

# IDMVS Client Software Installation and Operation

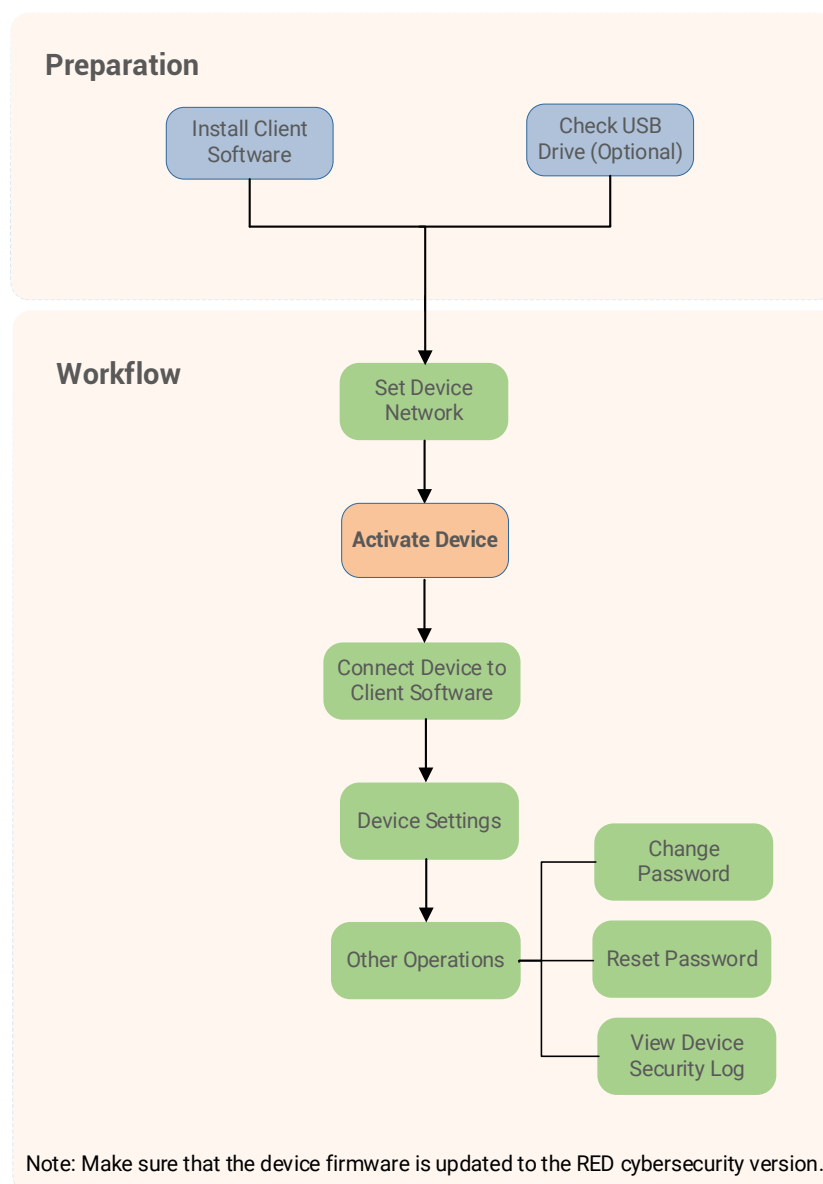
Quick Start Guide

# Chapter 1 Workflow

## Note

For European Union countries, the IDMVS client software meets the requirements of Radio Equipment Directive (RED) cybersecurity.

The overall workflow of using the device is shown below.



**Figure 1-1 Workflow**

## Chapter 2 Install Client Software

IDMVS is a client software for device configuration and remote operations.

---

### Note

- The client software is compatible with 32/64-bit Windows 7/10, and 64-bit Windows 11.
  - Only the IDMVS V4.2.3 supports the RED cybersecurity functions. You can contact technical support to get the client software installation package.
  - The USB type device supports IDMVS V2.3.0 and above that has integrated USB drive only. And there is no need to download and install other drivers.
  - The graphic user interface may differ by different versions of client software you use.
- 

### Steps

1. Double click the installation package to start installing the client software.
2. Select the language.
3. Read and check **Terms of the License Agreement**.
4. Click **Start Setup**.
5. Select installation directory and click **Next**.
6. Finish the installation according to the interface prompts.

