



Intelligent Server (Digital City Solution V3.0)

Deployment Manual






Foreword

General

This manual introduces the deployment of intelligent servers in Digital City Solution Deployment Guide V3.0. Read carefully before deploying, and keep the manual safe for future reference.

Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license 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, and comply with the guidelines when using it.

Transportation Requirements



- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Avoid heavy stress, violent vibration, and immersion during transportation.
- Transport the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the transporting temperature and humidity of the device.

Storage Requirements



- Store the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the storing temperature and humidity of the device.
- Avoid heavy stress, violent vibration, and immersion during storage.

Installation Requirements



- Make sure that the power is off when you connect the cables, install or disassemble the device.
- For devices with earthing systems, make sure they are grounded to avoid being damaged by static electricity or induced voltage, and prevent electrocution from occurring.
- All installation and operations must conform to local electrical safety regulations.
- Use accessories suggested by the manufacturer, and installed by professionals.
- Do not block the ventilator of the device, and install the device in a well-ventilated place.
- Do not expose the device to heat sources or direct sunlight, such as radiator, heater, stove or other heating equipment, which is to avoid the risk of fire.
- Do not place the device in explosive, humid, dusty, extremely hot or cold sites with corrosive gas, strong electromagnetic radiation or unstable illumination.
- Avoid heavy stress, violent vibration, and immersion during installation.



Safe and stable power supply is a prerequisite for proper operation of the device.

- Make sure that the ambient voltage is stable and meet the power supply requirements of the device.
- Prevent the power cord from being trampled or pressed, especially the plug, power socket and the junction from the device.
- For devices that can be powered by multiple supplies, do not connect them to two or more kinds of power supplies; otherwise, the device might be damaged.

- Refer to the specific user's manual for the power requirements of single device.



It is recommended to use the device with a lightning protector for better lightning-proof effect.

Operation Requirements



A suitable operating environment is the foundation for the device to work properly. Confirm whether the following conditions have been met before use.

- Use the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the operating temperature and humidity of the device.
- Use the device on a stable base.
- Do not let any liquid flow into the device to avoid damage to internal components. When liquid flows into the device, immediately disconnect the power supply, unplug all cables connected to it, and contact after-sales service.
- Do not plug or unplug RS-232, RS-485 and other ports with the power on, otherwise, the ports will be easily damaged.
- Back up data in time during deployment and use, in an effort to avoid data loss caused by abnormal operation. The company is not liable for data security.
- The company is not responsible for damages to the device or other product problems caused by excessive use or other improper use.

Maintenance Requirements.



- Contact professionals for regular inspection and maintenance of the device. Do not disassemble or dismantle the device without a professional present.
- Use accessories suggested by the manufacturer, and maintain the device by professionals.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Installing Servers	1
1.1 Safety Instructions	1
1.2 Installing Intelligent Operator Server	1
1.2.1 Installing GPUs.....	1
1.2.2 Modifying the IP Address.....	2
1.2.2.1 Confirming the Network Card.....	2
1.2.2.2 Modifying the IP	2
1.2.3 Installing Intelligent Operator Program	3
2 Configuring Unified O&M	5
3 Dongle	6
4 Configuring Operator	7
4.1 Uploading Operator Package	7
4.2 Creating Network.....	8
4.3 Deploying Algorithm	10
Appendix 1 Safety Inspection Checklist for Server Installation	12
Appendix 1.1 Server Rack Inspection Checklist	12
Appendix 1.2 Power Cable Inspection Checklist	14
Appendix 1.3 Signal Cable Inspection Checklist	16
Appendix 2 Cybersecurity Recommendations	18

1 Installing Servers

This chapter introduces the installation methods of all the servers.

1.1 Safety Instructions

Notes

- Wear anti-static work clothes. Do not attach any metal products to the anti-static work clothes.
- Wear an anti-static wrist strap. The wrist strap must be in good contact with your skin, and is grounded reliably. We recommend using the anti-static wrist strap in the current server room.
- When the server arrives at the site, you can unpack and check the server after the antistatic devices have been prepared.
- Ground the rack or the server.

