SADP Software

User Manual

UD08334B

User Manual

About this Manual

This Manual is applicable to SADP Software.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY

QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Contents

1 Introduction

1.1 Overview

Search Active Devices Protocol (SADP) software is user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

1.2 System Requirements

Operating System:
Microsoft Windows 10/Windows 8/Windows 8.1/Windows 7/Windows 2008 32/64-bit,
Windows XP/Windows 2003 32-bit
CPU: Intel Pentium IV @ 3.0 GHz or above
RAM: 1G or above
Video Card: RADEON X700 Series
Display: 1024*768 resolution or above

1.3 Conventions

In order to simplify the description, we define the “SADP software” as “software” in the following chapters.

1.4 Version Information

After installing the software, click  on the desktop to run the software.

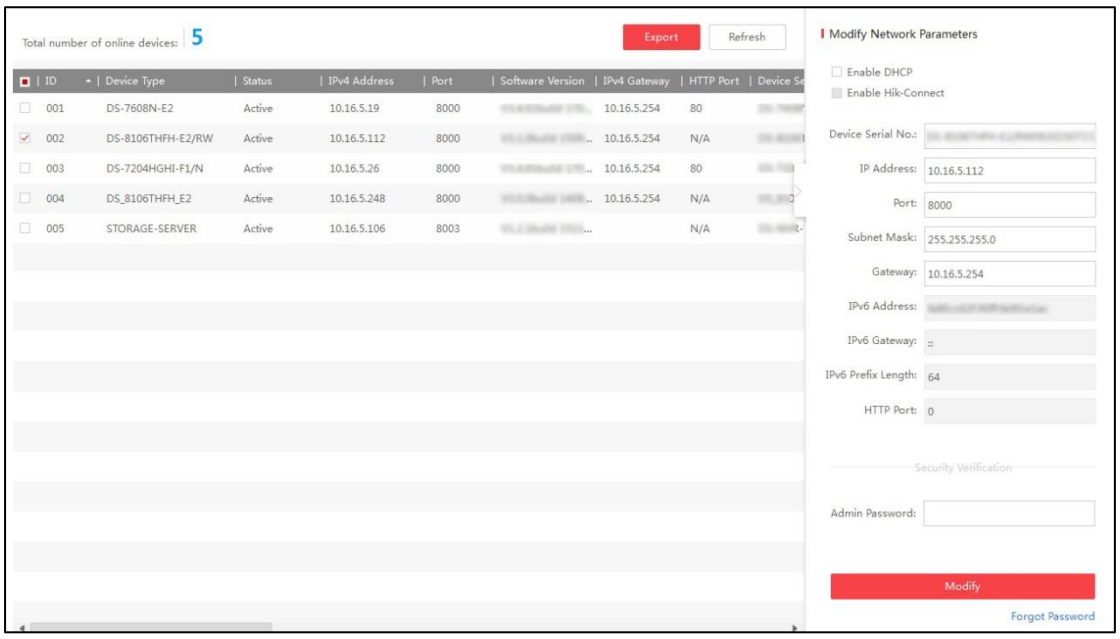
Click the  button in the upper-right corner to view the version information and you can click **User Manual** to get the User Manual of the software.

2 Operate SADP Software

2.1 Search Active Devices Online

Task 1: Search Online Devices Automatically

After launching the SADP software, it automatically searches the online devices every 1 minute from the subnet where your computer locates. It displays the total number and information of the found devices in the device list. Device information including the device type, IP address, port number, gateway, etc. will be displayed.



NOTE

- Device can be searched and displayed in the list immediately by clicking **Refresh** after it goes online. It also will be searched and displayed in the list in 1 minute automatically after it goes online.
- Device will be removed from the list immediately by clicking **Refresh** after it went offline. It also will be removed in 3 minutes automatically after it went offline.

Task 2: Search Online Devices Manually

You can also click **Refresh** to refresh the online device list manually. The newly found devices will be added to the list.

NOTE

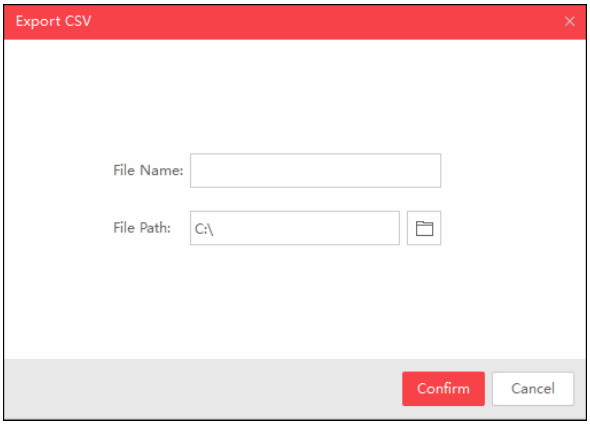
- You can click ▲ or ▼ on each column heading to order the information; you can click ▯ to expand the device table and hide the network parameter panel on the right side, or click ▯ to show the network parameter panel.

- Click and drag the column heading to change the heading sequence.
- You can view all information of the devices by dragging the scroll bar at the bottom to the right.

Double-click the IPv4 Address field of the found device, and the login interface via web browser of the device will be opened. You can enter the user name and password to log into the device.

You can save the information of the found devices as the following steps:

1. Select the device(s) by checking the checkbox(es)
2. Click **Export** to pop up the Export Excel dialog.
3. Input the file name in the dialog.
4. Click to select the saving path.
5. Click **Confirm** to save the information as CSV file.



2.2 Activate Device

Before you can log into the device properly, or modify the network parameters, you must create a password for the device's administrator user "admin" to activate it.

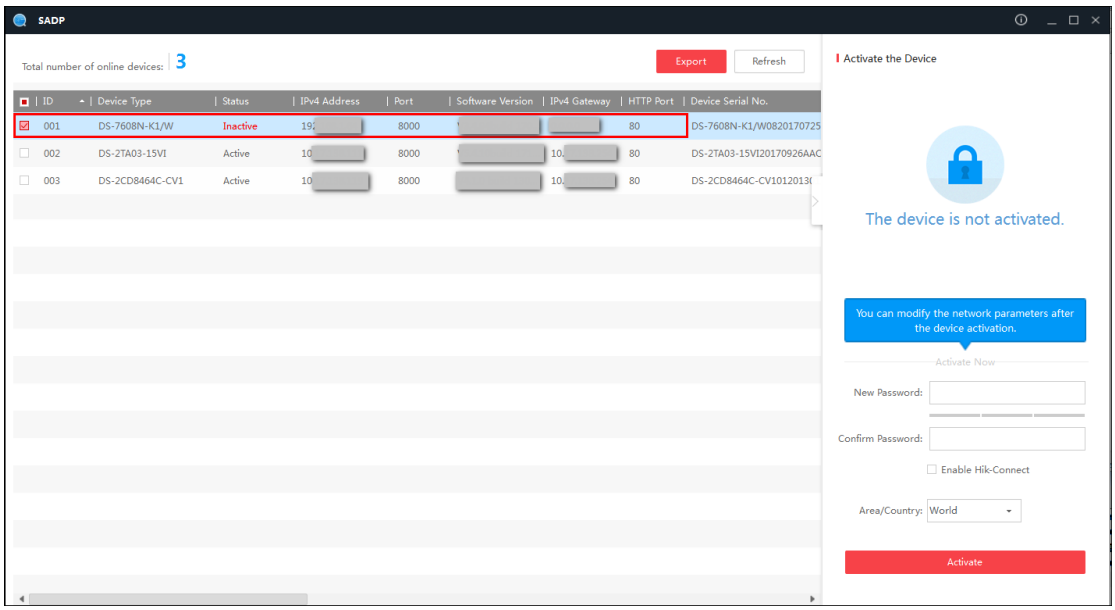
NOTE

This function should be supported by the devices.

