

Event Detection Intelligent Server

Deployment Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Foreword

General

This manual introduces the functions and operations of the Event Detection Intelligent Server (hereinafter referred to as "the Server").

Models

Device	Model
1U	DH-IVS-IP8000-E-GU1
2U	DH-IVS-IP8000-2E-GU2, DH-IVS-IP8000-3E-GU2, DH-IVS-IP8000-4E-GU2, DH-IVS-IP8000-5E-GU2, and DH-IVS-IP8000-6E-GU2

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
© <u>∽∿</u> TIPS	Provides methods to help you solve a problem or save time.
Π ΝΟΤΕ	Provides additional information as a supplement to the text.

Revision History

Revision Content	Release Time	Revision Content	
V1.0.0	First release.	December 2021	

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

• The manual is for reference only. Slight differences might be found between the manual and the product.



- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.



Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements

- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Only use the device within the rated power range.
- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.

Installation Requirements

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- Connect the device to the adapter before power on.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.



Table of Contents

Foreword	l
Important Safeguards and Warnings	
1 (Optional) Deploying Server	1
1.1 Before Deployment	1
1.1.1 Preparing USB Drive and Installation Package	1
1.1.2 System Requirements	1
1.2 Installing CentOS System and Program	2
1.2.1 Preparing USB Flash Drive	2
1.2.2 Selecting Bootup Menu	4
1.2.3 Selecting USB Flash Drive	4
1.2.4 Selecting Operating System	5
1.2.5 Selecting Language	5
1.2.6 Setting System Time	6
1.2.7 Selecting Software Installation Mode	7
1.2.8 Configuring Partition	9
1.2.9 Starting Installation	14
1.2.10 Setting Password	15
1.2.11 Restarting	16
1.2.12 Installing Basic Package and Driver	17
2 Service Software Installation	21
2.1 Modifying Script	21
2.2 Installing Service Software	24
3 Deploying Platform	26
3.1 Logging in to Unified Operation Platform	26
3.2 Initializing Unified Operation Platform	28
3.2.1 Searching Nodes	28
3.2.2 Deploying MySQL	29
3.2.3 Selecting Configuration Mode	30
3.3 Managing Server	31
4 Installing Event Detection Server	35
4.1 Managing Product	35
4.2 Installing New PaaS Cluster	37
4.3 Configuring Behavior SaaS	43
4.4 Configuring Operator	47
5 Applying for Encryption	49



	5.1 Checking Dongle	49
	5.2 Software-based Encryption	49
	5.3 Hardware-based Encryption	54
Ap	opendix 1 Cybersecurity Recommendations	56



1 (Optional) Deploying Server

If it is a baseline server, you can skip this chapter and install the service software directly. For details, see "2 Service Software Installation".

1.1 Before Deployment

Before deployment, you need to prepare all installation packages and required devices.

1.1.1 Preparing USB Drive and Installation Package

Before deployment, you need to prepare USB drive and download the following packages from GDP.

- CentOS 7.4 system package (material No.: 2.4.01.01.12619)CentOS-7-x86_64-Everything-1708.iso One USB flash drive (8 GB or larger size, 16 GB is recommended).
- Basic package (material No.: 2.7.07.01.01317)General_IVS-CentOS7.4-Base_CPU-X86-MD5-****_V1.***.******.*.R.******.tar.gz
- Atlas driver packageGeneral_IVS-CentOS7.4-Base_Driver_Atlas-X86-MD5-****_V1.***.*********.*.R.******.tar.gz
- Program packageGeneral_IVS-IP8000-E_ChnEng_MD5-****_V1.***.***********.tar.gz
- Client installation packageGeneral_IVS-IBC_Base_IS_V1.0.0.******.R.******.exe



The package name varies with version and release date.

1.1.2 System Requirements

Table 1-1 System requirements

Parameter	Description
Operating system	CentOS 7.4
Kernel version	3.10.0-693.el7.x86_64
CPU	Intel Xeon E3-1275 v5 @3.50 GHz
Intel graphics	P530
Graphics	AIX3200



1.2 Installing CentOS System and Program

Prepare the USB flash drive, and install the CentOS system.

You must execute the root commands to configure the settings.

1.2.1 Preparing USB Flash Drive

Prepare the USB flash drive for installing CentOS system of the server.

Prerequisites

- A USB flash drive with size≥8 GB.
- A computer installed with UltraISO.
- CentOS 7.4 system package was saved to the computer.

Background Information



Skip this chapter if CentOS 7.4 system has been installed on the server.

Procedure

- <u>Step 1</u> Double-click 🔂 to open UltralSO.
- <u>Step 2</u> Select **File** > **Open**, select the CentOS 7.4 installation package, and then click **Open**.

Figure 1-1	Open file
------------	-----------

🕥 UltralSO				- 🗆 >	<
File Actions Bootable Tools Opti	ons Help				
New >	🗟 🥝 🥭 🔍 🥥	🚯 🛛 Total Size: 📃	OKB 0% of C	D 650MB (+ 650MB)	
Reopen	🏂 🗙 📂 🗔 🔞 🏶 🍏 🛛 F	Path: /			
Solution (CD/DVD)	Filename	Size Type		Date/Time	LE
Image: Save Ctrl+S Image: Save As Simulated Save					
Create Checksums Verify Checksums					
Open Project File Ctrl+Alt+O Save Project File As Ctrl+Alt+S					
Import IML Compile IML to ISO	<				>
Properties	🎁 📂 🗙 🗖 🥳 🖗 🖉 📑	Path: D:\软件\UltralSO123			
🕞 Exit	Filename	Size Type		Date/Time	^
backup drivers	r 🛅 backup i drivers	Folde Folde Folde	er l	2020-11-19 19:50 2020-11-19 19:50 2020 11 19 19:50	
lang	History by	45 KB Tevt	n Document	2020-11-13 13:30	
Documents		78 KB Appli	cation Extension	2020-07-00 10:07	
	isoshl64.dll	152 KB Appli	cation Extension	2020-07-13 09:10	
	License.txt	4 KB Text	Document	2008-02-28 15:59	
i	Readme.txt	3 KB Text	Document	2007-04-17 16:32	
	👔 ultraiso.chm	427 KB Comp	piled HTML Hel	2009-08-06 11:48	
< >	💿 Ultral SO. exe	5.319 KB Apoli	cation	2020-11-01 12:31	\sim
Copyright (c)2002-2020 E2	ZB Systems, Inc.	Image: 0 files, 0 KB	Loc	al: 9 files, 6818 KB:	

<u>Step 3</u> Select **Bootable** > **Write Disk Image**.





Figure 1-2 Write disk image (1)

Step 4 Configure Disk Drive and Write Method, and then click Write.



\square

Generally, you only need to leave them as default.

Message:					Save
Time	Event				
T III C	V Godewe 1	010.0.0			
	windows i	0 V10.0 Dullu 13041			
<					
Diek D	rive:			1 hifu	
DISK D	inve.			only	
Image	File:	Colorado de la			
Image Write Met	File: hod: USB-HDD+	Calcultura V	ad I Porta		÷
Image Write Met	File: hod: USB-HDD+		and Spinked		
Image Write Met Hide Boot Parti	File: hod: USB-HDD+ ition: None	~	uat EDVA-st	Xpress Boot	÷
Image Write Met Hide Boot Parti Done:	File: hod: USB-HDD+ ition: None 0%	Elapsed:	00:00:00	Xpress Boot Remain:	00:00:
Image Write Met Hide Boot Parti Done:	File: hod: USB-HDD+ ition: None 0%	Elapsed:	00:00:00	Xpress Boot Remain:	00:00:
Image Write Met Hide Boot Parti Done:	File: hod: USB-HDD+ ition: None 0%	Elapsed:	00:00:00	Xpress Boot Remain: Speed:	00:00: 0KB/

<u>Step 5</u>

Click **Yes** in the pop-up window.

The system starts writing data, and the progress bar is displayed.

<u>Step 6</u> After successfully burning the USB drive, click **Close**.

1.2.2 Selecting Bootup Menu

Background Information

Insert the USB flash drive into the server, restart the server, and then select an option similar to boot manager.

\square

Different servers have different boot options. Refer to the options of the actual server.

1.2.3 Selecting USB Flash Drive

Background Information

Select the corresponding USB flash drive.



