



SADP Software for Mac

User Manual

Legal Information and Symbol Conventions

Legal Information

User Manual

©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Please use this user manual under the guidance of professionals.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.




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.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Overview	1
1.1 Introduction	1
1.2 Running Environment	1
Chapter 2 Operate SADP Software	2
2.1 Search Online Devices	2
2.2 Activate Device	3
2.3 Edit Device's Network Parameters	6
2.3.1 Edit Network Parameters of Single Device	6
2.3.2 Edit Network Parameters of Multiple Devices	7
2.4 Reset/Restore Device Password	9
2.4.1 Reset Password by Importing File	9
2.4.2 Reset Password by Entering Key	11
2.4.3 Reset Password by GUID	13
2.4.4 Reset Password by Answering Security Question	15
2.4.5 Reset Password by Sending Email	17
2.4.6 Restore Password	19
2.5 Export Device Information	20
2.6 More Functions	21

Chapter 1 Overview

1.1 Introduction

Search Active Devices Protocol (SADP) software is a user-friendly and installation-free online device search tool.

SADP software searches the online devices within your subnet and displays the information of the devices. You can use this software to edit the network parameters, reset the password, export device information, and so on.

The manual guides you to operate the SADP software. Follow this manual to perform searching device, activating device, editing device's network parameters, resetting device password, etc. To ensure the properness of usage and stability of the SADP software, refer to the contents below and read the manual carefully before installation and operation.

1.2 Running Environment

The recommended running environment for installing the SADP software is as follows.

Operating System

MAC 10.10 (64-bit)

CPU

Intel Pentium IV 3.0 GHz or Above

RAM

1 GB or Above

Video Card

RADEON X700 Series

Display

1024*768 Resolution or Above

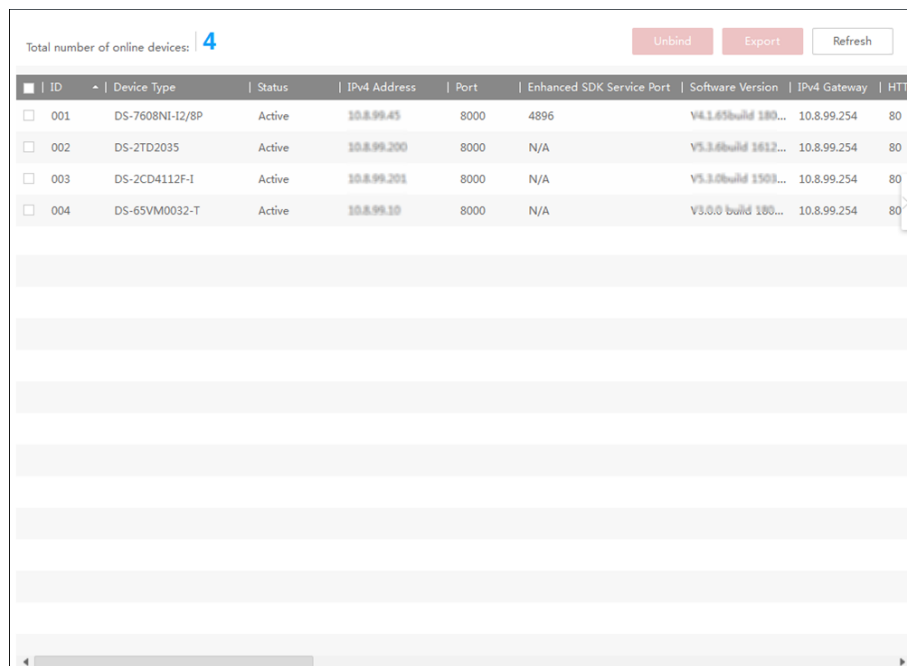
Chapter 2 Operate SADP Software

After installing and running the SADP software, you can use the software to search device, activate device, reset device password, etc.

2.1 Search Online Devices

SADP software can automatically search the online devices within subnet every 1 minute. You can also refresh the device list manually to add the newly found devices or delete the offline devices.

The information of searched device(s), including the total number, device type, IP address, port number, gateway, etc. will be displayed in the device list.



