

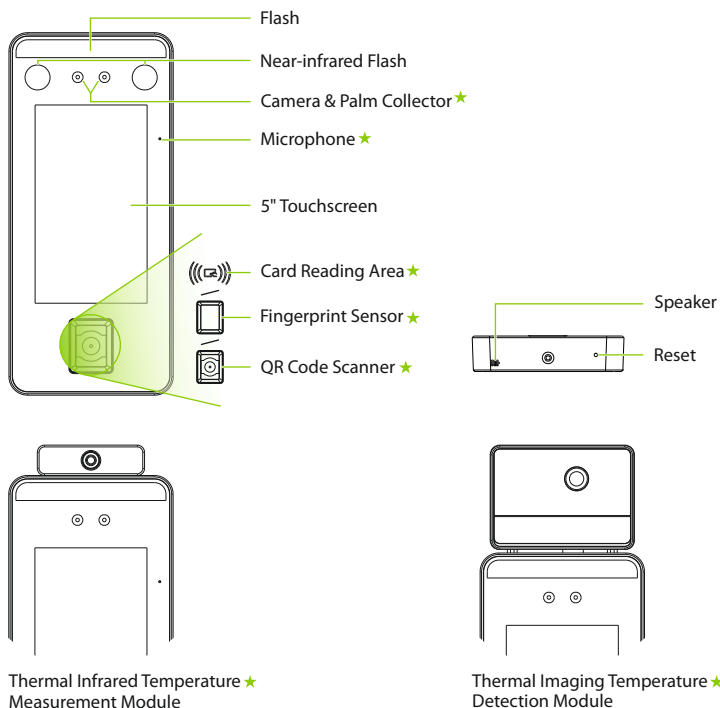
Quick Start Guide

5-inch Visible Light Terminals

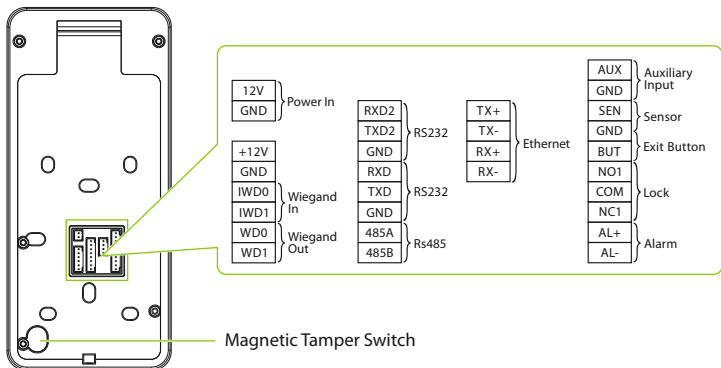
Version: 2.2

Overview

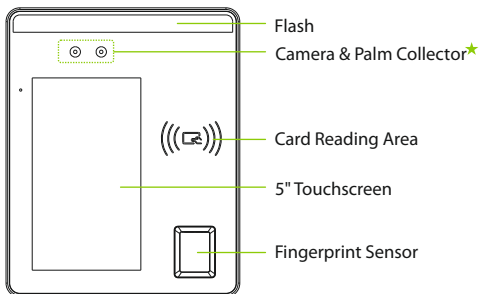
Model 1

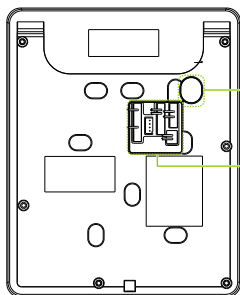


Note: Not all products have the function with ★, the real product shall prevail.



Model 2





Magnetic Tamper Switch

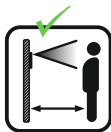
Terminal Block
(Same as Model 1)

Installation Environment

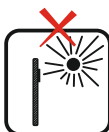
Please refer to the following recommendations for installation.



INSTALL INDOORS
ONLY



KEEP EFFECTIVE
DISTANCE OF
0.3 to 2m



AVOID DIRECT
SUNLIGHT
AND EXPOSURE



AVOID INSTALLATION
NEAR
GLASS WINDOWS



AVOID USE OF ANY
HEAT SOURCE
NEAR THE DEVICE

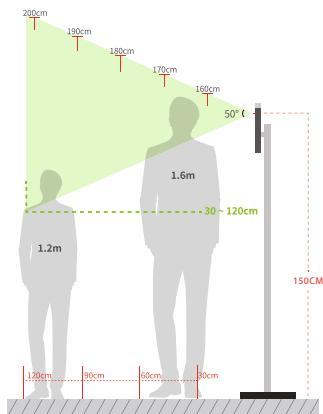
Installation Requirements

The installation requirements and indications associated with the device are given below:

Specification	Standard value	Remark
Operating Environment	Indoor, Avoid wind, Avoid direct sunlight, 16°C to 35°C (60.8°F to 95°F)	The recommended operating temperature is 25°C (77°F)
Distance (between face and device)	30 to 120cm (0.98ft to 3.94ft)	The recommended distance is 80cm (2.62ft)
Measurement Accuracy	$\pm 0.3^{\circ}\text{C}$ ($\pm 0.54^{\circ}\text{F}$)	This value is tested at a distance of 80cm or 2.63ft under 25°C (77°F) environment.

Note: The temperature measurement data is only for reference, and not for any medical purposes.