Figu	re 1-4 Select USB flash drive	
	P1:NUME ▲ MAC:00-00-00-00-00-00 MAC:3C-6A-2C-B1-4A-A2 MAC:3C-6A-2C-B1-4A-A3	
	EFI Shell P0:ST4000NM000A-2HZ100 P1:Kingston DataTraveler 3.0	

1.2.4 Selecting Operating System

Background Information

Select Install CentOS 7.

Figure	1-5	Select	onerati	nas	vstom
Figure	1-2	Select	operati	nys	ystem

Install CentOS 7			
Test this media & instal	1 CentOS 7		
Troubleshooting>			

1.2.5 Selecting Language

Procedure

- <u>Step 1</u> Select **English** > **English** (United States).
- <u>Step 2</u> Click **Continue** at the lower-right side.



Figure 1-6 Installation

What language would you like to	use during the installation process?	
English	English >	English (United States)
Afrikaans	Afrikaans	English (United Kingdom)
አማርኛ	Amharic	English (India)
العربية	Arabic English (Australia)	English (Australia)
অসমীয়া	Assamese	English (Canada)
Asturianu	Asturian	English (Denmark)
Беларуская	Belarusian	English (New Zealand)
Български	Bulgarian	English (Neev Zealand)
বাংলা	Bengali	English (Hong Kong SAR China)
Bosanski	Bosnian	English (Philippines)
Català	Catalan	English (Singapore)
Čeština	Czech	English (South Africa)
Cymraeg	Welsh	English (Zambia)
Dansk	Danish	English (Zimbabwe)
Deutsch	German	English (Botswana)
Ελληνικά	Greek	Engush (Antigua & Barbuda)
Español	Spanish	
Eesti	Estonian	
Euskara	Basque	
فارسى	Persian	
Suomi	Finnish	
Français	French	
Galego	Galician	
neni-fl	Calimonti	
	8	

1.2.6 Setting System Time

Procedure

<u>Step 1</u> On the **INSTALLATION SUMMARY** interface, click **DATE & TIME**.

Figure 1-7 Modify time (1)







Figure 1-8 Modify time (2)



<u>Step 3</u> Click **Done** at the upper-left side.

1.2.7 Selecting Software Installation Mode

Procedure

<u>Step 1</u> On the **INSTALLATION SUMMARY** interface, click **SOFTWARE SELECTION**.



Figure 1-9 Installation (1)



Step 2 Select Minimal Install.

Figure 1-10 Installation (2)

se Environment	Add-Ons for Sel	ected Environment	
Minimal Install Besic Functionality.			

Step 3 Click **Done** at the upper-left side.



1.2.8 Configuring Partition

Procedure

<u>Step 1</u> On the **INSTALLATION SUMMARY** interface, click **INSTALLATION DESTINATION**.

	Figure 1-11 Configure p	partition (1)
CentOS	INSTALLATION SUMMARY	CENTOS LINUX ALTARCH 7 INSTALLATION
	DATE & TIME Asia/Shanghai timezone LANGUAGE SUPPORT English (United States)	KEYBOARD English (US)
	SOFTWARE INSTALLATION SOURCE Local media SYSTEM	SOFTWARE SELECTION Minimal Install
	INSTALLATION DESTINATION Automatic partitioning selected	KDUMP Kdump is enabled SECURITY POLICY No profile selected
		Out Ebigin lessallation We work teach your diaks until your clock 'Begin hestallatio

Step 2Select USB drives from Local Standard Disks, select Automatically configure
partitioning and I would like to make additional space available from Other Storage
Options, and then click Done at the upper-left side. The system starts reclaiming disk
space.



Figure 1-12 Configure partition (2)



<u>Step 3</u> On the **RECLAIM DISK SPACE** interface, click **Delete all**, and then click **Reclaim space**.

Figure 1-13 Configure partition (3)

Disk.	Manne	Eile Sustem	Reclaimable Space	Action		
119.2 GIB TS128GMTE652T	nyme0n1	rae system	necialitative space	Preserve		
/boot/efi (CentOS Linux Linux 7.4.1708 for aarch64)	nvme0n1p1	EFI System Partition	Not resizeable	Preserve		
/boot (CentOS Linux Linux 7.4.1708 for aarch64) cla	nvmeOn1p2 nvmeOn1p3	xts physical volume (LVM)	Not resizeable	Preserve		
Free space 3726 GiB ATA ST4000NM000A-2HZ	sda	ext4	1334.5 KiB 3726.02 GiB total	Preserve		
Preserve Delete Shrink						Delete all
Preserve Delete Shrink disks; 3845.26 GiB reclaimable space (in file systems)						Delete all
Preserve Delete Shrink disks; 3845.26 GiB reclaimable space (in file systems)			Installation	enuires a to	Total select	Delete all ed space to reclaim: (MB for system data



Helpł

Figure 1-14 Configure partition (4)

and a				Etc. E. A.	R. J. L. F.	A		
/sk			Name	File System	Reclaimable Space	Action		
119.2 GiB	TS128GMT	E652T	nvme0n1		100.00	Delete		
- /boot/	efi (CentOS L	Linux Linux 7.4.1708 for aarch64)	nvme0n1p1	EFI System Partition	Not resizeable	Delete		
- /boot ((CentOS Linu	x Linux 7.4.1708 for aarch64)	nvmeOnlp2	xfs	Not resizeable	Delete		
cla		nvmeOnlp3 physica	physical volume (LVM)	Not resizeable 13345 KiB	Delete			
Free space 3726 GIB ATA ST4000NM000A-2HZ								
			sda	ext4	3726.02 GiB total	Delete		
Preserve	Delete	Shrink						Preserve all
Preserve disks; 3845	Delete 5.26 GiB rect	Shrink aimable space (in file systems)			Installation r	Total selec requires a tota	ted space to il of 1111.8 7	Preserve all reclaim: 3845.26 (Filb Tor system d

Go back to the INSTALLATION SUMMARY interface, and then click INSTALLATION <u>Step 4</u> **DESTINATION**.



Minimal Install

KDUMP Kdump is enabled

SECURITY POLICY

No profile selected

Quit

Figure 1-15 Configure partition (5)

Local media

INSTALLATION DESTINATION Automatic partitioning selected

NETWORK & HOST NAME Not connected

SYSTEM S

5

		We work touch your disks until your click 'Begin Installati	301° .
<u>Step 5</u>	Select USB	B drives from Local Standard Disks, select I will configure partitioning	j and I
	would like	ce to make additional space available from Other Storage Options , ar	าd then
	click Done	e at the upper-left side.	



Figure 1-16 Configure partition (6)

INSTALLATION DESTINATION	CENTOS LINUX ALTARCH 7 INSTALLATIO
Done 3	Help ⁱ
evice Selection	
Select the device(s) you'd like to install to. They will be left untouched until	you click on the main menu's "Begin Installation" button.
Local Standard Disks	
119.24 GiB 3726.02 GiB	14.44 GiB
	DebeTamular 2.0
ISI28GMTE6S2T ATAST4000NM000A-2H2 Kingsto nyme0n1 / 59.62 GiB free sda / 90.38 GiB free sdb	n Data Iraveler 3.0
Specialized & Network Disks	Disks aert Unselected here will not be touch
Add a disk	
	Dicks laft unrelacted here will not be touch
ther Storage Ontions	Links let unselected here will hok be touch
Partitioning	
Automatically configure partitioning. I will configure partitioning.	2
V I would like to make additional space available.	4
Enconting	
Encrypt my data. You'll set a passphrase next.	

<u>Step 6</u> Select **Click here to create them automatically**. The system automatically creates partitions.



MANUAL PARTITIONING	CENTOS LINUX ALTARCH 7 INSTALLATION 🖽 us Helpi
• New CentOS Linux AttArch 7 Installation You haven't created any mount points for your CentOS Linux AlbArch 7 installation yet. You can: • Click-here to create them automatically. • Create new mount points by clicking the '4' button. New mount points will use the following partitioning scheme: LVM	
	When you create mount points for your CentOS Linux AltArch 7 installation, you'll be able to view their details here.
+ - C AVAILABLE SPACE 3845.27 GIB 2 storage devices selected	Reset All

<u>Step 7</u> Allocate disk space.

• The total disk space < 1 TB

Do not allocate space separately to /home. Select /home, and then click - at the lower side to



delete the directory.