Total number of online devices: 4

ID	Device Type	Status	IPv4 Address	Port	Enhanced SDK Service Port	Software Version	IPv4 Gateway	HTTP
001	DS-7608NI-12/8P	Active	10.8.99.45	8000	4896	V4.1.65build 180...	10.8.99.254	80
002	DS-2TD2035	Active	10.8.99.200	8000	N/A	V5.1.6build 1612...	10.8.99.254	80
003	DS-2CD4112F-1	Active	10.8.99.201	8000	N/A	V5.1.0build 1503...	10.8.99.254	80
004	DS-65VM0032-T	Active	10.8.99.10	8000	N/A	V3.0.0 build 180...	10.8.99.254	80

Figure 2-1 Search Online Devices

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.

2.2 Activate Device

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

Perform this task to activate the device(s).

Steps

Note

This function should be supported by the device and the parameters displayed on Activate the Device panel may vary for different devices.

1. Check the device status (shown on **Status** column) and select the inactive device(s).



ID	Device Type	Status	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	
005	DS-2CD1121-I	Active	192.168.1.64	8000	...	192.168.1.1	80	
<input checked="" type="checkbox"/>	006	DS-2CD1321-I	Inactive	192.168.1.64	8000	...	192.168.1.1	80
<input type="checkbox"/>	001	DS-7004HUI-F2/S	Active	10.16.5.112	8000	...	10.16.5.254	80
<input type="checkbox"/>	002	DS-8106THFH-E2/RW	Active	10.16.5.112	8000	...	10.16.5.254	N/A
<input type="checkbox"/>	003	STORAGE-SERVER	Active	10.16.5.106	8003	...	N/A	

Figure 2-2 Select Inactive Device

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

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. **Optional:** For NVR device connected with the inactive network camera(s), create a password in **Channel Password** field for activating the network camera(s) via NVR.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password:

Confirm Password:

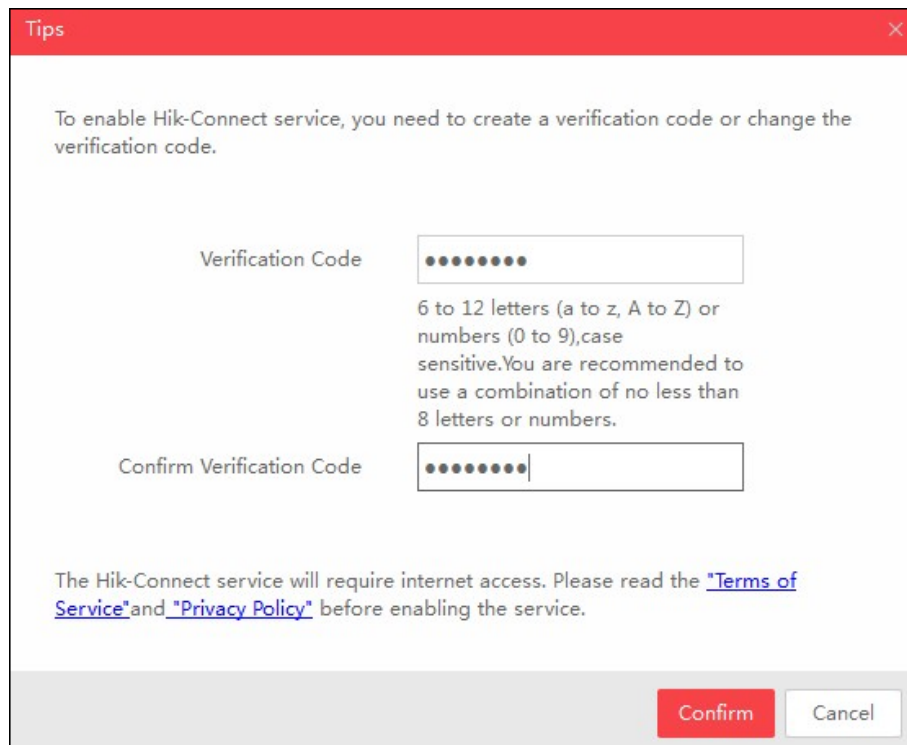
Channel Password:

Enable Hik-Connect

Activate

Figure 2-3 Set Channel Password

- 4. Optional:** For the device which supports Hik-Connect service, enable this function as follows.
- 1) Check **Enable Hik-Connctet** checkbox to open the Tips dialog.
 - 2) Create a verification code and confirm it for adding your device to the Hik-Connect app.
 - 3) Click and read **Terms of Service** and **Privacy Policy**.
 - 4) Click **Confirm** to enable Hik-Connect service.