Figure 1-1 Safety notes example



Checklist

For more information on the checklist for cabinet installation, signal cable installation, and power cable and protective ground cable installation, see "Appendix 1".

1.2 Installing Intelligent Operator Server

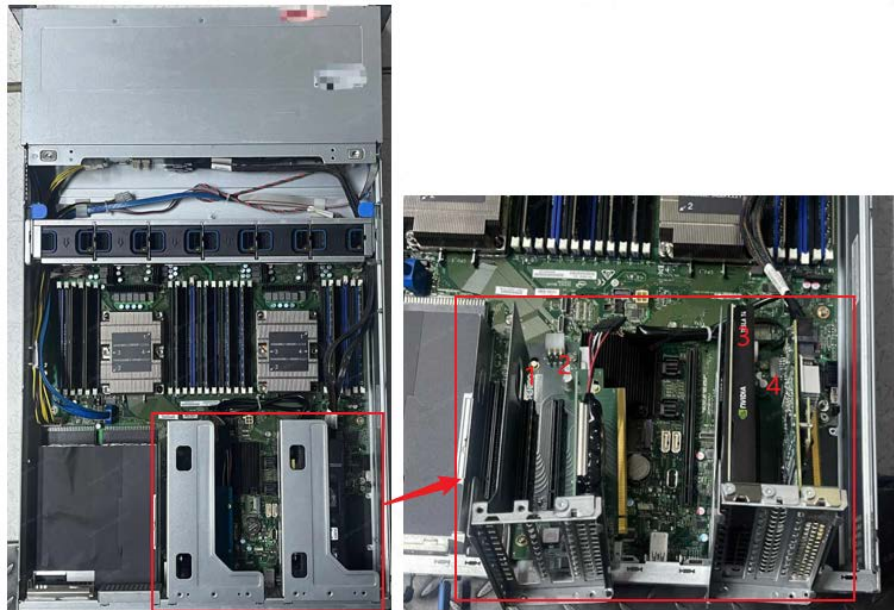
The intelligent operator server is delivered with the operating system and the corresponding drivers pre-installed. You do not have to install the operating system. If you need to reinstall the Linux operating system, or the server is provided by the customer and the operating system is not installed, you can obtain the operation manual from the delivery representative for reference.

1.2.1 Installing GPUs

If you receive a model GS8000 server and the GPUs that are separately packaged, then you need to install the GPUs.

Open the top cover of the server, insert the GPUs into the PCIe slot. No sequence requirements.

Figure 1-2 Install GPUs



1.2.2 Modifying the IP Address

1.2.2.1 Confirming the Network Card

Connect a network cable to a network card on the server (do not connect network cables to other network cards on the server), and then enter **ethtool network card name** (for example, **ethtool eth0**). If **Link detected** shows **yes**, it means that the network cable is connected to eth0. If **Link detected** shows **no**, try to connect the network cable to another network card, and retry the command until **yes** is displayed.

Repeat the above operations to confirm the name of each network card and make a record.

Figure 1-3 Confirm the network card

```
admin@localhost:~$ ethtool eth0
Settings for eth0:
  Supported ports: [ TP ]
  Supported link modes:   10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Half 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/Half 1000baseT/Full
  Advertised pause frame use: Symmetric
  Advertised auto-negotiation: Yes
  Advertised FEC modes: Not reported
  Link partner advertised link modes:   10baseT/Half 10baseT/Full
                                        100baseT/Half 100baseT/Full
                                        1000baseT/Full
  Link partner advertised pause frame use: No
  Link partner advertised auto-negotiation: Yes
  Link partner advertised FEC modes: Not reported
  Speed: 1000Mb/s
  Duplex: Full
  Port: Twisted Pair
  PHYAD: 1
  Transceiver: internal
  Auto-negotiation: on
  MDI-X: on
  Cannot get wake-on-lan settings: Operation not permitted
  Current message level: 0x000000ff (255)
  drv probe link timer ifdown ifup rx_err tx_err
  Link detected: yes
admin@localhost:~$
```

1.2.2.2 Modifying the IP

This section uses modifying IP address of bond0 as the example.



