



# Converter Tool

## User's Manual








# 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
V1.2.0	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

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Overview.....	1
2 Installing and Initializing Converter.....	2
2.1 Installing Converter.....	2
2.2 Initializing Converter.....	5
2.3 Logging in to Converter.....	6
3 Basic Operation.....	7
3.1 Converter Settings.....	7
3.1.1 Configuring CMS Connection.....	7
3.1.2 Configuring Network.....	11
3.1.3 Configuring Message Forwarding.....	12
3.2 Hub Setting.....	13
3.2.1 Adding Hub .....	13
3.2.2 Configuring Hub Status.....	27
3.3 Configuring Event Code.....	29
3.4 Viewing Logs.....	30
3.4.1 Viewing Event Logs.....	30
3.4.2 Viewing Operation Logs.....	31
4 Maintenance.....	32
4.1 Exporting System Logs.....	32
4.2 Importing and Exporting Configuration Data.....	32
5 Account Settings.....	34
5.1 Changing Account Password.....	34
5.2 Configuring Auto Logout Time.....	34
5.3 Logging Out.....	34
Appendix 1 Performance Requirement.....	35
Appendix 2 Data Migration.....	36
Appendix 3 Security Commitment and Recommendation.....	38

# 1 Product Overview

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

## 2 Installing and Initializing Converter

### 2.1 Installing Converter

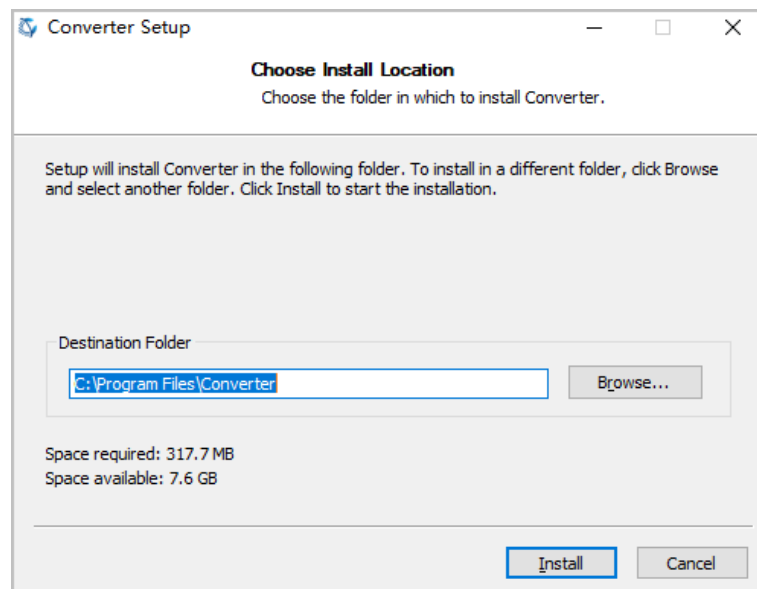
#### Prerequisites

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

#### Procedure

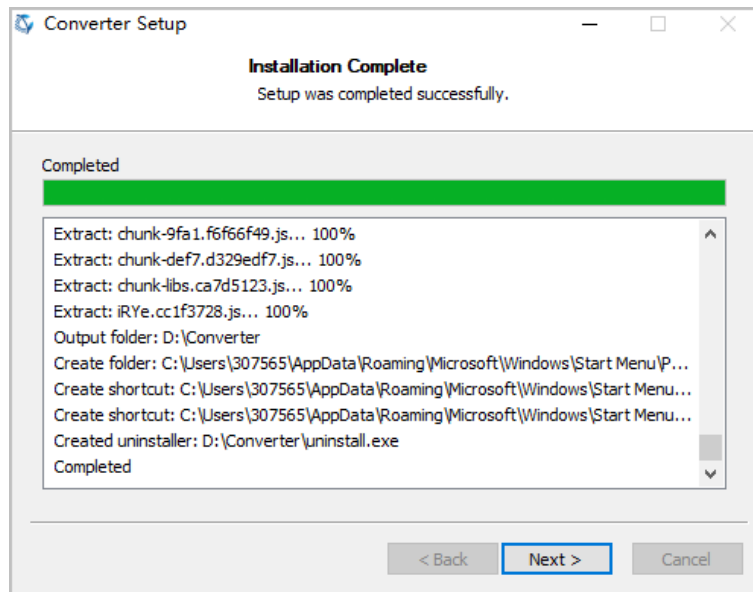
- Step 1 Right-click the install application to open the contextual menu, and then click **Run as administrator**.
- Step 2 Select the destination folder and then click **Install**.

Figure 2-1 Install(1)



- Step 3 Wait for the installation to be completed, and then click **Next**.

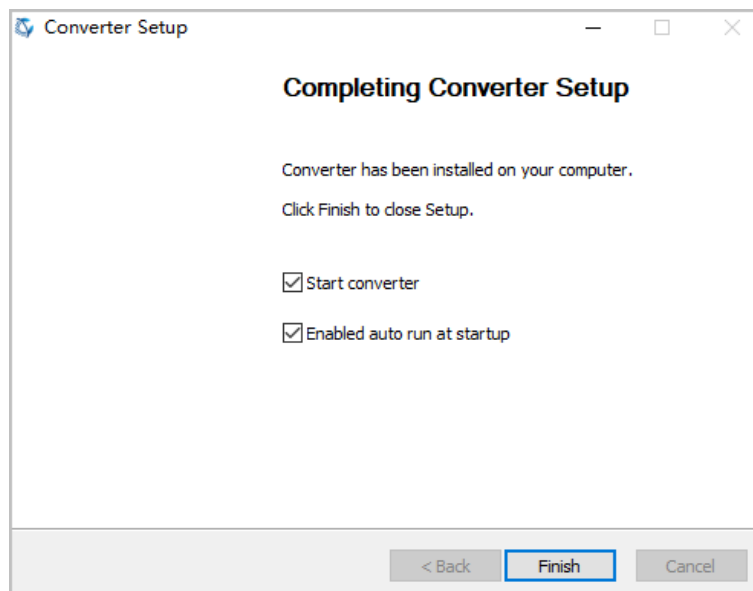
Figure 2-2 Install(2)



Step 4 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)



### Related Operations

- System Tray Setting


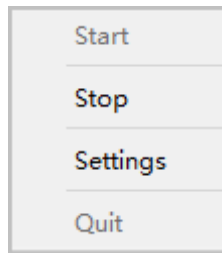
When the Converter is successfully installed and has been in operation, its icon  appears in the system tray. Right-click the icon to open the operation menu.

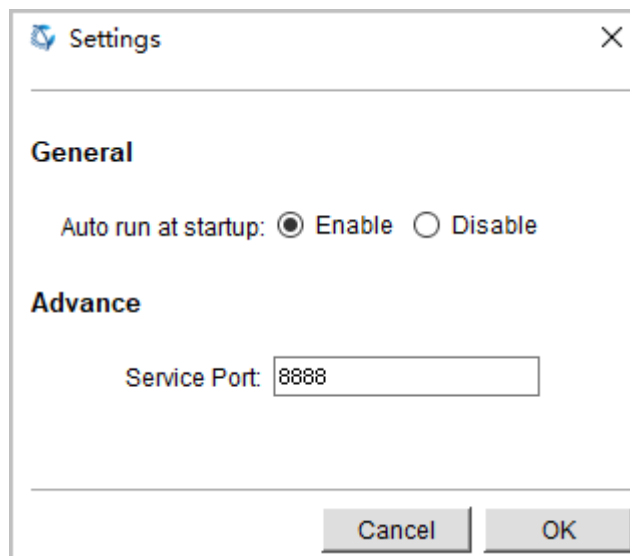


Figure 2-4 Menu



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

Figure 2-5 Settings



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

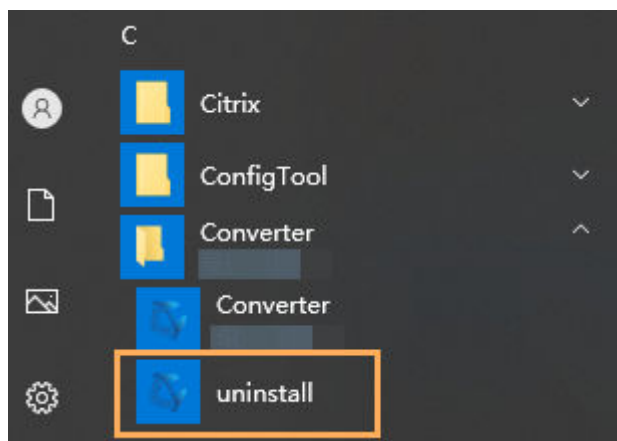


You need to click **Stop** and then **Quit** to exit the current program.

