

Access Control
Config Tool
(Windows version)
User's Manual

V1.0.3

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want

someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network






The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General

This user's manual (hereinafter referred to be "the Manual") introduces the functions and operations of the ACSConfig (hereinafter referred to be "the Tool").

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	July 8, 2016
2	V1.0.1	Delete "Installing and Uninstalling".	November 18, 2016
3	V1.0.2	Add "Initializing Devices", "Modifying Password" and "Resetting Password".	May 31, 2017
4	V1.0.3	1. Add "Privacy Protection Notice". 2. Update "About the Manual".	May 3, 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to:

providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

Cybersecurity Recommendations	I
Foreword	III
1 Overview	1
1.1 General	1
1.2 The Main User Interface	1
2 Basic Operations	3
2.1 Configuring the System Parameters	3
2.2 Adding Devices	3
2.2.1 Adding by Searching	4
2.2.2 Adding by Template	5
2.3 Initializing Devices	8
2.4 Modifying IP	10
2.4.1 Modifying One IP	10
2.4.2 Modifying IP in Batches	11
2.5 Configuring System Settings	12
2.5.1 Timing	12
2.5.2 Rebooting.....	13
2.5.3 Restoring.....	14
2.5.4 Modifying Password.....	16
2.5.5 Resetting Password.....	18
2.6 Upgrading Devices	24
2.6.1 Upgrading One Device	24
2.6.2 Upgrading Devices in Batches	24

1.1 General

The Tool configures and maintains the access control devices by providing the following operations:

- Modify device IP.
- Sync device time, reboot device, restore system default, modify and reset device password.
- Upgrade device.

1.2 The Main User Interface

For the main user interface of the Tool, see Figure 1-1, and for the details description, see Table 1-1.



- The Tool will search the devices according to the network segments setting in **Search setting** once it is launched.
- After the Tool is installed, the **Current Segment Search** check box is selected by default in the **Search setting** in the first launch.

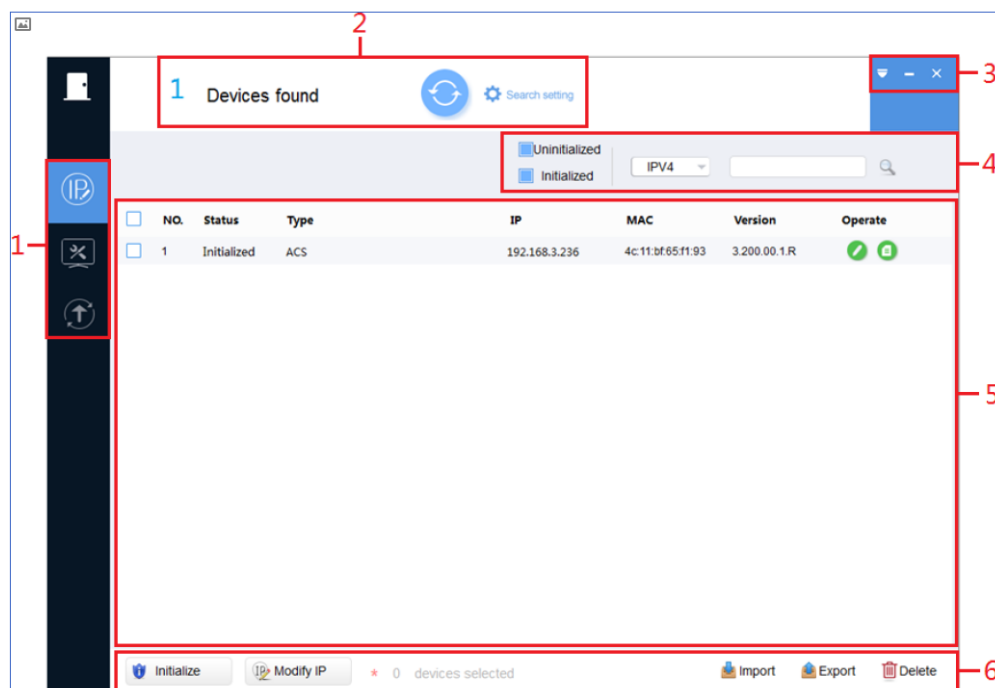


Figure 1-1








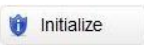
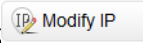




No.	Function	Description
1	Menu	<p>This function includes three tabs: Modify IP, Device Config, and Upgrade.</p> <ul style="list-style-type: none"> Modify IP ( to refresh the searched device list.
3	Help	<p>This function provides access to check the Help file and software version, set system parameters, minimize or exit the software.</p> <ul style="list-style-type: none"> Click  to check the Help file and software version, and set the alternate port for searching and update timing. Click  to minimize the software. Click  to exit the software.
4	Filtering	<p>This function provides filtering by selecting device type, initial status, and IP version (IPV4 or IPV6) to find the devices quickly.</p> <p>You can also manually enter the conditions such as device type, IP address, model, MAC address and version number to search the devices.</p>
5	Device list	<p>This function shows the searched devices and their information such as type, mode, IP, MAC and version.</p> <p>The Operate column provides the following functions:</p> <ul style="list-style-type: none"> Click  to modify device IP. Click  to view device details. <p> NOTE</p> <p>It is not supported to modify IP or view device details under IPV6.</p>
6	Function buttons	<p>You can operate the following functions:</p> <ul style="list-style-type: none"> Initialization: Select one device and click . Batch IP modification: Select devices and click . Device import: Click  Import to import one or multiple devices through template. Device details export: Select one or multiple devices and click . Device deleting from the list: Select one or multiple devices and click  Delete.

Table 1-1

2 Basic Operations

2.1 Configuring the System Parameters

Set the alternate port, update timeout and network timeout for searching devices.

Step 1 On the main user interface, click , and then select **Setting**.

The **Setting** dialog box is displayed. See Figure 2-1.

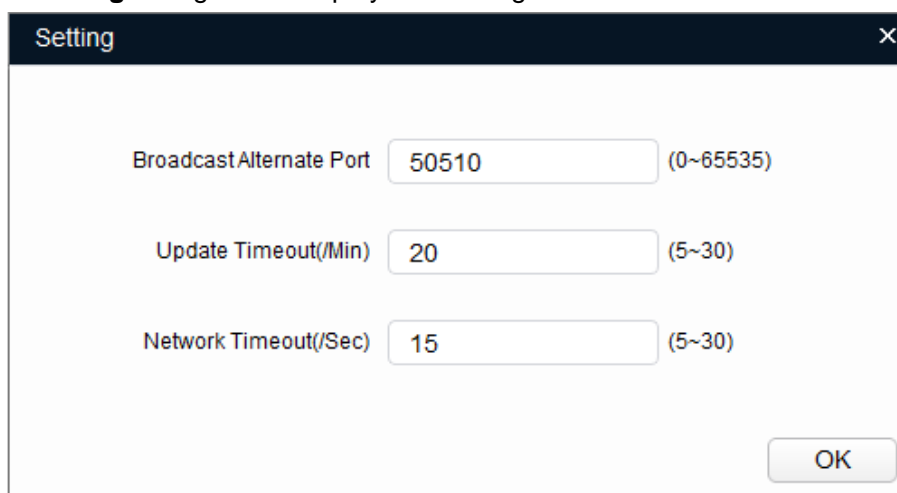
The image shows a 'Setting' dialog box with a dark title bar and a close button (X). It contains three configuration rows. The first row is 'Broadcast Alternate Port' with a text input field containing '50510' and a range '(0~65535)' to its right. The second row is 'Update Timeout(/Min)' with a text input field containing '20' and a range '(5~30)' to its right. The third row is 'Network Timeout(/Sec)' with a text input field containing '15' and a range '(5~30)' to its right. An 'OK' button is located at the bottom right of the dialog box.

Figure 2-1

Step 2 Set the system parameters. Refer to Table 2-1 for more information.

Parameter	Description
Broadcast Alternate Port	The alternate port for devices searching. If the default broadcast port cannot find the devices, the Tool will switch to the alternate port.
Update Timeout (/Min)	The maximum updating time for a single device. When the updating time is longer than the set value, the updating stops.
Network Timeout (/Sec)	The maximum time for network connecting during device updating. When the network connecting time is longer than the set value, the updating stops.

Table 2-1

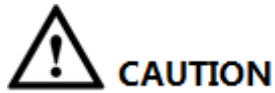
Step 3 Click **OK** to complete setting.

2.2 Adding Devices

You can add one or multiple devices depending on your actual situation.

- If you want to add the devices through searching within the current network segment, see "2.2.1 Adding by Searching."

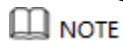
- If you have the template data of the device, add the devices through importing the template.
For details about how to add by template, see "2.2.2 Adding by Template."



Make sure the network is interworking between the device and the PC installed with the Tool; otherwise the Tool cannot find the device.

2.2.1 Adding by Searching

You can add devices by searching the current network segment. The system only supports searching the current network segment.