Do not use the setup command to modify the IP address.

Step 1 Log in to the background of the server through SSH. The default username is root or admin and connect delivery representative to acquire the default password.

Step 2 Ensure the current user is root (if not, run the command **su - root** to switch user to root), and then run the following command in any directory.

```
vim /etc/sysconfig/network-scripts/ifcfg-bond0
```

Figure 1-4 Modify the IP address

```
[root@rabbitmq1 ~]# vim /etc/sysconfig/network-scripts/ifcfg-bond0
```

Step 3 Modify the IP address, subnet mask, and default gateway of the server.

- 1) Run **i** to go to edit mode, and **INSERT** will be displayed at the bottom of the screen.
- 2) Modify the network information, including IP address, subnet mask, and default gateway.
- 3) Press Esc, run **:wq!**, and then press Enter to save the settings and exit.
- 4) Run **:q!**, and then press Enter to exit without saving changes.

Figure 1-5 Modify IP address

```
DEVICE=bond0
BOOTPROTO=static
DEFROUTE=yes
ONBOOT=yes
TYPE=Ethernet
UUID=eb79d48b-0abe-4674-bb23-9c35c2815b67
IPADDR=192.168.1.108
NETMASK=255.255.0.0
GATEWAY=192.168.0.1
BONDING_OPTS="resend_arp=1 updelay=0 use_carrier=1 arp_all_targets=any miimon=100 lp_i
te=none mode=active-backup all_slaves_active=0 arp_interval=0 ad_select=stable num_unso
```

Step 4 After modifying network information, run command **service network restart** to restart network services.



When modifying the IP, if the IP address is entered incorrectly, or there is extra or missing information, it might fail to restart the network services.

1.2.3 Installing Intelligent Operator Program

Prerequisites

Prepare the CVEngine program package, unified O&M package, and intelligent service sub node package according to "Digital City Solution Checklist". The following package names are for your reference:


- CVEngine program package: DH_IVE-CV_Base_VX.XXX.XXXXXXXXXX.X.R.XXXXXXX.tar.gz.



It is neither the package starting with DH_IVE-CV_Internal_Upgrade, which is all-in-one CVEngine server package, nor the package starting with DH_IVE-CV_Base-Minimal, which is the package for integrating into other products.

- Unified O&M package: DH_Phoenix_ChEng_Basic_VX.XXX.XXXXXXXXXX.X.R.XXXXXXX.tar.gz or General_Extreme_DSSC9100_MultiLang_Phoenix_VX.XXX.XXXXXXXXXX.X.R.XXXXXXX.tar.gz, depending on package included in the solution.
- Intelligent service sub node package: General_IVS-CVEngine_ChEng_Operator-Install-Base-MD5-XXXX-X86_V2.XXX.XXXXXXXXXX.X.R.XX XXXX.tar.gz.

Procedure

- Step 1 Run command **mkdir /home/ivs** on the server to create a new folder, and then upload the unified O&M package, the CVEngine program package, and the intelligent service sub node package to the /home/ivs directory.
- 
- You can use a remote computing tool (such as MobaXterm) to remotely log in to the server and upload the packages.
- Step 2 After uploading the packages, run command **md5sum file name** to check whether the last 4 digits after md5 are consistent with MD5_XXXX in the package name. If inconsistent, the package is damaged.
- Step 3 Ensure the current user is root, if not, run the command **su - root** manually to switch to root.
- Step 4 Unzip the intelligent server sub node package (package name example: General_IVS-CVEngine_ChnEng_Operator-Install-Base-MD5-XXXX-X86_V2.XXX.XXXXXXX.X.R.XXXXXX.tar.gz).
After unzipping, a shell folder will appear.
- Step 5 Go to the shell/uninstall folder, and then execute **sh uninstallAll.sh** to uninstall the old environment.
- Step 6 Go to the shell/install folder, and then execute **sh install.sh** to install the intelligent scheduling sub node and platform O&M sub node with one click.
- Step 7 Run command **cd /cloud/service/services** to go to the file directory, and then run command **ll** to check the service.

