Event Detection Intelligent Server

Deployment Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

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
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	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

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

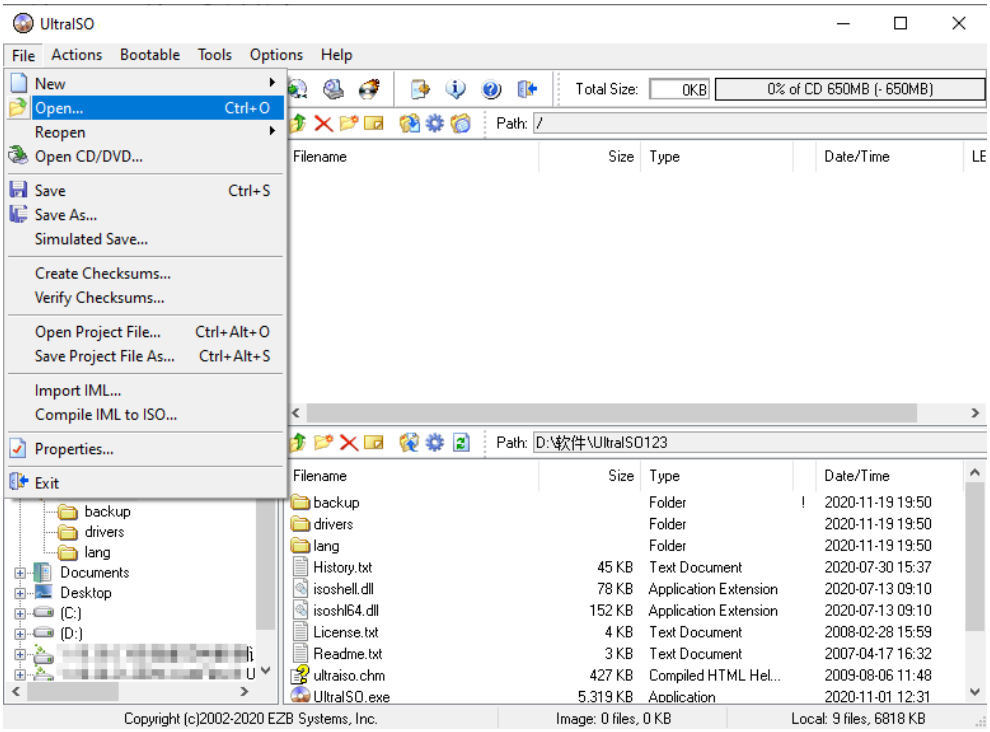
Skip this chapter if CentOS 7.4 system has been installed on the server.

Procedure

Step 1 Double-click  to open UltraISO.

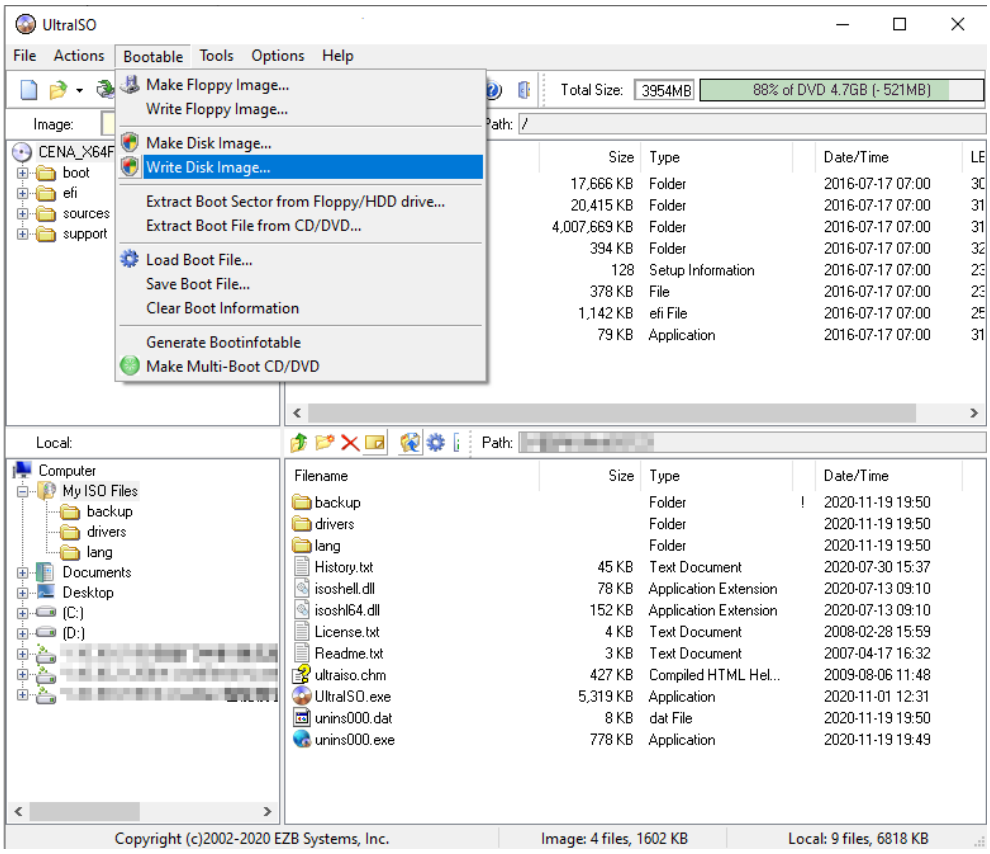
Step 2 Select **File** > **Open**, select the CentOS 7.4 installation package, and then click **Open**.

Figure 1-1 Open file



Step 3 Select **Bootable** > **Write Disk Image**.

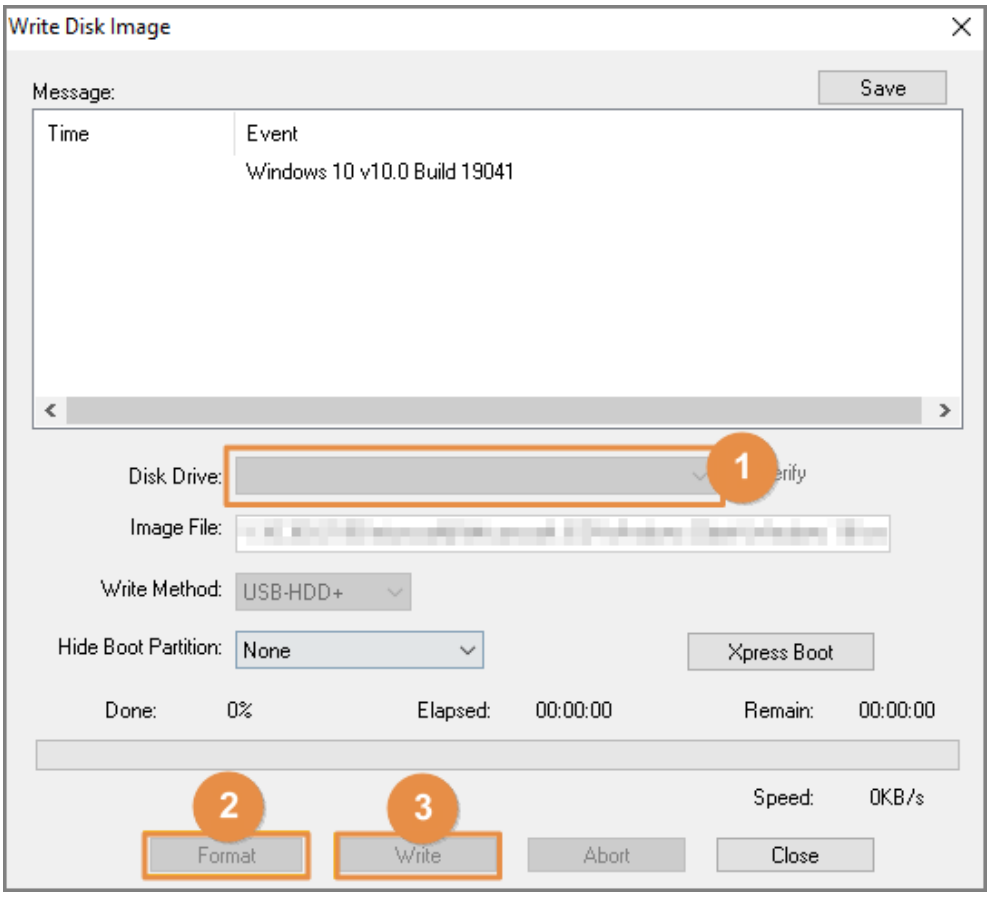
Figure 1-2 Write disk image (1)



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

Generally, you only need to leave them as default.

Figure 1-3 Write disk image (2)



Step 5 Click **Yes** in the pop-up window.

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

Step 6 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.

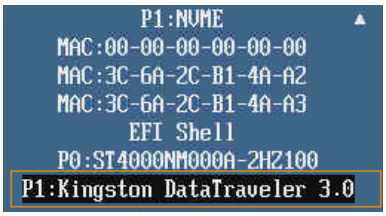
Different servers have different boot options. Refer to the options of the actual server.

1.2.3 Selecting USB Flash Drive

Background Information

Select the corresponding USB flash drive.

Figure 1-4 Select USB flash drive



1.2.4 Selecting Operating System

Background Information

Select **Install CentOS 7**.

Figure 1-5 Select operating system

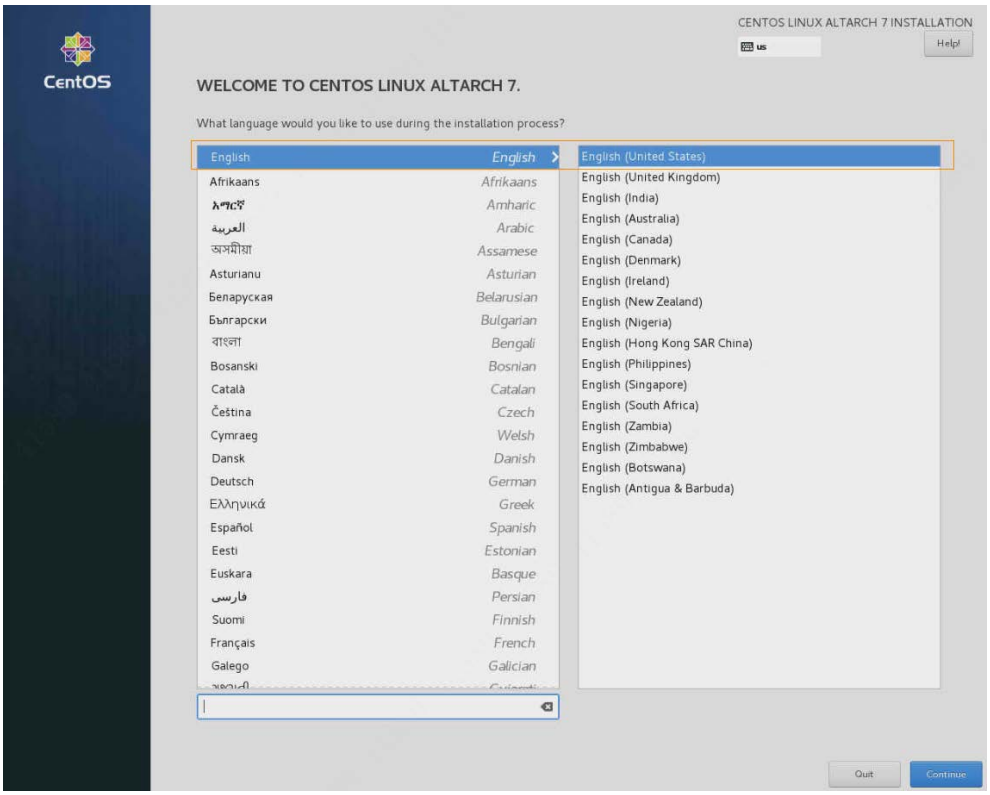
1.2.5 Selecting Language

Procedure

Step 1 Select **English** > **English (United States)**.

Step 2 Click **Continue** at the lower-right side.

Figure 1-6 Installation

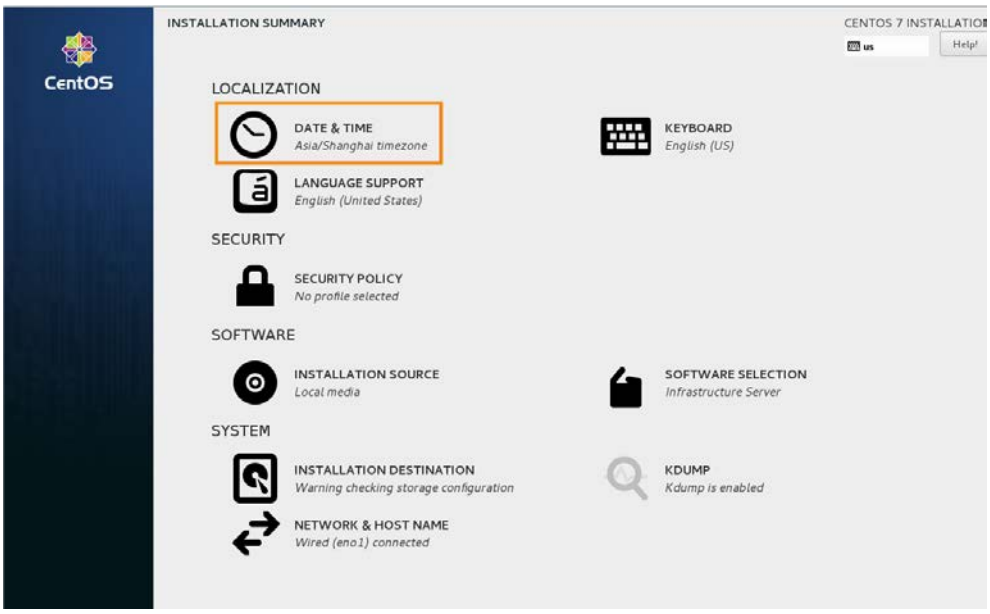


1.2.6 Setting System Time

Procedure

Step 1 On the **INSTALLATION SUMMARY** interface, click **DATE & TIME**.

Figure 1-7 Modify time (1)



Step 2 Set **Region** as **Asia**, set **City** as **Shanghai**, and leave the other parameters as default.

Figure 1-8 Modify time (2)

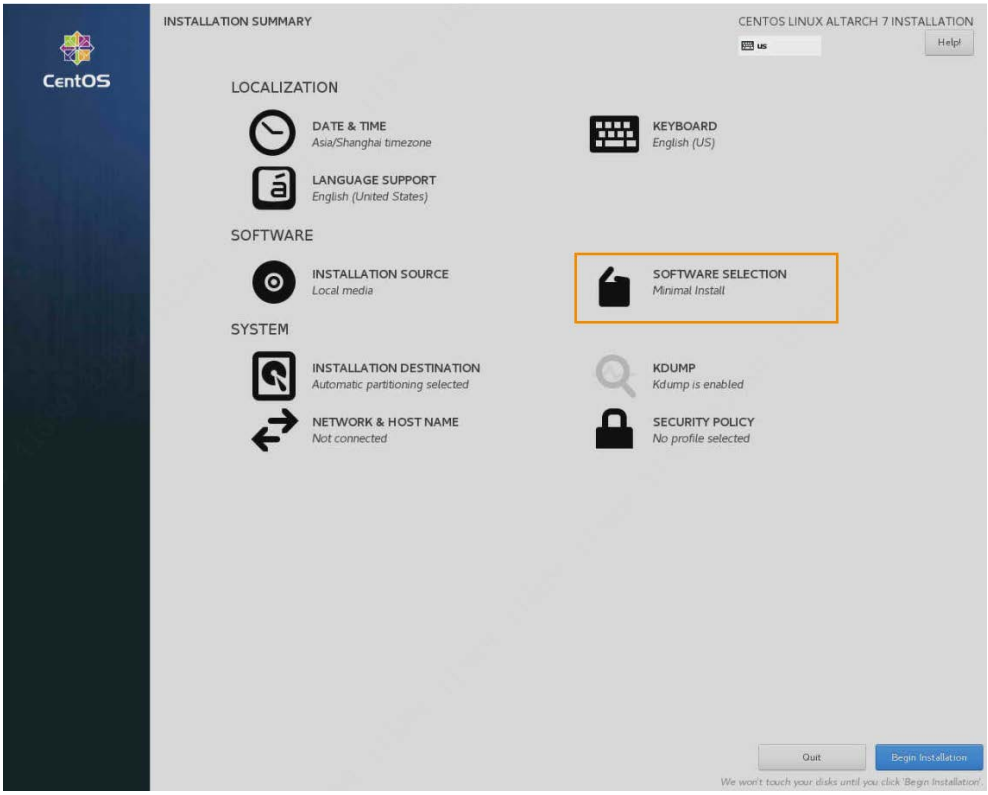
Step 3 Click **Done** at the upper-left side.