## Chapter 3 Check USB Drive

Checking the USB drive on the PC is required before using the USB type device. After the USB type device is connected to the PC, the Windows system will automatically detect a new hardware device and install its corresponding drive.

Go to **Device Manager** by either pressing Win+X or right-clicking on the Windows menu button, and locate and expand the **Network adapters** to check the drive.

---

### Note

You can use the drive management tool to reinstall the USB drive if the installation is failed.

---

## Chapter 4 Set Device Network

You can connect the device to the client software only when the device is in the same network segment with the PC where the client software is installed.

### Steps

1. Double click the client software to run it.
2. Click  to find the device.
3. Right click the device, and click **Modify IP**.
4. Set the IP address of the device in the same network segment with the PC.



**Figure 4-1 Modify IP Address**

5. Click **OK**.

## Chapter 5 Activate Device

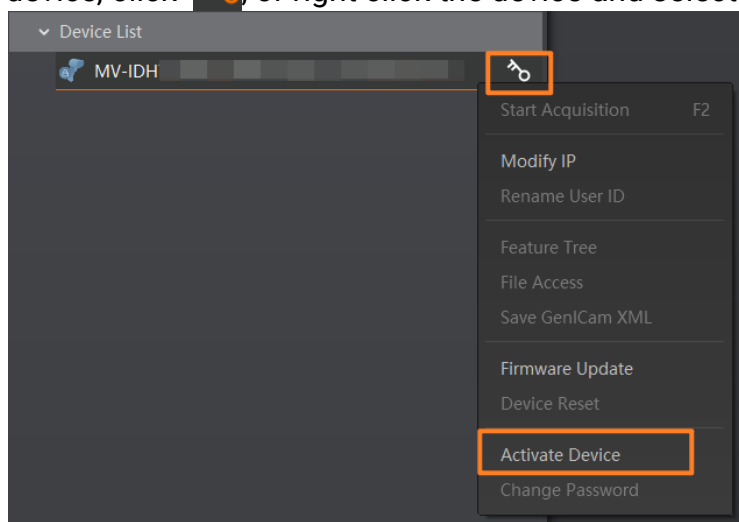
For the IDMVS client software with RED cybersecurity version, you should set a password and activate the device when connecting the device for the first time.

### Before You Start

Make sure that the device firmware is updated to the RED cybersecurity version (V5.0.7). If not, please contact technical support for firmware update.

