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

- 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 3

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 8

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 12

2.2.9 Check Online User 13

2.3 Level Two Protection **13**

2.3.1 Port Management 13

2.3.2 Hierarchical Account Management 14

2.3.3 Enable HTTPS Service 16

2.3.4 Audio Video Transmission Encryption 21

2.3.5 Black and White List Configuration 22

2.3.6 Limit Max Concurrency of Login 22

2.3.7 Backup Config Data 23

2.3.8 Automatic Network Resume 23

2.4 Level Three Protection **24**

2.4.1 Network Log 24

2.4.2 Enable 802.1x 25

2.4.3 Cluster Service 25

2.4.4 Physical Protection 27

2.4.5 Network Isolation 28

3 SAFE USE OF FUNCTION **29**

3.1 Complex Password **29**

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 **33**

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
HTTP	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.

Table 2-1

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
 Level 1 protection requires minimum security while level 3 protection requires Maximum security. Level 2 protection contains all the security items of level 1 protection and level 3 protection contains all the security items of level 2 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

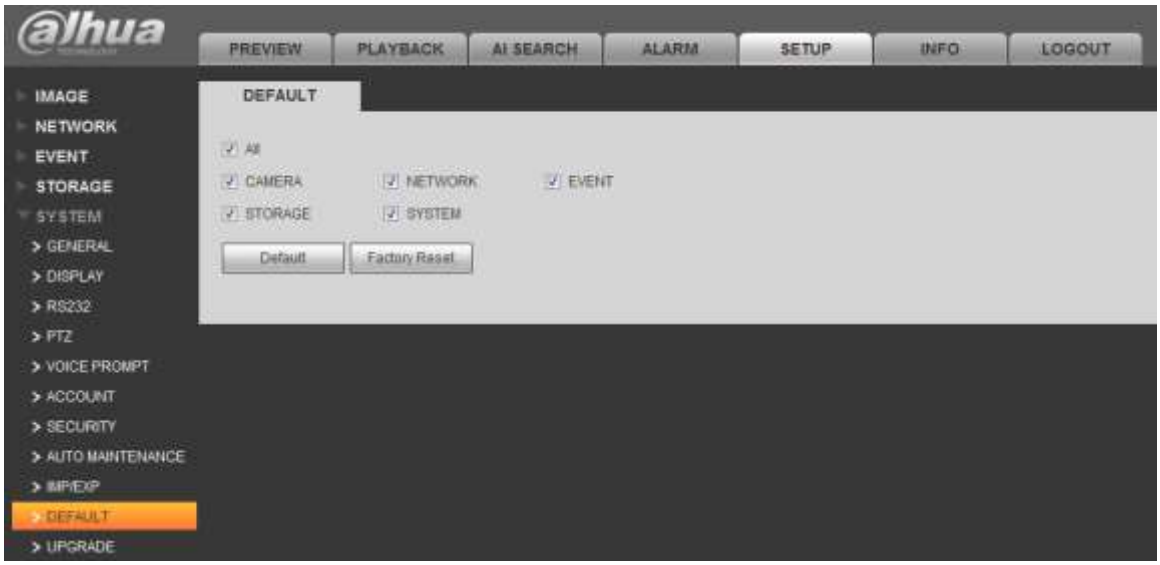
If the device is used by other people, it is recommended to restore factory default setting in order to guarantee device security.

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.

Figure 2-1



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

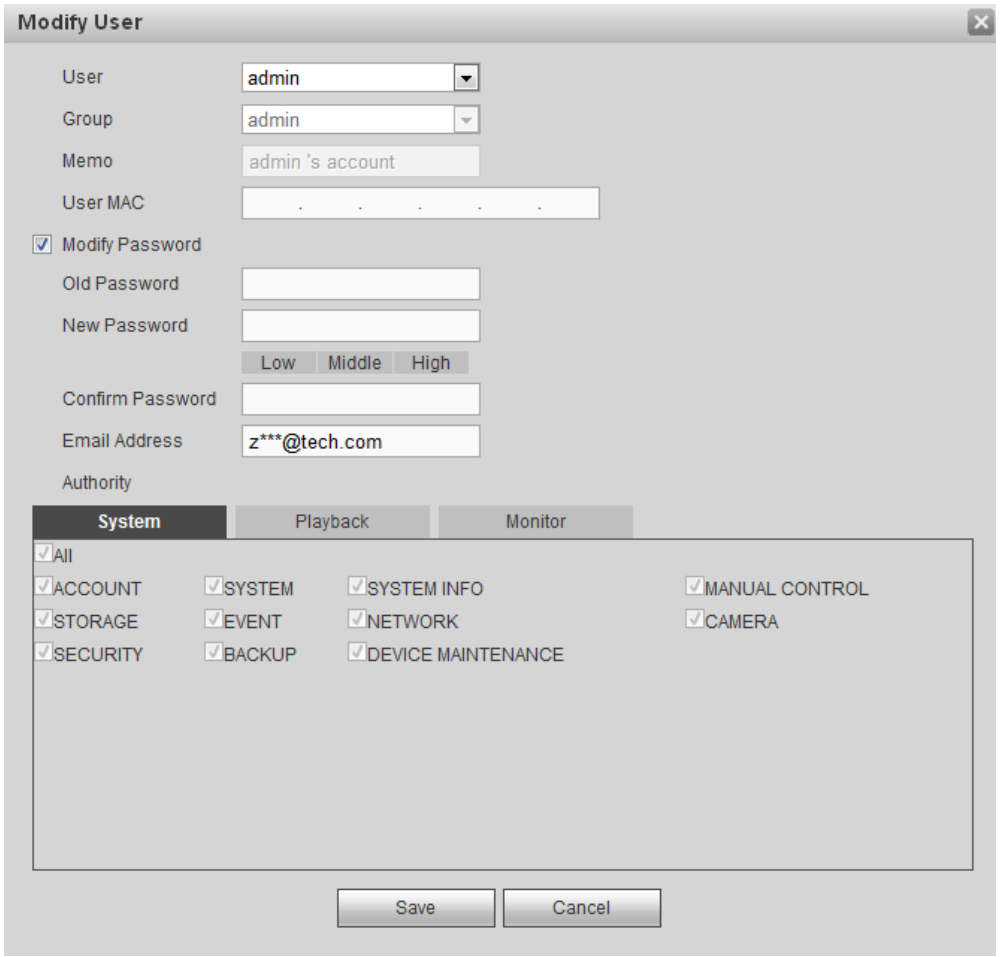
- Set password

  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 to modify device admin password.