- 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.

## 2.2 Initializing Converter

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

### Procedure


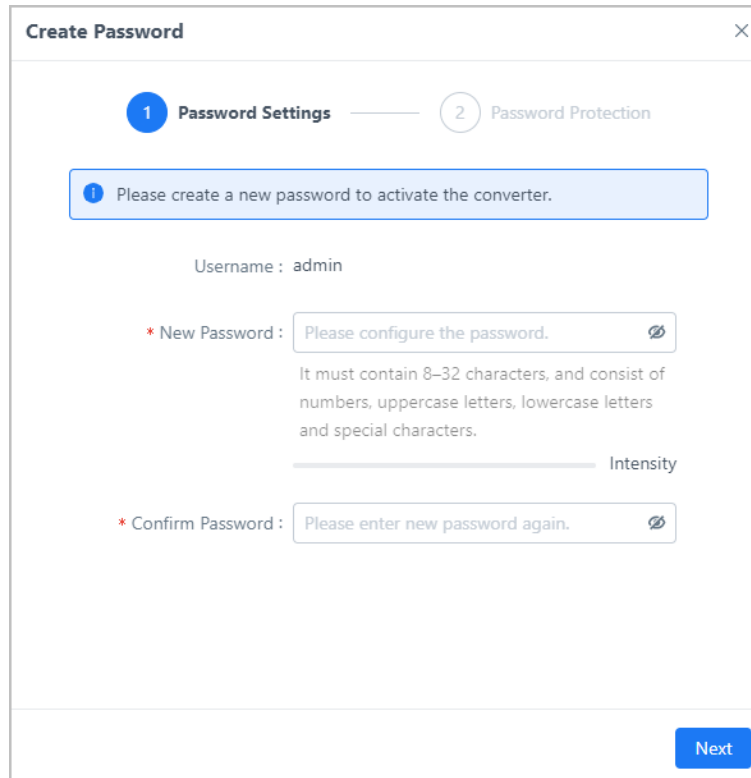
- Step 1 Double-click  to go to the webpage of Converter.
- Step 2 Configure the password for admin account, confirm it, and then click **Next**.  
The username is admin by default.

Figure 2-7 Create password



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

It will be automatically logged into the Converter after password configuration.

- Password protection questions are not required. Be cautious that you cannot recover the password if you do not configure questions.
- It is not required to take all of the 3 questions. You can pick one or more.
- You can click **Custom Question** in the question drop-down list to add custom questions if the default ones cannot meet your demand.

Figure 2-8 Configure password protection

**Create Password**

✓ Password Settings — 2 Password Protection

1 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 your dream job when you were... ▾

Answer : Please enter.

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

Answer : Please enter.

Previous OK

## 2.3 Logging in to Converter

### Procedure


- Step 1 Double-click  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**.

Figure 2-9 Login

**Converter**

admin

.....

I have read and agree to [User Agreement](#) and [Privacy Policy](#)

Login

[Forgot Password](#)

## 3 Basic Operation

### 3.1 Converter Settings

Configure CMS connection, network setting and message forwarding.

#### 3.1.1 Configuring CMS Connection

Establish a connection to CMS (Central Monitoring Station).

##### Procedure

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

Figure 3-1 CMS connection (Manitou)

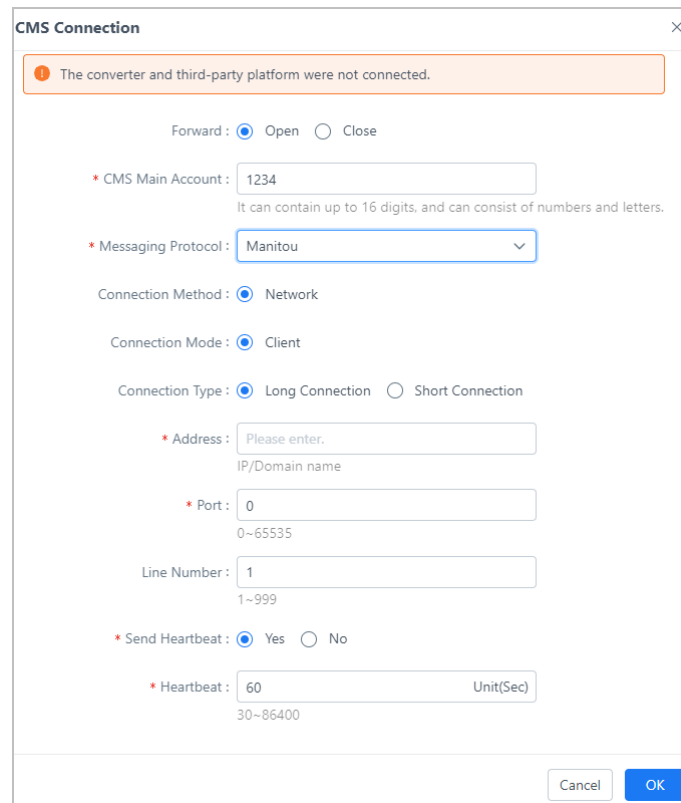


Figure 3-2 CMS connection (Surgard)

✕
CMS Connection

! The converter and third-party platform were not connected.

Forward :  Open  Close

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

\* Messaging Protocol :

\* Compatibility :

Connection Method :  Network  Serial Port

Connection Mode :  Client  Server

Connection Type :  Long Connection  Short Connection

\* Address :   
IP/Domain name

\* Port :   
0~65535

Receiver Number :   
It must have 2 digits.

Line Number :   
It must have 1 digits.

\* Send Heartbeat :  Yes  No

Figure 3-3 CMS(SIA)

✕
CMS Connection

! The converter and third-party platform were not connected.

Forward :  Open  Close

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

\* Messaging Protocol :

\* Data Format :

Connection Method :  Network

Connection Mode :  Client

Connection Type :  Long Connection  Short Connection

\* Address :   
IP/Domain name


\* Port :   
0~65535



CMS Encryption :

CMS Key :

Receiver Number :   Apply  
Hexadecimal, 0~FFFFFF

Table 3-1 Description of CMS connection parameter

Parameter		Description
Forward		Select <b>Open</b> to enable the forward function or <b>Close</b> to turn it off.
CMS Main Account		The account ID is assigned by the third-party platform to Converter, to support heartbeat interaction with the platform.
Messaging Protocol (SIA)	Data Format	Select <b>ContactID</b> or <b>DCS</b> .
	Connection Method	<b>Network</b> by default.
	Connection Mode	<b>Client</b> by default.
	Connection Type	<ul style="list-style-type: none"> <li>• <b>Long Connection</b> : The single TCP connection that is used to send and receive multiple TCP requests/responses.</li> <li>• <b>Short Connection</b> : During data transmission, a connection is established only when it is necessary to send data, and is disconnected after the service is completed.</li> </ul>
	Address	Enter the CMS address IP.
	Port	Enter the CMS port number.
	CMS Encryption	Select <b>None</b> or <b>AES</b> .It is <b>None</b> by default.
	CMS Key	32 characters, with each character being a hexadecimal digit.
	Receiver Number	Hexadecimal, 0–FFFFFF
	Line Number	
Messaging Protocol (Manitou)	Connection Method	<b>Network</b> by default.
	Connection Mode	<b>Client</b> by default.
	Address	Enter the CMS address IP.
	Port	Enter the CMS port number.
	Line Number	1-999.
Messaging Protocol (Surgard)	Compatibility	Select <b>MLR2</b> or <b>MLR2000</b> .  The actual selection of the compatibility depends on the third-party platform.
	Connection Method (Network)	Connection Mode: Select <b>Client</b> or <b>Server</b> .