1.2.7 Selecting Software Installation Mode

Procedure

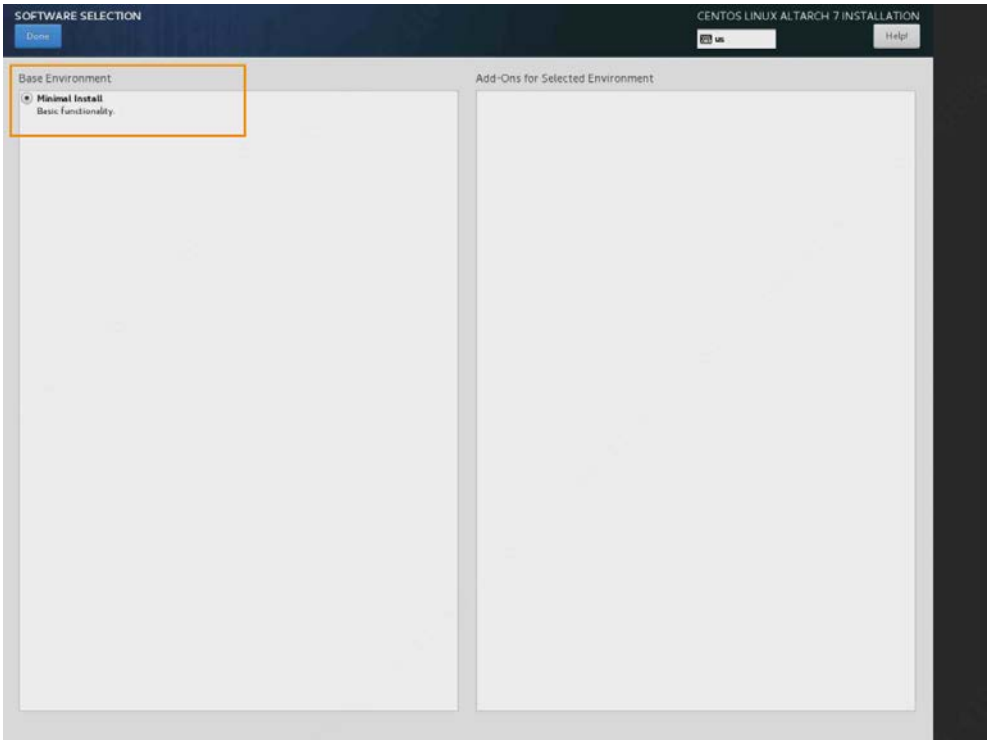
Step 1 On the **INSTALLATION SUMMARY** interface, click **SOFTWARE SELECTION**.

Figure 1-9 Installation (1)



Step 2 Select **Minimal Install**.

Figure 1-10 Installation (2)



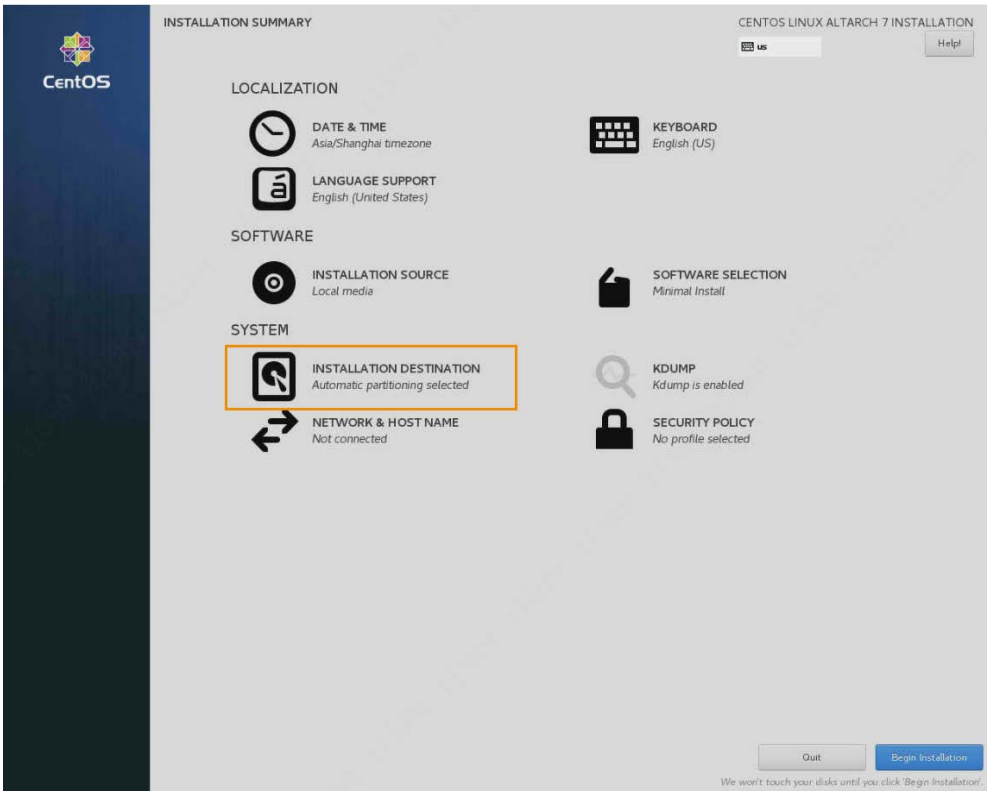
Step 3 Click **Done** at the upper-left side.

1.2.8 Configuring Partition

Procedure

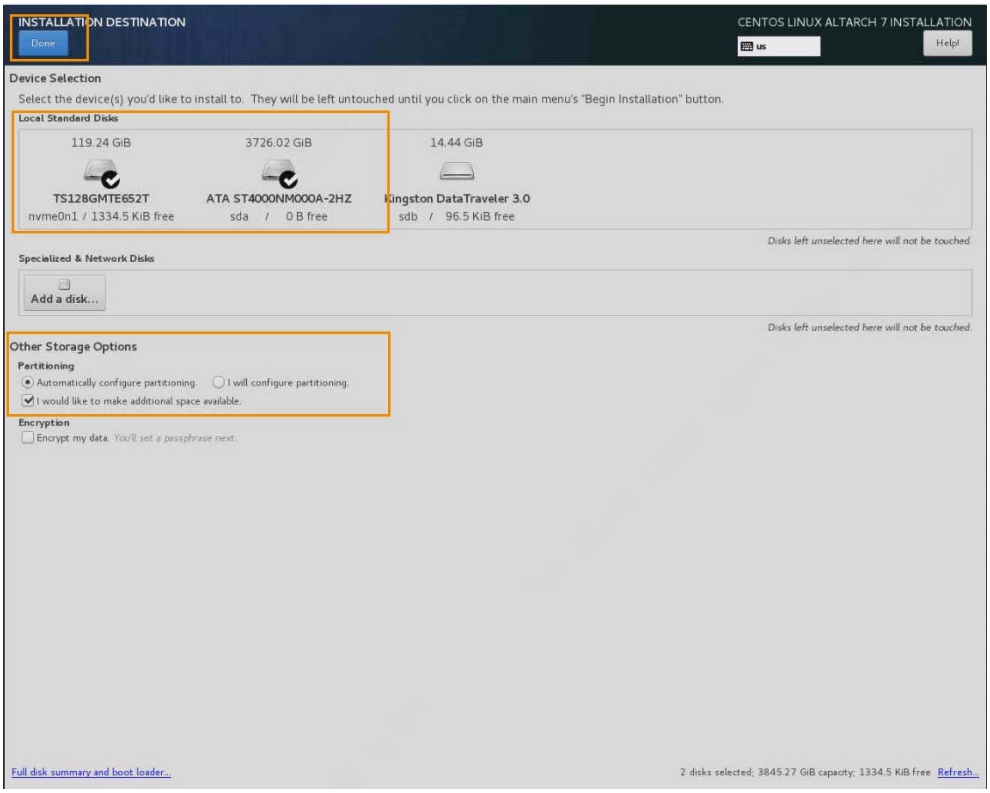
Step 1 On the **INSTALLATION SUMMARY** interface, click **INSTALLATION DESTINATION**.

Figure 1-11 Configure partition (1)



Step 2 Select 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)



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

Figure 1-13 Configure partition (3)

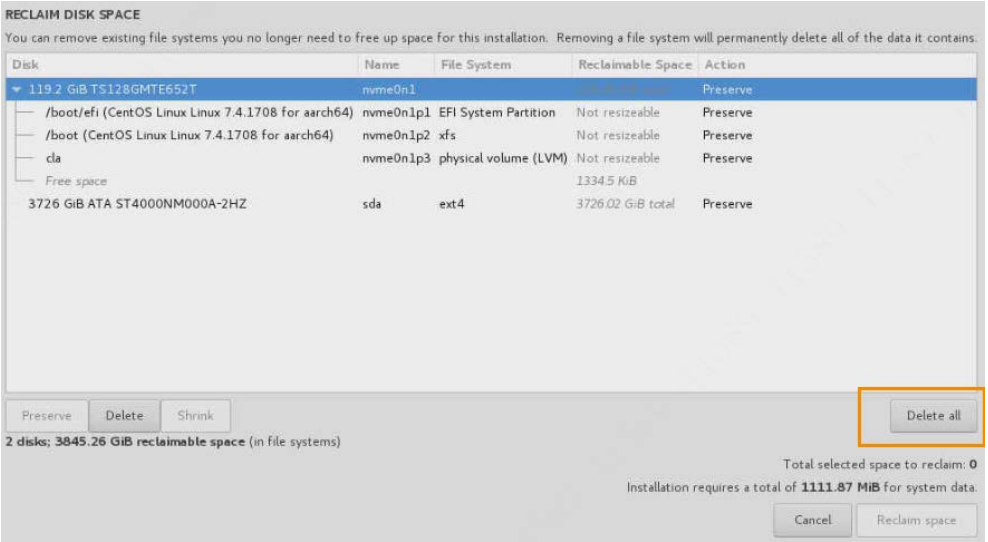
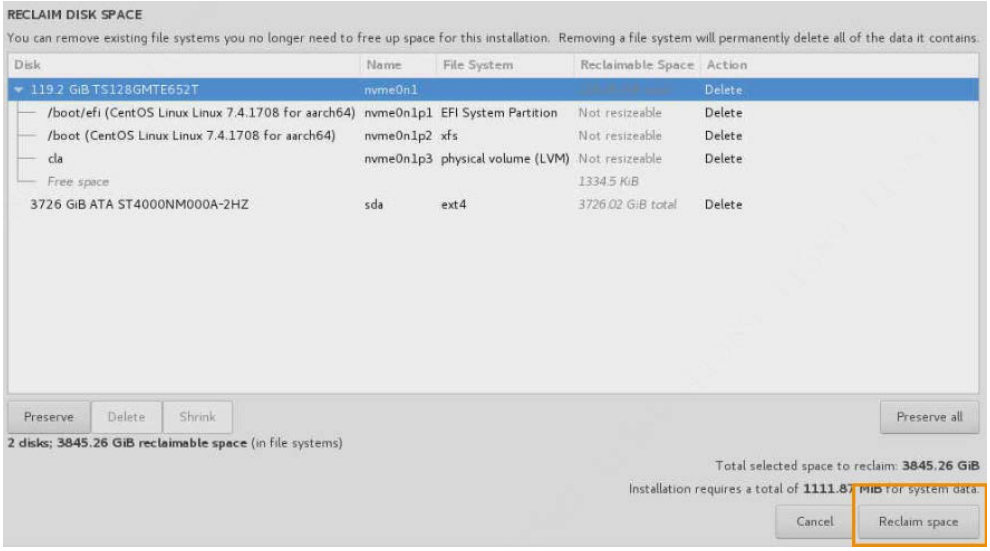
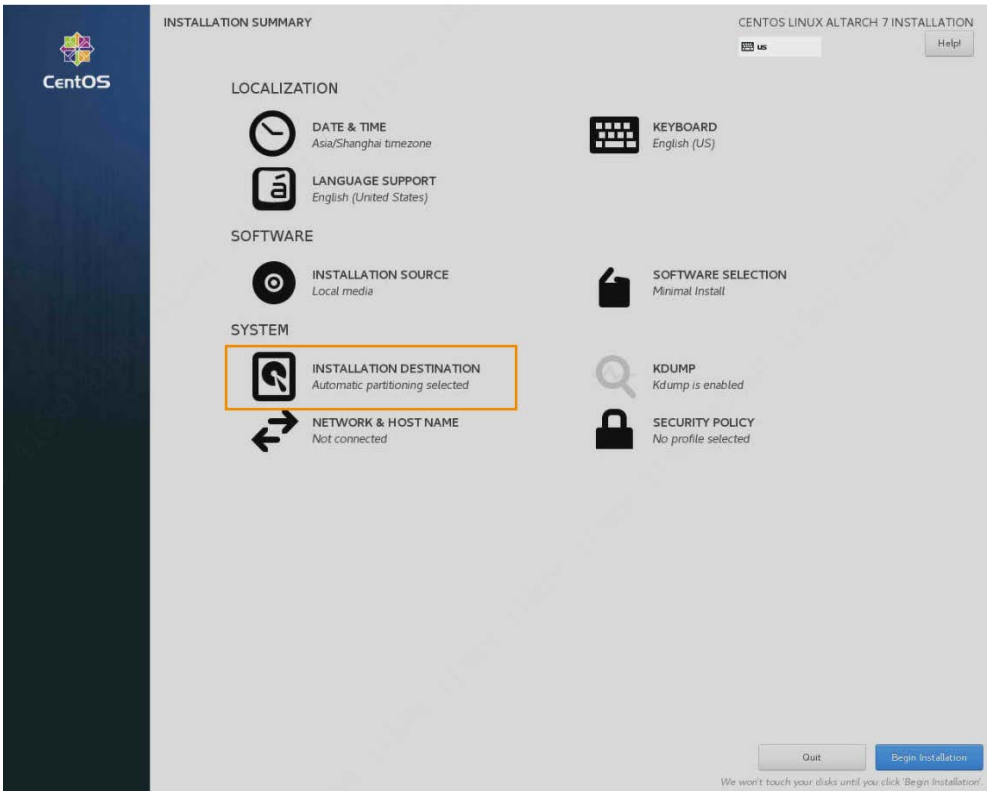


Figure 1-14 Configure partition (4)



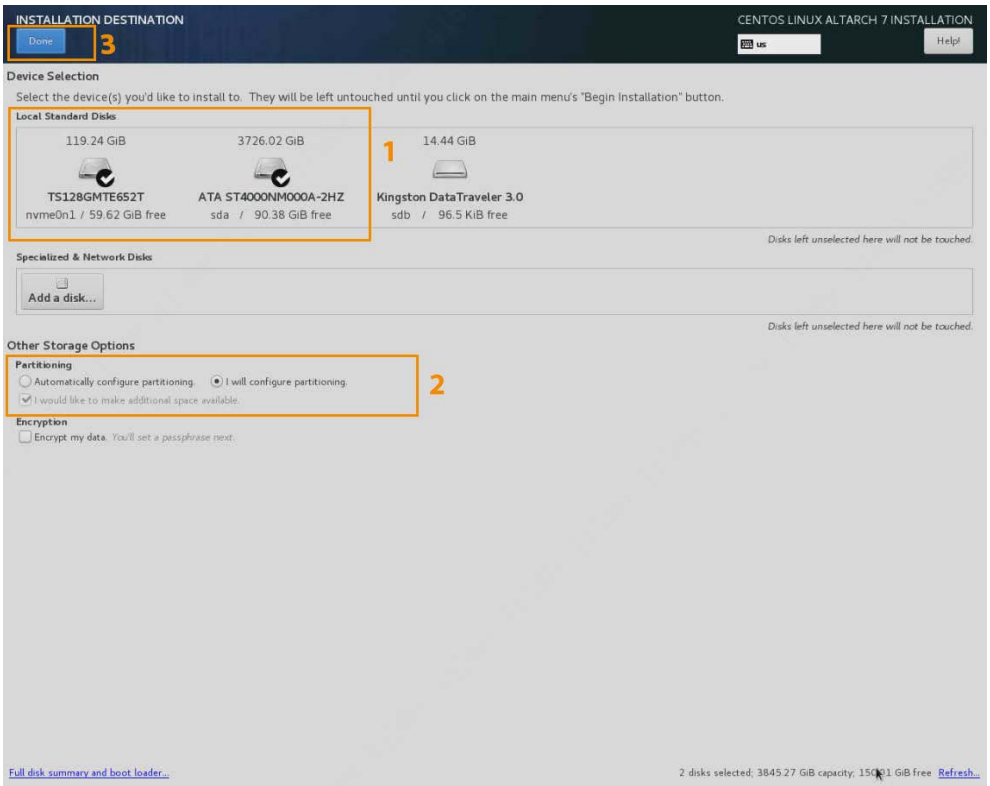
Step 4 Go back to the **INSTALLATION SUMMARY** interface, and then click **INSTALLATION DESTINATION**.