• The total disk space > 1 TB

Allocate 200 GB or more to the / directory, and allocate the remaining space to /home.

igure i	- S Conngu		
New CentOS Linux AltArch 7 Installation		sdal	
DATA /home cla-home	3178.37 GiB	Mount Point: /boot/efi	Device(s):
SYSTEM /boot dd2	1024 MiB	Desired Capacity: 200 MiB	
/boot/efi	200 MiB >		
nora I chanat	500 GiB		
swap cla-swap	15.69 GiB	-	ATA ST4000NM000A-2HZ (sda) and 1 other
		12	
			Modfy
		Standard Partition	
		File System:	
		Reformat	
		Label:	Name: sdal
			Update Settings
+ - C			Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.
AVAILABLE SPACE 150.01 GIB 3845.27 GIB			
2 storage devices selected			Reset All

Figure 1-18 Configure partition (8)

Table 1-2 Configure partition

Sequence	Partition	Capacity
1	boot	1 GB
2	swap	32 GB
3	/	1 TB
4	/home	Allocate the remaining space to / home

Step 8 Click Accept Changes to finish partitioning.



Figure 1-19 Configure partition (9)

Order	Action	Туре	Device Name	Mount point
1	Destroy Format	ext4	sda	
2	Destroy Format	EFI System Partition	nvme0n1p1	
3	Destroy Format	xfs	nvme0n1p2	
4	Destroy Format	swap	cla-swap	
5	Destroy Device	lymly	cla-swap	
5	Destroy Format	xfs	cla-root	
7	Destroy Device	lymly	cla-root	
3	Destroy Device	lvmvg	cla	
9	Destroy Format	physical volume (LVM)	nvme0n1p3	
10	Destroy Device	partition	nvme0n1p3	
11	Destroy Device	partition	nvme0n1p2	
12	Destroy Device	partition	nvme0n1p1	

1.2.9 Starting Installation

Background Information

On the **INSTALLATION SUMMARY** interface, click **Begin Installation**.



Figure 1-20 Installation



1.2.10 Setting Password

Procedure

<u>Step 1</u> On the **CONFIGURATION** interface, click **ROOT PASSWORD**.



Figure 1-21 Set password (1)

	CONFIGURATION		CENTOS LINUX AL	TARCH 7 INSTALLATION
CentOS	USER SETTINGS			
	ROOT PASSWORD Root password is not set	2	USER CREATION No user will be created	
EN PHY				
11112				
anti Alla				
BALLA &				
	• Setting up the installation environment			
	CentOS Virtual Virtualization in CentOS, vi wiki.centos.org/SpecialinterestGroup	ization SIG rtualization of CentOS.		

<u>Step 2</u> Enter the password, and then click **Done** at the upper-left side.

Figure 1-22 Set password (2)

ROOT PASSWORD	for the part of the	ST I I	CENTOS LINUX ALTA	RCH 7 INSTALLATION
	The root account is used i	or administering the system. Enter a password for the root user.		
	Root Password:	•••••		
		Good		
	Confirm	•••••		

1.2.11 Restarting

Background Information

The installation takes 10 minutes to 20 minutes. After installation, click **Reboot**. Wait for the server to restart, and then you can remove the USB drive from the server.



Figure 1-23 Restart

æ	CONFIGURATION	CENTOS LINUX ALT	ARCH 7 INSTALLATION
CentOS	USER SETTINGS		
	ROOT PASSWORD Root password is set	USER CREATION No user will be created	
in indian		_	
Z BARREN			
S.			
	Completel		
		CentOS Linux AltArch is now successfully installed and reac Go ahead and reboot	y for you to use! to start using it!
			Reboot
	$\hat{\mathbf{A}}$. Use of this product is subject to the license agreeme		

1.2.12 Installing Basic Package and Driver

Procedure

<u>Step 1</u> Log in to the CentOS system.

For first-time login, we recommend logging in with root.

<u>Step 2</u> Enter the **date** command to check whether the date and time of the server are correct. If not, enter the following command with actual time.

Figure 1-24 Change system time



 \square

The first command is to set the system time. The second one is to write the time to the motherboard, which must be executed.

<u>Step 3</u> Change IP address of network card.



1. Execute the cd /etc/sysconfig/network-scripts/

command to go to the network configuration path, and then execute the **Is**

command to view the number of network cards.[root@localhost network-scripts]# Is

ifcfg-eno1	ifdown-post	ifup-bnep	ifup-routes
ifcfg-eno2	ifdown-ppp	ifup-eth	ifup-sit
ifcfg-lo	ifdown-routes	ifup-ippp	ifup-Team
ifdown	ifdown-sit	ifup-ipv6	ifup-TeamPort
ifdown-bnep	ifdown-Team	ifup-isdn	ifup-tunnel
ifdown-eth	ifdown-TeamPor	t ifup-plip	ifup-wireless
ifdown-ippp	ifdown-tunnel	ifup-plusb	init.ipv6-global
ifdown-ipv6	ifup	ifup-post	network-functions
ifdown-isdn	ifup-aliases	ifup-ppp	network-functions-ipv6

As shown in the above-mentioned information, the server has two network cards.

2. Execute the ethtool
command to check which network card is connected to network.[root@localhost
network-scripts]# ethtool eno1
Settings for eno1:
Supported ports: [TP]
Supported link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supported pause frame use: No
Supports auto-negotiation: Yes
Supported FEC modes: Not reported
Advertised link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: No
Advertised auto-negotiation: Yes
Advertised FEC modes: Not reported
Speed: Unknown!
Duplex: Unknown! (255)
Port: Twisted Pair
PHYAD: 2
Transceiver: internal
Auto-negotiation: on
MDI-X: Unknown (auto)
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x0000007 (7)
drv probe link
Link detected: ves

The network card with the returned result Link detected: Yes is connected to network.



3. Execute the vi ifcfg-eno1 command and press i to edit the network card configuration file. After editing, press the Esc key, and then input :wq to save the configuration.[root@localhost network-scripts]# vi ifcfg-eno1 TYPE=Ethernet PROXY METHOD=none BROWSER_ONLY=no BOOTPROTO=static #Obtain static IP DEFROUTE=yes IPV4_FAILURE_FATAL=no IPV6INIT=yes IPV6_AUTOCONF=yes IPV6 DEFROUTE=yes IPV6_FAILURE_FATAL=no IPV6_ADDR_GEN_MODE=stable-privacy NAME=eno1 UUID=562aca55-52d3-40fb-8d0d-70eba5f1831f DEVICE=eno1 ONBOOT=**yes** #Launch on startup IPADDR=172.26.8.247 #Change to actual IP GATEWAY=**172.26.0.1** #Change to actual gateway NETMASK=**255.255.0.0** #Change to actual subnet mask

- <u>Step 4</u> Execute the **systemctl restart network** command to restart the network.
 After configuring the network, you can remotely log in to the server through SecureCRT or Xshell and according to SSH protocol. Here we use Xshell as an example.
- <u>Step 5</u> Log in to the server remotely through Xshell.
- <u>Step 6</u> Upload basic package and driver.
 - 1. Execute the **mkdir /home/base** command to go to the /home/base folder.
 - 2. Execute the **cd /home/base** command to go to the /home/base folder.
 - 3. Click in the Xshell navigation bar 🚺 , and then move the basic package and driver
 - from the local PC to the /home/base directory.
 - 4. Execute the **II**

```
command to view the /home/base folder, and confirm that the basic package and the driver are uploaded.[root@localhost ~]# mkdir /home/base
```

```
[root@localhost ~]# cd /home/base
```

```
[root@localhost base]# II
```

```
total 1085180
```

-rw-r--r-. 1 root root 793805331 Nov 20 18:03

General_IVS-CentOS7.4-Base_CPU-X86-MD5-c8ef_V1.003.0000001.0.R.201117.tar.g

```
-rw-r--r--. 1 root root 317414755 Nov 20 21:23
```

General_IVS-CentOS7.4-Base_Driver_Atlas-X86-MD5-e9e5_V1.003.0000001.0.R.2



01217.tar.gz

<u>Step 7</u> Execute the **sh shell/install.sh** command to unzip the basic package.

[root@localhost base]# tar xzvf

General_IVS-CentOS7.4-Base_CPU-X86-MD5-c8ef_V1.003.0000001.0.R.201117.tar.gz [root@localhost base]# **sh shell/install.sh**

-----Continue installation-----

-----[Begin:Deployment]-----

After unzipping the basic package, the script will automatically install the basic package and the driver.



The installation takes about half an hour, and the server will restart during the installation.



2 Service Software Installation

Log in to the server remotely through Xshell according to SSH protocol, and then install the service software. You need to modify the script before installing the service software.