2 Configuring Unified O&M

Finish the O&M deployment according to the “Digital City Solution Deployment Guide V3.0”.

3 Dongle

The operator server comes with a dongle by default. Insert it directly into the server, and then you can use it.

4 Configuring Operator

In this solution, you need to configure faces, vehicles, and structured operators.

4.1 Uploading Operator Package

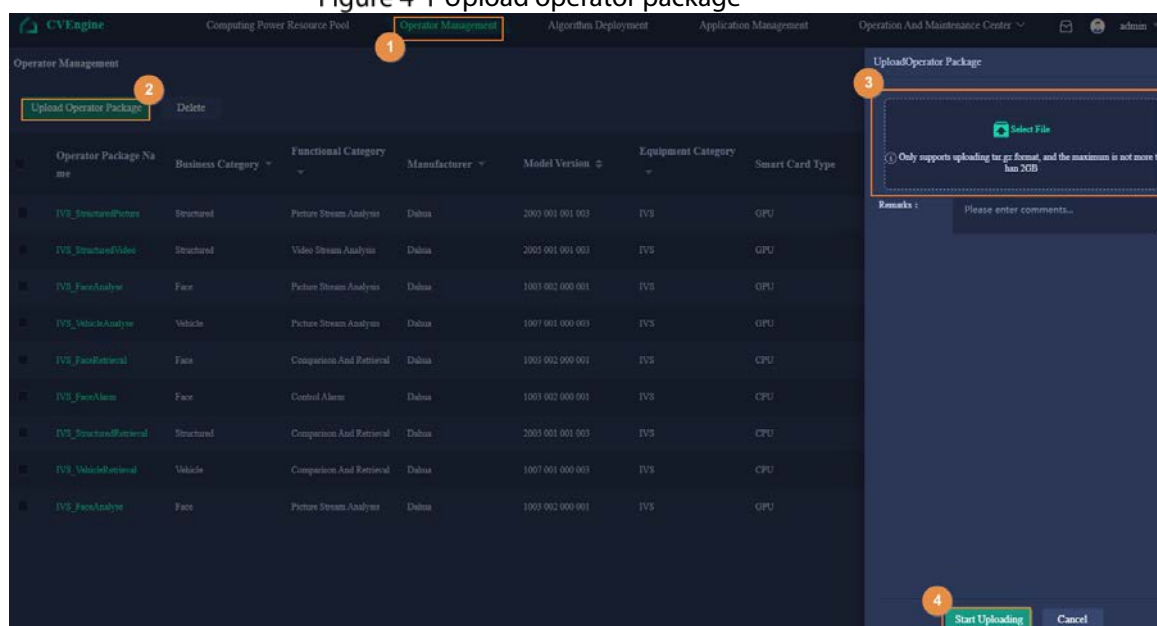
Prerequisites

Before configuring the operator, make sure that cloud storage is authorized, and files can be uploaded.

Procedure

- Step 1** Enter `https://CVEngine IP address:6400` in the browser address bar to go to the login page, and then press Enter.
- Step 2** Enter the login username and password, and then click **Login**.
- Step 3** Select Operator Management, and then click Upload Operator Package.
- Step 4** Click **Select File**, select the operator package, and then click **Start Uploading**.

Figure 4-1 Upload operator package



When uploading the package, the system automatically identifies the category, manufacturer, model version and other information of the operator package. You can view the uploaded operator package on the **Operator Management** page.

