Converter Tool

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.4.0

Foreword

General

This manual introduces the installation, functions and operations of the converter device (hereinafter referred to as the "Converter"). Read carefully before using the device, and keep the manual safe for future reference.

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

Version	Revision Content	Release Time
V1.4.0	Revised content structure.	December 2024
V1.4.0	Added new functions.	October 2024
V1.3.0	Added new functions.	June 2024
V1.2.0	Updated content.	March 2024
V1.1.0	Updated content.	August 2023
V1.0.0	First release.	May 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, audios 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.

Operation Requirements

⚠

- 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.
- Only use the device within the rated power range.
- 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.

Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- 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.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠

- 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.
- Use the power adapter or case power supply provided by the device manufacturer.
- 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 Product Overview

Dahua Converter is a software used for receiving events from Dahua control panel, processing the received data, transforming it and then presenting it to Central Monitoring Station (CMS) in appropriate formats.

2 Getting Converter

2.1 Getting Installation Package

Make sure that you have received the installation package from the https://depp.dahuasecurity.com/integration/guide/download/Converter.

2.2 System Requirement

Table 2-1 Function specifications

Function	Specifications
Max. Devices Supported	5000
Distribution without Video Event	100 TPS
Max. Event Search Number	50000
ARC Protocol Conversion	SurGard; Manitou; SIA-DC-09

Table 2-2 Performance Requirements

Type	Requirements
CPU	Intel(R) Core(TM) i5-7500 @ 3.0 GHz, 4-core or higher
Memory	At least 4GB (available)
Hard Disk	At least 200GB
Network Card	At least gigabit
Operating System	● Windows 7 (64-bit) ● Windows 10 (64-bit) ● Windows 11_pro (64-bit) ● Windows_Server_2012 (64-bit) ● Windows_Server_2016 (64-bit) ● Windows_Server_2019 (64-bit)
Browser	● Google Chrome 80 and later ● Microsoft Edge 107 and later ● Mozilla Firefox 65 and later

2.3 Installing Converter

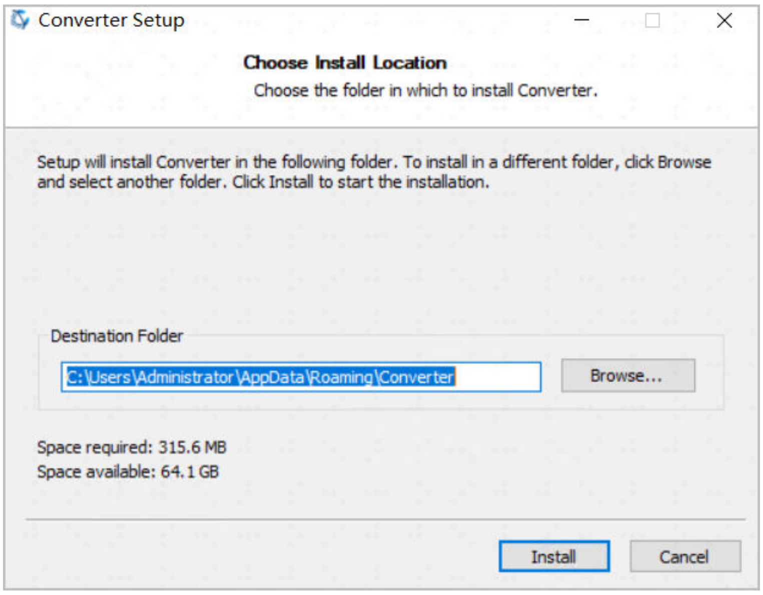
Procedure

Step 1 Log in to the computer as an administrator.

Step 2 Double-click the installation package.

Step 3 Select the destination folder and then click **Install**.

Figure 2-1 Install(1)



Converter Setup

Choose Install Location

Choose the folder in which to install Converter.

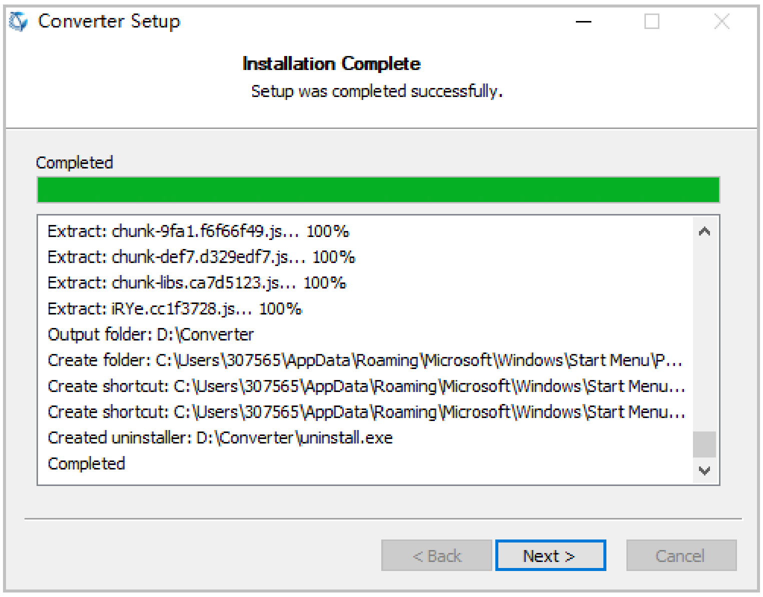
Setup will install Converter in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Users\Administrator\AppData\Roaming\Converter

Space required: 315.6 MB
Space available: 64.1 GB

Step 4 Wait for the installation to be completed, and then click **Next**.

Figure 2-2 Install(2)



Converter Setup

Installation Complete

Setup was completed successfully.

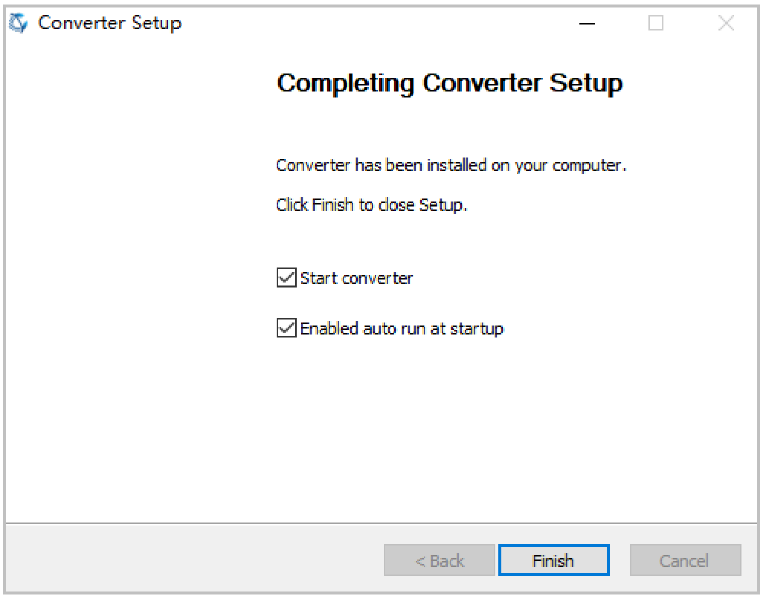
Completed

```
Extract: chunk-9fa1.f6f66f49.js... 100%
Extract: chunk-def7.d329edf7.js... 100%
Extract: chunk-libs.ca7d5123.js... 100%
Extract: iRYe.cc1f3728.js... 100%
Output folder: D:\Converter
Create folder: C:\Users\307565\AppData\Roaming\Microsoft\Windows\Start Menu\P...
Create shortcut: C:\Users\307565\AppData\Roaming\Microsoft\Windows\Start Menu...
Create shortcut: C:\Users\307565\AppData\Roaming\Microsoft\Windows\Start Menu...
Created uninstaller: D:\Converter\uninstall.exe
Completed
```

Step 5 Keep or cancel selecting **Start converter** or **Enabled auto run at startup** based on your needs (the two are selected by default), and then click **Finish**.

- **Start converter** : The webpage of Converter will be automatically opened after you click **Finish**.
- **Enabled auto run at startup** : The program runs automatically at startup.

Figure 2-3 Install(3)



Converter Setup

Completing Converter Setup

Converter has been installed on your computer.

Click Finish to close Setup.

☑ Start converter

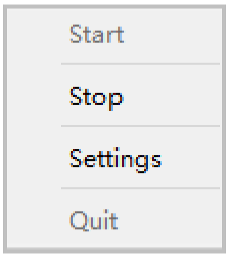
☑ Enabled auto run at startup

Related Operations

- System Tray Setting

  When the Converter is successfully installed and has been in operation, its icon appears in the system tray. Right-click the icon to open the operation menu.

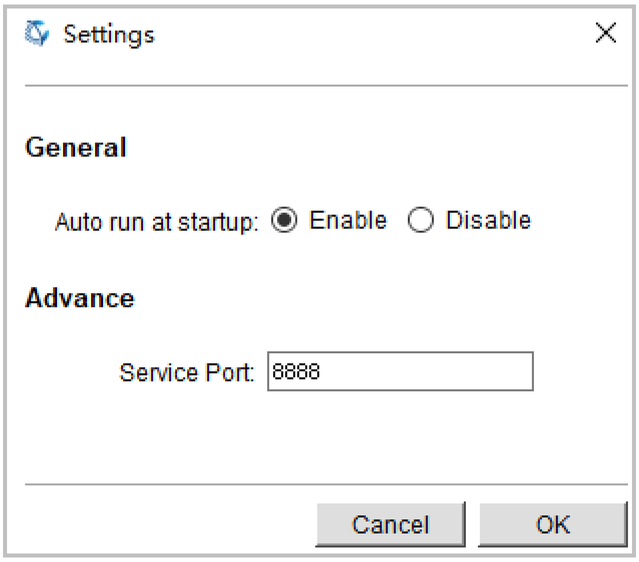
Figure 2-4 Menu



◇ Settings: Configure service port of Converter, or enable/disable auto run startup service.

The port is used for logging in to the Converter on the webpage.

Figure 2-5 Settings



General

Auto run at startup: ● Enable ○ Disable

Advance

Service Port: 8888

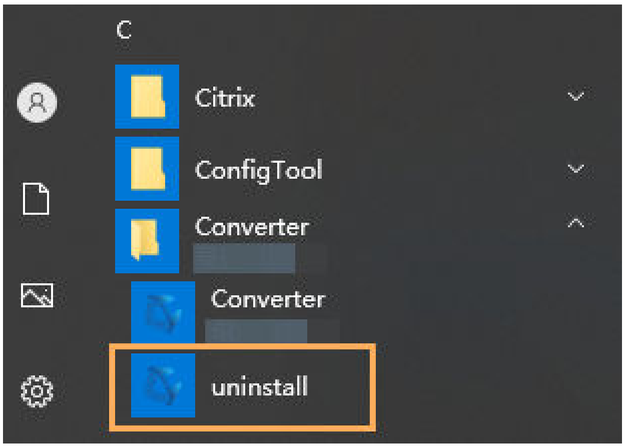
- ◇ Start/Stop: Start or stop service.
- ◇ Quit: Exit the program.

You need to click **Stop** and then **Quit** to exit the current program.

- Uninstall Converter

1. Double-click the installation package or click **Uninstall** under the shortcut of Converter in the Windows Start Menu, and the install window pops up.

Figure 2-6 Windows task bar



2. Click **Next** to install the program from the specified path.
3. (Optional) Select **Save Parameters** so that parameter files will be automatically replaced in next installation.
4. Click **Finish** to complete uninstalling.

2.4 (Optional) Updating Converter

There are two forms to backup or transfer data backup: Saving the data when installing or transferring data using a script.

Saving Data When Installing (Recommended)

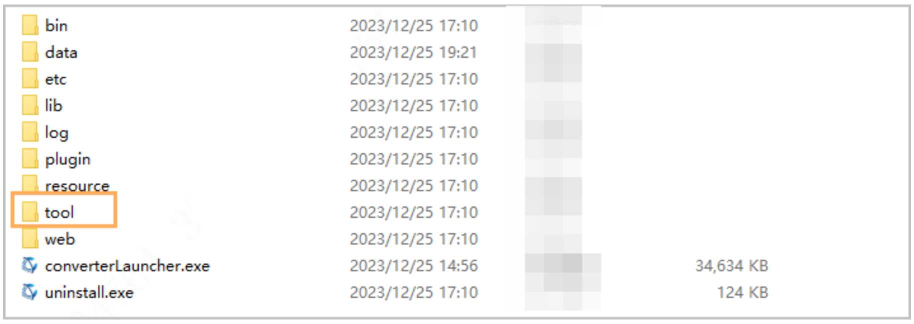
You can choose to uninstall the Converter without removing the user data.

Using A Script

Update the converter to latest versions and transfer the data. The datamigration.exe is used to transfer parameters configured in earlier versions of Converter to higher versions.

1. Open the installation folder of the Converter that you are currently using, and select **tool** > **datamigration** to obtain the datamigration.exe program.

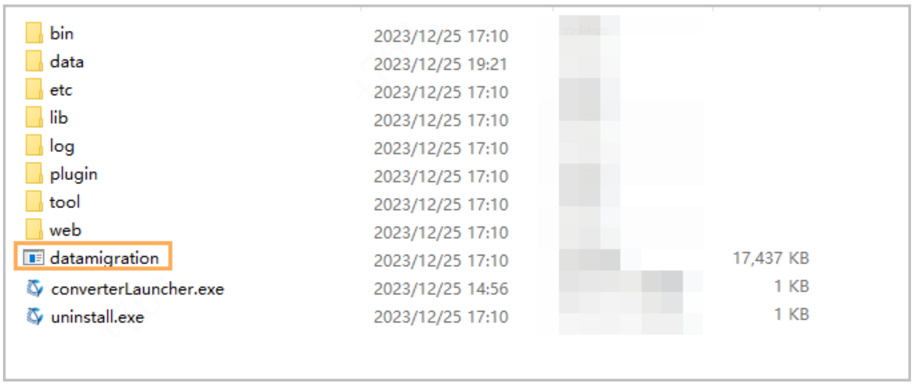
Figure 2-7 Tool folder



bin	2023/12/25 17:10	
data	2023/12/25 19:21	
etc	2023/12/25 17:10	
lib	2023/12/25 17:10	
log	2023/12/25 17:10	
plugin	2023/12/25 17:10	
resource	2023/12/25 17:10	
tool	2023/12/25 17:10	
web	2023/12/25 17:10	
converterLauncher.exe	2023/12/25 14:56	34,634 KB
uninstall.exe	2023/12/25 17:10	124 KB

2. Copy and paste the datamigration program to the directory of Converter that you want to export configuration data.
3. Double-click **datamigration** to run the program.

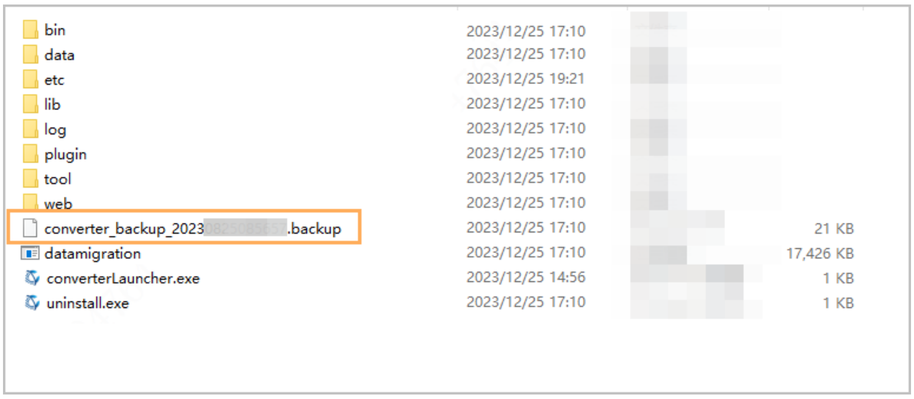
Figure 2-8 Migration



bin	2023/12/25 17:10	
data	2023/12/25 19:21	
etc	2023/12/25 17:10	
lib	2023/12/25 17:10	
log	2023/12/25 17:10	
plugin	2023/12/25 17:10	
tool	2023/12/25 17:10	
web	2023/12/25 17:10	
datamigration	2023/12/25 17:10	17,437 KB
converterLauncher.exe	2023/12/25 14:56	1 KB
uninstall.exe	2023/12/25 17:10	1 KB

A backup file that contains the system data is generated after running the program. The default password to import this file to Converter is admin123.

Figure 2-9 Backup file



bin	2023/12/25 17:10	[redacted]	
data	2023/12/25 17:10	[redacted]	
etc	2023/12/25 19:21	[redacted]	
lib	2023/12/25 17:10	[redacted]	
log	2023/12/25 17:10	[redacted]	
plugin	2023/12/25 17:10	[redacted]	
tool	2023/12/25 17:10	[redacted]	
web	2023/12/25 17:10	[redacted]	
converter_backup_2023[redacted].backup	2023/12/25 17:10	[redacted]	21 KB
datamigration	2023/12/25 17:10	[redacted]	17,426 KB
converterLauncher.exe	2023/12/25 14:56	[redacted]	1 KB
uninstall.exe	2023/12/25 17:10	[redacted]	1 KB

4. Log in to the webpage of Converter that you are currently using, and select **Maintenance** > **Import and Export** to import the backup file.

   The system data is therefore transferred.

2.5 Logging and Initializing Converter Local Account

For first-time use, you need to initialize the account.

Prerequisites

⚠

Make sure that you have cleared your browser cache after updating Converter to the latest version. Otherwise, problems might occur during your use.

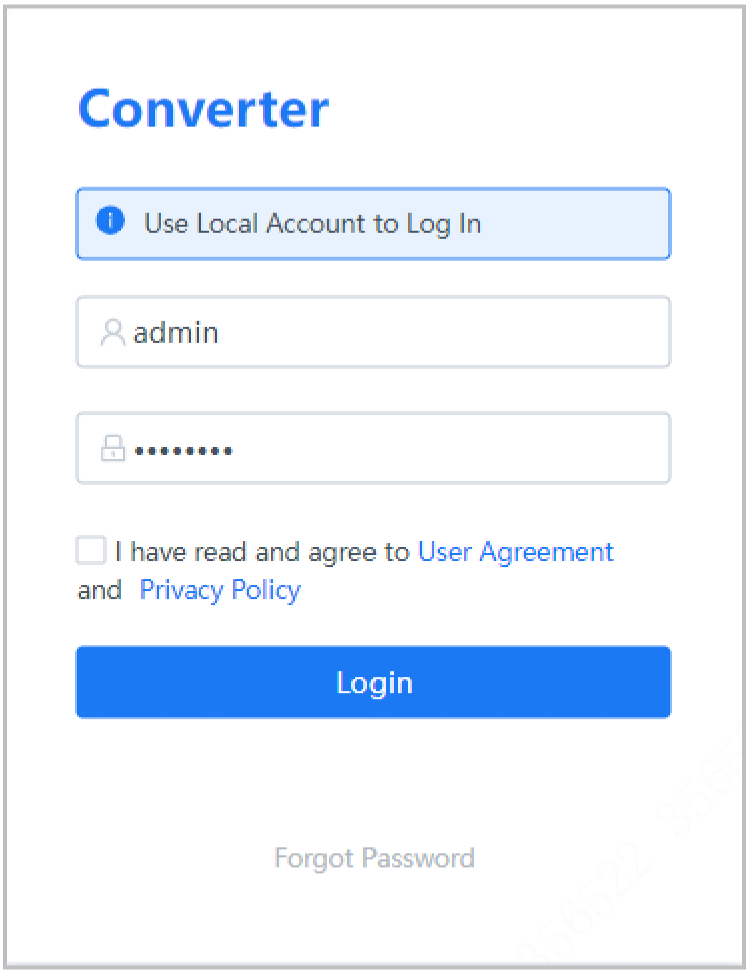
Procedure

Step 1 Double-click Converter to go to the webpage of Converter.

Step 2 Enter the username and password, and select **I have read and agree to User Agreement And Privacy Policy** , and then click **Login**.

The username is admin by default.