Forehead Temperature Detection

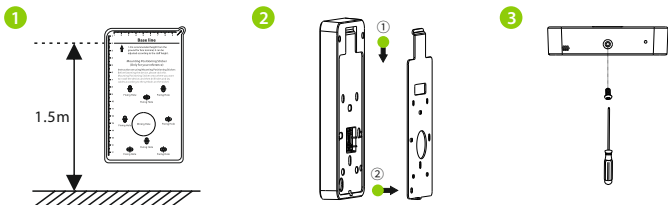


Indoor constant Temperature Environment

- Installation height: 1.55m
- FOV (Field Of View) of the thermal imaging device: 50°
- Temperature detection distance: 0.3m to 1.2m
- Height of the face adapted for detection: 1.2m to 2m

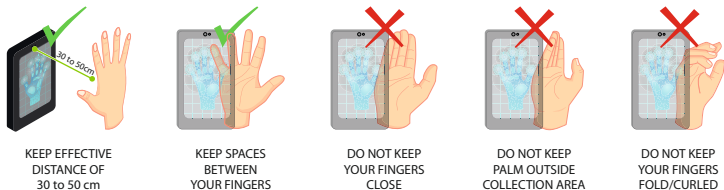
Device Installation

This guide uses the Model 1 as an example for installation, wiring, introduction of functions and instructions for use.



1. Attach the mounting template sticker to the wall, and drill holes according to the mounting paper. Fix the back plate on the wall using wall mounting screws.
2. Attach the device to the back plate.
3. Fasten the device to the back plate with a security screw.

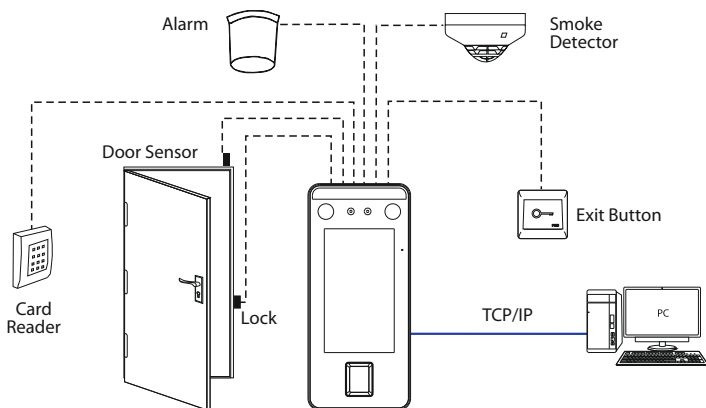
Recommended Palm Gestures ★



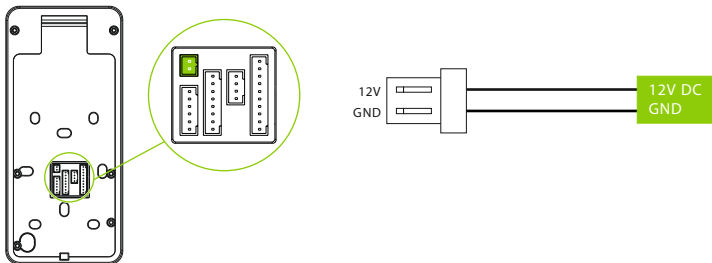
Note:

1. Place your palm within **30 to 50 cm** of the device.
2. Place your palm in the palm collection area, such that the palm is placed parallel to the device.
3. Make sure to keep space between your fingers.

Standalone Installation



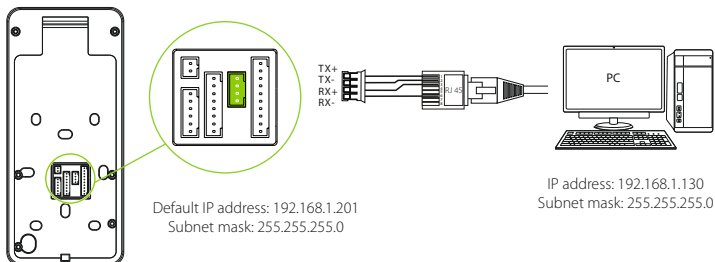
Power Connection



Recommended power supply

1. 12V $\pm$ 10%, at least 3,000mA.
2. To share the power with other devices, use a power supply with higher current ratings.

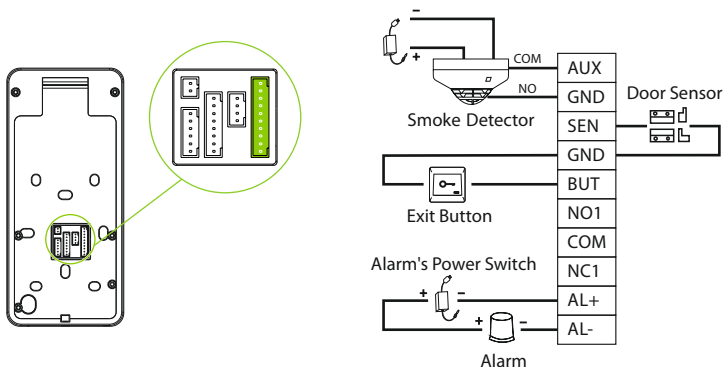
Ethernet Connection



Click **[COMM.]** > **[Ethernet]** > **[IP Address]** , input the IP address and click **[OK]**.

Note: In LAN, IP addresses of the server (PC) and the device must be in the same network segment when connecting to software.