Figure 1-15 Configure partition (5)



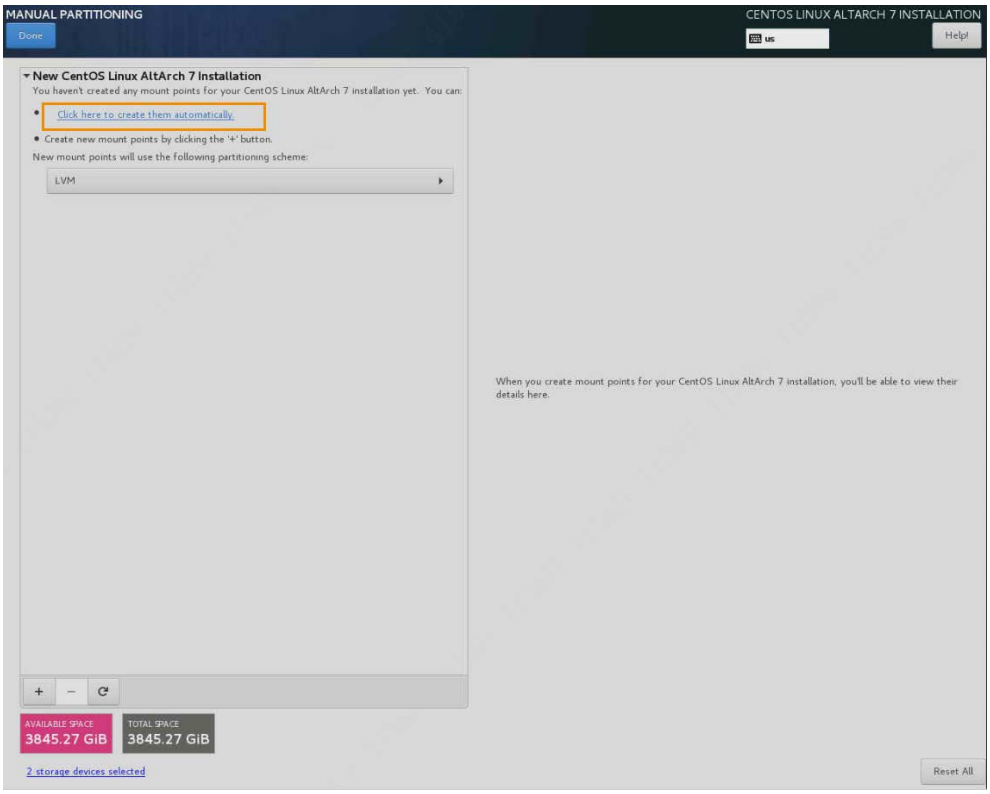
Step 5 Select USB drives from **Local Standard Disks**, select **I will configure partitioning** and **I would like to make additional space available** from **Other Storage Options**, and then click **Done** at the upper-left side.

Figure 1-16 Configure partition (6)



Step 6 Select **Click here to create them automatically**. The system automatically creates partitions.

Figure 1-17 Configure partition (7)



Step 7 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**.

Figure 1-18 Configure partition (8)

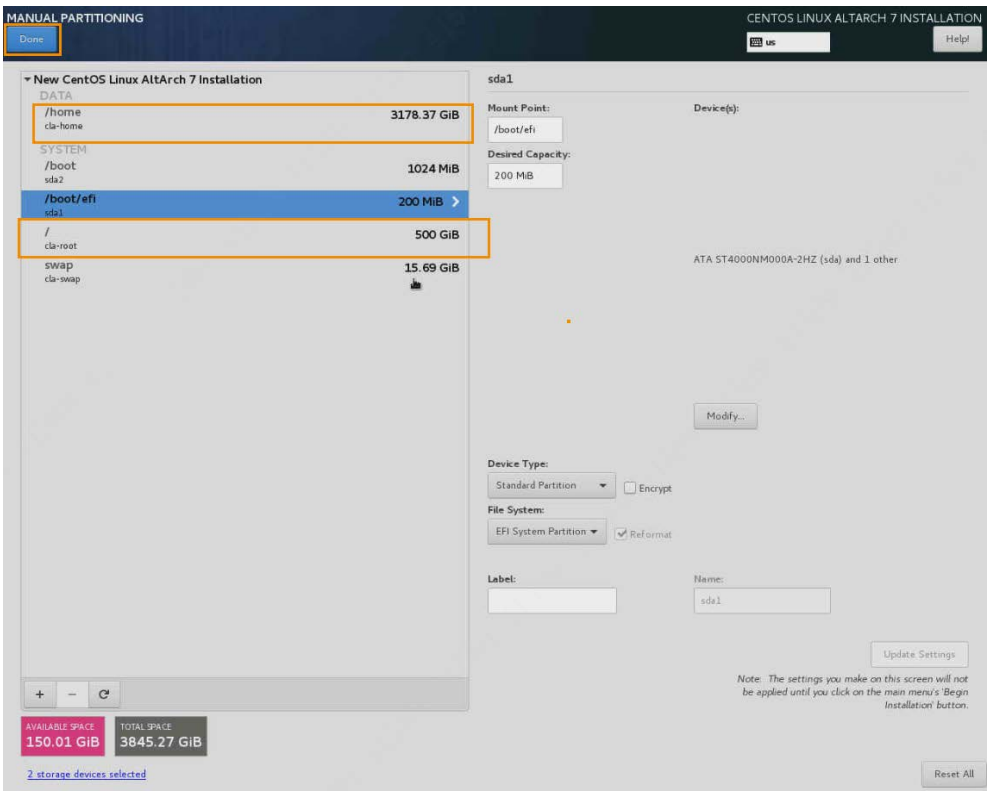
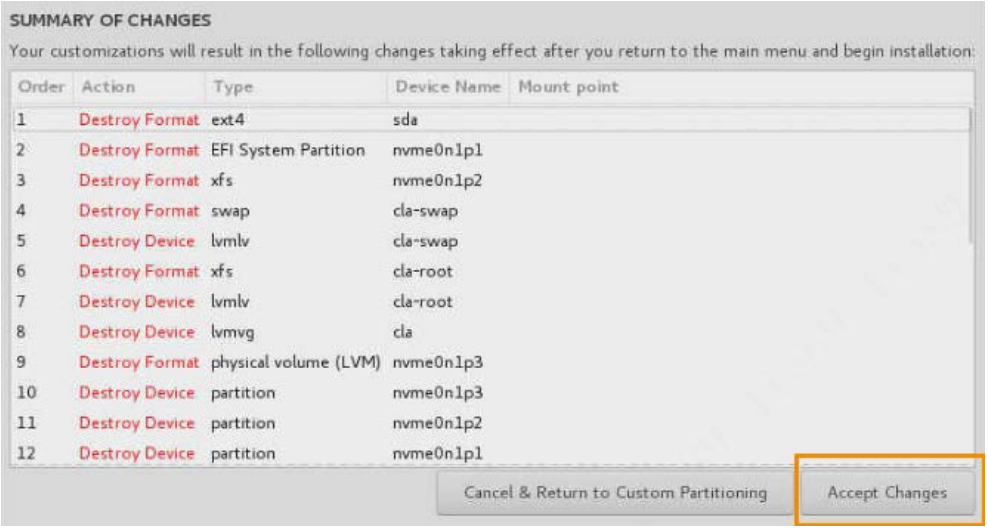


Table 1-2 Configure partition

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)

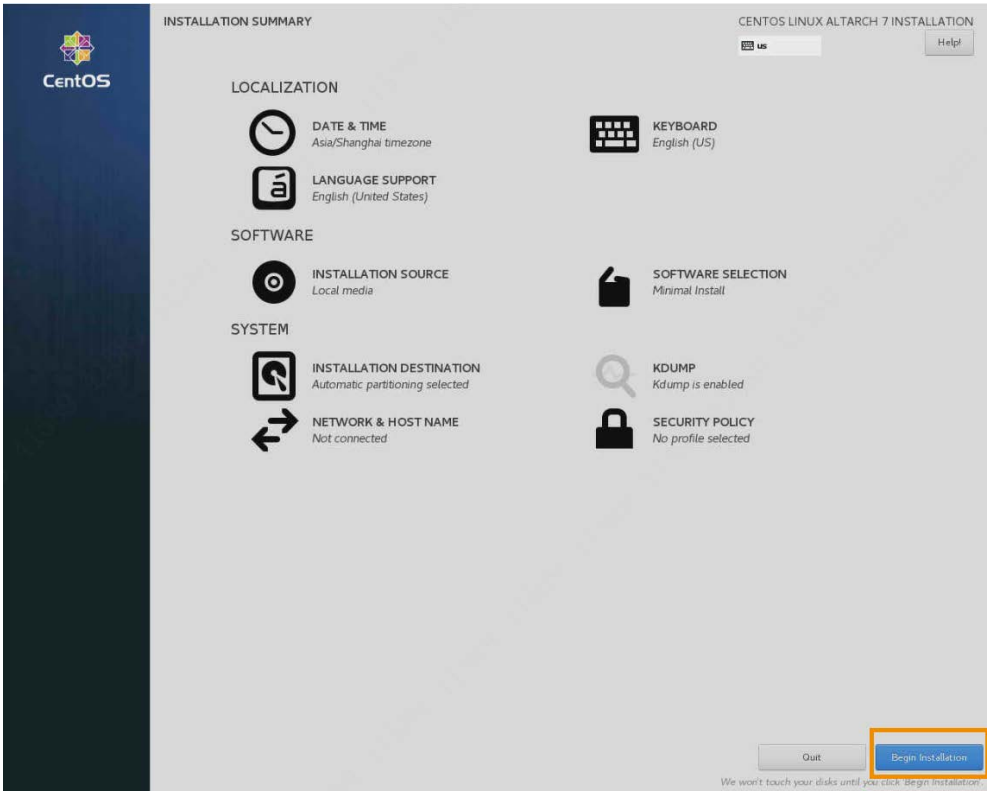


1.2.9 Starting Installation

Background Information

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

Figure 1-20 Installation

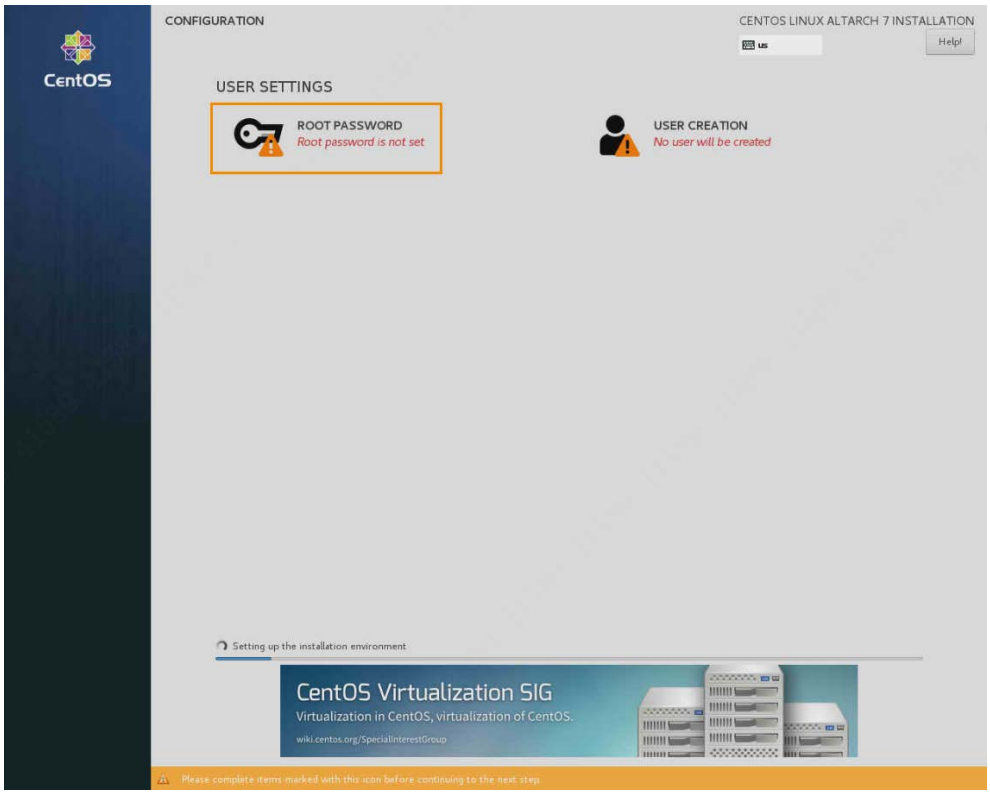


1.2.10 Setting Password

Procedure

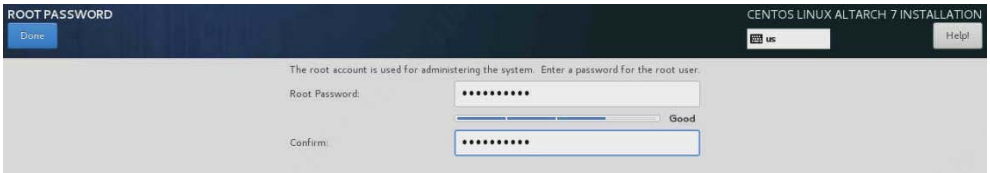
Step 1 On the **CONFIGURATION** interface, click **ROOT PASSWORD**.

Figure 1-21 Set password (1)



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

Figure 1-22 Set password (2)

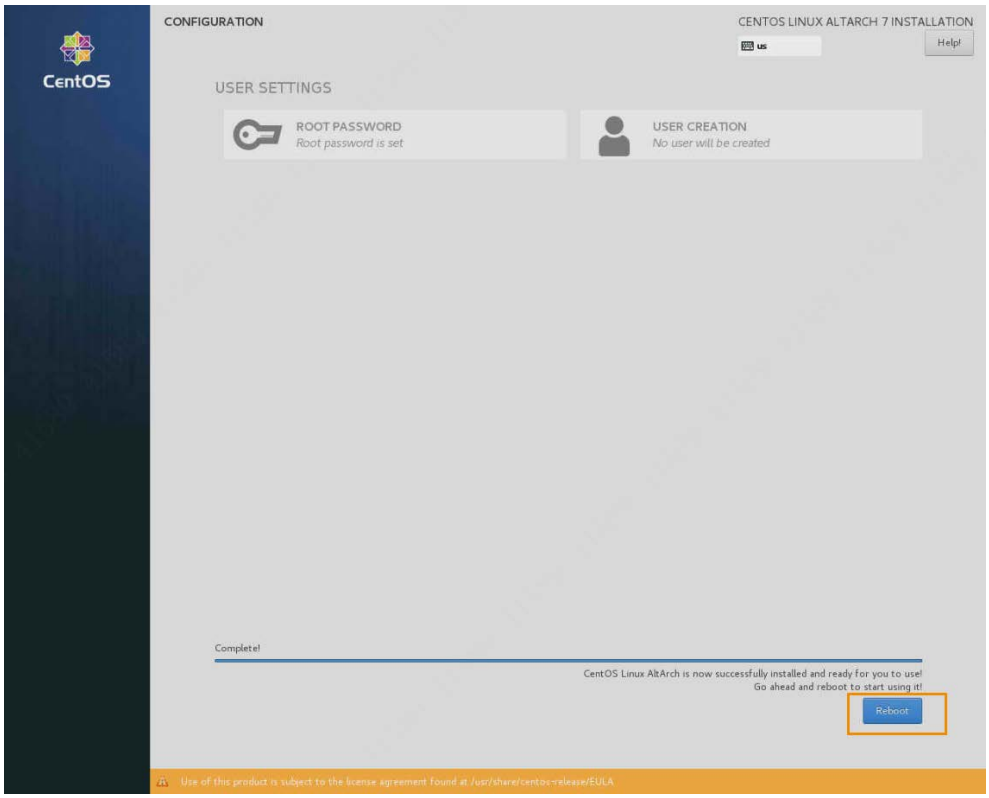


1.2.11 Restarting

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



1.2.12 Installing Basic Package and Driver

Procedure

Step 1 Log in to the CentOS system.

