http://www.vikylin.com

VKTOOL Software

User Manual

Legal Information and Symbol Conventions

Legal Information

About this Manual

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 of this Manual at the company website Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks Acknowledgement

Trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL OUR COMPANY 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, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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 Introduction

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

VKTOOL 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 VKTOOL 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 VKTOOL 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 VKTOOL software is as follows.

Operating System

Microsoft Windows 10/Windows 8/Windows 8.1/Windows 7/Windows 2008 (32-bit or 64-bit)

Microsoft Windows XP/Windows 2003 (32-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

1.3 Summary of Changes

The followings are the changes of different versions.

V3.0.3

Support prompt about remaining attempts and locking time for failed password reset. See ***Reset Password by Secret Key*** , ***Reset Password by GUID*** , ***Reset Password by Answering Security Question*** , and ***Reset Password by Sending Email*** .

V3.0.2

- Support filtering the detected online devices. See ***Search Online Devices*** for details.
- Support switching language and area. See ***More Functions*** for details.
- Support auto check for upgrade. See ***More Functions*** for details.

V3.0.0

- Support resetting password by sending Email.
- Support unbinding Guarding Vision account.
- Support setting Wi-Fi password when activating the device which supports Wi-Fi.
- Support default channel password setting for activating network camera(s) via NVR device.

Chapter 2 Operate VKTOOL Software

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

2.1 Search Online Devices

VKTOOL 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.

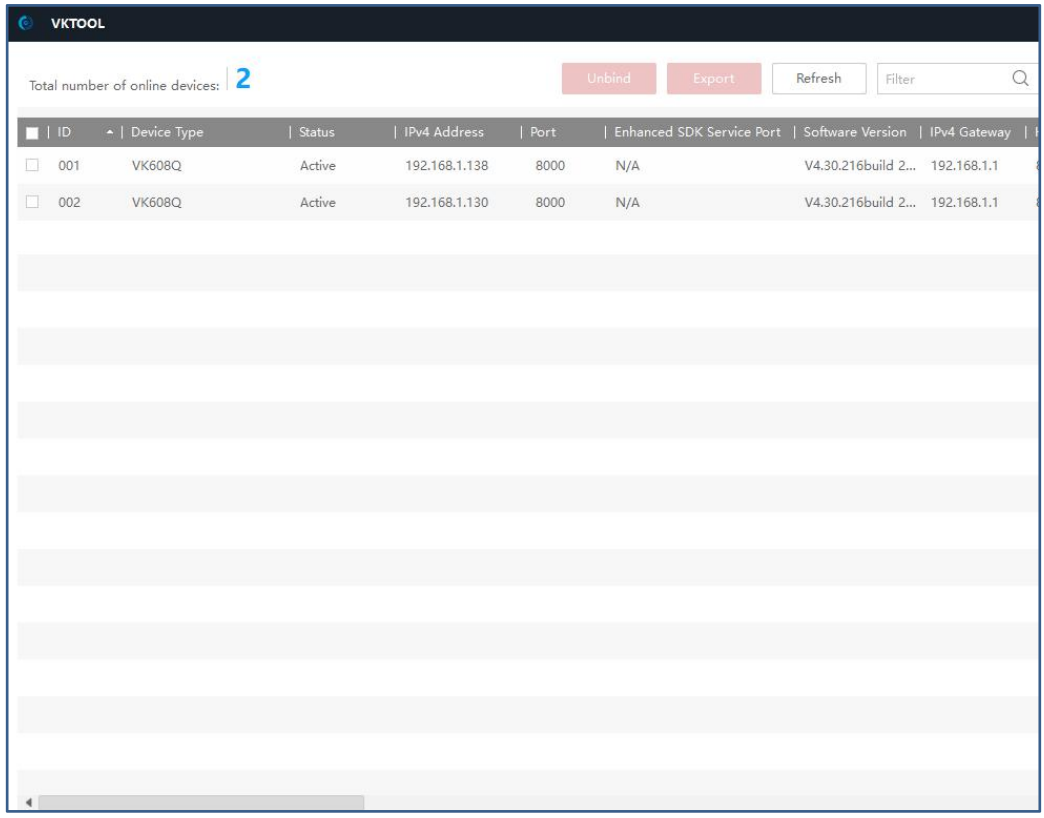

Figure 2-1 Search Online Devices

Note

- The software can automatically search and display the online devices within the subnet every 1 minute. You can also click **Refresh** to manually refresh the device list.
- The device will be removed from the list automatically if it is offline for over 3 minutes.

