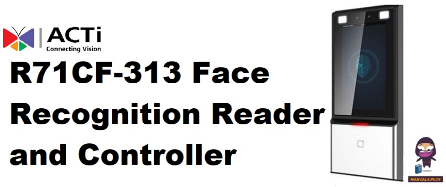


ACTi R71CF-313 Face Recognition Reader and Controller User Manual

Home » ACTi » ACTi R71CF-313 Face Recognition Reader and Controller User Manual

Contents

ACTi
Connecting Vision

ACTi R71CF-313 Face Recognition Reader and Controller

Specifications

- **Product Model**: R71CF-313
- **Date:** 2024/09/02
- Face Recognition Reader & Controller CE Marked
- **Compliance:** EMC Directive 2014/30/EU, RE Directive 2014/53/EU, RoHS Directive 2011/65/EU, WEEE Directive 2012/19/EU, Battery Directive 2006/66/EC

Product Usage Instructions

Safety Information

- It is important to follow the safety instructions to avoid danger or property loss. Dangers include unauthorized disassembly of the device.

Installation

- **Installation Environment:** Ensure the device is installed in a suitable environment as per the provided guidelines.
- **Wall Mounting:** Follow the instructions for proper wall mounting to ensure stability and functionality.

Initial Setup

- **Activate via Device:** Follow the activation process specified in the manual to enable the device.
- **Main Screen:** Familiarize yourself with the main screen interface for easy navigation.
- **Login:** Follow the login procedures to access the device’s features securely.

FAQ:

- **Q**: How do I dispose of the product in the European Union?

- **A:** Products marked with specific symbols need to be returned to designated collection points for recycling. Refer to the product documentation for battery disposal instructions.

Safety Information

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.
The precaution measure is divided into Dangers and Cautions:
Dangers: Neglecting any of the warnings may cause serious injury or death. Follow these safeguards to prevent serious injury or death.
Cautions: Neglecting any of the cautions may cause injury or equipment damage. Follow these precautions to prevent potential injury or material damage.

Danger:

- All electronic operations should be strictly compliance with the electrical safety regulations, fire prevention regulations, and other related regulations in your local region.
- Please use the power adapter, which is provided by the company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on walls or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Risk of explosion if the battery is replaced by an incorrect type
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- This equipment is not suitable for use in locations where children are likely to be present.
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrating surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.

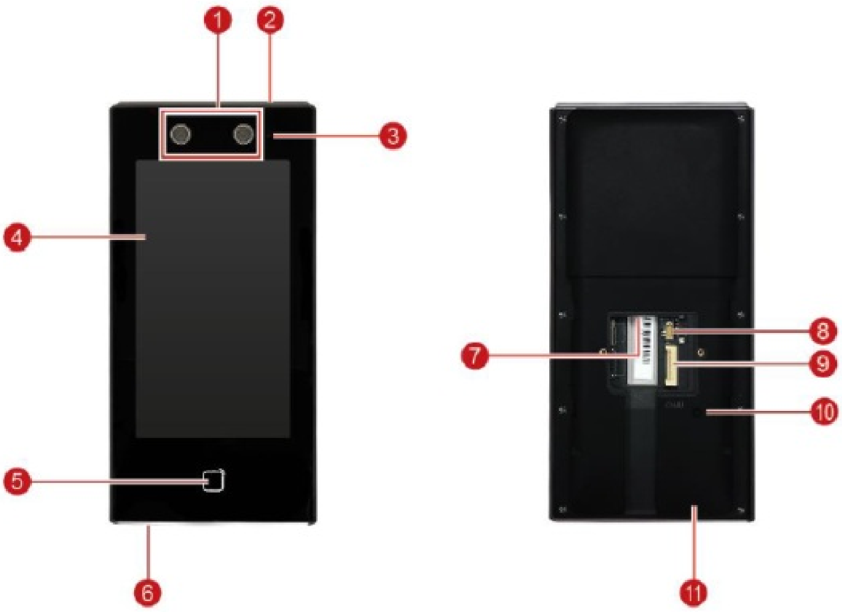
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when opening up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when cleaning inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpacking them for future use. In case of any failure, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage to the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Working temperature: 0 °C to 50 °C; Working humidity: 10% to 90% (no condensing)
- Indoor use. The device should be at least 2 meters away from the light, and at least 3 meters away from the window.
- Outdoor use or use in environment exceeding the device temperature measurement will affect the temperature measurement accuracy.