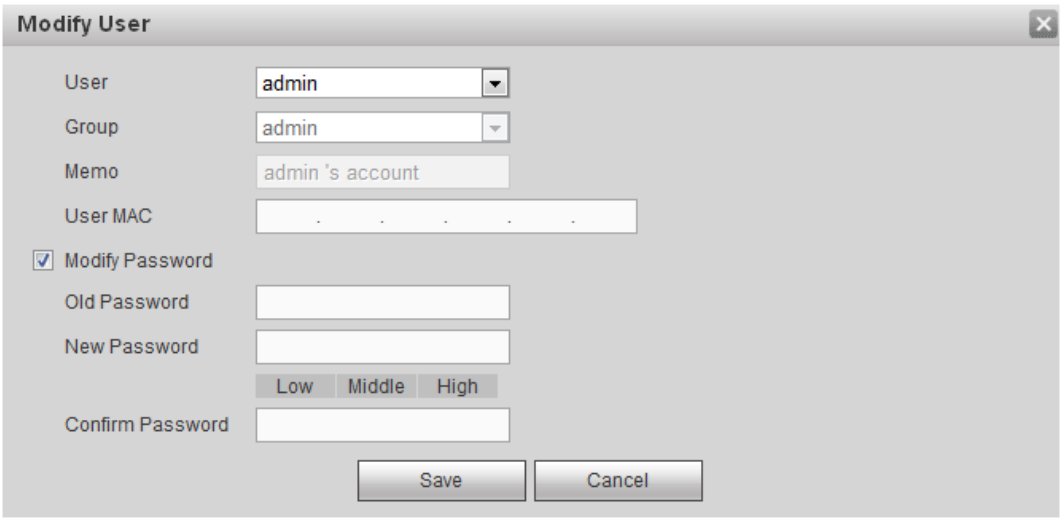
Figure 2-2



- Modify ONVIF access username and password

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

Figure 2-3



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

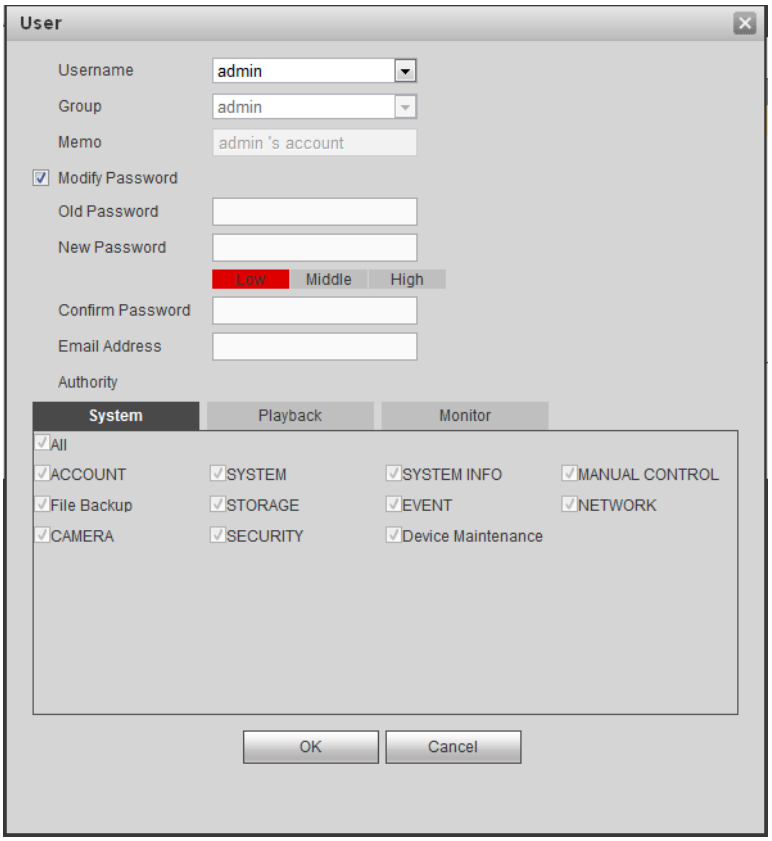
- Enable Password Reset Switch

  Select “Setting > System > Security Management > System Service”, enter “System Service” interface to operate.

Figure 2-4

- 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.

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.

Figure 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

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

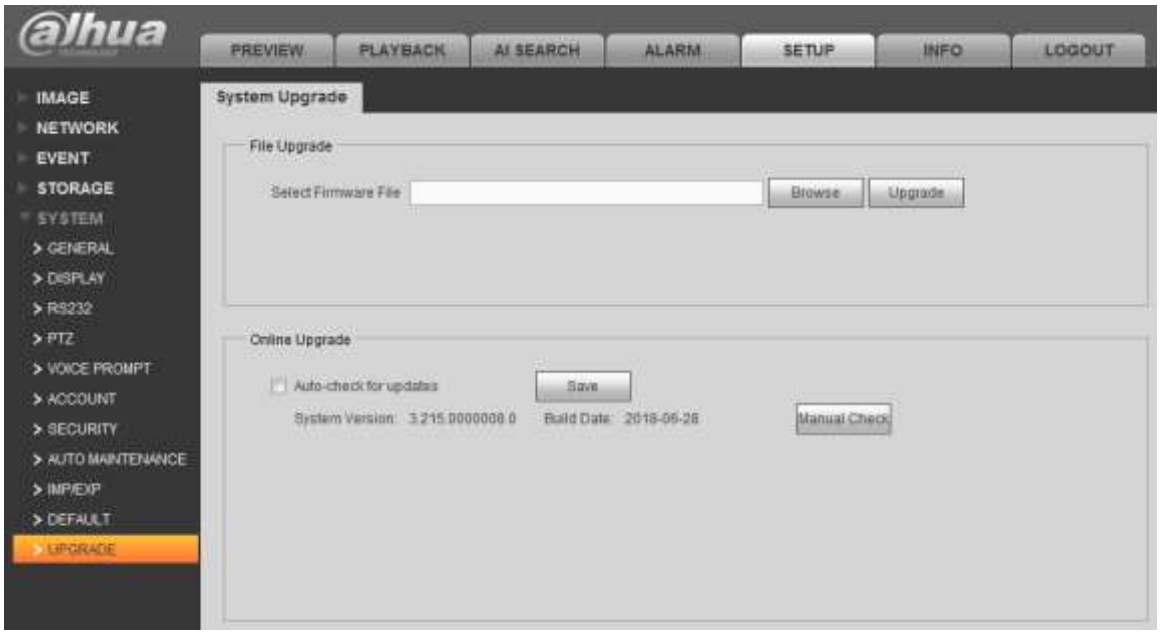
Log in Dahua website www.dahuatech.com to download the latest firmware version or client version, or you can download the latest mobile APP in application store.

- 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.

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.

Figure 2-8

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.