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).

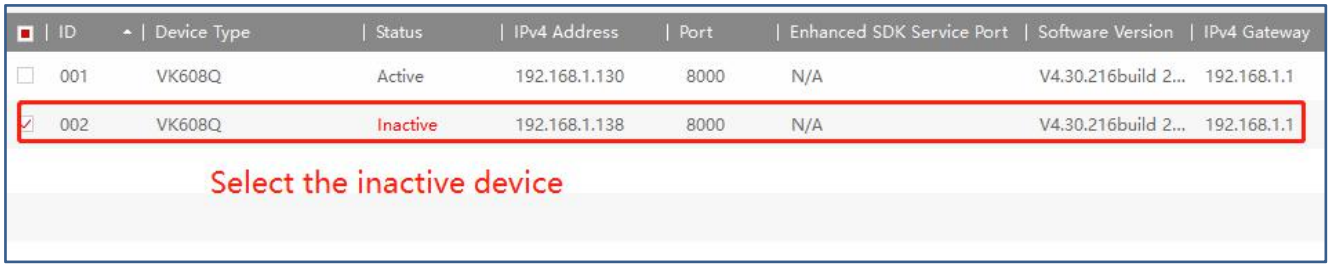

Figure 2-2 Select Inactive Device

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 change your password regularly, especially in the high security system, changing 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.