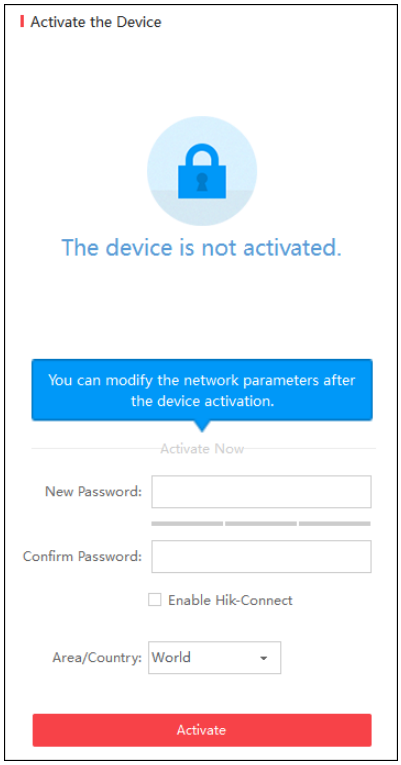
Activate Normal Device

Steps:

1. Select the device which is in inactive status by checking the checkbox.



2. In the Activate the Device panel, create a password for the device and confirm the password. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.



STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories:* ***numbers, lowercases, uppercases*** *and* ***special characters****. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your*

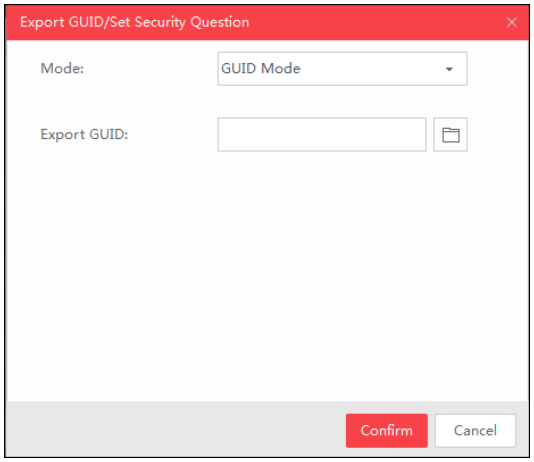
product.

3. Click **Activate** to activate the device. A "The device is activated." hint window pops up when the password is set successfully.

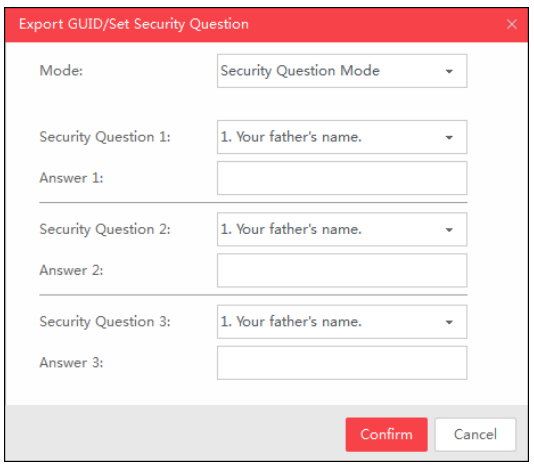
NOTE

After activation, the device IP address will be set as the default IP: 192.168.1.64. For modifying the IP address, refer to *Chapter 2.3 Modify the Network Parameters*.

4. Optionally, if the device you selected supports resetting password via GUID file or security question, the dialog **Export GUID/Set Security Question** will open. You can export the GUID file or set the security question for further password reset.

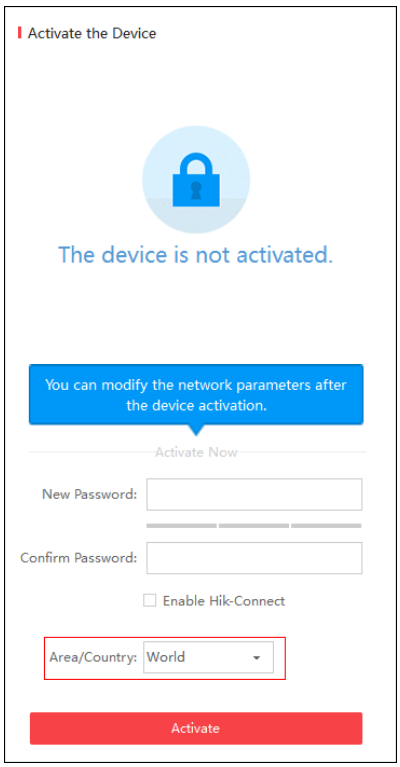


1) (Optional) Select the **GUID Mode.**
2) Click to set the saving path of exported GUID file.
3) Click **Confirm.**
4) (Optional) Select the **Set Security Question Mode.**



5) Set the security question as you desired.
6) Click **Confirm**.

5. Optionally, if the device you selected supports Wi-Fi, the **Area/Country** will appear. You can select the area or country supported by the device as you desired. The Wi-Fi signal strength is different of different area or country.



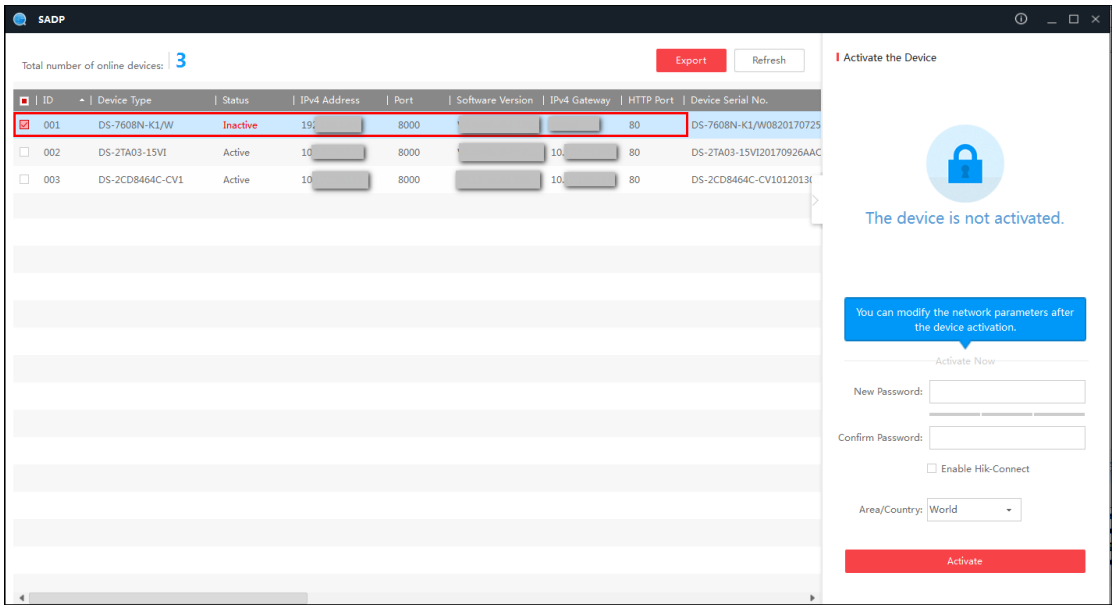
NOTE

- The selectable area or country depends on the device you selected.