### Steps

1. Double click the device, click , or right click the device and select **Activate Device**.



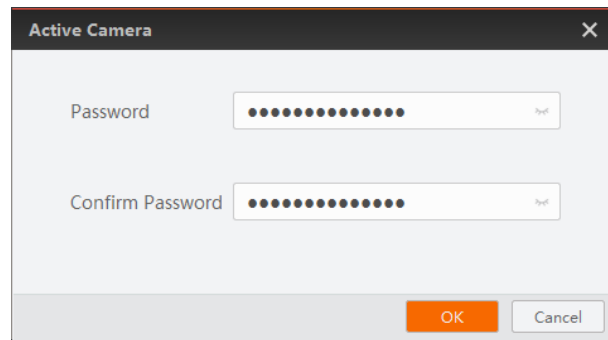
**Figure 5-1 Activate Device**

2. Set a password and confirm it in the pop-up window, and click **OK**.

---

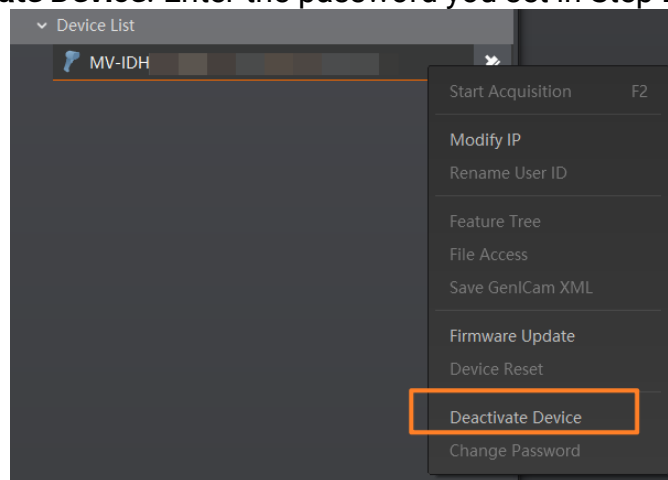
### Note

- The password requirements are shown in the pop-up window.
  - This password is required for device login and device deactivation. Please store the password securely.
  - The device will be locked after 5 incorrect password attempts. You can try again after 30 minutes. The lock time and login times are 30 minutes and 5 times by default, and you can go to **Feature Tree** → **Device Control** to set the two parameters.
  - Refer to section [Change Password](#) to edit the password, and section [Reset Password](#) to reset it.
  - When the  icon changes to , it means device activation is finished.
  - After the device is activated, the password is required if you want to change the IP address or update the firmware.
-



**Figure 5-2 Enter Password**

3. (Optional) If you need to restore the device to unactivated status, right click the device and select **Deactivate Device**. Enter the password you set in Step 2, and click **OK**.



**Figure 5-3 Deactivate Device**

---

### **Note**

The device can be deactivated only when the device is disconnected from the client software.

---

## Chapter 6 Connect Device to Client Software

Make sure that your device IP address is in the same network segment with the PC where you installed the client software before connecting the device to it.

After the device is activated, you can click  icon or double click the device in the device list, and enter the password to connect the device to the client software.

## Chapter 7 Client Software Layout

After connecting to the device, the client software can read the device information and display it.