You can set the filtering conditions to search the wanted device quickly.

Step 1 Click  [Search setting](#).

The **Setting** screen is displayed. See Figure 2-2.

Figure 2-2

Step 2 Select the **Current Segment Search** check box, and enter the user name in the **Username** box and password in the **Password** box.



NOTE


The user name and the password are also used to login the device when you want to modify IP, configure the system and update the device.

Step 3 Click **OK** to start searching.

After the searching is completed, the searched devices appear in the device list.

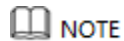


NOTE

- Click  to refresh the device list.
- The system saves the searching conditions when it exits the software and reuses the same conditions when the software is launched next time.

2.2.2 Adding by Template

You can quickly add the devices by using the template.



Make sure your PC is installed with Microsoft Excel.

2.2.2.1 Accessing to the Template

You can either manually fill in the template or export the device details file from the system.

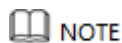
- For the details about how to fill in the template, see "Filling in the template."
- For the details about how to export the device details, see "Exporting the device details file."



- The template (DeviceTemplate.xls) must be opened and edited by Excel.
- If you want to delete the record in the template, right-click the record line, and then select **Delete**.

Filling in the Template

Step 1 Find the device template in the save path of the Tool and open it. See Figure 2-3.



The example in the template is for reference only.

	A	B	C	D	E	F	G	H	I	J
1	Type	Model	IP	Port	MAC	Serial No.	Version	Subnet Mask	Gateway	Initial Status
2	ACS	CAS-4MC	192.168.3.221	37777	4c:11:bf:4c:45:56	1L03699PAN02233	1.100.0.1	255.255.0.0	192.168.0.1	Initialized
3										
4										
5										
6										

Figure 2-3

Step 2 Enter the device parameters. Refer to Table 2-2 for more information.

Parameter	Description
Type	Mandatory. Device type, enter ACS.
Model	Optional. Device model.
IP	Mandatory. IP address of device.
Port	Mandatory. Port number of device.
MAC	Mandatory. Device MAC address that can be obtained from the device label.
Serial No.	Optional. Device serial number.
Version	Optional. Device version number.
Subnet Mask	Mandatory. Device subnet mask.
Gateway	Mandatory. Device gateway.
Initial Status	Mandatory. Device initialization status: Initialized or uninitialized.

Table 2-2

Step 3 Save and close the template.

Exporting the Device Details File

You can export the device details file and use it as a template to add or back up the device details.

Step 1 Click .

The **Modify IP** screen is displayed.

Step 2 Select the devices you want to export, and then click  **Export**.

The **Save As** dialog box is displayed.

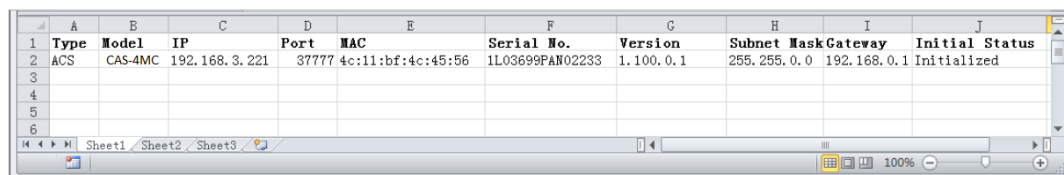
Step 3 Choose the save path, enter the file name such as Export Device in the **File name** box.

Step 4 Click **Save**. The system starts exporting the device details.

After the exporting is completed, a **Notice** dialog box is displayed.

Step 5 Click **OK**.

You can check the exported device details in the save path. See Figure 2-4.



	A	B	C	D	E	F	G	H	I	J
1	Type	Model	IP	Port	MAC	Serial No.	Version	Subnet Mask	Gateway	Initial Status
2	ACS	CAS-4MC	192.168.3.221	37777	4c:11:bf:4c:45:56	1L03699PAN02233	1.100.0.1	255.255.0.0	192.168.0.1	Initialized
3										
4										
5										
6										

Figure 2-4


2.2.2.2 Importing Devices

After you got the template, you can add the devices details into the template through which the devices can be added into the system list.



CAUTION

Close the template file before importing the devices.

Step 1 Click .

The **Modify IP** screen is displayed. See Figure 2-5.

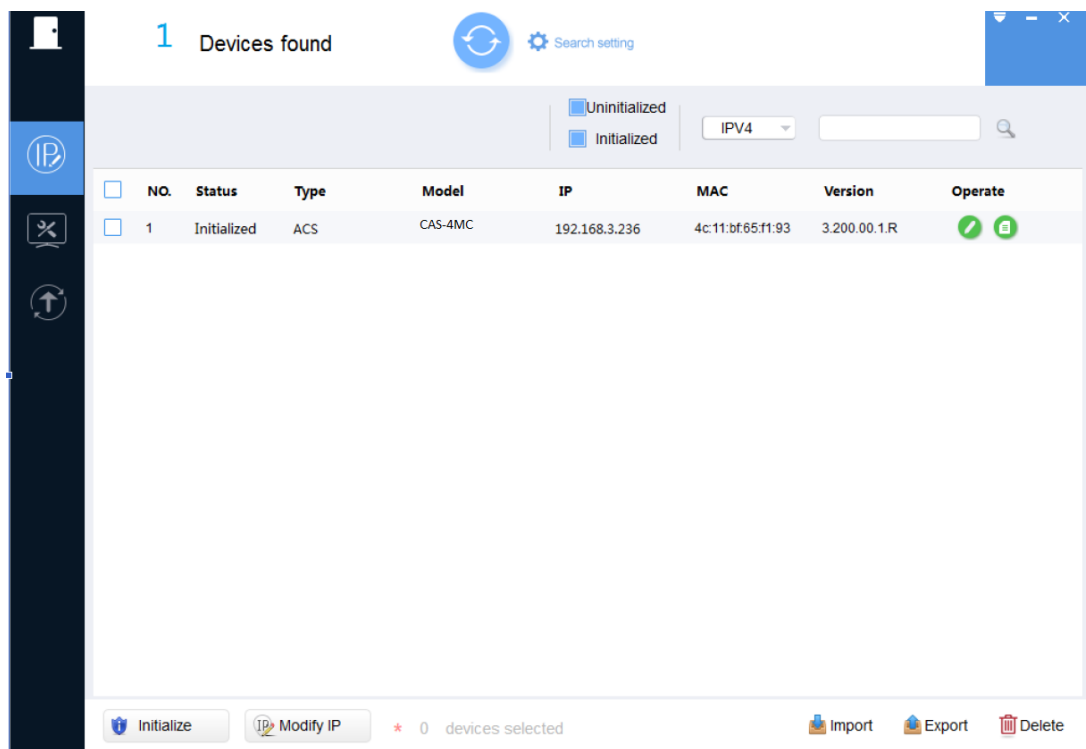


Figure 2-5

Step 2 Click **Import**.

The **Open** dialog box is displayed.

Step 3 Select the template and click **Open**. The system starts importing the devices details. After the importing is completed, a **Notice** dialog box is displayed.

Step 4 Click **OK**.

The newly imported devices appear in the device list. See Figure 2-6.

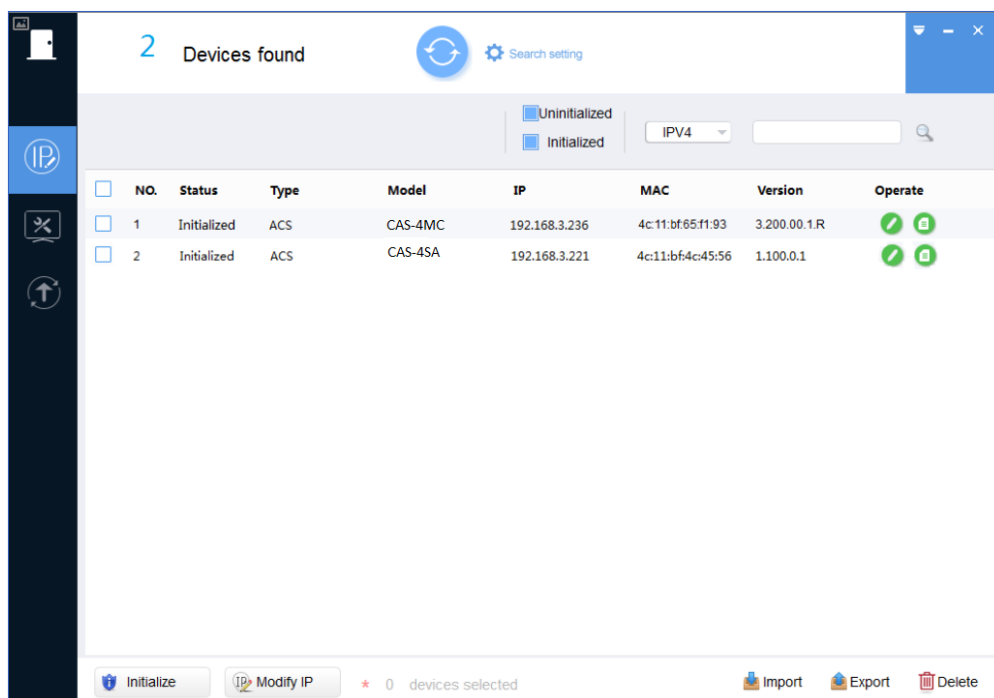



Figure 2-6

2.3 Initializing Devices

You can initialize one or multiple devices depending on your actual situation.