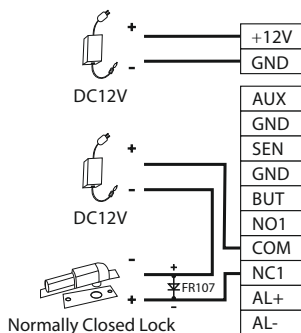
Door Sensor, Exit Button & Alarm Connection



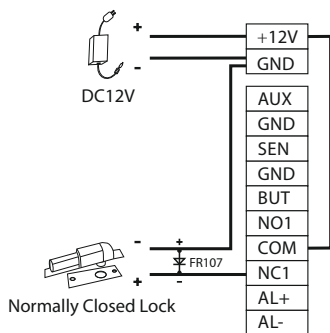
Lock Relay Connection

The system supports both **Normally Opened Lock** and **Normally Closed Lock**. The **NO Lock** (normally opened when powered) is connected with '**NO1**' and '**COM**' terminals, and the **NC Lock** (normally closed when powered) is connected with '**NC1**' and '**COM**' terminals. The power can be shared with the lock or can be used separately for the lock, as shown in the example with NC Lock below:

1) Device not sharing power with the lock

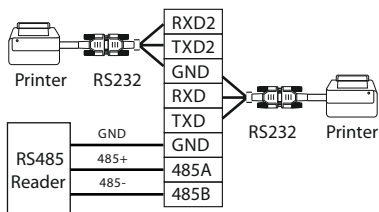
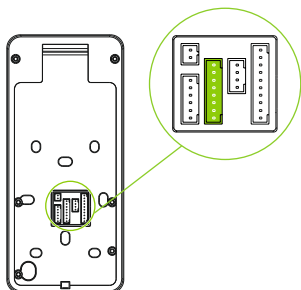


2) Device sharing power with the lock



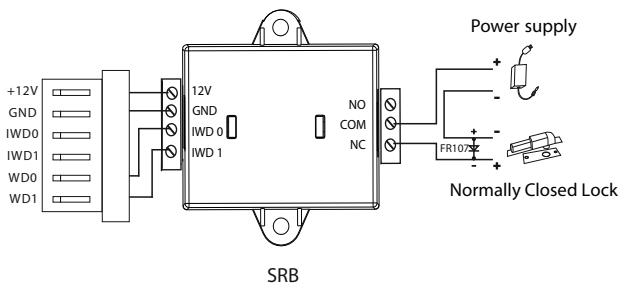
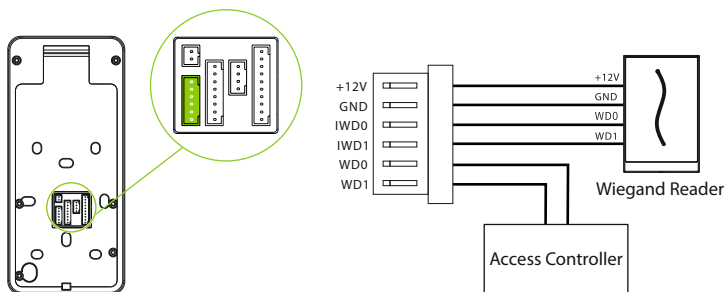
RS485 and RS232 Connection

The RS485 and the RS232 lets user connect to multiple readers to the device. Two RS232 and one RS485 can be connected to the terminal, as shown in the figure below.



Wiegand Reader/SRB Connection

Wiegand card reader connects to the top 4 pins of the wiegand terminal and the last two pins are used by the Access controller, as shown in the following figure. It sends the credentials to the device via wiegand communication.



User Registration

When there is no super administrator set in the device, click on ☰ to enter the menu. Add a new user and set User Role to Super Admin, then the system will request for the administrator's verification before entering the menu. It is recommended to register a super administrator initially for security purposes.

Method 1: Register on the Device

Click on ☰ > [User Mgt.] > [New User] to register a new user. The options include entering the user ID and Name, setting User Role, registering Palm★, Face, Card Number, Password and adding Profile Photo.



New User	
User ID	1
Name	Mike
User Role	Normal User
Palm	1
Face	1
Card Number	1
Password	*****
Profile Photo	1
Access Control Role	

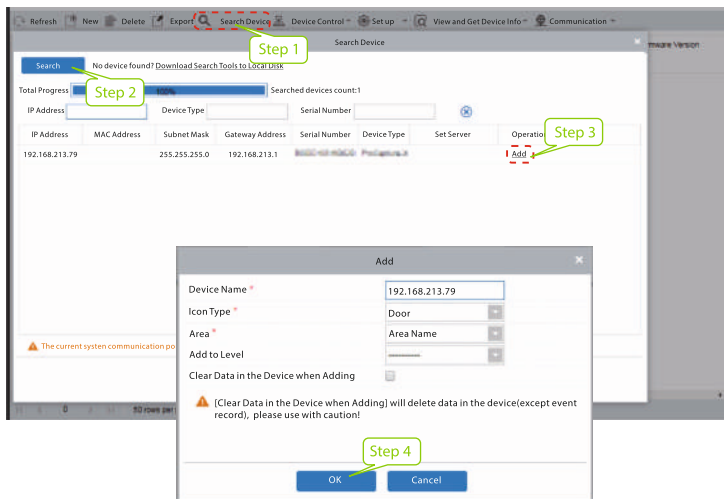


Method 2: Register on ZKBioAccess IVS Software

● Register on the PC

Please set the IP address and cloud service server address in the Comm. Menu option on the device.

1. Click **[Access]** > **[Access Device]** > **[Device]** > **[Search Device]** to search the device on the software. When an appropriate server address and port is set on the device, the searched devices are displayed automatically.