Introduction

Package Content

Reader & Controller	Wall Mount	Wire Cable	Mounting Template
Wrench	**Screw Pack**	**Mounting Screws**	**Warranty Card**

Physical Description



Item		Item	
1	Cameras	7	Ethernet Port
2	Indicator	8	Debugging Port (for service only)
3	Microphone	9	Cable Connector
4	Touch Screen	10	Tamper Key
5	Card Sensor	11	Speaker
6	USB Port		

Wiring

- The device comes with a wire cable that connects to power input, serial device, Wiegand device, alarm input/output devices, and door lock, among others. The wires are color-coded and labeled for easy wiring. After wiring to external devices, connect the
- wafer terminal connector to the device.
- You can connect a card reader using RS-485 connection. Connect the NC/NO and COM terminals to the door lock, connect the SEN and GND terminals to the door contact, and the BTN/GND terminal with the exit button, then connect the Wiegand terminal
- to the access controller.
- When you connect an access controller through Wiegand, the face recognition device can send authentication data to the access controller. The access controller will then decide whether to unlock the door based on this information.

NOTE: A power adapter is not supplied with the device, contact sales to purchase separately. Individual power supply is also needed for external devices like card readers, exit buttons, door locks, etc.

Wiring Terminal Description

Group	No.	Color	Label	Description
Power Input	A1	Red	+12 V	12 VDC Power Supply
	A2	Black	GND	Ground
Alarm Input	B1	Yellow / Blue	IN1	Alarm Input 1
	B2	Black	GND	Ground
	B3	Yellow / Orange	IN2	Alarm Input 2
Alarm Output	B4	Yellow / Purple	NC	Alarm Output Wiring
	B5	Yellow / Brown	COM	
	B6	Yellow / Red	NO	
RS-485	C1	Yellow	485+	RS-485 Wiring
	C2	Blue	485-	
	C3	Black	GND	Ground
Wiegand	C4	Green	W0	Wiegand Wiring 0
	C5	White	W1	Wiegand Wiring 1

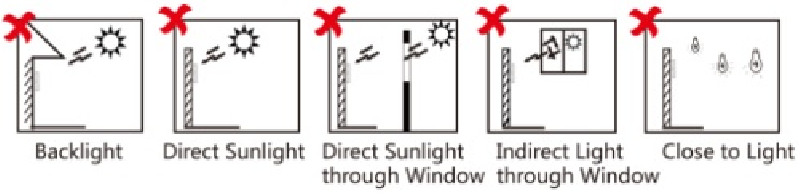
Group	No.	Color	Label	Description
Power Input	A1	Red	+12 V	12 VDC Power Supply
	A2	Black	GND	Ground
Alarm Input	B1	Yellow / Blue	IN1	Alarm Input 1
	B2	Black	GND	Ground
	B3	Yellow / Orange	IN2	Alarm Input 2

Alarm Output	B4	Yellow / Purple	NC	Alarm Output Wiring
	B5	Yellow / Brown	COM	
	B6	Yellow / Red	NO	
RS-485	C1	Yellow	485+	RS-485 Wiring
	C2	Blue	485-	
	C3	Black	GND	Ground
Wiegand	C4	Green	W0	Wiegand Wiring 0
	C5	White	W1	Wiegand Wiring 1

