	

protection.

Home users and small micro businesses are recommended to configure level 1



protection; medium-sized enterprises are recommended to configure level 2 protectionl large-sized enterprises and infrastructure projects are recommended to configure level 3 protection. Try to configure a higher security level than recommended if the condition permits.

2.2 Level 1 Protection

2.2.1 Factory Default Setting

If the device is used by other people, it is recommended to restore factory default setting in order to guarantee device security.

Operation method

The device supports the following two methods to restore factory default setting:

- Long press the button on device hardware to restore factory default setting.
- Select "Setting > System > Default" on the config interface and enter "Default" interface for operation.

(a)hua							
- Street All	PHEVIEW	PLAYBACK	AI SEANCH	ALANIA	SETUP	00-0	100001
MAGE	DEFAULT						
NETWORK							
EVENT	12 Al						
STORAGE	2 CAMERA	2 NETWORK	EVENT				
- SYSTEM	F STORAGE	2 SYSTEM					
> GENERAL	Default	Factory Reset					
> DISPLAY		1 - actual reason					
> R8232							
> PTZ							
> VOICE PROMPT							
> ACCOUNT							
> SECURITY							
> AUTO MAINTENANCE							
> MP/EXP							
S-DEFAULT							
> UPGRADE							



2.2.2 Password Management

Password includes device admin password and ONVIF access user password, it will cause the device to be invaded if the password is exposed or broken, and it is recommended to make password maintenance according to the following aspects:

- Adopt strong password.
 - Password length should be between 8 and 32 characters, it has to contain at least two kinds of characters including lower-case English letters a~z, capital English letters A~Z, numbers 0~9, special characters (except "'", """, ";", ";", ":", "&", blank and nonprinting characters).
 - The more kinds of character contained in the password, the stronger the password becomes with higher security. It is to set strong password according to



system prompt.

- The password is not recommended to use user name or inverted order of user name, Try to reduce continuous letters or numbers (such as 123, abc and so on).
 Try to reduce continuous use of the same character (such as 111, aaa and so on).
- Modify password regularly

If the password was used by non-staff, it can avoid password being preserved for long term and reduce device exposure risk via modifying password.

Operation method

Set password

It is required to initialize the device if it is the first time to use the device or the device is used for the first time after factory default setting. Please set strong password for admin user according to the interface prompt.

• Modify device admin password

Select "Setting > System > User Management > User Management", click is modify device admin password.

Modify User		X
User	admin	
Group	admin	
Memo	admin 's account	
User MAC		
Modify Password		
Old Password		
New Password		
	Low Middle High	
Confirm Password		
Email Address	z***@tech.com	
Authority		
System	Playback Monitor	_
	Same Consel	
	Save Cancel	

Figure 2-2

• Modify ONVIF access username and password



Select "Setting > System Management > User Management > ONVIF User", click to modify ONVIF access username and password.



Modify User	×
User	admin 💌
Group	admin
Memo	admin 's account
User MAC	· · · · · ·
Modify Password	
Old Password	
New Password	
	Low Middle High
Confirm Password	
	Save Cancel

2.2.3 Set Reset Password Info

Dahua device is equipped with the capability of password reset for admin user; it helps users to manage account better. In order to avoid the function being used by malicious attacker, please set reset password info in advance, please modify in time if there is information being altered. Reset password related info includes reserved email and security question. It is recommended not to use answers which are easy to be guessed when setting security question.

2.2.3.1 Set Reserved Email Address

Operation Method

Password reset operation via reserved email address includes enabling password reset switch and setting reserved email address.

Enable Password Reset Switch
 Select "Setting > System > Security Management > System Service", enter "System
 Service" interface to operate.