2.1 Modifying Script

Before modifying the script, check whether the basic package and the driver are normal.

Prerequisites

You have obtained the IP8000-E installation package

(General_IVS-TB8000-E_ChnEng_MD5-544e_V1.000.1028000.0.T.201118.tar.gz.) from Dahua GDP system.

Background Information

 \square

The package name varies with version and release date.

Procedure

<u>Step 1</u> Check whether the basic package and the driver are normal.

1. Log in to the server remotely through Xshell.

2. Execute the **rpm -qa | wc -l**

command to check whether the number of rpm is correct.[root@rabbitmq1 ~]# **rpm -qa | wc**

909

3. Execute the **uname -r**

command to check whether the kernel is correct.[root@rabbitmq1 ~]# uname -r

3.10.0-1160.el7.x86_64

4. Execute the **npu-smi info**

command to check whether the driver can be recognized. If the following message appears, it means that the driver is normal.



root@rabbitmql ~]# npu-smi info					
npu-smi	20.1.0		Version: 20.1.0		
NPU	Name	Health	Power(W)	Temp(C)	
Chip	Device	Bus-Id	AICore(%)	Memory-Usage(MB)	
129	310	OK	12.8	63	
0	0	0000:83:00.0	0	5406 / 8192	
129	310	OK	12.8	65	
1	1	0000:84:00.0	0	4997 / 8192	
129	310	OK	12.8	66	
2	2	0000:85:00.0	0	4587 / 8192	
129	310	OK	12.8	64	
3	3	0000:86:00.0	0	4505 / 8192	

Figure 2-1 Check the driver

[root@rabbitmol ~l#

Step 2 Install the patch.

- Execute the mkdir /home/patch command to create a /home/patch folder on the server. Execute the cd /home/patch/ command to go to the /home/patch directory.
- 2) Click in the Xshell navigation bar 🕕 , and then move the patch from your local

computer to the /home/patch directory.

3) Unzip the patch on the /home/patch directory. The patch name varies with the version and release date.

[root@rabbitmq1 patch]# tar xzvf

General_IVS-CentOS7.4-Base_Patch-MD5-6212_V1.003.0000001.1.R.210926.tar.g z

4) Execute the **cd shell**/ command to go to the /home/patch/ directory, and then execute the **install.sh** command to install the patch.

[root@rabbitmq1 patch]# cd shell/

[root@rabbitmq1 shell]# sh install.sh

 \square

The process takes about half an hour, during which the server restarts.

Step 3 Modify script.

 \square

For baseline product, IP8000-E program has already been installed on the /home/IP8000 directory. Please skip the first two steps.

- 1. Execute the **mkdir /home/IP8000** command, and then create a /home/IP8000 folder.
- 2. Click in the Xshell navigation bar 🚺 , and then move the IP8000-E program from the

local computer to the /home/IP8000 directory.

3. Execute the cd shell/install.sh

command to go to the /home/IP8000 directory. Unzip the IP8000-E program. The program name varies with the version and release date.[root@rabbitmq1 IP8000]# tar xzvf G eneral_IVS-IP8000-E_ChnEng_MD5-540e_V1.001.0000000.0.R.210929.tar.gz



- 4. Execute the **cd tools**/ command to go to the tools directory in the program.
- 5. Execute the vi set_bond_config.sh

command. Press i

on the keyboard to switch to the editing mode, and then modify the IP address of the server (HOST_IP, HOST_GATEWAY, HOST_MASK). After compeletion, press **Esc**, and then input **:wq**

to save the change.[root@localhost base]# **vi set_bond_config.sh** #!/bin/bash

set ip address#Change to actual IP addressHOST_IP=xx.xx.xx#Change to actual gatewayHOST_GATEWAY=xx.xx.xx#Change to actual gatewayHOST_MASK=255.255.0.0#Change to actual subnet mask

cd /etc/sysconfig/network-scripts/

#set bond0

echo 'DEVICE=bond0' >ifcfg-bond0
echo 'BOOTPROTO=static'>>ifcfg-bond0
echo 'DEFROUTE=yes'>>ifcfg-bond0
echo 'ONBOOT=yes'>>ifcfg-bond0
echo 'TYPE=Ethernet'>>ifcfg-bond0
echo IPADDR=\$HOST_IP>>ifcfg-bond0
echo NETMASK=\$HOST_MASK>>ifcfg-bond0
echo GATEWAY=\$HOST_GATEWAY>>ifcfg-bond0
echo 'BONDING_OPTS="resend_igmp=1 updelay=0 use_carrier=1
arp_all_targets=any miimon=100 lp_interval=1 min_links=0 downdelay=0
xmit_hash_policy=layer2 primary_reselect=always fail_over_mac=none
arp_validate=none mode=active-backup all_subs_active=0 arp_interval=0
ad_select=stable num_unsol_na=1 num_grat_arp=1">>ifcfg-bond0

<u>Step 4</u>	Execute the sn set_bond_config.sn command to execute the script.
	[root@rabbitmq1 home]# sh set_bond_config.sh

/root

The network has been set active-backup mode successfully!

If the above-mentioned message appears, it means that the script was successfully executed.

. .

. . .

<u>Step 5</u> Execute the **reboot** command to restart the server.

<u>Step 6</u>	Execute the ifconfig command to check whether the IP address was successfully modified.
	[root@rabbitmq1 tools]# ifconfig
	bond0: flags=5187 <up a="" broadcast="" f="" m="" multicast="" r="" running="" st=""> mtu 1500</up>

ond0: flags=5187<UP,BROADCAST,RUNNING,M A S T E R,MULTICAST> mtu 1500 inet 192.168.1.135 netmask 255.255.0.0 broadcast 192.168.255.255 inet6 fe80::ae1f:6bff:fed0:8dc5 prefixlen 64 scopeid 0x20<link> ether ac:1f:6b:d0:8d:c5 txqueuelen 1000 (Ethernet)



RX packets 11094721 bytes 14968530083 (13.9 GiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4630554 bytes 576851719 (550.1 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 endvnic: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet6 fe80::aa82:52ae:893:d73d prefixlen 64 scopeid 0x20<link> ether 10:1b:54:49:48:d3 txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 339 bytes 55954 (54.6 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 eno1: flags=6147<UP,BROADCAST,S L A V E,MULTICAST> mtu 1500 ether ac:1f:6b:d0:8d:c5 txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device interrupt 16 memory 0xdf200000-df220000 eno2: flags=6211<UP,BROADCAST,RUNNING,S L A V E,MULTICAST> mtu 1500 ether ac:1f:6b:d0:8d:c5 txqueuelen 1000 (Ethernet) RX packets 11094732 bytes 14968544793 (13.9 GiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4630558 bytes 576851935 (550.1 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device memory 0xdf100000-df17ffff lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 4042486 bytes 15085000798 (14.0 GiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4042486 bytes 15085000798 (14.0 GiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

2.2 Installing Service Software

You need to install all services of the behavior analysis server, and the Unified Operation platform.

Procedure

<u>Step 1</u> Log in to the server remotely through Xshell.



<u>Step 2</u> Execute the **cd /home/IP8000/shell/** command to go to the home/IP8000/shell directory.

If the service software has been installed, we recommend uninstalling it first by executing the **sh uninstallAll.sh** command.

<u>Step 3</u> Execute the **sh install.sh** command to install the service software.

Installation takes about 18 minutes.



3 Deploying Platform

Background Information

Log in to the Unified Operation platform, initialize the platform, and configure servers.

3.1 Logging in to Unified Operation Platform

Background Information

You can log in to the Unified Operation platform by entering IP address and port number (8068 by default).

Procedure

<u>Step 1</u>

Open Google Chrome browser, enter *https://server IP address:8068* in the browser address bar, and then press Enter.



Use Chrome 52.0.2743.116 or later.

Step 2 Click Advanced.

Figure 3-1 Your connection is not private

Your connection is not private	
Attackers might be trying to steal your information from the set of (for example, passwords, messages, or credit cards). <u>Learn more</u>	
NET::ERR_CERT_AUTHORITY_INVALID	
Help improve Safe Browsing by sending some <u>system information and page content</u> to Google. <u>Privacy policy</u>	
Advanced Back to safet	у

Step 3 Click Proceed to IP address (unsafe).