Table 2-2

Function	Entry Condition	Factory Default Status
UPnP	Select “Setting > Network > UPnP”	Disable
Multicast	Select ‘Setting > Network > Multicast”	Disable
SSH (Only supported by IPC and PTZ camera)	Select “Setting > System > Security > SSH”.	Disable
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

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

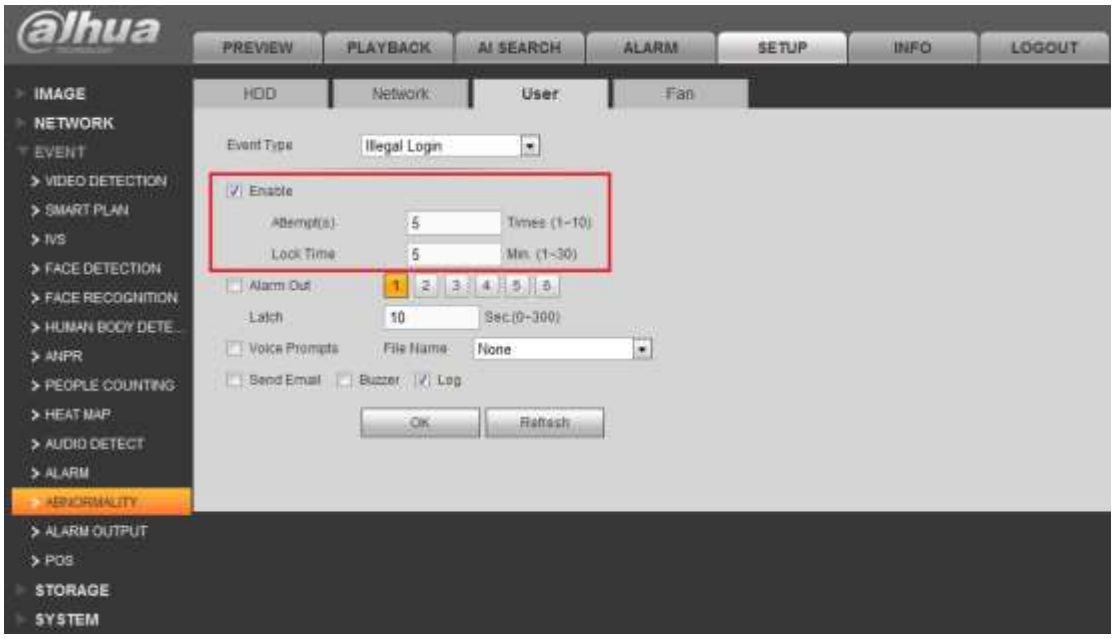
The attacker may log in the device forcibly via trying password for several times, account locking can avoid the possibility of attackers trying continuously for several times and it can protect the device account security.

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



- 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.

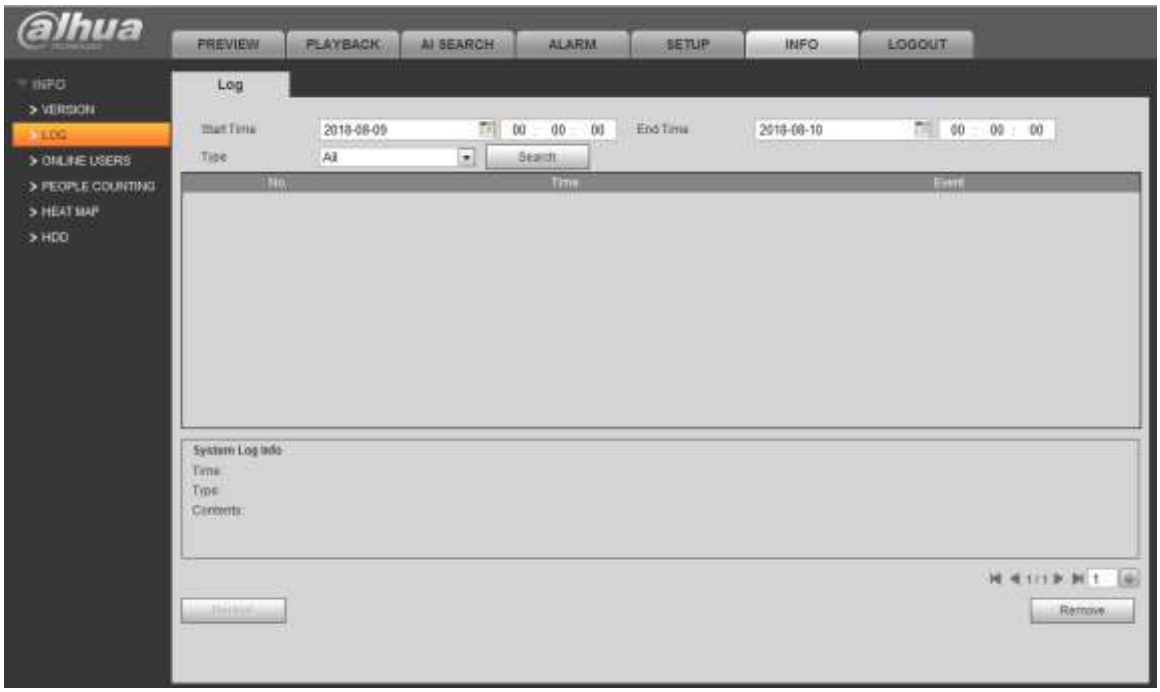
2.2.8 Check Log

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



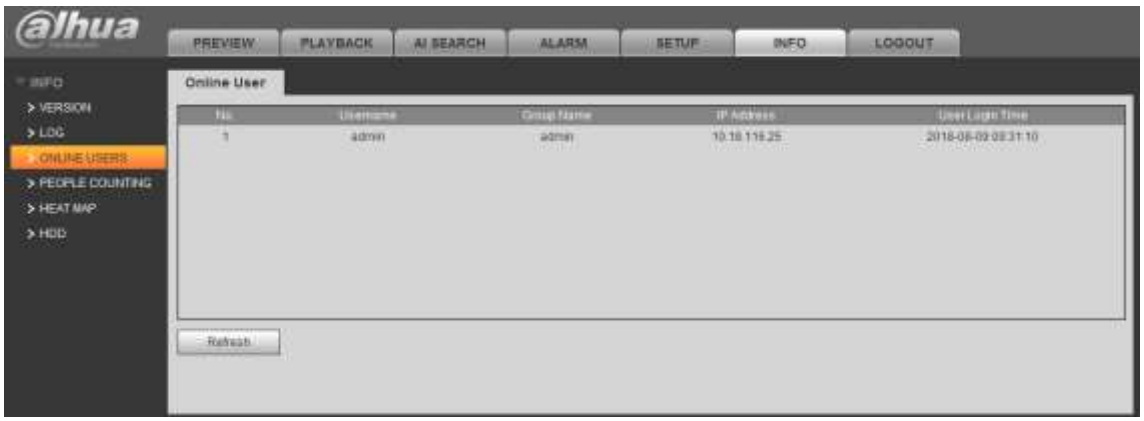
2.2.9 Check Online User

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.

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

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.