Figure 2-4



@lhua	PREVIEW PLAYBACK SMARTPLAY ALARM BETUP INFO LODOUT
MAGE NETWORK EVENT STORAGE STORAGE STORAGA STO	PREVEINS PLAYBACK SMART PLAY ALARM SETUP INFO LODOUT UP FILTER Rystem Service HITTPS HITTPS PAIRWORD RESET (*) Datase HITTPS D01 (*) Entase D03 (*) Entase D04 (*) Entase D05 Reference D1 (*) Entase D1 (*) Entase D2 Entagene
> AUTO MANTENANCE > MPEXP > DEFAULT > UPDAUE	

- Set Reserved Email Address
 - The device is required to initialize if it is the first time to use the device or the device is used after factory default setting, please set reserved email address according to the interface prompt.
 - Select "Setting > System > User Management", enter "User" interface to modify reserved email address.

User			×
Username	admin	•	
Group	admin	•	
Memo	admin 's account		
Modify Password			
Old Password			
New Password			
	Low Middle	High	
Confirm Password			
Email Address			
Authority			
System	Playback	Monitor	
ACCOUNT	SYSTEM	SYSTEM INFO	MANUAL CONTROL
✓File Backup	STORAGE	✓ EVENT	✓NETWORK
	SECURITY	Device Maintenance	
	OK	Cancel	
	UN	Cancer	

Figure 2-5

2.2.3.2 Set Security Question



Only storage device supports setting security question.

Operation Method

- The device is required to initialize if it is the first time to use the device or the device is used after factory default setting, please set security question according to the interface prompt.
- Some storage devices are configured locally, select "Main menu > Setting > System > User Management > Security question" and it supports modifying security question.

	SETTING	
CAMERA	TNETWORK 📸 EVENT STORAGE SYSTEM	
GENERAL DISPLAY RS232 PTZ	User Group Security Qu ONVIF User Please set a security question so that you can find the password of admin again.	
BROADCAST VOICE PROMPT	Ouestion 1 (What is your favorite children's book? Answer	
ACCOUNT SECURITY AUTO MAINTE	Question 2 (What was the first name of your first boss?	
IMP/EXP DEFAULT UPGRADE	Question 3 (What is the name of your favorite fruit?	
	Setting Delete	

Figure 2	2-6
----------	-----

2.2.4 Use Latest Firmware or Client

When some key system vulnerabilities are found, we will release new firmware in order to repair vulnerabilities and stop attackers trying to adopt known vulnerabilities to attack device. Meanwhile the client is matched with device firmware for repairing function or hole. In order to enhance device security level and lower the risks of device being attacked or invaded, please make sure you use the latest firmware version and client which conform to Dahua security baseline.

Operation Method

• Acquire the latest firmware

Ш

Acquiring the latest firmware or client is only used for manual upgrade, please ignore this if you are using online upgrade function.



Log in Dahua website www.dahuatech.com to download the latest firmware version or client version, or you can download the latest mobile APP in application store.

• Uprade Device

It supports file upgrade and online upgrade. File upgrade requires that firmware has been obtained. Online upgrade requires that your device has been accessed to public network. Online upgrade function can remind you of latest firmware information in order to help you find latest version in time.

Select "Setting > System > System Upgrade", enter "System Upgrade" interface to upgrade firmware version.

(a)hua	PREVIEW	PLAYBACK	AI SEARCH	ALARM	SETUP	INFO	LOGOUT
IMAGE NETWORK EVENT STORAGE SY&TEM > GENERAL > DISPLAY > R9232	System Upgrad	se mware File			Browse	Upgrade	
> PTZ > VOICE PROMPT > ACCOUNT > SECURITY > AUTO MAINTENANCE > IMPROP > DEFAULT > UPGRADE	Online Uppr Colline Uppr Auto-t Byste	ade check for updates m Version 321500	00008.0 Build Date	2018-06-28	blanual Che	3	

Figure 2-7

2.2.5 System Time Calibration

From a security perspective, it is very important to set correct date and time. It will destroy the retrospectivity of recorded file and log if the device time is not correct.

It is recommended to use NTP time sync function. You can adopt public NTP server if NTP server is not deployed, such as time.windows.com.

Operation method

Select "Setting > System >General > Date", enter "Date" interface to set.