Figure 2-10 Login



Converter

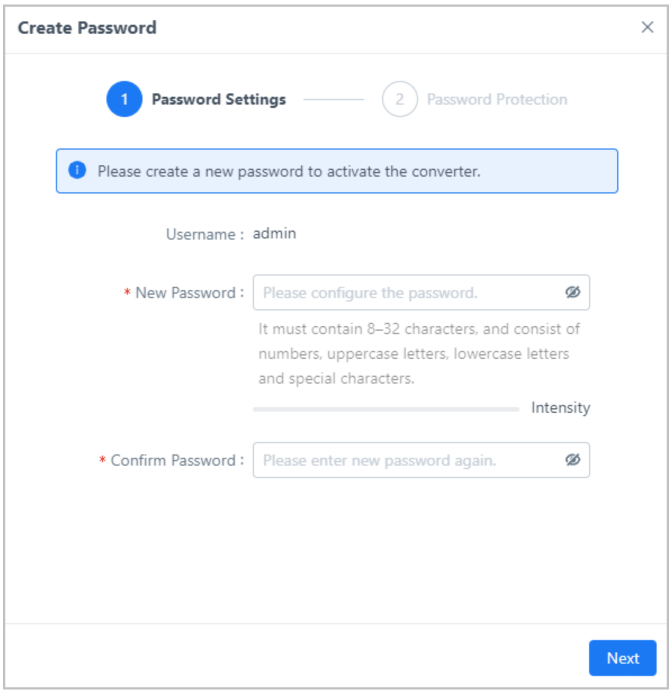
Use Local Account to Log In

admin

••••••••

□ I have read and agree to User Agreement and Privacy Policy

Figure 2-11 Create password



Create Password

Please create a new password to activate the converter.

Username : admin

* New Password : Please configure the password.

It must contain 8–32 characters, and consist of numbers, uppercase letters, lowercase letters and special characters.

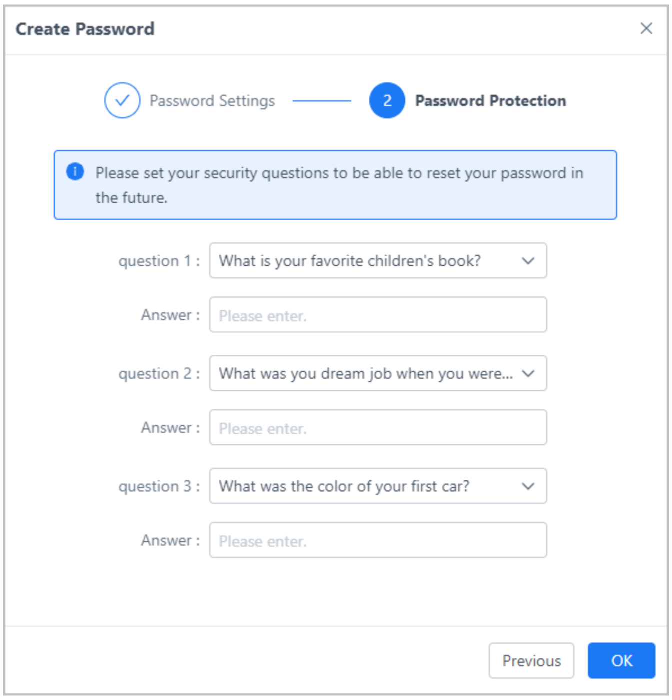
* Confirm Password : Please enter new password again.

Step 3 Configure the password protection questions, and then click **OK**.

It will be automatically logged into the Converter after you configure the password.

- While you do not have to set password protection questions, if you choose not to set them, you will be unable to recover your password in the future.
- You do not have to set all 3 questions. You can pick 1 or 2.
- You can click **Custom Question** in the question drop-down list to create your own custom questions if the default ones are not suitable.

Figure 2-12 Configure password protection



Create Password

Password Settings — 2 Password Protection

Please set your security questions to be able to reset your password in the future.

question 1 : What is your favorite children's book?

Answer : Please enter.

question 2 : What was you dream job when you were...

Answer : Please enter.

question 3 : What was the color of your first car?

Answer : Please enter.

3 Understanding How Converter Works

Working Principle

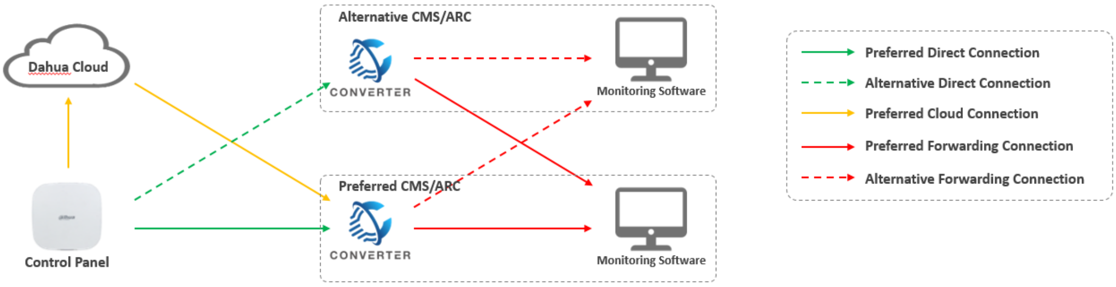
The Converter receives a message from the control panel, decrypts it, converts it into standardized protocol messages, and transfer it into the monitoring software, or CMS software.

Specifically, the transmission method includes direct connection and cloud connection.

- Direct connection: The control panel directly sends events and alarm videos to the Converter through Dahua SDK protocol.
- Cloud connection: Dahua cloud forwards events and alarm videos received from control panel to the corresponding Converter.

The two methods can be used together or separately.

Figure 3-1 How converter works


Dahua Cloud
Control Panel
Alternative CMS/ARC
CONVERTER
Monitoring Software
Preferred CMS/ARC
CONVERTER
Monitoring Software
Preferred Direct Connection
Alternative Direct Connection
Preferred Cloud Connection
Preferred Forwarding Connection
Alternative Forwarding Connection

Main Features

- Converter can download alarm videos from control panel or cloud and directly forward them to the third-party platform through the private protocol supported by the third-party platform, or send the URL of the video through the standard protocol SIA, and then the third-party platform downloads it according to the URL.
- Converter supports free custom development for integrating third-party private protocols.
- Supports import and export of Converter configuration parameters and added device data.
- Converter supports Primary/Secondary configuration of two network interface cards on the same server, as well as Primary/Secondary configuration between two different servers to ensure that the secondary network link or secondary server is enabled in case of a failure of the primary network link or primary sever.
- A cloud account can be created to log in to the Converter, so that the Converter can receive alarm events and videos from Dahua Cloud.

4 Connecting Control Panel to Converter

Add the control panel to Converter. Make sure that you have installed DoLynk Care app or DMSS app.

4.1 Direct Connection

4.1.1 Configuring Converter Parameters

Configure the network status of the Converter.

Procedure

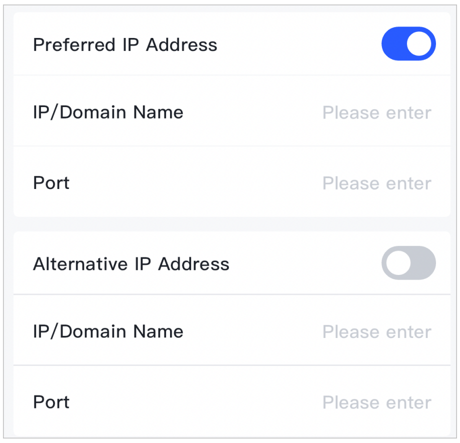
Step 1 Log in to the webpage of Converter.

Step 2 Select **Setting** > **Direct Connection**.

Step 3 Configure the UUID, select the local listening IP and configure the port, or enable the backup listening IP and port if you have a second network card.

When the IP and port number in **Preferred IP Address** under the **Hub Settings** > **Alarm Receiving Center** of DMSS and DoLynk is that of the primary Converter and the IP and port number in **Alternate IP Address** is that of the secondary Converter, then their UUID should be the same to avoid event loss during network switch. In other cases, the UUID does not need to be the same.

Figure 4-1 Preferred IP and Alternate IP



Preferred IP Address ●

IP/Domain Name Please enter

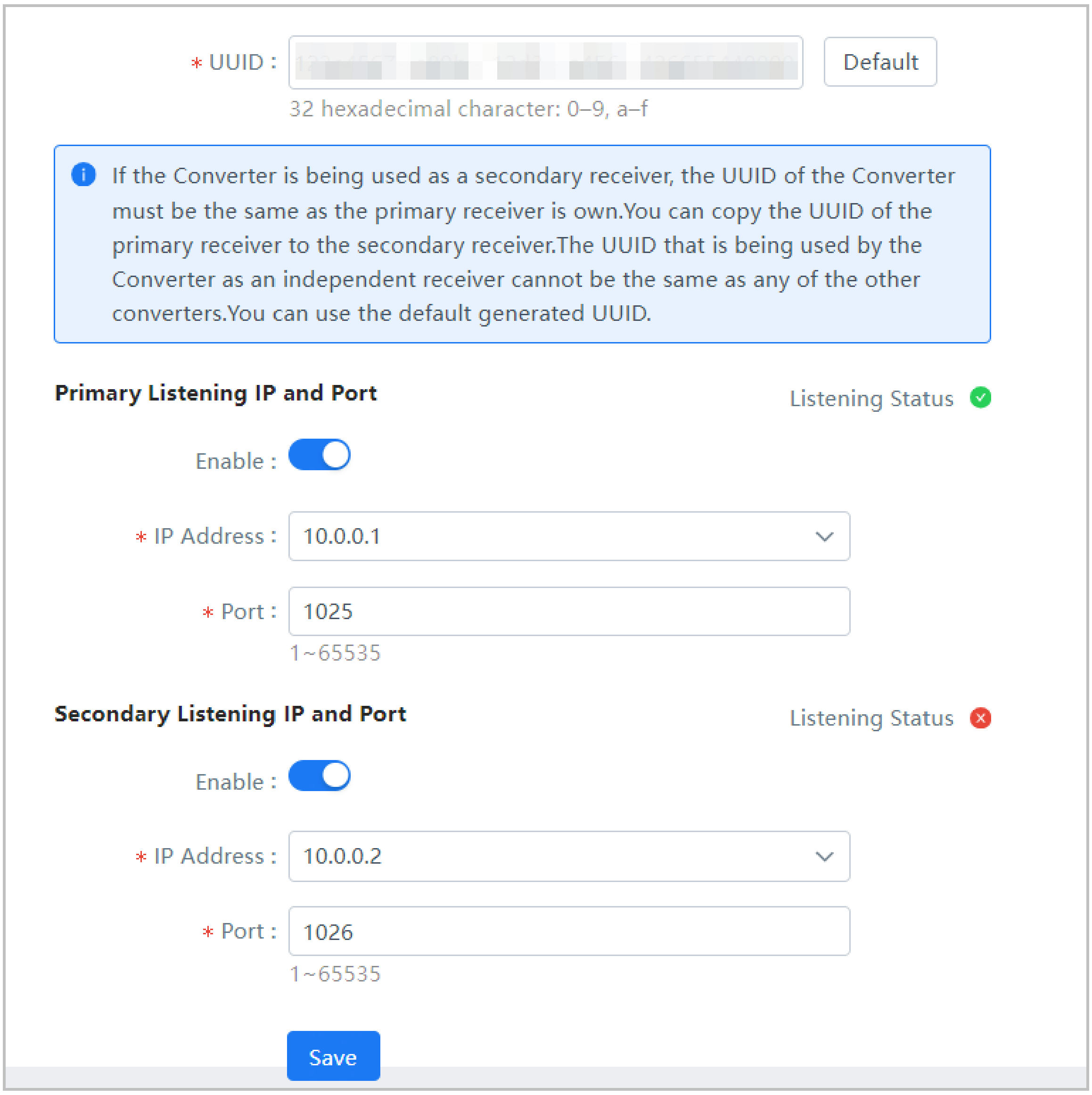
Port Please enter

Alternative IP Address ○

IP/Domain Name Please enter

Port Please enter

Figure 4-2 Network



* UUID : [redacted] Default

32 hexadecimal character: 0–9, a–f

If the Converter is being used as a secondary receiver, the UUID of the Converter must be the same as the primary receiver is own.You can copy the UUID of the primary receiver to the secondary receiver.The UUID that is being used by the Converter as an independent receiver cannot be the same as any of the other converters.You can use the default generated UUID.

Primary Listening IP and Port Listening Status ✓

Enable :

* IP Address : 10.0.0.1

* Port : 1025

1~65535

Secondary Listening IP and Port Listening Status ✕

Enable :

* IP Address : 10.0.0.2

* Port : 1026

1~65535

Save

Step 4 Click **Save**.

The listening status will be updated.

4.1.2 Adding Control Panel

You can add the control panel to the Converter through direct connection.

Background Information

The operation on DMSS is similar to that on DoLynk Care, and here the DMSS is used as an example.

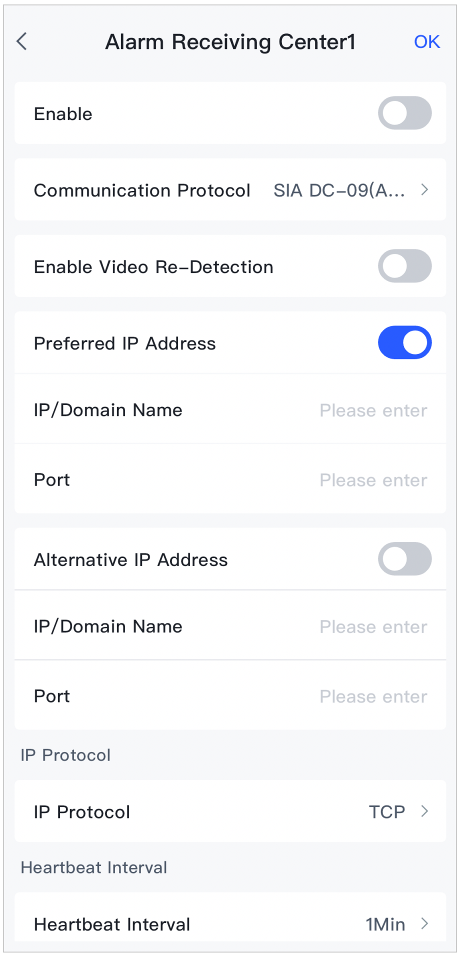
Procedure

Step 1 On your phone, tap to open the DMSS app.

1. On the **Login** screen, enter your email and password, and then tap **Log in**.
2. On the **Hub Setting** screen, tap **Alarm Receiving Center**.

3. Tap **Enable** to enable the alarm receiving function, select the communication protocol based on your needs, and enter the IP address and port number of the computer where Converter is installed on.
4. Tap **Scheduled Test** , enable **Scheduled Test**, select the auto report period, and then tap **OK**.
5. Tap **OK**.

Figure 4-3 Configure IP address and port



Alarm Receiving Center1 OK

Enable ○

Communication Protocol SIA DC-09(A... >

Enable Video Re-Detection ○

Preferred IP Address ●

IP/Domain Name Please enter

Port Please enter

Alternative IP Address ○

IP/Domain Name Please enter

Port Please enter

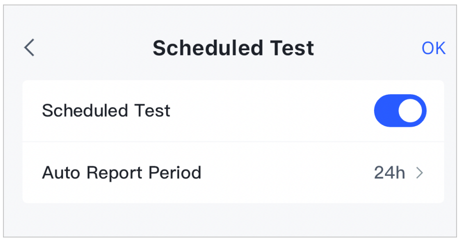
IP Protocol

IP Protocol TCP >

Heartbeat Interval

Heartbeat Interval 1Min >

Figure 4-4 Auto report period



Scheduled Test OK

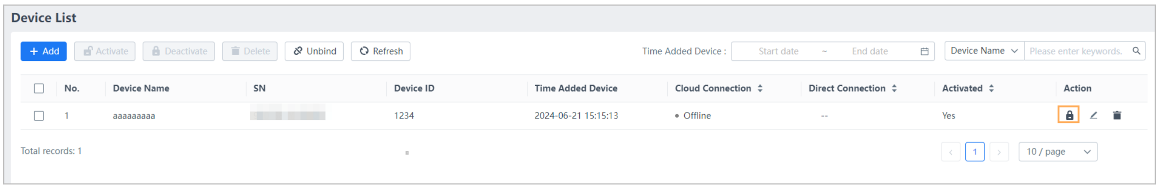
Scheduled Test ●

Auto Report Period 24h >

- The IP address and port number must be consistent with that you configured in "4.1.1 Configuring Converter Parameters" .
- You would better enable **Enable Video Re-Detection** if you have added IPC or PIR-Camera to the control panels and want to receive alarm messages with videos or pictures attached.
- Different alarm receiving centers of the same control panel cannot be set to connect to the same Converter.

Step 2 On the **Device List** page of Converter, click **Add**.

Figure 4-5 Device list

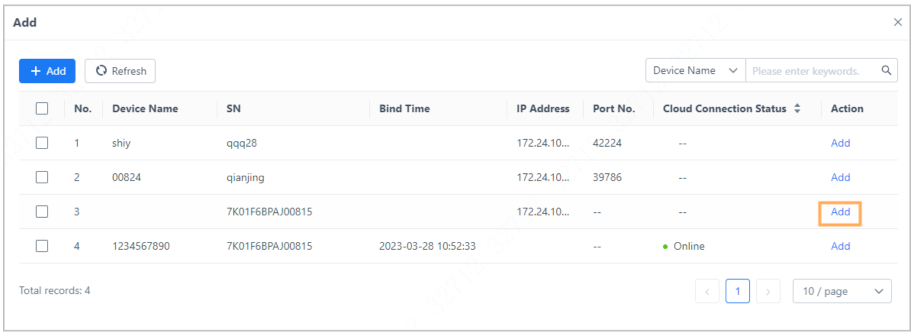


□	No.	Device Name	SN	Device ID	Time Added Device	Cloud Connection	Direct Connection	Activated	Action
□	1	aaaaaaaaa	[redacted]	1234	2024-06-21 15:15:13	● Offline	--	Yes	

Total records: 1

Step 3 Select the device you just configured, and then click **Add**.

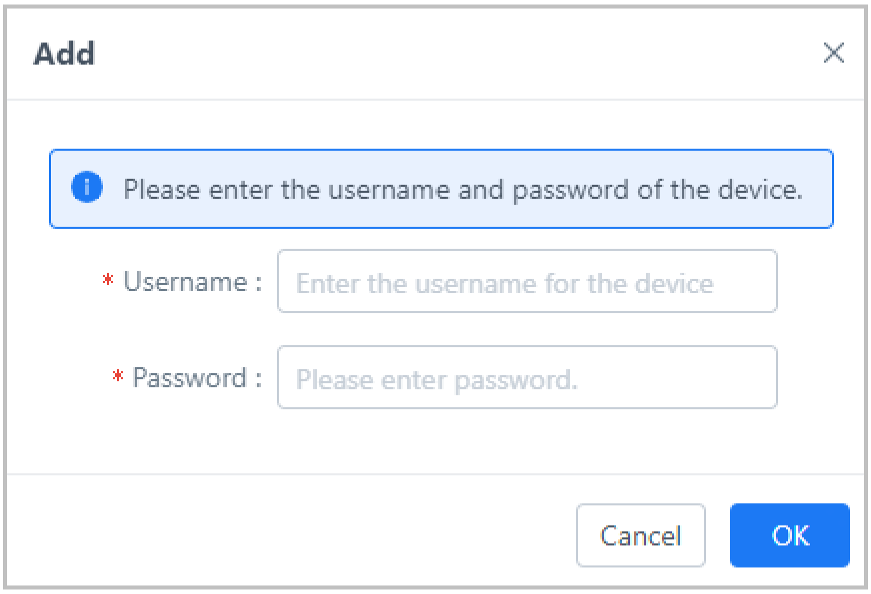
Figure 4-6 Add page



□	No.	Device Name	SN	Bind Time	IP Address	Port No.	Cloud Connection Status	Action
□	1	shiy	qqq28		172.24.10...	42224	--	Add
□	2	00824	qianjing		172.24.10...	39786	--	Add
□	3		7K01F6BPAJ00815		172.24.10...	--	--	Add
□	4	1234567890	7K01F6BPAJ00815	2023-03-28 10:52:33		--	● Online	Add

Total records: 4

Figure 4-7 Add device



Add

Please enter the username and password of the device.

* Username : Enter the username for the device

* Password : Please enter password.

If you use batch adding function, which is through clicking the + Add icon at the top left of the **Add** page, then you will be asked to enter the username and password of the device for successful adding when there is at least one device that is connected through auto registration among all the selected devices.