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

Step 2 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

```
[root@localhost ~]#
[root@localhost ~]# date
Mon Oct 11 20:44:27 CST 2021
[root@localhost ~]#
[root@localhost ~]# date -s "2021-10-11 20:45:00"
Mon Oct 11 20:45:00 CST 2021
[root@localhost ~]#
[root@localhost ~]# hwclock -w
[root@localhost ~]#
[root@localhost ~]#
```

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

Step 3 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 **ls** command to view the number of network cards.[root@localhost network-scripts]# **ls**

```
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-TeamPort    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: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

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
```

Step 4 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.

Step 5 Log in to the server remotely through Xshell.

Step 6 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 **ll** 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]# ll
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
    z
-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

Step 7 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

The package name varies with version and release date.

Procedure

Step 1 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 -l**
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.

Figure 2-1 Check the driver

```
[root@rabbitmq1 ~]# 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           |
+===================+=================+=========================================+
[root@rabbitmq1 ~]#
```

Step 2 Install the patch.

1) 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.gz
```

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
```

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

Step 3 Modify script.

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 General_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
HOST_IP=xx.xx.xx.xx                #Change to actual IP address
HOST_GATEWAY=xx.xx.xx.xx           #Change to actual gateway
HOST_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
```

Step 4 Execute the **sh set_bond_config.sh** 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.

Step 5 Execute the **reboot** command to restart the server.

Step 6 Execute the **ifconfig** command to check whether the IP address was successfully modified.

```
[root@rabbitmq1 tools]# ifconfig
bond0: 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

Step 1 Log in to the server remotely through Xshell.

Step 2 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.

Step 3 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).

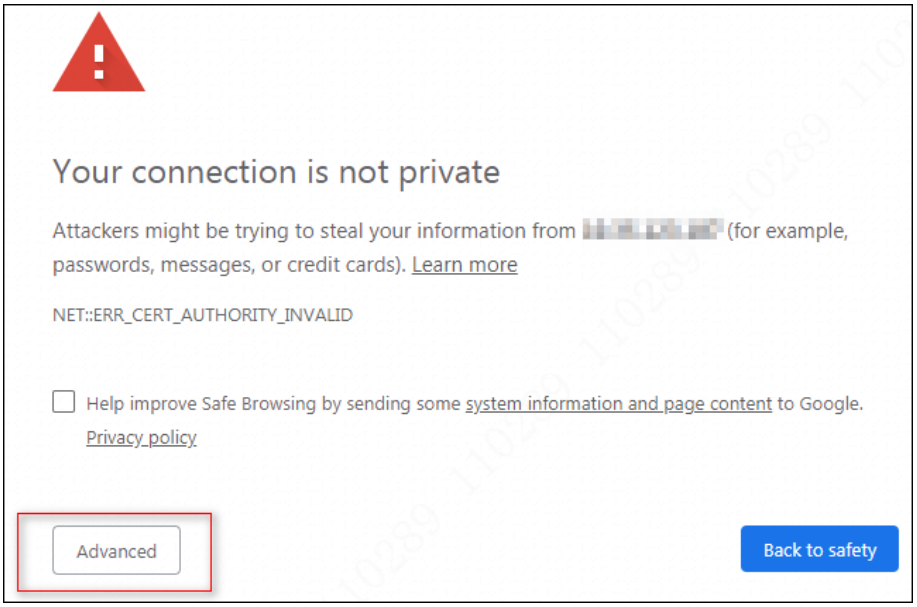
Procedure

Step 1 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.

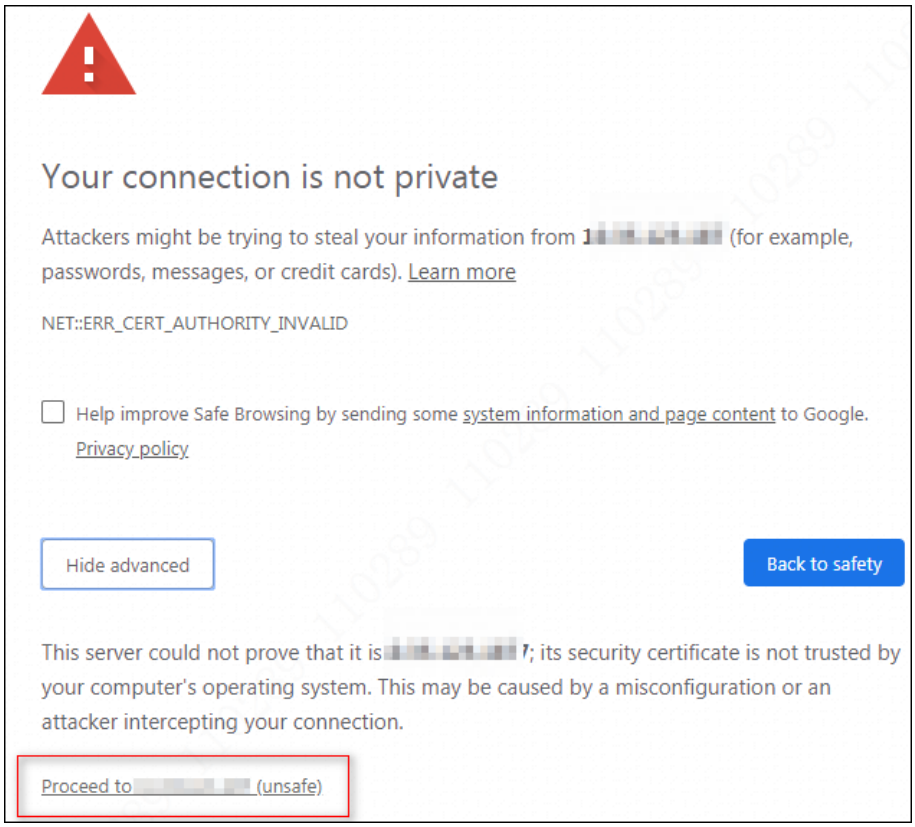
Step 2 Click **Advanced**.

Figure 3-1 Your connection is not private



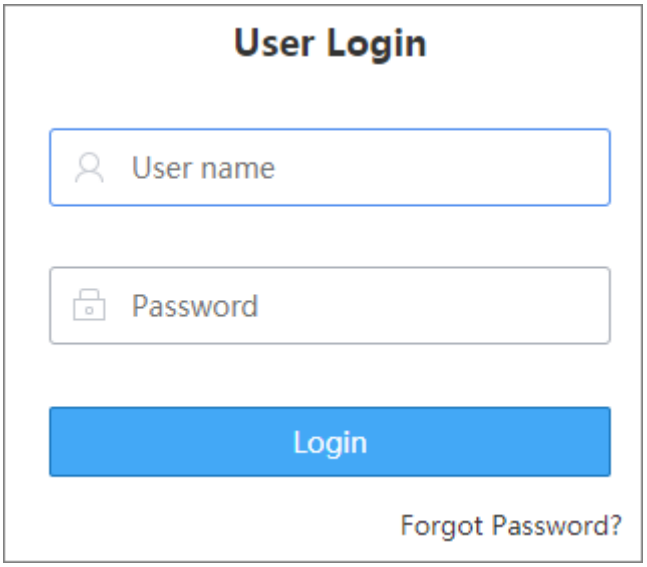
Step 3 Click **Proceed to IP address (unsafe)**.

Figure 3-2 Advanced



Step 4 Enter username and password, and then click **Login**.

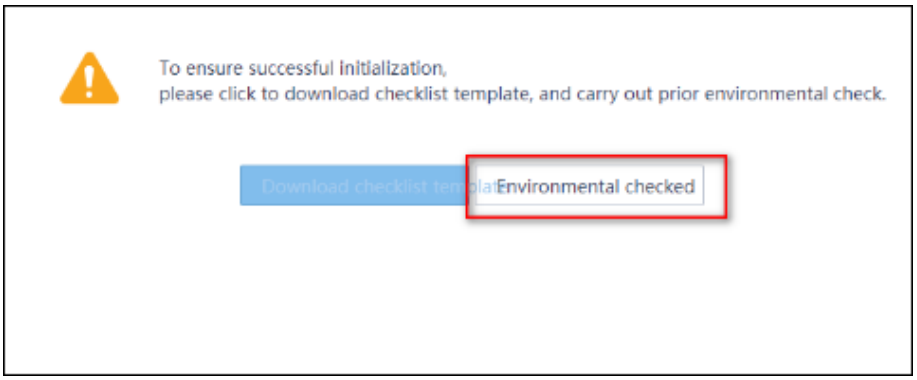
Figure 3-3 Login



- 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".

Step 5 Click **Download checklist template**. Check the items in the checklist template and then click **Environment Checked**.

Figure 3-4 Environment checked



Step 6 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.

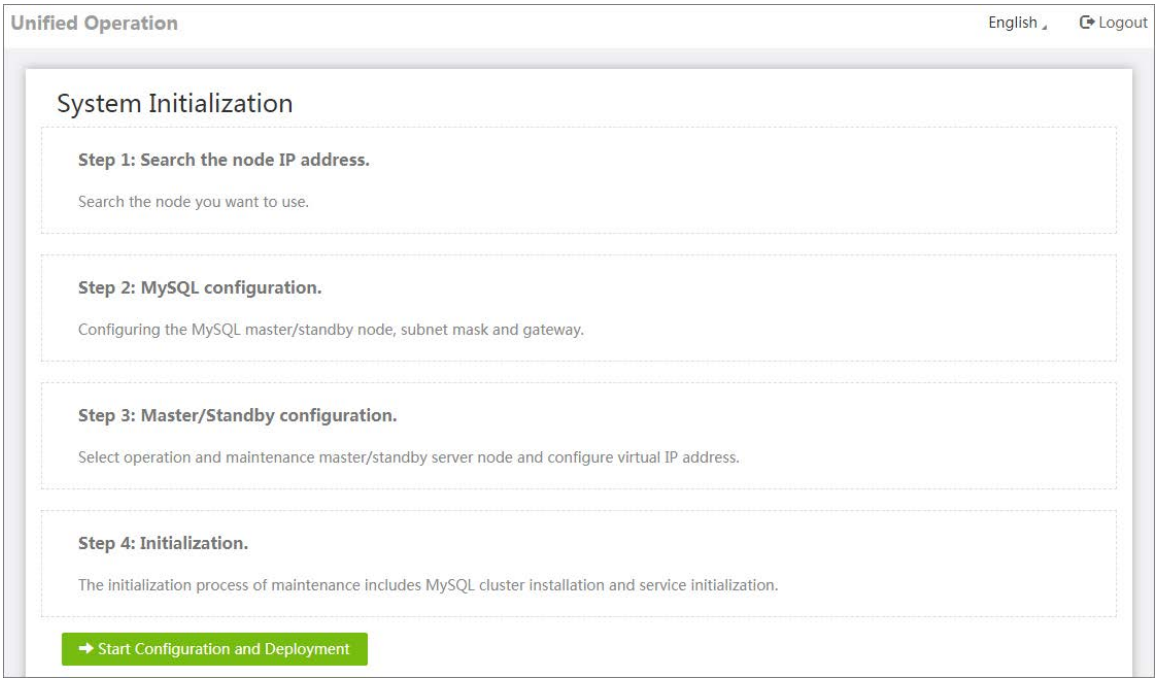
3.2.1 Searching Nodes

Procedure

Step 1 Log in to the Unified Operation platform.

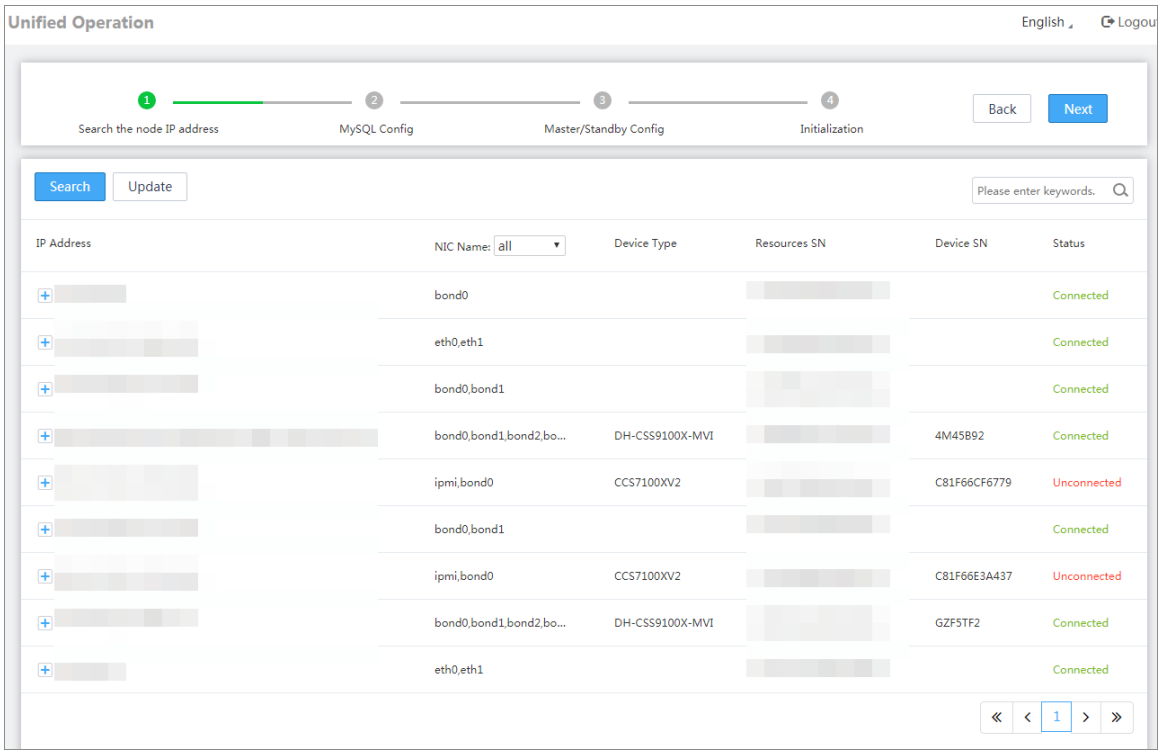
Step 2 Click **Start Configuration and Deployment**.

Figure 3-5 Start configuration and deployment



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

Figure 3-6 Search for servers



Step 4 Click **Next**.