NOTE

- Only some models support this function.
- The initializing operation can only be performed to the devices within the local area network.
- You cannot operate the uninitialized devices that are shown in gray background. And the uninitialized devices do not appear in other interfaces of the Tool.

Step 1 Click .

The **Modify IP** screen is displayed.

Step 2 Select one or several uninitialized devices.

Step 3 Click .

The **Device initialization** screen is displayed. See Figure 2-7.

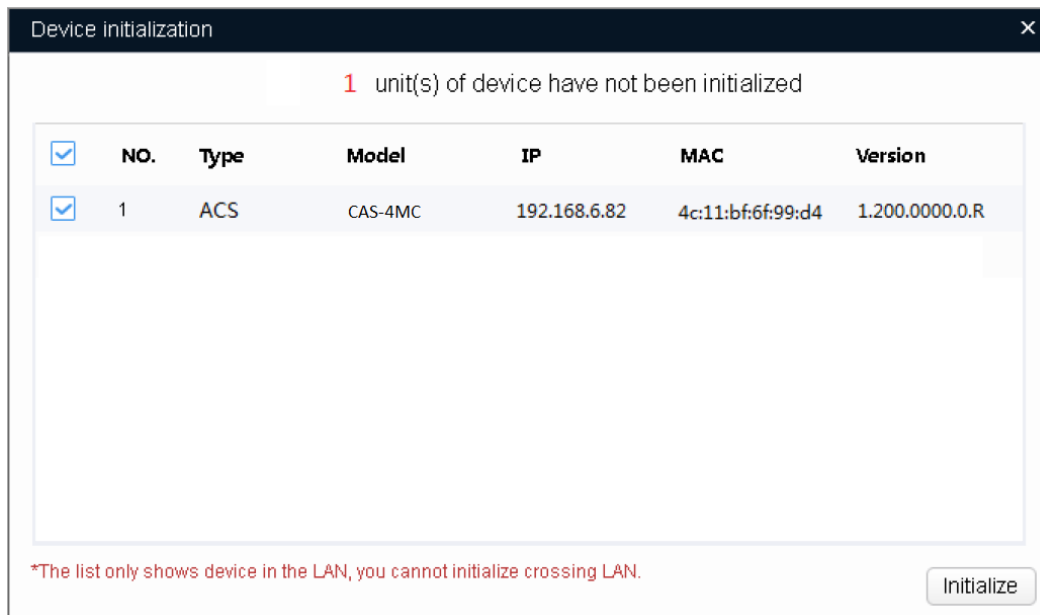


Figure 2-7

Step 4 Select the device, and then click **Initialize**.

The **Device initialization** screen is displayed. See Figure 2-8.

NOTE

- The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- If you do not provide the reserve information for password reset, you can reset the password only through XML file.

Device Initialization

1 unit(s) of device have not been initialized

Username: admin

New Password: [text input]

Confirm Password: [text input]

The password shall be 8-32 digits. It is a combination of number(s), letter(s), symbol(s) with at least two kinds of them.

☒ Email Address: [text input] (for password reset)

*After you have set new password, please set password again in Search Setup.

Initialize

Figure 2-8

Step 5 Set the initialization parameters for the device. Refer to Table 2-3 for more information.

Parameter	Description
Username	By default, the user name is admin .
New Password	<p>There are two setting rules for new password dependent on the devices, and please following the instructions on the interface to set the new password.</p> <ul style="list-style-type: none"> The new password can be set between 8 digits and 32 digits and contain at least two types from number, letter and special characters (excluding "'", '"', ";", ":", and "&"). The new password can only be set as four numbers.
Confirm Password	Confirm the new password.
Email Address	<p>Selected by default.</p> <p>The email address will be used for password reset.</p>

Table 2-3

Step 6 Click **Initialize** to start initializing the device.

The **Initialization** screen is displayed after initializing is completed. See Figure 2-9.

Click the success icon (✓) or click the failure icon (⚠) for the details.

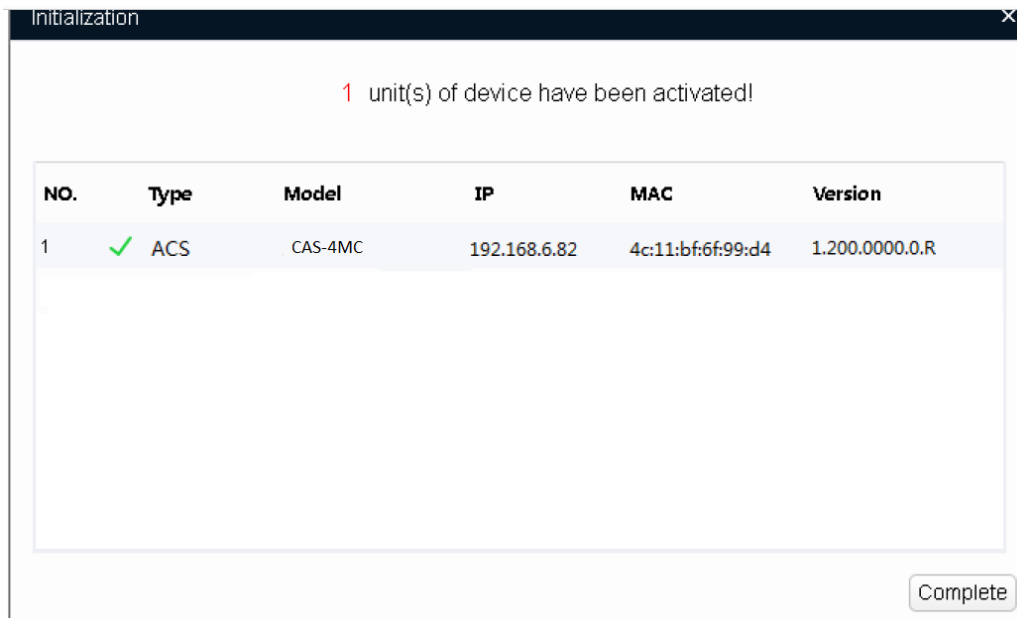


Figure 2-9

Step 7 Click **Complete**.

After the initialization is completed, the status of the devices shows as **Initialized** on the main user interface of the Tool. Meanwhile, the devices appear in other interfaces of the Tool.


2.4 Modifying IP

You can modify IP for one or multiple devices depending on your actual situation.

- When the devices quantity is small or their login passwords are different, you can modify one IP at a time.
- When the devices quantity is big and they share the same login password, you can modify IP in batches.

2.4.1 Modifying One IP

You can choose this procedure for modifying one IP.

Step 1 Click .

The **Modify IP** screen is displayed. See Figure 2-10.

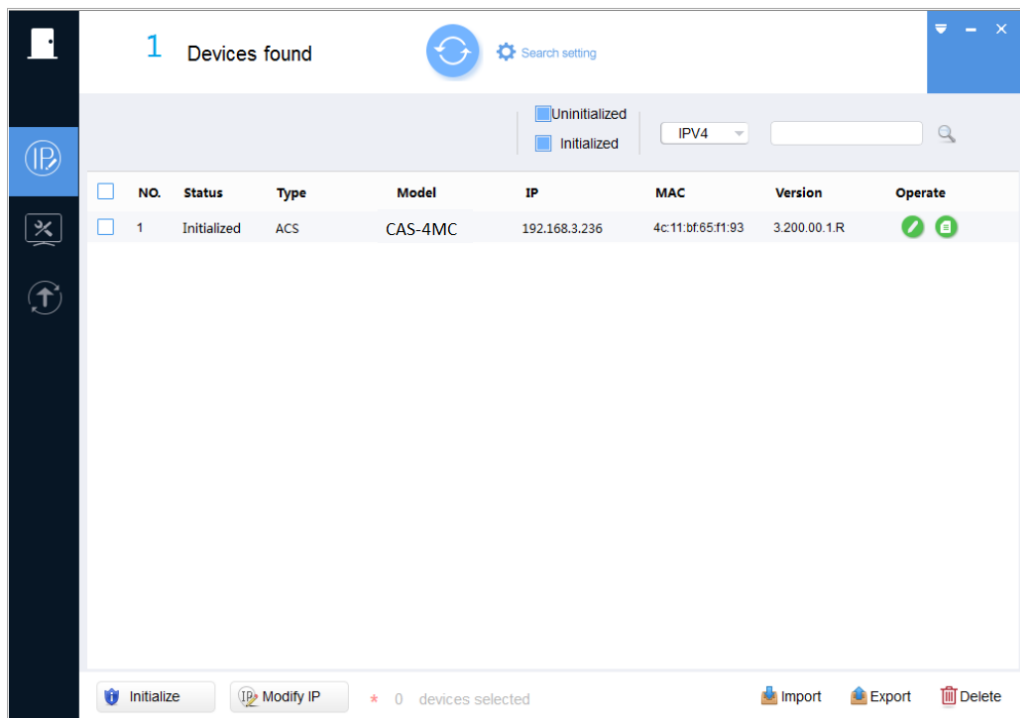


Figure 2-10

Step 2 Click the **IP Modification** button  of the device.