Installation

Installation Environment

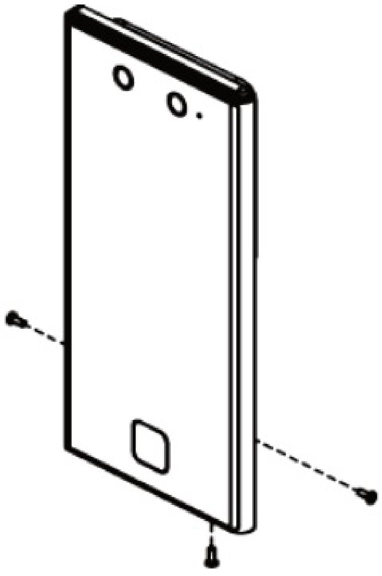
- Recommended wall installation height of device = 1.43 m to 1.9 m
- Avoid backlight, direct and indirect sunlight.



- For better recognition, there should be a light source in or near the installation environment. Below is a light source illumination reference value:
  - Candle: 10 lux
  - Bulb: 100 ~ 850 lux
  - Sunlight: More than 1200 lux
- There should be no strong reflective objects (such as glass doors/walls, stainless steel objects, ceramic tiles, etc.) within 1 meter of the field of view of the device.
- Avoid device reflection.
- Keep the camera clean.
- Make sure the wall can bear three (3) times the weight of the device.
- For accurate face recognition, the recognition distance should be greater than 30 cm.

Wall Mounting

1. Stick the supplier d mounting template to the target wall. Drill the screw holes (Hole1 as indicated on template), and the cable hole (Hole3). If using a gang box (not supplied), make sure to consider its placement within the wall and should not exceed the size of the device.
   NOTE: Gang box is not supplied; purchase separately, as needed.
2. Mount the wall mounting plate on the wall using the supplied screws.
3. Route the cable through the cable hole, wire the cables and insert the cables inside the wall or in the gang box (if any).
   NOTE: Apply silicon sealant among the cable wiring area to keep the raindrom from entering.
4. Connect the cables to the device.
5. Align the device with the mounting plate to hang it, then push it down to lock the device in place.
6. Then attach the bundled lock screws on the bottom hole and two (side holes of the device) to secure the device.

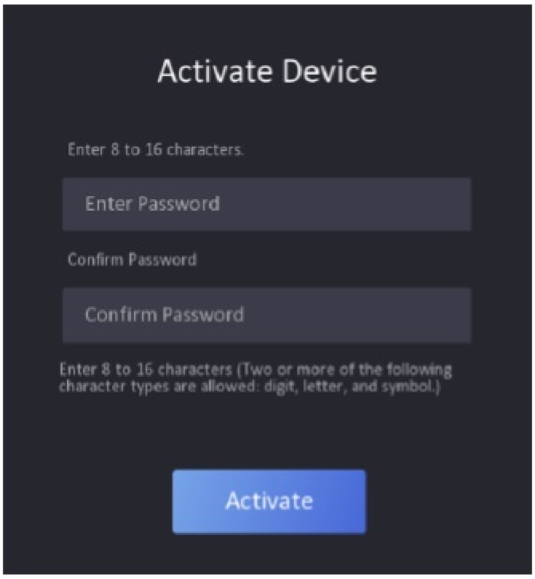


Initial Setup

Before using the device, activate the device first. The easiest way to do this is to activate through the device itself.

Activate via Device

After powering on the device, the system will go to the Activate Device page.

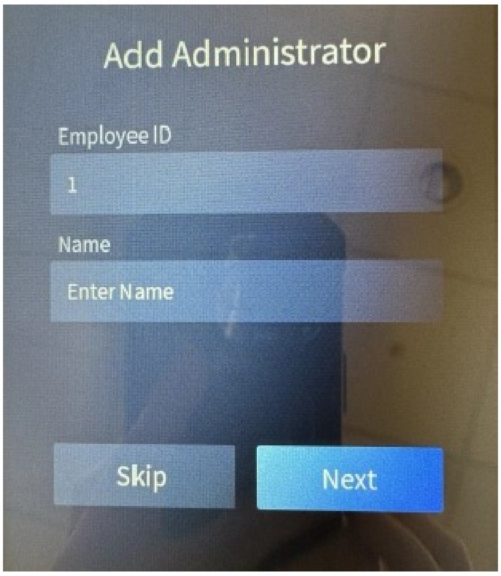


Activate Device

Enter 8 to 16 characters.