Figure 2-13

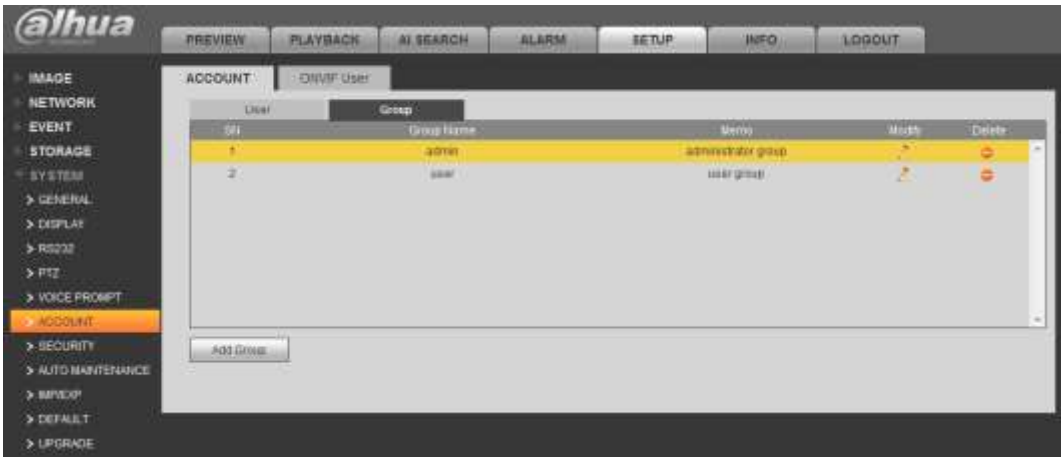
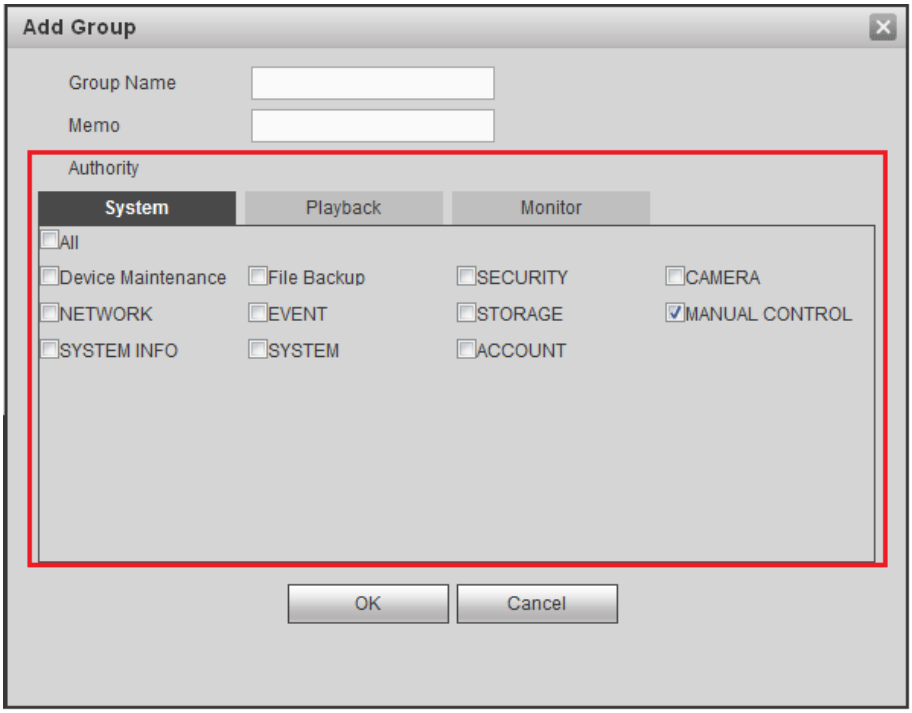


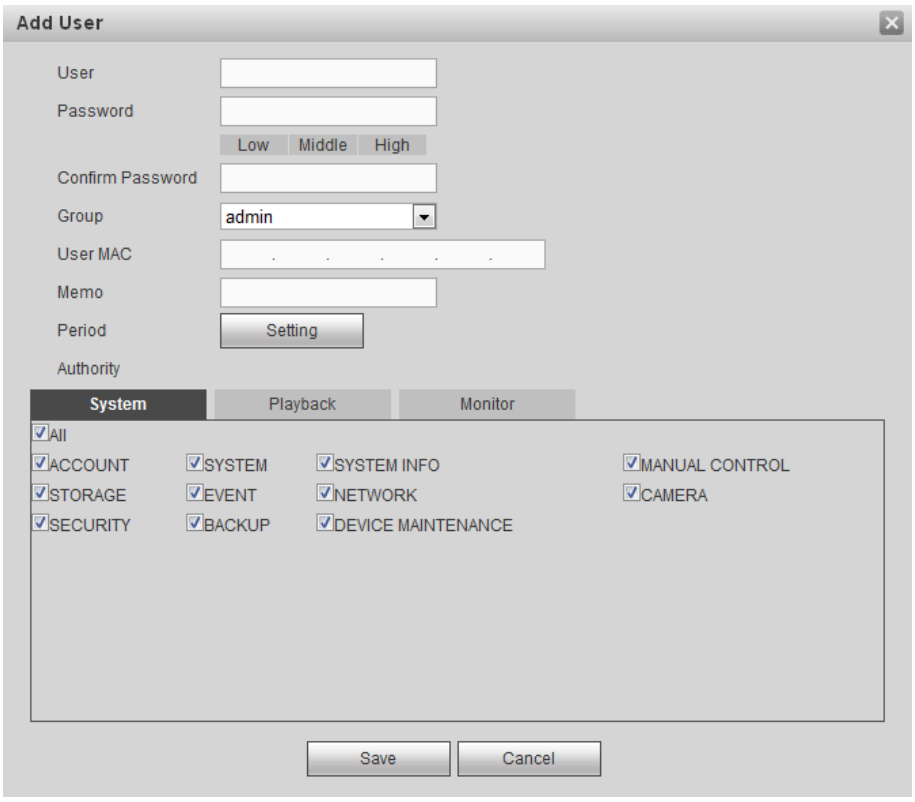
Figure 2-14



Step 2

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

Figure 2-15



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

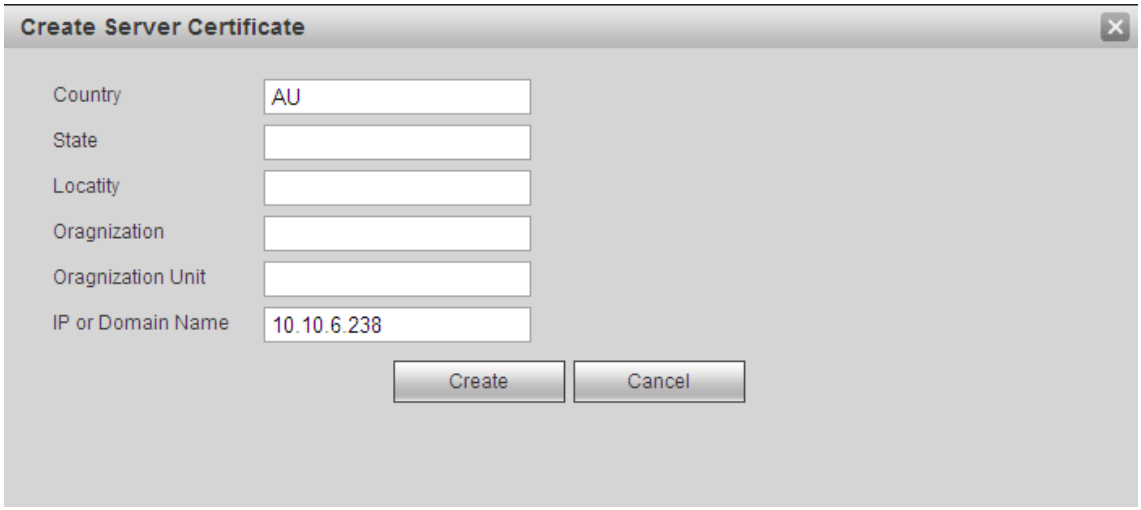
Step 2

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



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.