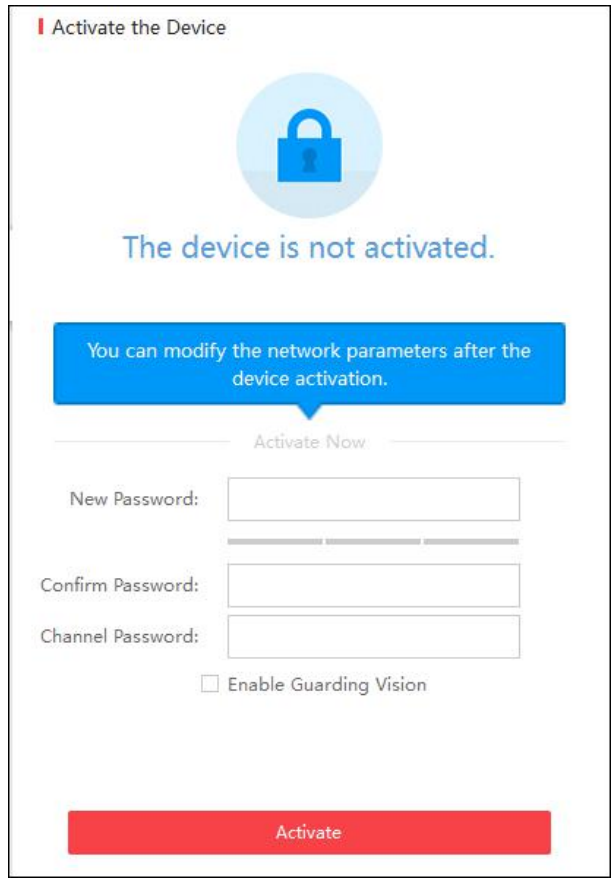

Figure 2-3 Set Channel Password

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

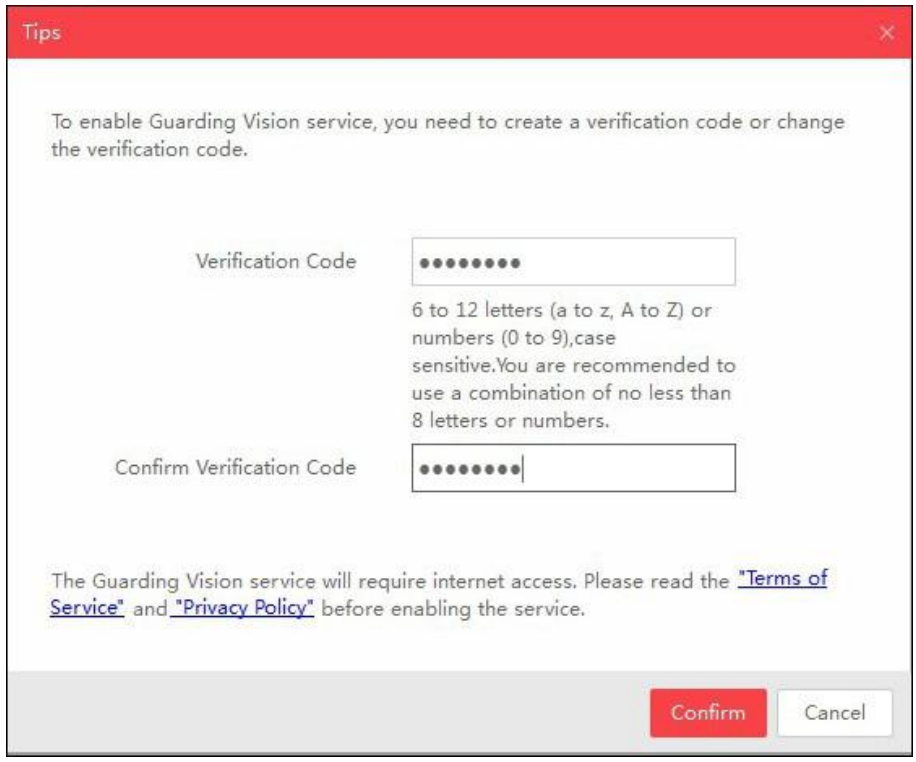

Figure 2-4 Enter Verification Code

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.

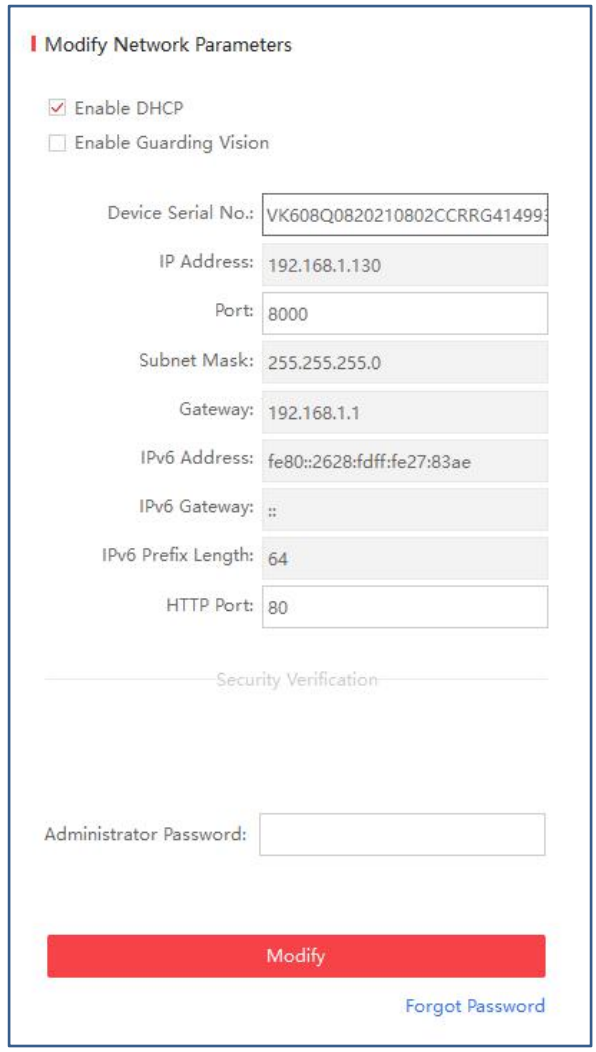

Figure 2-5 Edit Network Information of Single Device

3. **Optional:** Check **Enable Guarding Vision** to enable Guarding Vision function.