Activate Hik-Connect Device

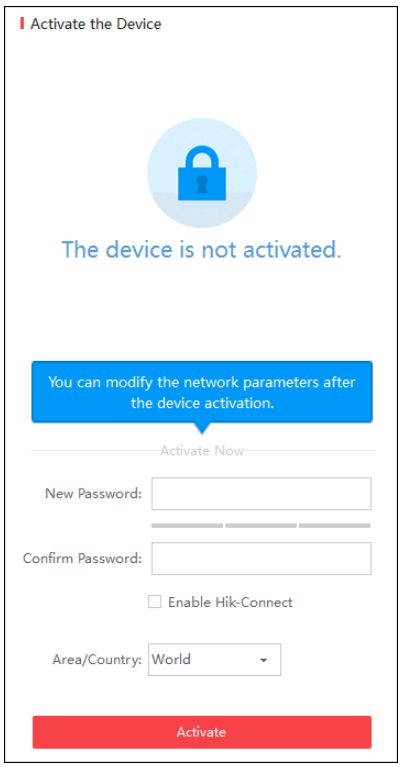
Steps:

1. Select the device which is in inactive status by checking the checkbox.



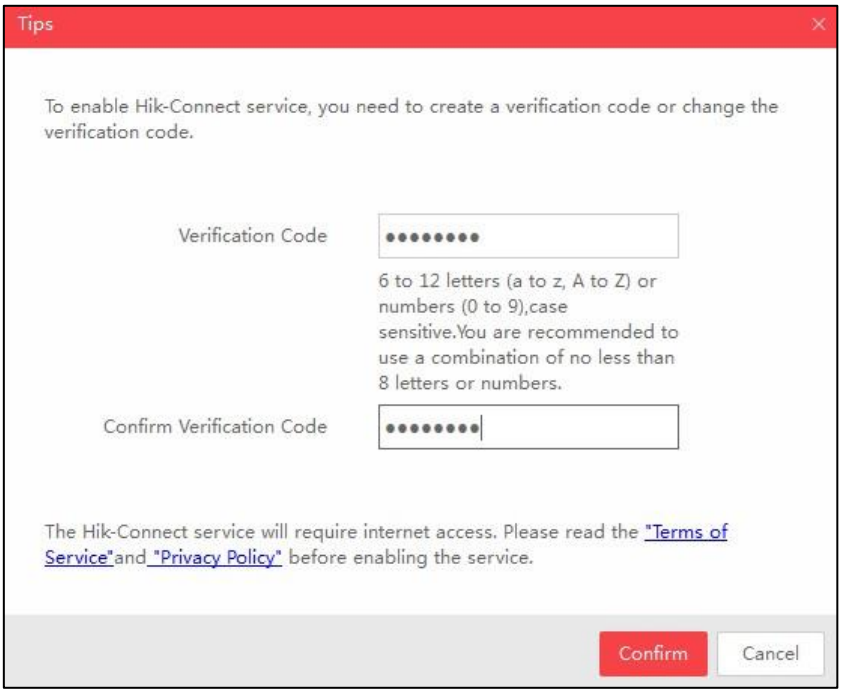
2. In the Activate the Device panel, create a password for the device and confirm the password. The system will judge password strength automatically, and we

highly recommend you to use a strong password to ensure your data security.



STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories:* ***numbers***, ***lowercases***, ***uppercases*** *and* ***special characters****. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*

3. If the Hik-Connect service haven't been enabled, you can enable it by following the steps:
   1) Check the **Enable Hik-Connect** checkbox on the Activate the Device panel to pop up the Tips dialog.
   2) Create a verification code in the Tips dialog.
   3) Confirm the verification code in the Tips dialog.
   4) Click and read "Terms of Service" and "Privacy Policy".
   5) Click **Confirm** to enable Hik-Connect service.



NOTE

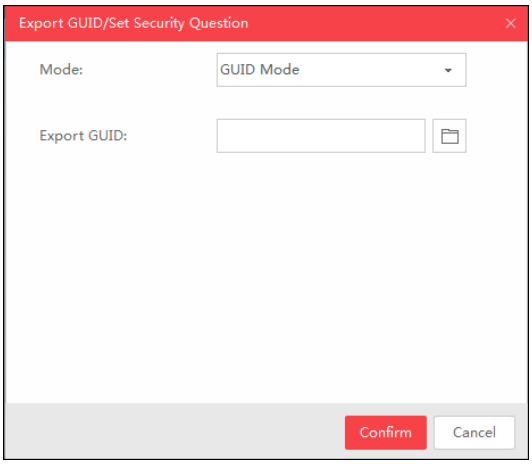
- The verification code is needed when you add your device to the Hik-Connect app.
- The length of verification code ranges from 6 to 12 letters (a to z, A to Z) or numbers (0 to 9). The verification code is case sensitive. You are recommended to use a combination of no less than 8 letters or numbers for the Verification Code.
- The Hik-Connect service requires internet access. Please read the “Terms of Service” and “Privacy Policy” before enabling the service.

4. Click **Activate** to activate the device. A “The device is activated.” hint window pops up when the password is set successfully.

NOTE

After activation, the device IP address will be set as the default IP: 192.168.1.64. For modifying the IP address, refer to *Chapter 2.3 Modify the Network Parameters*.

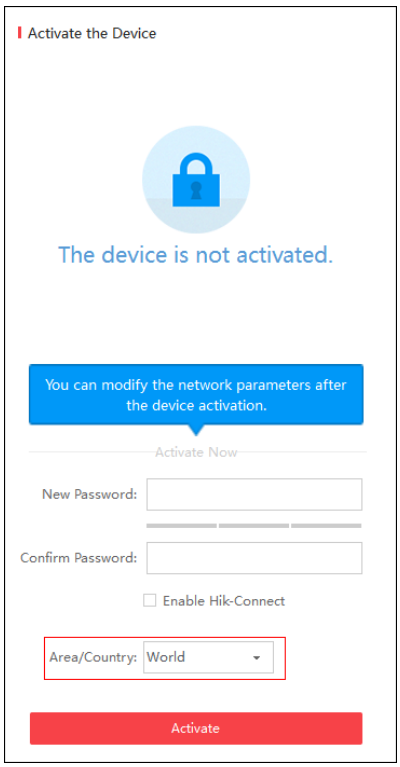
5. Optionally, if the device you selected supports resetting password via GUID file or security question, the dialog **Export GUID/Set Security Question** will open. You can export the GUID file or set the security question for further password reset.