Wait for a while after adding, or click **Refresh** , and the **Direct Connection Status** of the newly added device is online.

Step 4 On the **Device List** page, click ✎ of a device, enter the device ID, user name and password used to log into the web page of the device, and then click **OK**.

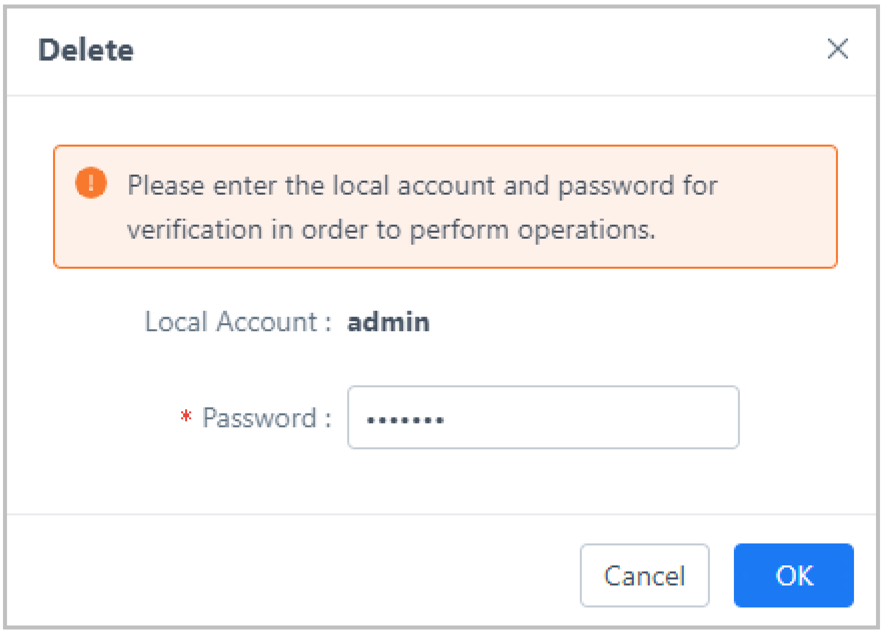
The device ID is the unique device identification code sent to the third-party alarm receiving center. It helps the alarm receiving center to determine which device sent the event. The device ID must be 4 characters. It can be 4 digits or a combination of uppercase letters and digits (totally 4 characters). We recommend that you use 4 digits.

Related Operations

Delete the control panel:

1. Select **Device** > **Device List**, select the device, and then click **Delete**.
2. Enter the password of the Converter admin account, and then click **OK** to delete the chosen devices.

Figure 4-8 Delete confirmation



Delete

Please enter the local account and password for verification in order to perform operations.

Local Account : admin

* Password : ••••••••

4.1.3 Device Management

4.1.3.1 Activating/Deactivating the Control Panel

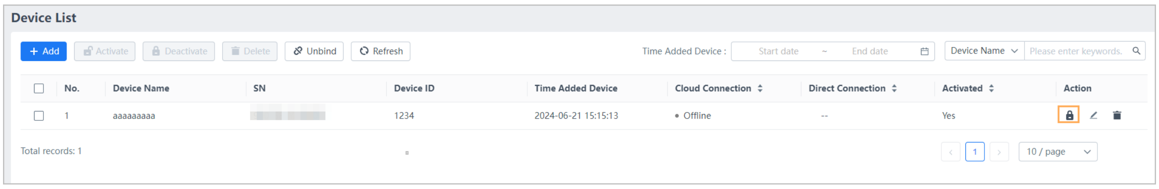
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Device** > **Device List**.

Step 3 Select the device, click 🔓 next to a device, or click **Activate** on the top left corner of the page to activate the chosen device(s).

Figure 4-9 Activation page



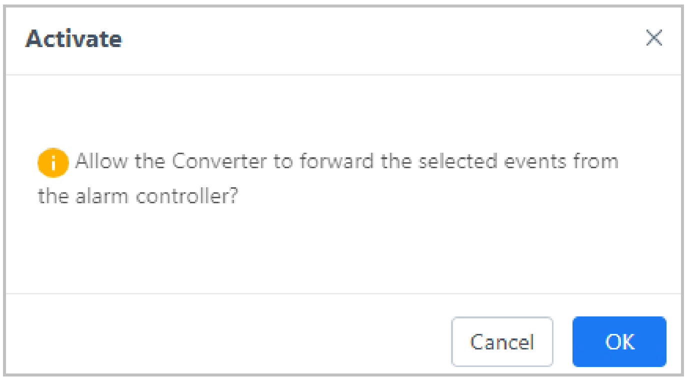
Device List

□	No.	Device Name	SN	Device ID	Time Added Device	Cloud Connection	Direct Connection	Activated	Action
□	1	aaaaaaaaa	[redacted]	1234	2024-06-21 15:15:13	● Offline	--	Yes	🔒

Total records: 1

Step 4 On the **Activate** window, click **OK** to confirm the activation.

Figure 4-10 Activate the device



Activate

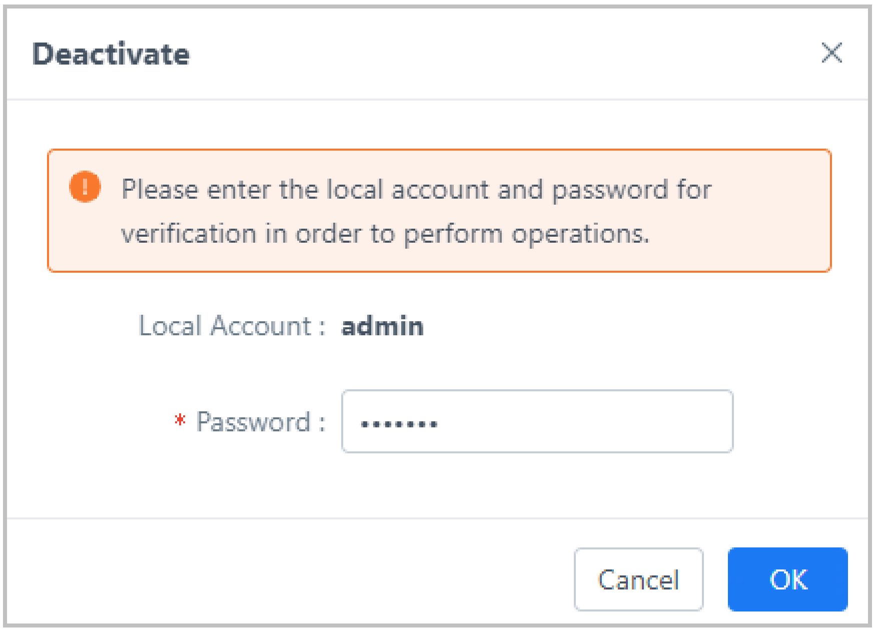
Allow the Converter to forward the selected events from the alarm controller?

Related Operations

Deactivating the control panel:

1. Select **Device** > **Device List**, select the device, and then click **Deactivate**.
2. Enter the password of Converter account, and then click **OK** to deactivate the selected devices.

Figure 4-11 Deactivate confirmation



Deactivate

Please enter the local account and password for verification in order to perform operations.

Local Account : admin

* Password : ••••••••

4.1.3.2 Unbinding the Control Panel

Background Information

Unbind the device if the alarm services expire or in case of false operation. Be advised that unbinding for expired services must be done through the cloud.

The device will be removed from the device list after unbinding.

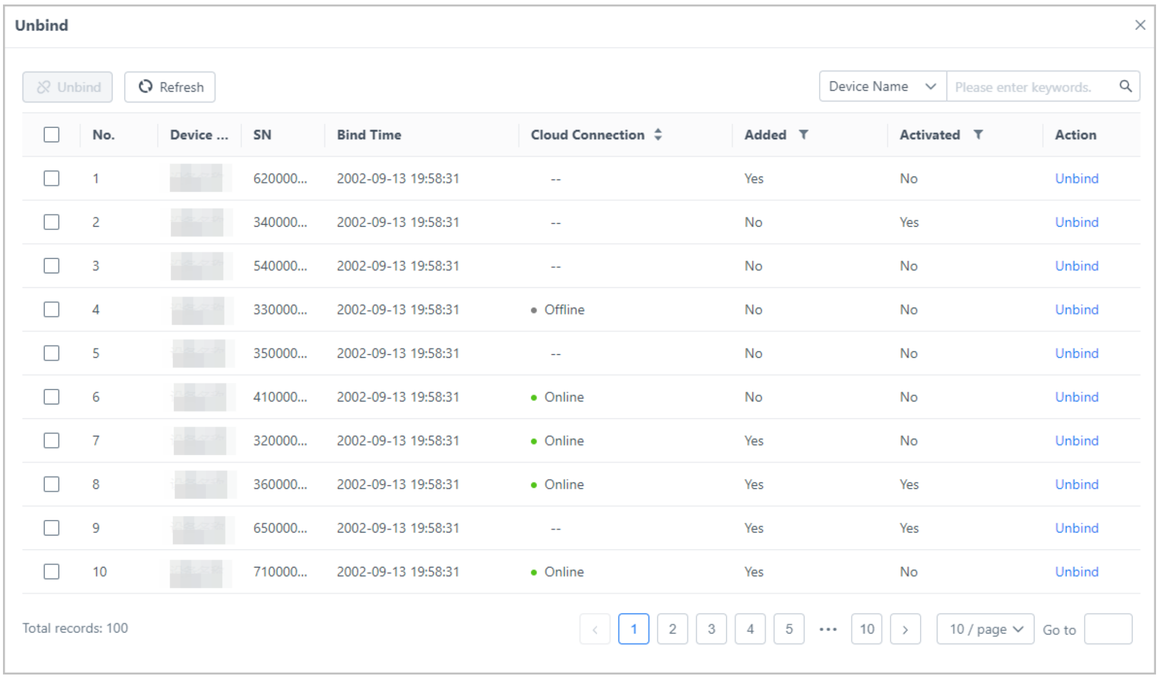
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Device** > **Device List**, and then click **Unbind** to go to the **Unbind** page.

You can filter devices that are added or activated.

Figure 4-12 Enter unbind page



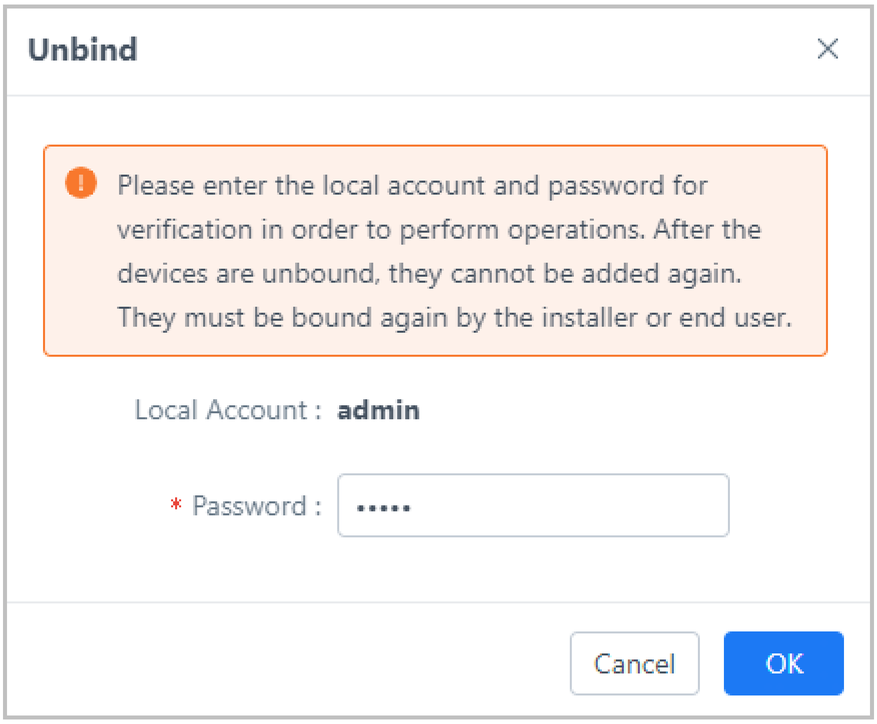
Unbind

□	No.	Device ...	SN	Bind Time	Cloud Connection	Added	Activated	Action
□	1	[redacted]	620000...	2002-09-13 19:58:31	--	Yes	No	Unbind
□	2	[redacted]	340000...	2002-09-13 19:58:31	--	No	Yes	Unbind
□	3	[redacted]	540000...	2002-09-13 19:58:31	--	No	No	Unbind
□	4	[redacted]	330000...	2002-09-13 19:58:31	● Offline	No	No	Unbind
□	5	[redacted]	350000...	2002-09-13 19:58:31	--	No	No	Unbind
□	6	[redacted]	410000...	2002-09-13 19:58:31	● Online	No	No	Unbind
□	7	[redacted]	320000...	2002-09-13 19:58:31	● Online	Yes	No	Unbind
□	8	[redacted]	360000...	2002-09-13 19:58:31	● Online	Yes	Yes	Unbind
□	9	[redacted]	650000...	2002-09-13 19:58:31	--	Yes	Yes	Unbind
□	10	[redacted]	710000...	2002-09-13 19:58:31	● Online	Yes	No	Unbind

Total records: 100

Step 3 Click **Unbind** next to a device, enter the password of the Converter account, and then click **OK** to unbind the chosen devices.

Figure 4-13 Unbind



Unbind

Please enter the local account and password for verification in order to perform operations. After the devices are unbound, they cannot be added again. They must be bound again by the installer or end user.

Local Account : admin

* Password : •••••

Or you can select multiple pieces of information, and then click **Unbind** at the top left corner of the page to batch unbind the devices.

4.2 Cloud Connection

You can add the control panel to Converter through cloud connection.

Prerequisites

- Make sure that you have added the control panel to Dolynk Care app or DMSS. For detailed operation of device adding, see their user's manual for reference.
- Make sure that you have created a cloud account and configured cloud settings. See "4.2.1 Creating Converter Cloud Account".

4.2.1 Creating Converter Cloud Account

You need to create a cloud account to have Converter access to cloud if you want to add devices through cloud access.

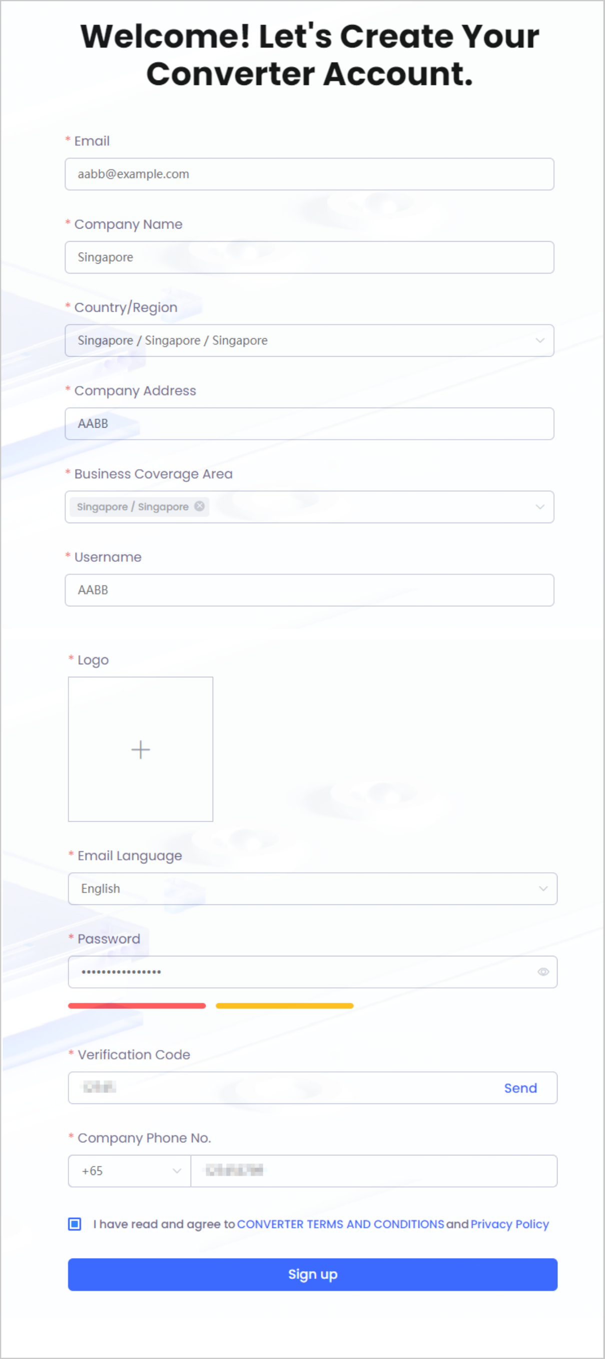
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Cloud Connection** , and then click **Create Cloud Account**.

Step 3 Enter the registration information.

Figure 4-14 Registration



Welcome! Let's Create Your Converter Account.

* Email

aabb@example.com

* Company Name

Singapore

* Country/Region

Singapore / Singapore / Singapore

* Company Address

AABB

* Business Coverage Area

Singapore / Singapore

* Username

AABB

* Logo

+

* Email Language

English

* Password

••••••••••••••••

* Verification Code

[redacted] Send

* Company Phone No.

+65 [redacted]

☑ I have read and agree to CONVERTER TERMS AND CONDITIONS and Privacy Policy

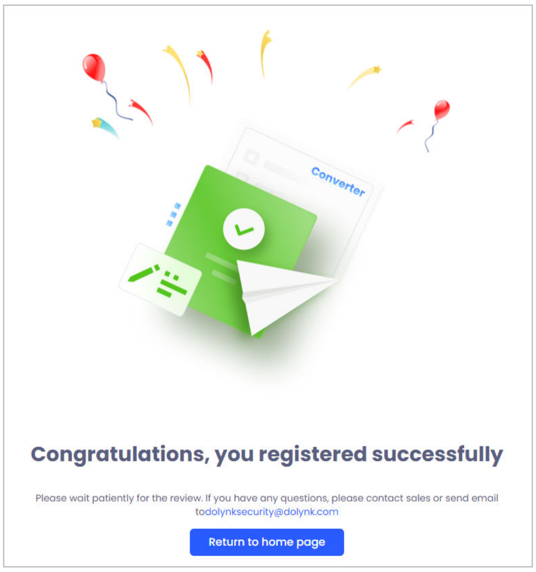
Sign up

Step 4 Click **Send** and the verification will be sent to the email address that is filled in the registration page in few minutes. Enter the received code in the check box.

Step 5 Click the check box next to **I have read and agree to User Agreement And Privacy Policy** after you read them, and then click **Sign up** to finish the registration.

Contact the technical support from the country you select in registration to approve the account you submitted. Only after successful approval, you can progress with login.

Figure 4-15 Registration succeed



Congratulations, you registered successfully

Please wait patiently for the review. If you have any questions, please contact sales or send email todolynksecurity@dolynk.com

Step 6 Log in to the webpage of Converter.

Step 7 Select **Setting** > **Cloud Connection**

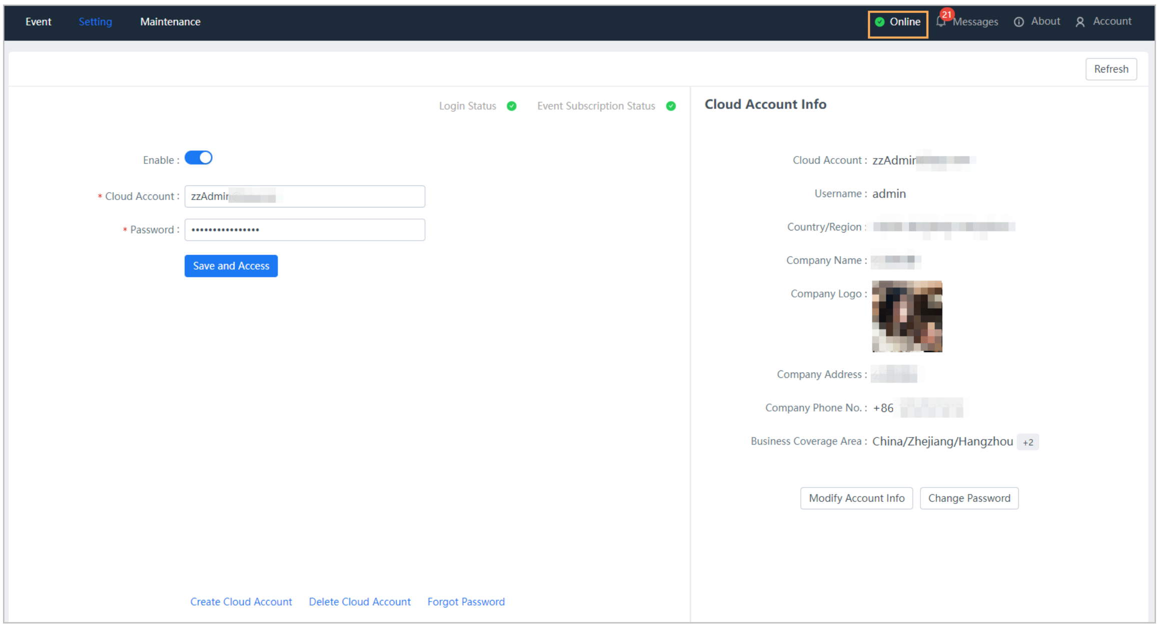
Step 8 Click **Enable** to enable the cloud access function.