Note

- This function should be supported by the device, or the checkbox is invalid.
- If the function Guarding Vision 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 Guarding Vision**.

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.

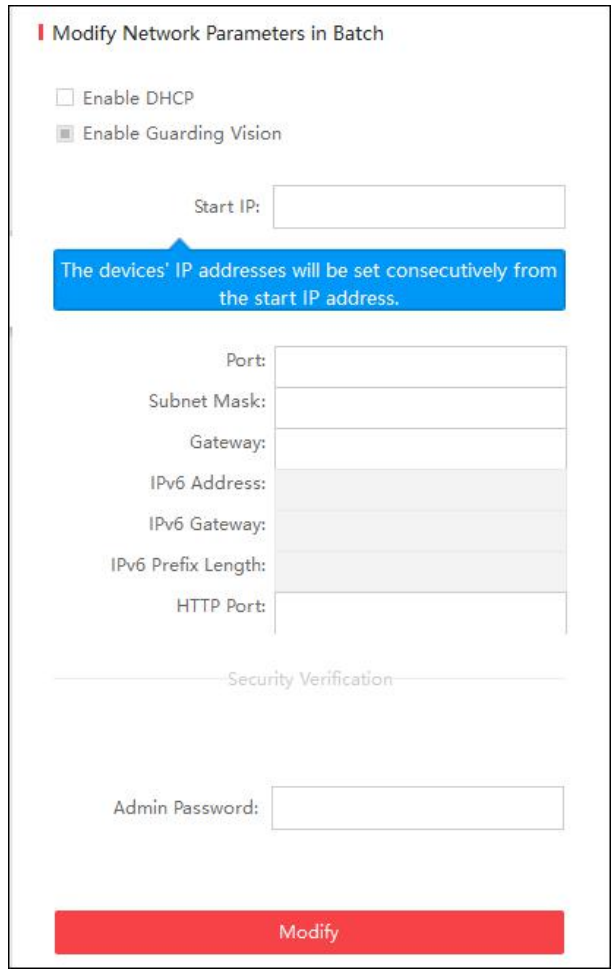

Figure 2-6 Edit Network Parameters of Multiple Devices

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 Guarding Vision function in batch after activating device(s). If you select multiple devices in the device list, the **Enable Guarding Vision** 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 Secret Key

You can export the device's key request file or copy device's QR code picture and send it to our technical engineers. Our technical engineer will reply you a secret key information. You can import the key file or enter the key to reset the password.

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. Click **Export** or **QR code** to download the key request file or copy the QR Code picture.

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 to get secret key information.
6. Select **Import File** or **Input Key** as the password resetting mode.