Parameter		Description
		Connection Type: <ul style="list-style-type: none"> <li>● <b>Long Connection</b> : The single TCP connection that is used to send and receive multiple TCP requests/responses.</li> <li>● <b>Short Connection</b> : During data transmission, a connection is established only when it is necessary to send data, and is disconnected after the service is completed.</li> </ul>
		Address: Enter the CMS address IP.
		Port: Enter the CMS port number.
	Connection Method (Serial Port)	COM Number: Select the serial port number that the local computer (where the Converter is installed on) establish connection with third-party platform.
		Baud Rate: The unit of measurement of symbol rate that determines the speed of communication over data. The higher the rate is, the faster the communication.
		Data Bits: The number of bits used to represent one character of data. You can select from <b>5</b> , <b>6,7</b> and <b>8</b> . For example, if you select <b>8</b> , then it means the serial communication can transfer a total of eight bits that valued 0 or 1. 
		Most forms of data requires eight bits.
		Stop Bits: A bit(s) that marks the end of a unit of transmission. You can select from <b>1</b> , <b>1.5</b> and <b>2</b> . 
		The greater the number of stop bits, the more tolerance for synchronization. But the data transmission rate is slower.
		Parity: A parity error check method that is used to verify the accuracy of serial communication. <ul style="list-style-type: none"> <li>● <b>None</b> : No parity bit.</li> <li>● <b>Odd</b> : 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.</li> <li>● <b>Even</b> : 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.</li> <li>● <b>Mark</b> : The parity bit is 1.</li> <li>● <b>Space</b> : The parity bit is 0.</li> </ul>
Receiver Number	It must have 2 digits.	

Parameter		Description
	Line Number	It must have 3 digits when selecting <b>MLR2000</b> as compatibility, and 1 digit when <b>MLR2</b> .
Send Heartbeat		Select <b>Yes</b> if you need this function, or <b>No</b> to disable it.
Heartbeat		A regular interval sent between machines.
Listen for COM port heartbeat answers		If you select <b>Connection Method</b> as the <b>Serial Port</b> , you can enable the <b>Listen for COM port heartbeat answers</b> . It is enabled by default.

**Step 4** Click **OK**.

It displays the connection status as for whether Converter and the third-party platform is successfully connected at the top-center of the window.

### 3.1.2 Configuring Network

Configure the network status of the Converter.

#### Procedure

**Step 1** Log in to the webpage of Converter.

**Step 2** Select **Settings > Network Setting**.

**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 **Alarm Receive Central** 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 3-4 Preferred IP and Alternate IP

Preferred IP Address	
IP/Domain	Please enter
Port	0
Alternative IP Address	
IP/Domain	Please enter
Port	0



Figure 3-5 Network settings

**Network Settings**

\* UUID: [ ] - [ ] - [ ] - [ ] - [ ] [Default]  
32 hexadecimal character: 0-9, a-f

**Information:** 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 IP and Port** Listening Status ✔

\* IP Address: [ ]

\* Port: 9500

**Secondary IP and Port** Listening Status ✘

Enable:  Open  Close

\* IP Address: [ ]

\* Port: 0

Cancel OK

**Step 4** Click **OK**.

The listening status will be updated.

### 3.1.3 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 **Settings > Message Forwarding Config**.

**Step 3** Select the forwarding configuration that you need.

- **Event Type:** Select the event type for forwarding.
- **Video Switch:** Select **Open** to forward the video or images of the event, or **Close** to disable forwarding.

Figure 3-6 Message forward configuration

**Message Forwarding Config**

\* Event Type:  Alarm  Arming/Disarming  Operation  Fault

\* Video Switch:  Open  Close

Cancel OK

**Step 4** Click **OK**.

## 3.2 Hub Setting

Add the hub and modify hub status.

### 3.2.1 Adding Hub

Add the alarm hub to Converter.

#### Prerequisites

Make sure that you have installed DoLynk Care app or DMSS app if you want to use auto registration and cloud connection.

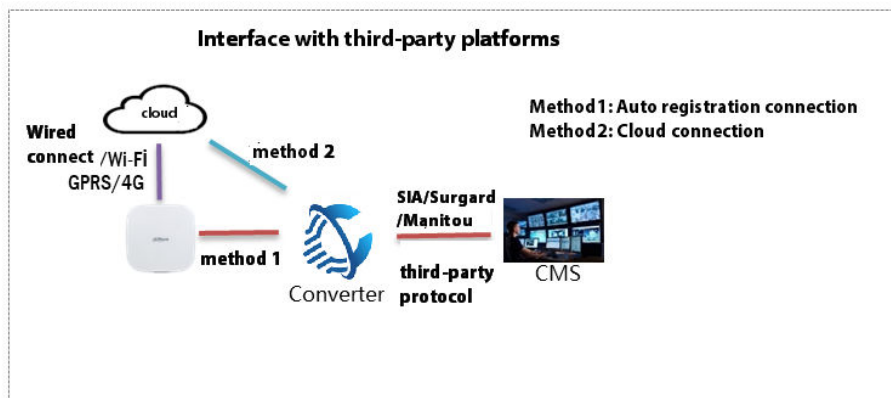


Both DoLynk Care and DMSS support cloud connection and auto registration. You can download any of them or both of them depending on your needs.

#### Background Information

- The hub can establish connection with Converter through either Dahua cloud or auto registration. The two methods can be used simultaneously. Converter would select one method as the primary link and the other as the alternate link depending on situation. You can also choose to use one of the two methods alone.
- If you want to connect through cloud access, make sure that you have configured the cloud access settings. See "3.2.1.2.1 Creating Cloud Account".

Figure 3-7 Hub connection method



#### 3.2.1.1 Auto Registration

You can add the hub to the Converter through auto registration.

#### Prerequisites

Make sure that you have configured network settings. See "3.1.2 Configuring Network".

#### Procedure

- Step 1** On your phone, tap to open the DMSS app or to open DoLynk Care.



The operation on DMSS or DoLynk Care is the same. Here uses DMSS as an example.

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

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

Figure 3-8 Configure IP address and port

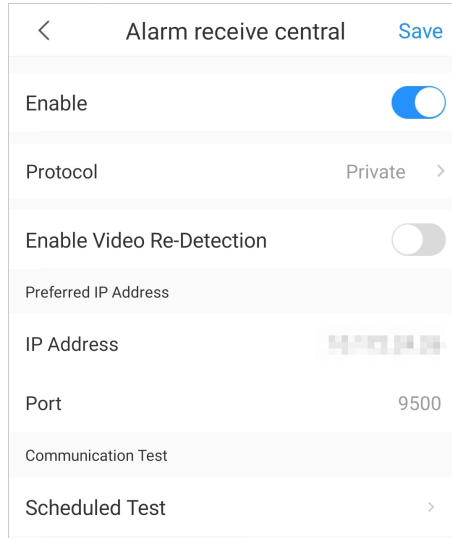
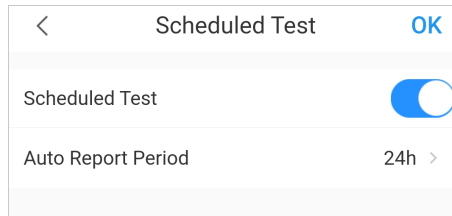


Figure 3-9 Auto report period



- The IP address and port number must be consistent with that you configured in "3.1.2 Configuring Network".
- You would better enable **Enable Video Re-Detection** if you have added IPC or PIR-Camera to the alarm hub and want to receive alarm messages with videos or pictures attached.
- Different alarm receiving centers of the same alarm hub cannot be set to connect to the same Converter.

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

Figure 3-10 Device list

No.	Device Name	SN	Device ID	Time Added Device	Cloud Connection Status	Direct Connection Status	Activate Status	Action
1	shiy	qqq28		2023-03-27 20:44:24	--	Online	Not Activated	
2	1234567890	7X01F6BPAJ00615	9990	2023-03-27 20:44:24	Online	Offline(Network connection I	Activated	
3	00824	qianjing	0099	2023-03-27 20:44:24	--	Online	Activated	

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

Figure 3-11 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		7K01F68PAJ00815		172.24.10...	--	--	Add
4	1234567890	7K01F68PAJ00815	2023-03-28 10:52:33		--	Online	Add

Figure 3-12 Add device

**Add**

\* Username : admin

\* Password : .....

Cancel OK



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, username 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.