- The function is turned off by default.
- You need to enable the function if you want to add devices through cloud access. Otherwise, keep it by default.

Step 9 Enter the user name and password of the cloud account, and then click **Save and Access**.

The online or offline status of the cloud account will be displayed at the top-right corner of the page.

Figure 4-16 Cloud access



Login Status
Event Subscription Status

Enable :

* Cloud Account : zzAdmi[redacted]

* Password : ••••••••••••••••

Cloud Account Info

Cloud Account : zzAdmi[redacted]

Username : admin

Country/Region : [redacted]

Company Name : [redacted]

Company Logo : [redacted]

Company Address : [redacted]

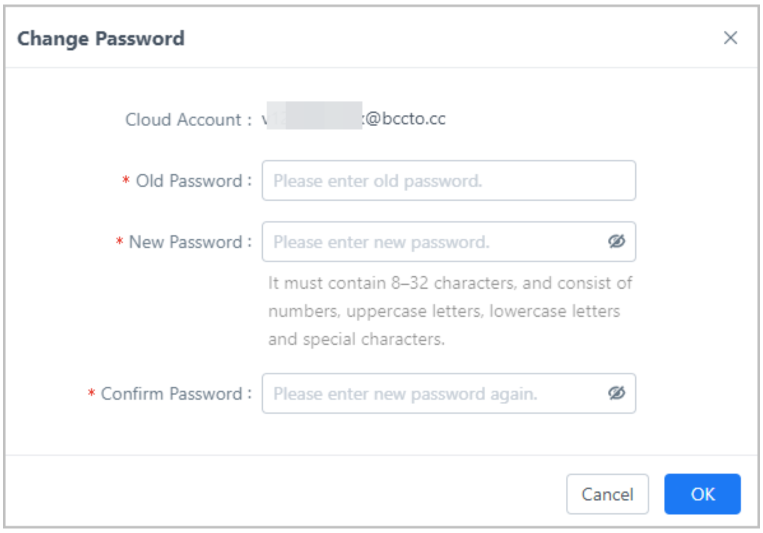
Company Phone No. : +86 [redacted]

Business Coverage Area : China/Zhejiang/Hangzhou +2

Step 10 Click **Refresh** to update the webpage, and then the **Cloud Account Info** displays the account information.

Step 11 (Optional) Click **Change Password** to change the password for the account, and then click **OK**.

Figure 4-17 Change password



Change Password

Cloud Account : v[redacted]@bccto.cc

* Old Password : Please enter old password.

* New Password : Please enter new password.

It must contain 8–32 characters, and consist of numbers, uppercase letters, lowercase letters and special characters.

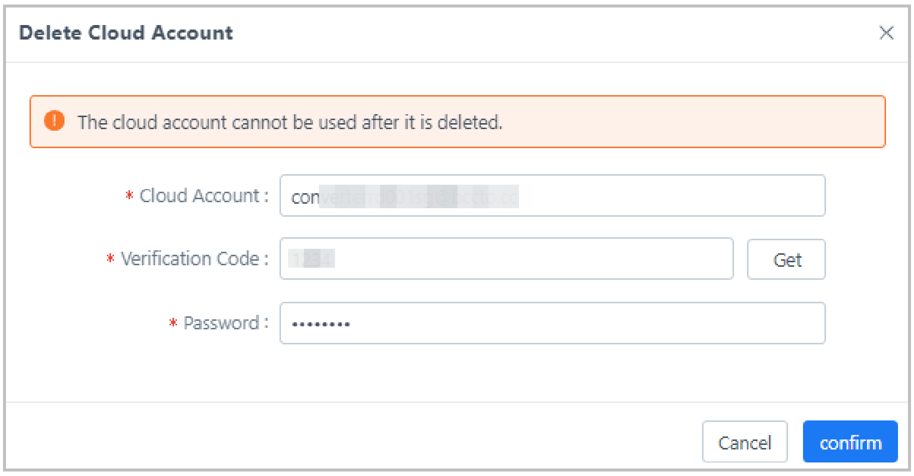
* Confirm Password : Please enter new password again.

Related Operations

- Delete cloud account:

  1. Click **Delete Cloud Account** , enter the cloud account to be deleted, click **Get** to obtain the verification code, and then enter the password for the account.

     Figure 4-18 Delete cloud account

     Delete Cloud Account

     The cloud account cannot be used after it is deleted.

     * Cloud Account : con[redacted]

     * Verification Code : [redacted]

     * Password : ••••••••

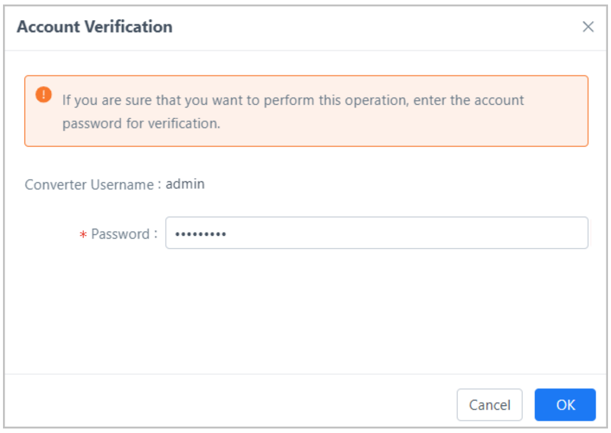
  2. Click **Confirm**.

- Modify cloud account:

  1. Click **Modify Account Info**.
  2. Enter the password to log in to the current cloud account, and then modify the information.

     The modified information requires approval from the company on DoLynk Care. When the approval process is ongoing, the **Modify Account Info** button will be disabled and appear grayed out.

Figure 4-19 Enter password



Account Verification

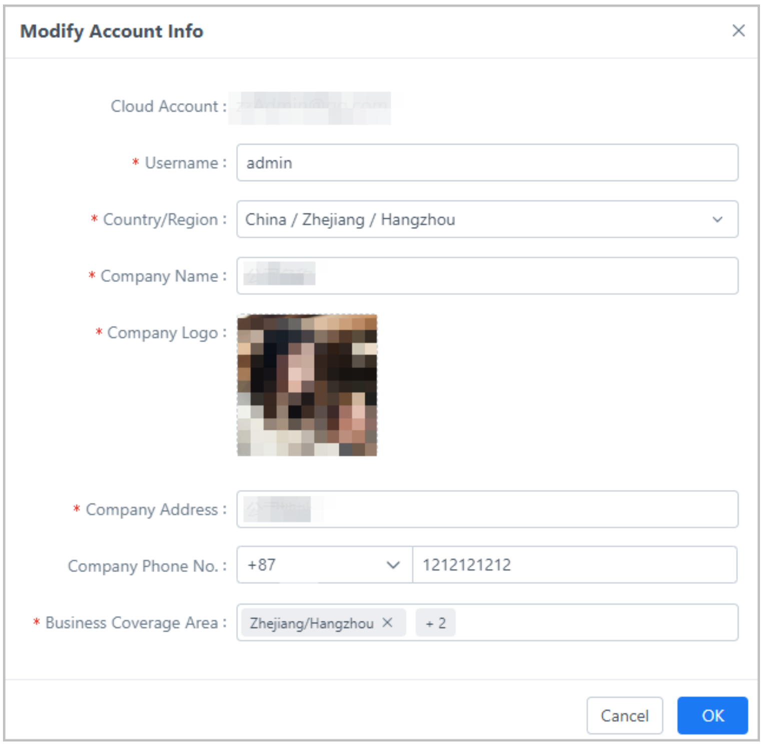
If you are sure that you want to perform this operation, enter the account password for verification.

Converter Username : admin

* Password : •••••••••

Cancel OK

Figure 4-20 Modify information



Modify Account Info

Cloud Account : [redacted]

* Username : admin

* Country/Region : China / Zhejiang / Hangzhou

* Company Name : [redacted]

* Company Logo : [redacted]

* Company Address : [redacted]

Company Phone No. : +87 1212121212

* Business Coverage Area : Zhejiang/Hangzhou × + 2

Cancel OK

4.2.2 Adding Control Panel

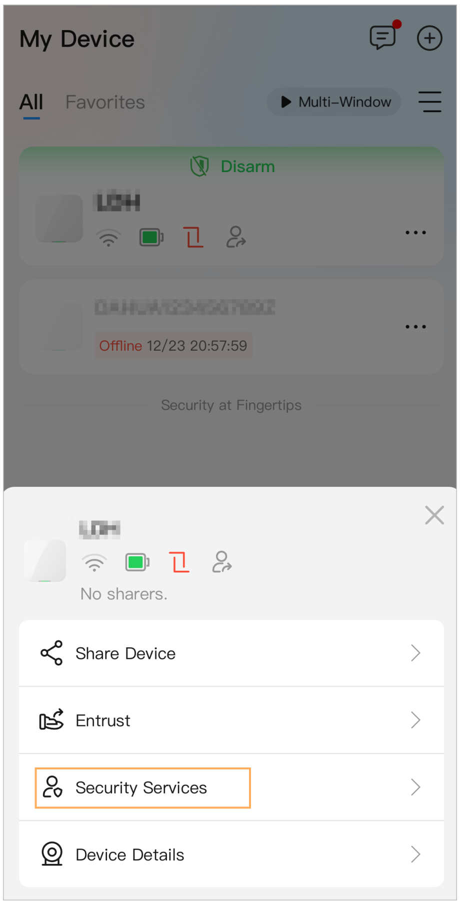
Add the control panel through DMSS or DoLynk Care. The operation on DMSS and DoLynk Care are alike, and here the DMSS is used as an example.

Procedure

Step 1 On your phone, tap to open the DMSS app.

Step 2 On the **Device** screen, tap ••• next to a device, and then tap **Security Services**.

Figure 4-21 Apply for security services



My Device

All Favorites ▶ Multi-Window

Disarm

Offline 12/23 20:57:59

Security at Fingertips

No sharers.

Share Device

Entrust

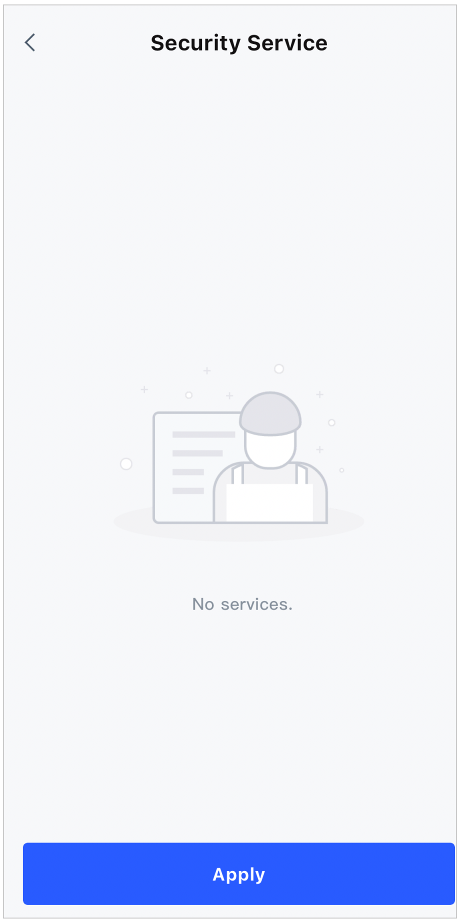
Security Services

Device Details

Step 3 Select the services from the list, and then tap **OK**.

If there are no services added, you can tap **Apply**.

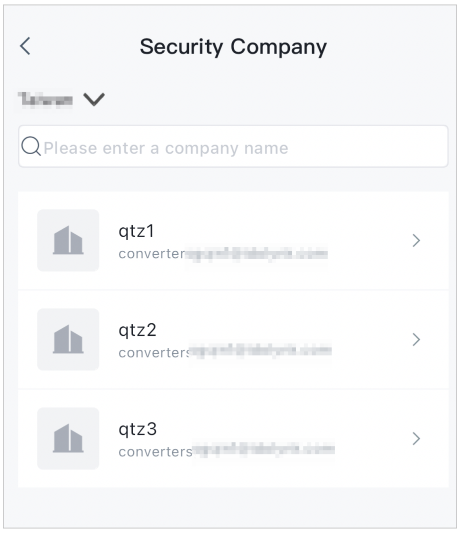
Figure 4-22 Apply



Security Service

No services.

Figure 4-23 Select country or region



Security Company

[redacted]

Please enter a company name

qtz1
converter[redacted]

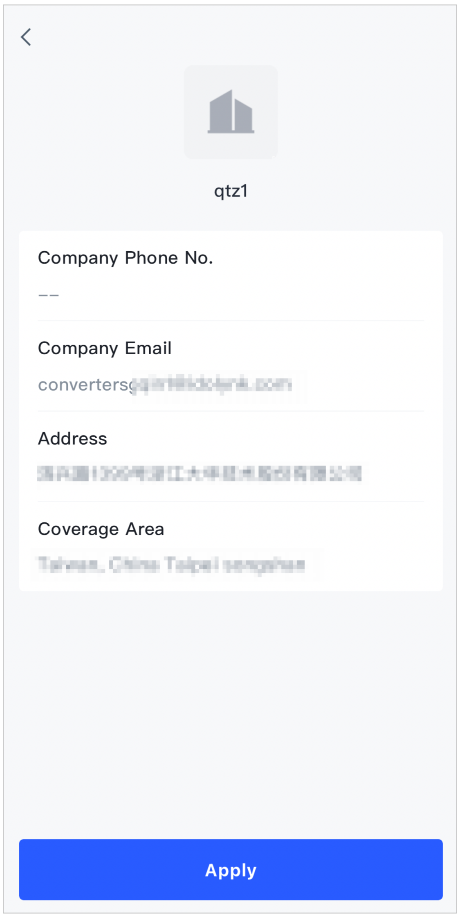
qtz2
converters[redacted]

qtz3
converters[redacted]

Step 4 Select a cloud account under the country or region you select, and then tap **Apply** to bind it.

If you do not know which region the cloud account is registered under, you can enter the complete cloud account to perform accurate search for cloud accounts under the server.

Figure 4-24 Select account



qtz1

Company Phone No.

--

Company Email

converters[redacted]

Address

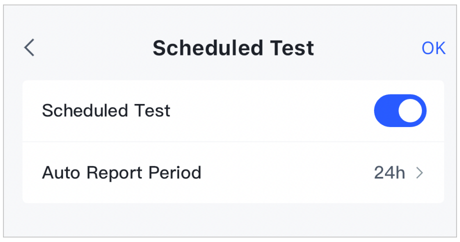
[redacted]

Coverage Area

[redacted]

Step 5 On the **Companies Applied for** screen, tap ⚙, and enable **Scheduled Test** and configure the auto report period, and then tap **OK**.

Figure 4-25 Auto report period



Scheduled Test ●

Auto Report Period 24h >

4.2.3 Device Management

4.2.3.1 Activating/Deactivating the Control Panel

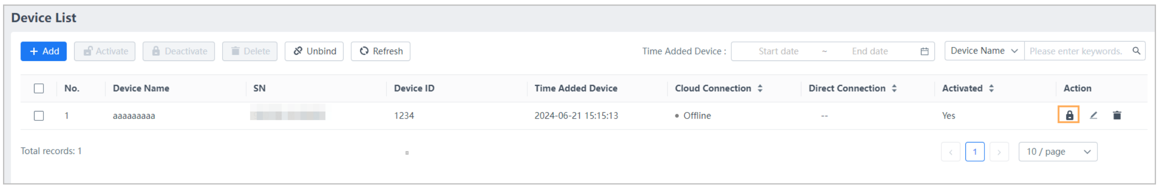
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Device** > **Device List**.

Step 3 Select the device, click 🔓 next to a device, or click **Activate** on the top left corner of the page to activate the chosen device(s).

Figure 4-26 Activation page



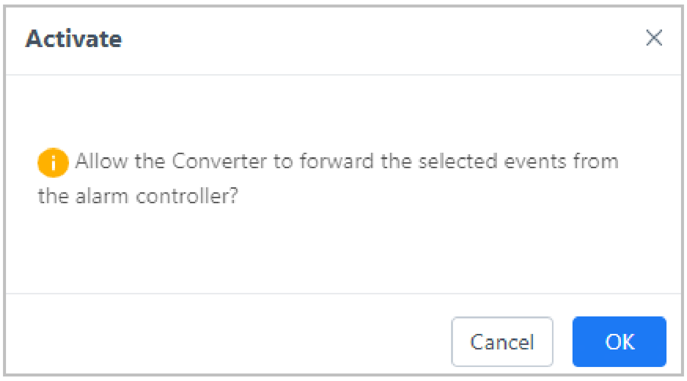
Device List

□	No.	Device Name	SN	Device ID	Time Added Device	Cloud Connection	Direct Connection	Activated	Action
□	1	aaaaaaaaa	[redacted]	1234	2024-06-21 15:15:13	• Offline	--	Yes	

Total records: 1

Step 4 On the **Activate** window, click **OK** to confirm the activation.

Figure 4-27 Activate the device



Activate

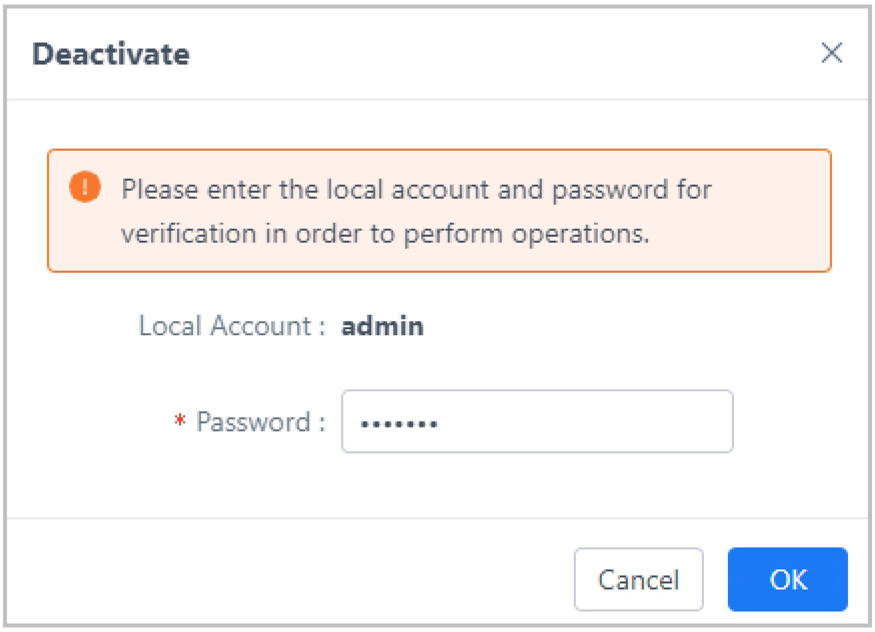
Allow the Converter to forward the selected events from the alarm controller?

Related Operations

Deactivating the control panel:

1. Select **Device** > **Device List**, select the device, and then click **Deactivate**.
2. Enter the password of Converter account, and then click **OK** to deactivate the selected devices.

Figure 4-28 Deactivate confirmation



Deactivate

Please enter the local account and password for verification in order to perform operations.

Local Account : admin

* Password : •••••••

4.2.3.2 Unbinding the Control Panel

Background Information

Unbind the device if the alarm services expire or in case of false operation. Be advised that unbinding for expired services must be done through the cloud.