1) (Optional) Select the **GUID Mode.**
2) Click to set the saving path of exported GUID file.
3) Click **Confirm.**
4) (Optional) Select the **Set Security Question Mode.**

5) Set the security question as you desired.
6) Click **Confirm**.

6. Optionally, if the device you selected supports Wi-Fi, the **Area/Country** will appear. You can select the area or country supported by the device as you desired. The Wi-Fi signal strength is different of different area or country.



NOTE

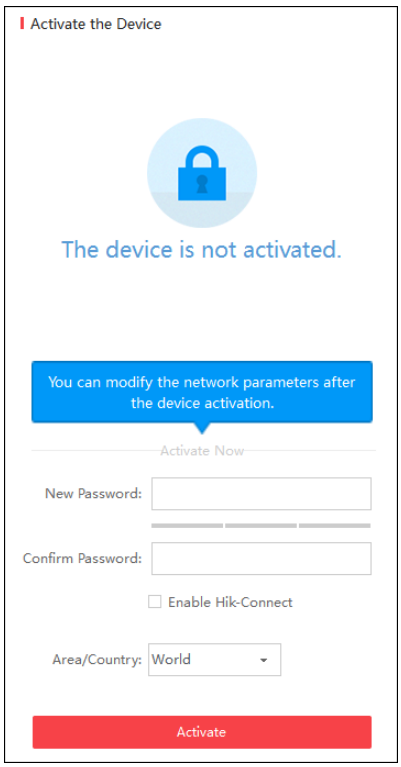
The selectable area or country depends on the device you selected.

Activate Normal Devices in Batch

You can activate multiple devices at the same time with the same admin password.

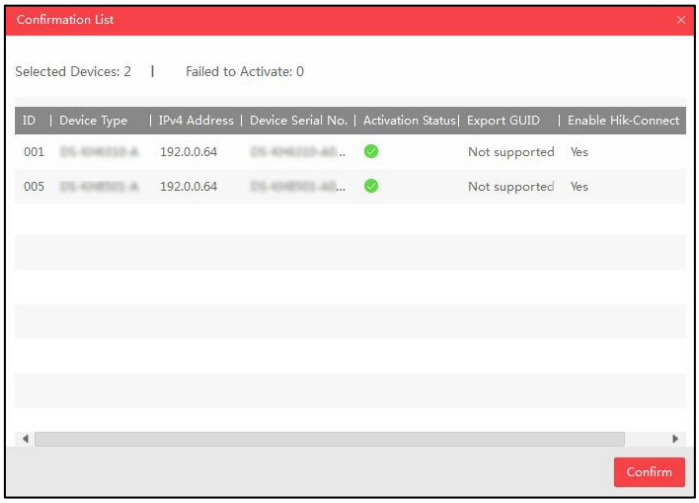
Steps:

1. Select multiple devices to be activated by checking the checkboxes in the device list.
2. Create a password in the New Password field for the devices, and confirm the password. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.



STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories:* ***numbers***, ***lowercases***, ***uppercases*** *and* ***special characters****. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*

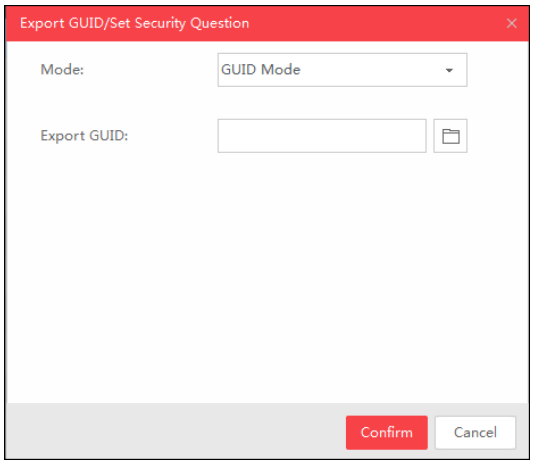
3. Click **Activate** to activate the device.
4. After activation, the confirmation list will pop up, showing the total selected device number, the activation failed number, and the details of each device.



NOTE

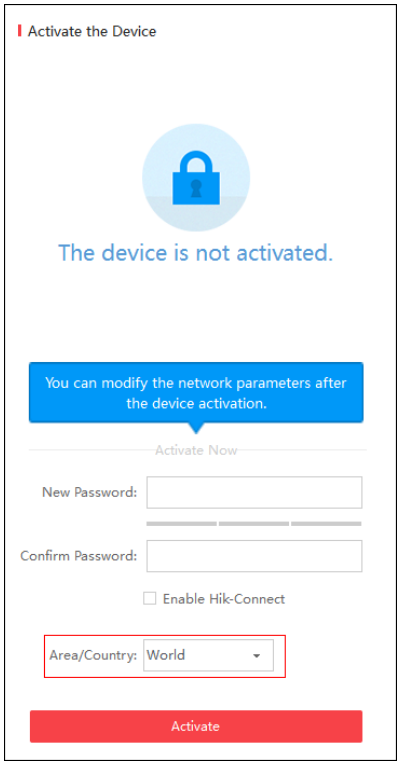
After activation, the devices IP addresses will be set as the default IP: 192.168.1.64. For modifying the IP address, refer to *Chapter 2.3 Modify the Network Parameters*.

5. Optionally, if the devices you selected support resetting password via GUID file or security question, the dialog **Export GUID/Set Security Question** will open. You can export the GUID file of selected devices for further password reset.



   1) (Optional) Select the **GUID Mode.**
   2) Click 🗀 to set the saving path of exported GUID file.
   3) Click **Confirm.**

6. Optionally, if the devices you selected support Wi-Fi, the **Area/Country** will appear. You can select the supported area or country as you desired. The Wi-Fi signal strength is different of different area or country.



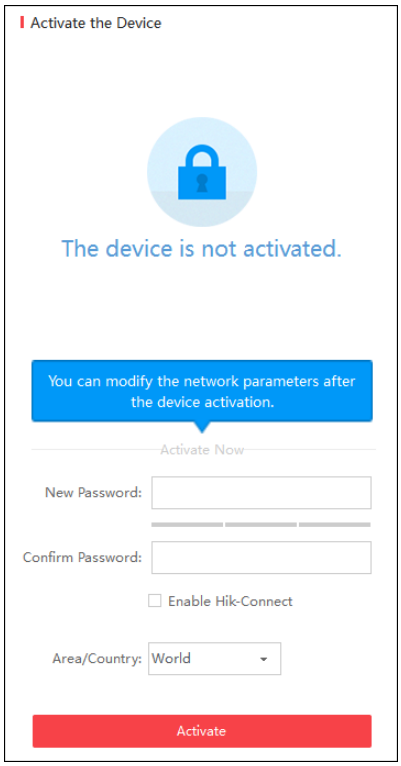
- If the devices you selected support different area or country, the Area/Country is not available.
- If some of the devices you selected do not support Wi-Fi, the Area/Country is not available.