Figure 4-2 View the uploaded operator package

Operator Package Name	Business Category	Functional Category	Manufacturer	Model Version	Equipment Category	Smart Card Type	Hardware Model	Upload Time	Operation
ITS_StructuredPerson	Structured	Picture Stream Analysis	Dahua	2005 901 001 001	ITS	GPU	Tenda T4	2022-08-19 10:16:48	↕ ⚙
ITS_StructuredVideo	Structured	Video Stream Analysis	Dahua	2005 901 001 003	ITS	GPU	Tenda T4	2022-08-19 10:16:47	↕ ⚙
ITS_FaceAnalysis	Face	Picture Stream Analysis	Dahua	1001 802 000 001	ITS	GPU	Tenda T4	2022-08-19 10:15:23	↕ ⚙
ITS_VehicleAnalysis	Vehicle	Picture Stream Analysis	Dahua	1007 801 000 001	ITS	GPU	Tenda T4	2022-08-19 10:14:15	↕ ⚙
ITS_FaceRetriev	Face	Comparison And Retrieval	Dahua	1001 802 000 001	ITS	CPU	x86_64	2022-08-19 10:13:38	↕ ⚙
ITS_FaceAlarm	Face	Control Alarm	Dahua	1001 802 000 001	ITS	CPU	x86_64	2022-08-19 10:13:38	↕ ⚙
ITS_StructuredRetriev	Structured	Comparison And Retrieval	Dahua	2005 901 001 001	ITS	CPU	x86_64	2022-08-19 10:12:38	↕ ⚙
ITS_VehicleRetriev	Vehicle	Comparison And Retrieval	Dahua	1007 801 000 001	ITS	CPU	x86_64	2022-08-19 10:12:38	↕ ⚙
ITS_FaceAnalysis	Face	Picture Stream Analysis	Dahua	1001 802 000 001	ITS	GPU	Tenda T4	2022-08-19 10:12:48	↕ ⚙

4.2 Creating Network

Create a functional network of face, vehicle, structured, and allocate computing resources for each functional business in the network according to actual application scenarios.

Only one network can be created for each functional business, and the network cannot be repeatedly created.

Step 1 Enter `https://CVEngine IP address:6400` in the browser address bar to go to the login page, and then press Enter.

Step 2 Enter the login username and password, and then click **Login**.

Step 3 After logging in, select **Computing Power Resource Pool**, and then click **Create Network**.

Step 4 Define network name, select business type, and then click **Save**.

Figure 4-3 Create network

The screenshot shows the 'Computing Power Resource Pool' page with the following data:

Resource Type	Distribution Rate	Surplus	Allocated	Total
CPU(Nucleus)	46%	52	44	96
GPU(Individual)	67%	2	4	6

The 'Create Network' dialog box is open, showing the following fields:

- Network Name:** Please enter the network name...
- Business Type:** Face, Vehicle, Structured
- Remarks:** Please enter comments...
- Buttons:** Save, Cancel

Step 5 Select the function category to allocate resources, and then click **Start Allocation**.

- When Business Type is set to Face, select Picture Stream Analysis, Control Alarm, and Comparison And Retrieval.
- When Business Type is set to Vehicle, select Picture Stream Analysis and Comparison And Retrieval.
- When Business Type is set to Structured, select Picture Stream Analysis, Comparison And Retrieval, and Video Stream Analysis.

Figure 4-4 Select function category

Step 6 Select the function category from the top of the right area, and set the computing power specification required by a single application and number of application.

- Click **-/+** or enter the value to set the specification.
- Click **Restore default specifications** to restore to the default specifications.
- Click **+** to add a new function category; select a function category, and then click **Delete Configuration** to delete it.
- Drag the smart card frame from the **Allocatable Resource pool** area on the left to the right area to add a smart card. Each function category supports adding one smart card at most.



- The application here refers to the operator. You can set the computing power resources required by each operator and the number of operators according to your actual needs.
- The **Allocatable Resource pool** area on the left shows the remaining resources that can be allocated (including CPU, Tesla smart card, AIC smart card and AIX smart card). Resources in red means the resources are insufficient and cannot be allocated any more.