Enter 8 to 16 characters (Two or more of the following character types are allowed: digit, letter, and symbol.)

1. On the prompt, create the password. The password should be 8 to 16 characters with digits, upper and lower case letters and symbols.
2. Type again to confirm it, then tap Activate or Next to activate the device.
3. After activation, the device will prompt for basic settings, follow the on-screen prompt to proceed.
4. Select the language, then tap Next.
5. Type the email address to use with the device, then tap Next.
6. Set the network parameters. By default, DHCP is enabled. To continue using DHCP, tap Next. Otherwise, disable DHCP, and then fill in the network parameters manually. See Communication Settings on page 28 for more information.
7. When prompted for access to a third-party platform, retain it as disabled and tap Next to continue.
8. Select the privacy settings according to your actual needs, then cilick Next.
    1. Upload Pic. When Auth.: This function uploads the pictures captured during authetication to the platform automatically.
    2. Save Pic. When Auth.: This function saves the pictures when authenticating to the device.
    3. Save Registerd Pic.: The registered face picture will be saved to the system.
    4. Upload Picture After Linked Cature: This function uploads the pictures captured by a linked camera to the platform automatically.
    5. Save Picture After Linked Capture: This function saves the picture captured by a linked camera to the device.
9. You will be prompted to add an administrator. Enter the Employee ID and Name. Then tap Next.



Add Administrator

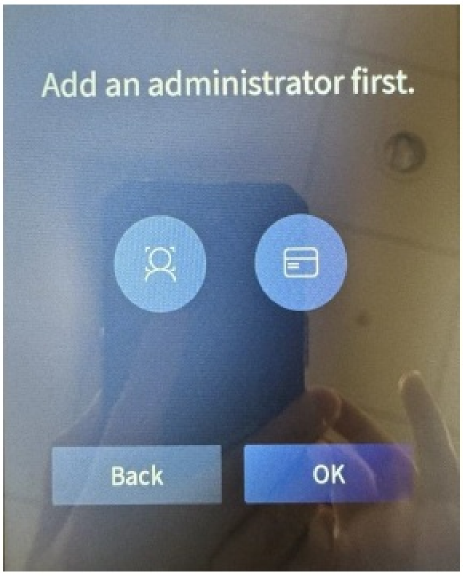
Employee ID

1

Name

Enter Name

10. The Add an Administrator first page appears.



Add an administrator first.

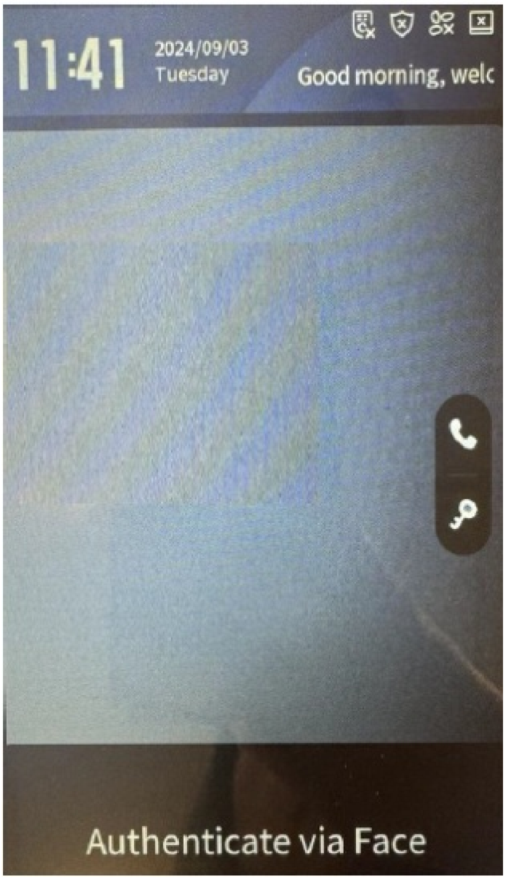
Tap either of the following icons to configure the administrator’s face or card for access:

- Face icon: Tap to capture the administrator’s face. Face forward towards the camera. On the screen, place the face in the face recognition area. Tap 📷 to capture the face and tap the check icon to confirm.
- Card icon: Tap to configure the card access of the administrator. Type

You can configure face recognition or card access or both. Once either face or card has been configured, the system will go back to Add an Administrator’s first page. Repeat step 9 to add another access type or when all access has been configured, tap OK to complete setup.

Main Screen

The Main Screen shows the date and time and status icons on the upper part of the screen. On the right panel are shortcut icons. These functions need integration and are not readily available. If needed, contact your system integrator for details.



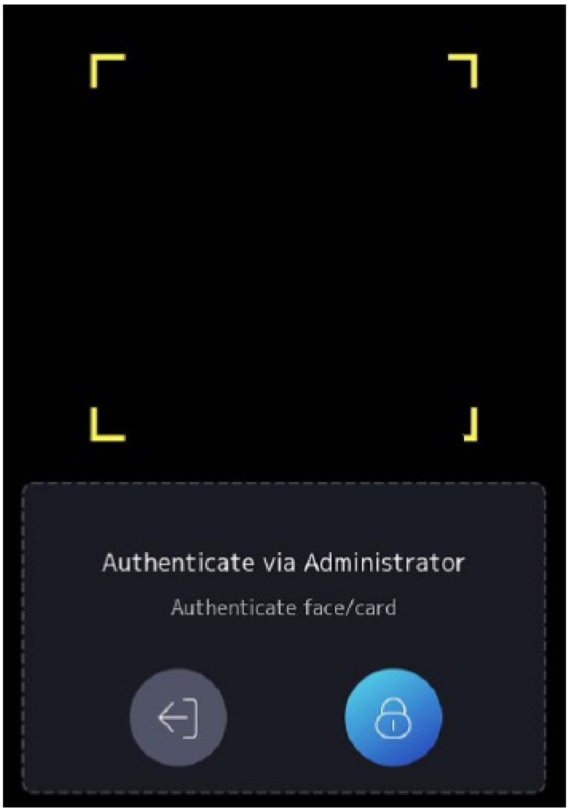
11:41 2024/09/03 Tuesday Good morning, welc

Authenticate via Face

Login

Administrators can log in to the device for device configuration and manage users for access control.

1. Long tap the screen for 3 seconds and slide your finger left / right.
2. Authenticate the administrator’s face or swipe the card to enter the Main Menu page.



Authenticate via Administrator

Authenticate face/card

Alternatively, you can also tap 🔒 to login by entering the device password. Tap ⇦ to exit the login page.

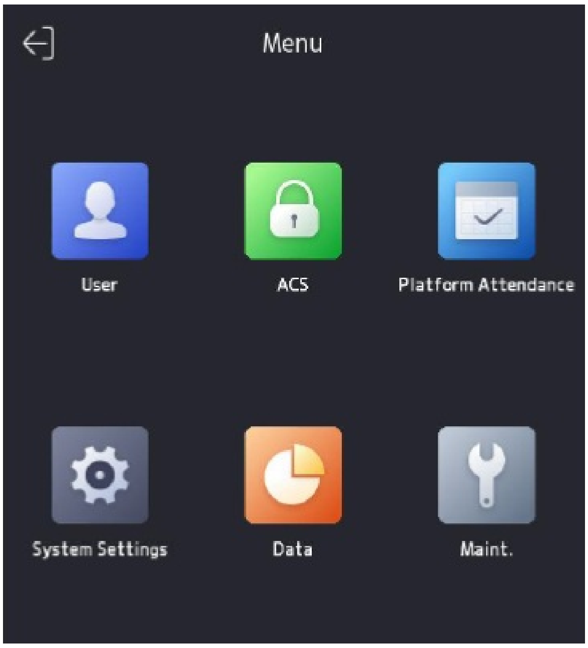
3. Once logged in, the Main Menu page appears

NOTE: The device will be locked for 30 minutes after five (5) failed card attempts are made.