The **Modify IP Address** dialog box is displayed. See Figure 2-11.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Modify IP Address

Mode ☒ Static

Target IP

Subnet Mask

Gateway

Selected number of devices: 1

Figure 2-11

Step 3 Select **Static** and enter **Target IP**, **Subnet Mask**, and **Gateway**.

Step 4 Click **OK** to complete modification.

2.4.2 Modifying IP in Batches

You can choose this procedure for modifying IP for multiple devices at a time.

Step 1 Click .

The **Modify IP** screen is displayed.

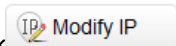
Step 2 Select the devices you want to modify IP.



NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 3 Click



The **Modify IP Address** dialog box is displayed. See Figure 2-12.

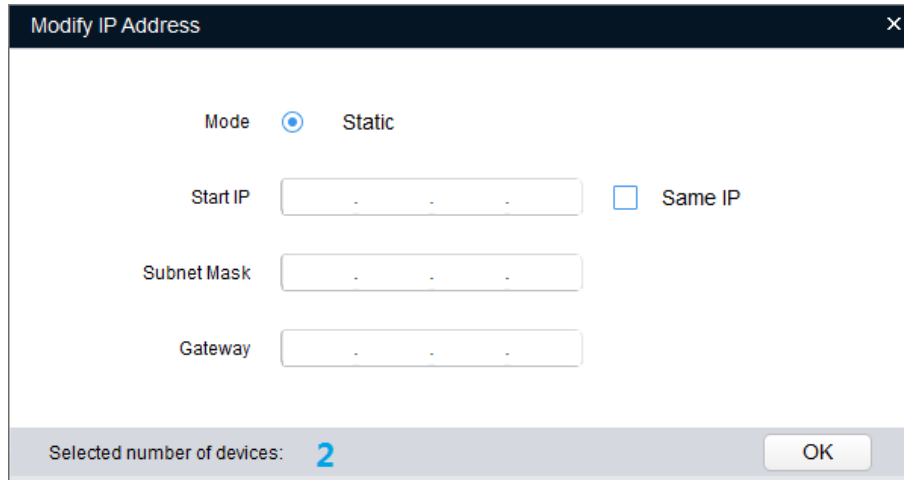
The image shows a 'Modify IP Address' dialog box. It has a title bar with a close button. Inside, there's a 'Mode' section with a radio button selected for 'Static'. Below that are three input fields: 'Start IP', 'Subnet Mask', and 'Gateway', each containing a dash. To the right of the 'Start IP' field is a checkbox labeled 'Same IP'. At the bottom, there's a status bar that says 'Selected number of devices: 2' and an 'OK' button.

Figure 2-12

Step 4 Select **Static** and enter **Target IP**, **Subnet Mask**, and **Gateway**.



NOTE

If you select the **Same IP** check box, the IP address of the devices will be set to be the same one.

Step 5 Click **OK** to complete modification.

The IP address increases sequentially from the start IP.

2.5 Configuring System Settings

You can configure the settings for system time, reboot, restore, password modification and reset.

2.5.1 Timing

You can calibrate the device time through configuration.



NOTE

DST (Daylight Saving Time) function is not supported currently.

Step 1 Click



The **Timing** screen is displayed. See Figure 2-13.

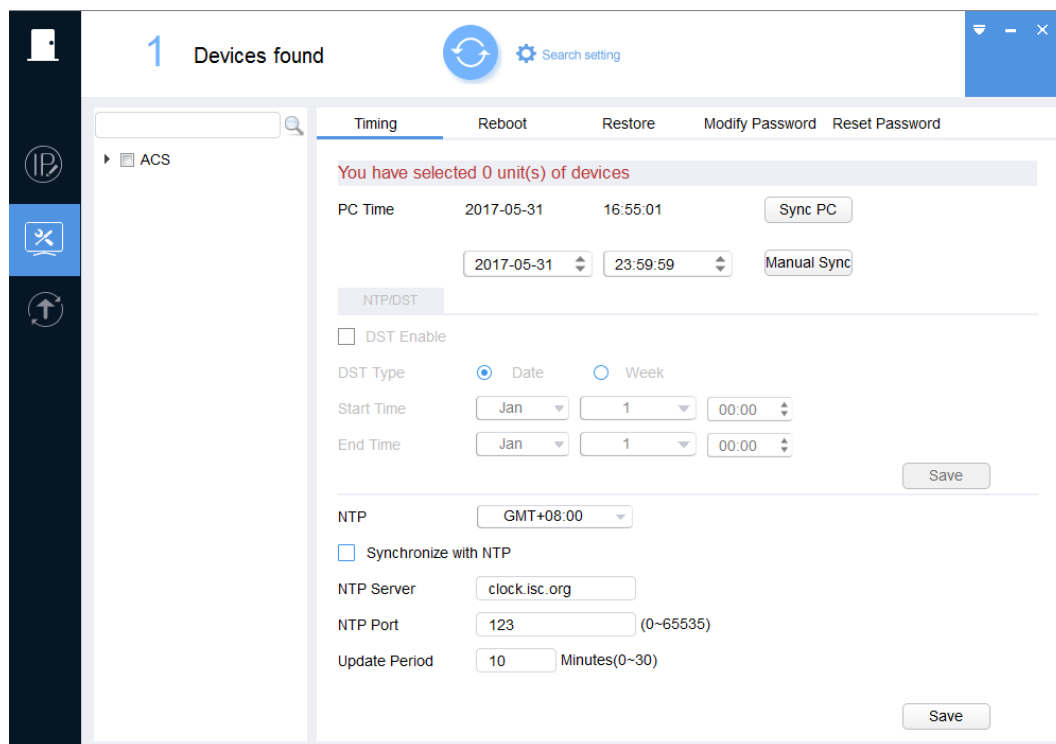




Figure 2-13

Step 2 Click  next to the device type.

The device list is displayed.

Step 3 Select one or multiple devices.

 **NOTE**

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 4 Select the time sync way for the device.

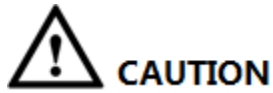
- Manual sync: Type the time and select the time zone, and then click **Manual Sync**. The device time will sync with the setting.
- PC sync: Click **Sync PC**. The device time will sync with the PC time.
- NTP sync: Select **Synchronize with NTP** check box and set the parameters. Refer to Table 2-4 for more information. Then click **Save**.

Parameter	Description
NTP Sever	Type the IP address or domain name of the corresponding NTP server.
NTP Port	Type the port number of corresponding NTP server.
Update Period	Type the time interval that device sync with the NTP.

Table 2-4

2.5.2 Rebooting

You can manually reboot the device.



CAUTION

Rebooting will interrupt operations, so please reboot the device when the operation is not so frequent.

Step 1 Click

The **Timing** screen is displayed.

Step 2 Click the **Reboot** tab.

The **Reboot** screen is displayed. See Figure 2-14.

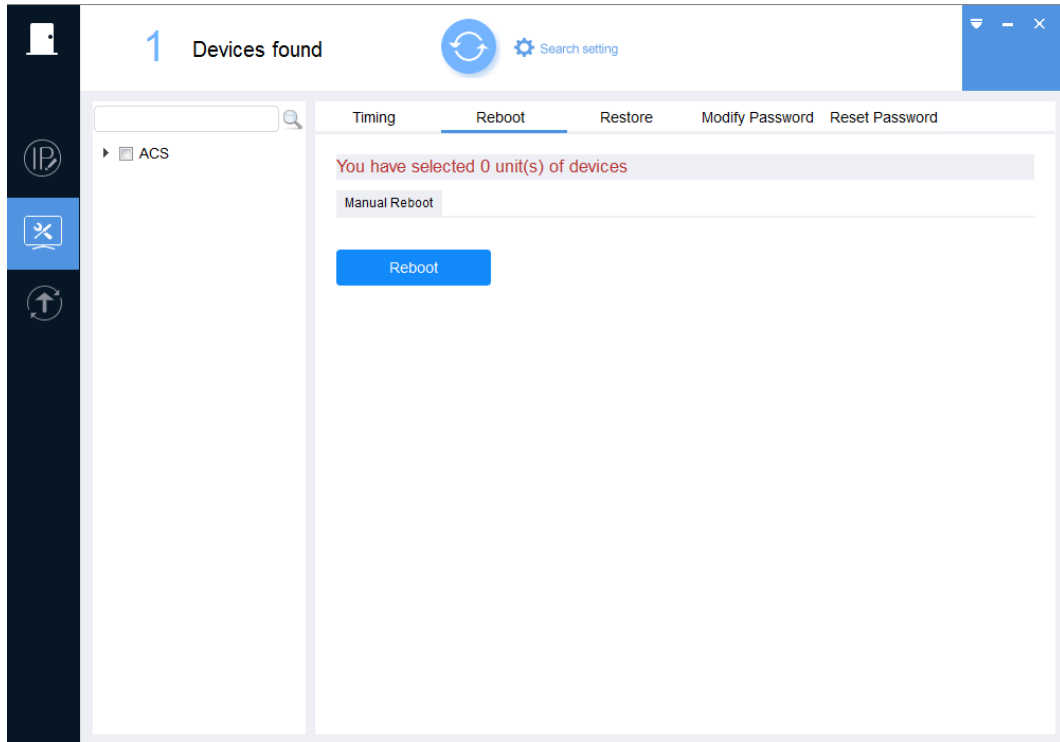


Figure 2-14

Step 3 Click next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 5 Click **Reboot**

The device reboots immediately.