Activate Hik-Connect Devices in Batch

You can activate multiple devices at the same time with the same admin password.

Steps:

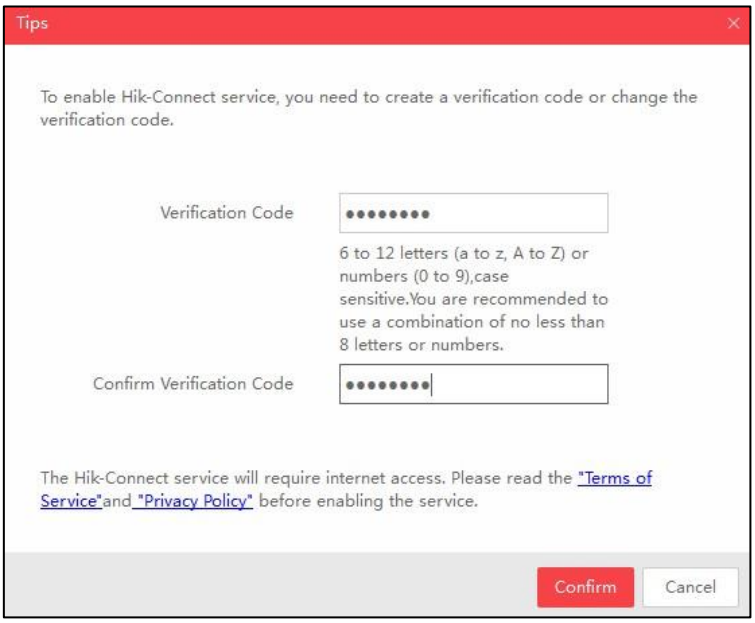
1. Select multiple devices to be activated by checking the checkboxes in the device list.
2. Create a password in the New Password field for the devices, and confirm the password. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.



STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories:* ***numbers***, ***lowercases***, ***uppercases*** *and* ***special characters****. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*

3. Enable the Hik-Connect service by following steps:

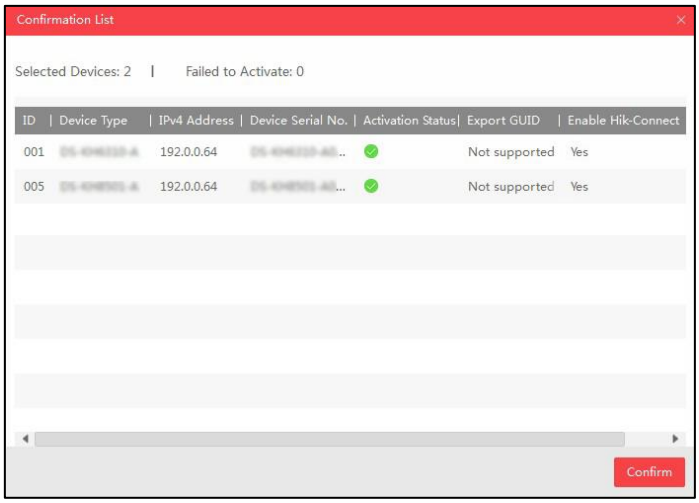
1) Check the **Enable Hik-Connect** checkbox on the Activate the Device panel.
2) Create a verification code in the Tips dialog.
3) Confirm the verification code in the Tips dialog.
4) Click and read “Terms of Service” and “Privacy Policy”.
5) Click **Confirm** to enable Hik-Connect service.



NOTE

- If all the devices you selected have enabled the service, the **Enable Hik-Connect** checkbox won’t appear on the Activate the Device panel.
- If some of the device(s) have enabled the service, the **Enable Hik-Connect** checkbox will be solid and uncheckable as ▣.
- The length of verification code ranges from 6 to 12 letters (a to z, A to Z) or numbers (0 to 9). The verification code is case sensitive. You are recommended to use a combination of no less than 8 letters or numbers for the Verification Code.
- The Hik-Connect service requires internet access. Please read the “Terms of Service” and “Privacy Policy” before enabling the service.

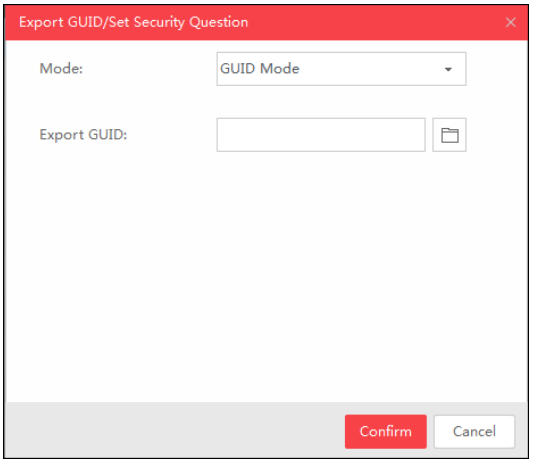
4. Click **Activate** to activate the device.
5. After activation, the confirmation list will pop up, showing the total selected device number, the activation failed number, and the details of each device.



NOTE

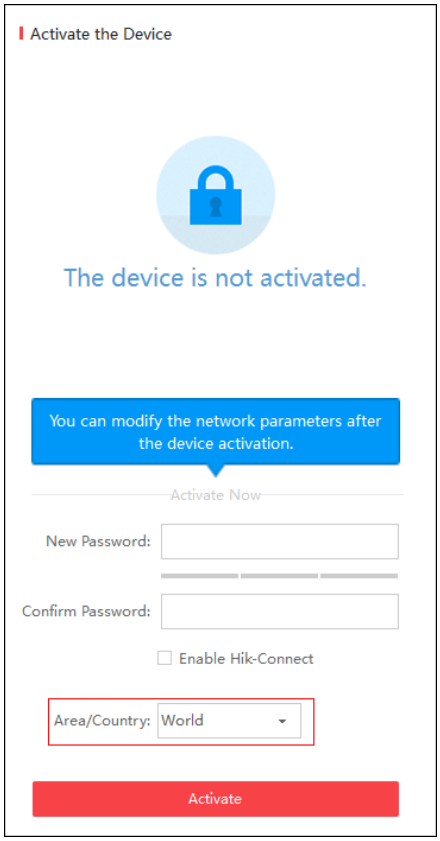
After activation, the devices IP addresses will be set as the default IP: 192.168.1.64. For modifying the IP address, refer to *Chapter 2.3 Modify the Network Parameters*.

6. Optionally, if the devices you selected support resetting password via GUID file or security question, the dialog **Export GUID/Set Security Question** will open. You can export the GUID file of selected devices for further password reset.



   1) (Optional) Select the **GUID Mode.**
   2) Click 🗀 to set the saving path of exported GUID file.
   3) Click **Confirm.**

7. Optionally, if the devices you selected support Wi-Fi, the **Area/Country** will appear. You can select the supported area or country as you desired. The Wi-Fi signal strength is different of different area or country.