Figure 3-2 Advanced

Your connection is not private
Attackers might be trying to steal your information from 1 (for example, passwords, messages, or credit cards). <u>Learn more</u>
NET::ERR_CERT_AUTHORITY_INVALID
Help improve Safe Browsing by sending some <u>system information and page content</u> to Google. <u>Privacy policy</u>
Hide advanced Back to safety
This server could not prove that it is 1999 , its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to (unsale)

<u>Step 4</u> Enter username and password, and then click **Login**.

Figure 3-3 Login

	User Log	gin
2	User name	
	Password	
	Login	
		Forgot Password?

- The username and the password are admin/Admin123 by default.
- For first-time login, you need to initialize the Unified Operation platform. For details, see "3.2 Initializing Unified Operation Platform".
- <u>Step 5</u> Click **Download checklist template**. Check the items in the checklist template and then click **Environment Checked**.



Figure 3-4 Environment checked



<u>Step 6</u> In the pop-up window, enter login password, and then click **OK**.

3.2 Initializing Unified Operation Platform

Background Information

When logging in for the first time, you need to complete the initialization according to onscreen instructions.

3.2.1 Searching Nodes

Procedure

<u>Step 1</u> Log in to the Unified Operation platform.

Step 2 Click Start Configuration and Deployment.



Unified Operation	English "	C+ Logou
System Initialization		
Step 1: Search the node IP address.		
Search the node you want to use.		
Step 2: MySQL configuration.		
Configuring the MySQL master/standby node, subnet mask and gateway.		
Step 3: Master/Standby configuration.		
Select operation and maintenance master/standby server node and configure virtual IP address.		
Step 4: Initialization.		
The initialization process of maintenance includes MySQL cluster installation and service initialization.		
→ Start Configuration and Deployment		

<u>Step 3</u> Click **Search** to search for all servers on the same network segment with the login IP.



Figure 3-6 Search for servers

Unified Operation					En	iglish 🚬 🕒 Logou
Search the node IP address	MySQL Config	Master/St	3andby Config	Initialization	Back	Next
Search Update					Please ente	r keywords. Q
IP Address	NI	IC Name: all	Device Type	Resources SN	Device SN	Status
+	bo	ond0				Connected
+	et	h0,eth1				Connected
+	bo	ond0,bond1				Connected
÷	bo	ond0,bond1,bond2,bo	DH-CSS9100X-MVI		4M45B92	Connected
±	ip	mi,bond0	CCS7100XV2		C81F66CF6779	Unconnected
+	bo	ond0,bond1				Connected
E	ip	mi,bond0	CCS7100XV2		C81F66E3A437	Unconnected
±	bo	ond0,bond1,bond2,bo	DH-CSS9100X-MVI		GZF5TF2	Connected
±	et	h0,eth1				Connected
					« <	1 > >

Step 4 Click Next.

3.2.2 Deploying MySQL

Procedure

- <u>Step 1</u> On the **MySQL Config** interface, click **MySQL Undeployed**, and then select **Standalone Mode**.
- <u>Step 2</u> Enter server IP in **MySQL Database IP**.
- <u>Step 3</u> Click **Business IP** of **MySQL M a s t e r Server**, and then in the displayed m a s t e r server list, select IP address of the event detection server. Click the IP address with bond0 gateway name.

Heartbeat IP and business IP are the same, and the heartbeat IP is automatically filled in after you select the business IP.



Figure 3-7 Deploy MySQL

	0		_ 0		@			Back	Next	
Search the	node IP address		MySQL Config		Master/Standby Config		Initialization	MOLE	146.41	
abase User										
User name:	AgSf3h5hw		3-32 characters containin _ @, or .	g letters, numbers,	* Password:	••••••	۵	14-32 characters, the combination number, Ψ_{i} ' Φ_{i} ' Φ_{i}^{i} ' Φ_{i}^{i} ' Φ_{i}^{i} ' Φ_{i}^{i} , Φ_{i}^{i	of letter (case s	ensiti
Please select dep	oloyment mode o	f MySQL.								
MySQL										
Configur	NySQL Deployed	Master and Standby	Mode 🖲 Standalone m	ode						
• MAPAT	Database IP:	Virtual IP								
* MySQL Ma	ster Server									
Busine	ess IP:	c	þ							
Heartbe	at IP:									

<u>_~r</u>

- Different ports of the same server are collapsed. You can click 🛨 to expand the information.
- Enter keywords in the text box at the upper-right corner, and then click Q to search for IP address.
- <u>Step 4</u> Click **OK** on the pop-up box.
- Step 5 Click Next.

3.2.3 Selecting Configuration Mode

Procedure

<u>Step 1</u> Select **Standalone Mode**, and the server address is automatically filled. Then click **Next**.



Figure 3-8 Select configuration mode

ified Operation				English 🔎 🕞 Logou
Search the node IP add	ress MySQL Config	3 Master/Standby Config	4	Back
(i) Please choose the cor	nfiguration mode of maintenance syster	n.		
Master/Standby				
Mode Standa	lone Mode			
* Server Address:		*		
* System Abbreviation:				
WAN Virtual IP:	IP Address of Maintenance Access			
WAN NIC Name:	WAN NIC Name			

<u>Step 2</u> In the pop-up window, click **OK**.

The system starts initialization. After that, the system goes to the login page.

<u>Step 3</u> Log in to the Unified Operation system again, and then change the default password and set up the security questions within 2 minutes.

\square

We recommend setting the answers to security questions to 1, which is easy to remember.

Step 4 Click **OK**.

The system goes to the login page.

3.3 Managing Server

Background Information

Manage the deployed platform server in the Unified Operation system for central management.

Procedure

- <u>Step 1</u> Use the new password to log in to the Unified Operation platform.
- <u>Step 2</u> In the pop-up window, click **OK**.
- <u>Step 3</u> Select **Resource** from the left navigation bar.



Figure 3-9 Resource



<u>Step 4</u> Click **Manage**, and then you can start managing servers.

 \square

You can manage servers by search or one by one.

• Manage servers by search

You can manage servers by auto search or manual search.

- Manage servers by auto search
 - 1. On the **Resource Management** interface, click **Search** to search for servers that are on the same network segment with the login IP. After that, click **Update**.

Figure	3-10	Autom	atically	search	corvorc
rigule	5-10	Autom	alically	search	servers

Ш	Resource	Search ² Update	3 Manage	Manual M	lanagemen	t Insta	ll Agent	P	lease enter t	he IP addre 🔍
ଚ	Resource Po	IP Address	NIC Name: all 🗸 🗸	System Type	Device SN	Device Type	Update Time	Status: Manag	jeable 🗸	Operation
ē	Resource Mo	. +		bond0		linux	CCS71	00XV2	2021-	S No
杀									07-29 18:21:16	pulse

2. Select the server to be managed according to the serial number on the server label.



<u>_~r</u>

Different ports of the same server are collapsed. You can click	+	to expand
he information.		

- 3. Click **Manage**, and then in the pop-up window, click **OK**.
- Manage servers by manual search
 - Enter IP address of the server to be managed in the search box at the upper-right corner of the **Resource Management** interface, and then click Search.

```
\square
```

If batch management is required, use fuzzy search. For example, the IP addresses of the server to be managed are 192.168.0.108 and 192.168.0.110, then you can enter "192.168.0" to search.

2. Select the server to be managed according to the serial number on the server label.

<u>0-11</u>

Different ports of the same server are collapsed. You can click 🕂 to expand the information.

- 3. Click **Manage**, and then in the pop-up window, click **OK**.
- Manual management
 - 1. On the Resource Management interface, click Manual Management.
 - 2. Enter the IP segment to be managed, click **Confirm to Manage**. In the pop-up window, click **OK**.

 \square

- Click Add to add multiple IP sections.
- ◊ Click to clear the corresponding IP section.

Figure 3-11 Enter server IP

Manual Managemen	t	\times
Add	Please enter the IP segment to manually manage resource.	
	Confirm to Manag	е

<u>Step 5</u> Select **Resource** > **Resource Management**, and then you can view the information of managed servers.



Related Operations

Manage new servers

On the **Resource Management** interface, click **Add**, and then you can repeat step 3–step 5 to manage new servers.

• Cancel managing servers

On the **Resource Management** interface, select servers from the server list, click **Cancel** or click

the corresponding in , enter login password in the pop-up window, and then click **OK**.



4 Installing Event Detection Server

4.1 Managing Product

Procedure

- <u>Step 1</u> Log in to the Unified Operation platform.
- <u>Step 2</u> Select **Product > Product Management**.
- Step 3 Click Install.