(alhua)	PREVIEW	PLAYBACK AI SE	IRCH ALAR	M	SETUP	INFO	LOGOUT
	PREVIEW General Date Format Time Format Date Separator Time Zone System Time System Time DST Type Start Time End Time End Time Server Port	PLAYBACK AI SEA Date&Time YYYYY MM DD 24-HOUR - GMT+08:00 2018 - 08 - 09 Date Week Jan • Last We Jan • Last We time windows com 123	ALAR Holiday Holiday Holiday Holiday Holiday Holiday Holiday Holiday Holiday Holiday Holiday Holiday Holiday	M Sync PC 00 00	90 00	INFO	LOGOUT
> UPGRADE	Interval	60 OK]	Min (0-65535) Refresh	Default.	1		

2.2.6 Function Minimization

It is recommended to conform to the minimization principle when using device function, for reducing device attack surface and improving device security.

Function	Entry Condition	Factory	Default
FUNCTION		Status	
UPnP	Select "Setting > Network > UPnP"	Disable	
Multicast	Select 'Setting > Network > Multicast"	Disable	
SSH			
(Only			
supported by	Select "Setting > System > Security > SSH".	Disable	
IPC and PTZ			
camera)			
Onvif	Select "Setting > System > Security > System".	Enable	
CGI	Select "Setting > Security > System".	Enable	
Wi-Fi	Select "Setting > Network > Wi-Fi".	Disable	
3G/4G	Select "Setting > Network > 3G".	Disable	
AP Hotspot	Select "Setting > Network > AP Hot Spot".	Disable	
PPPoE	Select "Setting > Network > PPPoE".	Disable	
DDNS	Select "Setting > Network > DDNS".	Disable	
SNMP	Select "Setting > Network > SNMP".	Disable	

T	ab	ole	2-	2



Function	Entry Condition	Factory Default
		Status
Bonjour (Only supported by IPC and PTZ camera)	Seelct "Setting > Network > Bonjour".	Enable
Register	Select "Setting > Network > Register".	Disable
FTP	Select "Setting > Storage > FTP Storage".	Disable
NAS	Take IPC for example, select "Setting > Storage > NAS".	Disable
Password reset	Select 'Setting > System > Security > System Service".	Enable
P2P	Select "Setting > Network > P2P".	Enable
Audio	Select "Setting > Camera > Encode > Stream"	IPC/NVR/DVR: Main stream is enabled by default, sub stream is disabled by default. PTZ camera: It is disabled by default.
Alarm center	Select "Setting > Network > Alarm Center".	Disable
SMTP	DVR/NVR: Select "Setting > Network > Email Setting". IPC/PTZ: Select "Setting > Network > SMTP (Email).	Disable
ISCSI (Only supported by some NVR)	Select "Setting > Storage > ISCSI"	Disable
GB 28181	Select 'Setting > Network > GB 28181".	Disable
Anonymity login (Only supported by IPC and PTZ camera)	Seelct "Setting > System > User > User".	Disable

2.2.7 Set Account Locking rules

The attacker may log in the device forcibly via trying password for several times, account locking can avoid the possibility of attackers trying continuously for several times and it can protect the device account security.

Operation Method

• NVR/DVR: select "Setting > Event > Abnormity > User", enter the "User" interface to set, the fewer attempts allowed, the longer the lock time becomes and the higher the



security level is.

- :	~ ~
Figure	2-9

(alhua	PREVIEW	PLAYBACK	AL SEARCH	ALARM	SETUP	INFO	LOGOUT
	HDD	Network	User	Fan			
T EVENT	Event Type	Illegal Login		_			
VIDEO DETECTION SMART PLAN	(V) Enable Attempt(s)	5	Times (1-10)				
> IVS > FACE DETECTION	Lock Time	6	Min. (1~30)				
> FACE RECOGNITION > HUMAN BOOY DETE.	Latch	1 2 3	(4 5 5 Sec(0-300)				
> ANPR	Voice Prompts	File Name	None	•			
> HEAT MAP	1 100.0000.0000000000	OK	Fielfresh				
> AUDIO DETECT > ALARM							
> ABACIRMALITY > ALARM OUTPUT							
> POS							
STORAGE							

• IPC/PTZ Camera: Seelct "Setting > Event > Abnormity > Illegal Access", enter the "Illegal Access" interface to set, the fewer login error allowed, the higher the security level becomes.