NOTE

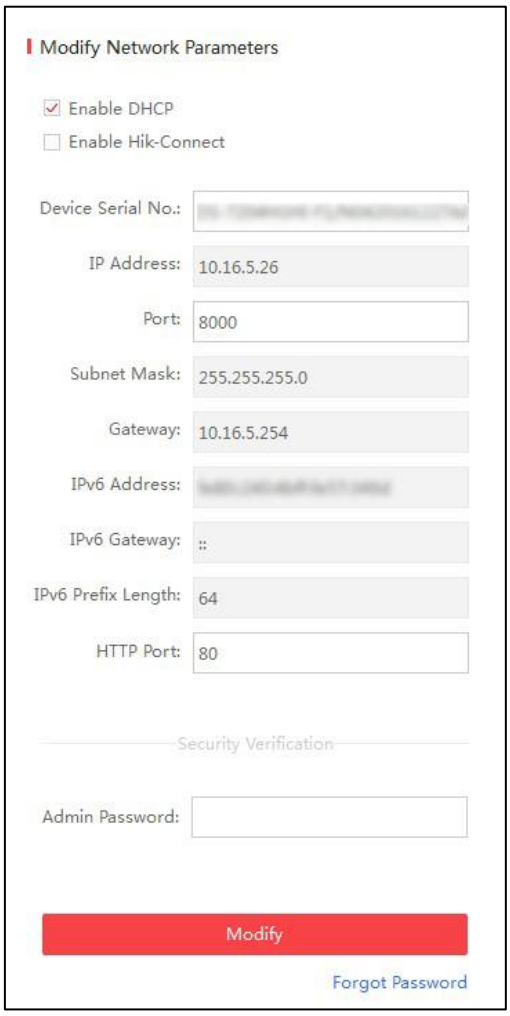
- If the devices you selected support different area or country, the Area/Country is not available.
- If some of the devices you selected do not support Wi-Fi, the Area/Country is not available.

2.3 Modify the Network Parameters

Task 1: Modify Network Parameters of One Device

Steps:

1. Select the device to be modified in the device list by checking the checkbox and the network parameters of the device will be displayed in the **Modify Network Parameters** panel on the right side.
2. If the DHCP function of the device is enabled, you can edit the device's port No. and HTTP port No.. You can also uncheck the **Enable DHCP** checkbox to set the modifiable network parameters (e.g., IP address, subnet mask) manually.



NOTE

You can enable the DHCP function on devices before you activating devices on the software. For details, refer to the User Manuals of the device.

3. If the DHCP function of the device is not enabled, you can set the modifiable network parameters (e.g., IP address, subnet mask) as desired. You can also check **Enable DHCP** checkbox to obtain the IP Address, Subnet Mask, IPv4 Gateway, IPv6 Address and IPv6 Gateway of the device automatically.

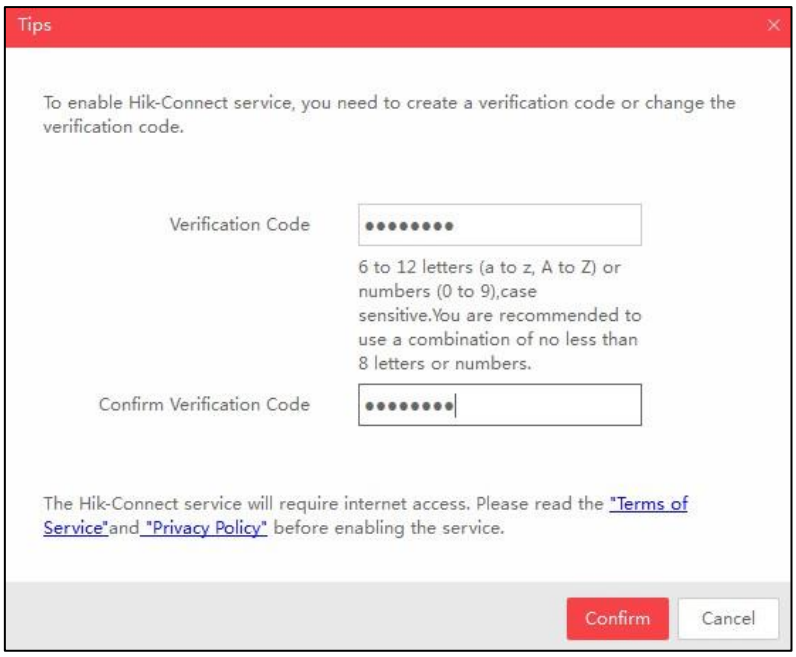
NOTE

- The IPv6 should be supported by the device.
- The DHCP function should be supported by the device and the router that the device connected with.

4. Optionally, if the device you selected supports Hik-Connect service and the service hasn't been enabled, you can check the **Enable Hik-Connect** checkbox to enable Hik-Connect service.

NOTE

If the Hik-Connect function is enabled for the first time, you are required to create a verification code or change the verification code in the dialog shown below when you check the **Enable Hik-Connect** checkbox.



5. Enter the password of the admin account of the device in the Admin Password field and click Modify to modify the parameters.

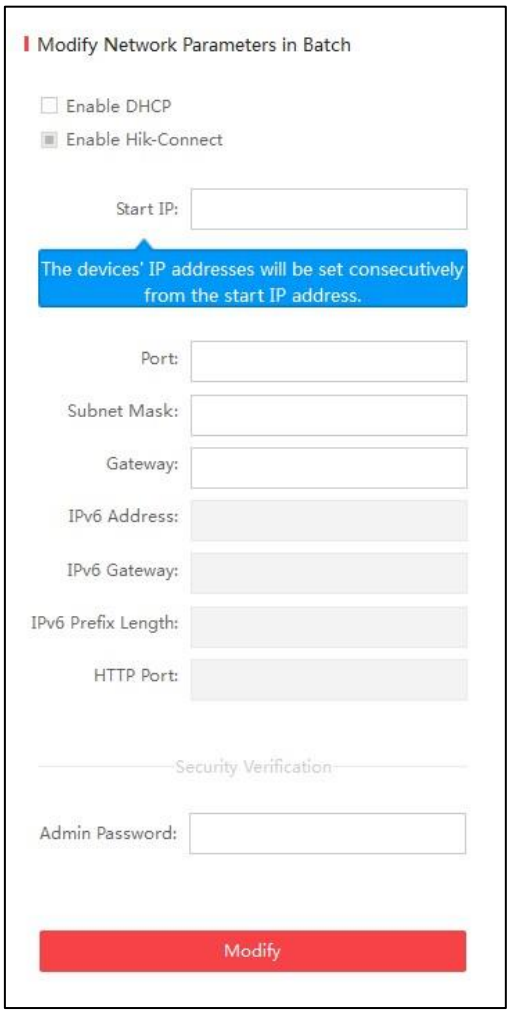
Task 2: Modifying Network Parameters of Multiple Devices

You can modify multiple devices' network parameters which have the same admin password.