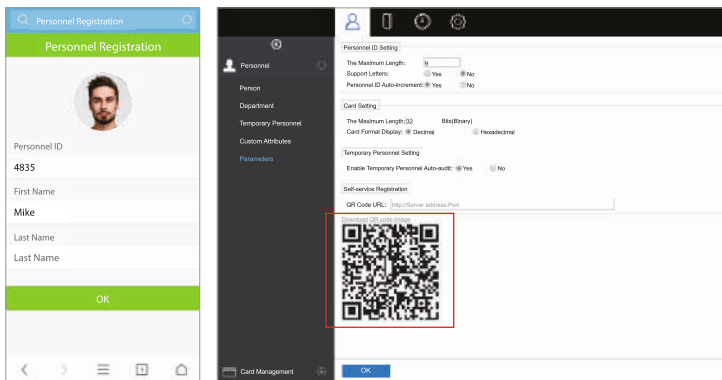
2. Click **[Add]** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdowns and click **[OK]** to add the device.
3. Click **[Personnel]** > **[Person]** > **[New]** and fill in all the required fields to register a new users in the software.
4. Click **[Access]** > **[Device]** > **[Device Control]** > **[Synchronize All Data to Devices]** to synchronize all the data to the device including the new users.

For more details, please refer to the *ZKBioAccess IVS User Manual*.

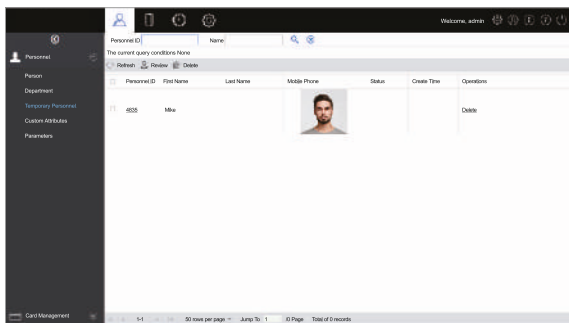
● Register on the Phone

Once the ZKBioAccess IVS software is installed, the users could enroll their face via a browser application on their own mobile phone.

1. Click **[Personnel]** > **[Parameters]**, input “http://Server address: Port” in the QR Code UGL bar. The software will automatically generate a QR code. Scan the QR code or login onto “http://Server address: Port/app/v1/adreg” by the mobile phone to register users.



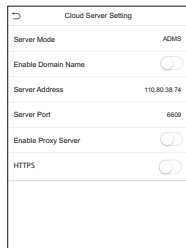
2. The users will be displayed in **[Personnel]** > **[Temporary Personnel]**, click **[Review]**.



Ethernet and Cloud Server Settings

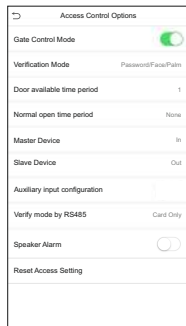
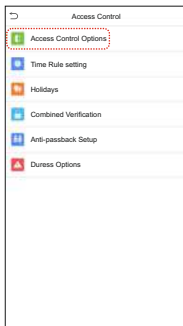
Click on  > **[COMM.]** > **[Ethernet]** to set the network parameters. If the TCP/IP communication of the device is successful, the icon  will be displayed in the upper right corner of the standby interface.

Click on  > **[COMM.]** > **[Cloud Server Setting]** to set the server address and server port, that is, the IP address and port number of the server after the software is installed. If the device communicates with the server successfully, the icon  will be displayed in the upper right corner of the standby interface.



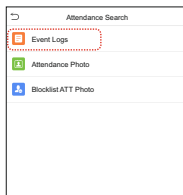
Access Control Setting

Click on  > **[Access Control]** to enter the access control management interface and set relevant parameters of access control.



Attendance Record

Click on  > **[Attendance Search]** > **[Event Logs]** to enter the logs query interface, input the user ID and select the time range, the corresponding event logs will be displayed.

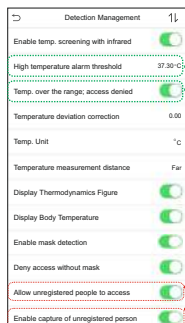
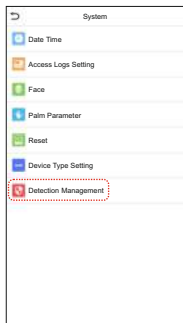


Personal Record Search		
Date	User ID	Time
03-03		
		Number of Records:04
	4	11:25
	2	11:25 11:22
	3	11:25
03-04		
		Number of Records:04
	1	11:29
	3	11:29 11:21
	2	11:28
	4	11:26
03-05		
		Number of Records:04
	1	11:27
	4	11:27
	3	11:27
	2	11:27

Detection Management Settings ★

Click on  > **[System]** > **[Detection Management]** to enter the setting interface.

- 1 You can set the value of **High temperature alarm threshold**, and enable the **Temperature over the range; access denied** and the **Trigger external alarm**, the device will send an alarm prompt when the temperature of the user detected exceeds this value, meanwhile the user will be forbidden to access, as shown in the following figure. The method of enabling **Mask detection** is the same.
- 2 When the **Allow unregistered people to access** is enabled, optionally, set **Enable capture of unregistered person** to save the temperature data.

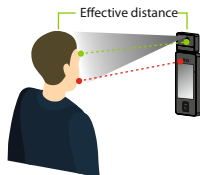


Detection Management	1
Temp. Unit	°C
Temperature measurement distance	Far
Display Thermodynamics Figure	☒
Display Body Temperature	☒
Enable mask detection	☒
Deny access without mask	☒
Allow unregistered people to access	☒
Enable capture of unregistered person	☒
Trigger external alarm	
Clear external alarm	
Enter alarm delay(s)	255
Update Firmware	



Note:

1. The effective distance for temperature detection is within 50cm.
2. Recommended for indoor use.
3. Temperature measurement data is for reference only, not for medical use.
4. Remove the mask to register the face, wear a mask to recognize the face, the type of mask, the size of the face covered by the mask, and bangs will affect the facial recognition effect.
5. Facial verification for masked individuals will increase FAR. Palm verification[★] for masked individuals is recommended.