2.5.3 Restoring

You can only restore the default configurations such as network (except IP configuration) and common settings.

Step 1 Click

The **Timing** screen is displayed.

Step 2 Click the **Restore** tab.

The **Restore** screen is displayed. See Figure 2-15.

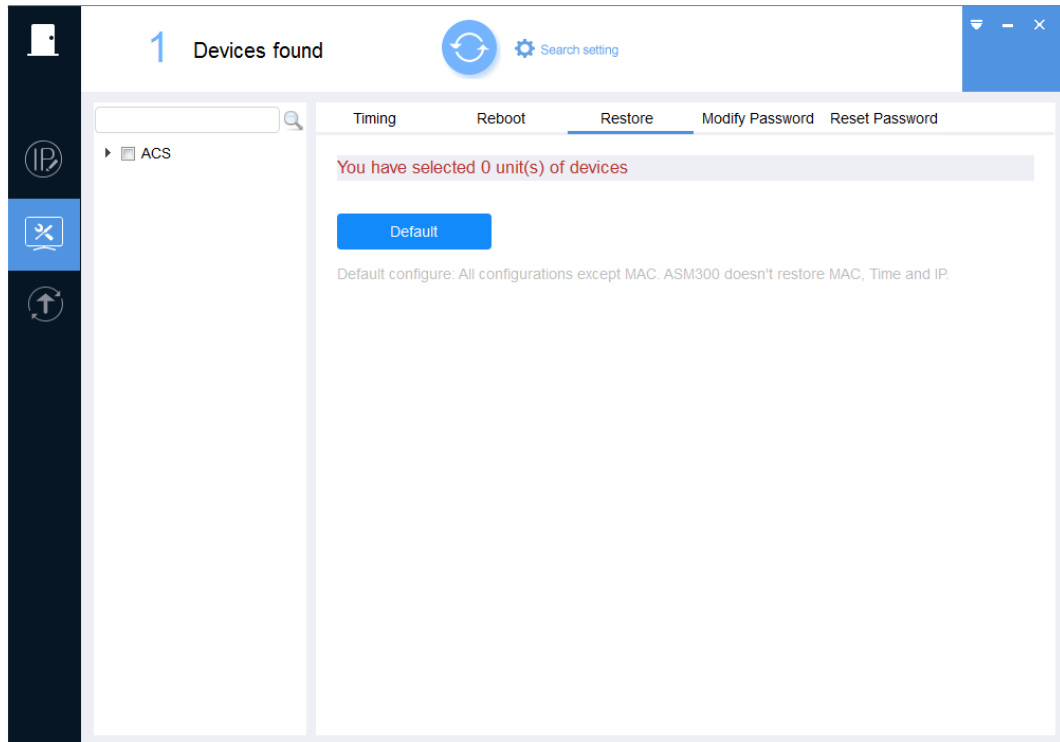




Figure 2-15

Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices.

 **NOTE**

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 5 Click **Default** to start restoring the selected devices.

After restoring is completed, the result is displayed. See Figure 2-16.

Click the success icon (✓) or click the failure icon (⚠) for the details.

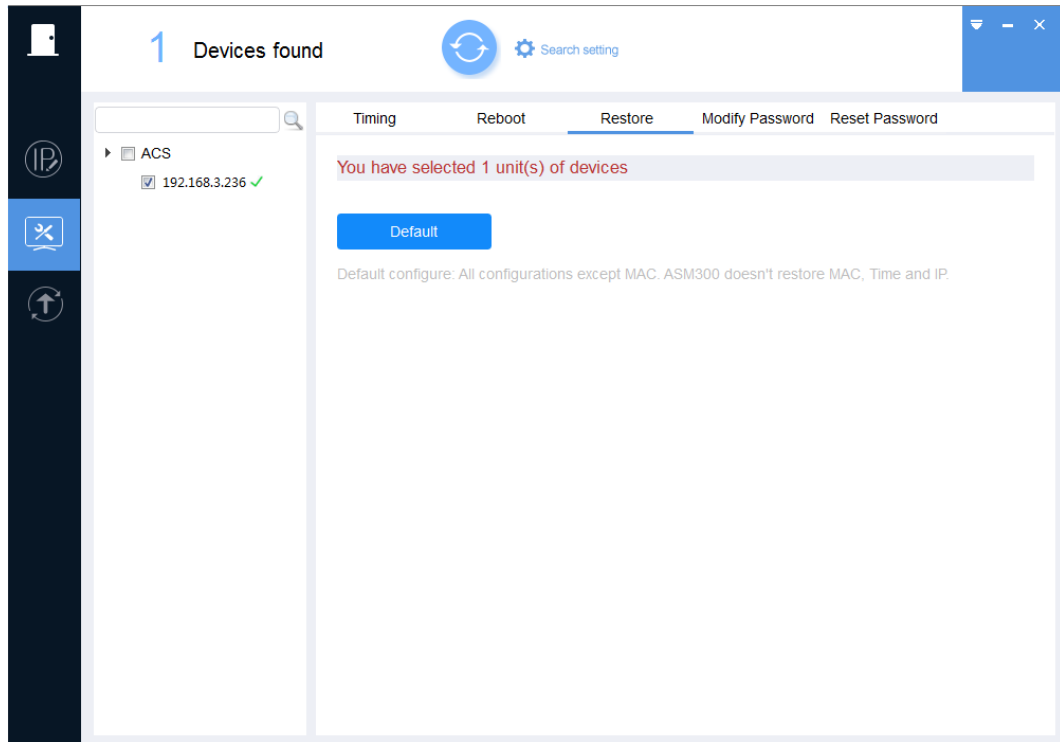


Figure 2-16

2.5.4 Modifying Password

You can modify the device login password.

Step 1 Click .

The **Timing** screen is displayed.

Step 2 Click the **Modify Password** tab.

The **Modify Password** screen is displayed. See Figure 2-17.

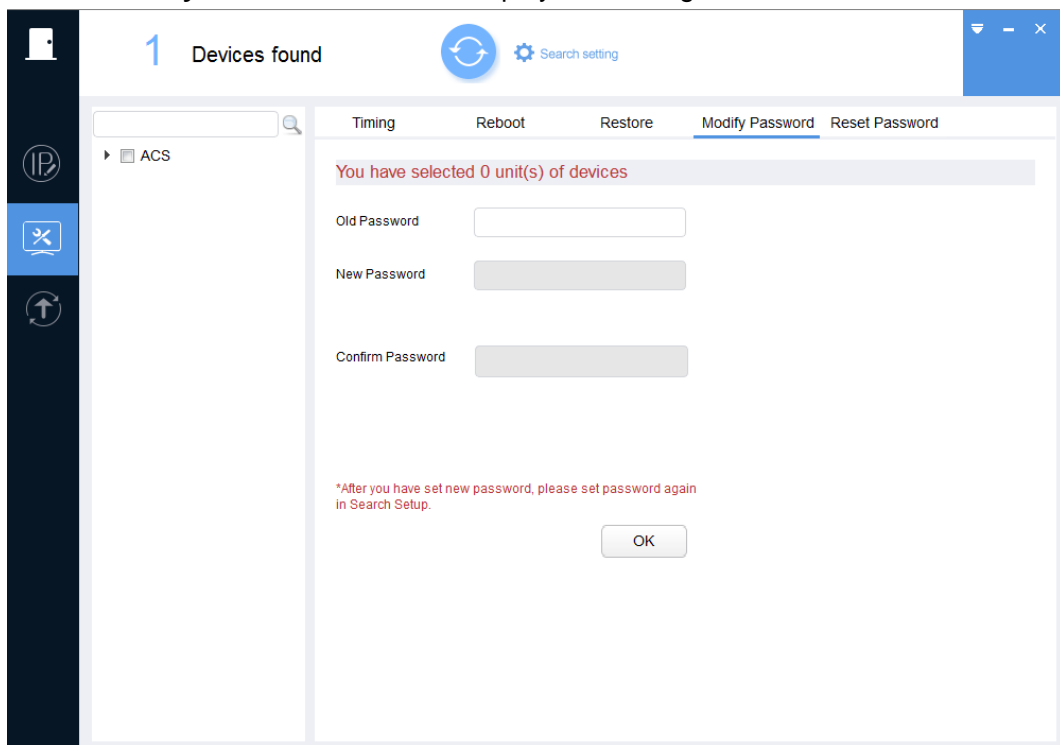




Figure 2-17

Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices.