The screenshot shows a 'Tips' dialog box with a red title bar. The main text reads: 'To enable Hik-Connect service, you need to create a verification code or change the verification code.' Below this, there are two input fields. The first is labeled 'Verification Code' and contains seven dots. To its right, the text specifies: '6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.' The second input field is labeled 'Confirm Verification Code' and contains seven dots with a cursor at the end. At the bottom of the dialog, there is a red 'Confirm' button and a white 'Cancel' button. A note at the bottom states: 'The Hik-Connect service will require internet access. Please read the ["Terms of Service"](#) and ["Privacy Policy"](#) before enabling the service.'

Figure 2-4 Enter Verification Code

5. **Optional:** For the device which supports Wi-Fi, 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.

6. **Optional:** For the device which supports Wi-Fi, set the Wi-Fi parameters to connect the wireless network.
- 1) Click **Set Wi-Fi**.
 - 2) Enter the Wi-Fi network name and password.
 - 3) **Optional:** Click **Verify** to test the Wi-Fi network connection.
 - 4) Click **Save** to save the settings.
 - 5) Click **Back** to go back the Activate page.
7. Click **Activate** to activate the device.

 **Note**

If the device(s) you selected supports resetting password via GUID file, security question or Email, you need to export the GUID file, set the security question or set reserved Email address for further password reset.

After activation, the device IP address will be set as the default IP: 192.168.1.64. For modifying the IP address, refer to **Edit Device's Network Parameters**.

2.3 Edit Device's Network Parameters

After activating device, you can edit the network parameters for one online device, or multiple online devices at the same time.

2.3.1 Edit Network Parameters of Single Device

You can edit the network parameters for one device, such as IP address, port, subnet mask or other parameters.

Before You Start

Make sure the device status is activate.

Perform this task to edit the network parameters for one device.

Steps

1. Select one device to be edited in the device list .

The network parameters of the device will be displayed in the Modify Network Parameters panel on the right side.

2. **Optional:** Check **Enable DHCP** to obtain the IP Address, Subnet Mask, IPv4 Gateway, IPv6 Address and IPv6 Gateway of the device automatically.



Note

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

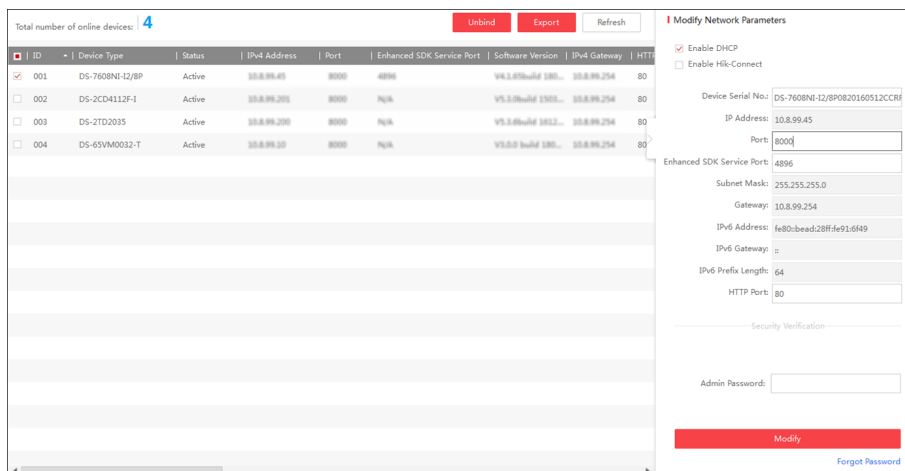


Figure 2-5 Edit Network Information of Single Device

3. **Optional:** Check **Enable Hik-Connect** to enable Hik-Connect function.