Effective distance:

-● Temperature: 30 to 120cm
-● Palm[★]: 30 to 50cm
-● Face: 30 to 200cm

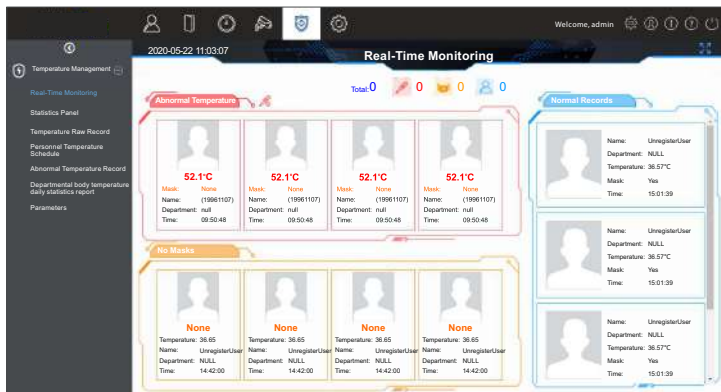
Real-time Monitoring on the ZKBioAccess IVS Software

Once ZKBioAccess IVS software installed, users could perform temperature detection management on browser.

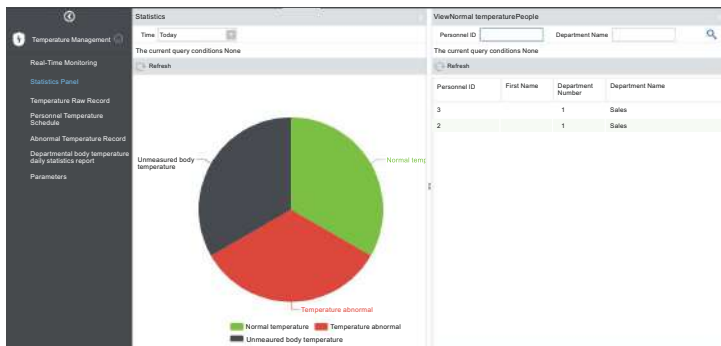
1. Please set the IP address and cloud service server address on the device and add the device to the software.

- Click **[Temperature Detection] > [Temperature Management] > [Real-time monitoring]** to view all the events include the Abnormal Temperature, No Masks and Normal Records.
- Click **[Temperature Management] > [Statistics Panel]** to view the analysis of statistical data and view the personnels with normal temperature.

Real-Time Monitoring

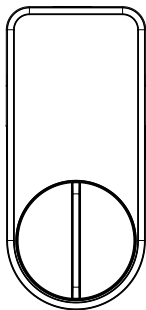


Statistics Panel



For more details, please refer to the *ZKBioAccess IVS User Manual*.

Connecting to A1 Bluetooth Lock★

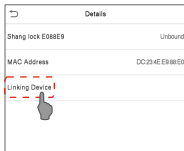


A1 Bluetooth Lock

Tap **[Bluetooth Settings]** on the **[Comm.]** Settings interface to set the Bluetooth.

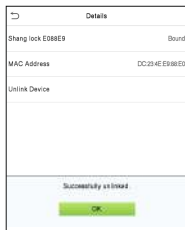
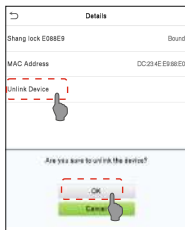
● Bind Lock

1. Click **[Bluetooth]** to enable the Bluetooth function.
2. You need to wake up the lock, the device will search through Bluetooth and display the Bluetooth lock to be bound on the **[Bluetooth Settings]** interface.
3. Select the unbound Bluetooth lock again to enter the **[Details]** interface.
4. Please wake up the device first, and then click **[Linking Device]**, the Bluetooth lock will emit a beep sound, and the interface will pop up a "Linked" prompt, indicating that the device is successfully bound



● Unbind Lock

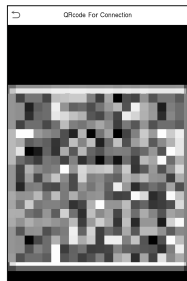
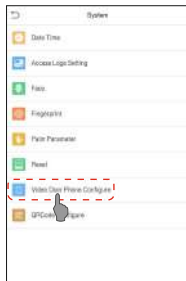
1. Tap on **[Comm.]** > **[Bluetooth Settings]**, select the bound Bluetooth lock, and enter the **[Details]** interface.
2. Please wake up the device first, click **[Unlink Device]** on the **[Details]** interface. The interface will pop up a "Are you sure to unlink the device?" prompt, then click **[OK]**.
3. After the Bluetooth lock emits three beep sound, the interface will pop up a "Successfully unlinked." prompt, indicating that the unbinding of the device is complete.



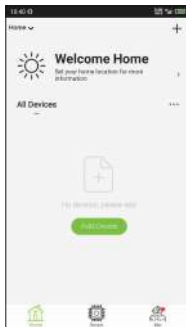
Connect to ZSmart★

After download and install the ZSmart App on the phone, open the App and add the device by scanning the QRcode. The process is as follows:

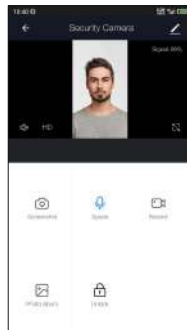
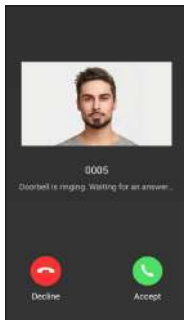
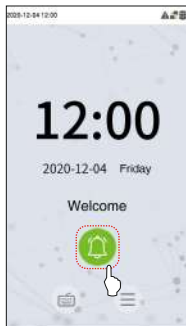
1. On the device, click on **☰** > **[System]** > **[Video Door Phone Configure]** > **[Connection QRcode]**.