Menu Settings

Menu Page

After login, the Menu page appears. Below is the summary of the Menu.



NOTE: This photo is for reference only, icons and the menu position may slightly vary. Follow the actual menu on the device

Menu Tree

Menu	Description
User	The **User Management** menu allows you to add, edit, delete, and search users, as well as set the authentication mode, permission level, and modify credentials.
ACS (Access Control Settings)	The Access Control Settings (ACS) menu allows you to configure the authentication mode and card encryption to use, door access, etc.
Platform Attendance	The **Platform Attendance** allows you to enable or disable attendance management through the device. Set attendance to manual or auto.
System Settings	The **System Settings** menu allows you to configure communications, basic, biometrics, preferences, and password settings.
Data	The **Data Management** menu allows you to import, export and delete user data.
Maintenance	The **System Maintenance** menu allows you to view the system information, and device capacity, and upgrade, and restore the device to factory settings. **NOTE:** It is not recommended to restore to default factory settings. Instead, contact your sales agents or the customer help desk for assistance.

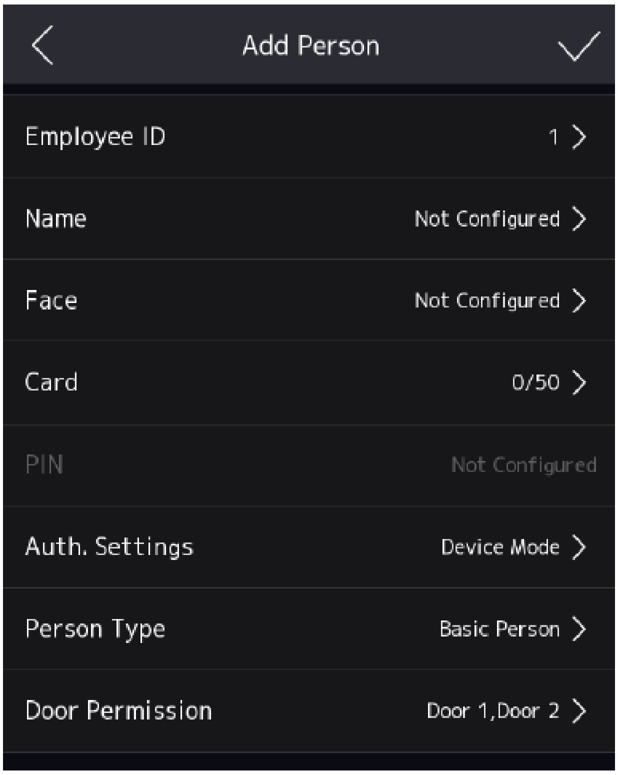
User

The User menu is used for user management; to add, edit, delete, and search for users or employees.

Manage User

Add User

1. On the main menu page, tap User, then tap +.



Add Person

Employee ID	1
Name	Not Configured
Face	Not Configured
Card	0/50
PIN	Not Configured
Auth. Settings	Device Mode
Person Type	Basic Person
Door Permission	Door 1,Door 2

2. Tap the menu items to edit.
    1. **Employee ID:** The employee ID should be less than 32 characters. It can be a combination of lowercase and uppercase letters, and numbers. This should be unique per employee; should not be duplicated.
    2. **Name:** Up to 32 characters are allowed for the Name. Numbers, upper case and lower case letters, and special characters are also allowed.
    3. **Face:** Tap to capture the face picture. See Add Face Picture on page 22.
    4. **Card:** Tap to register a card under this user. See Add Card on page 23.
    5. **Authentication Settings:** Select “Device Mode” to set the device as access control. Or, “Custom” to combine different authentication modes together according to your actual need.
    6. Person Type: Select “Administrator” to set the employee as an administrator or “Basic Person” as a general user.
    7. Door Permission: Select the door(s) to give access to this user.
3. Tap ✓ to complete add user

Edit User

- On the main menu page, tap User.
- Tap a username on the screen to enter the Personal Details page.
- Tap an item to edit its content. The data is automatically saved once you exit the page.