3.2.2 Deploying MySQL

Procedure

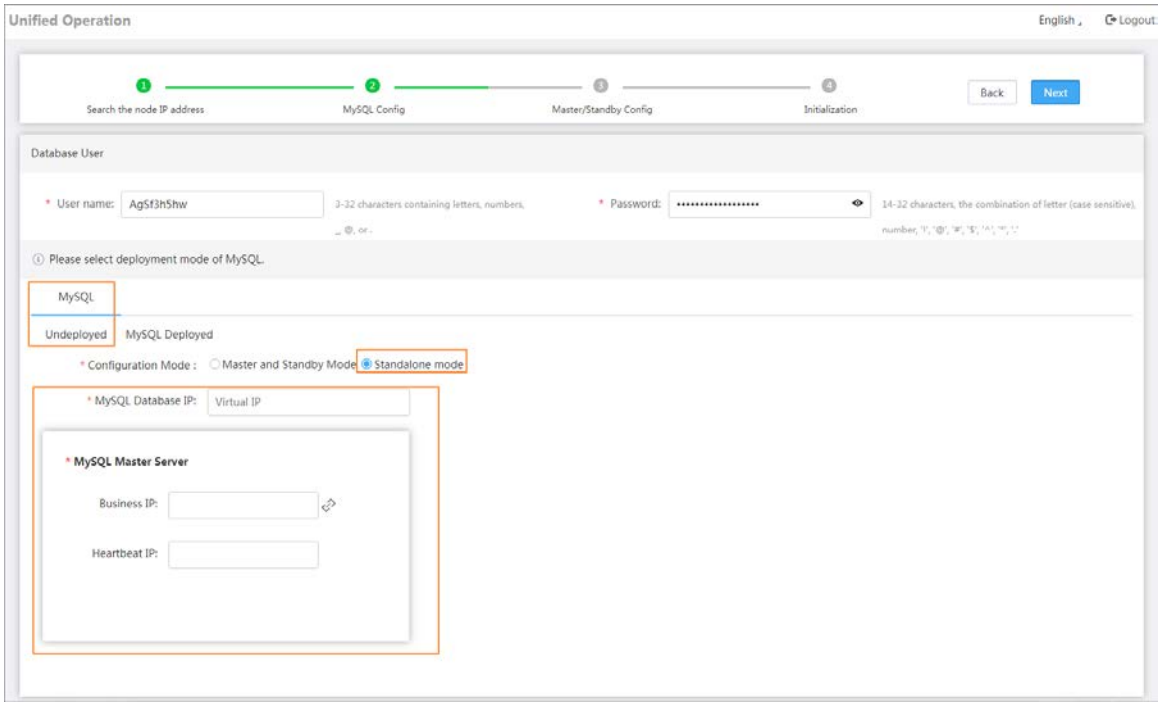
Step 1 On the **MySQL Config** interface, click **MySQL Undeployed**, and then select **Standalone Mode**.

Step 2 Enter server IP in **MySQL Database IP**.

Step 3 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



- 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 to search for IP address.

Step 4 Click **OK** on the pop-up box.

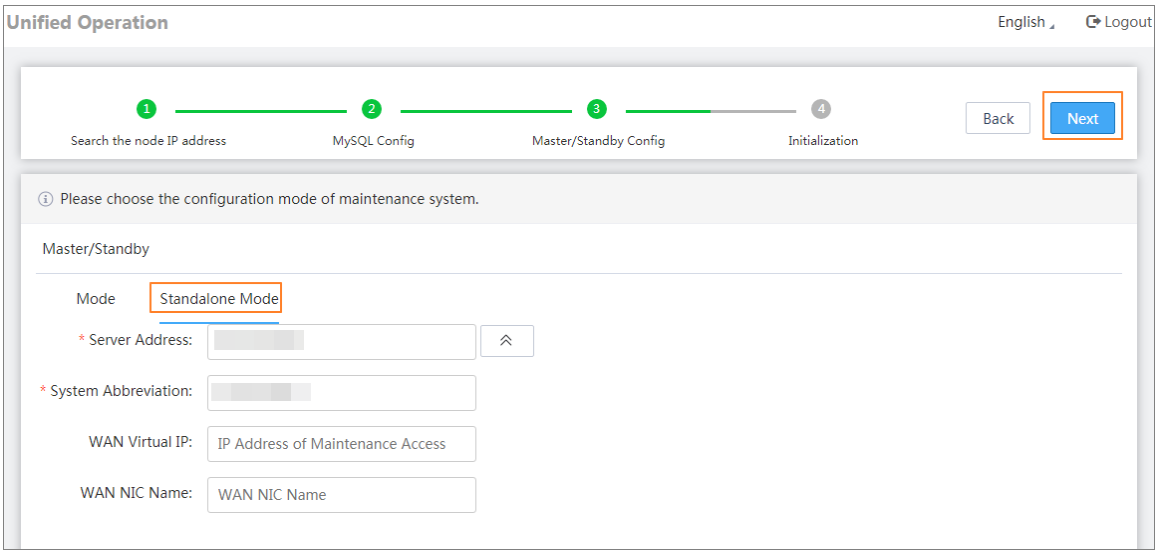
Step 5 Click **Next**.

3.2.3 Selecting Configuration Mode

Procedure

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

Figure 3-8 Select configuration mode



Step 2 In the pop-up window, click **OK**.

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

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

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.

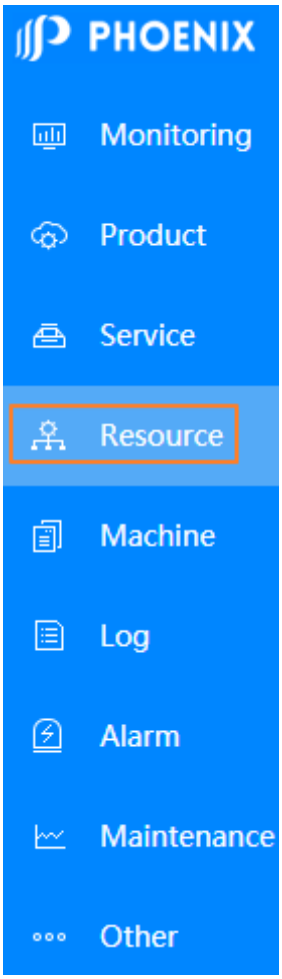
Procedure

Step 1 Use the new password to log in to the Unified Operation platform.

Step 2 In the pop-up window, click **OK**.

Step 3 Select **Resource** from the left navigation bar.

Figure 3-9 Resource



Step 4 Click **Manage**, and then you can start managing servers.

You can manage servers by search or one by one.

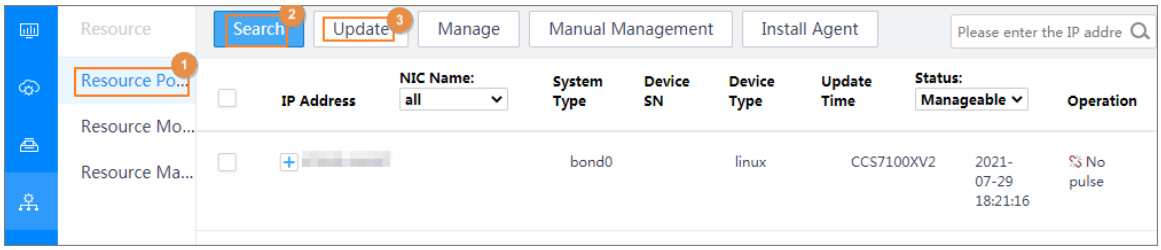
- Manage servers by search

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 Automatically search servers



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

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**.

◇ Manage servers by manual search

1. 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**.

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.

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**.

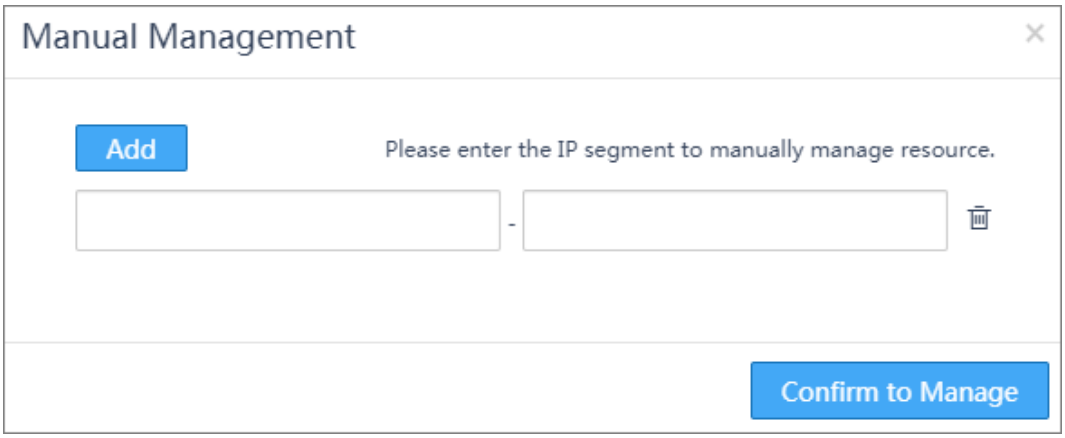
- Manual management

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**.

◇ Click **Add** to add multiple IP sections.

◇ Click to clear the corresponding IP section.

Figure 3-11 Enter server IP



Step 5 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 , enter login password in the pop-up window, and then click **OK**.

4 Installing Event Detection Server

4.1 Managing Product

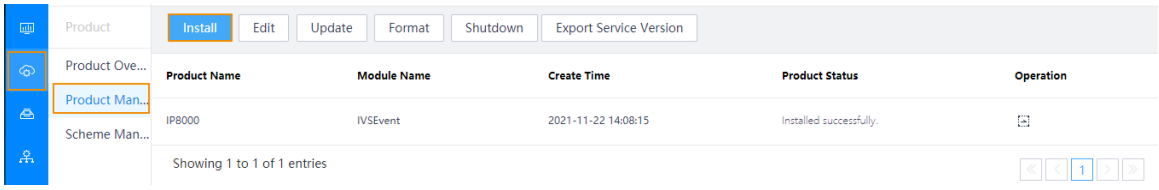
Procedure

Step 1 Log in to the Unified Operation platform.

Step 2 Select **Product** > **Product Management**.

Step 3 Click **Install**.

Figure 4-1 Install server

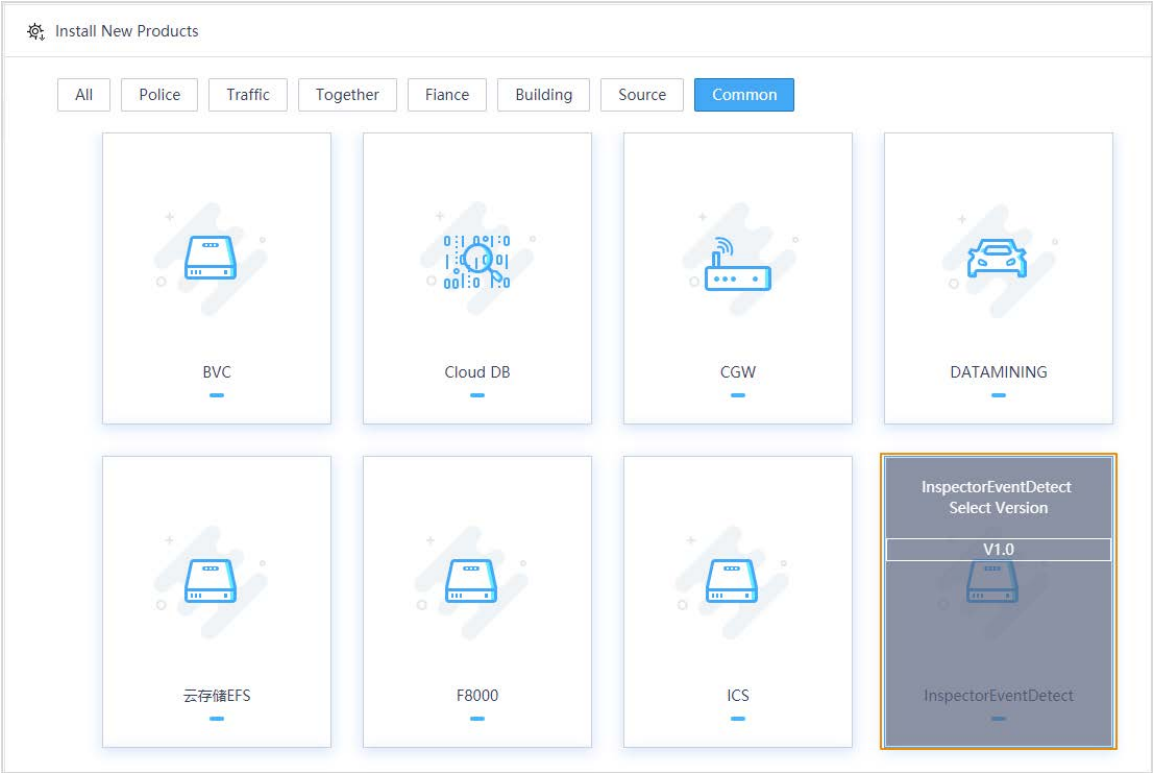


Step 4 Select **Common** > **InspectorEventDetect**, and select the corresponding version of **InspectorEventDetect**.

Step 5 Click **V1.0**.

Only V1.0 is available.

Figure 4-2 Select event detection server

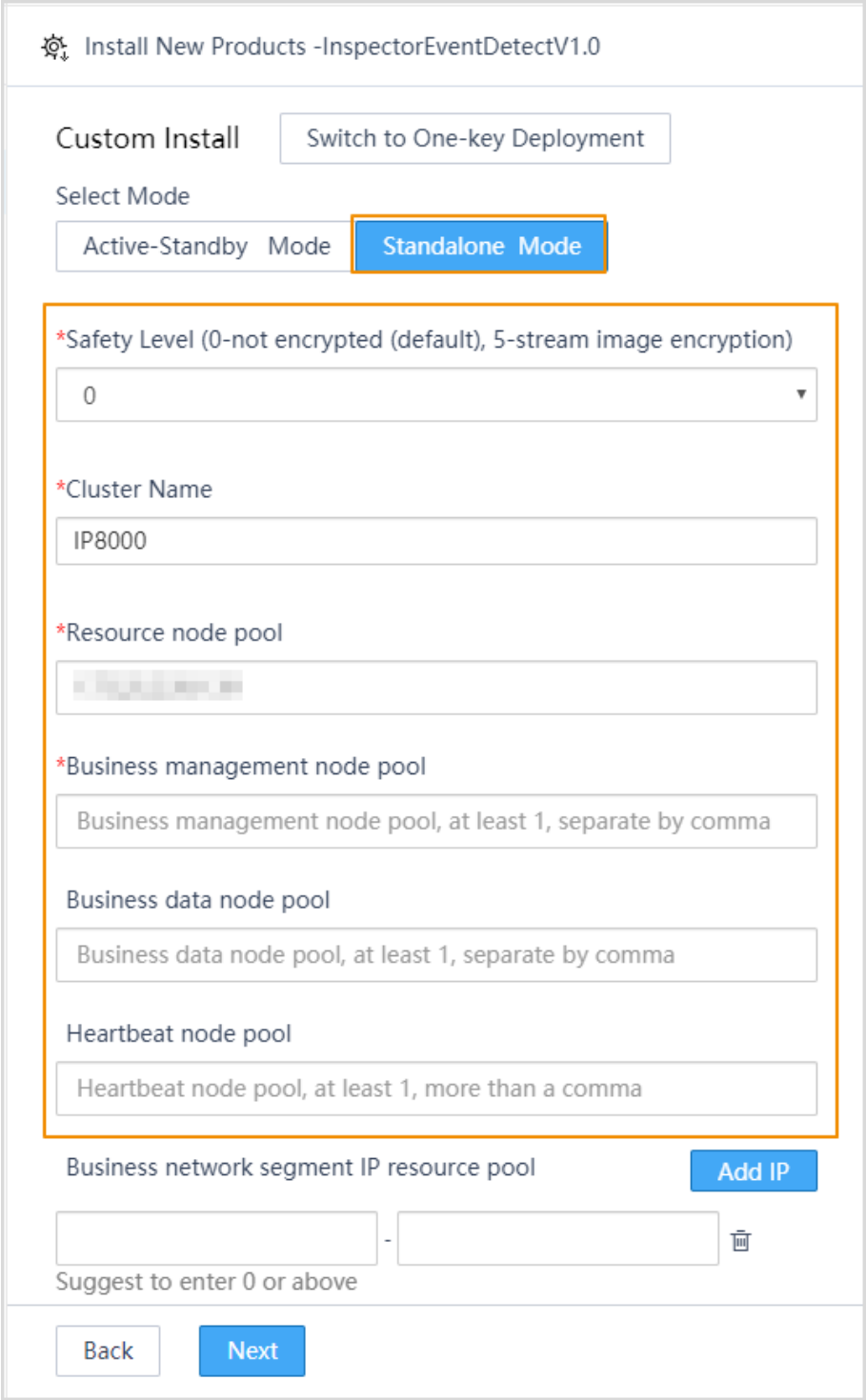


Step 6 In the pop-up window, click **OK**.