Figure 3-13 Edit

**Edit**

\* Device ID : 1235

\* Username : admin

\* Password : .....

Cancel OK

### 3.2.1.2 Cloud Connection

You can add the hub to Converter through cloud connection.

#### Prerequisites

- Make sure that you have added hub to Dolyнк 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 "3.2.1.2.1 Creating Cloud Account".

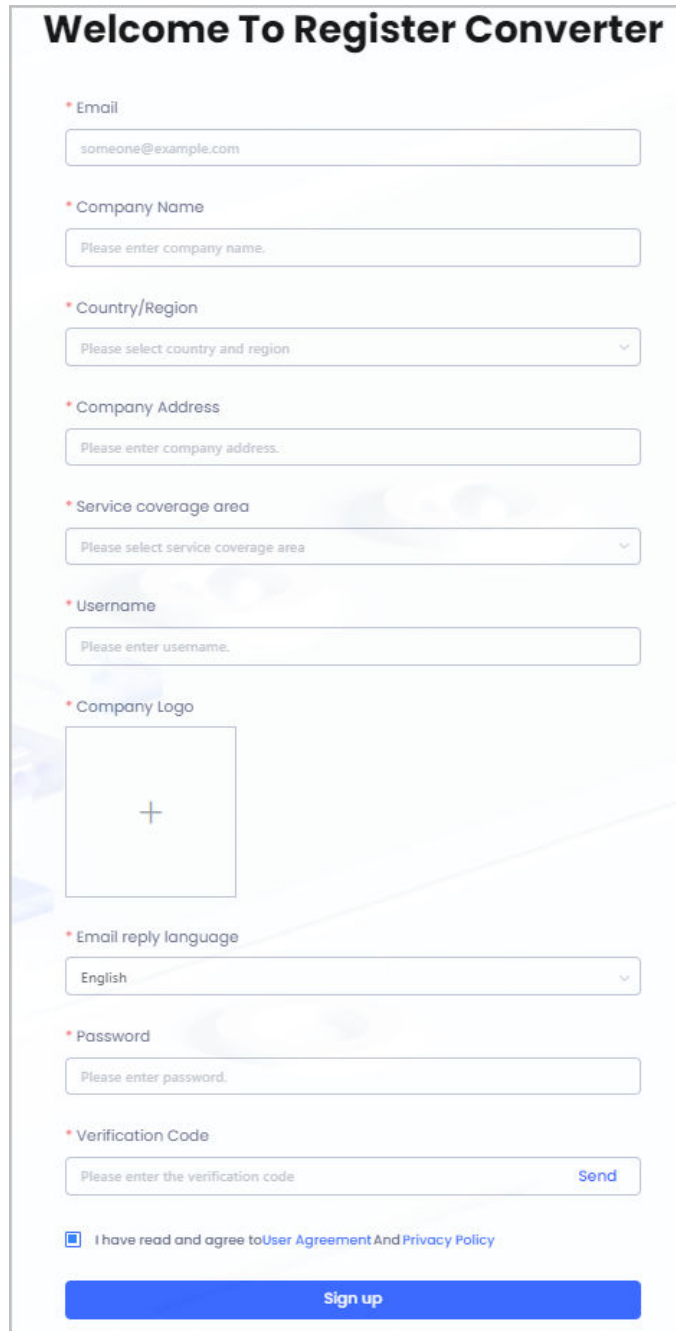
#### 3.2.1.2.1 Creating Cloud Account

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 Access**, and then click **Create Cloud Account**.
- Step 3 Enter the registration information.

Figure 3-14 Registration



**Welcome To Register Converter**

\* Email

\* Company Name

\* Country/Region

\* Company Address

\* Service coverage area

\* Username

\* Company Logo

\* Email reply language

\* Password

\* Verification Code

I have read and agree to [User Agreement And Privacy Policy](#)

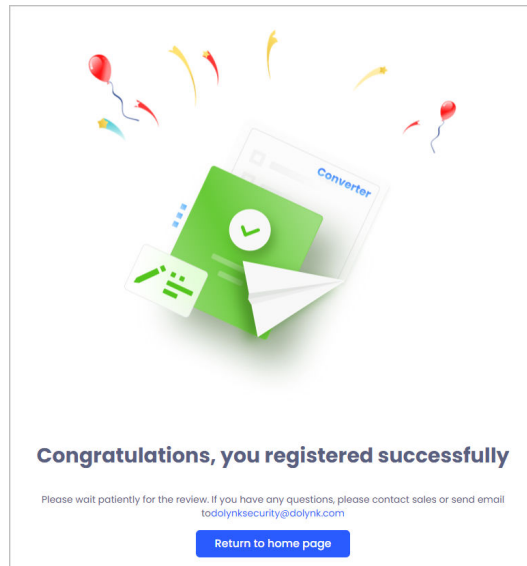
**Step 4** Click **Send** and the verification will be sent to the email address that is filled in the registration page in few minutes. Enter the received code in the check box.

**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 3-15 Registration succeed



### Related Operations

Click **Forgot Password** on the Log-in page to reset the password.

1. Enter the email address.
2. Click **Get** to obtain the verification code sent to your email inbox, and then enter the received code in the check box.
3. Enter the new password and confirm it, and then click **OK**.

Figure 3-16 Forget password

**Forgot Password** ×

\* Cloud Account :

\* Verification Code :

\* New Password :

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

\* Confirm Password :

### 3.2.1.2.2 Configuring Cloud Access

You need to configure cloud access if you want to add devices through cloud access.

#### Procedure

- Step 1 Log in to the webpage of Converter.
- Step 2 Select **Cloud Access**.
- Step 3 Select **Enable** to enable the cloud access function.

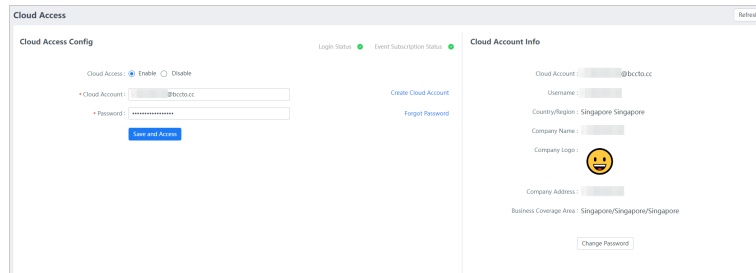


- **Disable** is selected by default.
- You need to select **Enable** if you want to add devices through cloud access. Otherwise, keep it by default.

**Step 4** Enter the username and password of the cloud account, and then click **Save and Access**.

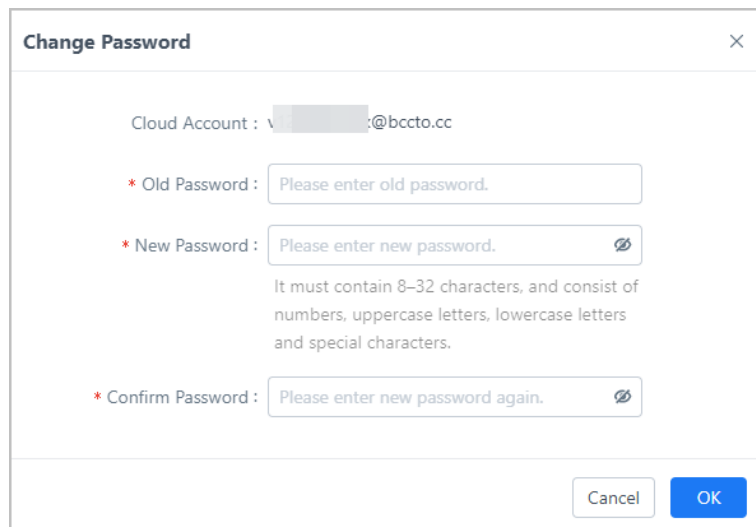
**Step 5** Click **Refresh** to update the webpage, and then the **Cloud Account Info** displays the account information.

Figure 3-17 Cloud access



**Step 6** (Optional) Click **Change Password** to change the password for the account, and then click **OK**.

Figure 3-18 Change password



### 3.2.1.2.3 Adding through DoLink Care

Add the hub through DoLink Care.