The device will be removed from the device list after unbinding.

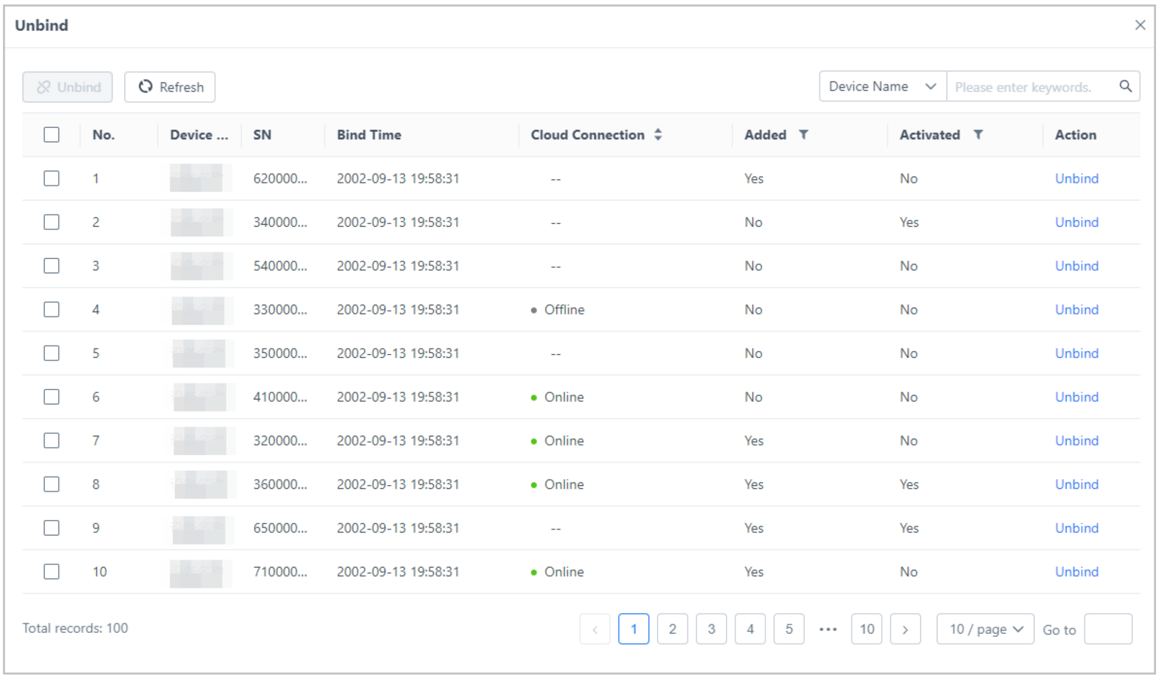
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Device** > **Device List**, and then click **Unbind** to go to the **Unbind** page.

You can filter devices that are added or activated or not.

Figure 4-29 Enter unbind page



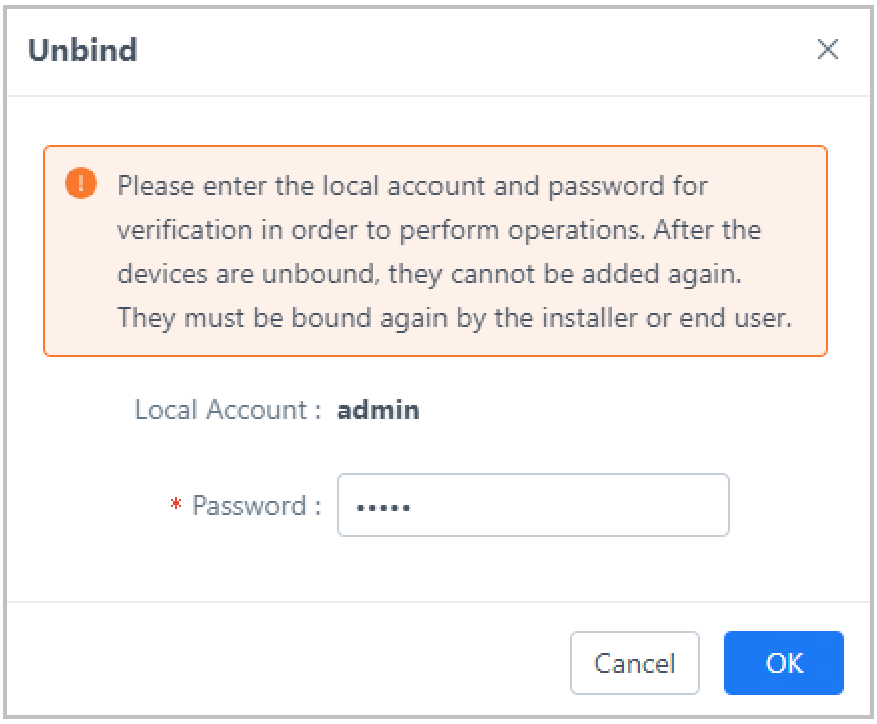
Unbind

□	No.	Device ...	SN	Bind Time	Cloud Connection	Added	Activated	Action
□	1	[redacted]	620000...	2002-09-13 19:58:31	--	Yes	No	Unbind
□	2	[redacted]	340000...	2002-09-13 19:58:31	--	No	Yes	Unbind
□	3	[redacted]	540000...	2002-09-13 19:58:31	--	No	No	Unbind
□	4	[redacted]	330000...	2002-09-13 19:58:31	● Offline	No	No	Unbind
□	5	[redacted]	350000...	2002-09-13 19:58:31	--	No	No	Unbind
□	6	[redacted]	410000...	2002-09-13 19:58:31	● Online	No	No	Unbind
□	7	[redacted]	320000...	2002-09-13 19:58:31	● Online	Yes	No	Unbind
□	8	[redacted]	360000...	2002-09-13 19:58:31	● Online	Yes	Yes	Unbind
□	9	[redacted]	650000...	2002-09-13 19:58:31	--	Yes	Yes	Unbind
□	10	[redacted]	710000...	2002-09-13 19:58:31	● Online	Yes	No	Unbind

Total records: 100

Step 3 Click **Unbind** next to a control panel, enter the password of the Converter account, and click **OK** to unbind the chosen devices.

Figure 4-30 Unbind



Unbind

Please enter the local account and password for verification in order to perform operations. After the devices are unbound, they cannot be added again. They must be bound again by the installer or end user.

Local Account : admin

* Password : ••••••

Or you can select multiple pieces of information, and click **Unbind** at the top left corner of the page to batch unbind the devices.

5 Connecting Converter to CMS

5.1 Configuring Message Forwarding

After configuring the forwarding events, the device can forward the selected events when it is activated.

Procedure

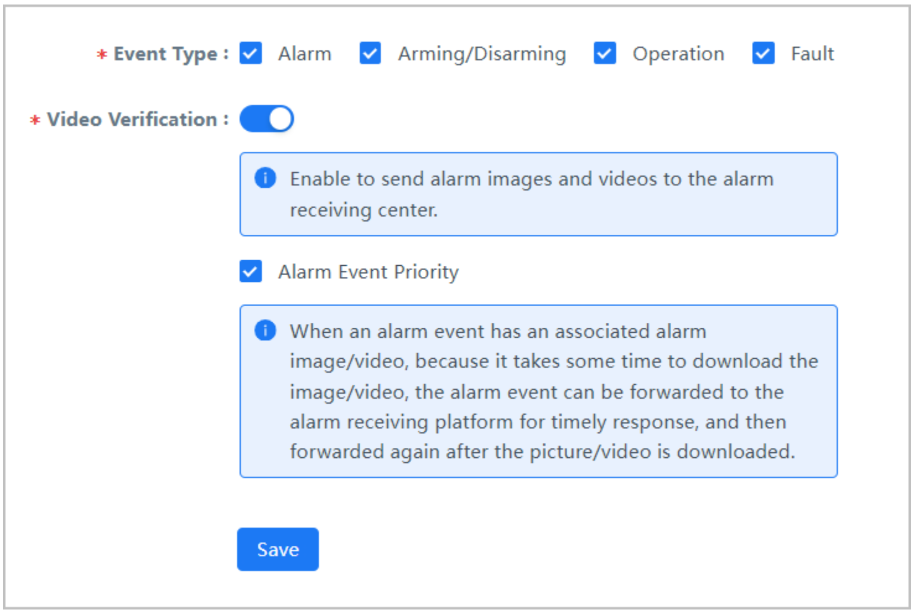
Step 1 Log in to the webpage of Converter.

Step 2 Select **Setting** > **Message Forwarding**.

Step 3 Select the forwarding configuration that you need.

- Event type: Select the event type for forwarding.
- Video verification: Enable the function to send alarm images and videos to the alarm receiving center.
- Alarm event priority: Enable the function to set the priority for alarm messages.

Figure 5-1 Message forward configuration



* Event Type : ☑ Alarm ☑ Arming/Disarming ☑ Operation ☑ Fault

* Video Verification : ●

Enable to send alarm images and videos to the alarm receiving center.

☑ Alarm Event Priority

When an alarm event has an associated alarm image/video, because it takes some time to download the image/video, the alarm event can be forwarded to the alarm receiving platform for timely response, and then forwarded again after the picture/video is downloaded.

Step 4 Click **Save**.

5.2 Configuring Local Storage

Configure storage for images and videos.

Procedure

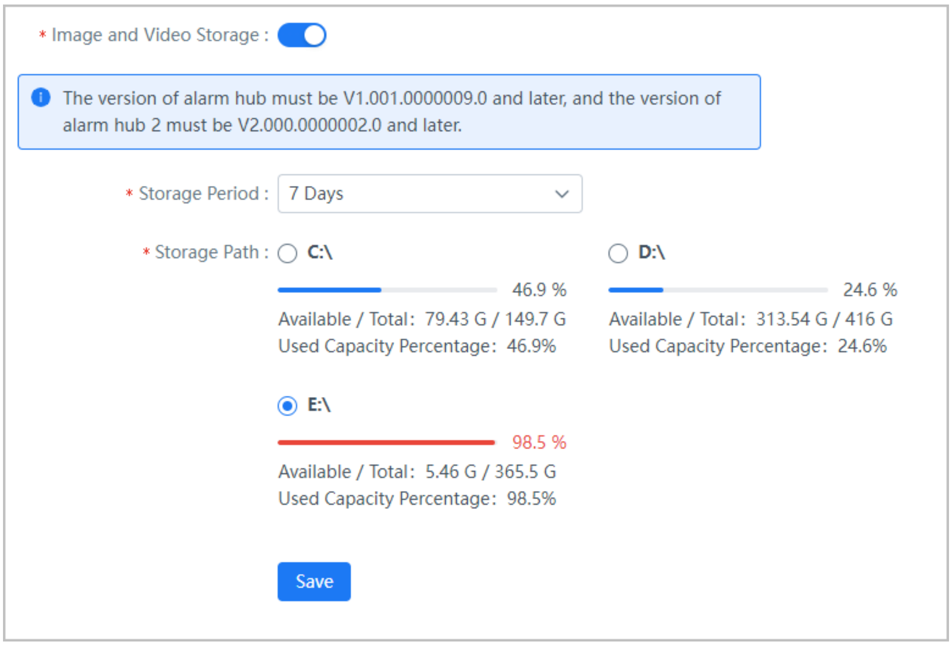
Step 1 Log in to the webpage of Converter.

Step 2 Select **Setting** > **Storage**.

Step 3 Enable the **Image and Video Storage** function.

Step 4 Configure the storage period and select the storage path.

Figure 5-2 Storage



* Image and Video Storage :

The version of alarm hub must be V1.001.0000009.0 and later, and the version of alarm hub 2 must be V2.000.0000002.0 and later.

* Storage Period : 7 Days

* Storage Path : ○ C:\ 46.9 % Available / Total: 79.43 G / 149.7 G Used Capacity Percentage: 46.9%

○ D:\ 24.6 % Available / Total: 313.54 G / 416 G Used Capacity Percentage: 24.6%

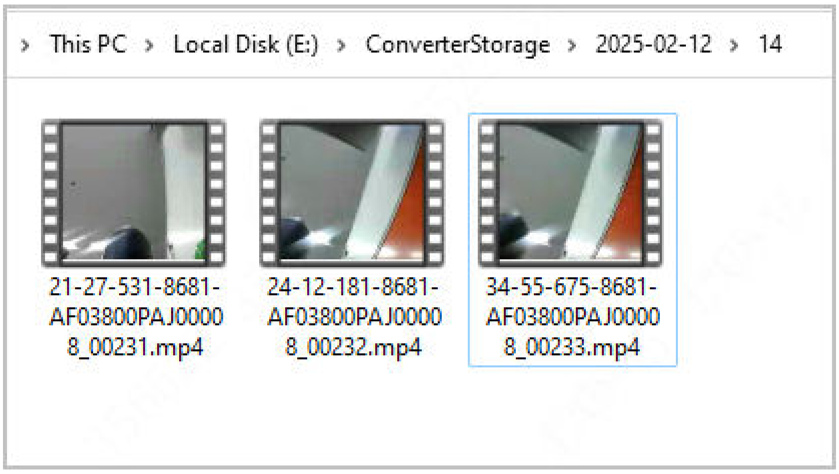
● E:\ 98.5 % Available / Total: 5.46 G / 365.5 G Used Capacity Percentage: 98.5%

Step 5 Click **Save**.

Example

If the local disk E is selected as the storage path, then you can view the images and videos of the alarm event on disk E.

Figure 5-3 Local storage path



› This PC › Local Disk (E:) › ConverterStorage › 2025-02-12 › 14

21-27-531-8681-AF03800PAJ00008_00231.mp4

24-12-181-8681-AF03800PAJ00008_00232.mp4

34-55-675-8681-AF03800PAJ00008_00233.mp4

5.3 Event

5.3.1 Configuring Event Code

Configure the new event code or edit the existing code.

Procedure

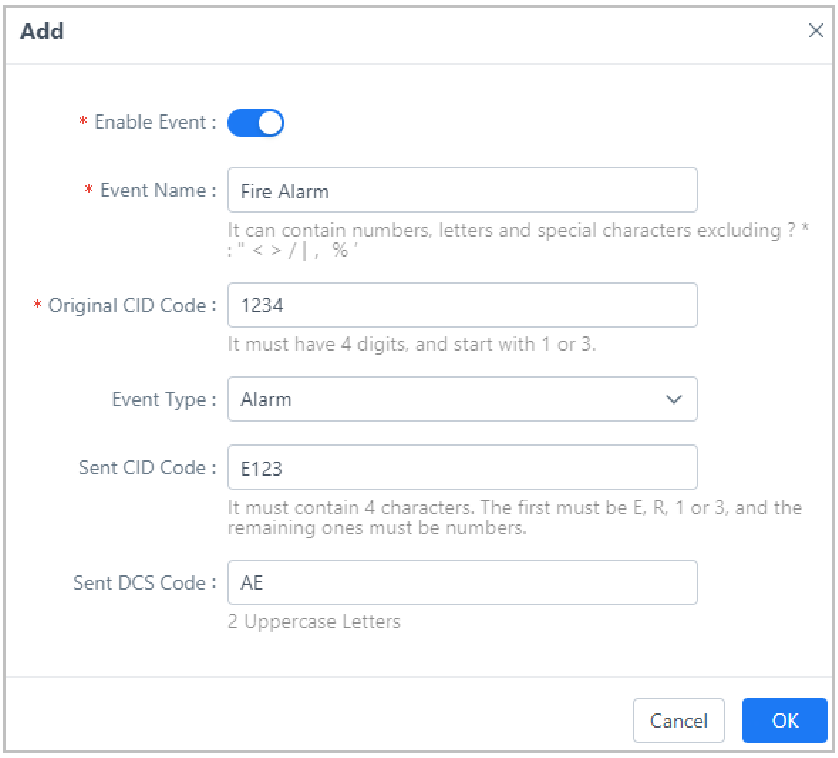
Step 1 Log in to the webpage of the Converter.

Step 2 Select **Event** > **Event Code**.

Step 3 Click **Add** to add new event.

Step 4 Configure the parameters.

Figure 5-4 Event code



Add

* Enable Event : ●

* Event Name : Fire Alarm

It can contain numbers, letters and special characters excluding ? * : " < > / | , % '

* Original CID Code : 1234

It must have 4 digits, and start with 1 or 3.

Event Type : Alarm

Sent CID Code : E123

It must contain 4 characters. The first must be E, R, 1 or 3, and the remaining ones must be numbers.

Sent DCS Code : AE

2 Uppercase Letters

Step 5 Click **OK**.

Related Operations

- **Default** : Restore the event list to default settings.
- **Export** : Export all of the events in the current list.
- **Import** : Import the event list (.xlsx/.xls format) from your local computer.

  You need to finish the excel of the event list. Refer to the exported excel as the template.
- **Delete** : Delete the selected event.

5.3.2 Viewing Log History

View logs of the event, including device name, device ID, event name, event code, event time and time when messages are sent.

Procedure

Step 1 Log in to the webpage of Converter.

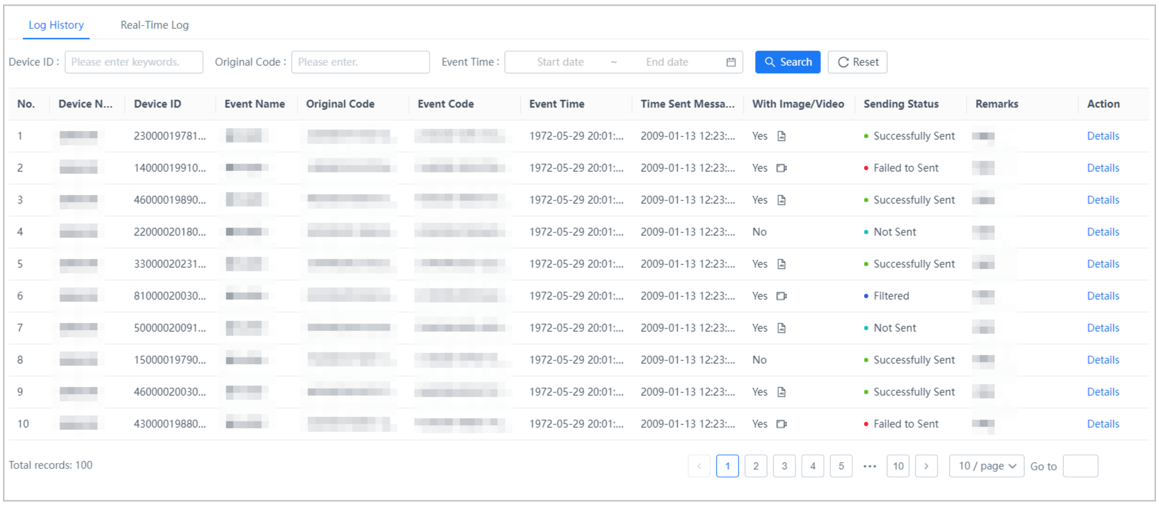
Step 2 Select **Event** > **Event Monitoring** > **Log History**.

Step 3 View log history.

- **Event Time** : The local time zone of the computer where Converter is installation on.
- **Remarks** : Record the reason why the alarm information is discarded.

  The remarks remain empty only when messages are successfully sent.