Step 7 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.

Figure 4-3 Custom install



Step 8 Click **Next**.

The Install New PaaS Cluster page is displayed.

4.2 Installing New PaaS Cluster

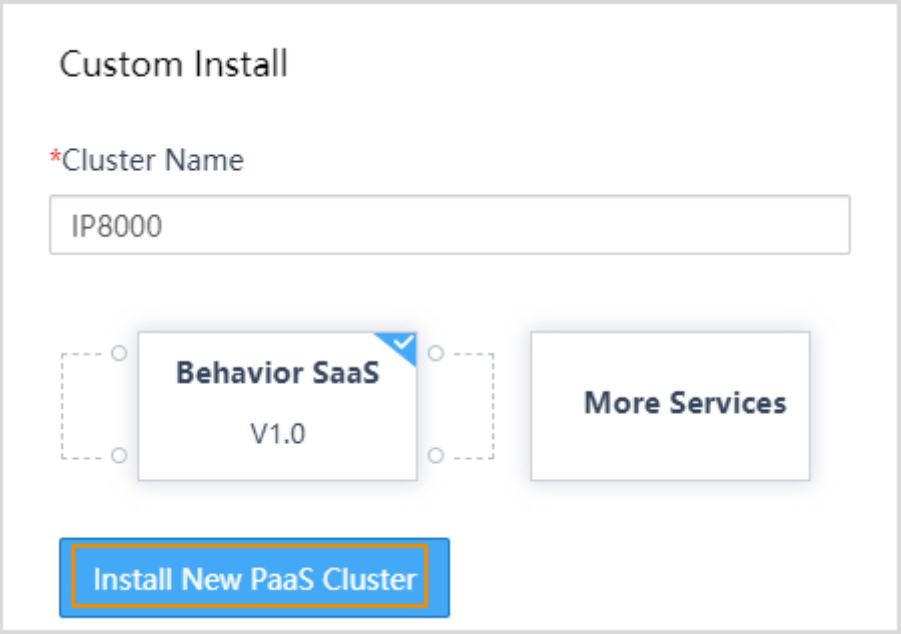
Prerequisites

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**.

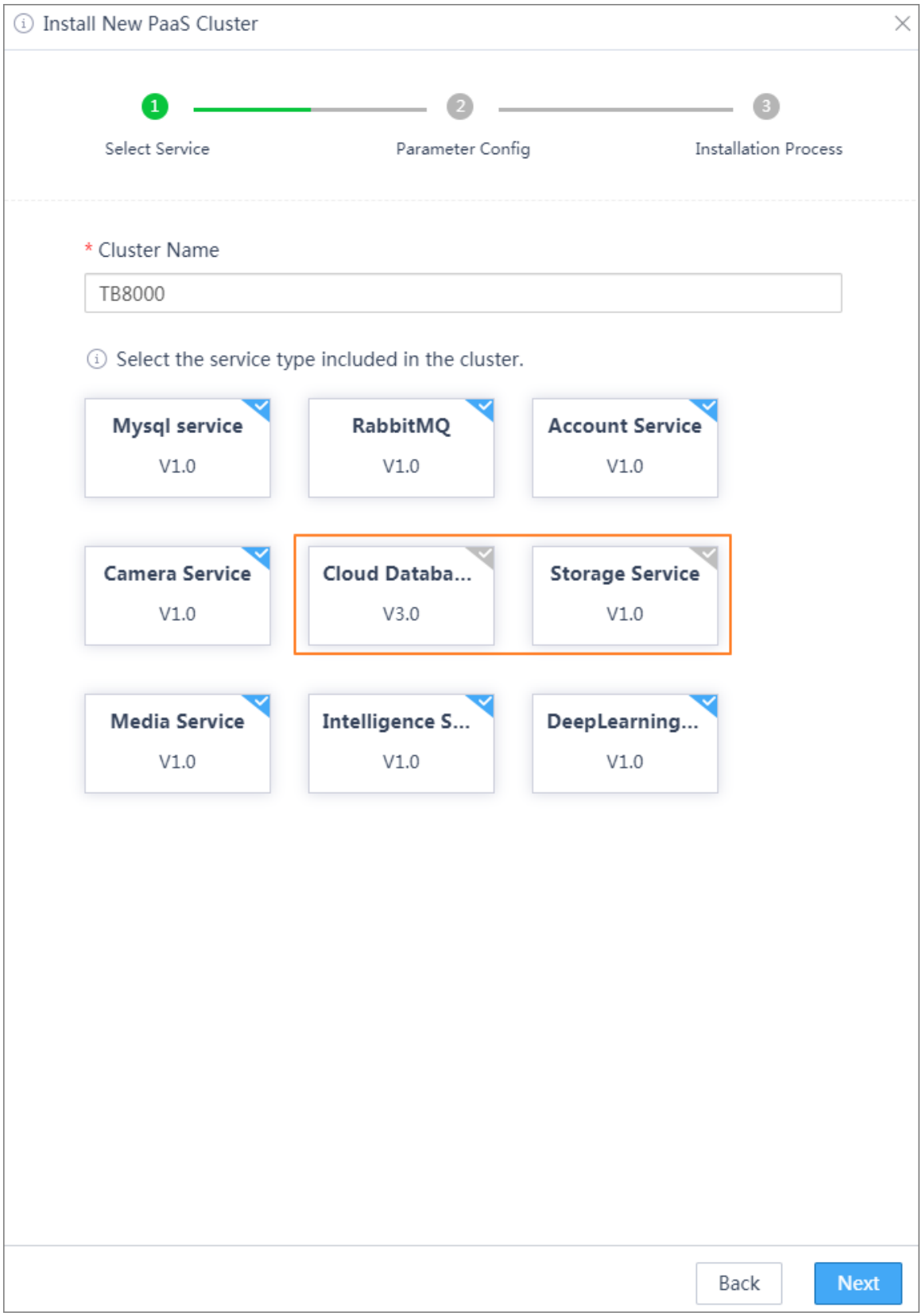
Figure 4-4 Install new PaaS cluster



Step 2 Select service type.

1. Clear **Cloud Database Service** and **Storage Service**.

Figure 4-5 Select service type



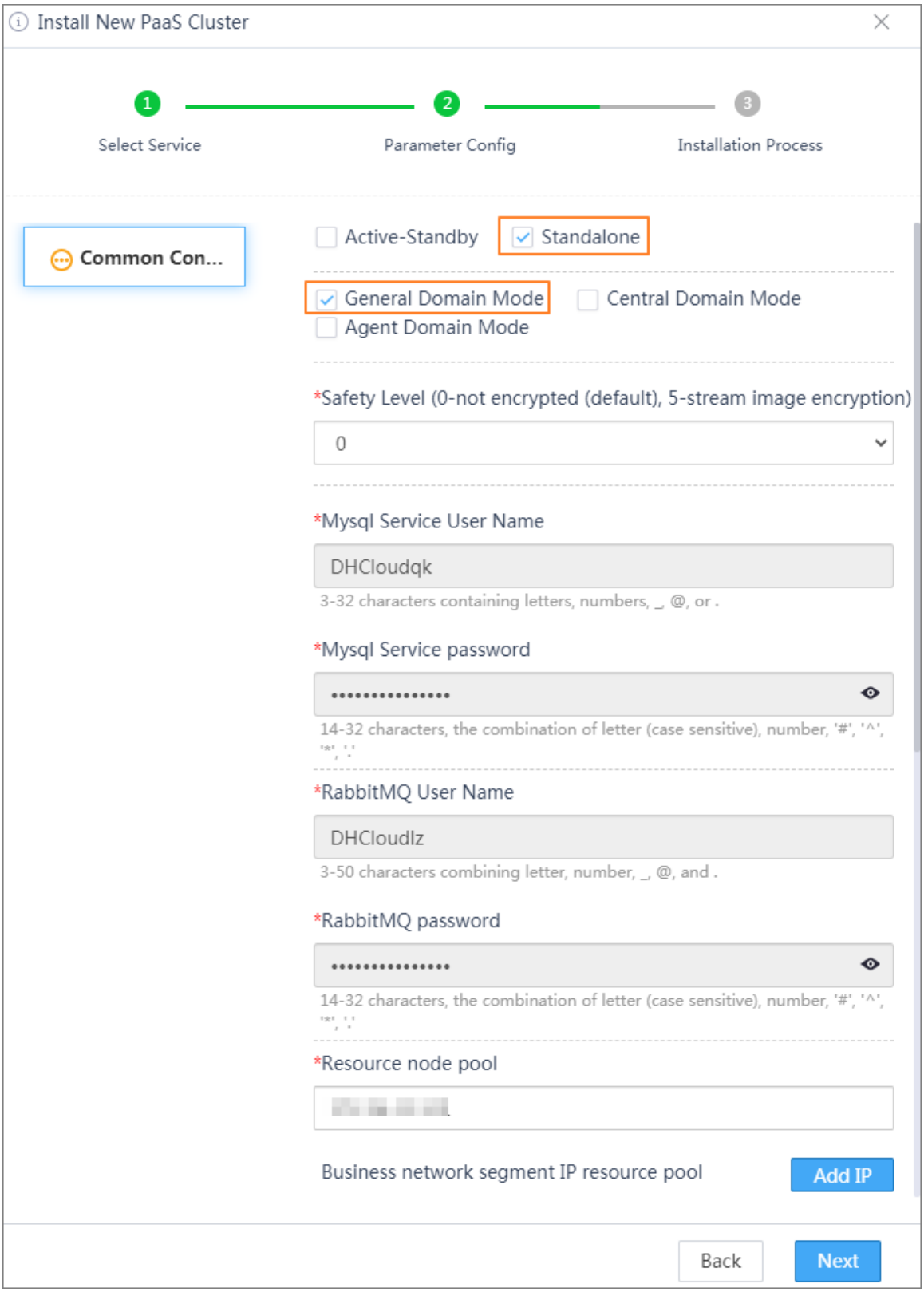
2. Click **Next**.

Step 3 Configure the parameters.

1. 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

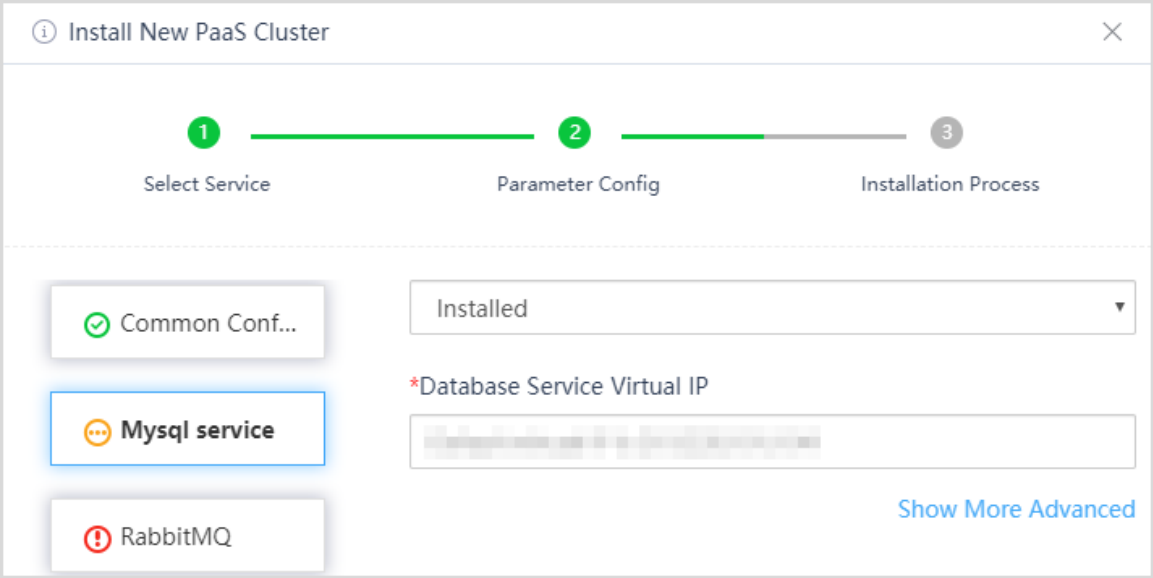


2. On the **Mysql service** page, install MySQL. Select **Installed**.

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

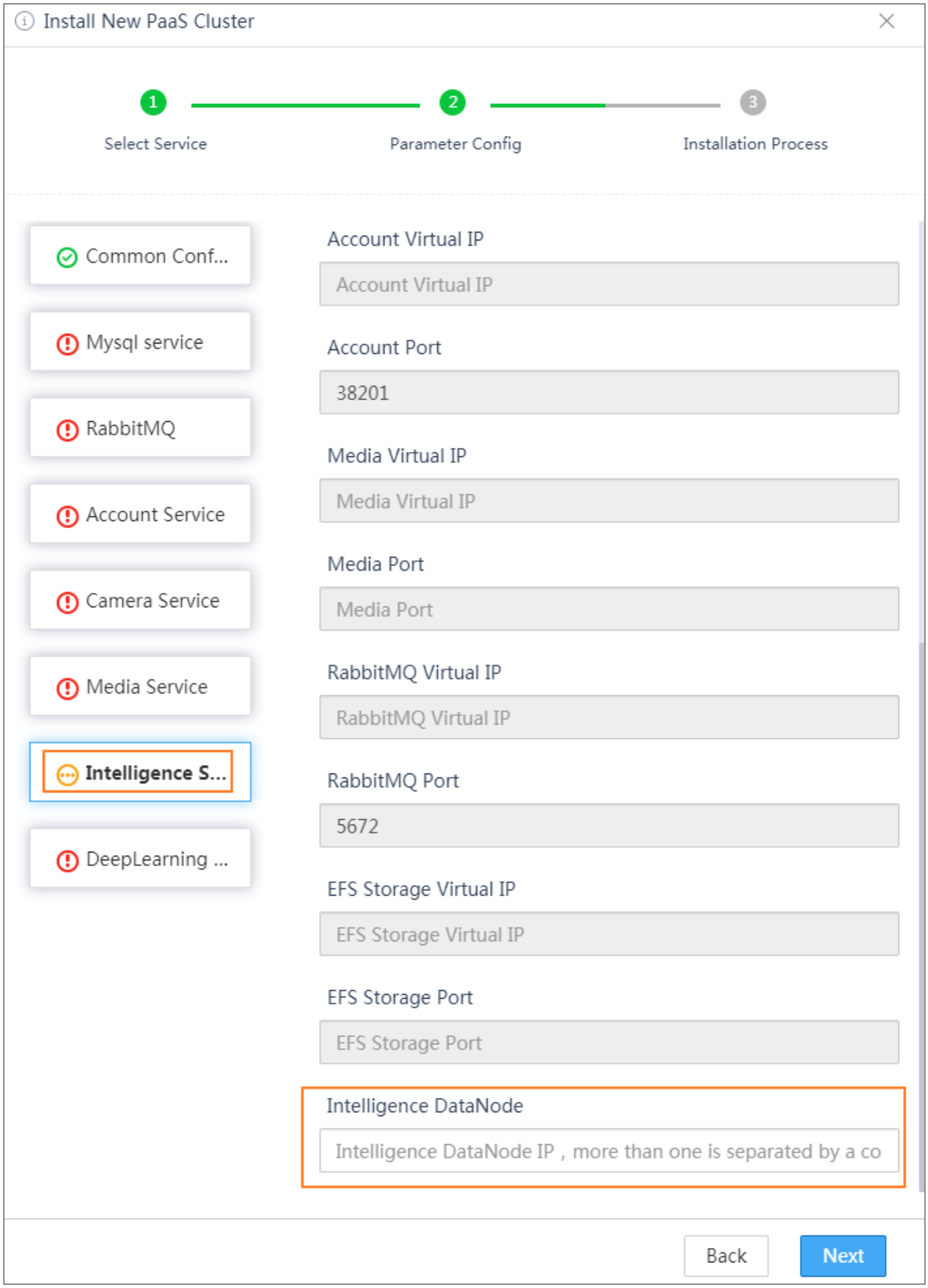
If it is not displayed, manually enter the server IP address.

Figure 4-7 MySQL service



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.