Figure 4-5 Configure operator

Step 7 Click Complete Allocation.

Table 4-1 Specifications of operators

Business Type	Operator	Specification
Face	Picture stream analysis	T4 × 1, CPU× 4
Face	Control alarm	CPU× 28 (cannot be less than 10)
Face	Comparison and retrieval	CPU× 28 (reduce it if the resource is not enough, but the performance will be reduced)
Vehicle	Picture stream analysis	T4 × 1, CPU× 4
Vehicle	Comparison and retrieval	CPU× 28 (reduce it if the resource is not enough, but the performance will be reduced)
Structured	Picture stream analysis	T4 × 1, CPU× 4
Structured	Video stream analysis	T4 × 1, CPU× 4
Structured	Comparison and retrieval	CPU× 28 (reduce it if the resource is not enough, but the performance will be reduced)

4.3 Deploying Algorithm

Deploy algorithm programs of devices in the same network according to the uploaded model version, to ensure that the algorithm version is unified.

Step 1 Enter `https://CPEngine IP address:6400` in the browser address bar to go to the login page, and then press Enter.

Step 2 Enter the login username and password, and then click **Login**.

Step 3 Click **Algorithm Deployment**, and then select network, such as **Face Network**.

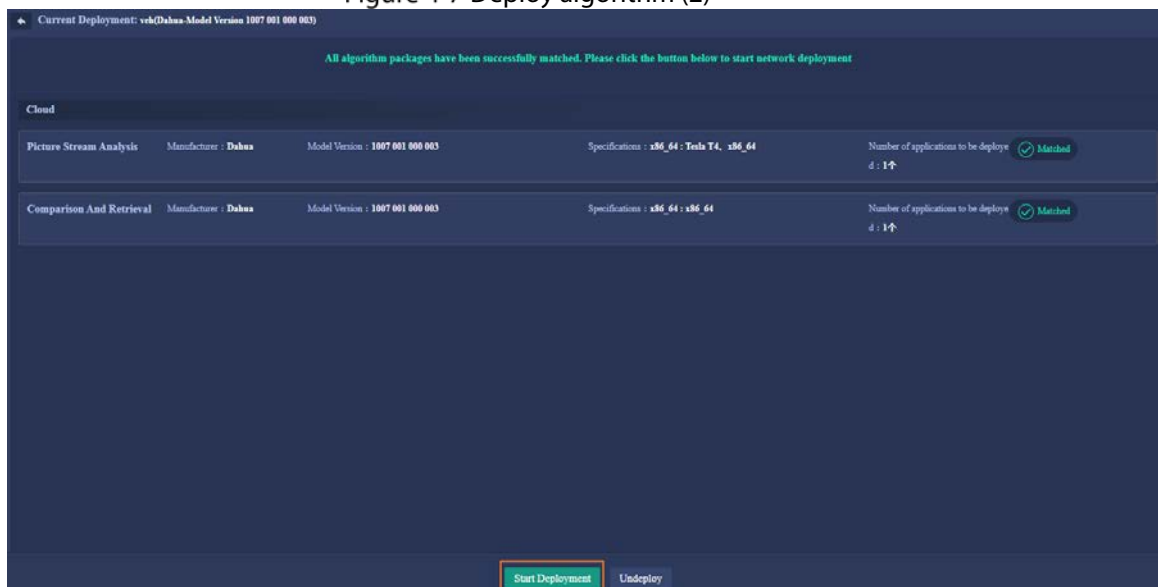
Step 4 Drag the model version to be updated on the right side to the **Drag in the model version to start deployment** area.

Figure 4-6 Deploy algorithm (1)



Step 5 Click Start Deployment.

Figure 4-7 Deploy algorithm (2)



If the system detects that the algorithm package is missing, it can stop the deployment or force the deployment according to the actual situation (only the algorithm package that matched successfully will be deployed).



You need to add the operator IP to the RTSP allowlist: Log in to the platform webpage (<https://C9100/IP:8320>), select **System Config > RTSP IP allowlist Config**, click **Add**, and then add the operator IP to the allowlist.