Figure 2-18

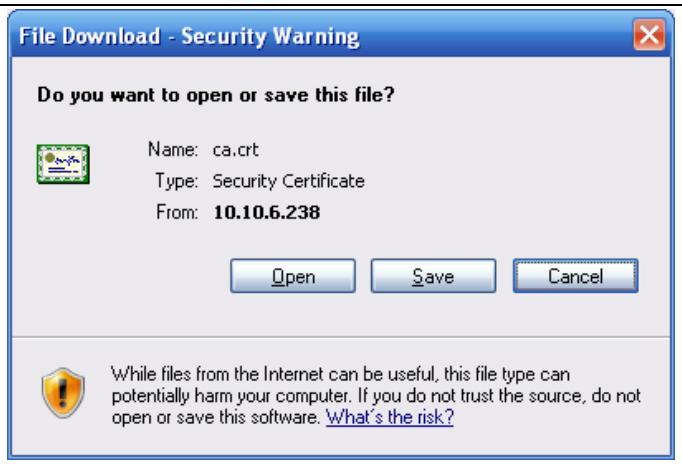
Step 3

Download root certificate.

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

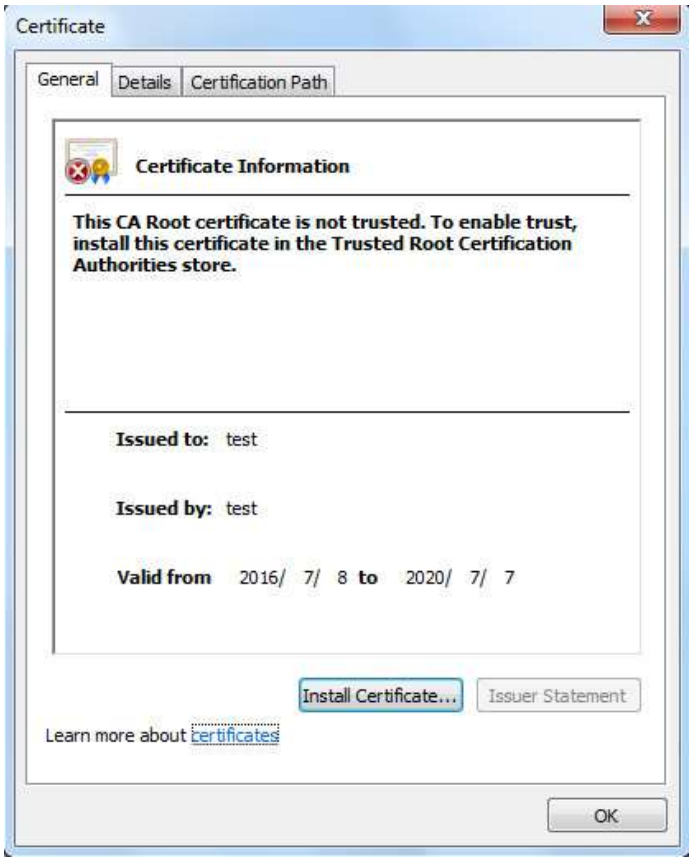
1. Select “Setting > Port > HTTPS”, the system will display “HTTPS” Interface.
2. Click “Download Root Certificate”, the system will display the interface of “File Download”.