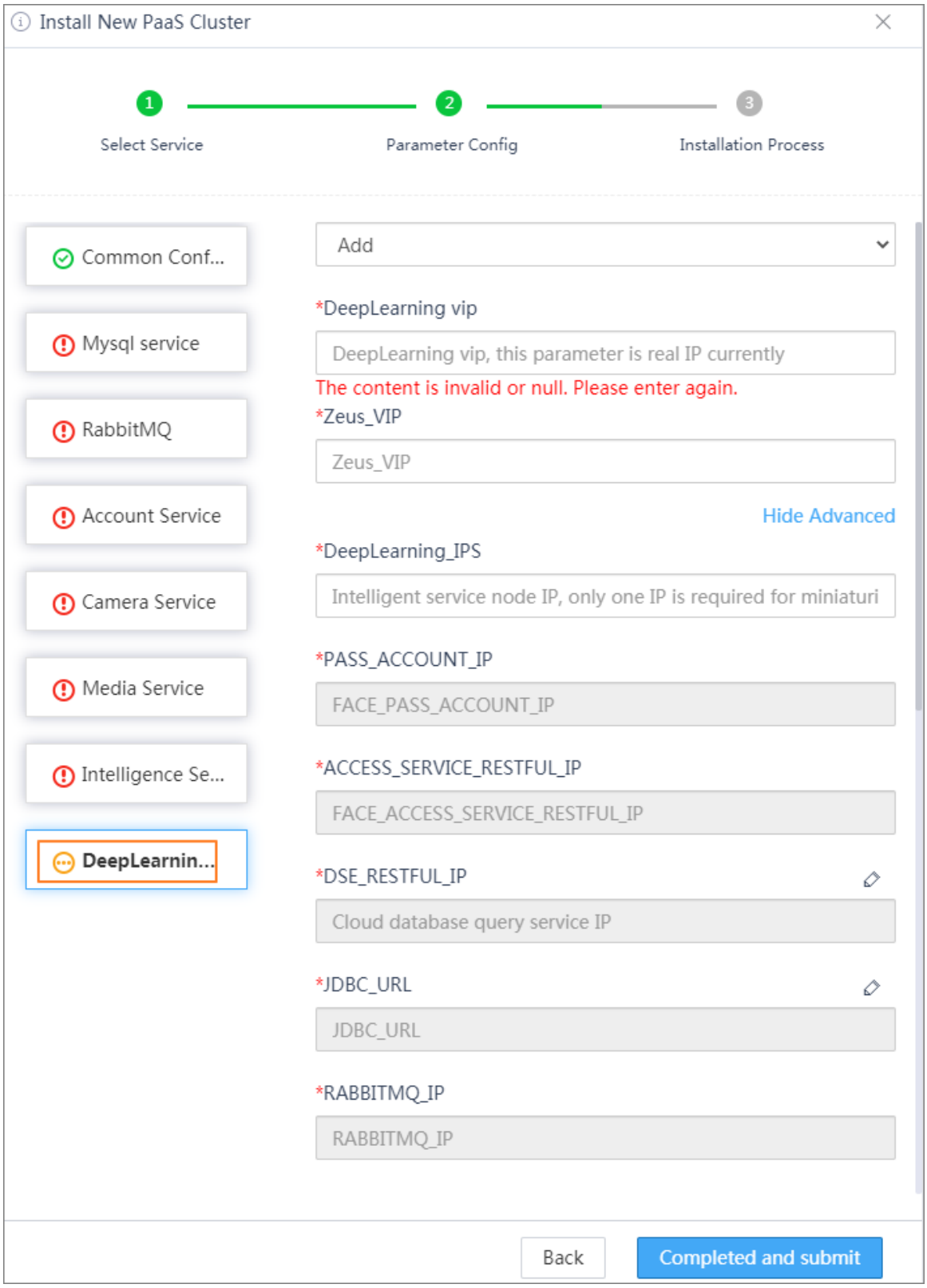
Figure 4-8 Intelligence service



4. Select the **DeepLearning Service** tab, click **Show More Advanced**, enter **DeepLearning vip**, and leave the other parameters as default.

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

Figure 4-9 Deep learning service



5. Click **Completed and submit**, and then in the pop-up window, click **OK**.

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

4.3 Configuring Behavior SaaS

Prerequisites

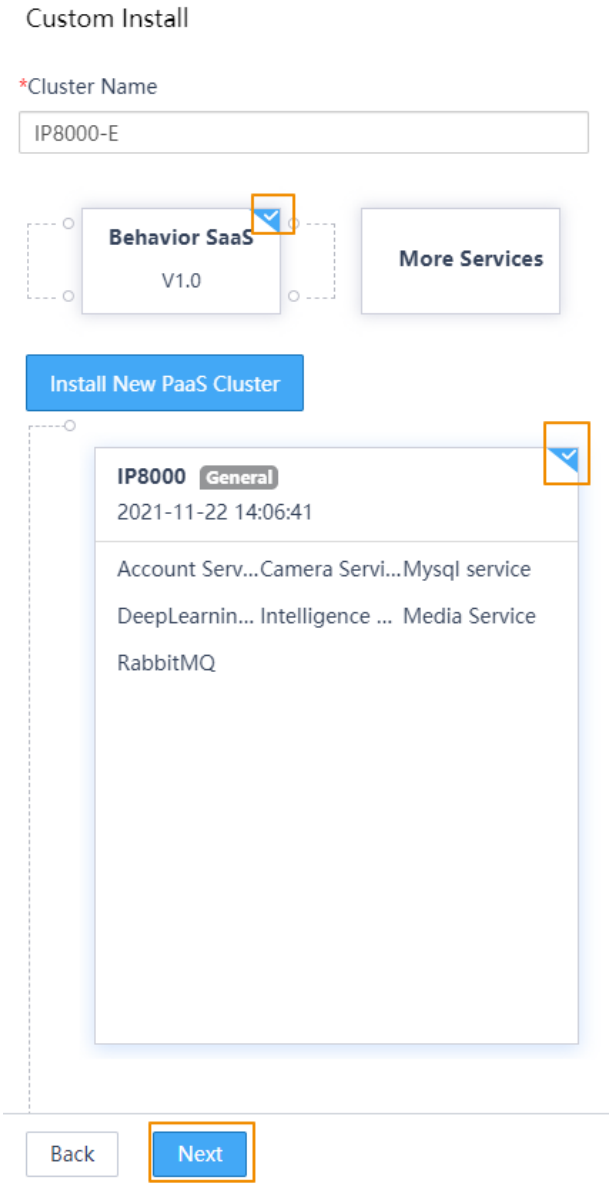
Make sure that new PaaS cluster is installed. For details, see "4.2 Installing New PaaS Cluster".

Procedure

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

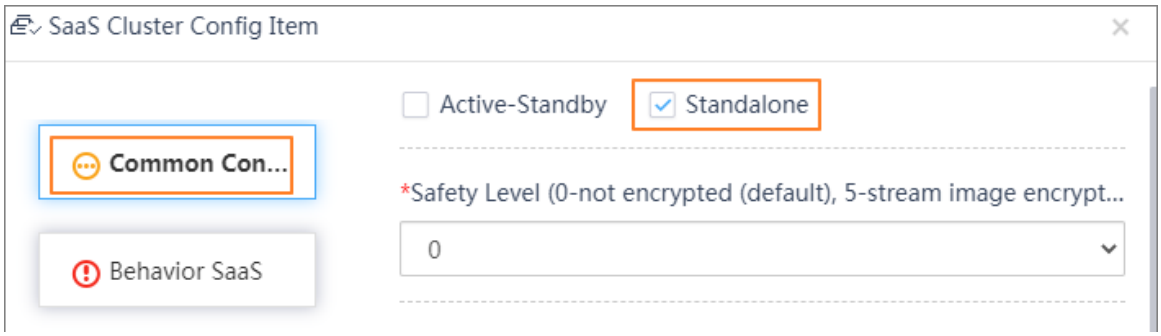
means selected, and means not selected.

Figure 4-10 Select SaaS and PaaS



Step 2 Click **Common Configuration**, select **Standalone**, and leave the other parameters as default.

Figure 4-11 Common configuration

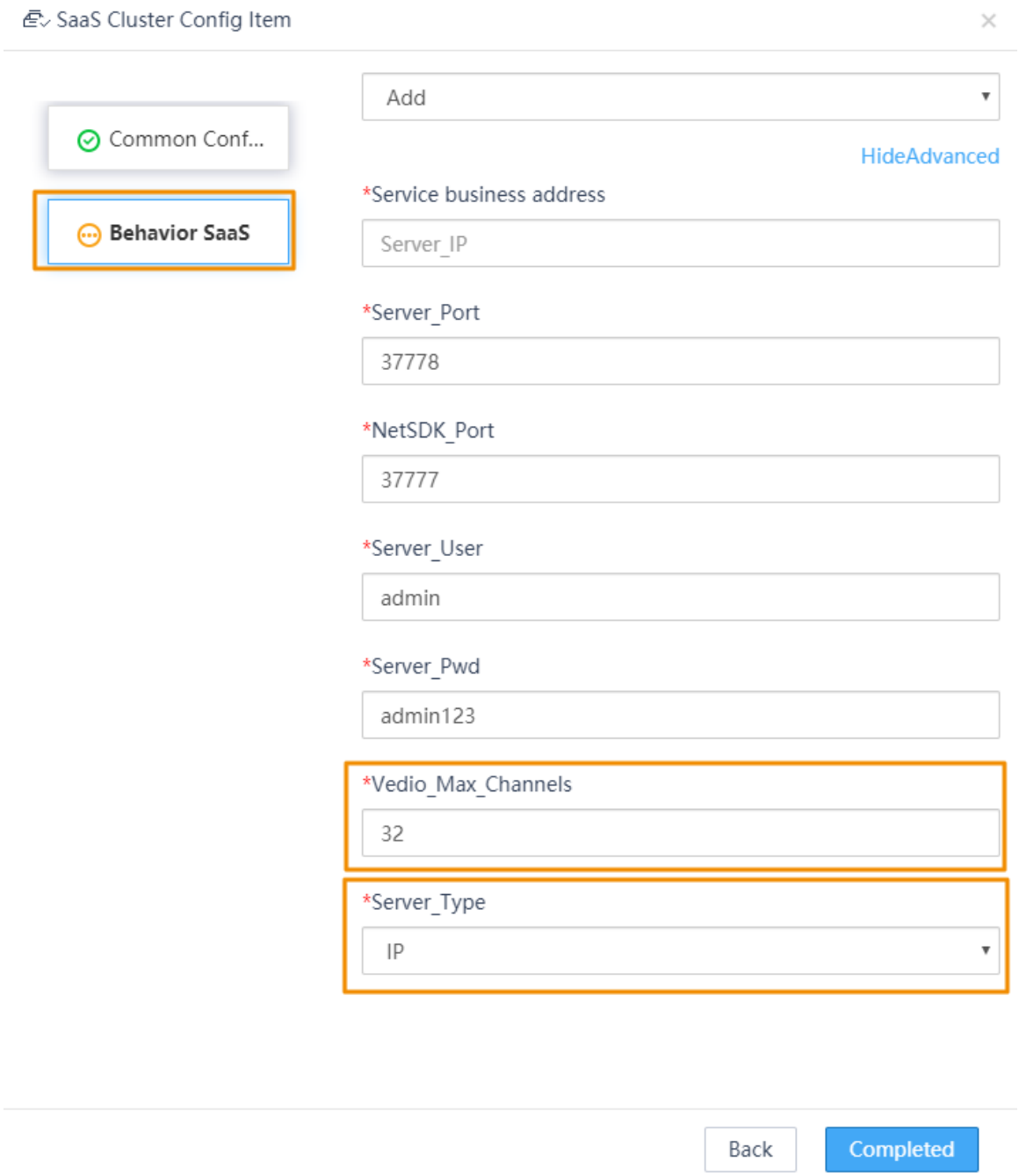


Step 3 Click **Bahavior SaaS**, and then click **Show More Advanced**. Enter **Video_Max_Channels** (the maximum number of video analysis channels), select **Server_Type** as **IP**, and leave the other parameters as default. Click **Completed**.

The system goes to the **Custom Install** page.

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.

Figure 4-12 Configure behavior SaaS

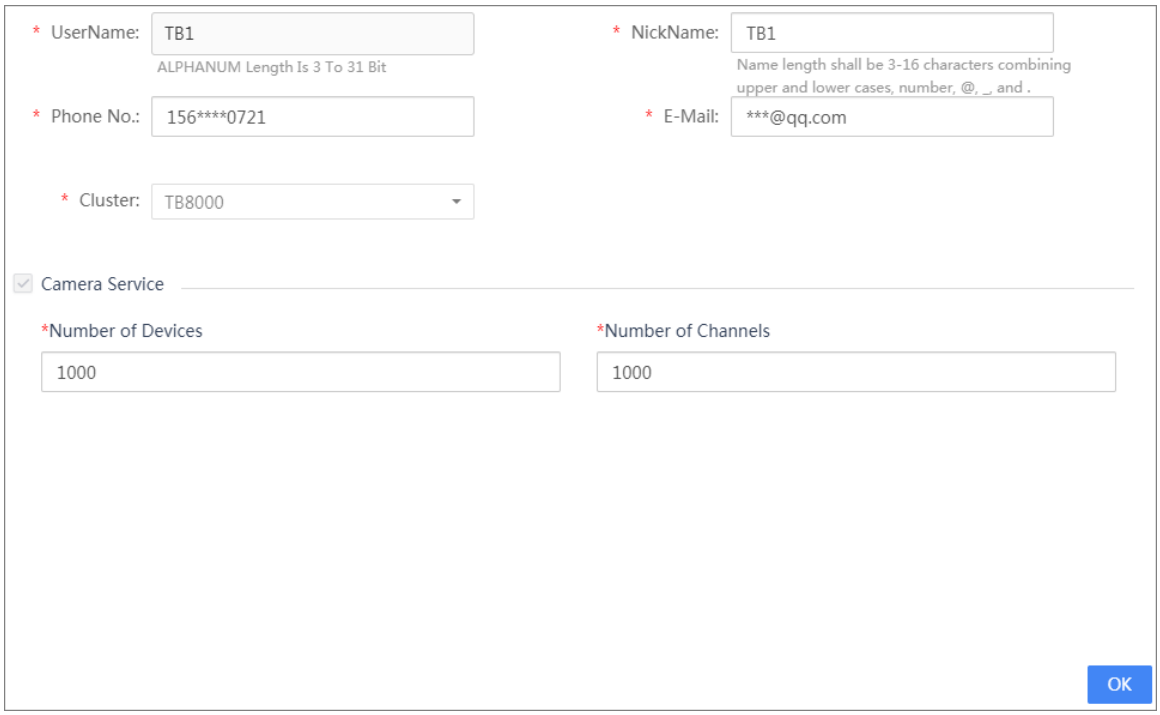


Step 4 On the **Custom Install** interface, click **Add** to add authorization user.

Step 5 Enter **UserName**, **NickName**, **Password**, and **E-Mail**. Select **Camera Service**, enter **Number of Devices** and **Number of Channels**.

- **Number of Devices**: The maximum number of devices that can be connected.
- **Number of Channels**: The number of channels that can be connected.

Figure 4-13 Enter user information



Step 6 Click **OK**.

After user authorization, the system automatically goes to the **Custom Install** interface.

Step 7 Click **Completed and submit**, and then in the pop-up window, click **OK**.

After installation, select **Product** > **Product Management**, and then you can view **Installed successfully** from **Product Status**.