2. On the APP, click **[Add Device]** at Home Page.
3. Click the  icon in the upper right corner to scan the QRcode and add devices.



Visitors click the  on the main interface of the device to call and the phone will ring. The user can select accept or decline the call. After the user accepting, it will enter the video door phone interface.



LAN Video Intercom Function Settings

Step 1: Install the ZKBioAccess IVS Software and ZKBio VMS Plugin

1. Choose the **"Video-VMS"** module of the ZKBioAccess IVS software to install. (The Video module and the Video-VMS module cannot be installed together.)
2. Install the **ZKBio VMS Plugin**. (To recognize the intercom function, the ZKBioAccess IVS software and the ZKBio VMS Plugin must be opened simultaneously.)

Step 2: Configuration Parameters

1. Add site on the Video-VMS Plugin

- a. Click **[Choose site]** > **[Site management]** > **[Add]** on the login interface, enter the Name, IP address, and port to add a site.

IP Address: Enter the local IP address.

Port: The default port number is 5252.

- b. Login to the Video-VMS plugin after adding the site. The user name and the initial password are both **"admin"**. (When the Video-VMS plugin is connected successfully to the ZKBioAccess IVS, the password changes to the admin user password of the ZKBioAccess IVS.)

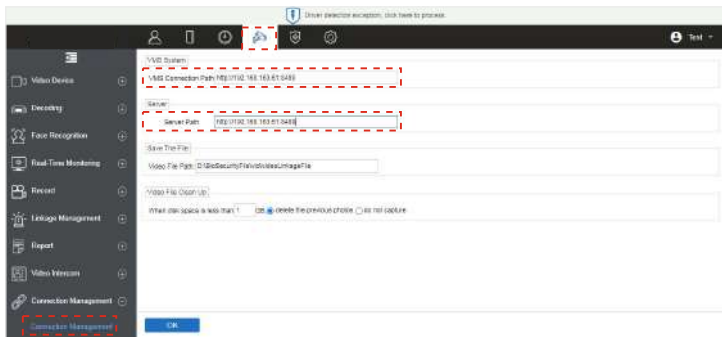


2. Configure the connection path of the ZKBioAccess and VMS plugin

Click **[Video]** > **[Connection]** > **[Connection Management]** to change the path, as shown in the following figure.

VMS Connection Path: "<http://local IP address: port>", Port: **8489** by default. (eg., <http://192.168.163.61:8489>).

Server Path: "<http://server IP address: port>". The port is the service port set during installation (not the ADMS port) (eg., <http://192.168.163.61:8098>).

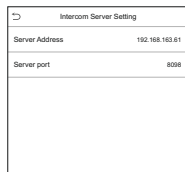
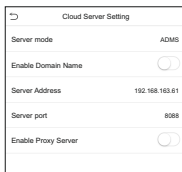
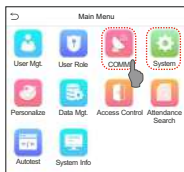


3. Configure the parameters on the device

- Click on > **[COMM.]** > **[Cloud Server Setting]** to set the server address and server port, that is, the IP address and port number of the server after the software is installed. The icon is displayed in the upper right corner of the standby interface when the device communicates with the server successfully.
- Click on > **[System]** > **[Video intercom parameters]** > **[Intercom Server Setting]** to set the server address and server port.

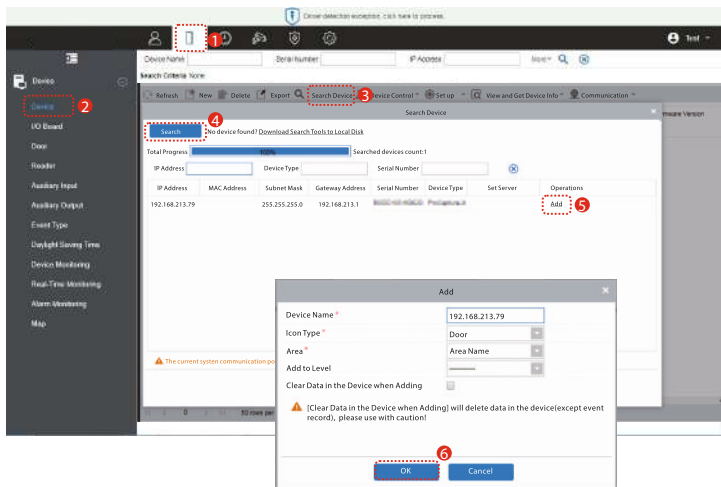
Server Address: Enter the ZKBioAccess IVS installation IP address.

Server Port: It is the service port set during installation (not the ADMS port).