2.2.8 Check Log

Log is the important basis to trace device abnormity, you are advised to check log regularly, such as security type log, illegal user login and so on, and it has to troubleshoot if the device is safe timely.

Operation Method

Seelct "Information > Log", enter "System Log" interface to inquire if there is log of security type.

Figure 2-10



ala anna an	PREVIEW	PLAYBACK	AI SEARCH	ALARM	SETUP	INFO	LOGOUT
FØ	Log						
tirsion	mattine	2018-08-09	77	00 00 00	End Time	2018-08-10	00 00 00
MLINE USERS	Tjpe	Al	•	Search			
EOPLE COUNTING	C INO			Tême			Erm
EATMAP							
tio							
	System Log into						
	System Log ado Time Type						
	System Log into Time Type Centerts						
	System Log ado Time Type Contents						
	System Log into Time Type Contents						
	System Log ado Tana Type Contents						H 4 111 P M T

2.2.9 Check Online User

The device is equipped with the function which can display the info of online users; it is recommended that you can check online user info occasionally and troubleshoot if the device is logged in illegally. NVR/DVR also supports the function of removing unexpected users.

Operation Method

Select "Information > Online User", enter "Online User" interface to inquire.

	PREVIEW	PLAYBACK AI BEAR	CH ALARM	BETUF INFO	LOGOUT
mPO	Online User				
> VERSION > LOC • COUNE VEERS > PEOPLE COUNTING > HEAT MAP > HOD	1	Unertrainte admin	Group Harrie admin	10 A01444	00116-06-02-02-31 10
	Reheab				

Figure 2-11

2.3 Level Two Protection

2.3.1 Port Management

Batch attacks in a network often look for well-known ports as direct entry points for attacks. Modifying the port can hide itself and block certain attacks, it is recommended that you customize service port number of the device.



Operation Method

Select "Setting > Network > Port", enter "Port" interface to set.

```
Figure 2-12
```

aniua	PREVIEW	PLAYBACK	AI SEARCH	ALARM	SETUP	INEG	LOGOUT
IMAGE NETWORK	PORT	HTTPS					
TCPMP	Mas Connection	128	10	-1280			
Part	TCP Port	37777	61	(25-65830)			
PPPoE	UDP Port	37778	010	125-6953E)			
+ DONS	HTTP Pair	80	0	(66535)			
SINC TIME RIGHT	HTTPS Port	443	(1	65535) Enative			
EMAL	RTSP Part	554	(1-	-005351			
UPnP	POS Pod	38800	0	-05535)			
SIMF MULTICAST	RTSP Format	rtsg /HUse	name: «Password»	g-IP Address - Port	-/camireaimonitor?ch	iannel-18.subhpe-0	
REGISTER		- Commenter	outrent, reset, anosetter	Constantin Append		MONTO -	
ALARM CENTER			Belter	h Detaul	termine 1		
P2P							
SWITCH							
VENT							
TORAGE							
SYSTEM							

2.3.2 Hierarchical Account Management

Hierarchical account management realizes different authorities for people with different identity, which is to avoid exceeding authority. For example, an video surveillant is limited to check video. It is recommended that you classfy and decentrailize system users and assign the minimum scope of authority required for each user to control the risk of misuse of equipment, while facilitating security audits.

Operation Method

Step 1

Select "Setting > System > User > User > User Group", enter "User Group" interface to set user group and give the user group corresponding authority.