Figure 4-14 Completed and submit

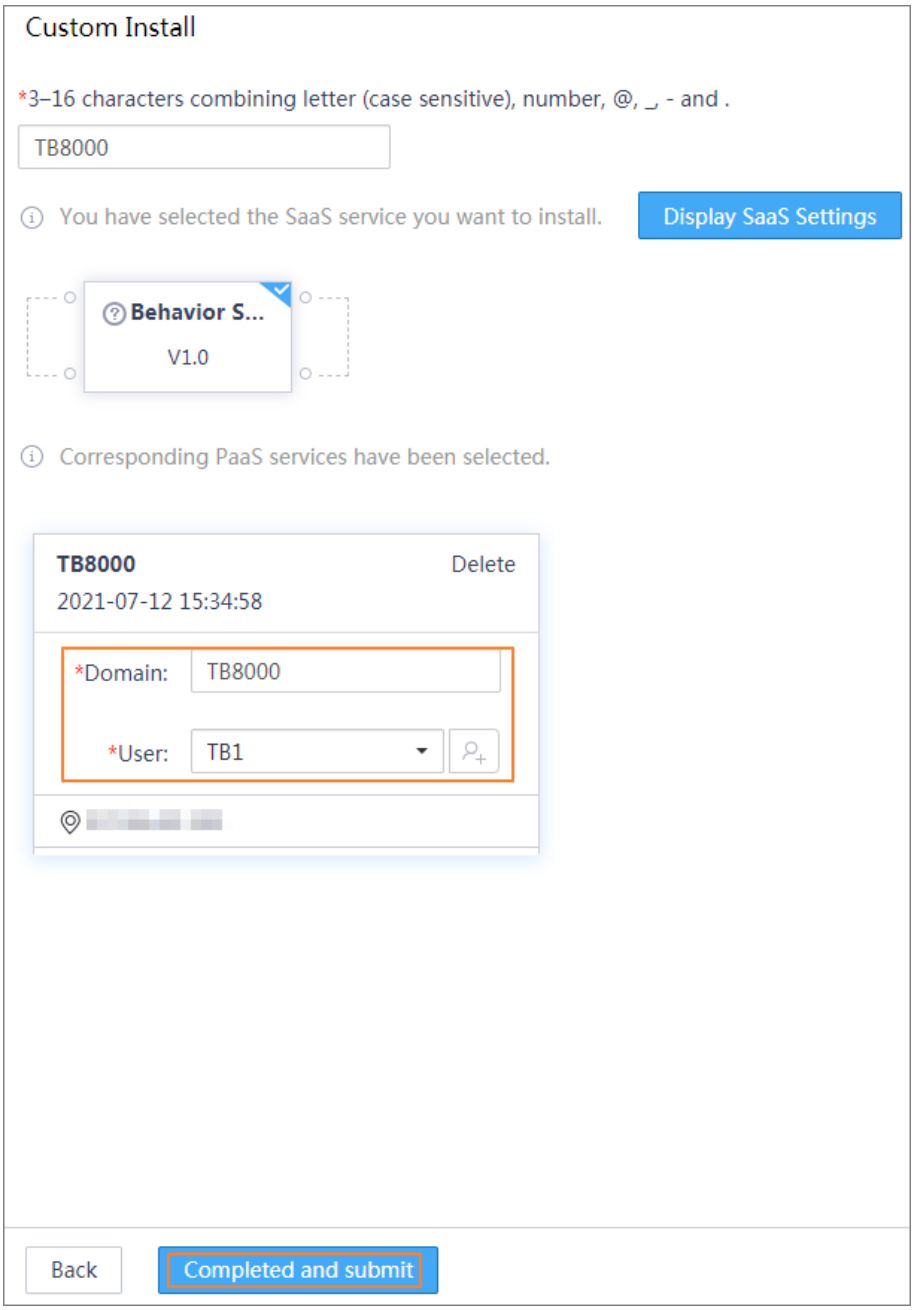
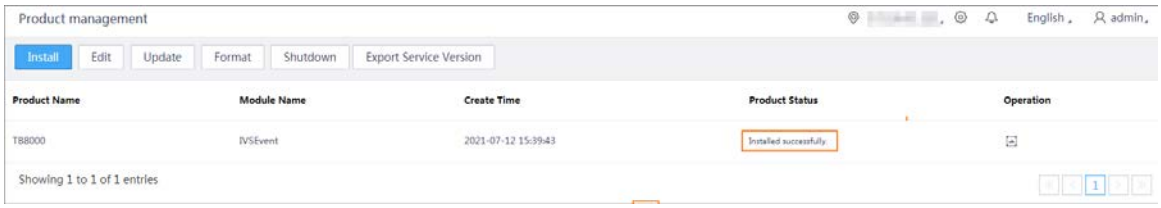


Figure 4-15 Installed successfully



4.4 Configuring Operator

Background Information

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

Procedure

Step 1 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**.

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

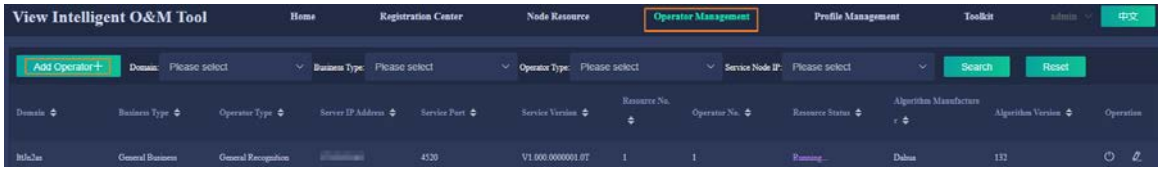
4. Change the default password in two minutes, and then click **OK**. After that, log in to the View Intelligent O&M Tool with the new password.

Step 2 (Optional) Select **Node Resource**, and then you can view the server information.

Figure 4-16 Node resource

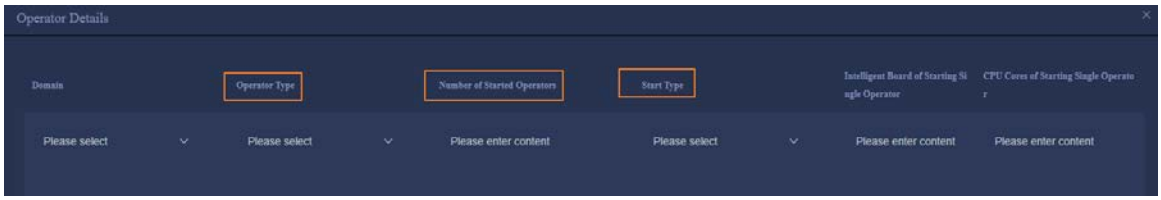
Step 3 Select **Operator Management** > **Add Operator+**.

Figure 4-17 Add operator



Step 4 Click 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.

Figure 4-18 Edit operator



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.

Step 2 Execute the **lsusb** command to check whether dongle is installed on the server.

```
[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.

Step 2 Execute the **cd /Tools** command to go to the Tools directory.

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(µ¼³¶): /**connection_server.dat**

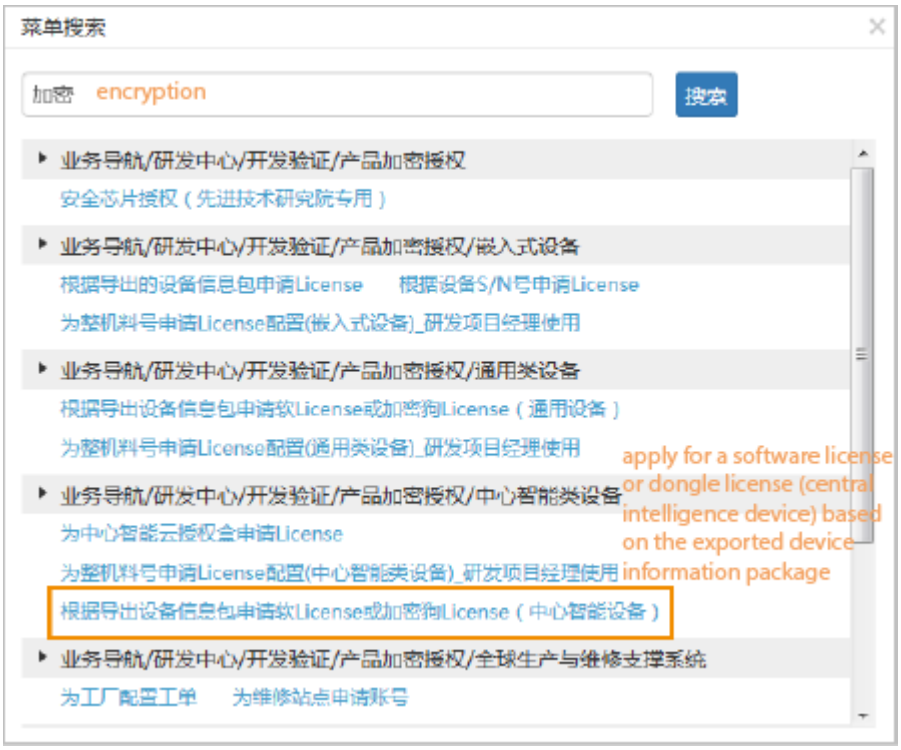
File name varies with version and release date.

Step 4 In the Tools directory, execute the **sz connection_server.dat** command to save the file to the local PC.

Step 5 Apply 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.

1. 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



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

Figure 5-2 Add application

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.

Figure 5-3 Enter application information

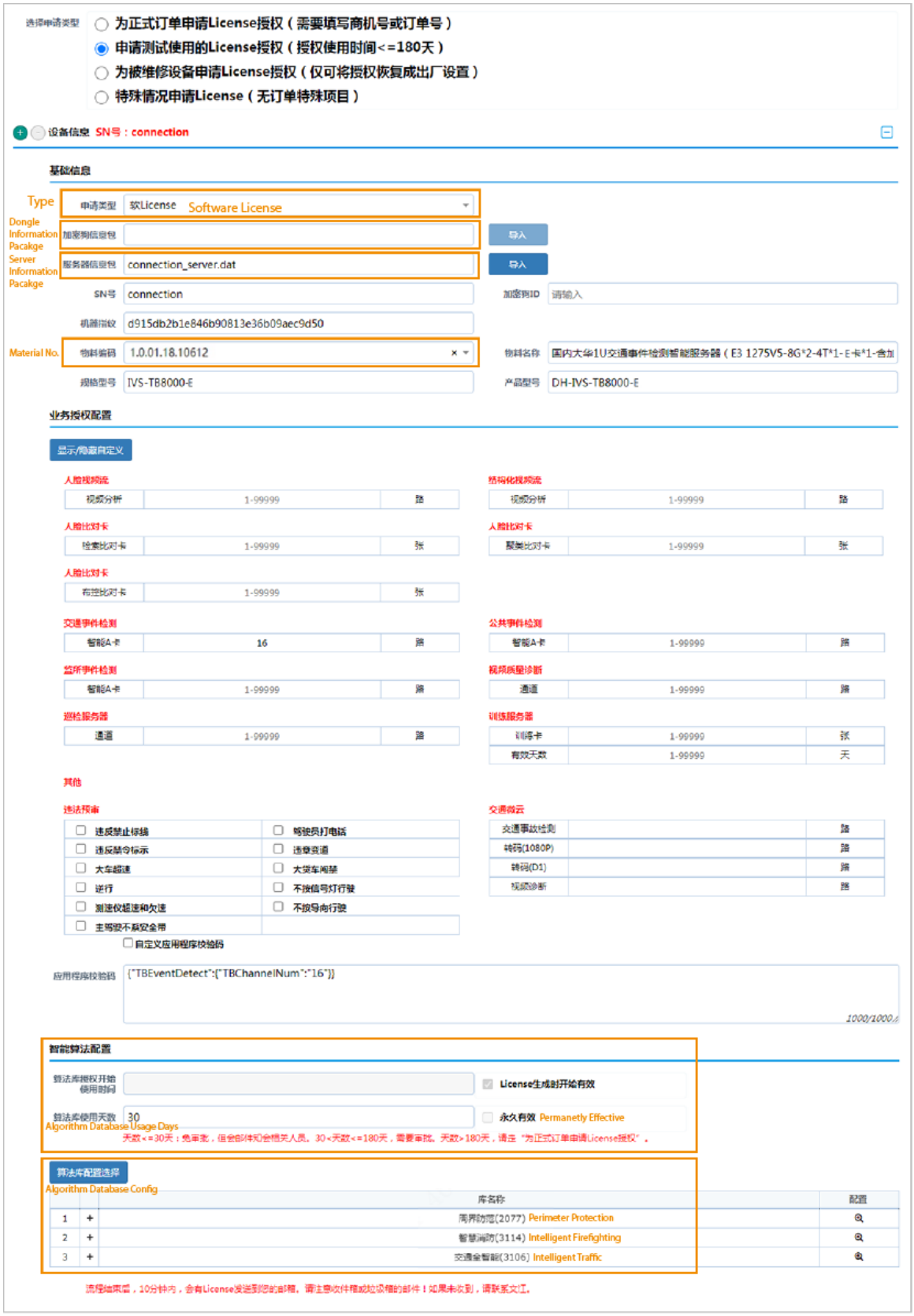


Table 5-1 Parameter description

Parameter	Description

Parameter	Description
Type	Select the application type. ● For hardware-based encryption, select 加密狗 (dongle). ● For software-based encryption, select 软**License** (software License).
Dongle Information Package	Click 加密狗信息包 (dongle information package), and then select the exported **connection_server.dat** file. ● The file name varies according to the version and release date. ● If you select 软加密 (software-based encryption), you do not need to upload files.
Server Information Package	Click 服务器信息包 (server information package), and then select the exported **connection_server.dat** file. The file name varies according to the version and release date.
Material No.	Click the text box, and then enter the material No. of the server. For server material No., see Table 5-2.
Algorithm Database Usage Days	Set the usage days. ● Clear the 永久有效 (permanently effective) checkbox, and then 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
```

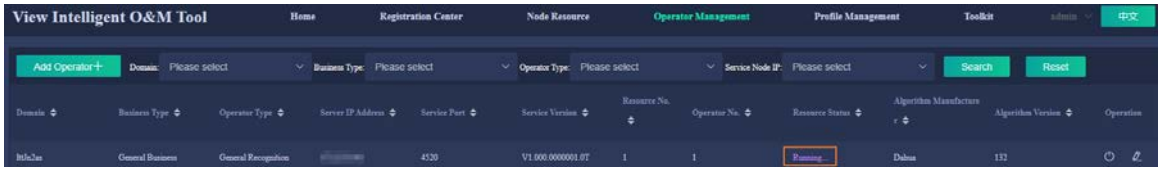
```
Begin Date:    2021-05-19 16:05:55
End Date:      2021-06-18 16:05:55
Days:      30
Count:      3
ID:    2077,3114,3106
```

4. Execute the **/etc/init.d/Intelligence-DataNode restart** command to restart the operator service.

Step 7 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



5.3 Hardware-based Encryption

Procedure

Step 1 Insert the dongle into the server.

Step 2 Log in to the server remotely through Xshell.

Step 3 Execute the **cd /Tools** command to go to the Tools directory.

Step 4 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.

Step 5 Execute the **./LicenseUpdateTool.exe -dog export** command to get the connection_dog.dat file.

```
[root@rabbitmq1 Tools]# ./LicenseUpdateTool.exe -dog export
============================
SUCCESS:
Export base information successfully.
Path(µ¼³¶): /connection_dog.dat
```

The file name varies according to the version and release date.

Step 6 Apply for the dongle on Dahua portal. For details, see step 5 in "5.2 Software-based Encryption".

Step 7 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.

```
[root@rabbitmq1 Tools]# ./LicenseUpdateTool.exe -dog 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 -dog display** command to view encryption information.

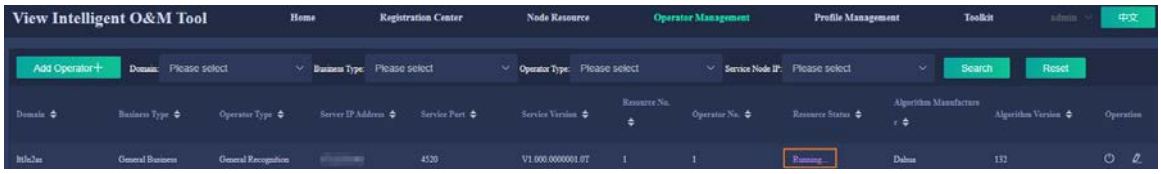
```
[root@rabbitmq1 ~]# /Tools./LicenseUpdateTool.exe -dog display
============================
SUCCESS:
SN:        ad33d8b0-1f7b-cab9-9447-ba07f855b143
Begin Date:    2021-05-19 16:05:55
End Date:          2021-06-18 16:05:55
Days:        30
Count:            3
ID:    2077, 3106, 6145
```

4. Execute the **/etc/init.d/Intelligence-DataNode restart** command to restart the operator service.

Step 8 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



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

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