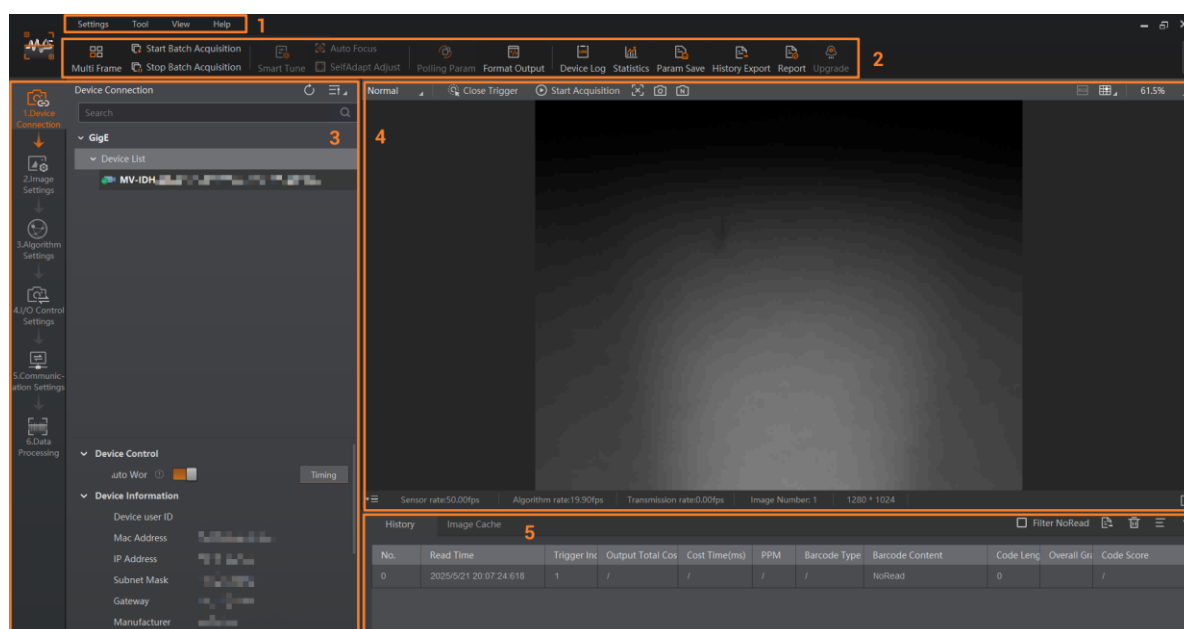


Figure 7-1 Main Window

### Note

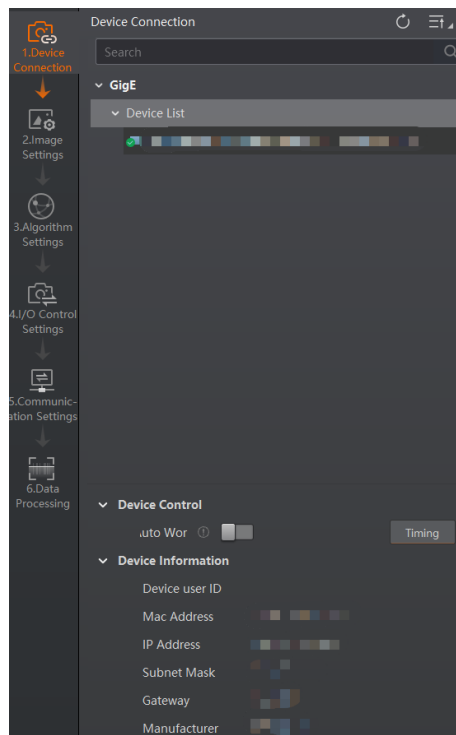
- The specific interfaces of the client software may differ by its versions.
- Refer to the user manual of the client software for detailed introductions and operations.

Table 7-1 Description of Main Window

| No. | Name     | Description                                                                                                       |
|-----|----------|-------------------------------------------------------------------------------------------------------------------|
| 1   | Menu Bar | The menu bar displays function modules, including <b>Settings</b> , <b>Tool</b> , <b>View</b> , and <b>Help</b> . |

| No. | Name                           | Description                                                                                                                                                                                       |
|-----|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2   | Control Toolbar                | The control toolbar provides quick operations for the device. You can click different icons to start or stop batch acquisition, change window layout, view statistics information and device log. |
| 3   | Device Configuration Area      | You can connect or disconnect device, set parameters, and modify device IP address in this area.                                                                                                  |
| 4   | Live View Window               | This area displays the acquisition images and algorithm reading result in real time. You can click different icons to capture and save image, record, etc.                                        |
| 5   | History Record and Image Cache | This area displays different barcode information read by the device in real-time. You can also set image cache here.                                                                              |

You can set device parameters in device configuration area.



**Figure 7-2 Device Configuration Area**

**Table 7-2 Configuration Area Description**

| No. | Module Name        | Description                                                                                   |
|-----|--------------------|-----------------------------------------------------------------------------------------------|
| 1   | Device Connection  | You can connect or disconnect device, modify device IP address, view device information, etc. |
| 2   | Image Settings     | You can set image parameters, light parameters, etc.                                          |
| 3   | Algorithm Settings | You can add different codes, set number of codes, etc.                                        |



| No. | Module Name            | Description                                                                   |
|-----|------------------------|-------------------------------------------------------------------------------|
| 4   | I/O Control Settings   | You can set parameters related to input or output.                            |
| 5   | Communication Settings | You can select different communication protocols, and set related parameters. |
| 6   | Data Processing        | You can set filter rule for output result.                                    |

## Chapter 8 Change Password

You can follow the steps below to change the password.

### **Before You Start**

Make sure that the device is connected to the client software.

### **Steps**

1. Right click the device, and select **Change Password**.
2. Enter the old password and new password, and confirm it.

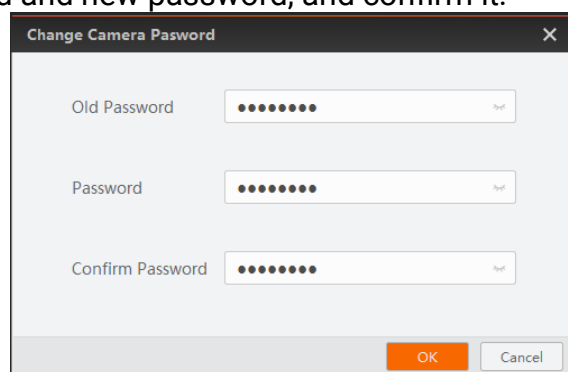


Figure 8-1 Change Password

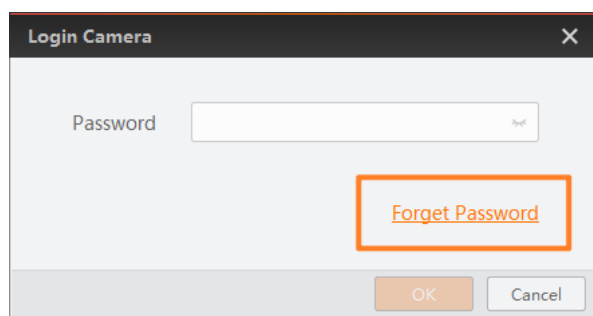
## Chapter 9 Reset Password

If you forget the password, follow the steps below to reset the password.