Figure 4-1 Install server

Product Ove Product Name Module Name Create Time Product Status Operation Product Man Product Man IPB000 IVSEvent 2021-11-22 14:08:15 Installed successfully. Image: Comparison of the successfully. Scheme Man Showing 1 to 1 of 1 entries Stowing 1 to 1 of 1 entries Image: Comparison of the successfully. Image: Comparison of the successfully.	W	Product	Install Edit	Update Format Shut	down Export Service Version		
Product Man IP8000 IVSEvent 2021-11-22 14:08:15 Installed successfully. Scheme Man Showing 1 to 1 of 1 entries Image: Comparison of the successfully.	¢	Product Ove	Product Name	Module Name	Create Time	Product Status	Operation
Showing 1 to 1 of 1 entries	۵	Product Man Scheme Man	IP8000	IVSEvent	2021-11-22 14:08:15	Installed successfully.	Ξ
	A.		Showing 1 to 1 of 1 en	tries			≪ < 1 > ≫

- <u>Step 4</u> Select **Common** > **InspectorEventDetect**, and select the corresponding version of **InspectorEventDetect**.
- <u>Step 5</u> Click **V1.0**.

Only V1.0 is available.





<u>Step 6</u> In the pop-up window, click **OK**.

<u>Step 7</u> On the **Custom Install** page, select **Standalone Mode**, enter **Cluster Name** and **Resource node pool** (IP address of the server), **Business management node pool** (IP address of the



server), **Business data node pool** (IP address of the server), **Heartbeat node pool** (IP address of the server), and leave the other values as default.

Custom Install	Switch to One-key Deployment
Select Mode	
Active-Standby	Mode Standalone Mode
*Safety Level (0-no	t encrypted (default), 5-stream image encryptic
0	
*Cluster Name	
IP8000	
*Resource node po	ol
*Resource node po	ol
*Resource node po	
*Resource node po	ol nent node pool
*Resource node po *Business manager Business manage	ol nent node pool ment node pool, at least 1, separate by comma
*Resource node po *Business manager Business manage Business data nod	ol nent node pool ment node pool, at least 1, separate by comma e pool
*Resource node po *Business manager Business manage Business data nod Business data nod	ol nent node pool ment node pool, at least 1, separate by comma e pool de pool, at least 1, separate by comma
*Resource node po *Business manager Business manage Business data nod Business data nod Heartbeat node po	ol nent node pool ment node pool, at least 1, separate by comma e pool de pool, at least 1, separate by comma pool
*Resource node po *Business manager Business manager Business data nod Business data nod Heartbeat node po Heartbeat node p	ol nent node pool ment node pool, at least 1, separate by comma e pool de pool, at least 1, separate by comma pool pool, at least 1, more than a comma
*Resource node po *Business manager Business manager Business data nod Business data nod Heartbeat node po Heartbeat node po Business network	ol nent node pool ment node pool, at least 1, separate by comma e pool de pool, at least 1, separate by comma cool cool, at least 1, more than a comma segment IP resource pool Add
*Resource node po *Business manager Business manager Business data nod Business data nod Heartbeat node po Heartbeat node po Business network	ol nent node pool ment node pool, at least 1, separate by comma e pool de pool, at least 1, separate by comma cool cool, at least 1, more than a comma segment IP resource pool Add

Figure 4-3 Custom install

Step 8 Click Next.

The Install New PaaS Cluster page is displayed.



4.2 Installing New PaaS Cluster

Prerequisites

Event detection server is installed. For details, see "4.1 Managing Product".

Procedure

Step 1 On the Custom Install page, click Install New PaaS Cluster.



Figure 4-4 Install new PaaS cluster

- Select service type. <u>Step 2</u>
 - 1. Clear Cloud Database Service and Storage Service.



Figure 4-5 Select service type

0	2		3
Select Service	Parameter Co	nfig	Installation Proces
* Cluster Name			
TB8000			
i) Select the service t	ype included in the clust	er.	
Mysql service	RabbitMQ	Account Service	×
V1.0	V1.0	V1.0	
Camera Service	Cloud Databa	Storage Service	Y
V1.0	V3.0	V1.0	
Media Service	Intelligence S	DeepLearning	~
V1.0	V1.0	V1.0	

<u>Step 3</u> Configure the parameters.

 Select Standalone > General Domain Mode, leave the other parameters as default, and then click Next.



Currently IP8000-E only supports standalone.

Figure 4-6	Configure	PaaS	cluster	parameters
				1

Install New PaaS Cluster	×	
0	3	
Select Service	Parameter Config Installation Process	
	Active-Standby Standalone	
💮 Common Con	General Domain Mode Central Domain Mode	
	Agent Domain Mode	
	*Safety Level (0-not encrypted (default), 5-stream image encryption	
	*Mysql Service User Name	
	3-32 characters containing letters, numbers, _, @, or .	
	*Mysql Service password	
	•••••••••••••••••••••••••••••••••••••	
	*RabbitMQ User Name	
	DHCloudIz 3-50 characters combining letter, number,, @, and .	
	*RabbitMQ password	
	14-32 characters, the combination of letter (case sensitive), number, '#', '^',	
	*Resource node pool	
	Business network segment IP resource pool Add IP	
	Back	

2. On the **Mysql service** page, install MySQL. Select **Installed**.

Database Service Virtual IP (server IP address) is displayed.



If it is not displayed, manually enter the server IP address.

	Figure 4-7 MySQL service	
i) Install New PaaS Cluster		×
0		3
Select Service	Parameter Config	Installation Process
⊘ Common Conf	Installed	•
	*Database Service Virtual IP	
Mysql service	1.000	
() RabbitMQ		Show More Advanced

3. Select the Intelligence Service tab, click Show More Advanced, and then click Intelligence DataNode edit box. Select server IP address, and leave the other parameters as default.



Deployment Manual

Figure 4-8 Intelligence service

Install New PaaS Cluster	
1 Select Service	2 3 Parameter Config Installation Process
⊘ Common Conf	Account Virtual IP
() Mysql service	Account Virtual IF
RabbitMQ	38201
() Account Service	Media Virtual IP Media Virtual IP
() Camera Service	Media Port
() Media Service	RabbitMQ Virtual IP
Intelligence S	RabbitMQ Virtual IP
	5672
DeepLeanning	EFS Storage Virtual IP
	EFS Storage Port
	EFS Storage Port
	Intelligence DataNode Intelligence DataNode IP , more than one is separated by a co
	Back Next

- **DeepLearning vip**, and leave the other parameters as default.

For **DeepLearning vip**, enter the server IP address.



Deployment Manual

Figure 4-9 Deen learning service

	-	-
Select Service	Parameter Config	Installation Process
⊘ Common Conf	Add	
	*DeepLearning vip	
Mysql service	DeepLearning vip, this parame	ter is real IP currently
RabbitMO	The content is invalid or null. Ple *Zeus_VIP	ase enter again.
O	Zeus_VIP	
() Account Service		Hide Advanc
	*DeepLearning_IPS	
() Camera Service	Intelligent service node IP, only	y one IP is required for miniatur
	*PASS_ACCOUNT_IP	
Media Service	FACE_PASS_ACCOUNT_IP	
① Intelligence Se	*ACCESS_SERVICE_RESTFUL_IP	
J	FACE_ACCESS_SERVICE_RESTF	UL_IP
💮 DeepLearnin	*DSE_RESTFUL_IP	6
	Cloud database query service I	р
	*JDBC_URL	4
	JDBC_URL	
	×KARRIIMGTb	
	rabbitmq_ip	
	Back	Completed and submit

If error occurs during installation, you can just click the close button





4.3 Configuring Behavior SaaS

Prerequisites

Make sure that new PaaS cluster is installed. For details, see "4.2 Installing New PaaS Cluster".

Procedure

<u>Step 1</u> On the **Custom Install** page, select the installed SaaS service and PaaS cluster, and then click Next.

Figure 4-10 Select SaaS and PaaS
Custom Install
*Cluster Name
IP8000-E
Behavior SaaS V1.0
Install New PaaS Cluster
IP8000 General 2021-11-22 14:06:41
Account ServCamera ServiMysql service DeepLearnin Intelligence Media Service RabbitMQ
Back

Click Common Configuration, select Standalone, and leave the other parameters as <u>Step 2</u> default.