Figure 4-8 Add allowlist

Start IP	End IP	Operation
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]
192.168.1.1	192.168.1.255	[edit] [delete]

Appendix 1 Safety Inspection Checklist for Server Installation

Appendix 1.1 Server Rack Inspection Checklist

No.	Item
1	Place the rack according to the requirements of the engineering design drawings.
2	When there is anti-static floor in the server room, the bracket installation position and the distance between brackets must be consistent with the installation hole diagram.
3	When there is anti-static floor in the server room, make sure that each bracket is secured to the ground and installed correctly.
4	When there is anti-static floor in the server room, install the bracket assembly correctly.
5	When there is anti-static floor in the server room, and a floor support needs is required, install anti-static floor supports properly and at the same height.
6	The rack is well insulated from the bracket (or ground).
7	Install the top and bottom of the rack with plastic covers to avoid damages caused by rats.
8	Accessories such as side doors, front and rear doors are required.
9	Row labels, column labels, and product labels must be applied correctly and completely.
10	Insert the ESD wrist strap into the ESD mounting hole on the rack.
11	When racks are combined, the connecting plate of the racks must be properly installed.
12	Insulation is required when connecting vibration-proof components between multiple rows of racks.
13	All screws must be fully tightened, and flat washers and spring washers must be installed. The flat washers and spring washers must not be reversed.
14	Keep the rack stable and neat.
15	Keep adjacent racks close, and the surfaces of the entire row and column of racks must be on the same plane with no bumps.
16	The vertical deviation of the rack is less than 3 mm.
17	The side doors on the both sides of channels must be aligned straight, with the error less than 5 mm.
18	The surface of the rack must be clean and tidy (no stains, fingerprints), and the paint decoration is intact. Make sure that there is no dust, residual wire buckles and other sundries in the rack (including dead corners).
19	The various signs on the rack are correct, clear and complete.
20	Install the front and rear doors of the rack, and make sure that the doors can be opened and closed smoothly.
21	Align the modules in the rack.

No.	Item
22	Install all the dummy panels.
23	Install the boards properly, and correctly set DIP switches.
24	The parts on the rack shall not fall off or be damaged, and the connections shall not be damaged or broken.
25	The paint of each part of the rack are not peeled off, bumped or deformed.

Appendix 1.2 Power Cable Inspection Checklist

No.	Item
1	Use blue cable for the -48V power cable, black cable for the RTN power cable, and yellow-green cable for the PGND cable. In special circumstances, follow the requirements in actual situations.
2	Use copper core cables for all the power cables and protective grounding cables.
3	The cross-sectional area of the power cable and protective grounding cable connected to the PDF cannot be less than 95 mm ² . In special circumstances, follow the requirements in actual situations.
4	The cross-sectional area of the power cable and the protective grounding cable connected from the PDF to the rack cannot be less than 25 mm ² . In special circumstances, follow the requirements in actual situations.
5	The power cable and the protective grounding cable are intact without damage or breakage.
6	The power cable and the protective grounding cable must be made of a whole section of material, with no joints in the middle of the cable.
7	Do not connect devices such as switches and fuses in the electrical connection path of the grounding system.
8	Cut off the excessive parts of the power cable and the protective grounding cable. Do not coil these excessive parts.
9	Adopt dual-circuit hot backup method when connecting the cable from the DC power distribution panel to the PDF.
10	Connect the GND ground row and the PGND ground row provided by the customer to the same grounding body.
11	Ground resistance < 10 Ω.
12	After the PDF grounding wire is led to the positive pole of the DC power distribution panel, use a cable with the diameter that meets specification requirements when leading to the ground.
13	Reliably connect the PGND grounding row of PDF to the protective grounding row provided by the bureau.
14	PDF and output current limiting insurance of DC distribution screen should meet the requirements.
15	Do not short circuit or reversely connect the power cables and ground cables.
16	Firmly solder or crimp the OT terminals of the power cable and the protective grounding cable.
17	Do not expose the bare wires at the terminals and the OT terminal handle. Tightly wrap them with insulating tape or cover them with heat-shrinkable sleeves.
18	Firmly install each OT terminal with a flat washer and a spring washer. Make sure that the terminal and the washers are in good contact.