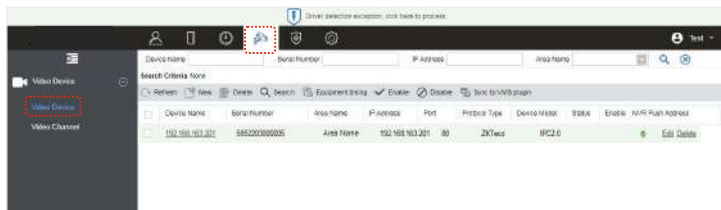


Step 3: Adding Device on ZKBioAccess IVS Software

1. Click **[Access] > [Device] > [Device] > [Search]** to add the device on the ZKBioAccess IVS software.

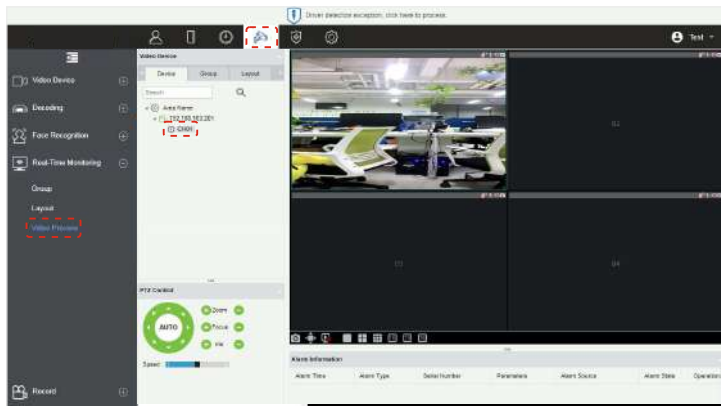


2. After the device is added successfully to the access module, it automatically adds to the video module. User can click **[Video] > [Video Device] > [Search]** to view. (If the device is not added to the Video module, please check whether the parameter settings are correct.)



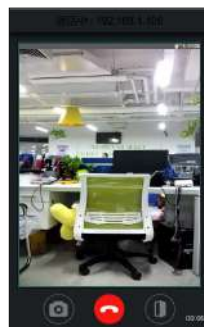
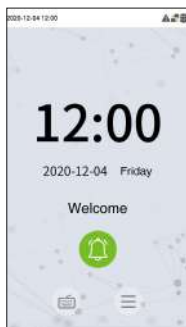
Step 4: Video Preview

Click **[Video]** > **[Real-Time]** > **[Video Preview]** to enter the preview interface of the device.



Step 5: Make a Call on the Device

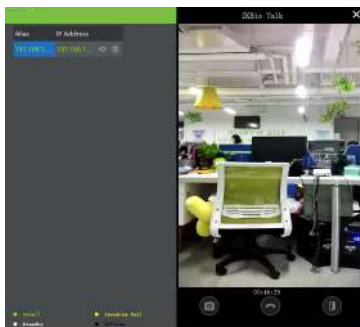
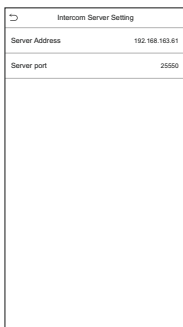
Click on  icon on the main interface of the device to get to the call window. The user can click  icon to accept the call, click  icon to take a snapshot, or click  icon to open the door remotely, as shown in the following figure. For more details, please refer to the User Manual.



Connect to ZKBio Talk

1. Keep the parameter settings of ZKBioAccess IVS software unchanged. And then install the ZKBioTalk software.
2. Click on  > **[System]** > **[Video intercom parameters]** > **[Intercom Server Setting]** on the device, to change the server address and server port.
Server Address: Enter the current server installation IP address.
Server Port: The default server port is **25550**.
3. Double click the  icon to open the ZKBioTalk software. Then click on  icon on the main interface of the device to get to the call window. The user can click  icon to accept the call, click  icon to take a snapshot, or click  icon to open the door remotely.

For more details, please refer to the User Manual.



SIP Settings★

This function needs to be used with the indoor station Vpad A2.

Local Area Network Use

Set the IP address on the indoor station. In LAN, the IP addresses of the indoor station and the device must be in the same network segment.

Network	
Accounts	1. Connection Mode: Static IP
Network	2. IP Address: 192.168.163.199
Security	3. Mask: 255.255.255.0
Maintenance	4. Gateway: 192.168.163.1
Device	5. Primary DNS: 114.114.114.114
	6. Secondary DNS: 8.8.8.8

● Directly Enter the IP Address of the Indoor Station

Tap the  icon on the device screen and entering the IP address of the indoor station in the jumping interface the indoor station.



● Custom the Punch Status Options

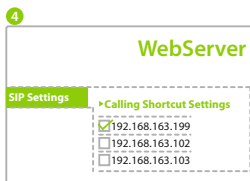
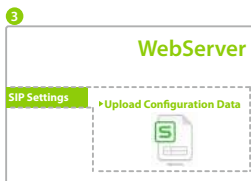
1. Configure SIP parameters for the device on the Webserver.



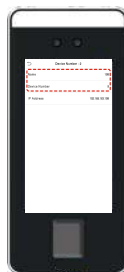
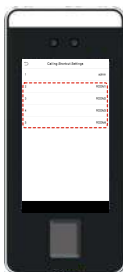
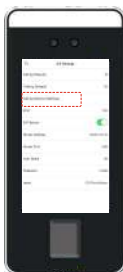
2

Excel

IP Address	Subnet Mask	Gateway	Dialing Number
192.168.163.199	255.255.255.0	192.168.163.1	101
192.168.163.102	255.255.255.0	192.168.163.1	102
192.168.163.103	255.255.255.0	192.168.163.1	103
192.168.163.104	255.255.255.0	192.168.163.1	104



2. Configure SIP parameters on the device.





SIP Server

On the device, tap **[SIP Server]**, after the device is rebooted, enter the server-related parameters.



For more details, please refer to the *SpeedFace-V5L&H5L Series User Manual*.