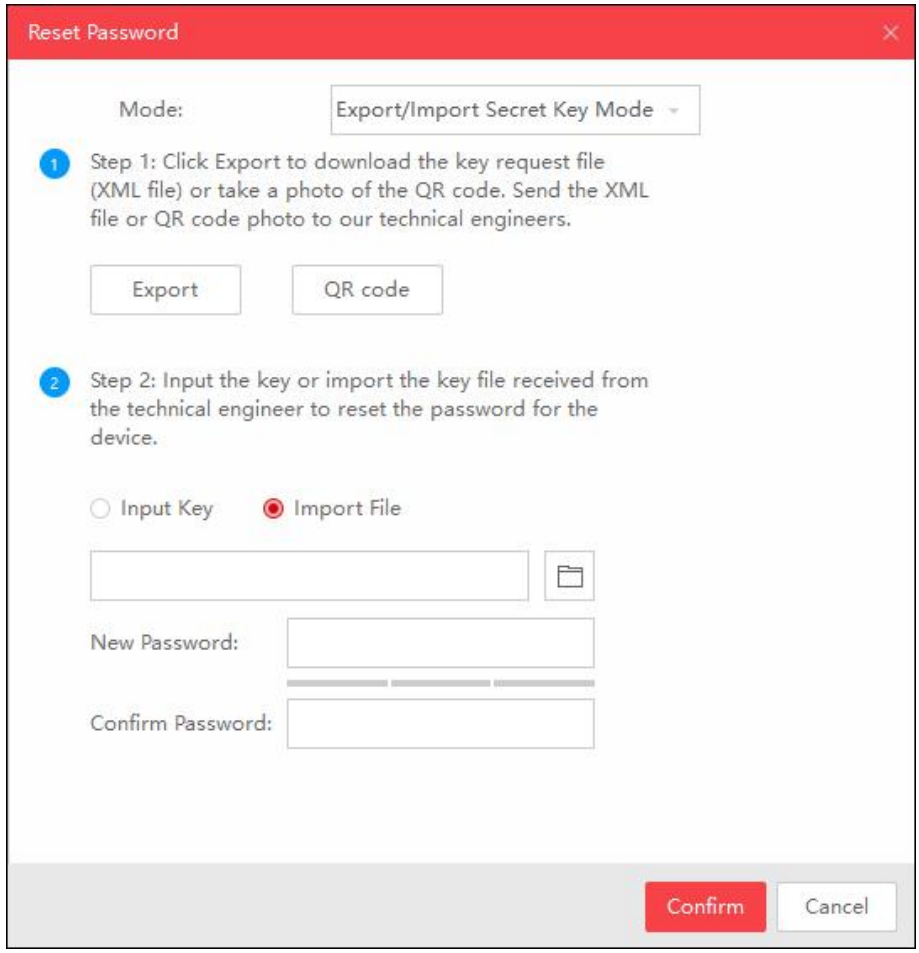

Figure 2-7 Import File

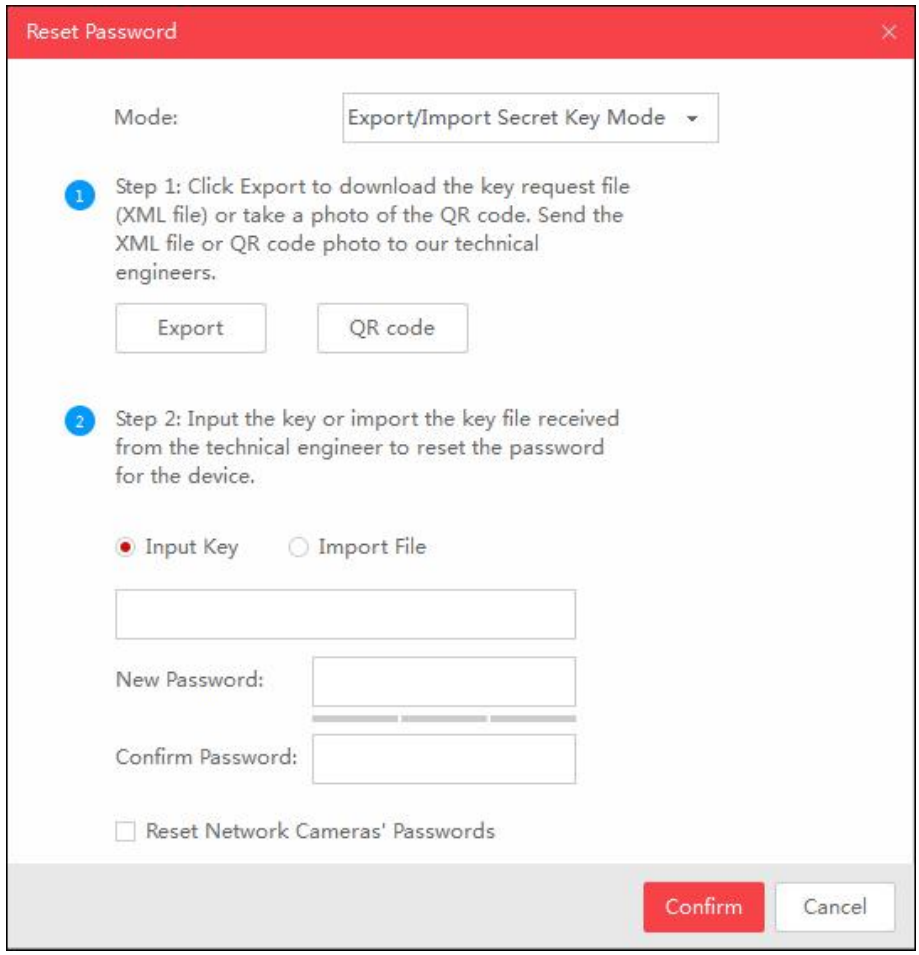

Figure 2-8 Enter Key

7. Click and select the key file or enter the key.
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 change your password regularly, especially in the high security system, changing 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. **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.