(alhua	PLAYS	ACK A) SEARCH ALAR		LOBOUT	
IMADE NETWORK EVENT STORAGE SY STEM CONERNL CONERNL OUSPLAT NOLOC PROMPT AUDOLART SECURITY SUCCORTY	Diski Diski 2 2 5 3 2 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5	User Geop Doop lane adren aan	Nervis administrator group wear group	Width Dr 2	
> DEFAULT > UPGRADE					

Figure 2-13



Figure 2-14

,	Add Group			×	3
	Group Name Memo				
	Authority				
	System	Playback	Monitor		
	AII Device Maintenance NETWORK SYSTEM INFO	File Backup	SECURITY STORAGE	CAMERA	
		ок	Cancel		

Step 2

Select "Setting > System > User > User > User", enter "User" interface to add user or modify user group.

F	ig	ur	е	2-	1	5
		-	-			_

Add User		X
User		
Password		
	Low Middle High	
Confirm Password		
Group	admin 💌	
User MAC		
Memo		
Period	Setting	
Authority		
System	Playback Monitor	_
	VENT VENTK CAMERA	
	Save Cancel	



2.3.3 Enable HTTPS Service

HTTPS is the protocol service based on TLS encrypted link transmission. It ensures that the data is encrypted during transmission when it accesses to device via WEB, which is to prevent attackers stealing it maliciously, it is recommended that you have to enable and use HTTPS to access device WEB.

Operation method

Take NVR for example; please refer to the corresponding user manual for operation if it needs to configure IPC or PTZ camera.

Step 1

Select "Setting > Port > Port", enter "Port" interface to enable HTTPS function.

Note

Please select "Setting > Network > HTTPS" for config access of IPC and PTZ camera.



Figure 2-16

Step 2

Create server certificate.

It needs to implement "Create Server Certificate" if it is your first time to use the function or modify device IP.

- 1. Select "Setting > Port > HTTPS", enter "HTTPS" interface.
- 2. Click "Create Server Certificate", the system will display the dialog box of "Create Server Certificate".

Figure 2-17



Create Server Certificate						
Country	AU					
State						
Locatity						
Oragnization						
Oragnization Unit						
IP or Domain Name	10.10.6.238					
	Create Cancel					

3. Fill in the corresponding "Country", "Province" and other info, click "Create". The system will prompt "Successfully created" after it is created successfully.

Note

The value of "IP or Domain Name" has to be in accordance with the device IP or domain name.



HTTPS		
Create Server Certificate	Download Root Certificate	

Step 3

Download root certificate.

It needs to implement "Download Root Certificate" if it is your first time to use HTTPS on your computer.

- 1. Select "Setting > Port > HTTPS", the system will display "HTTPS" Interface.
- 2. Click "Download Root Certificate", the system will display the interface of "File Download".

Figure 2-19



File Dow	File Download - Security Warning 🛛 🔀			
Do you want to open or save this file?				
Name: ca.crt Type: Security Certificate From: 10.10.6.238				
1	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>			

3. Click "Open", the system will display the interface of "Certificate" info.

8	Certificate Information
Thi: inst Aut	s CA Root certificate is not trusted. To enable trust, all this certificate in the Trusted Root Certification horities store.
7 <u>2</u>	Issued to: test
	Issued by: test
	Valid from 2016/ 7/ 8 to 2020/ 7/ 7

Figure 2-20

4. Click "Install Certificate", the system will display the interface of "certificate Import Wizard".

Figure 2-21





5. Click "Next", the system will display the interface of selecting certificate storage area.

Figure 2-22



Certificate Store	
Certificate stores are system area	as where certificates are kept,
Windows can automatically select the certificate.	a certificate store, or you can specify a location for
Automatically select the cer	tificate store based on the type of certificate
Place all certificates in the finance of the fin	ollowing store
Certificate store:	
Trusted Root Certification	Authorities Browse
.earn more about <u>certificate stores</u>	
	< Back Next > Cancel

6. Click "Next", the system will display the interface of "Completing certificate import wizard".

Figure 2-23



7. Click "Finish", the system will display the interface of "Import successfully", which means certificate download has been completed.





2.3.4 Audio Video Transmission Encryption

Audio and video data carries a large amount of personal privacy content, which is the key object protected by device. It is recommended to enable the function of audio video transmission encryption in order to avoid audio video data being stealed maliciously by attackers during transmission; it can guarantee data security during transmission.