Figure 5-5 Log list



Log History | Real-Time Log

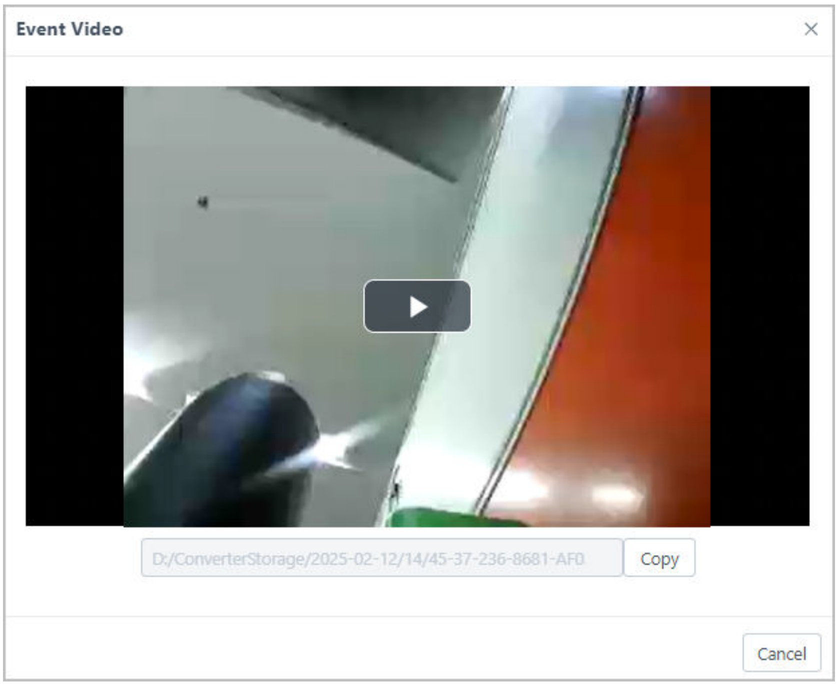
Device ID : Please enter keywords. Original Code : Please enter. Event Time : Start date ~ End date Search Reset

No.	Device N...	Device ID	Event Name	Original Code	Event Code	Event Time	Time Sent Messa...	With Image/Video	Sending Status	Remarks	Action
1	[redacted]	23000019781...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 🖼	● Successfully Sent	[redacted]	Details
2	[redacted]	14000019910...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 📹	● Failed to Sent	[redacted]	Details
3	[redacted]	46000019890...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 🖼	● Successfully Sent	[redacted]	Details
4	[redacted]	22000020180...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	No	● Not Sent	[redacted]	Details
5	[redacted]	33000020231...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 🖼	● Successfully Sent	[redacted]	Details
6	[redacted]	81000020030...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 📹	● Filtered	[redacted]	Details
7	[redacted]	50000020091...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 🖼	● Not Sent	[redacted]	Details
8	[redacted]	15000019790...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	No	● Successfully Sent	[redacted]	Details
9	[redacted]	46000020030...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 🖼	● Successfully Sent	[redacted]	Details
10	[redacted]	43000019880...	[redacted]	[redacted]	[redacted]	1972-05-29 20:01:...	2009-01-13 12:23:...	Yes 📹	● Failed to Sent	[redacted]	Details

Total records: 100

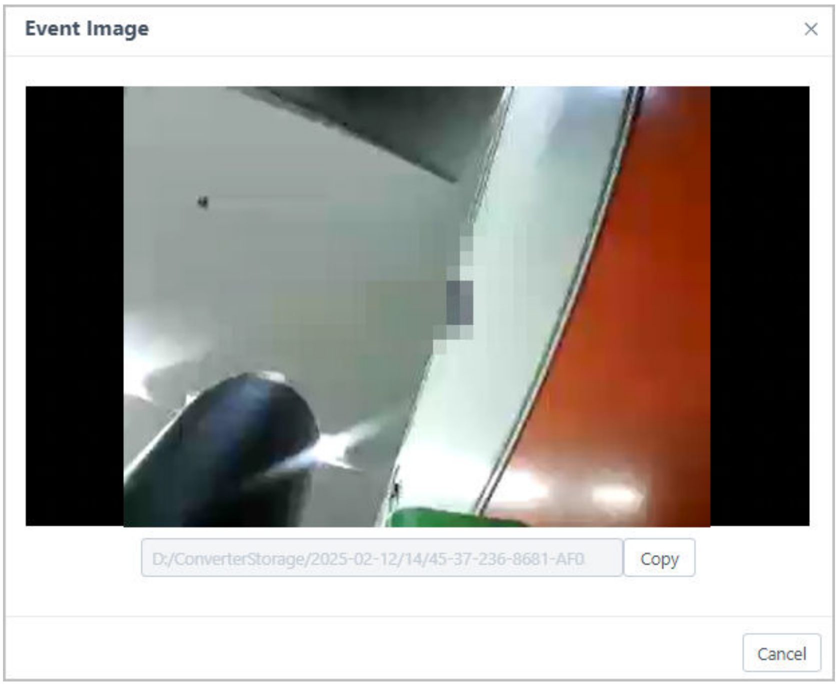
Step 4 (Optional) Click 🖼 to view event image, and click 📹 to view event video.

Figure 5-6 Video



D:/ConverterStorage/2025-02-12/14/45-37-236-8681-AF0

Figure 5-7 Image



D:/ConverterStorage/2025-02-12/14/45-37-236-8681-AF0

Step 5 Click **Details** to view the details of the event.

Related Operations

- Enter the device ID to search for the event logs.
- Enter the original code to search for event logs.
- Enter the start date and end date to search for event logs.

5.3.3 Viewing Real-Time Log

View real-time logs.

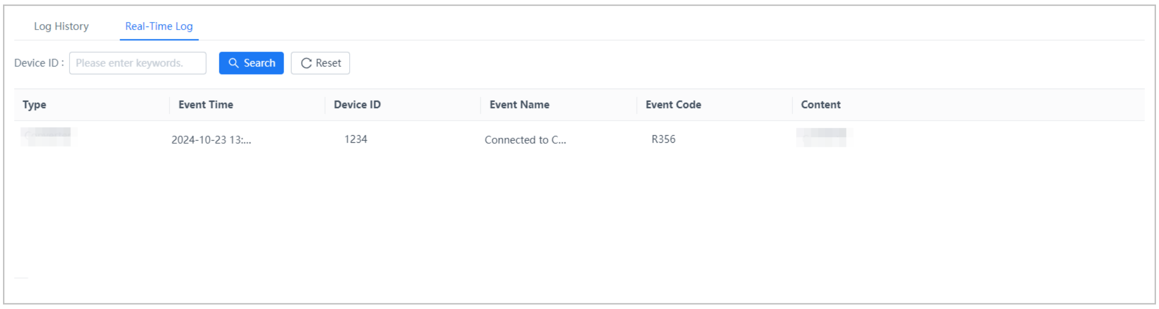
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Event** > **Event Monitoring** > **Real-Time Log**.

Step 3 View real time logs.

Figure 5-8 View real-time logs



Device ID : Please enter keywords.

Type	Event Time	Device ID	Event Name	Event Code	Content
[redacted]	2024-10-23 13:...	1234	Connected to C...	R356	[redacted]

Related Operations

- Enter the device ID to search for the event logs.
- Click **Reset** to restore to default settings.

6 Event Transfer Protocols

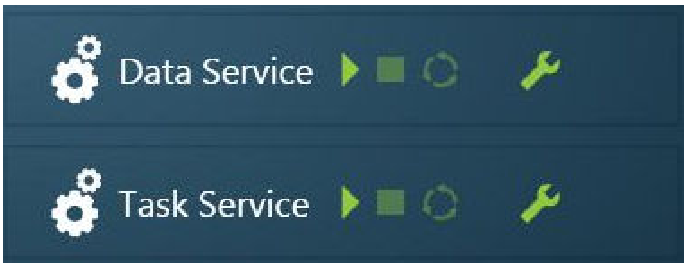
6.1 Event Transfer Configuration

Third-party Configuration

Here uses SIA protocol as an example for illustration.

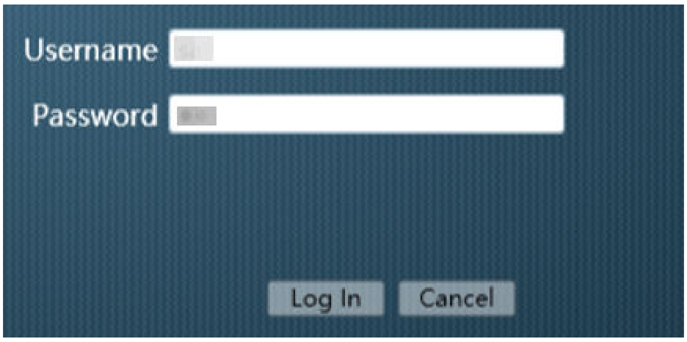
1. Open PatriotConfigurator.exe, complete configuration, and then run the **Data Service** and **Task Service**.

Figure 6-1 Run services



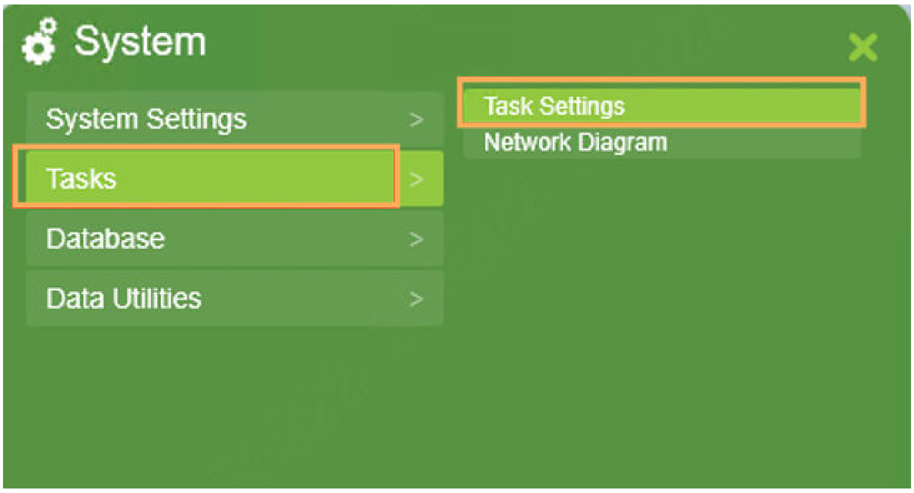
2. Log in to the client.

Figure 6-2 Log in



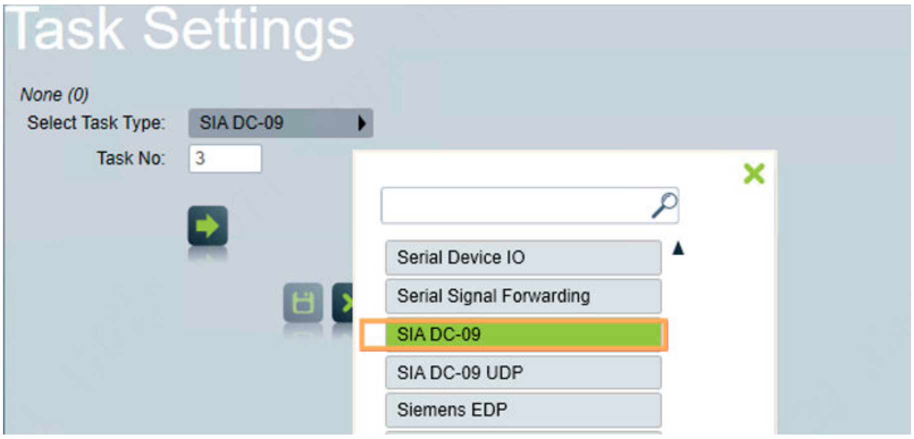
3. Select **System** > **Tasks** > **Task Settings**.

Figure 6-3 Task settings



4. Create a task.
    a. Select the task type as **SIA-DC 09**.

Figure 6-4 Select task type



Task Settings

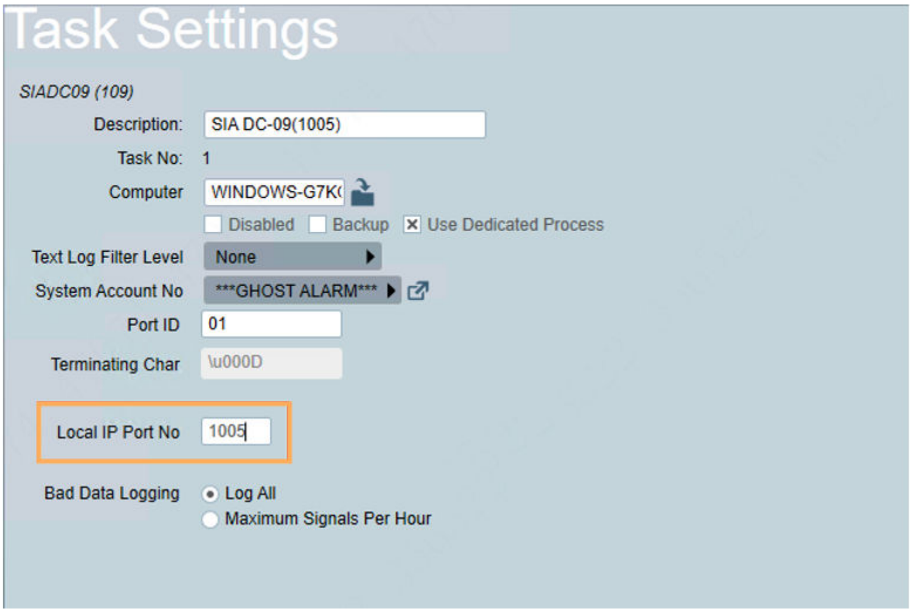
None (0)

Select Task Type: SIA DC-09

Task No: 3

    b. Configure the local IP port number.

Figure 6-5 Configure port number



Task Settings

SIADC09 (109)

Description: SIA DC-09(1005)

Task No: 1

Computer WINDOWS-G7K(

□ Disabled □ Backup ☒ Use Dedicated Process

Text Log Filter Level None

System Account No ***GHOST ALARM***

Port ID 01

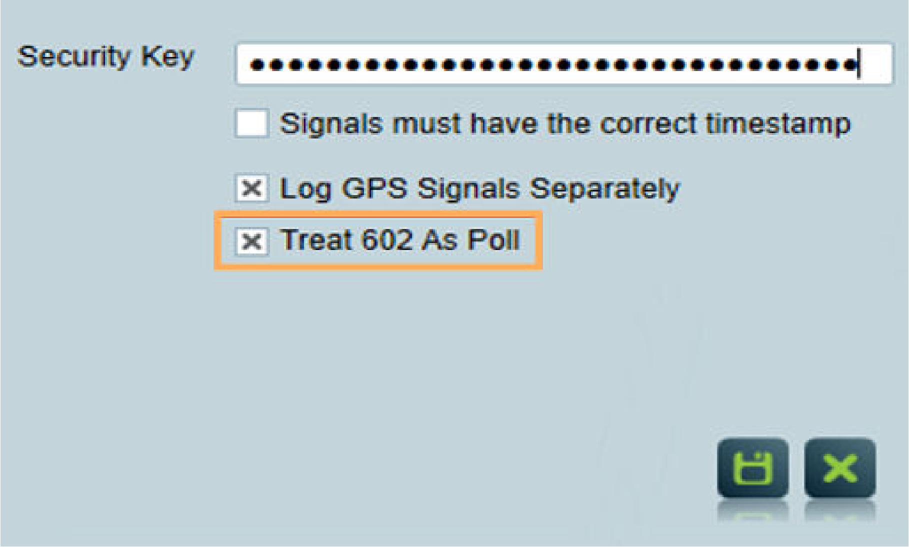
Terminating Char \u000D

Local IP Port No 1005

Bad Data Logging ● Log All ○ Maximum Signals Per Hour

    c. Configure the security key, cancel selection of **Treat 602 As Poll** , and then click **Save**.

Figure 6-6 Security key



Security Key ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

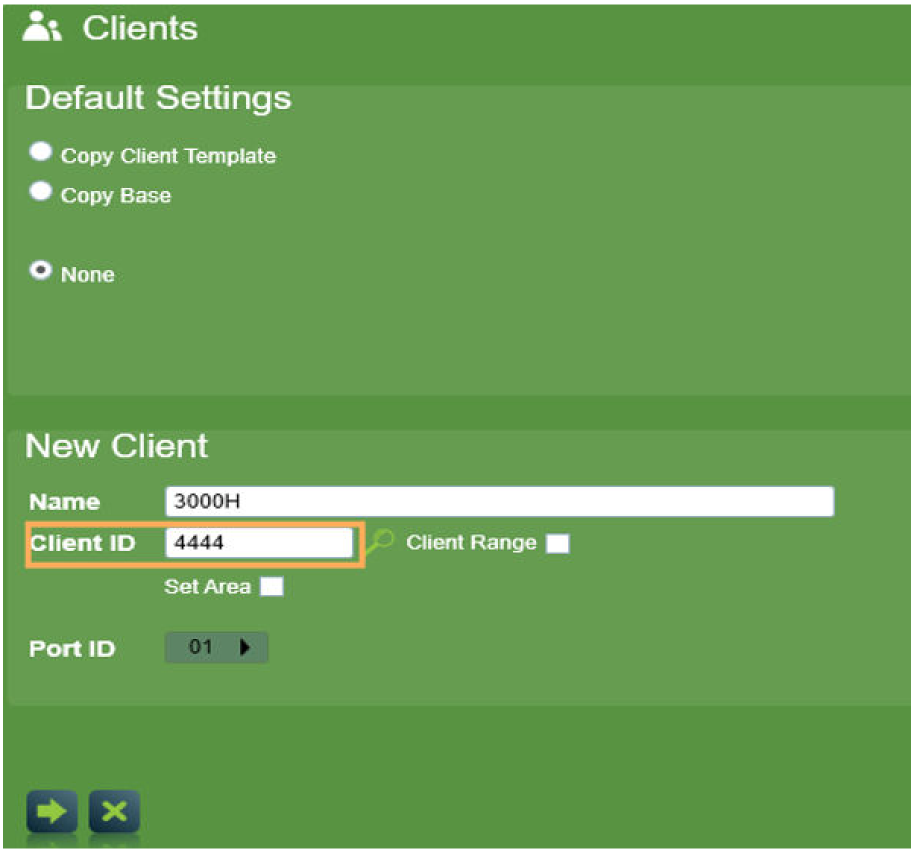
□ Signals must have the correct timestamp

☒ Log GPS Signals Separately

☒ Treat 602 As Poll

5. Create the main account ID and the name, which is the CMS main account that you will apply.

Figure 6-7 Main account ID and name



Clients

Default Settings

○ Copy Client Template

○ Copy Base

● None

New Client

Name 3000H

Client ID 4444 Client Range □

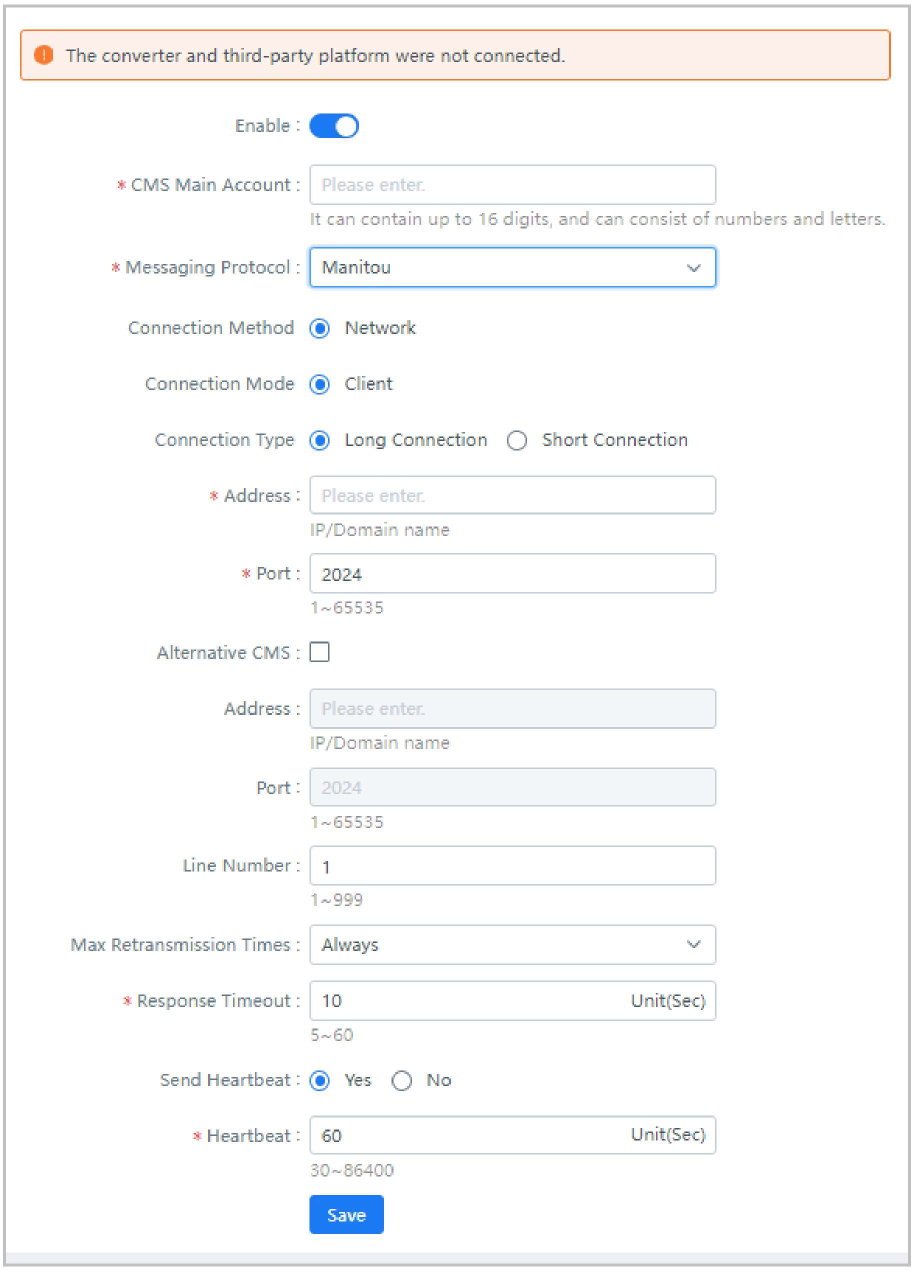
Set Area □

Port ID 01

CMS Configuration

1. Log in to the webpage of Converter.
2. Select **Setting** > **CMS Connection**.
3. Configure the CMS settings.

Figure 6-8 CMS connection (Manitou)



The converter and third-party platform were not connected.