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

Note

If resetting password failed, you can see the remaining attempts. When the failed times reach the limit, the account will be locked and you can see the remaining locking time.

2.4.2 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**.

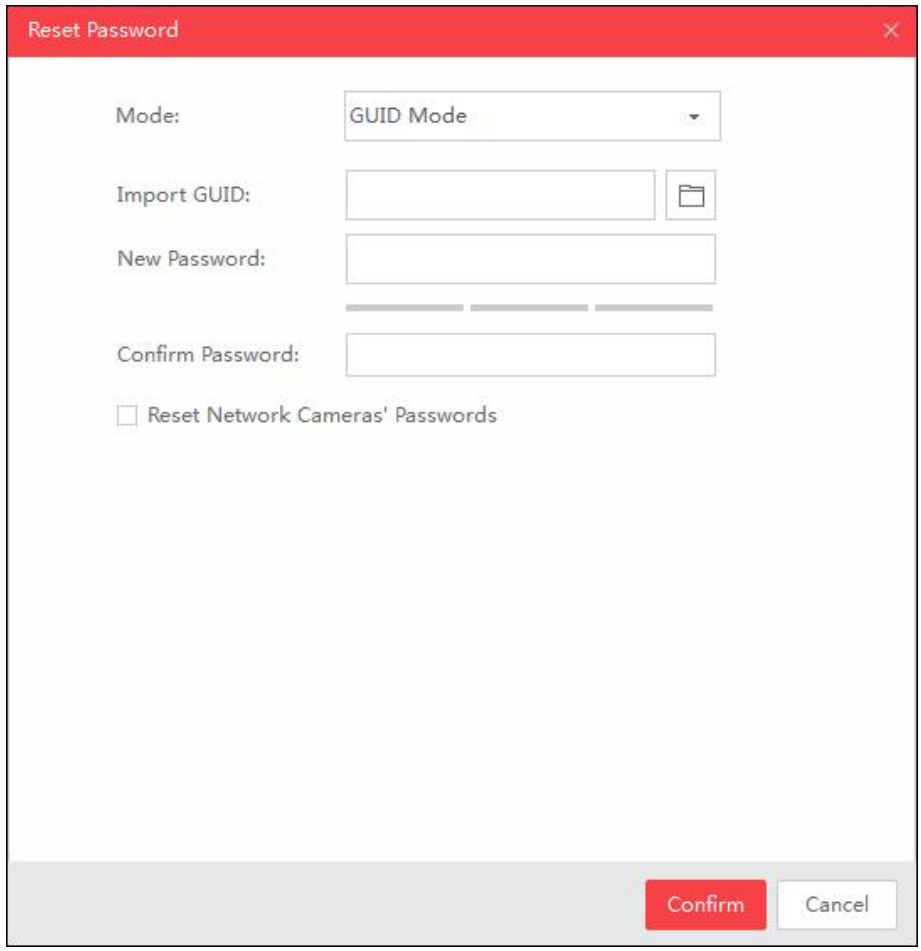

Figure 2-9 Reset Password by GUID

4. Click to select the GUID file, which is exported during activation and click **Open**.
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 change your password regularly, especially in the high security system, changing 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.

Note

If resetting password failed, you can see the remaining attempts. When the failed times reach the limit, the account will be locked and you can see the remaining locking time.

2.4.3 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**.