#### Procedure

**Step 1** On your phone, tap  to open the DoLink Care app.


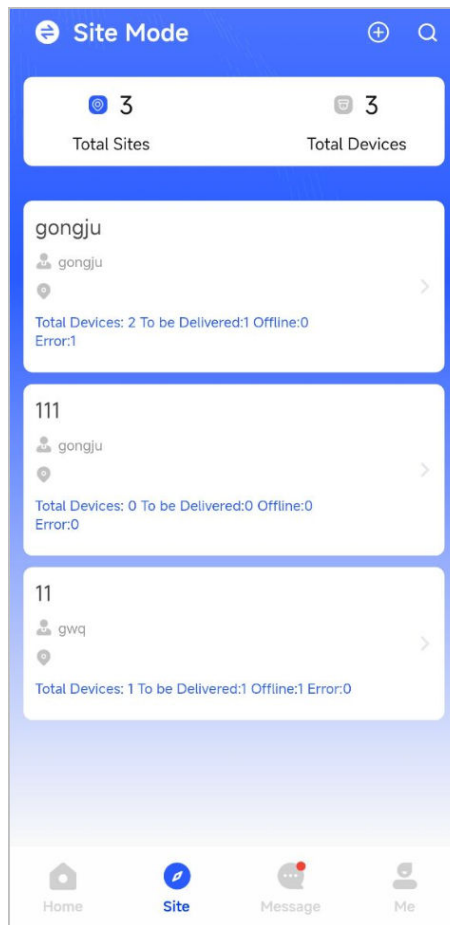
**Step 2** On the **Site** screen, tap  on the upper-left corner to switch to **Site Mode**.

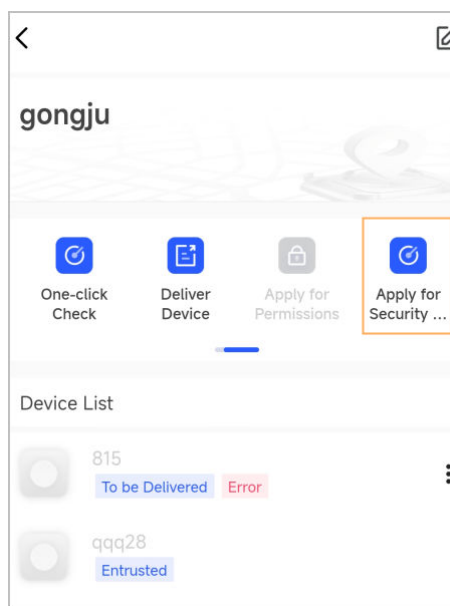


Figure 3-19 Site mode



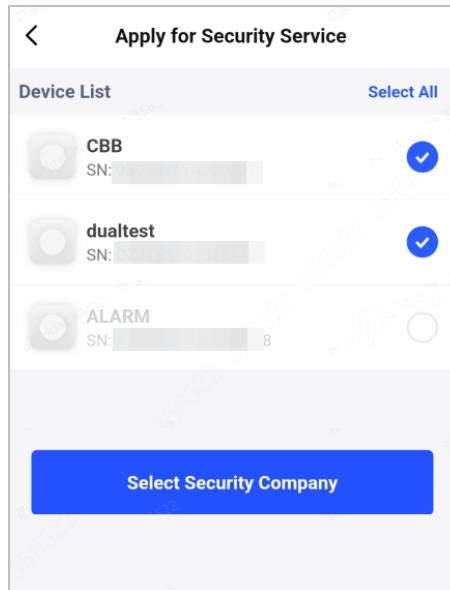
**Step 3** Tap a site on the **Site Mode** screen, and tap **Apply for Security Service** on the home screen of this site.

Figure 3-20 Apply for security service



**Step 4** Select the hub from the list, and tap **Select Security Company** to select a security company, and then tap **OK** to complete the binding process.

Figure 3-21 Select hub

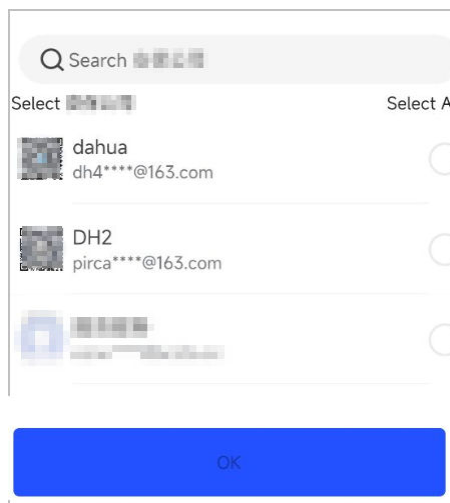


The screen displays **The application for security service was successful sent...** prompt to indicate that your binding is successful.



If you do not find the security company you want in the list, you can use fuzzy search to filter hubs on the list through entering keywords or account names, or you can search for accounts in all regions under the server through entering cloud accounts if the companies are not on the list.

Figure 3-22 Select security company




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

Figure 3-23 Companies Applied for

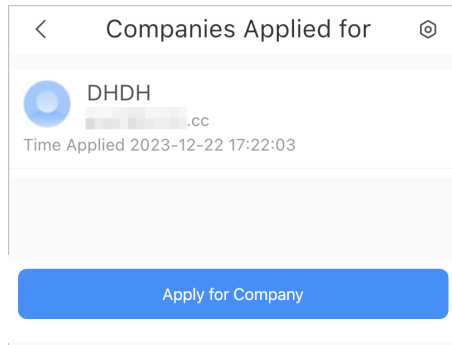
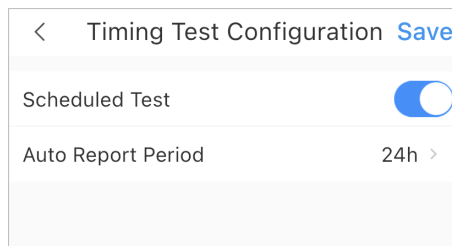
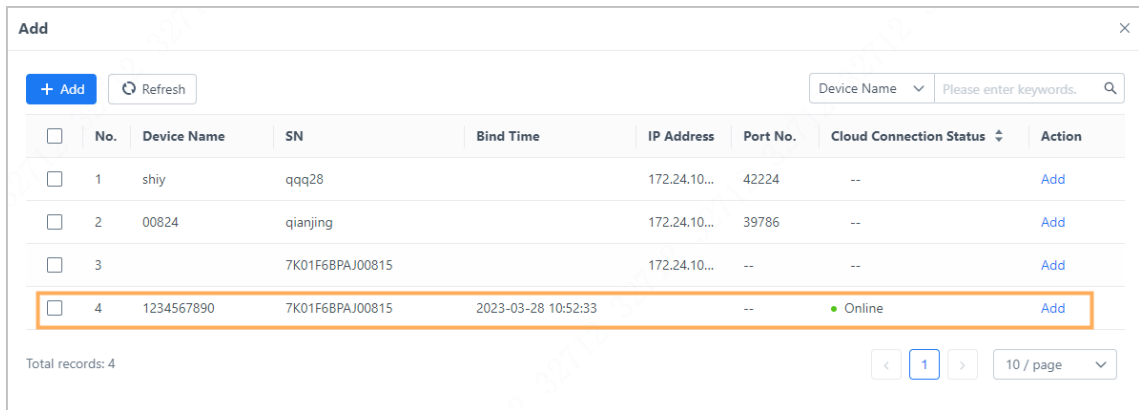


Figure 3-24 Auto report period



- Step 6** Log into the webpage of Converter.
- Step 7** On the **Device List** page of Converter, click **Add**.
- Step 8** Select the device you just configured, and then click **Add**.  
The page displays **Successfully added** prompt.

Figure 3-25 Cloud connection device

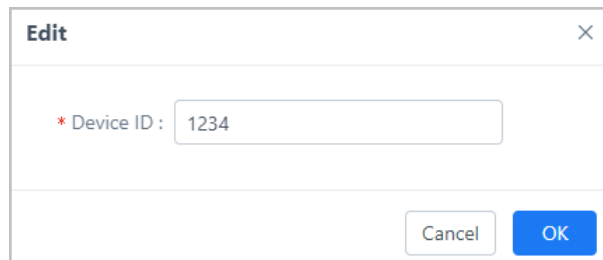


- Step 9** On the **Device List** page, click of a device, enter the device ID (4 digits), and then click **OK**.