Figure 2-19



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

Figure 2-20

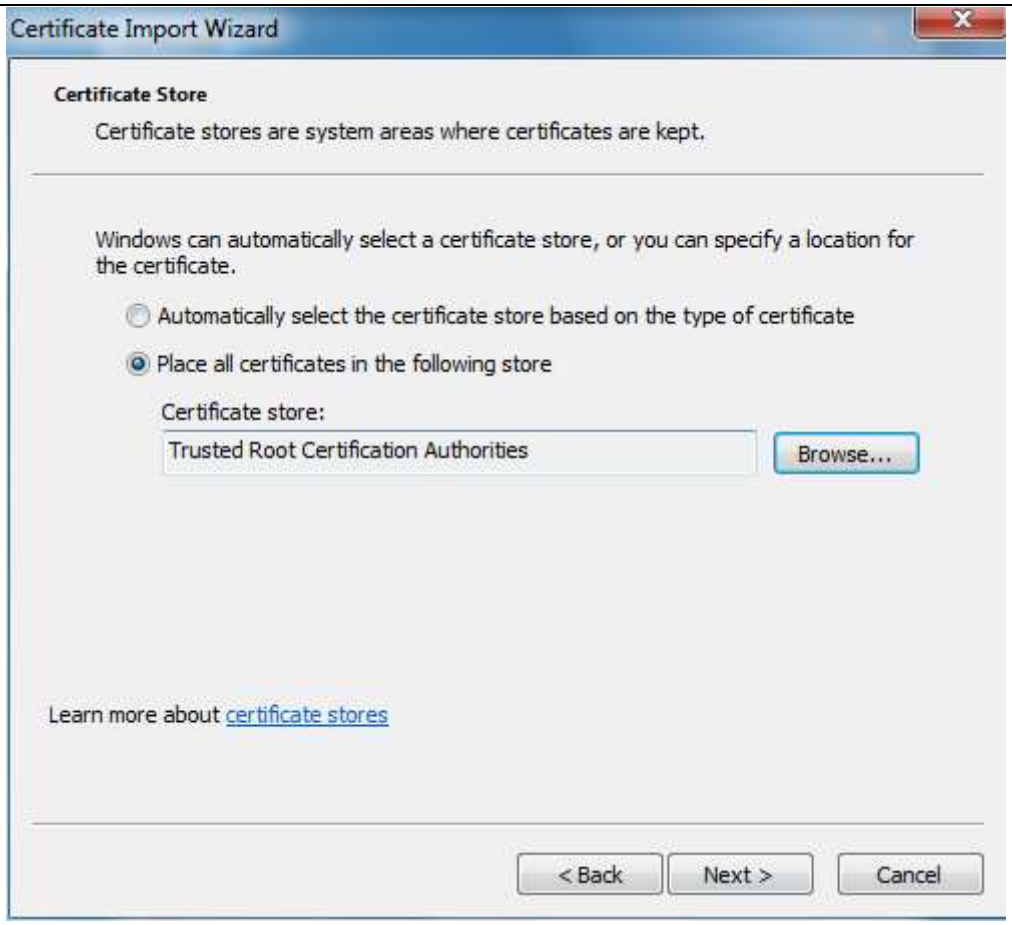


4. Click “Install Certificate”, the system will display the interface of “certificate Import Wizard”.

Figure 2-21

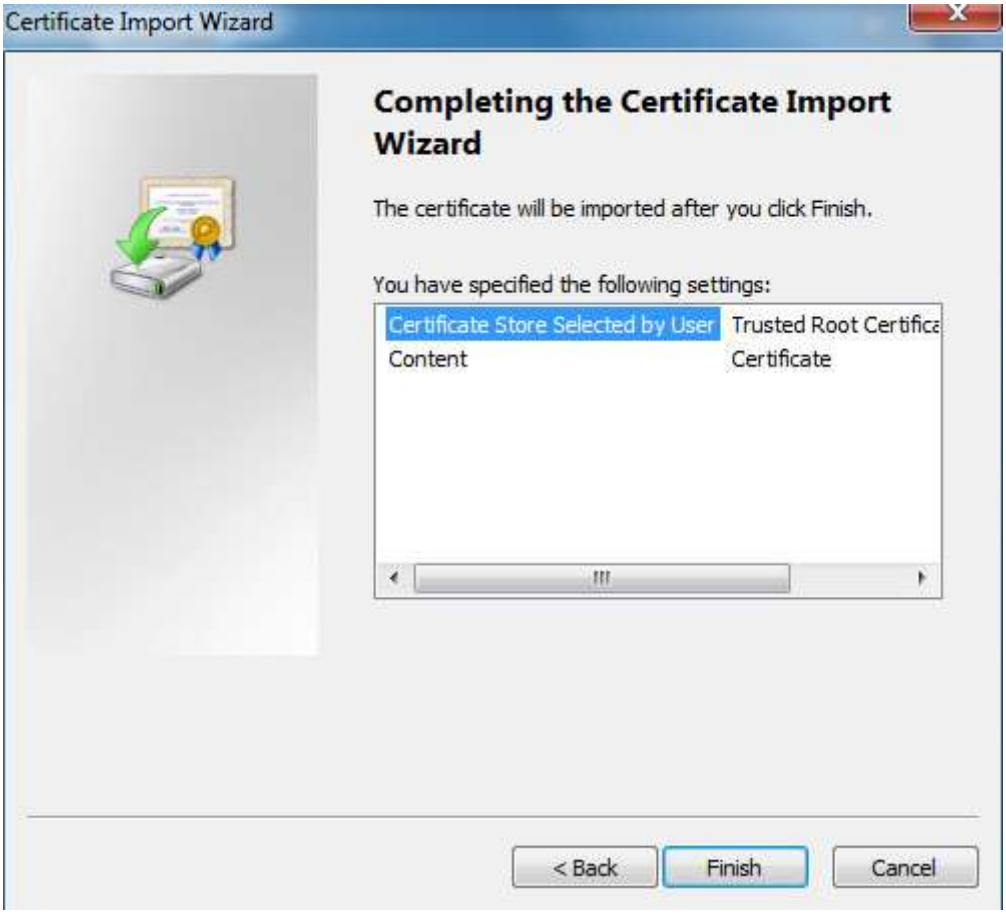
5. Click “Next”, the system will display the interface of selecting certificate storage area.

Figure 2-22



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.

Figure 2-24

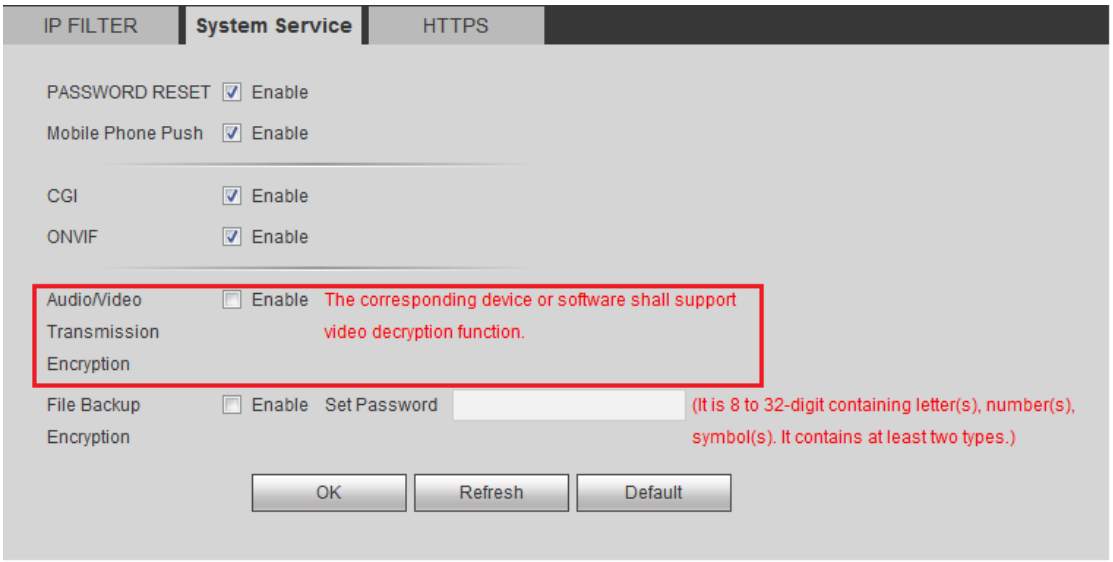
2.3.4 Audio Video Transmission Encryption

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



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.

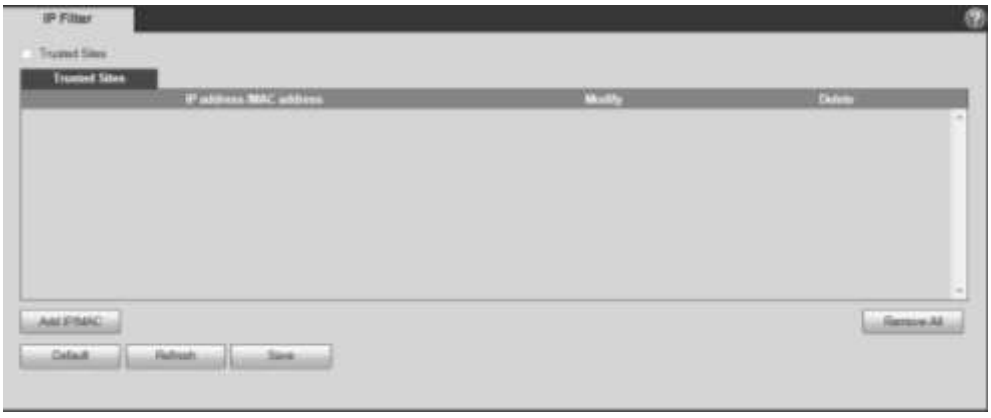
Note

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



2.3.6 Limit Max Concurrency of Login

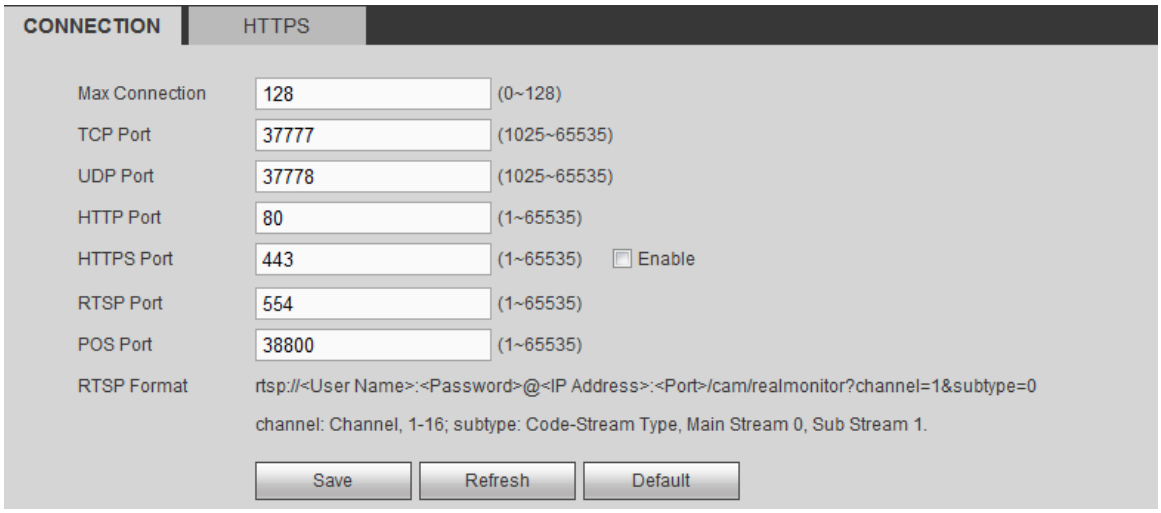
It is to limit the number of clients (WEB client, platform client and mobile client etc.) that devices allow to log in at the same time, help the device limit malicious flow attack and