No.	Item
19	When two or more cables are installed on one terminal, adopt cross-installation or back-to-back installation, and bend the OT terminals at 45° or 90° if the terminals must be overlapped. If overlapped, make sure that the smaller OT terminal is over the larger OT terminal.
20	Correctly install the power cable and ground cable from the power distribution box to each functional module, and the protective grounding cable between each module and the PGND bus bar of the rack. Make sure that the connected cables are in good contact.
21	For the side door, front door and rear door of the rack, connect a 6 mm ² yellow-green cable to the grounding bolt on the lower enclosure frame of the rack.
22	Power cables and protective grounding cables should be bundled separately from other cables.
23	When the terminals of the power cable and the protective grounding cable are connected to the terminals in the frame and the PDF, ensure straight wiring and neat binding, and mark the frame number on the PDF switch.
24	Attach the power cable engineering labels to both ends of the power cable and the protective grounding cable.
25	Install the power cable of the alarm box with a PVC cable duct on the wall.

Appendix 1.3 Signal Cable Inspection Checklist

No.	Item
1	The signal cable routing should be consistent with the engineering design drawings.
2	Make sure that there is no connector in the middle of any signal cable.
3	The signal cable cannot be damaged or broken.
4	Signal cable plugs must be intact, and installed correctly and securely.
5	Thread the signal cables for easy maintenance and capacity expansion in the future.
6	When the signal cable is routed on the cable tray, if there is only a cable ladder, the signal cable should be fixed on the beam of the cable ladder with a cable tie. If a cable slot is available, you do not have to bind the signal cable, but you need to straighten the cables in the slot. Do not cross and overflow the channel of the slot. Bind and connect the signal cable in series at the part where the signal cable enters and exits the channel and where the signal cable turns.
7	Leave appropriate part at the signal cable plug for easy plugging.
8	Leave appropriate part of signal cable at the turning point, and the turning radius should meet the requirements of various cables.
9	When threading out the signal cable from rack, leave appropriate part at the outlet of the rack to protect the cable.
10	When threading out the signal cable from the cabling tray, leave appropriate part at the outlet hole to protect the cable.
11	The cables with the plugs farther from the upper line should be arranged on the outside of the cable harness, and the cables with the plugs closer to the upper line should be arranged on the inner side of the cable harness.
12	When the signal cable is led out of the subrack, follow the principle of "left line goes left, and right line goes right".
13	When laying optical fibers out of the rack, be sure to use plastic corrugated protective sleeves, and bind and fix both ends of the protective sleeves. The openings at both ends of the protective sleeves must be smooth (or cut-resistant).
14	When laying out the optical fibers, the bends should not be too tight or intertwined with each other. Straighten and bundle the paired optical fibers with appropriate binding force. Make sure that the optical fibers can be freely twitched in the wire buckle.
15	After laying out the fiber cable, make sure that there are no other cables pressing on the fiber.
16	During installation, coil the redundant fiber in a rear-mounted fiber-optic box behind the switch rack.
17	For laid optical fibers not in use, install a fiber cap on the optical connector to protect the optical fiber.
18	Protect the signal cable of the alarm box with PVC wire ducts on the wall. Coil the redundant part of the signal cable, and place the redundant part under the floor on the side of the alarm box or on the cable ladder.
19	Bundle signal cables separately from power cables.

No.	Item
20	Make sure that the binding of signal cables is neat and beautiful, with uniform spacing between wire buckles, moderate tightness, and consistent orientation.
21	All wire buckles should be cut flat.
22	The signs at both ends of signal cables should be clear (labeled), neatly positioned and oriented in the same direction.

Appendix 2 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

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883