 **NOTE**

- If you select multiple devices, their login passwords must be the same.
- If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 5 Enter the old password, and then click **OK**. The **Modify Password** screen indicating the password setting rules is displayed. See Figure 2-18.

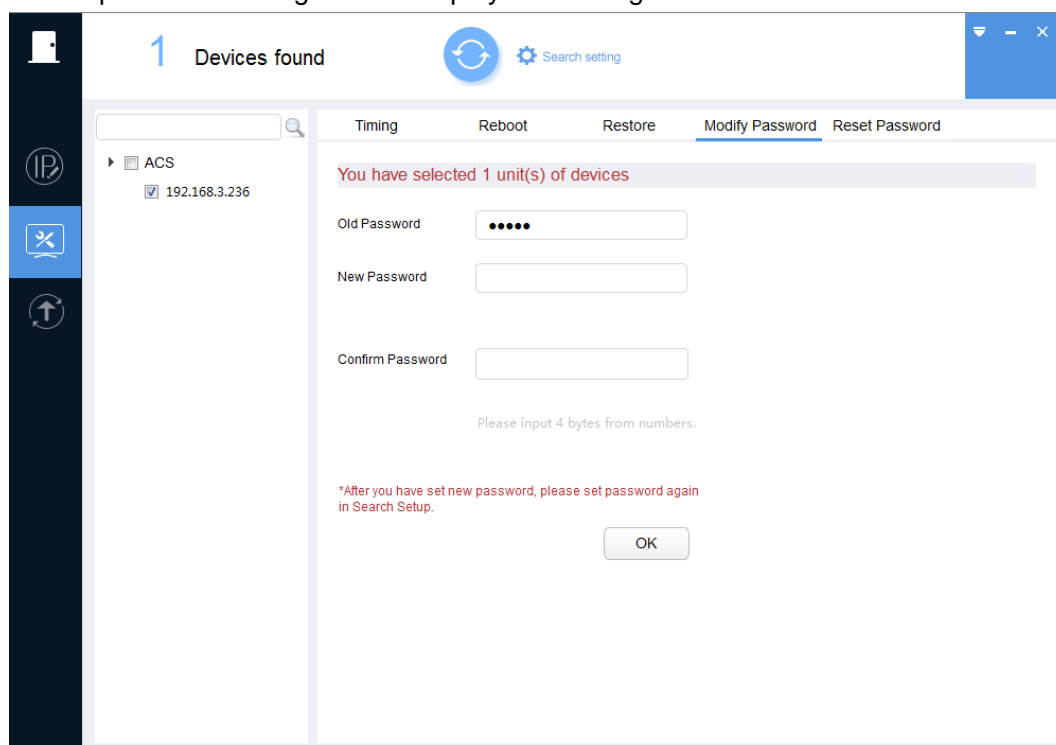



Figure 2-18

Step 6 Enter the new password and confirm password.


There are two setting rules for new password dependent on the devices, and please following the instructions on the interface to set the new password.

- The new password can be set between 8 digits and 32 digits and contain at least two types from number, letter and special characters (excluding "'", '"', ";", ":", and "&").
- The new password can only be set as four numbers.

 **NOTE**

After setting the new password, when you search the devices by **Search setting**, use the new password to login the device.

Step 7 Click **OK** to complete modification.

 **NOTE**

If the new password is the same with the old password, a **Notice** dialog box is displayed after clicking **OK**. Then you need to click **OK** to go back and reset the new password.

2.5.5 Resetting Password

You can reset the password through the quick response code (QR code) or XML file.

NOTE

- The password resetting operation can only be performed to the devices within the local area network.
- If you did not type the reserve information for password reset during device initializing, you can reset the password only through XML file.

2.5.5.1 Using the QR Code

You can reset the password by scanning the QR code. This procedure can only reset one device at a time.

Step 1 Click .

The **Timing** screen is displayed.

Step 2 Click the **Reset Password** tab.

The **Reset Password** screen is displayed. See Figure 2-19.

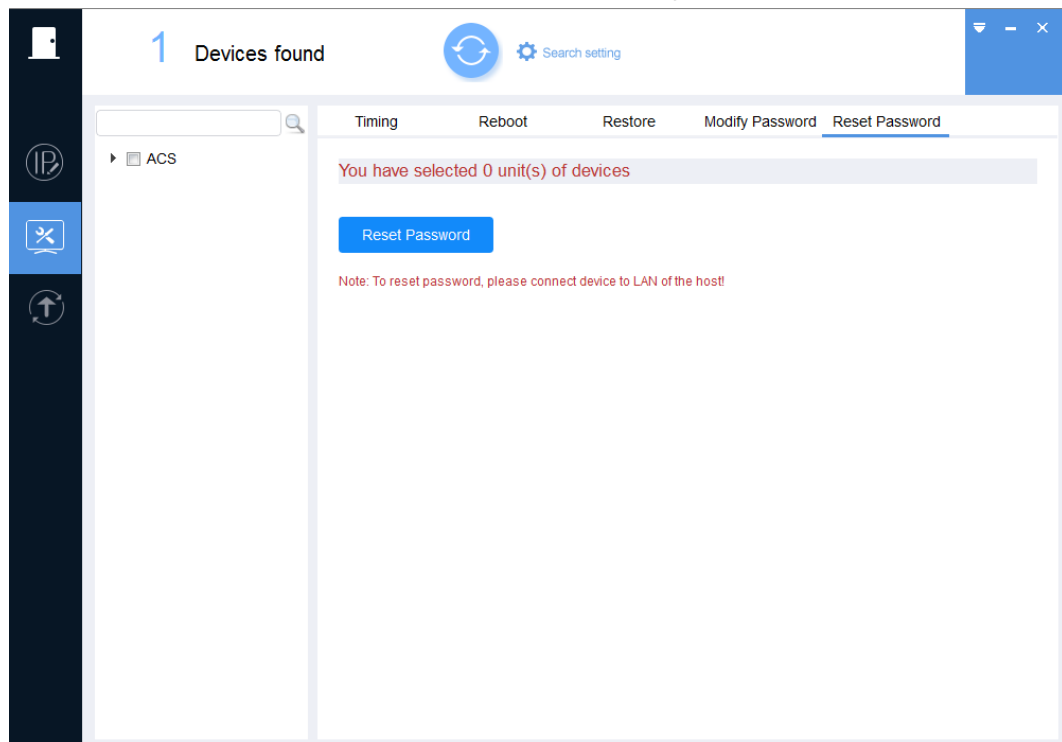



Figure 2-19

Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select the device that needs to reset the password.

NOTE

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 5 Click **Reset Password**.

- If the device does not support this function, a **Notice box** is displayed.
- If the device supports this function, the **Reset Password** screen is displayed. See

Figure 2-20.



NOTE

The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.

Figure 2-20

Step 6 Under **Reset Mode**, select **QR Code**.

Step 7 Operate according to the instructions on the interface to obtain the security code.



CAUTION

- You can obtain the security code twice at most by scanning one QR code.
- After you receive the security code, please use it to reset the password within 24 hours; otherwise the security code will become invalid.

Step 8 Enter the security code, new password, and confirm password.

There are two setting rules for new password dependent on the devices, and please follow the instructions on the interface to set the new password.

- The new password can be set between 8 digits and 32 digits and contain at least two types from number, letter and special characters (excluding "'", '"', ";", ":" and "&").
- The new password can only be set as four numbers.

Step 9 Click **OK** to start resetting the password.

After restoring is completed, the result is displayed. See Figure 2-21.

Click the success icon (✓) or click the failure icon (⚠) for the details.