protect normal operation of important business.

Operation Method

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

Figure 2-27



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

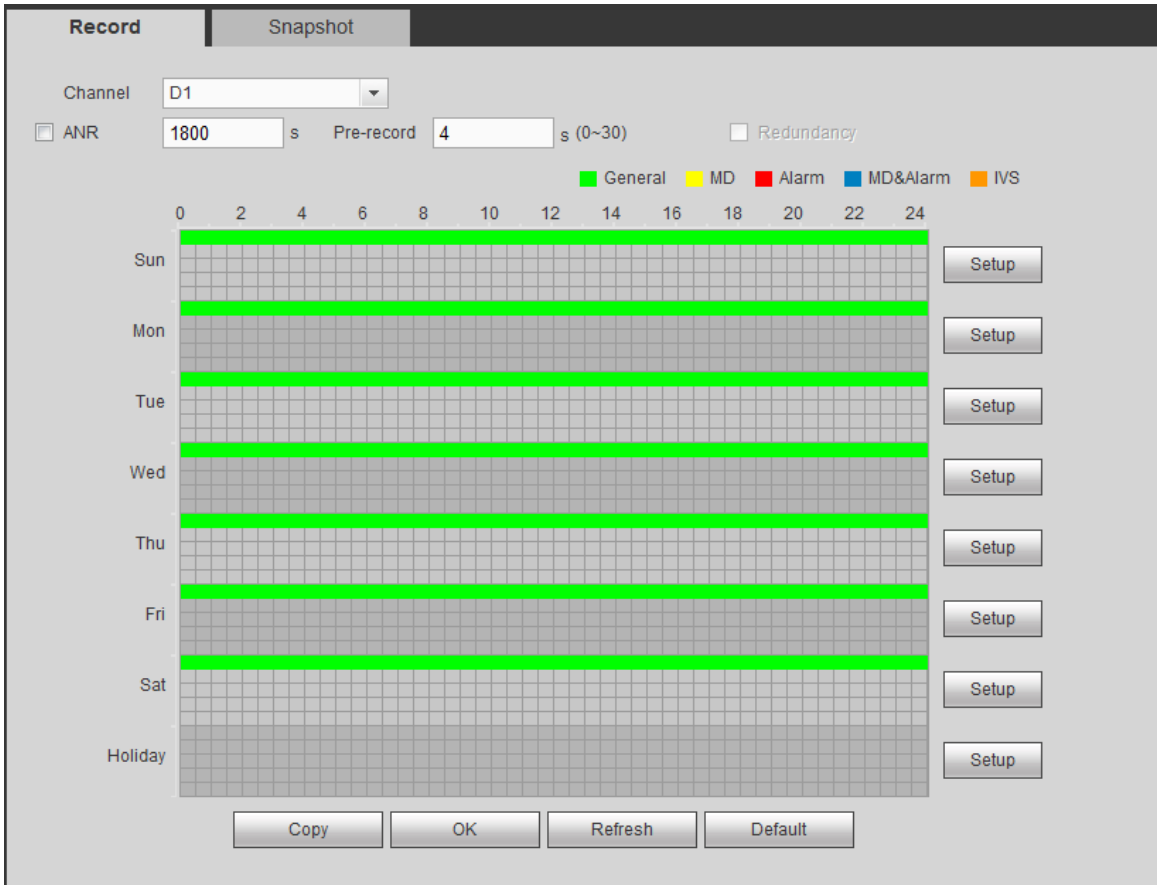
the period when the network is disconnected, so as to guarantee the integrity of the video recording of the IPC channel in the NVR equipment. The function can help you better ensure the integrity if your video.

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

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

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

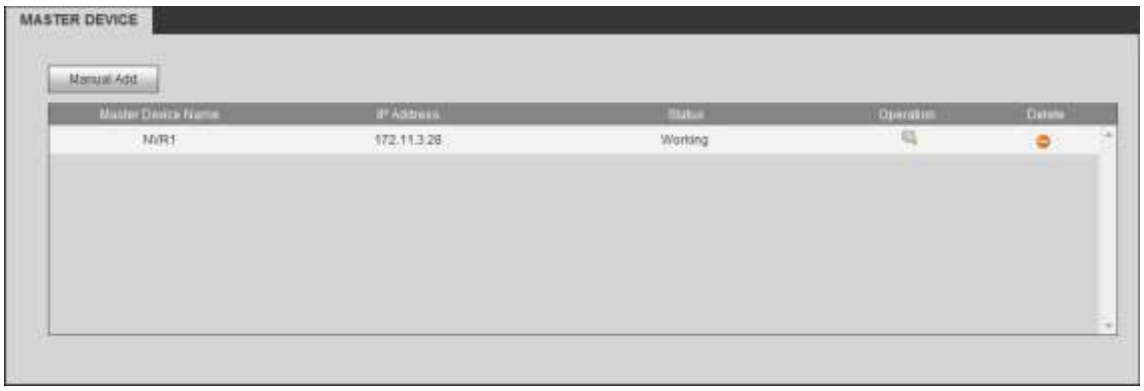
Step 1

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



- 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

Step 2

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

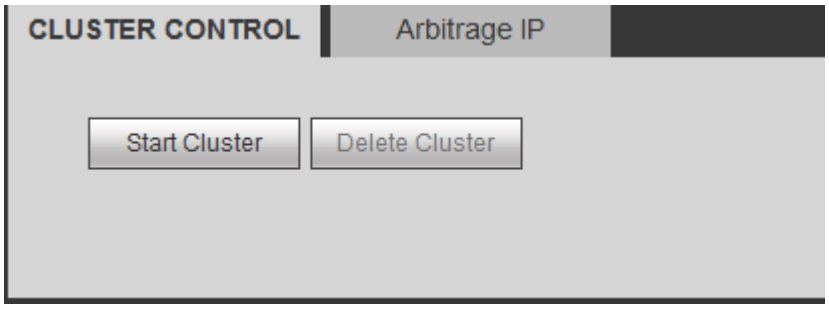
Note

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

Select “Setting > Cluster Service > Cluster Control > Cluster Control” and enable cluster function.