Operation Method



Select "Setting > System > Security > System Service", enter the interface of "System Service" to set.

Figure 2-25

IP FILTER	System Service HTTPS
PASSWORD RE	ET 🔽 Enable
Mobile Phone Pu	sh 🗹 Enable
CGI	C Enable
ONVIF	✓ Enable
Audio/Video	Enable The corresponding device or software shall support
Transmission	video decryption function.
Encryption	
File Backup	Enable Set Password (It is 8 to 32-digit containing letter(s), number(s),
Encryption	symbol(s). It contains at least two types.)
	OK Refresh Default

2.3.5 Black and White List Configuration

Enable white list, it can access the device only when IP/MAC addresses are added to the white list. Enable black list, the IP/MAC addresses added to black list is prohibited to access to device. It is recommended to enable black list or white list, it is to set the minimum range that the device can be accessed to, and reduce the device attack surface via black and white list function.

Note

IPC/PTZ camera only supports white list function.

Operation method

Select "Setting > System > Security > IP Filter", enter "IP Filter" interface to set.

Figure 2-26

		9
S. Anna J. A. C. A. C. A. C. A.		
abliess MAC abliess	Mailly	Dates
		3
		Gartere Ad
Sint		

2.3.6 Limit Max Concurrency of Login

It is to limit the number of clients (WEB client, platform client and mobile client etc.) that devices allow to log in at the same time, help the device limit malicious flow attack and



protect normal operation of important business.

Operation Method

Select "Setting > Network > Port", enter the "Port" interface to set.

F	'n	ıır	þ	2.	.2	7
L	ıy	uı	e	۷.	· _	1

CONNECTION	HTTPS	
Max Connection	128	(0~128)
TCP Port	37777	(1025~65535)
UDP Port	37778	(1025~65535)
HTTP Port	80	(1~65535)
HTTPS Port	443	(1~65535) 🔲 Enable
RTSP Port	554	(1~65535)
POS Port	38800	(1~65535)
RTSP Format	rtsp:// <user name="">:<passw< th=""><th>vord>@<ip address="">:<port>/cam/realmonitor?channel=1&subtype=0</port></ip></th></passw<></user>	vord>@ <ip address="">:<port>/cam/realmonitor?channel=1&subtype=0</port></ip>
	channel: Channel, 1-16; sub	type: Code-Stream Type, Main Stream 0, Sub Stream 1.
	Save	efresh Default

2.3.7 Backup Config Data

Backup the config data timely and it can recover quickly when the config data is destroyed.

Operation method

Select "Setting > System > Config Backup", enter the interface of "Configure Import Export" to operate.



Figure 2-28

2.3.8 Automatic Network Resume

IPC continues to record when NVR device detects a break in the network connection with IPC. After the network is recovered, the NVR will download the video from the IPC during



the period when the network is disconnected, so as to guarantee the integrity of the video recording of the IPC channel in the NVR equipment. The function can help you better ensure the integrity if your video.

Operation Method

IPC/PTZ camera enables the function by default; the device is able to store the video data locally without any other config during network disconnection when it is equipped with a SD card.

On the interface of NVR/DVR config interface, select "Setting > Storage > Storage > Record", enter "Record" interface and enable ANR function and set prerecord duration.



Figure 2-29

2.4 Level Three Protection

2.4.1 Network Log

Due to limited storage capacity of the device and limited logging capability, it is recommended that you enable network logging, which will ensure that critical logs are synchronized to the network log server. The function is only supported by IPC and PTZ camera.

Operation Method

Note

Please make sure the syslog server is deployed on the remote host and the server is



enabled before using the function.

Take IPC for example, select "System Info > System Log > Remote Log Record".