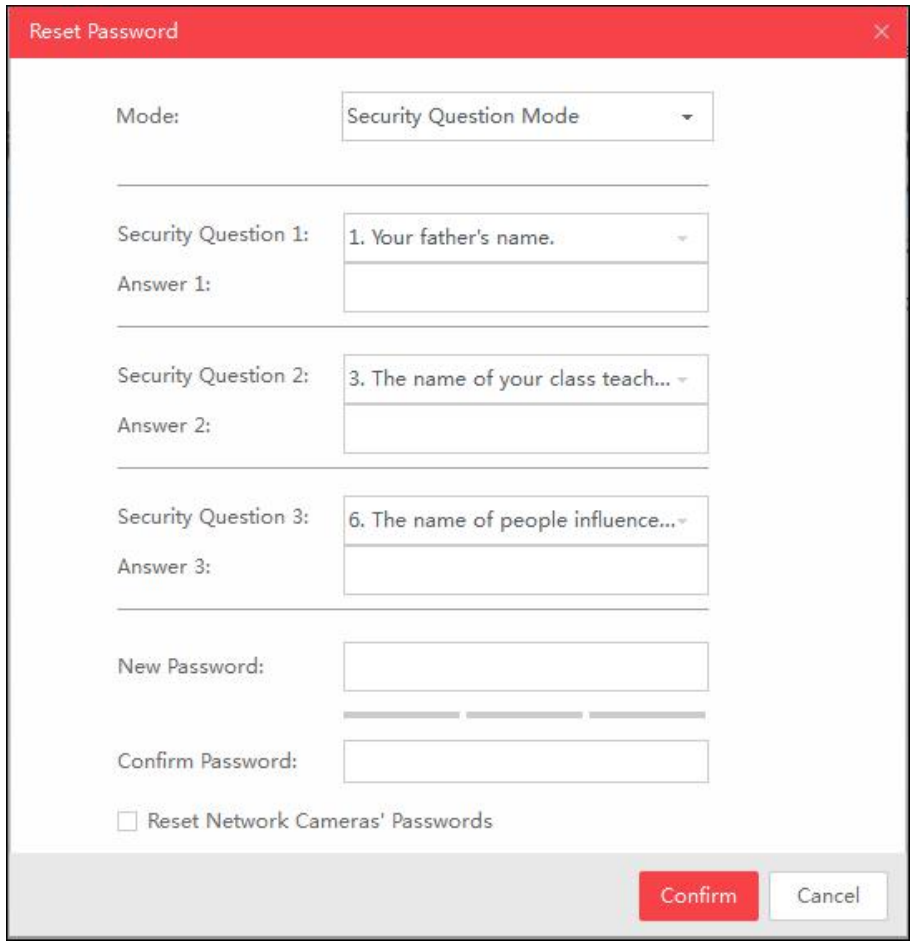

Figure 2-10 Reset Password by Answering Security Question

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 change your password regularly, especially in the high security system, changing 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.

Note

If resetting password failed, you can see the remaining attempts. When the failed times reach the limit, the account will be locked and you can see the remaining locking time.

2.4.4 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**.