 **Note**

- This function should be supported by the device, or the checkbox is invalid.
 - If the function Hik-Connect is enabled for the first time, you are required to create a verification code or change the verification code in the dialog when you check **Enable Hik-Connect**.
-

4. Edit the network parameters as you desired.
 - If the DHCP function of the device is enabled, you can edit the device's port No., enhanced SDK service port No. or HTTP port No..
 - 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.
-

 **Note**

The IPv6 should be supported by the device.

5. Enter the password of the admin account of the device in the **Admin Password** field.
6. Click **Modify** to modify the parameters.

2.3.2 Edit Network Parameters of Multiple Devices

You can edit the network parameters of multiple devices with the same admin password.

Before You Start

Make sure the device status is activate.

Perform this task to edit the network parameters for multiple devices.

Steps

1. Select multiple devices to be edited in the device list.

Modify Network Parameters in Batch

Enable DHCP
 Enable Hik-Connect

Start IP:

The devices' IP addresses will be set consecutively from the start IP address.

Port:
Subnet Mask:
Gateway:
IPv6 Address:
IPv6 Gateway:
IPv6 Prefix Length:
HTTP Port:

Security Verification

Admin Password:

Modify

Figure 2-6 Edit Network Parameters of Multiple Devices

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. **Optional:** Check **Enable DHCP** to enable the DHCP function for the selected devices.
In this way, the IP Address, Subnet Mask, IPv4 Gateway, IPv6 Address and IPv6 Gateway and 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.
 5. Click **Modify** to modify the parameters.
-

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** will become solid and uncheckable.

2.4 Reset/Restore Device Password

You can reset the password or restore the password to the default password if you forget the device's admin password. According to the device, we provide five different methods selectable for resetting the password: importing file, entering key, GUID, answering security question and sending Email.

2.4.1 Reset Password by Importing File

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

Perform this task to reset device password by importing file.

Steps

Note

This function should be supported by the devices.

1. Select the device for resetting the password.
 2. Click **Forgot Password** to open Reset Password window.
 3. Select **Export/Import Secret Key Mode**.
 4. Download the key request file.
 - 1) Click **Export**.
 - 2) Set the file saving path.
 - 3) Click **Select Folder** to save the device key request file on your PC.
-

Note

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.

The engineer will reply you a key file back.
6. Select **Import File** as the password resetting mode.