Figure 2-30

og	Remote Lo	g				
Enable						
IP Address	192	168	0	108		
Port	514				(1~65534)	
Device Numbe	22				(0-23)	
	D	efault		Re	tresh	Save
			-		-	

2.4.2 Enable 802.1x

802.1x is a network access authentication protocol. Only after passing the authentication, can it implement normal network communication. It is recommended that you establish an 802.1x access control system to block malicious terminal access to private network. IPC and PTZ camera can support 802.1x access authentication now.

Operation Method

Take IPC for example, select "Setting > Network > 802.1x", enter "802.1x" interface to set.

Figure 2-31

(a)hua				Live	112	Paybas	Satup	Alarm	Logout
- Camera	802.1x	1							0
 Hertwork TCMP Connection PPTNE DOME IF Filter SPTPErsell 	¥ Erate Automication (Inverse Passwort	PEAP sone 	Refeat						
> Shat ² > Doux# > Matsat = 00211 > Coll = Event = Bronige = System = Information									

2.4.3 Cluster Service

Cluster service refers to a cluster composed of multiple isomprphic devices. When one or more of the devices fail the function is switched to the standby device and the standby device replaces the primary device. The failure of master equipment will not result in the inability to view real-time monitoring or loss of video. Only some NVR support this function.

Operation Method

Step 1

Add master device and standby device on the standby device.

• Select "Setting > Cluster Service > Master Device", enter the interface of "Master



Device" and add master device.

Figure 2-32

Manual Alexandra		UPPER LINE	CHARGE WAR	
Mather Divide Harter M/R1	172.11.3.28	Working	Operation	Cistone

 Select 'Setting > Cluster Service > Standby Device", enter the interface of "Standby Device" and add standby device.

Note

Add all the standby equipments except itself.

Figure 2-33

Slave Device Name	IP Address	Replace IF	Status	Operation	Detete
NVR2	172.11.2.233		DCS Working Device+Free	P	0

Step 2

Select "Setting > Cluster Service > Cluster IP" on the master device, enable cluster service and set virtual IP.

Note

The IP address in "TCP/IP" is used for cluster internal control (that is, for internal interaction between master and standby devices), and the virtual IP address set here is used for cluster external control (that is, for use with an external network connection).

Figure 2-34



Enable												
IP Address	0	÷	0	16	0		0					
Subnet Mask	0	30	0	×.	0		0					
Default Gateway	0	÷	0	æ	0		0					
		0	ж	_	7	Č.	R	ish	Def	ault	1	

Select "Setting > Cluster Service > Cluster Control > Cluster Control" and enable cluster function.

	Antoitean an ID	
CLUSTER CONTROL	Arbitrage IP	
Start Cluster	Delete Cluster	

Figure 2-35

2.4.4 Physical Protection

• Device anti-theft

Prevent device being stolen, it is recommended that you install mobile alarm; digital detection alarm and component lock etc. when installing the device.

- Device anti-damage
 Prevent the device being damaged, it is recommended that you install vandal proof enclosure when installing the device.
- Device anti-thunder

Prevent the device being damaged by thunder, it is recommended that you install lightning arrester when installing the device.

Figure 2-36



2.4.5 Network Isolation

It is suggested that you partition the network according to the actual network needs. If there is no communication requirement between two subnets, it is recommended to use VLAN, gateway or other means to divide the network to reduce the attack surface faced by the subet. Improve network security by reducing subnet entry surface.



3 Safe Use of Function

3.1 Complex Password

The complex password mentioned in this chapter should meet at least the following requirements.

- The password length is no less than 8 characters.
- Contains at least two types of character.
- The password does not contain the reverse order of the account name or the account name.
- Do not use continuous strings such as 123, ABC etc.
- Do not use consecutive identical characters, such as 111, aaa etc.

3.2 Config SNMP Securely

SNMP (simple network management protocol) which can support network management systems to monitor whether there are any situations that cause management concerns when it is connected to the network. If you need to deploy an SNMP system, it is recommended that you use SNMP safely.

- Choose the more secure version of SNMP v3;
- Read and write assign passwords to different accounts;
- Set complex authentication codes;
- Set complex encrypted password;
- Adopt a more secure form of authentication SHA.