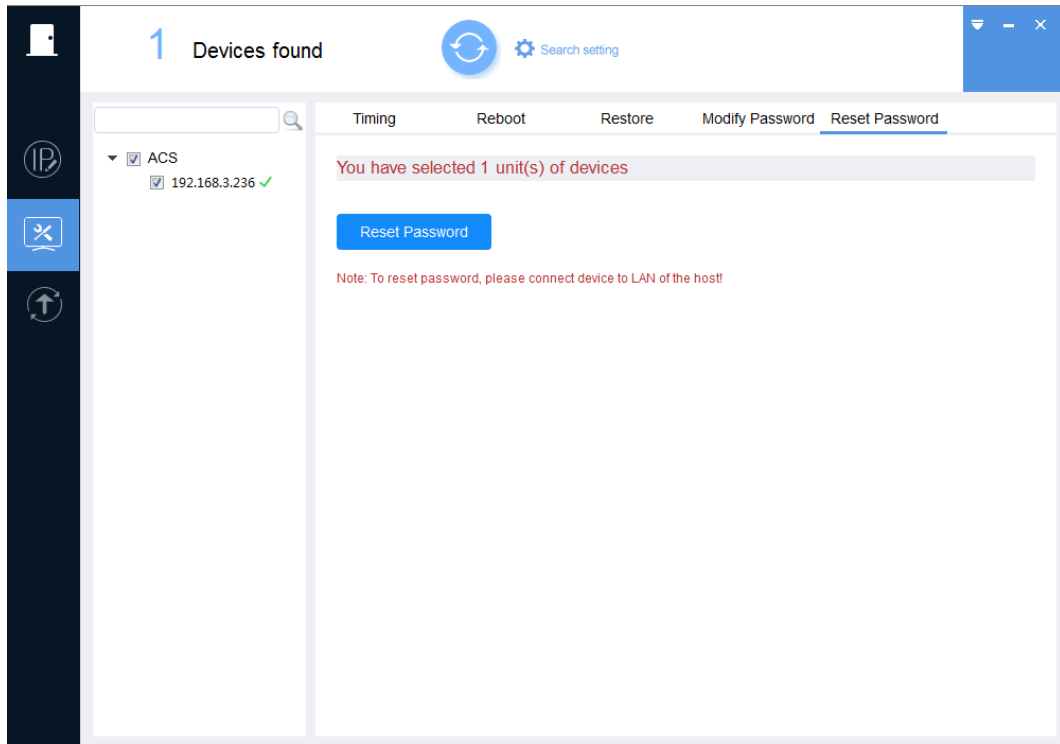



Figure 2-21

2.5.5.2 Using the XML File

You can also reset the password by XML file for one device or multiple devices.

Step 1 Click .

The **Timing** screen is displayed.

Step 2 Click the **Reset Password** tab.

The **Reset Password** screen is displayed. See Figure 2-22.

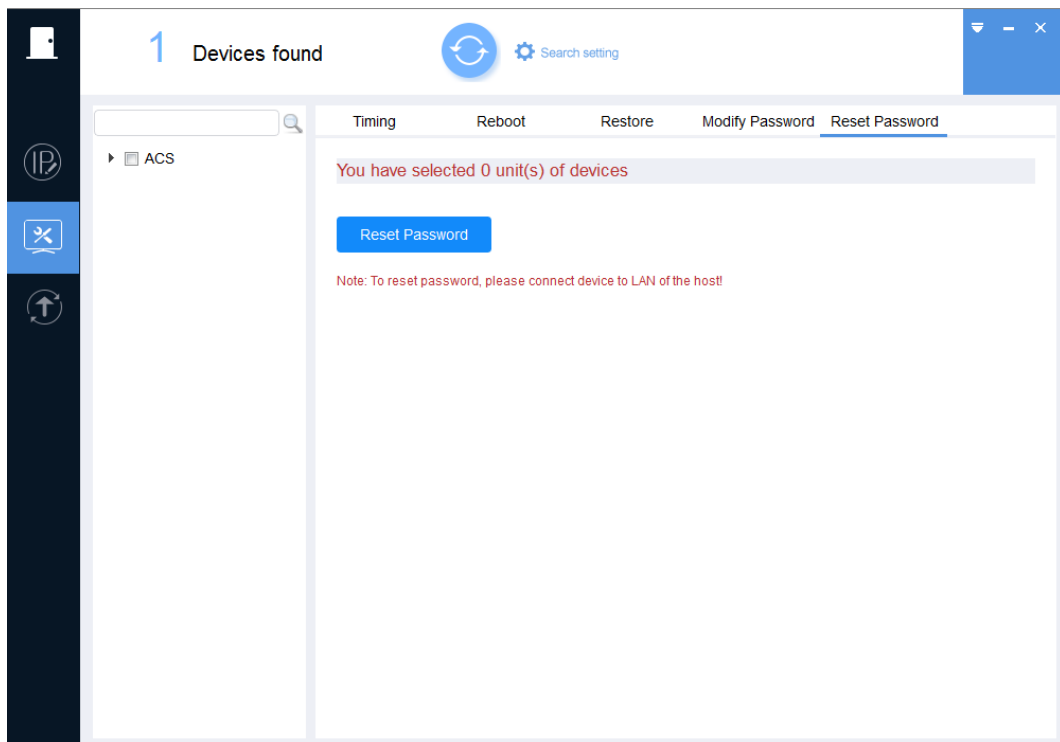



Figure 2-22

Step 3 Click  next to the device type.

The device list is displayed.

Step 4 Select one or multiple devices that need to reset the password.

 **NOTE**

If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 5 Click **Reset Password**.

- If the device does not support this function, a **Notice box** is displayed.
- If the device supports this function, the **Reset Password** screen is displayed. See Figure 2-23.


 **NOTE**

The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.

Figure 2-23

Step 6 Under **Reset Mode**, select **XML File**.

The **Reset Password-Export XML** screen is displayed. See Figure 2-24.

 **NOTE**

The user interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.

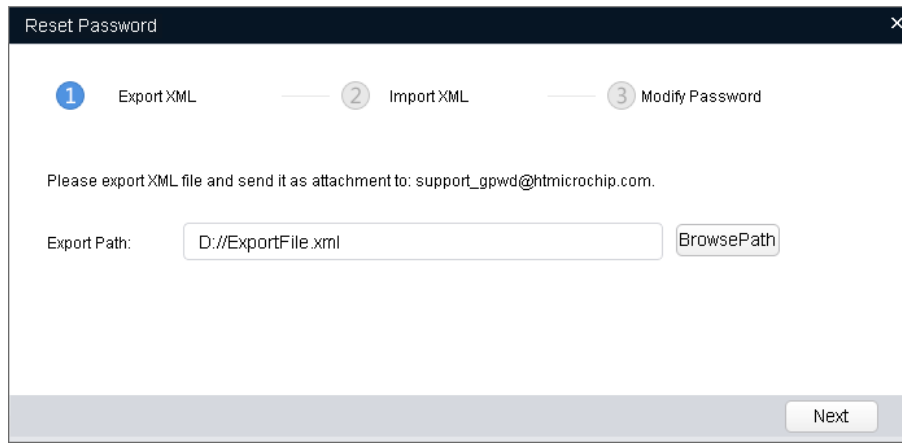


Figure 2-24

Step 7 Export XML.

1. Click **BrowsePath** to select the save path for the exported XML file.
2. Click **Next** to start exporting.
After the exporting is completed, a **Notice** dialog box will be displayed.
3. Click **OK** to complete exporting.
After completing exporting the XML, the **Reset Password-Import XML** screen is displayed.

Step 8 Obtain the **result.xml** file.

Find the **ExportFile.xml** under the save path and send it as an attachment to the designated mailbox indicated on the interface. In a few minutes, you will receive a **result.xml** file as an attachment and save it properly.

Step 9 Import XML.



NOTE

If the **Reset Password-Import XML** screen is closed, click **System Settings > Reset Password**. On the **Reset Password** tab, click **Note: To reset password, please connect device to LAN of the host!** to continue the operation.

1. Click **Open** to import the **result.xml** file from the save path. See Figure 2-25.

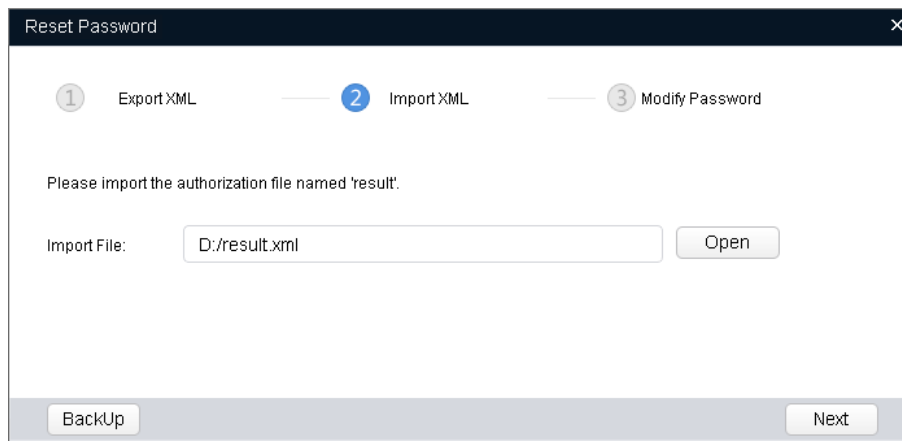
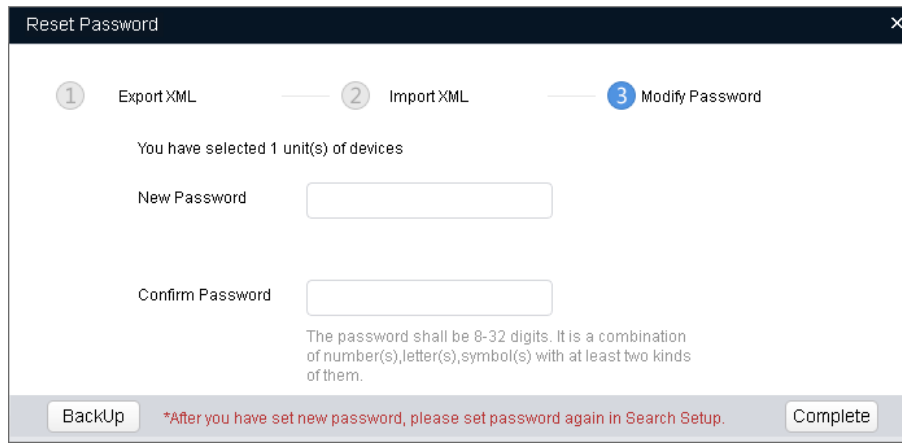


Figure 2-25

2. Click **Next** to start importing.
After the exporting is completed, the **Reset Password-Modify Password** screen is displayed. See Figure 2-26.