Enable : ●

* CMS Main Account : Please enter.
It can contain up to 16 digits, and can consist of numbers and letters.

* Messaging Protocol : Manitou

Connection Method ● Network

Connection Mode ● Client

Connection Type ● Long Connection ○ Short Connection

* Address : Please enter.
IP/Domain name

* Port : 2024
1~65535

Alternative CMS : □

Address : Please enter.
IP/Domain name

Port : 2024
1~65535

Line Number : 1
1~999

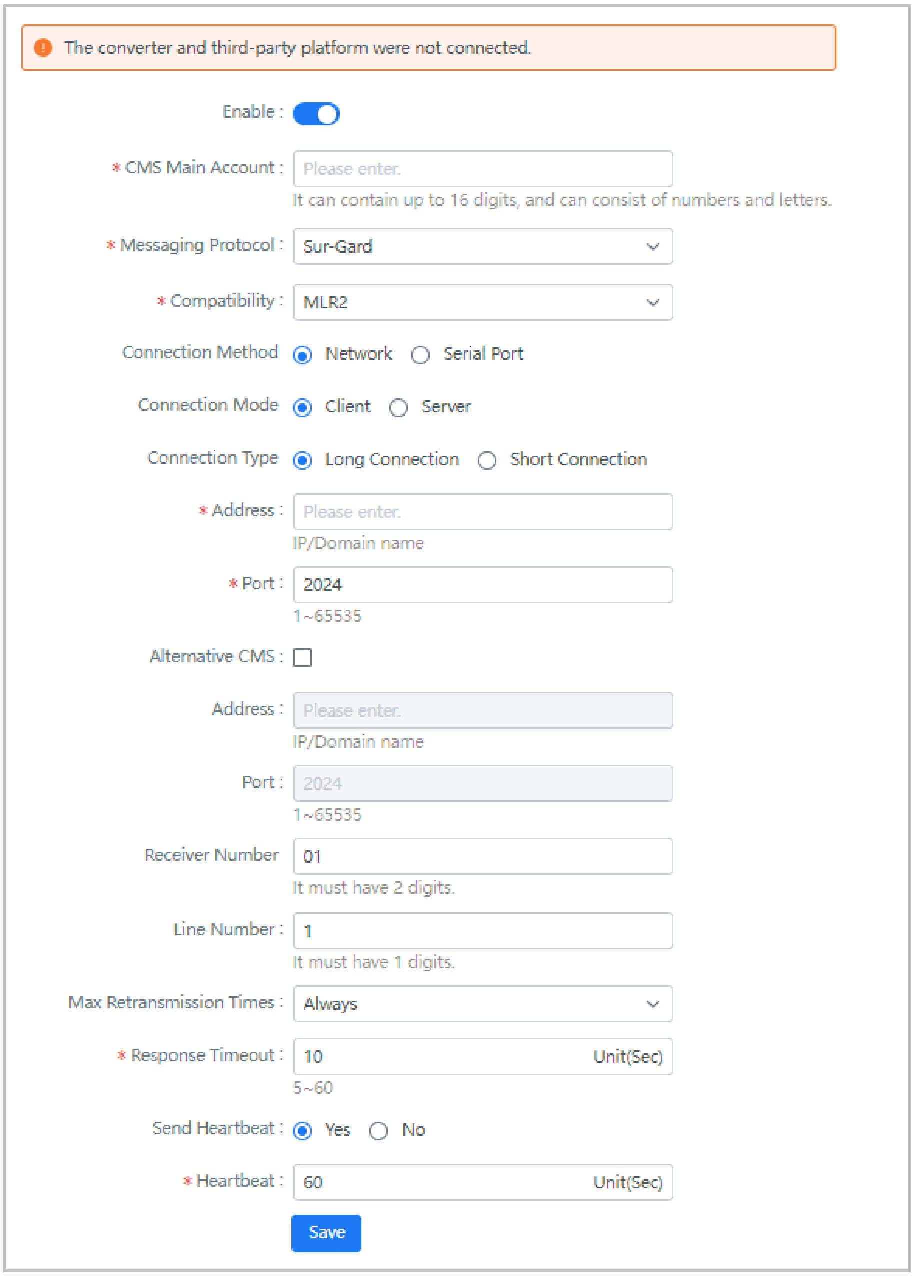
Max Retransmission Times : Always

* Response Timeout : 10 Unit(Sec)
5~60

Send Heartbeat : ● Yes ○ No

* Heartbeat : 60 Unit(Sec)
30~86400

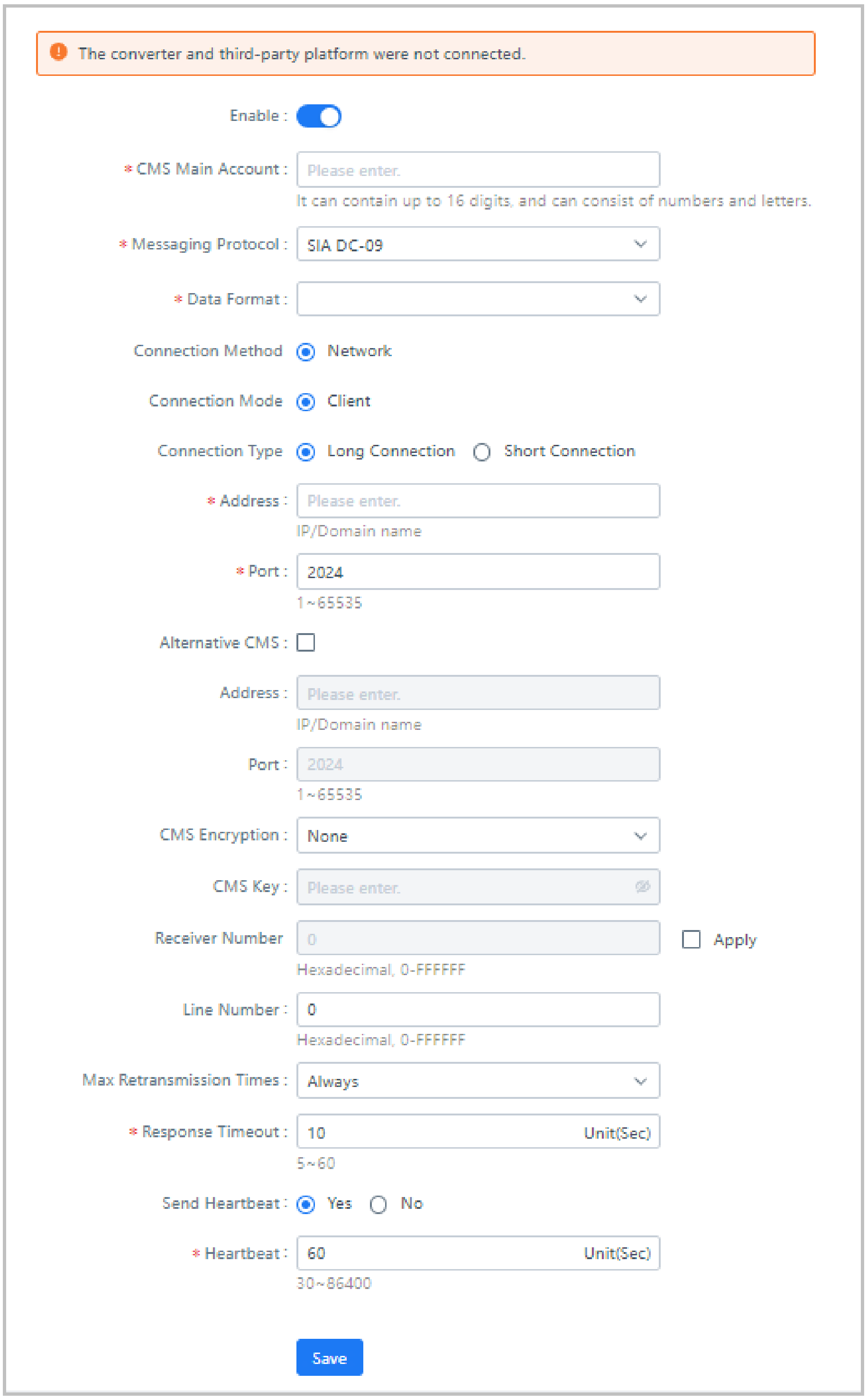
Figure 6-9 CMS connection (Surgard)



The converter and third-party platform were not connected.

Enable :	●
* CMS Main Account :	Please enter. It can contain up to 16 digits, and can consist of numbers and letters.
* Messaging Protocol :	Sur-Gard
* Compatibility :	MLR2
Connection Method	● Network ○ Serial Port
Connection Mode	● Client ○ Server
Connection Type	● Long Connection ○ Short Connection
* Address :	Please enter. IP/Domain name
* Port :	2024 1~65535
Alternative CMS :	□
Address :	Please enter. IP/Domain name
Port :	2024 1~65535
Receiver Number	01 It must have 2 digits.
Line Number :	1 It must have 1 digits.
Max Retransmission Times :	Always
* Response Timeout :	10 Unit(Sec) 5~60
Send Heartbeat :	● Yes ○ No
* Heartbeat :	60 Unit(Sec)

Figure 6-10 CMS(SIA)



The converter and third-party platform were not connected.

Enable : ●

* CMS Main Account : Please enter.
It can contain up to 16 digits, and can consist of numbers and letters.

* Messaging Protocol : SIA DC-09

* Data Format :

Connection Method ● Network

Connection Mode ● Client

Connection Type ● Long Connection ○ Short Connection

* Address : Please enter.
IP/Domain name

* Port : 2024
1~65535

Alternative CMS : □

Address : Please enter.
IP/Domain name

Port : 2024
1~65535

CMS Encryption : None

CMS Key : Please enter.

Receiver Number 0 □ Apply
Hexadecimal, 0-FFFFFF

Line Number : 0
Hexadecimal, 0-FFFFFF

Max Retransmission Times : Always

* Response Timeout : 10 Unit(Sec)
5~60

Send Heartbeat : ● Yes ○ No

* Heartbeat : 60 Unit(Sec)
30~86400

Table 6-1 Description of CMS connection parameter

Parameter	Description
Enable	Enable the forward function.

Parameter		Description
CMS Main Account		The main account is the account of the Converter, which can send heartbeat events to the CMS. The CMS uses the Main account to determine whether the communication between the Converter and the CMS is functioning properly. 📖 The account ID is assigned by the third-party platform to Converter.
Alternative CMS		Enable the function, and enter the address and port of the alternative CMS. 📖 It is decided by the CMS.
Messaging Protocol (SIA)	Data Format	Select **ContactID** or **DCS**.
	Connection Method	**Network** by default.
	Connection Mode	**Client** by default.
	Connection Type	● **Long Connection** : The single TCP connection that is used to send and receive multiple TCP requests or responses. ● **Short Connection** : During data transmission, a connection is established only when it is necessary to send data, and is disconnected after the service is completed.
	Address	Enter the IP address of the server where the event receivers of the monitoring software is located. 📖 It is decided by the CMS.
	Port	Enter the listening port number of the event receiver of the monitoring software (CMS). 📖 It is decided by the CMS.
	CMS Encryption	Select **None** or **AES**. It is **None** by default.
	CMS Key	It can contain 32 characters, where each character is a hexadecimal digit. It is provided by CMS.
	Receiver Number	It can be a hexadecimal from 0–FFFFFF.
	Line Number	
Messaging Protocol (Manitou)	Connection Method	It is **Network** by default.
	Connection Mode	It is **Client** by default.
	Address	Enter the IP address of the server where the event receiver of the monitoring software (CMS) is located. 📖 It is decided by the CMS.

Parameter		Description
	Port	Enter the listening port number of the monitoring software (CMS). 📖 It is decided by the CMS.
	Line Number	It can be 1-999.
Messaging Protocol (Surgard)	Compatibility	Select **MLR2** or **MLR2000**. 📖 The option you select for compatibility is based on the third-party platform.
	Connection Method (Network)	Connection Mode: Select **Client** or **Server**.
		Connection Type: ● **Long Connection** : The single TCP connection that is used to send and receive multiple TCP requests/responses. ● **Short Connection** : During data transmission, a connection is established only when it is necessary to send data, and is disconnected after the service is completed.
		Address: Enter the IP address of the server where the event receiver of the monitoring software (CMS) is located. 📖 It is decided by the CMS.
		Port: Enter the listening port number of the event receiver of the monitoring software (CMS). 📖 It is decided by the CMS.
	Connection Method (Serial Port)	COM Number: Select the serial port number for the local computer, with the Converter installed on, to establish a connection with third-party platform.
		Baud Rate: The unit of measurement for symbol rate that determines the speed of communication. The higher the rate is, the faster the communication will be.
		Data Bits: The number of bits used to represent one character of data. You can select **5** , **6**,**7** and **8**. For example, if you select **8**, then it means the serial communication can transfer a total of eight bits that valued 0 or 1. 📖 Most forms of data requires 8 bits.

Parameter		Description
		Stop Bits: A bit(s) that marks the end of a unit of transmission. You can select **1** , **1.5** and **2**. 📖 The greater the number of stop bits, the more tolerance there is for synchronization. But the data transmission rate is slower.
		Parity: A method to check for parity error that is used to verify the accuracy of serial communication. ● **None** : No parity bit. ● **Odd** : The parity bit is set to 1 if there is an odd number of one bits in a one-byte data item. If the number of one bits adds up to an even number, the parity bit is set to 0. ● **Even** : The parity bit is set to 0 if there is an even number of one bits in a one-byte data item. If the number of one bits adds up to an odd number, the parity bit is set to 1. ● **Mark** : The parity bit is 1. ● **Space** : The parity bit is 0.
	Receiver Number	It must have 2 digits.
	Line Number	It must have 3 digits when **MLR2000** is selected as compatibility, and 1 digit when **MLR2** is selected.
Max Retransmission Times		Once the number of retransmissions reaches the defined value, all remaining alarm messages that are sent will be filtered out.
Response Timeout		The duration of time that the system waits for a response before considering it as a failure or timeout.
Send Heartbeat		Select **Yes** if you need this function, or **No** to disable it.
Heartbeat		A regular interval sent between machines.
Listen for COM port heartbeat answers		If you set **Connection Method** as the **Serial Port**, you can enable the **Listen for COM port heartbeat answers**. It is enabled by default.

6.2 Protocol Overview

The Converter supports protocols for transmitting events to CMS.

Table 6-2 Protocol introduction

Protocol	Description
SIA DC-09 (ADM-CID)	Messages can transmit additional information in the form of a link to a web resource, geographic coordinates, or other standardized data. This protocol supports: ● Alarm and event transmission ● Transmission of visual alarm verifications

Protocol	Description
SurGard	This protocol supports alarm and event transmission.
MANITOU	This protocol supports: ● Alarm and event transmission ● Transmission of visual alarm verifications

6.2.1 SIA Configuration

For details, see the SIA part in "6.1 Event Transfer Configuration".

6.2.2 SurGard Configuration

For details, see the SurGard part in "6.1 Event Transfer Configuration".

6.2.3 MANITOU Configuration

For details, see the MANITOU part in "6.1 Event Transfer Configuration".

7 Maintenance

7.1 Viewing Operation Logs

View logs of the operation on Converter.

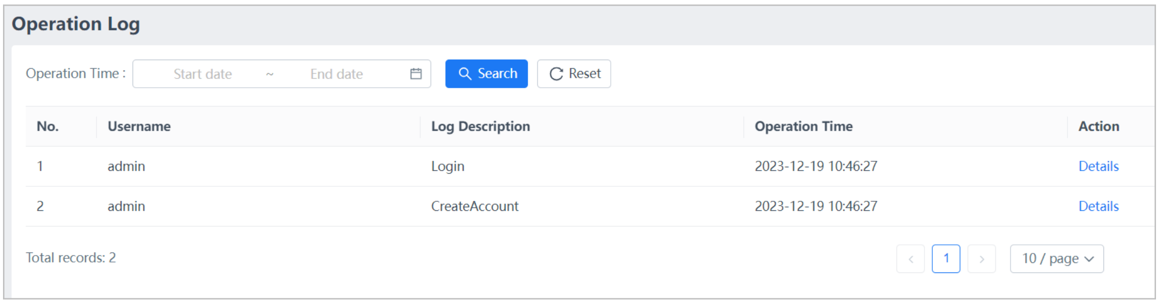
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Maintenance** > **Operation Logs**.

Step 3 Configure the operation time to view the operation logs.

Figure 7-1 Operation logs



No.	Username	Log Description	Operation Time	Action
1	admin	Login	2023-12-19 10:46:27	Details
2	admin	CreateAccount	2023-12-19 10:46:27	Details

Total records: 2

Step 4 Click **Details** to view the details of the specific operation.

7.2 Managing Protocols

Manage different protocols.

Background Information

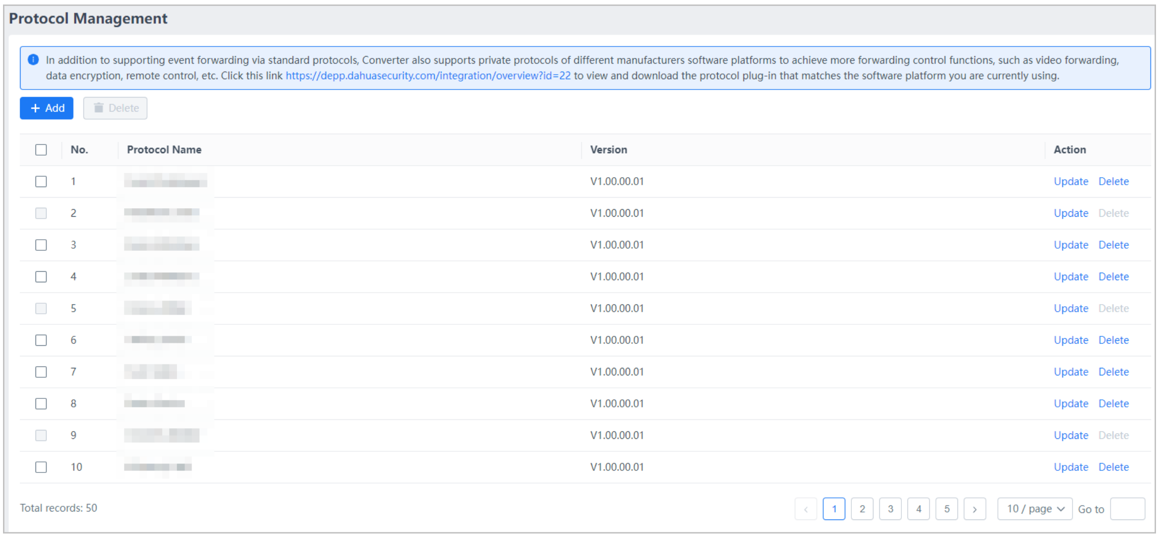
In addition to supporting event forwarding via standard protocols, Converter also supports private protocols of different manufacturers software platforms to achieve more forwarding control functions, such as video forwarding, data encryption and remote control.

Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Maintenance** > **Protocol Management**.