Figure 4-11 Common configuration

Ē√ SaaS Cluster Config Item	×
😁 Common Con	Active-Standby Standalone *Safety Level (0-not encrypted (default), 5-stream image encrypt
() Behavior SaaS	0

<u>Step 3</u> Click **Bahavior SaaS**, and then click **Show More Advanced**. Enter **Video_Max_Channels** (the maximum number of video analysis channels), select **Server_Type** as **IP**, and leave the other parameters as default. Click **Completed**. The system goes to the **Custom Install** page.

 \square

The maximum number of analysis video channels is related to the number of intelligent cards in the server. One intelligent card corresponds to 32 video channels. You can know the number of intelligent cards in the server from the label on the server.



4-12 Configure behavior SaaS	
	×
Add *Service business address Server_IP	▼ HideAdvanced
*Server_Port 37778 *NetSDK_Port 37777 *Server_User admin *Server_Pwd admin123	
*Vedio_Max_Channels 32 *Server_Type IP	
	4-12 Configure behavior Saas Add *Service business address Server_IP *Server_Port 37778 *NetSDK_Port 37777 *Server_User admin *Server_Pwd admin123 *Vedio_Max_Channels 32 *Server_Type IP



- <u>Step 4</u> On the **Custom Install** interface, click **Add** to add authorization user.
- <u>Step 5</u> Enter UserName, NickName, Password, and E-Mail. Select Camera Service, enter Number of Devices and Number of Channels.
 - \square
 - Number of Devices: The maximum number of devices that can be connected.
 - Number of Channels: The number of channels that can be connected.



	5		
* UserName:	TB1	* NickName:	TB1
	ALPHANUM Length Is 3 To 31 Bit		Name length shall be 3-16 characters combining
		1	upper and lower cases, number, @, _, and .
* Phone No.:	156****0721	* E-Mail:	***@qq.com
t Chuster			
Cluster:	188000		
Camera Servi	C 8		
Califera Servi			
*Number of [Devices	*Number of Cha	nnels
1000		1000	
1000		1000	
			ОК
Sten 6 Clic	- k OK		
Aft	er user authorization, the sys	stem automatically go	es to the Custom Install interface.

Step 7Click Completed and submit, and then in the pop-up window, click OK.After installation, select Product > Product Management, and then you can viewInstalled successfully from Product Status.



Figure 4-14 Completed and submit

Custom Install
*3–16 characters combining letter (case sensitive), number, @, _, - and .
TB8000
(i) You have selected the SaaS service you want to install. Display SaaS Settings
Omega Omega <th< td=""></th<>
(i) Corresponding PaaS services have been selected.
TB8000 Delete 2021-07-12 15:34:58
*Domain: TB8000
*User: TB1 • 2+
Back Completed and submit

Figure 4-15 Installed successfully

Product management		9 I I I I I I I I I I I I I I I I I I I	🔲, 🐵 🗘 English , 🎗 admin ,	
Install Edit Update	Format Shutdown	Export Service Version		
Product Name Module Name		Create Time	Product Status	Operation
Т88000	IVSEvent	2021-07-12 15:39:43	Installed successfully.	Ξ
Showing 1 to 1 of 1 entries			_	

4.4 Configuring Operator

Background Information

Log in to the View Intelligent O&M Tool to configure the operator.



Procedure

<u>Step 1</u> Log in to the View Intelligent O&M Tool.

- 1. Enter *https://server IP:6400* in the browser address bar, and then press Enter.
- 2. Enter username and password, and then click Log in.

The default username and password are both admin.

3. Set security questions, and then click Next.

 \square

We recommend setting answers that are easy to remember to security questions.

- 4. Change the default password in two minutes, and then click **OK**. After that, log in to the View Intelligent O&M Tool with the new password.
- <u>Step 2</u> (Optional) Select **Node Resource**, and then you can view the server information.

Figure 4-16 Node resource

	rigate i fortoac resource										
Viev	w Intelligent O&	M Tool	Hom	e Registratio	a Center No	de Resource	Operator Management	Profile Ma	asgement	Toolkit	admin 🖂 🗰
Domain:			Node IP Address:	Please select	🗸 Oslav	Statue Please select		Search	Reset		
	• •			Ouline Status 🗢							
		10.0.00		•	40	1				0	Q

<u>Step 3</u> Select **Operator Management > Add Operator+**.

Figure 4-17 Add operator

View Intellige	ent O&M Too	1	Home	Registration Center	Node Re	source	Operator Man	agement	Profile Manag	ement Too	ka admin	· 中文
Add Operator+	Domain: Please	select	👻 Durinens Type	Please select	Operator Typ	e Please selec		Service Node IP	Please select	×	rch Reset	l
Domaia 🜩												
40.00												

Step 4Click the edit button in the Operation column, and then on the Edit Operator interface,
select Road Recognition from Operator Type, select aix3200 from Start Type, leave
other parameters default.



Operator Details								×
Domain		Operator Type		Number of Started Operators	Start Type		Intelligent Board of Scarting Si ugle Operator	CPU Cores of Starting Single Operato 7
Please select	×	Please select	~	Please enter content	Please select	~	Please enter content	Please enter content

Step 5 Click OK.

The system goes to the **Operator Management** interface. Apply for encryption, and after the operator starts, the resources status changes to **Running**. For details on applying for encryption, see "5 Applying for Encryption".



5 Applying for Encryption

Background Information

TB8000 supports two encryption methods: hardware-based encryption and software-based encryption.

5.1 Checking Dongle

Background Information

Use Xshell to remotely log in to the server, and then you can check whether a dongle is installed. The tool recognizes the dongle information first by default. If no dongle is recognized, then it tries to recognize software-based encryption.

Procedure

- Step 1 Log in to the server remotely through Xshell.
- Execute the **Isusb** command to check whether dongle is installed on the server. Step 2
 - [root@rabbitmq1~]# lsusb

Bus 002 Device 002: ID 8087:8000 Intel Corp. Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub Bus 006 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub Bus 005 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub Bus 001 Device 002: ID 8087:8008 Intel Corp. Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub Bus 003 Device 002: ID 096e:0202 Feitian Technologies, Inc. Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub If Feitian Technologies, Inc. information appears, it means that the dongle was recognized; otherwise, there is no dongle, and you need to apply for the software-based encryption.

5.2 Software-based Encryption

Procedure

- Step 1 Log in to the server remotely through Xshell.
- Execute the **cd** /**Tools** command to go to the Tools directory. <u>Step 2</u>
- Step 3 Execute the ./LicenseUpdateTool.exe -server export command to get the connection_server.dat file. [root@rabbitmq1 Tools]# ./LicenseUpdateTool.exe -server export _____ SUCCESS:



Export base information successfully.

$Path(\mu \frac{1}{4}^{3}\P): /connection_server.dat$

 \square

File name varies with version and release date.

- <u>Step 4</u> In the Tools directory, execute the **sz connection_server.dat** command to save the file to the local PC.
- Step 5Apply for software-based encryption on Dahua portal. The portal only supports the
Chinese version. Contact our technical support to help you with the application process.
 - In the portal menu navigation bar, search 加密 (encryption), select 根据导出设备信 息包申请软License或加密狗License (中心智能设备) (apply for a software license or dongle license (central intelligence device) based on the exported device information package).

Figure 5-1 Search for encryption

菜单搜索	×
加密 encryption 搜索	
业务导航/研发中心/开发验证/产品加密授权 安全芯片授权(先进技术研究院专用)	•
▶ 业务导航/研发中心/开发验证/产品加密授权/嵌入式设备 根据导出的设备信息包申请License 根据设备S/N号申请License 为整机料号申请License配置(嵌入式设备)_研发项目经理使用	=
 ・ 业务导航/研发中心/开发验证/产品加密度权/通用类设备 根据导出设备信息包申请软License或加密狗License(通用设备) 为整机料号申请License配置(通用类设备)_研发项目经理使用 apply for a software ・ 出名目的(研究中心)、研究303(1)(方目)、如約3(1)(方目)、如約3(2)(方目)、 	e license central
 业务导机/研发中心/开发短心/产品加密投仪/中心智能突设备 intelligence device on the exported de 为整机料号申请License配置(中心智能类设备)_研发项目经理使用 information packag 根据导出设备信息包申请软License或加密狗License(中心智能设备)) based evice ge
 业务导航/研发中心/开发验证/产品加密接权/全球生产与维修支撑系统 为工厂配置工单 为维修站点申请账号 	+

2. Click 新增 (add) to add a software-based encryption application.

Figure 5-2 Add application

局新増 🗹 f	8改 🛞 删除 🔔 导出				
Add 单描编号		制单人	请选择		Ŧ
审核状态	请选择		查询	清除条件	

3. Enter the application information.

If you apply for permanent encryption, enter the project name, business opportunity No., and corresponding technical support in the reason field, and then attach the contract.