Reset Password

1 Export XML — 2 Import XML — 3 Modify Password

You have selected 1 unit(s) of devices

New Password

Confirm Password

The password shall be 8-32 digits. It is a combination of number(s), letter(s), symbol(s) with at least two kinds of them.

BackUp *After you have set new password, please set password again in Search Setup. Complete

Figure 2-26

Step 10 Modify Password.

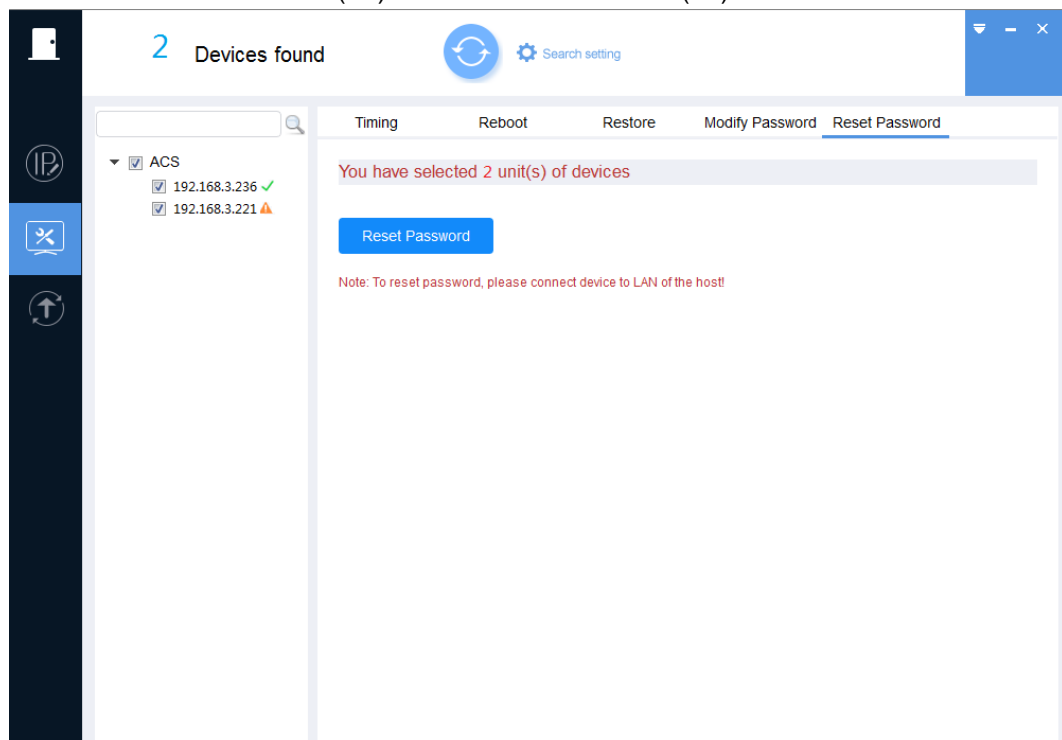
Enter the new password and confirm password. There are two setting rules for new password dependent on the devices, and please following the instructions on the interface to set the new password.

- The new password can be set between 8 digits and 32 digits and contain at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&").
- The new password can only be set as four numbers.

Step 11 Click **Complete** to start resetting the password.

After operation is completed, the result is displayed. See Figure 2-27.

Click the success icon (✓) or click the failure icon (⚠) for the details.



2 Devices found

Timing Reboot Restore Modify Password Reset Password

ACS

- 192.168.3.236 ✓
- 192.168.3.221 ⚠

You have selected 2 unit(s) of devices

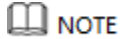
Reset Password

Note: To reset password, please connect device to LAN of the host!

Figure 2-27

2.6 Upgrading Devices


You can upgrade one or multiple devices.



If the device is disconnected during upgrading, as long as you keep staying on the upgrading interface, the device will continue to upgrade when it is connected back to the network.

2.6.1 Upgrading One Device

You can choose this procedure for upgrading one device.

Step 1 Click .

The **Upgrade** screen is displayed. See Figure 2-28.

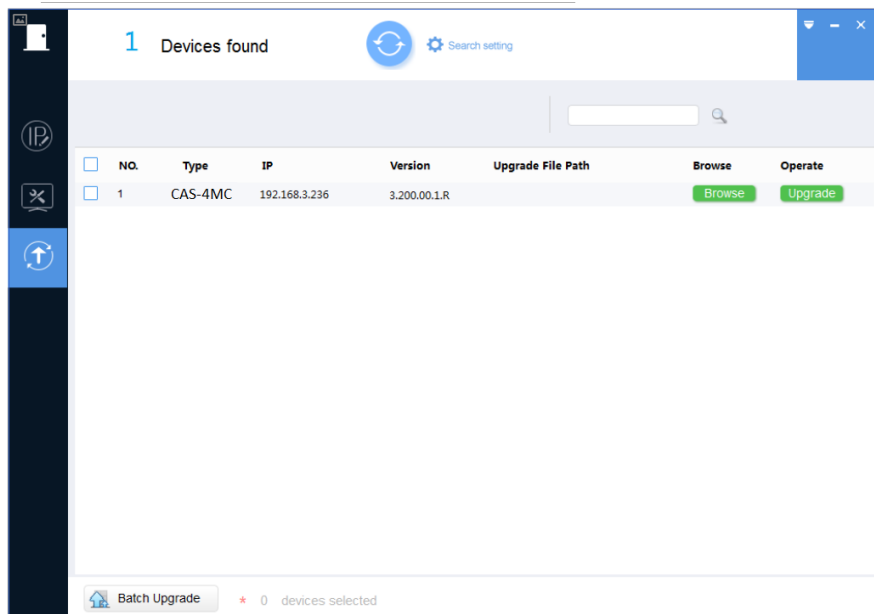


Figure 2-28

Step 2 Click **Browse** next to the device that you want to upgrade, and then select the specific file that needs to be upgraded and click **Open**.



NOTE


If the device is not in the device list, search again. For the details about how to search devices, see "2.2 Adding Devices."

Step 3 Click **Upgrade** to start upgrading.

After upgrading is completed, a **Notice** dialog box will be displayed indicating the success of upgrading. Then the device reboots automatically.

2.6.2 Upgrading Devices in Batches

You can upgrade multiple devices to the same software version.

Step 1 Click .

The **Upgrade** screen is displayed.

Step 2 Select the devices that need to be upgraded.



NOTE

- If the device is not in the device list, searching again. For the details about how to search devices, see "2.2 Adding Devices."
- Make sure the selected devices are subject to be upgraded to the same software version.

Step 3 Click  **Batch Upgrade**.

The **Batch Upgrade** dialog box is displayed. See Figure 2-29.

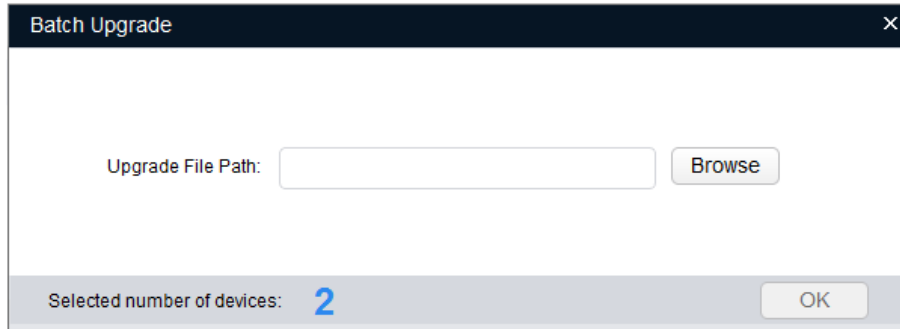


Figure 2-29

Step 4 Click **Browse** to select the files that need to be upgraded.

Step 5 Click **OK** to start upgrading.