### **Steps**

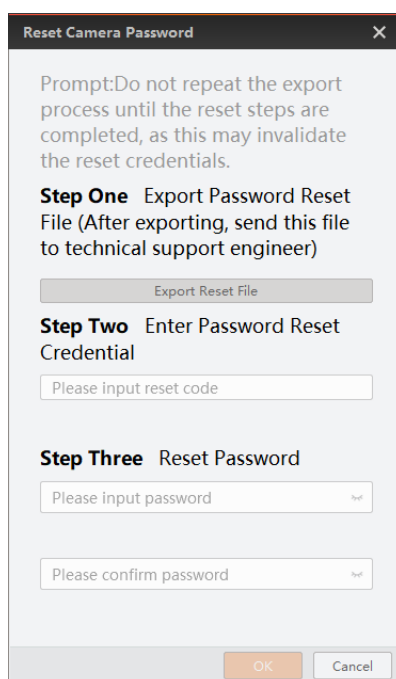
1. On the password entering page, click **Forget Password**, and a pop-up window will be

displayed.



**Figure 9-1 Forget Password**

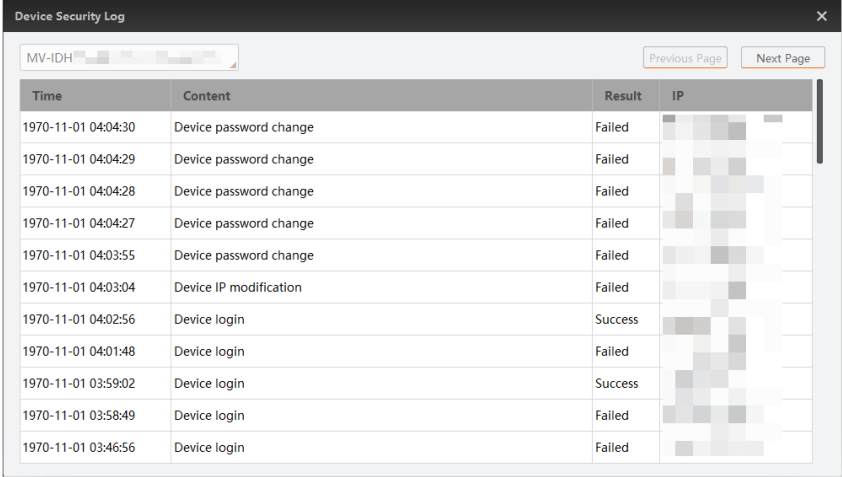
2. Click **Export Reset File**, save this file to local directory, and send it to the technical support.
3. Obtain a password reset credential, and enter in **Enter Password Reset Credential**.
4. Enter a new password, and confirm it.
5. Click **OK**.



**Figure 9-2 Reset Password**

## Chapter 10 View Device Security Log

You can click  in control toolbar to open the device security log window, and view log details related to RED cybersecurity functions.



The screenshot shows a window titled "Device Security Log" with a search bar containing "MV-IDH" and "Previous Page" and "Next Page" buttons. The table below lists security events with columns for Time, Content, Result, and IP.

| Time                | Content                | Result  | IP |
|---------------------|------------------------|---------|----|
| 1970-11-01 04:04:30 | Device password change | Failed  |    |
| 1970-11-01 04:04:29 | Device password change | Failed  |    |
| 1970-11-01 04:04:28 | Device password change | Failed  |    |
| 1970-11-01 04:04:27 | Device password change | Failed  |    |
| 1970-11-01 04:03:55 | Device password change | Failed  |    |
| 1970-11-01 04:03:04 | Device IP modification | Failed  |    |
| 1970-11-01 04:02:56 | Device login           | Success |    |
| 1970-11-01 04:01:48 | Device login           | Failed  |    |
| 1970-11-01 03:59:02 | Device login           | Success |    |
| 1970-11-01 03:58:49 | Device login           | Failed  |    |
| 1970-11-01 03:46:56 | Device login           | Failed  |    |

**Figure 10-1 View Device Security Log**