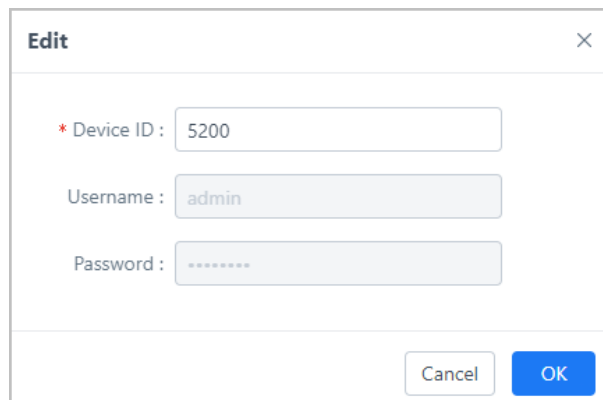
The device ID is the unique device identification code sent to the third-party alarm receiving center. It helps the alarm receiving center to determine which device sent the event.

Figure 3-26 Edit



If a device is added through two methods (both auto registration and cloud connection) simultaneously, and the auto registration works normally, then you just need to enter the device ID, and then click **OK**.

Figure 3-27 Edit (2)



### 3.2.1.2.4 Adding through DMSS

Add the hub through DMSS.

#### Procedure



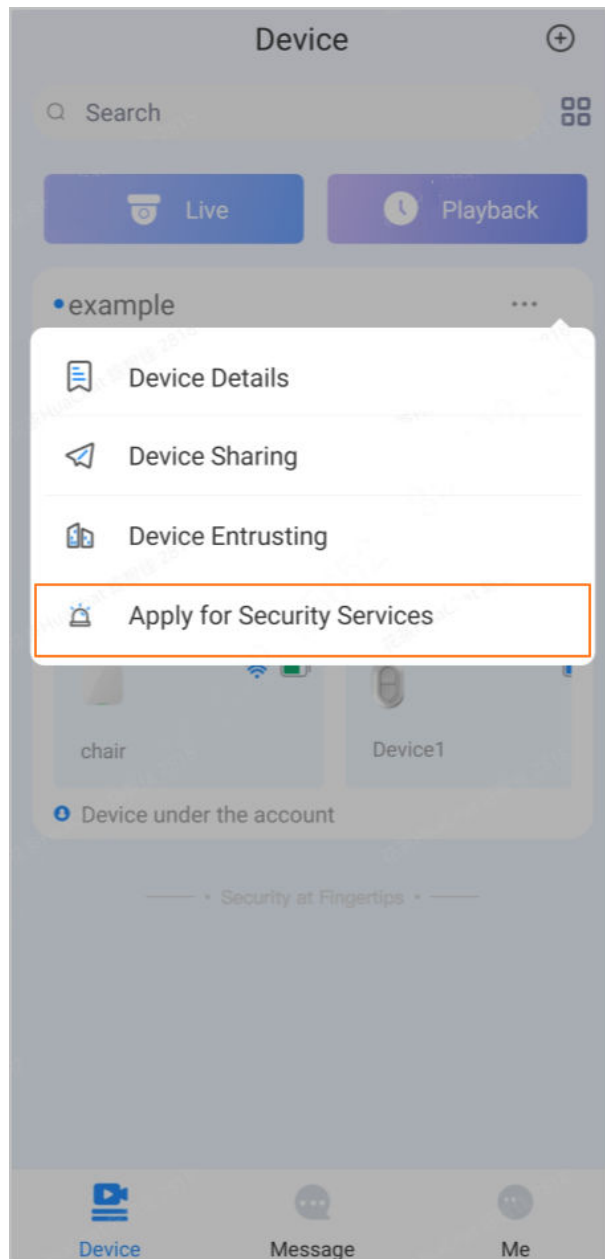
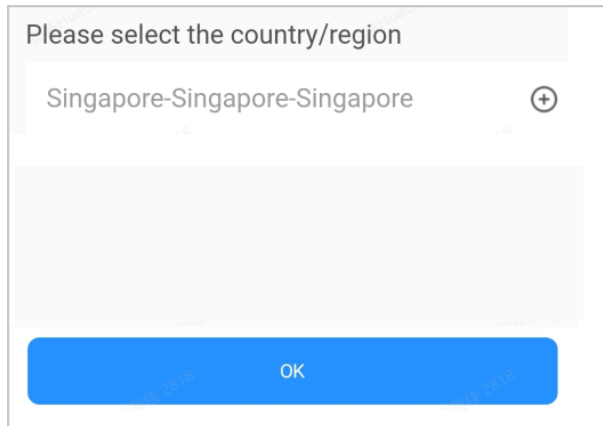
- Step 1 On your phone, tap  to open the DMSS app.
- Step 2 On the **Device** screen, tap  next to a device, and then tap **Apply for Security Services**.

Figure 3-28 Apply for security services



**Step 3** Select the country or region, and then tap **OK**.

Figure 3-29 Select country or region



**Step 4** Select a cloud account under the country or region you select, and then tap **OK** 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 3-30 Select account

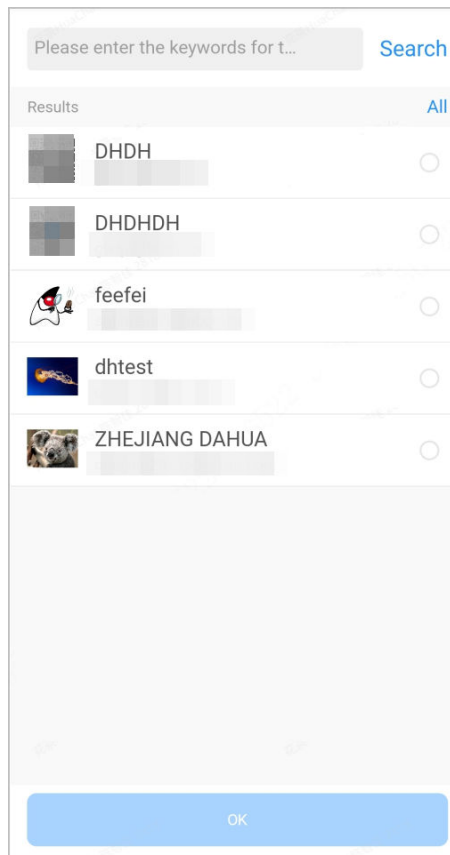
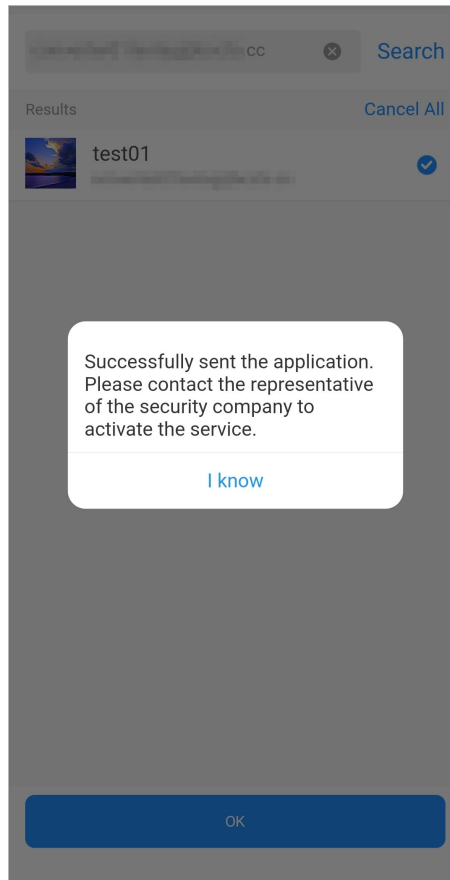


Figure 3-31 Bind by searching



Step 5 Repeat Step 6 to Step 9 to finish the settings.


Step 6 On the **Companies Applied for** screen, tap , and enable **Scheduled Test** and select the auto report period, and then tap **OK**.