Connect to ACMS★

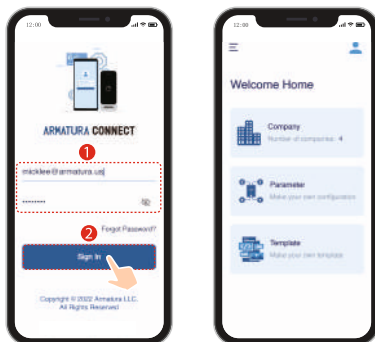
Set up on Armatura Connect

1. The Branch/Partner needs to create a customer on the ACMS first. Then add an installer and assign the installer to the customer. Once the installer has activated the account, the device can be assigned.

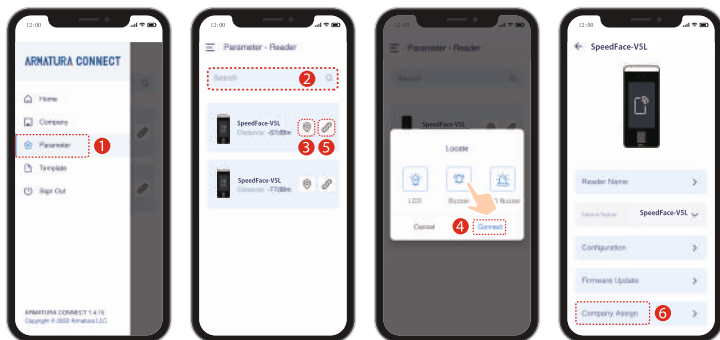
The screenshot shows two side-by-side panels from the Armatura Headquarters interface. The left panel is titled 'Create Customer' and contains fields for 'Company Profile' (Company Name, U.S. Tax ID, Phone, Email), 'Account Profile' (Last Name, First Name, Email), and 'Orderer Type' (Armatura ID, Private ID). A red dashed box highlights the 'Save' button at the bottom, with a red circle '1' next to it. The right panel is titled 'Create Installer' and contains fields for 'Basic Info' (First Name, Last Name, Email, Phone), 'Product' (dropdown), and 'Address' (Address Line 1, Address Line 2, City, State, Zip, Country). A red dashed box highlights the 'Save' button at the bottom, with a red circle '2' next to it. A green callout bubble labeled 'Customer' points to the 'Create Customer' panel, and another green callout bubble labeled 'Installer' points to the 'Create Installer' panel. A green callout bubble labeled 'Armatura Connect Mobile' points to the 'Armatura Connect Mobile' checkbox in the 'Permissions' section of the 'Create Installer' panel.

The screenshot shows the 'Assign' and 'Activate Account' steps in the Armatura Headquarters interface. The top panel is titled 'Assign' and shows a table of 'Installer Selection' with columns for 'Installer ID', 'Account', 'Name', and 'Email'. A red dashed box highlights the 'Assign' button at the bottom, with a red circle '4' next to it. The bottom panel is titled 'Activate Account' and shows a 'Dear User,' message with instructions to activate the account. A red dashed box highlights the 'Activate Account' button at the bottom, with a red circle '5' next to it. A green callout bubble labeled 'Customer' points to the 'Customer' dropdown in the 'Assign' panel, and another green callout bubble labeled 'Assign' points to the 'Assign' button. A green callout bubble labeled 'Activate Account' points to the 'Activate Account' button.

2. Search for the "Armatura Connect" App in the iOS App Store or the Google Play Store. Install and log in to the installer account.
3. Login the Armatura Connect App.



4. Bind devices and set up company assignments.

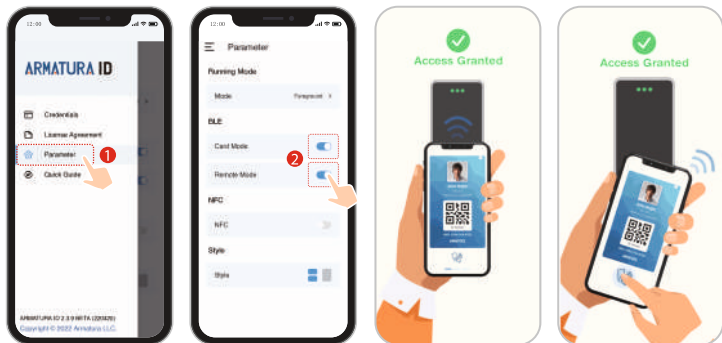


Use the Armatura ID App

1. Download the ARMATURA ID App.
2. Activate the credential on the App.



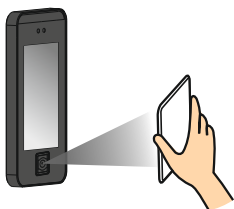
3. Setting the card mode, then you can swipe the card with the mobile phone close to the device, or swipe the card remotely within the set range.



For more details, please refer to *Armatura CONNECT User Manual* and *Armatura ID User Manual*.

QR Code Verification ★

1. In **[System] > [Basic Management] > [Parameters]** of ZKBioSecurity software, set **Enable QR Code** to "Yes", and select the QR code status according to the actual situation.
2. On the Server, choose **[System] > [Authority Management] > [Client Register]** to add a registered App client.
3. Open the App, enter the IP address or domain name of the server, and its port number, scan the QR Code of the new App client. After the connection is successful, tap on Employee to switch to Employee Login screen. Enter the Employee ID and Password (Default: 123456) to login.
4. Tap **[Mobile Credential]** on the App, and a QR code will appear, parallel the phone screen to the device QR code scanner. For details, please refer to *SpeedFace-V5L&H5L Series User Manual*.



Note: Place your phone within **15 to 50cm** of the device (distance depends on the size of the phone screen), do not block the device QR code scanner and QR code in the phone screen.