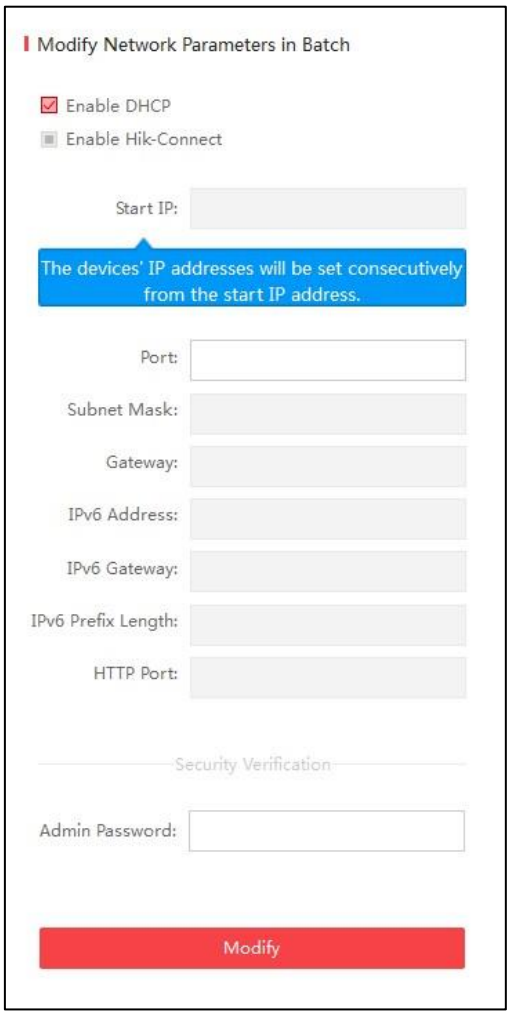
Steps:

1. Select multiple devices to be modified by checking the checkboxes in the device list.
2. In the **Modify Network Parameters in Batch** panel on the right side, edit the modifiable network parameters, e.g. start IP address and port. The devices' IP addresses will be set consecutively from the start IP address and other parameters will be set to the same.

   Example: If you select three devices for modification and set the start IP address as 10.16.1.21, then the IP addresses of the devices will be modified as 10.16.1.21, 10.16.1.22 and 10.16.1.23 in order.



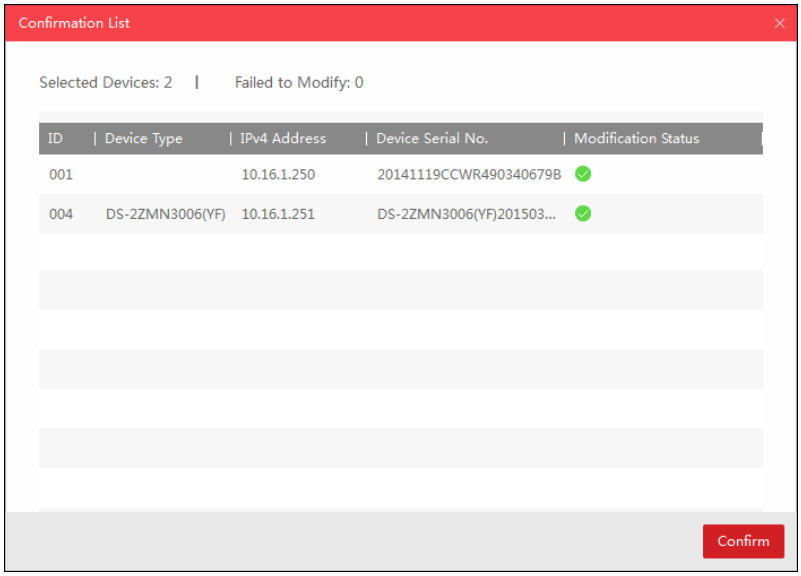
3. Or you can check **Enable DHCP** checkbox to enable the DHCP function for the selected devices. In this way, the IP Address, Subnet Mask, IPv4 Gateway, IPv6 Address and IPv6 Gateway of the devices can be obtained automatically.



NOTE

- The IPv6 should be supported by the device.
- The DHCP function should be supported by the device and the router that the device connected with.

4. Enter the password of the admin account of the devices in the **Admin Password** field and click **Modify** to modify the parameters.
5. After modification, the confirmation list will pop up, showing the total selected device number, the modification failed number, and the details of each device.



NOTE

The software does not support enabling Hik-Connect function in batch after activating device(s). If you select multiple devices in the device list, the **Enable Hik-Connect** checkbox will become solid and uncheckable as ▣.

2.4 Reset Password

Purpose:

You can reset the password if you forget the device's *admin* password.

According to the device, we provide four different methods selectable for resetting the password if you forget the device's *admin* password: **Import File**, **Input Key**, **GUID Mode**, or **Security Question Mode**.

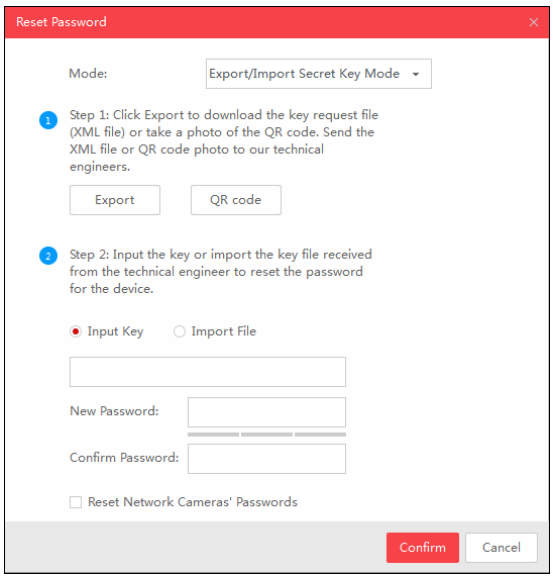
- **Option 1: Import File**

You can export the device's key request file and send it to our technical engineers. Our technical engineer will send you another key file which contains the resetting permission resetting. You can import the key file to reset the password.

This function should be supported by the devices.

Steps:

1. Select the device for resetting the password by checking the checkbox.
2. Click **Forgot Password** to enter the Reset Password interface.



3. Select **Export/Import Secret Key Mode**.
4. Click **Export** button to download the key request file. Set the file path in the pop-up window.
   Click **Select Folder** to save the device key request file on your PC.

   The exported key request file is XML file which is named as **Device Serial No.-System Time**.
5. Send the key request file to our technical engineers and the engineer will send you a key file back.
6. Select **Import File** radio button as the resetting mode.
7. Click to select the key file (XML file) returned by the technical engineer and click **Open**.
8. Input new password in text fields of **New Password** and **Confirm Password**. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

   STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories: **numbers**, **lowercases**, **uppercases** and **special characters**. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*
9. (Optional) You can check the checkbox of **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

   The function should be supported by the device.