Figure 3-32 Companies Applied for

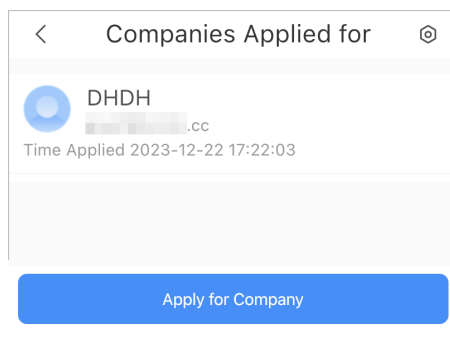
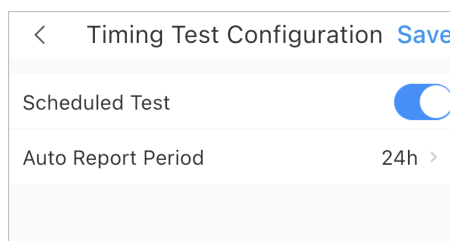


Figure 3-33 Auto report period



## 3.2.2 Configuring Hub Status

### 3.2.2.1 Deleting Hub

#### Procedure

- Step 1 Log in to the webpage of Converter.
- Step 2 On the **Device List** page, click **Delete**.
- Step 3 Enter the password of the Converter admin account, and click **OK** to delete the chosen devices.

Figure 3-34 Deleting confirmation

The dialog box titled "Delete" contains a message: "Please enter the username and password for verification in order to perform operations." Below the message, it shows "Converter Username : admin" and a password field with the placeholder "Please enter password." There are "Cancel" and "OK" buttons at the bottom right.

### 3.2.2.2 Activating Hub

#### Procedure

- Step 1 Log in to the webpage of Converter.
- Step 2 Select **Device List**.
- Step 3 Click next to an individual piece of hub, or **Activate** on the top left corner of the page to activate the chosen device(s).

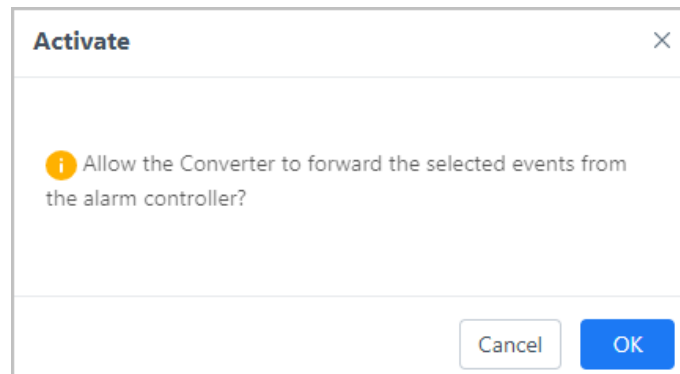
Figure 3-35 Activation page

No.	Device Name	SN	Device ID	Time Added Device	Cloud Connection Status	Direct Connection Status	Activate Status	Action
1	shly	qqq28		2023-03-27 20:44:24	--	Online	Not Activated	
2	1234567890	7K01F6BPAJ00815	9990	2023-03-27 20:44:24	Online	Offline(Network connection)	Activated	
3	00824	qianjing	0099	2023-03-27 20:44:24	--	Online	Activated	

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



Figure 3-36 Activate the device



### 3.2.2.3 Unbinding Hub

#### Background Information

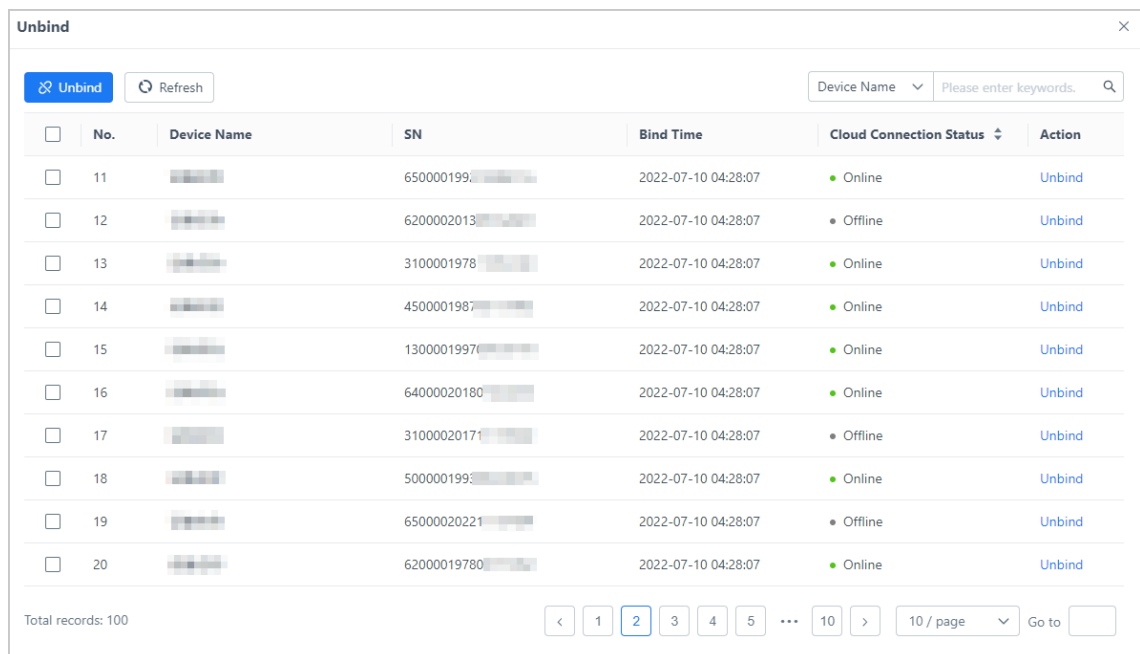
- It only applies to devices that is added to Converter through cloud connection.
- The device cannot be added by Converter after unbinding. You need to re-apply security services on Dolyink Care or DMSS.

#### Procedure


**Step 1** Log in to the webpage of Converter.

**Step 2** On the **Device List** page, click  to enter the **Unbind** page.

Figure 3-37 Enter unbind page



**Step 3** Click **Unbind** next to the individual piece of hub, enter the password of the Converter account, and click **OK** to unbind the chosen devices.

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

### 3.2.2.4 Refreshing Hub

#### Procedure

- Step 1 Log in to the webpage of Converter.
- Step 2 On the **Device List** page, click  to refresh the chosen devices.



When the device status in the device list changes, we recommended that you click **Refresh** to update the latest status. Otherwise, the device status might not be synchronized.

### 3.2.2.5 Disabling Hub

#### Procedure


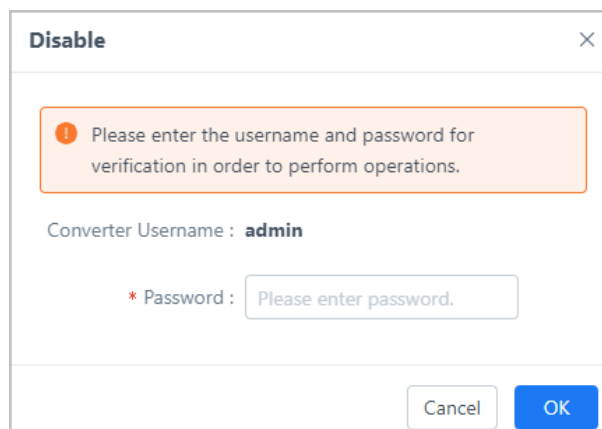
- Step 1 Log in to the webpage of Converter.
- Step 2 On the **Device List** page, click .
- Step 3 Enter the password of Converter account, and click **OK** to disable the chosen devices.

Figure 3-38 Disabling confirmation



## 3.3 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 Code**.
- Step 3 Click **Add** to add new event.
- Step 4 Configure the parameters.

Figure 3-39 Event code

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.

## 3.4 Viewing Logs

### 3.4.1 Viewing Event Logs

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 **Log List** > **Event Logs** to view the event logs.