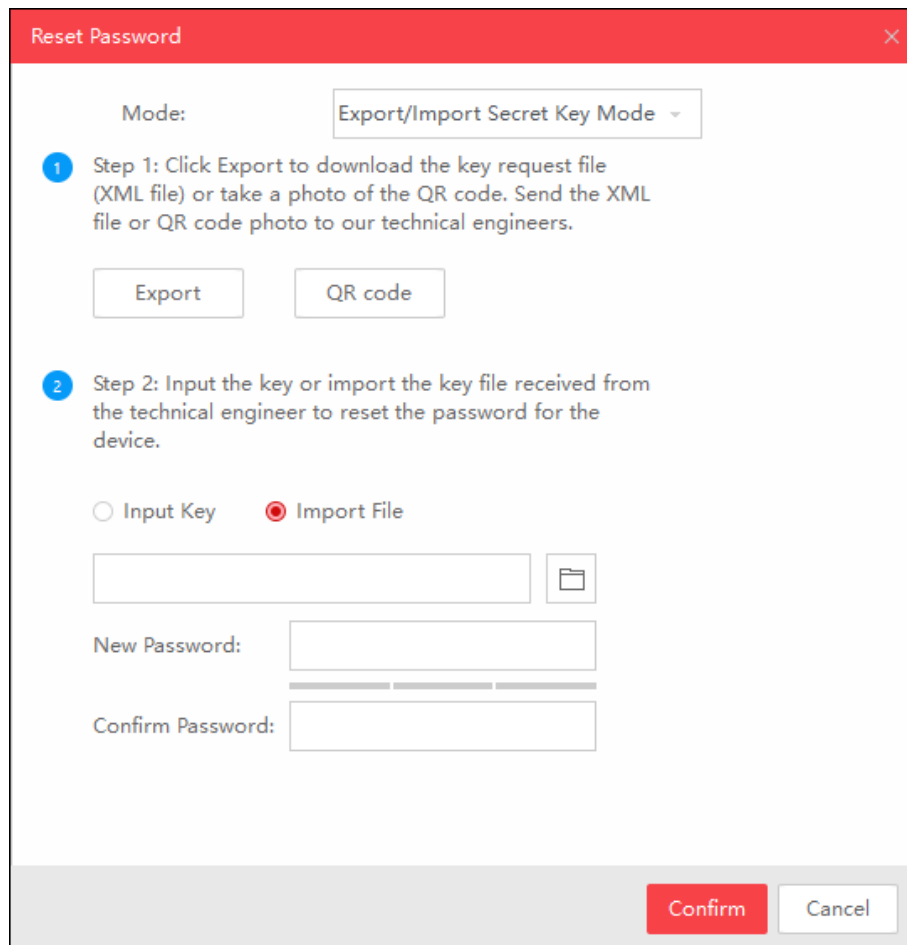



Figure 2-7 Reset Password by Importing File

7. Click  to select the key file (XML file) returned by the technical engineer and click **Open**.
8. Enter new password in text fields of **New Password** and **Confirm Password**.

The system will check password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

-
9. Check **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

 **Note**

This function should be supported by the device.

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

2.4.2 Reset Password by Entering Key

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

Perform this task to reset device password by entering key.

Steps

 **Note**

This function should be supported by the devices.

1. Select the device for resetting the password.
2. Click **Forgot Password** to open Reset Password window.
3. Select **Export/Import Secret Key Mode**.
4. Take a picture of the QR code and send the picture to our technical engineers.

Our engineer will reply you a key back.

 **Note**

The key returned from the technical engineer is an 8-bit character string.

5. Select **Input Key** as the password resetting mode.

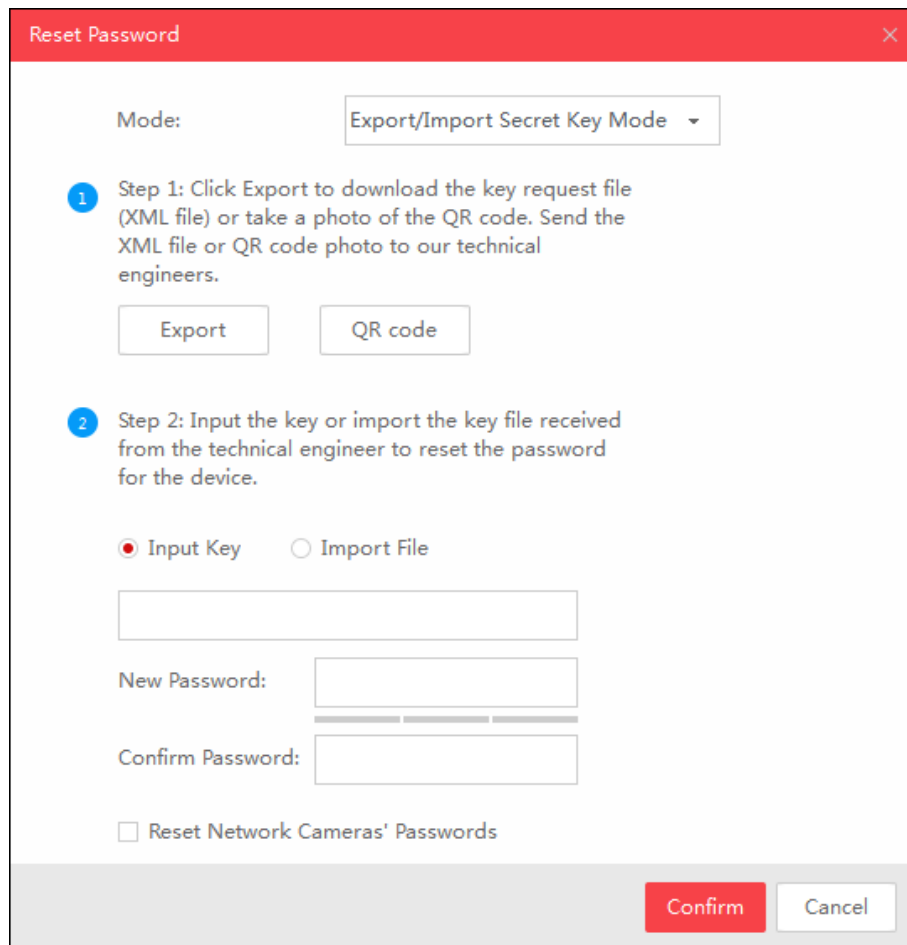


Figure 2-8 Reset Password by Entering Key

6. Enter the key received from the technical engineer.
7. Enter new password in text fields of **New Password** and **Confirm Password**.