10. Click **Confirm** to reset the password.

- **Option 2: Input Key**

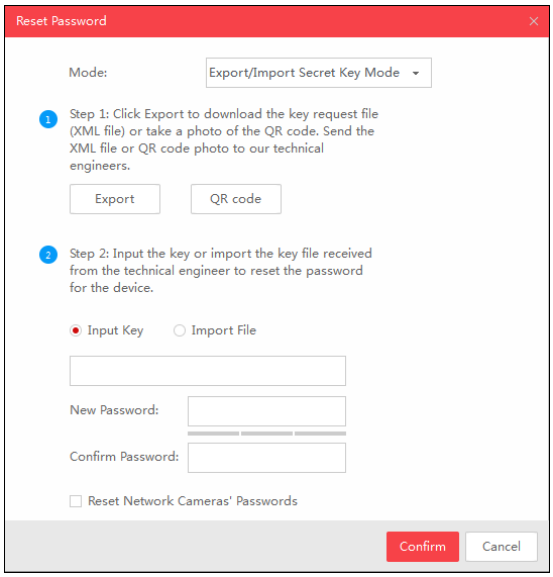
You can take a picture of the device's QR code and send it to our technical engineer. Our technical engineer will send you a key which indicates the resetting permission. You can input the key to reset the password.

NOTE

The function should be supported by the device.

Steps:

1. Select the device for resetting the password by checking the checkbox.
2. Click **Forgot Password** to enter the Reset Password interface.



3. Select **Export/Import Secret Key Mode**.
4. You can use phone to take a picture of the QR code and send the code to our technical engineers. Our engineer will send you a key back.

   NOTE

   The key returned from the technical engineer is an 8-bit character string.
5. Select **Input Key** radio button as the resetting mode.
6. Input the key received from the technical engineer.
7. Input new password in text fields of **New Password** and **Confirm Password**. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

   STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories: **numbers**, **lowercases**, **uppercases** and **special characters**. And we recommend you reset your password regularly, especially in*

the high security system, resetting the password monthly or weekly can better protect your product.

8. (Optional) You can check the checkbox of **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

NOTE

The function should be supported by the device.

9. Click **Confirm** to reset the password.

- **Option 3: Import GUID File**

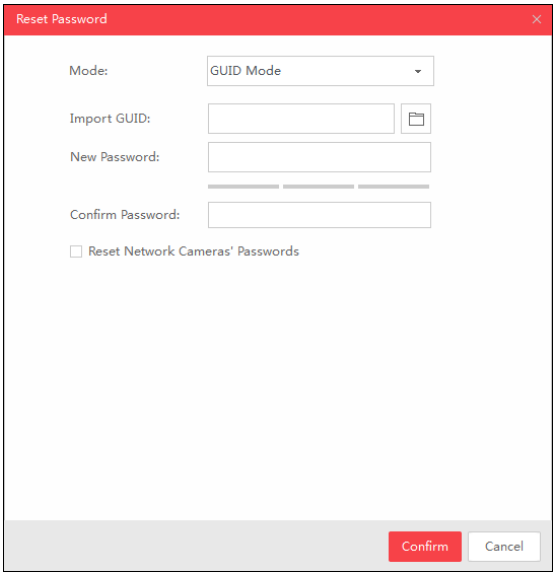
You can import the GUID file of device, which is exported during activation.

NOTE

The function should be supported by the device.

Steps:

1. Select the device for resetting the password by checking the checkbox.
2. Click **Forgot Password** to enter the Reset Password interface.
3. Select **GUID Mode**.



4. Click to select the GUID file, which is exported during activation and click Open.
5. Input new password in text fields of **New Password** and **Confirm Password**. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories: **numbers**, **lowercases**, **uppercases** and **special characters**. And we recommend you reset your password regularly, especially in*

the high security system, resetting the password monthly or weekly can better protect your product.

6. (Optional) You can check the checkbox of **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

NOTE

The function should be supported by the device.

7. Click **Confirm** to reset the password.

- **Option 4: Answer Security Question**

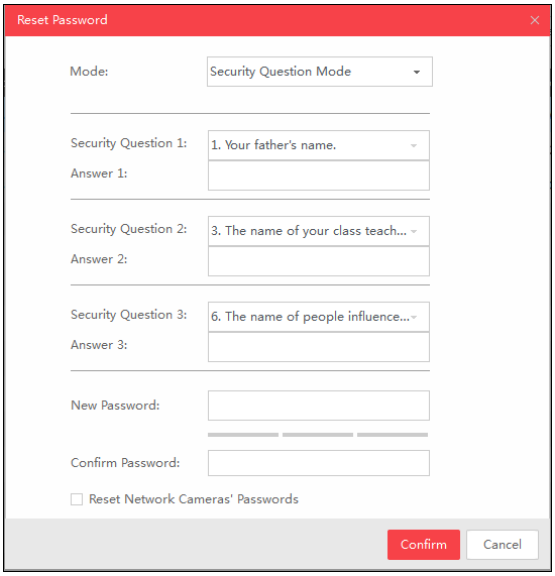
You can answer the security question, which is set during activation.

NOTE

The function should be supported by the device.

Steps:

1. Select the device for resetting the password by checking the checkbox.
2. Click **Forgot Password** to enter the Reset Password interface.
3. Select **Security Question Mode**.



4. Input the correct answer of security question, which is set during activation.
5. Input new password in text fields of **New Password** and **Confirm Password**. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

STRONG PASSWORD RECOMMENDED - *A strong password ranges from 8 to 16 characters, and must contain at least two of the following categories: **numbers**, **lowercases**, **uppercases** and **special characters**. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your*

product.

6. (Optional) You can check the checkbox of **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

NOTE

The function should be supported by the device.

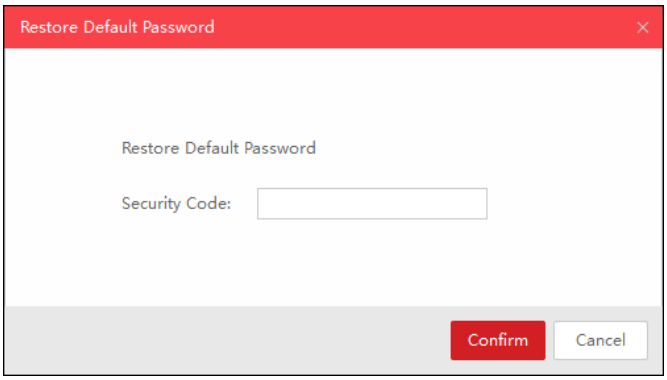
7. Click **Confirm** to reset the password.

NOTE

For some old devices, if you forget the *admin* password of your device, you can restore the default password.

Steps:

1. Send the serial No. of the device which needs password recovery to our technical engineers and you will get a security code.
2. Select the device for restoring default password by checking the checkbox. Click **Forgot Password** to activate the Restore Default Password window.
3. Input the code in the **Security Code** field and click **Confirm** to restore the default password of the device.



- *The default password (12345) for the Admin account is for first-time log-in purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.*
- *We highly recommend you to use a strong password to ensure your data security. A strong password ranges from 8 to 16 characters, and must contain at least three of the following categories: numbers, lowercases, uppercases and special characters.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

First Choice for Security Professionals