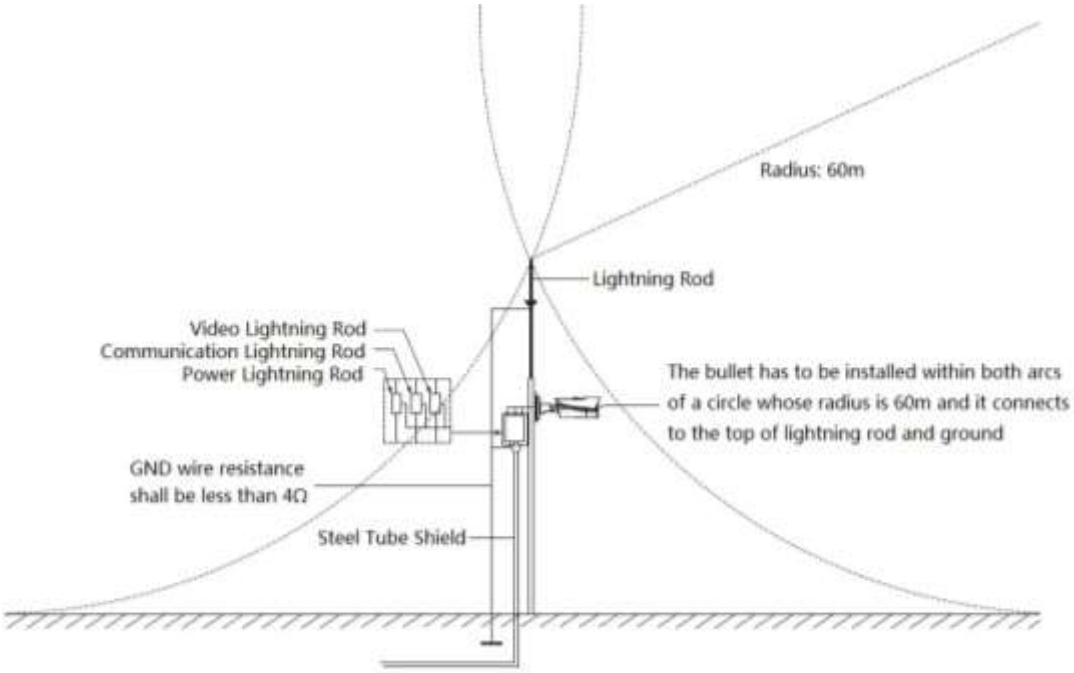
Figure 2-35



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.

Figure 3-1

3.3 Config AP Hotspot Securely

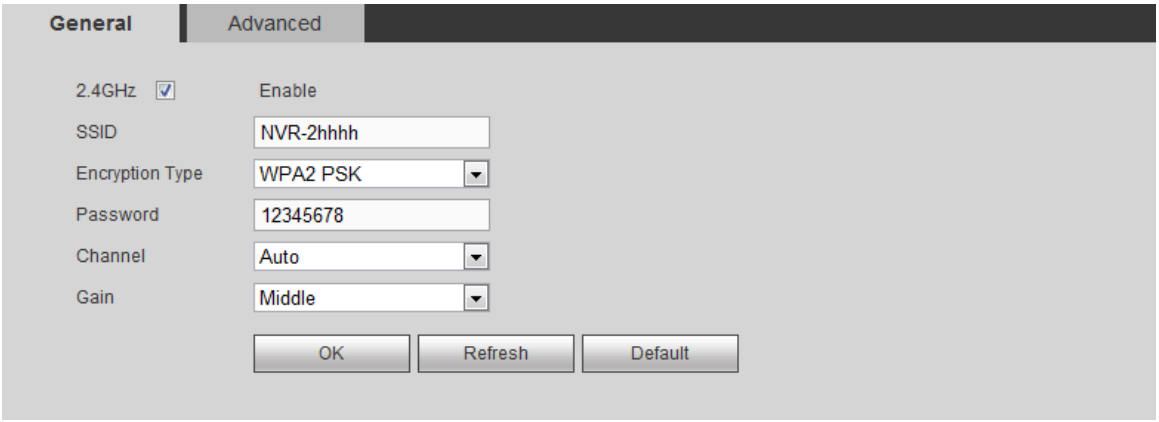
If you need to use the device'AP hotspot function for network deployment, it is recommended that you configure the AP hotspot function safely.

- 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.

Figure 3-2



3.4 Config SMTP Securely

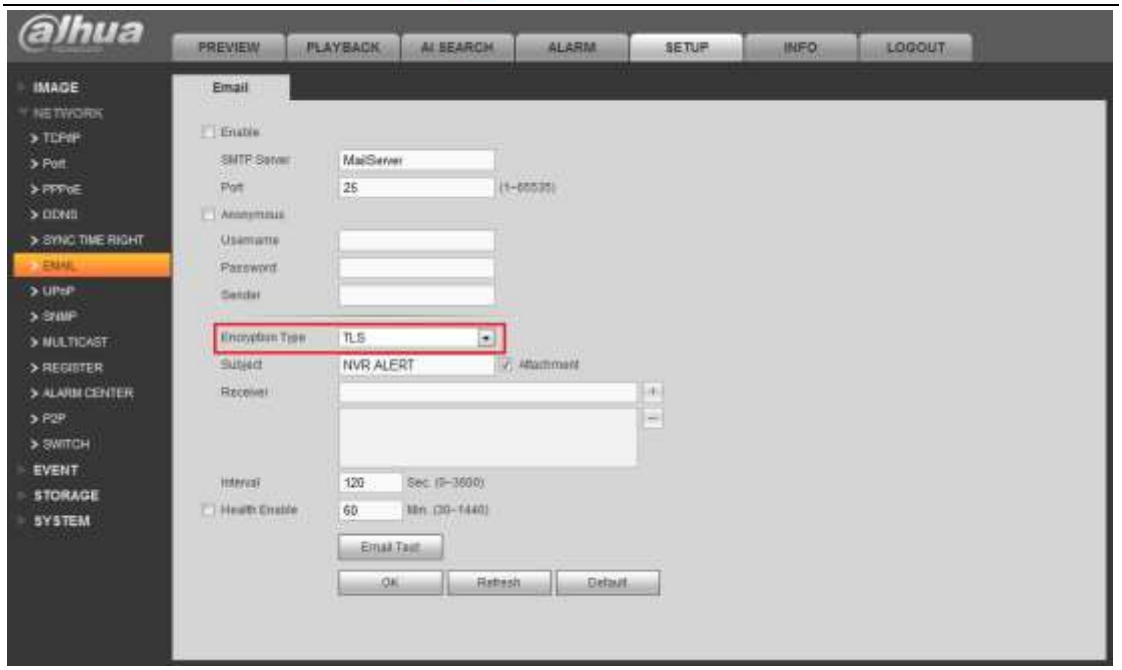
SMTP function is integrated to cooperate with the device abnormity alarm notification, if you need to listen to the device abnormity and notify you via email; it is recommended that you conform to the following application methods:

- 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



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

- 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 https://www.dahuatech.com/service/resource.html 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 cybersecurity@dahuatech.com to report the hole. Please encrypt the email if it concerns the sensitive information.