The system will check password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

8. **Optional:** Check **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

 **Note**

This function should be supported by the device.

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

2.4.3 Reset Password by GUID

For resetting password of some devices (e.g. NVR), you can import the GUID file of device, which is exported during activation.

Before You Start

Make sure you have downloaded GUID file to local PC when activating the device.

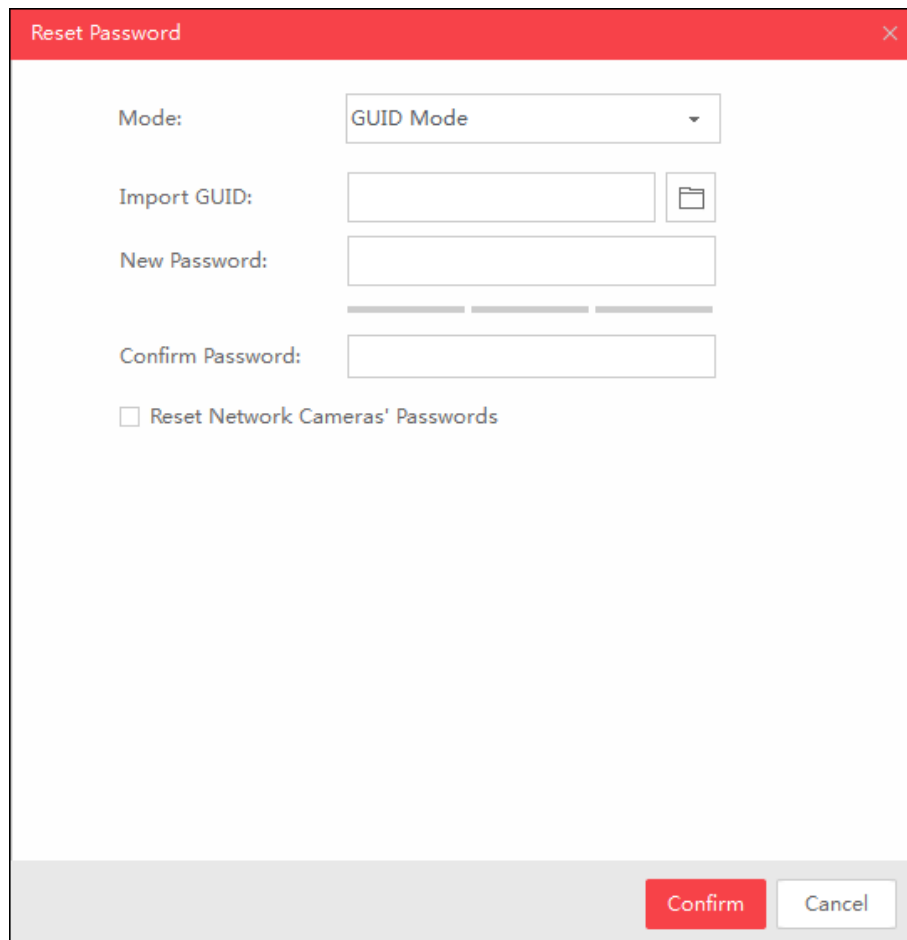
Perform this task to reset device password by GUID.

Steps

 **Note**

This function should be supported by the devices.

1. Select the device for resetting the password.
2. Click **Forgot Password** to open Reset Password window.
3. Select **GUID Mode**.



The screenshot shows a 'Reset Password' dialog box with the following elements:

- Mode:** A dropdown menu currently showing 'GUID Mode'.
- Import GUID:** A text input field followed by a folder icon for file selection.
- New Password:** A text input field.
- Confirm Password:** A text input field.
- Reset Network Cameras' Passwords**
- Buttons:** 'Confirm' (red) and 'Cancel' (white) buttons at the bottom right.