Table 5-1 Parameter description

Parameter	Description
-----------	-------------



Parameter	Description
	Select the application type.
Туре	● For hardware-based encryption, select 加密狗 (dongle).
	 For software-based encryption, select 软License (software License).
	Click 加密狗信息包 (dongle information package), and then select the exported connection_server.dat file.
Dongle	
Package	• The file name varies according to the version and release date.
rackage	 If you select 软加密 (software-based encryption), you do not need to upload files.
Server Information	Click 服务器信息包 (server information package), and then select the exported connection_server.dat file.
Package	
	The file name varies according to the version and release date.
	Click the text box, and then enter the material No. of the server.
Material No.	
	For server material No., see Table 5-2.
	Set the usage days.
Algorithm Database Usage	• Clear the 永久有效 (permanently effective) checkbox, and then
Days	select 算法库使用天数 (algorithm database usage days). 💌 means
	selected, and 🔲 means not selected.
	 No approval is needed if usage days are under 30 days.
Algorithm Database Config	Select 算法库配置选择 (Algorithm Database Config), and then select 周 界防范 (2077) (perimeter protection (2077)), 智慧消防(3114) (intelligent firefighting (3114)), and 交通全智能 (3106) (intelligent traffic (3106)).
Reason	Enter the reason for your application.

Table 5-2 Server material No.

Server Name and Model	Part No.
Domestic Dahua 1U Traffic Event Detection Intelligent Server (E3 1275V5-8G*2-4T*1-E-dongle included) DH-IVS-TB8000 - E-A	1.0.01.18.10612
Domestic Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*2-dongle included) DH-IVS-TB8000-2A-GU2	1.0.01.18.10613
Domestic Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*6-dongle included) DH-IVS-TB8000-6A-GU2	1.0.01.18.10614
Domestic Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*4-dongle included) DH-IVS-TB8000-4A-GU2	1.0.01.18.10615



Server Name and Model	Part No.
Domestic Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*6-dongle included) DH-IVS-TB8000-6A-GU2	1.0.01.18.10616
Domestic Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*6-dongle included) DH-IVS-TB8000-6A-GU2	1.0.01.18.10617
Overseas Dahua 1U Traffic Event Detection Intelligent Server (E3 1275V5-8G*2-4T*1-E-dongle included) DHI-IVS-TB8000 - E-A	1.0.01.18.10618
Overseas Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*2-dongle included) DHI-IVS-TB8000-2A-GU2	1.0.01.18.10619
Overseas Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*6-dongle included) DHI-IVS-TB8000-6A-GU2	1.0.01.18.10620
Overseas Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*4-dongle included) DHI-IVS-TB8000-4A-GU2	1.0.01.18.10621
Overseas Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*6-dongle included) DHI-IVS-TB8000-6A-GU2	1.0.01.18.10622
Overseas Dahua 2U Traffic Event Detection Intelligent Server (Silver4114T*2-16G*4-4T*4-E Card*6-dongle included) DHI-IVS-TB8000-6A-GU2	1.0.01.18.10623

4. At the upper-left side of the application page, click 保存 (save), and then click 提交 (submit). After the process is approved, you will receive an email from the portal. Click the link in the email to download the software-based encryption certificate, which is a zip file named after the application date.

Step 6 Start encryption.

- 1. Log in to Xshell, and then in the Tools directory, execute the **rz** command to upload the downloaded certificate.
- 2. Execute the ./LicenseUpdateTool.exe -server import

command to import the encryption certificate.[root@rabbitmq1

Tools]# ./LicenseUpdateTool.exe -server import xxxx.zip

SUCCESS:

Import successfully.

Change the name of xxxx.zip to the actual file name.

3. In the Tools directory, execute the ./LicenseUpdateTool.exe -server display

command to view encryption information.[root@rabbitmq1 ~]#

/Tools./LicenseUpdateTool.exe -server display

SUCCESS:

SN: ad33d8b0-1f7b-cab9-9447-ba07f855b143



 Begin Date:
 2021-05-19 16:05:55

 End Date:
 2021-06-18 16:05:55

 Days:
 30

 Count:
 3

 ID:
 2077,3114,3106

- 4. Execute the **/etc/init.d/Intelligence-DataNode restart** command to restart the operator service.
- <u>Step 7</u> Log in to the View Intelligent O&M Tool to view the operator status.

If the Resource Status shows Running, it means that the encryption was successful.

Figure 5-4 Resource status

View Intellige	nt O&M Tool		lome	Registration Center	Node Resor	irce	Operator Management	Profile Managem	sent Toolki	i admin s	中文
Add Operator+	Domain: Please s	elect	👻 Business Type:	Please select	Operator Type:	Please select	Service Node IP	Please select	 Search 	Reset	1
Domain 🜩											Operation
itin3as	General Basiness	General Recognition	-	4120	V1 000 000000	1.07 1	1	Ranning	Debue	182	0 1

5.3 Hardware-based Encryption

Procedure

<u>Step 1</u>	Insert the dongle into the server.									
<u>Step 2</u>	Log in to the server remotely through Xshell.									
<u>Step 3</u>	<u>3</u> Execute the cd / Tools command to go to the Tools directory.									
<u>Step 4</u>	Execute the ./LicenseUpdateTool.exe -server export command to get the									
	connection_server.dat file.									
	[root@rabbitmq1 Tools]# ./LicenseUpdateTool.exe -server export									
	connection									
	connection									
	file_len:11. length:10file_len:11. length:10									
	=======================================									
	SUCCESS:									
	Export base information successfully.									
	Path(µ¼³¶): /Tools/ connection_server.dat									
	The file name varies according to the version and release date.									
<u>Step 5</u>	Execute the ./LicenseUpdateTool.exe -dog export command to get the									
	connection_dog.dat file.									
	[root@rabbitmq1 Tools]# ./LicenseUpdateTool.exe -dog export									
	======================================									
	Export base information successfully									
	Path(μ^{3} () : /connection dog dat									
	rath(µ/4 1). / connection_uog.uat									



.OGY	Deployment Manual							
	The file name varies according to the version and release date.							
<u>Step 6</u>	Apply for the dongle on Dahua portal. For details, see step 5 in "5.2 Software-based							
	Encryption".							
<u>Step 7</u>	Start encryption.							
	1. Log in to Xshell, and then in the Tools directory, execute the rz command to upload the							
	downloaded encryption certificate.							
	2. Execute the ./LicenseUpdateTool.exe -dog import command to import the							
	encryption certificate.							
[r	oot@rabbitmq1 Tools]# ./LicenseUpdateTool.exe -dog import xxxx.zip							
=	=======================================							
SI	UCCESS:							
In	nport successfully.							
	Change the name of xxxx.zip to the actual file name.							
	3. In the Tools directory, execute the ./LicenseUpdateTool.exe -dog display command							
	to view encryption information.							
[r	oot@rabbitmq1 ~]# /Tools ./LicenseUpdateTool.exe -dog display							
=	=======================================							
S	N_{1} ad33d8h0-1f7h-cah9-9447-ba07f855h143							
B	egin Date: 2021-05-19 16:05:55							
E	nd Date: 2021-06-18 16:05:55							
D	avs: 30							
C	ount: 3							
IC	D: 2077, 3106, 6145							
	4. Execute the /etc/init.d/Intelligence-DataNode restart command to restart the							
	operator service.							
<u>Step 8</u>	Log in to the View Intelligent O&M Tool to view the operator status.							

If the status changes to **Running**, it means that the encryption was successful.

Figure 5-5 Resource status

View Intelligent O&M Tool		в	me	Registration Center	Node Resource	Operat	tor Management	Profile Manage	ment To	olkit admin	中文
Add Operator+	Domaia: Please s	elect ·	Business Type:	Please select	V Operator Type: Pilcar		Service Node IP:	Please select	× 80	arch Reset	
Domaia \$											Operation
ittle2es	General Business	General Recognition	-	4530	V1 000 0000001 0T	1	1	Running	Dahaa	182	οı



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;
- 2. Update Firmware and Client Software in Time
 - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
 - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between



1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.



• Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

ENABLING A SAFER SOCIETY AND SMARTER LIVING