Operation Method

Select "Setting > Network > SNMP", enter "SNMP" interface to set.

SNMP			
9MP Verse	- 9MP-1 - 9MP	2 (2) \$1880 v3	
Shall Fuel	161	(1-60238)	
Head Community	public		
Write Community	private		
Trup Address			
Top Port	162		
Read-only Username	public		
Autoretation Type	# MDS () 1946		
Authentication Password			
Energebox Type	· CEC-DES		
Encrypton Planavorti			
Readlants Gampres	private		
Authentication Type	■ M05 ○ IPH		
Adheritation Passionst			
Energyton Type	· CEC-DES		
Encryption Password			
	Oytan	Hefresh	

Figure 3-1



3.3 Config AP Hotspot Securely

If you need to use the device'AP hotspot function for network deployment, it is recommended that you configure the AP hotspot function safely.

- Set complex password for AP hotspot
- Adopt secure encryption WPA2 PSK

Operation Method

Select "Setting > Network > WiFi Module > General Config", enter the interface of "General Config" to set.

General Ad	Jvanced
2.4GHz 🔽	Enable
SSID	NVR-2hhhh
Encryption Type	WPA2 PSK
Password	12345678
Channel	Auto
Gain	Middle
	OK Refresh Default



3.4 Config SMTP Securely

SMTP function is integrated to cooperate with the device abnormity alarm notification, if you need to listen to the device abnormity and notify you via email; it is recommended that you conform to the following application methods:

- Use TLS to access the mailbox server.
- Set complex password for mailbox.

Operation Method

Select "Setting > Network > Email", enter the interface of "Email" to set.

Figure 3-3



(a)hua	PREVIEW		ALARM SETUP INFO LOGOUT
	Email Enable SMTP Server Port Anseymous Oberneme Password Denster	MaiServer 25	(1-65535)
> SYMP > MULTICAST > REGISTER > ALAVIA CENTER > SWITCH = EVENT = STORAGE = SYSTEM	Encrydan Type Subject Receiver Hiterali Interali	TLS • NVR ALERT 120 120 Sec (F-3600) 60 Min (20-6440) Email Tage 04	rtresh Default

3.5 Safe Config FTP Function

FTP function is to extend data storage capacity through network storage. If you need to use FTP for data storage expansion, it is recommended that you follow the following safe application.

- Use more secure SFTP
- Set a complex password when establishing SFTP service.
- The upload file directory is set in the non-system root directory.
- It is recommended that the SFTP remote directory be exclusive and not shared with other applications.

Operation Method

 NVR/DVR: Select "Setting > Storage > FTP Storage", enter the interface of "FTP Storage" to set.

Figure 3-4



(a)hua	PREVIEW PLAYBACK AI SEARCH ALARM SETUP IMPO LOGOUT
IMAGE NETWORK EVENT STORAGE > BASC > BASC > BOHEDULE > HOD WANAGER FIP > RECORD > ADVANCED	FTP Enuble FTP Builde FTP Heattiff 0 0 Put 21 Platemente Password Remate Directory File Size 0 Image Op/condmented
	Chantel D1 T Vestica Thursday * Period1 00 00 24 00 ALARMAN/SAPOS MD Regular Period2 00 00 24 00 ALARMAN/SAPOS MD Regular FTF Tast

• IPC/PTZ Camera: Select "Setting > Storage > Storage > FTP", enter the interface of "FTP" to set.



4 Incident Response

4.1 Security Incident Response Mechanism

Dahua technology has established Dahua Cybersecurity Center (DHCC) to resolve cybersecurity issues, and provide more reliable and much safer solution to our users. It includes security vulnerabilities report, process flows, publize security knowledges, etc. Please log in <u>https://www.dahuatech.com/service/resource.html</u> if you need to check the latest suggestion for security information.

4.2 Security Incident Response Email

Once you encounter Dahua product vulnerabilities information, please send an email to <u>cybersecurity@dahuatech.com</u> to report the hole. Please encrypt the email if it concerns the sensitive information.