Figure 2-9 Reset Password by GUID

- Click  to select the GUID file, which is exported during activation and click **Open**.
- Enter new password in text fields of **New Password** and **Confirm Password**.

The system will check password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- Optional:** Check **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

 **Note**

This function should be supported by the device.

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

2.4.4 Reset Password by Answering Security Question

If you have set some security questions when activating the device, you can answer the security questions for resetting password.

Before You Start

Make sure you have set the security questions when activating the device.

Perform this task to reset device password by answering security question.

Steps

 **Note**

This function should be supported by the devices.

1. Select the device for resetting the password.
2. Click **Forgot Password** to open Reset Password window.
3. Select **Security Question Mode**.

Reset Password

Mode: Security Question Mode

Security Question 1: 1. Your father's name.

Answer 1:

Security Question 2: 3. The name of your class teach...

Answer 2:

Security Question 3: 6. The name of people influence...

Answer 3:

New Password:

Confirm Password:

Reset Network Cameras' Passwords

Confirm Cancel

Figure 2-10 Reset Password by Answering Security Question

4. Enter the correct answer of the security question, which is set during activation.
5. Enter new password in text fields of **New Password** and **Confirm Password**.

The system will check password strength automatically, and we highly recommend you to use a strong password to ensure your data security.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.

 **Note**

This function should be supported by the device.

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

2.4.5 Reset Password by Sending Email

If you have set the Email address when activating the device and forgot the device password, you can send the QR code picture or XML file to the specified Email address ,and then receive an Email with the verification code in your reserved Email address, which is used to reset password.

Before You Start

Make sure that you have set reserved Email address when activating the device.

Perform this task to reset device password by sending Email.

Steps

 **Note**

This function should be supported by the device.

1. Select the device for resetting the password.
2. Click **Forgot Password** to open Reset Password window.
3. Select **Reserved Email**.