- **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 3-40 Log list

**Log List**

Device ID:  Original Code:  Event Time:  ~

No.	Device Name	Device ID	Event Name	Original Code	Event Code	Event Time	Time Sent Mes...	With Image/Wi...	Sending Status	Remarks	Action
1	cbb	1235	Connection lost	1355	XT	2023-12-21 14:4...	2023-12-21 14:4...	No	Successfully Sent		<a href="#">Details</a>
2	cbb	1235	Lid was opened	1137	TA	2023-12-21 14:4...	2023-12-21 14:4...	No	Successfully Sent		<a href="#">Details</a>
3	cbb	1235	Reactivated	3502	QU	2023-12-21 14:4...	2023-12-21 14:4...	No	Successfully Sent		<a href="#">Details</a>
4	cbb	1235	Temporarily dea...	1502	UB	2023-12-21 14:4...	2023-12-21 14:4...	No	Successfully Sent		<a href="#">Details</a>
5	cbb	1235	Lid was opened	1137	TA	2023-12-21 14:3...	2023-12-21 14:3...	No	Successfully Sent		<a href="#">Details</a>
6	cbb	1235	Reactivated	3502	QU	2023-12-21 14:3...	2023-12-21 14:3...	No	Successfully Sent		<a href="#">Details</a>

Total records: 17    Go to

**Step 3** 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.

## 3.4.2 Viewing Operation Logs

View logs of the operation on Converter.

### Procedure

- Step 1** Log in to the webpage of Converter.
- Step 2** Select **Log List** > **Operation Logs**.
- Step 3** Configure the operation time to view the operation logs.

Figure 3-41 Operation logs

**Operation Log**

Operation Time:  ~

No.	Username	Log Description	Operation Time	Action
1	admin	Login	2023-12-19 10:46:27	<a href="#">Details</a>
2	admin	CreateAccount	2023-12-19 10:46:27	<a href="#">Details</a>

Total records: 2

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

## 4 Maintenance

### 4.1 Exporting System Logs

Export the device list logs, event code list logs, CMS connection logs, operation logs, network setting logs and message forwarding logs in a zip format.

#### Procedure

- Step 1 Log in to the webpage of the Converter.
- Step 2 Select **Maintenance** > **Export System Logs** to download the system logs.

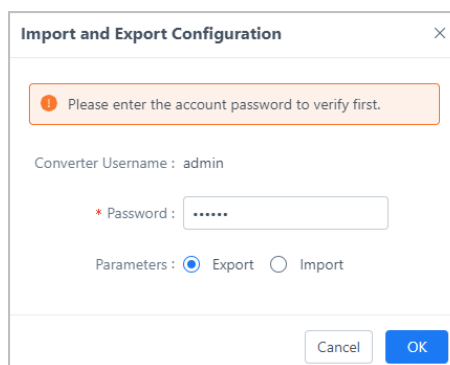
### 4.2 Importing and Exporting Configuration Data

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 and Export Configuration**.
- Step 3 Enter the password of the Converter account that you currently log in to, and select the **Parameter** as either **Export** or **Import**, and then click **OK**.

Figure 4-1 Import and export

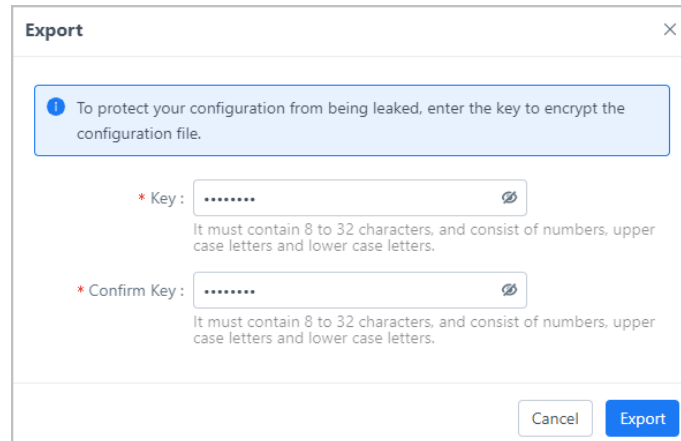


- Step 4 Configure the settings.
  - Export: Enter the password for exporting, and confirm it, and then click **Export**.
  - Import: Enter the same password for importing, and upload the file from local computer, and then click **Import**.



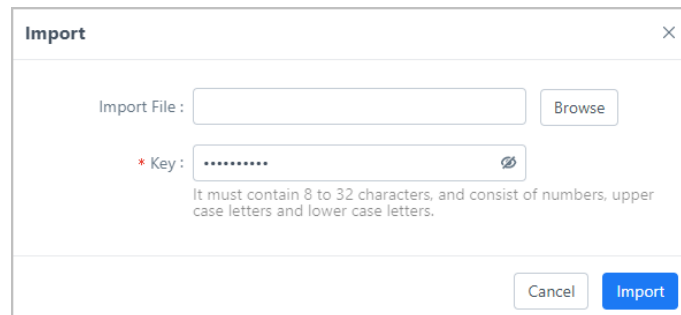
- The password can be the same as or different from the login password of the Converter admin account that you are currently use.
- The password for exporting or importing are the same.

Figure 4-2 Export



The 'Export' dialog box features a close button (X) in the top right corner. A blue information box at the top contains the text: 'To protect your configuration from being leaked, enter the key to encrypt the configuration file.' Below this, there are two password fields. The first is labeled '\* Key:' and the second is labeled '\* Confirm Key:'. Each field contains seven dots and a toggle icon. Below each field is a note: 'It must contain 8 to 32 characters, and consist of numbers, upper case letters and lower case letters.' At the bottom right, there are 'Cancel' and 'Export' buttons.

Figure 4-3 Import



The 'Import' dialog box features a close button (X) in the top right corner. It contains an 'Import File:' label followed by a text input field and a 'Browse' button. Below this is a password field labeled '\* Key:' with seven dots and a toggle icon. A note below the key field states: 'It must contain 8 to 32 characters, and consist of numbers, upper case letters and lower case letters.' At the bottom right, there are 'Cancel' and 'Import' buttons.

## 5 Account Settings

### 5.1 Changing Account Password

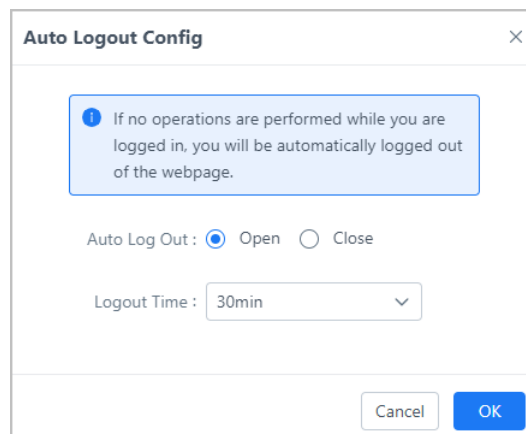
Log in to the webpage of Converter, and select **Account** > **Change Password** to reset the password for the account.

### 5.2 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 5-1 Auto logout



- Step 4 Click **OK**.

### 5.3 Logging Out

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

# Appendix 1 Performance Requirement

Appendix Table 1-1 Function specifications

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

Appendix Table 1-2 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	<ul style="list-style-type: none"> <li>● Windows 7 (64-bit)</li> <li>● Windows 10 (64-bit)</li> <li>● Windows 11_pro (64-bit)</li> <li>● Windows_Server_2012 (64-bit)</li> <li>● Windows_Server_2016 (64-bit)</li> <li>● Windows_Server_2019 (64-bit)</li> </ul>
Browser	<ul style="list-style-type: none"> <li>● Google Chrome 80 and later</li> <li>● Microsoft Edge 107 and later</li> </ul>



## Appendix 2 Data Migration

The datamigration.exe is used to transfer parameters configured in earlier versions of Converter to higher versions.

### Procedure

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

Appendix Figure 2-1 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		
<b>tool</b>	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

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

- Step 3** Double-click **datamigration** to run the program.

Appendix Figure 2-2 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		
<b>datamigration</b>	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.

Appendix Figure 2-3 Backup file

bin	2023/12/25 17:10		
data	2023/12/25 17:10		
etc	2023/12/25 19:21		
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		
<b>converter_backup_2023... .backup</b>	2023/12/25 17:10		21 KB
datamigration	2023/12/25 17:10		17,426 KB
converterLauncher.exe	2023/12/25 14:56		1 KB
uninstall.exe	2023/12/25 17:10		1 KB

Step 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.

## Appendix 3 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](http://www.dahuasecurity.com) | Postcode: 310053

Email: [dhoverseas@dhvisiontech.com](mailto:dhoverseas@dhvisiontech.com) | Tel: +86-571-87688888 28933188