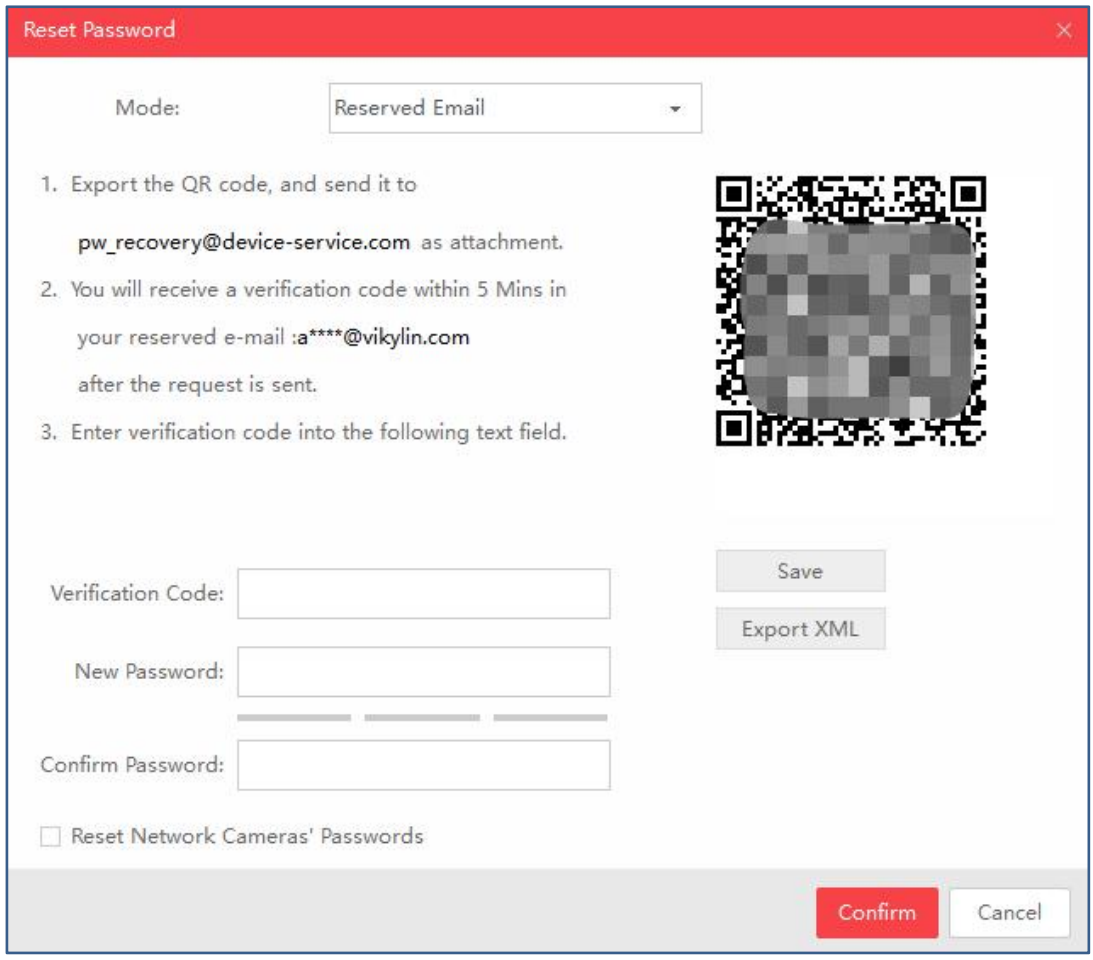

Figure 2-11 Reset Password by Sending Email

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 change your password regularly, especially in the high security system, changing 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.

Note
If resetting password failed, you can see the remaining attempts. When the failed times reach the limit, the account will be locked and you can see the remaining locking time.

2.4.5 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

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

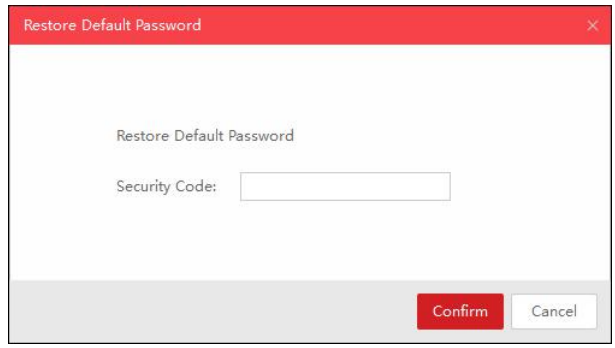

Figure 2-12 Restore Default Password

4. Enter the security code in the **Security Code** field.
5. 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 change your password regularly, especially in the high security system, changing 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 Unbind Guarding Vision Account

If the device is added to Guarding Vision account, you can unbind it from the account via VKTOOL software.

Note

For some areas with specialized servers such as Russia, you should switch area before unbinding Guarding Vision account. For details, refer to ***More Functions*** .

From the device list, select the device which Guarding Vision service is enabled for and has been added to Guarding Vision account, and click **Unbind** to perform the operations as follows:

- Method 1: For the device which supports unbinding function, enter device **Password** (admin user) to unbind the device from Guarding Vision account.
- Method 2: For the device which does not support unbinding function, enter **User Name**, **Password** and **Verification Code** to unbind the device from Guarding Vision account.

2.7 More Functions

There are some more functions supported by VKTOOL software, such as ordering device list, adjusting heading sequence, switching language, etc.

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.

Switch Language/Area

Click on the top right corner of the Home Page to switch language (English or Simplified Chinese) and area (Russia or Other)


VIKYLIN
VIKYLIN