Delete User

- On the main menu page, tap User.
- Tap a username on the screen to enter the Personal Details page.
- Tap 🗑 to delete the user.
- Tap OK to confirm.

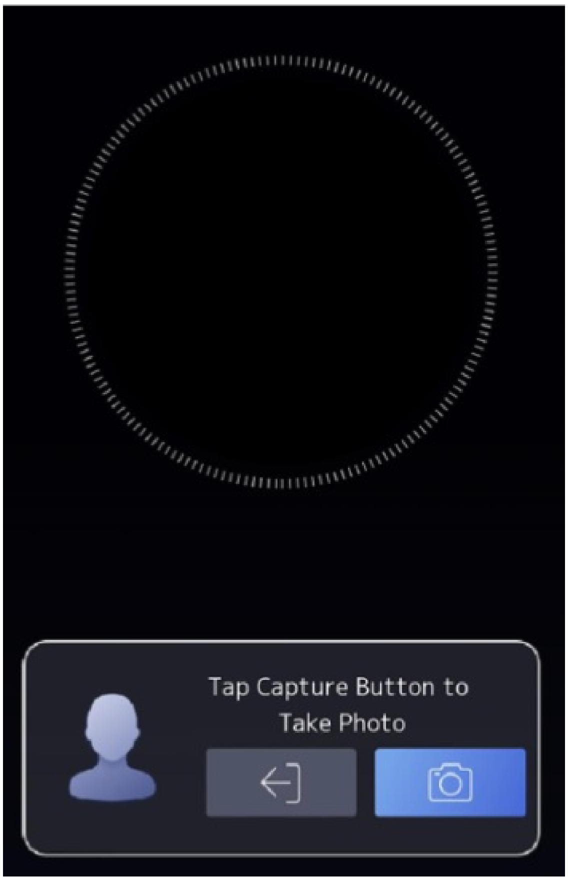
Search User

- On the main menu page, tap User.
- Type the name of the user on the search bar, then click 🔍

Add Face Picture

Add a user’s face picture directly by capturing the face through the device. The face will then be used for authentication.

1. On the main menu page, tap + User, then tap to enter the Add Person page, or tap an existing employee record.
2. Fill in or edit the employee ID and credentials as needed. See Add User on page 20 for details.
3. Tap Face, then position your face towards the circular recognition area



NOTE: Make sure the captured face is in good quality and is accurate. For details about taking the face picture, see Tips in Picture Taking on page 33.

4. Click 📷 to capture the photo.
5. Tap Save to save the face picture. Or, tap Try Again to redo the picture.

Add Card

Add a card for the user to use it for authentication.

1. On the main menu page, tap User, then tap + to enter Add Person page or tap an existing employee record.
2. Fill in or edit the employee ID and credentials as needed. See Add User on page 20 for details.