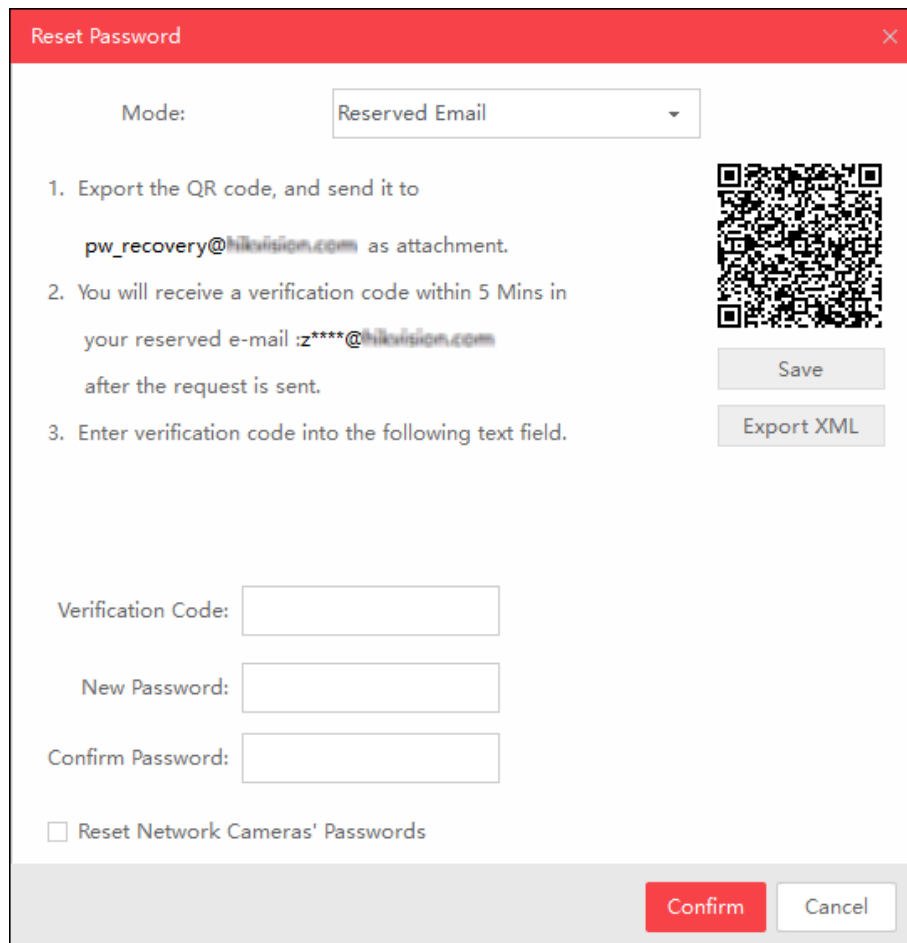


Figure 2-11 Reset Password by Sending Email

4. Click **Save** or **Export XML** to download the QR code picture or XML file to local PC and then send it to the specified Email address.

 **Note**

You will receive an Email with the verification code for resetting the password.

5. Enter the received verification in **Verification Code** field.
6. Enter the new password in fields of **New Password** and **Confirm Password**.

The system will check password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special

characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- 7. Optional:** Check **Reset Network Cameras' Passwords** to reset the connected network cameras' passwords to the same one.
-



Note

This function should be supported by the device.

- 8.** Click **Confirm** to reset the password.

2.4.6 Restore Password

For some old version devices, if you forget the admin password of the searched devices, you can restore the device's default password.

Perform this task to restore device password.

Steps

- Send the serial No. of the device which needs password recovery to our technical engineers.
You will get a security code.
- Select the device in the device list for restoring default password.
- Click **Forgot Password** to open Restore Default Password window.

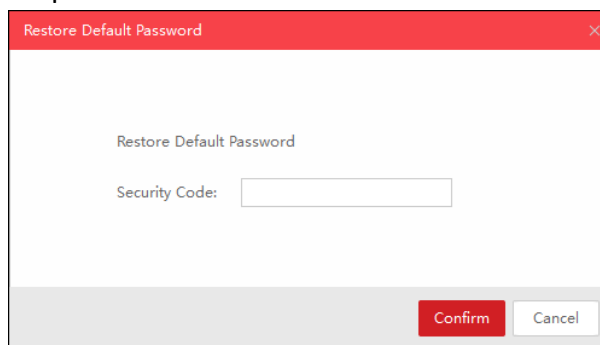


Figure 2-12 Restore Default Password

- Enter the security code in the **Security Code** field.
 - Click **Confirm** to restore the default password of the device.
-



Note

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.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

2.5 Export Device Information

You can save the information of the searched devices as a CSV file, including device type, IP address, port, software version and so on.


Perform this task to export device information.

Steps

1. Select the device(s).
2. Click **Export** to open the Export CSV window.



Figure 2-13 Export Device Information

3. Enter the file name.
4. Click  to set the saving path.
5. Click **Confirm** to save the information as CSV file.

2.6 More Functions

There are some more functions supported by SADP software, such as unbinding Hik-Connect account, ordering device list, adjusting heading sequence, etc.

Unbinding Hik-Connect Account

If you want to delete the device from Hik-Connect account, you can select the device which supports Hik-Connect service from the device list, click **Unbind**, and enter **User Name**, **Password** and **Verification Code** to delete the device from Hik-Connect account.

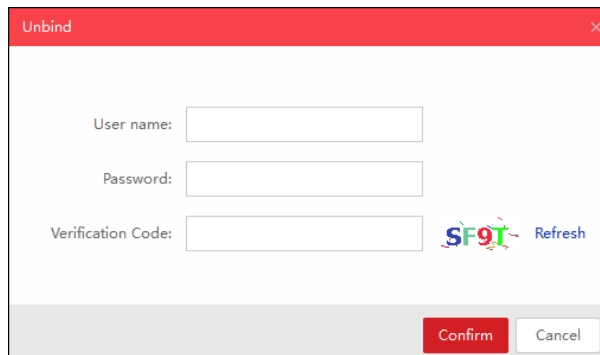




Figure 2-14 Unbind Hik-Connect Account

Ordering Device List

You can click  or  on each column heading to move down or move up the device list.

Adjusting Heading Sequence

You can click and drag the column heading to change the heading sequence.

Accessing Device via Web Browser

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.



See Far, Go Further