Figure 7-2 Protocol management



Protocol Management

In addition to supporting event forwarding via standard protocols, Converter also supports private protocols of different manufacturers software platforms to achieve more forwarding control functions, such as video forwarding, data encryption, remote control, etc. Click this link https://depp.dahuasecurity.com/integration/overview?id=22 to view and download the protocol plug-in that matches the software platform you are currently using.

□	No.	Protocol Name	Version	Action
□	1	[redacted]	V1.00.00.01	Update Delete
□	2	[redacted]	V1.00.00.01	Update Delete
□	3	[redacted]	V1.00.00.01	Update Delete
□	4	[redacted]	V1.00.00.01	Update Delete
□	5	[redacted]	V1.00.00.01	Update Delete
□	6	[redacted]	V1.00.00.01	Update Delete
□	7	[redacted]	V1.00.00.01	Update Delete
□	8	[redacted]	V1.00.00.01	Update Delete
□	9	[redacted]	V1.00.00.01	Update Delete
□	10	[redacted]	V1.00.00.01	Update Delete

Total records: 50

Step 3 Click **Add** to add new protocols.

Related Operations

- Click **Update** to update the protocol.
- Click **Delete** to delete the protocol.

7.3 Exporting System Logs

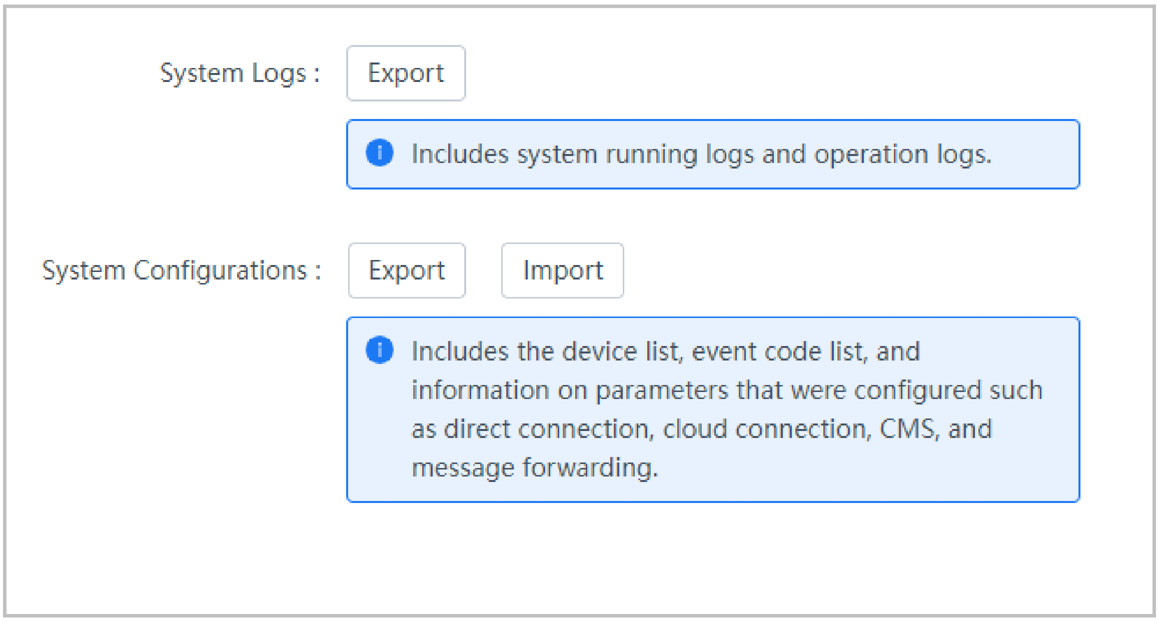
Export system logs.

Procedure

Step 1 Log in to the webpage of the Converter.

Step 2 Select **Maintenance** > **Import/Export**.

Figure 7-3 Import or export



Includes system running logs and operation logs.

Includes the device list, event code list, and information on parameters that were configured such as direct connection, cloud connection, CMS, and message forwarding.

Step 3 Click **Export** next to **System Logs**.

7.4 Importing and Exporting Configuration Data

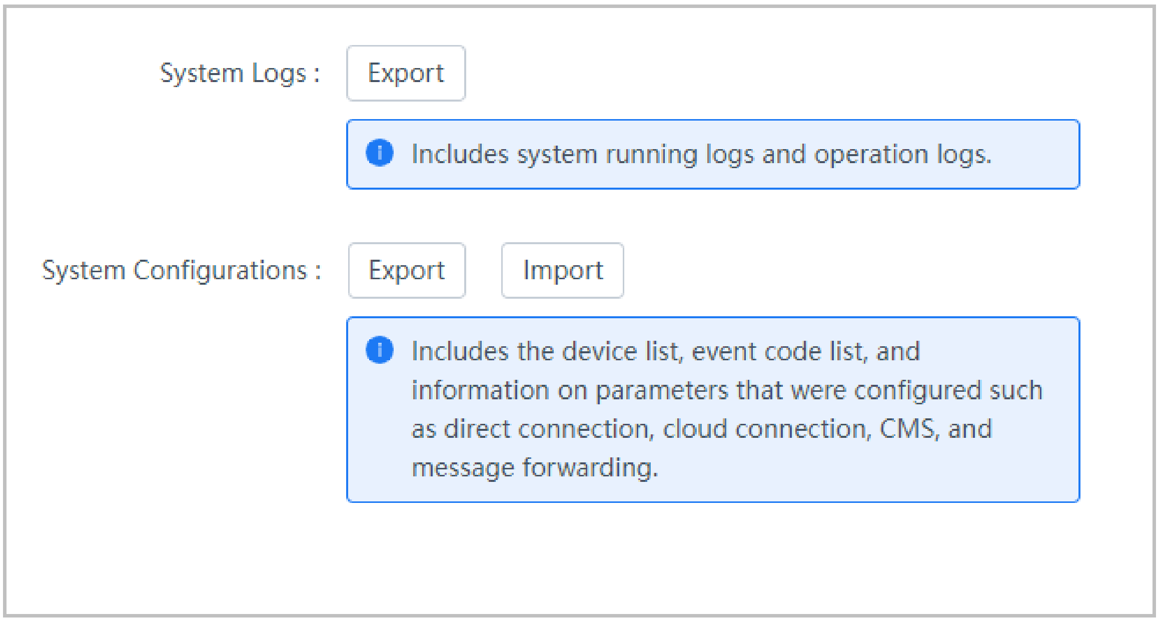
Import or export the system data into the Converter.

Procedure

Step 1 Log in to the webpage of the Converter.

Step 2 Select **Maintenance** > **Import/Export**.

Figure 7-4 Import or export



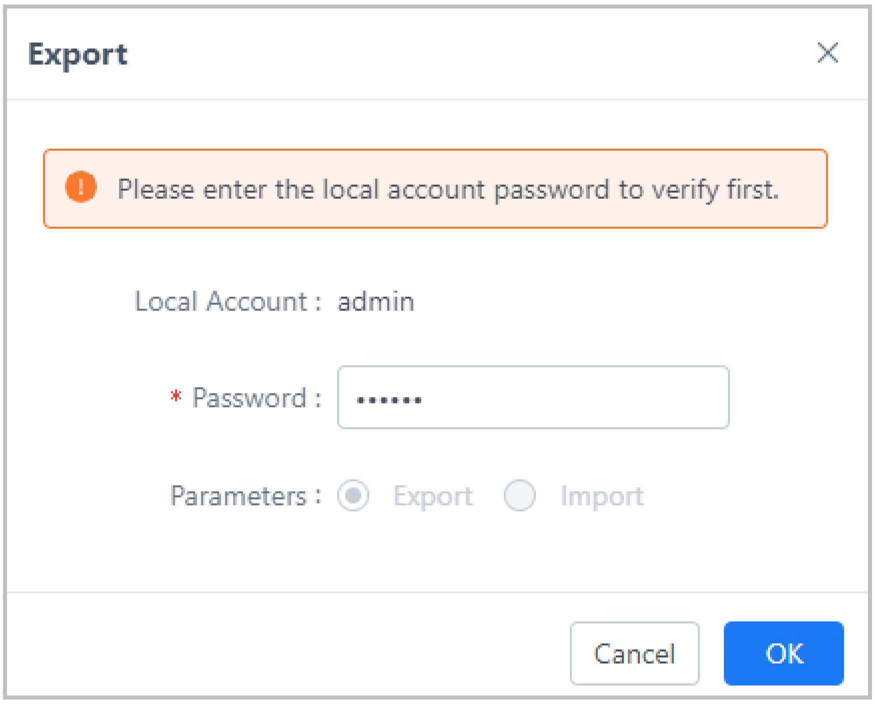
Includes system running logs and operation logs.

Includes the device list, event code list, and information on parameters that were configured such as direct connection, cloud connection, CMS, and message forwarding.

Step 3 Export system configuration.

1. Click **Export**, and then enter the password of the Converter account that you currently log in to.
2. Click **OK**.

Figure 7-5 Export



Export

Please enter the local account password to verify first.

Local Account : admin

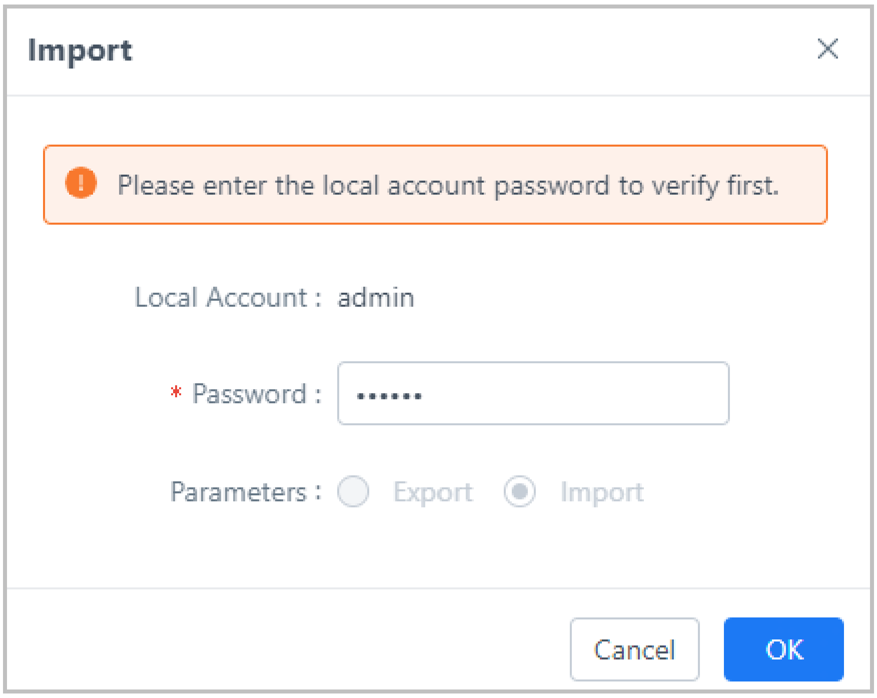
* Password : ••••••

Parameters : ● Export ○ Import

Step 4 Import system configuration.

1. Click **Import**, and then enter the password of the Converter account that you currently log in to.
2. Click **OK**.

Figure 7-6 Import (2)



Import

Please enter the local account password to verify first.

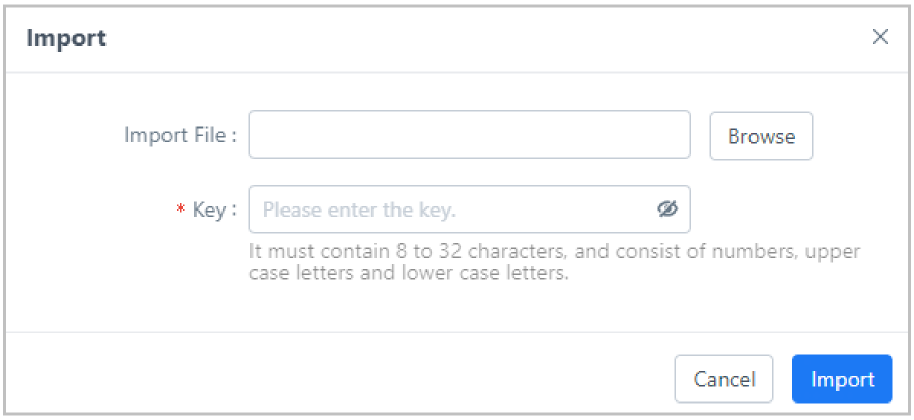
Local Account : admin

* Password : ••••••

Parameters : ○ Export ● Import

3. Click **Browse** to select the import file, and then enter the key.
4. Click **Import**.

Figure 7-7 Import(2)



Import

Import File :

* Key : Please enter the key.

It must contain 8 to 32 characters, and consist of numbers, upper case letters and lower case letters.

8 Viewing Message Notifications

View message notifications.

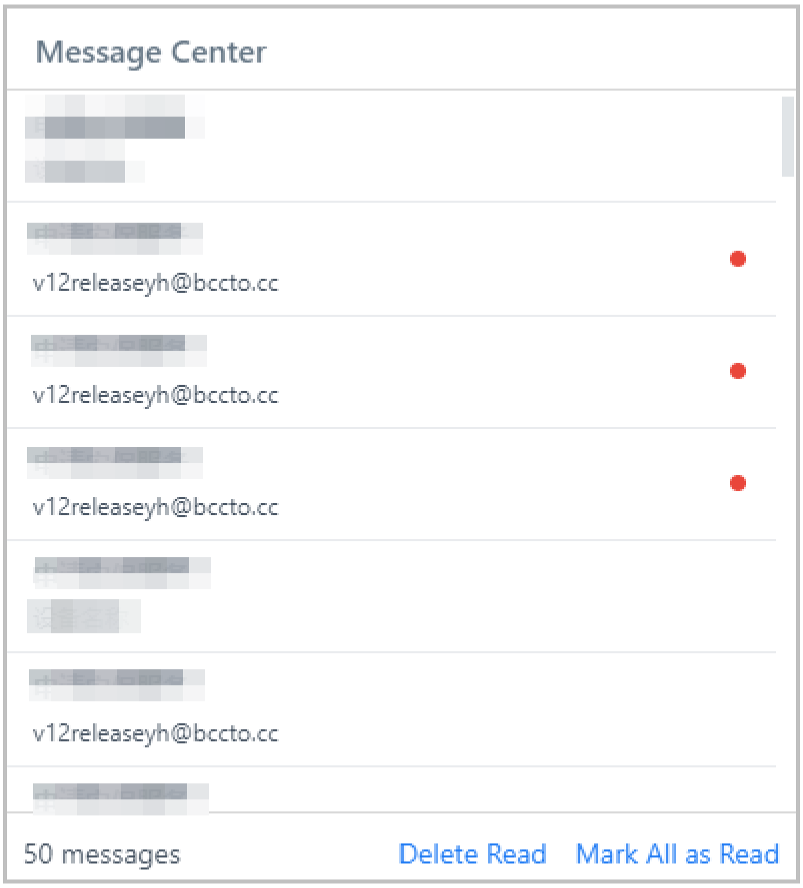
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Messages** at the top-right corner of the page.

Step 3 View messages notifications.

Figure 8-1 Message center



Message Center

v12releaseyh@bccto.cc ●

v12releaseyh@bccto.cc ●

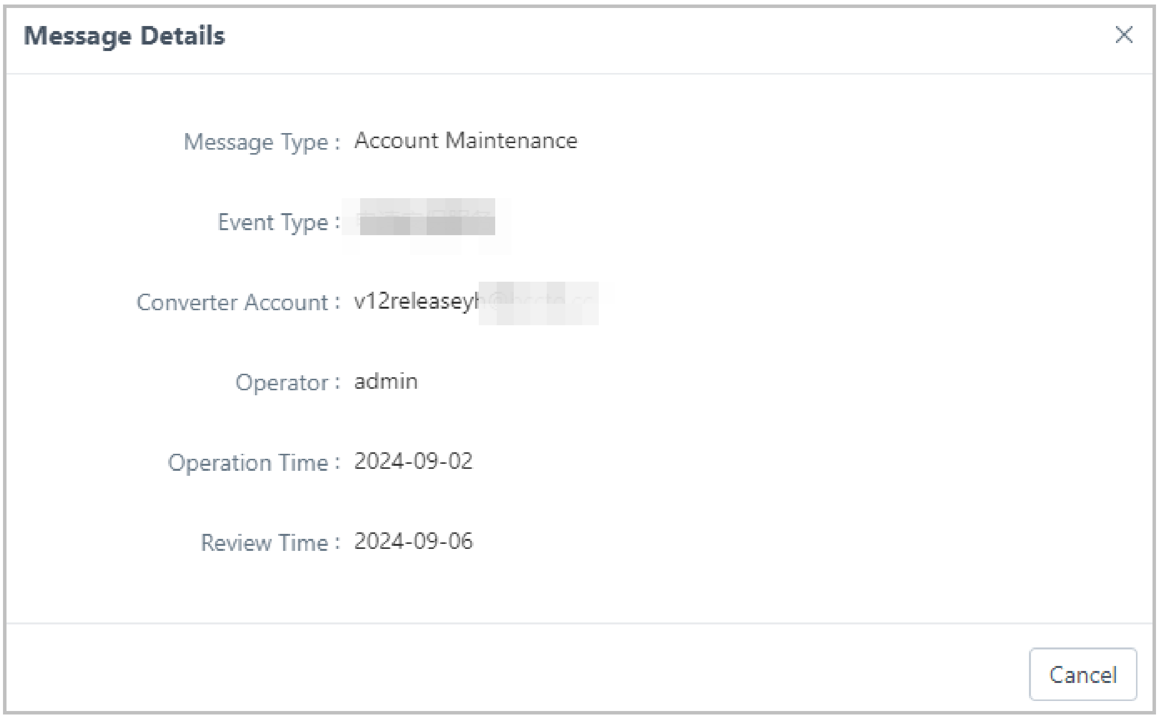
v12releaseyh@bccto.cc ●

v12releaseyh@bccto.cc

50 messages

Step 4 Click the notification to view message details.

Figure 8-2 Message details



Message Type : Account Maintenance

Event Type : [redacted]

Converter Account : v12releasey[redacted]

Operator : admin

Operation Time : 2024-09-02

Review Time : 2024-09-06

Related Operations

- Click **Delete Read** to delete read messages.
- Click **Mark All as Read** to mark unread messages as read.

9 Account Settings

9.1 Changing Account Password

Log in to the webpage of Converter, and select **Account** > **Change Password** to reset the password for the account.

9.2 Configuring Auto Logout Time

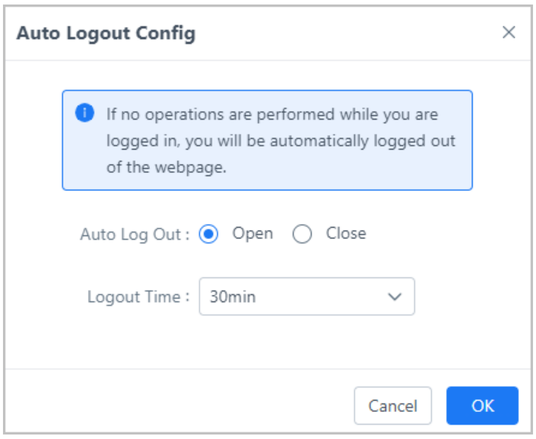
Procedure

Step 1 Log in to the webpage of Converter.

Step 2 Select **Account** > **Auto Logout Config**.

Step 3 Select **Open** to enable the auto log out function, and then select the logout time.

Figure 9-1 Auto logout



Auto Logout Config

If no operations are performed while you are logged in, you will be automatically logged out of the webpage.

Auto Log Out : ● Open ○ Close

Logout Time : 30min

Step 4 Click **OK**.

9.3 Logging Out

Log in to the webpage of Converter, and select **Account** > **Log Out**.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

Account Management

1. **Use Strong 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. **Change Password Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Assign Accounts and Permissions Reasonably**

   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.
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. **Set and Update Passwords Reset Information Timely**

   The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.
6. **Enable Account Binding IP/MAC**

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

Service Configuration

1. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
2. **Disable Unnecessary Services and Choose Secure Modes**

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

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

   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.

Network Configuration

1. **Enable Firewall Allowlist**

   We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.
2. **Network Isolation**

   The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

Security Auditing

1. **Check Online Users**

   It is recommended to check online users irregularly to identify whether there are illegal users logging in.
2. **View the Platform Log**

   By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. For example, place the device 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.

Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188