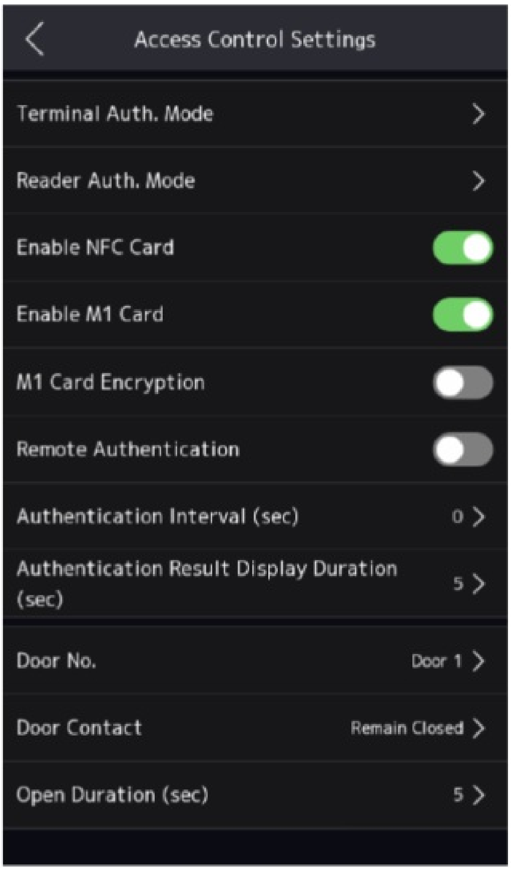
3. Tap Card, and then tap +.
4. Configure the card number: you can enter the card number manually or hover the card towards the device to get the card number.

   NOTE: The card number cannot be empty and it cannot be duplicated.
5. Configure the card type.
6. Tap ✓ to save the settings.

Access Control Settings

After adding a user's face picture or card credentials, go to Access Control Settings to set the authentication mode and access control parameters.

1. On the main menu page, tap 🔒 to access the Access Control Settings (ACS) page



Access Control Settings

Terminal Auth. Mode	>
Reader Auth. Mode	>
Enable NFC Card	●
Enable M1 Card	●
M1 Card Encryption	○
Remote Authentication	○
Authentication Interval (sec)	0 >
Authentication Result Display Duration (sec)	5 >
Door No.	Door 1 >
Door Contact	Remain Closed >
Open Duration (sec)	5 >

2. Tap an item then configure its contents.
   - Terminal Authentication Mode: Select "Single Credential" if only one is required for authentication like either Face or Card. Select "Multiple Credential" if both face and card are required for authentication.
   - Reader Authentication Mode: Select the card reader authentication mode.
   - Enable NFC Card: Enable to use NFC card for authentication.
   - Enable M1 Card: Enable to use M1 card for authentication.
   - M1 Card Encryption: Enable or disable M1 card encryption.
   - Remote Authentication: Enable or disable platform to control whether to grant\ access or not remotely.
   - Authentical Interval: Set the device authentication interval. Available interval range: 0 to 65535 seconds.
   - Authentication Result Display Duration: (1 to 99). Set how long will the authentication result be displayed (1 to 99 seconds) after authentication.

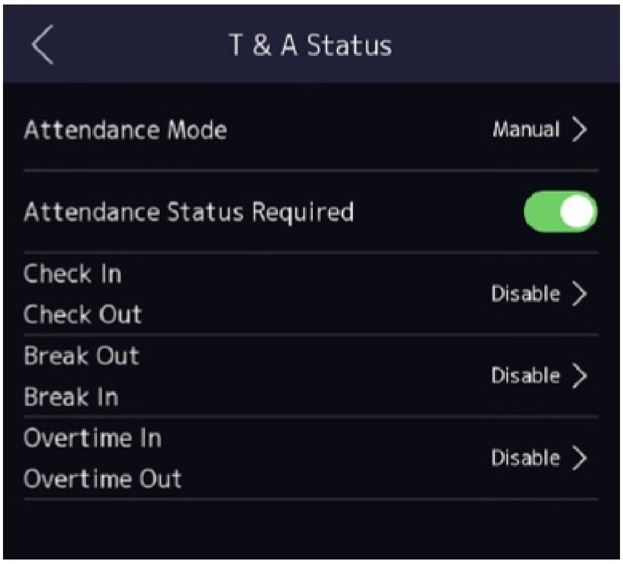
- Door No.: Select the door to configure
- Door Contact: Select “Open (Remain Open)” or “Close (Remain Closed)” according to your actual needs. By default, it si Close (Remain Closed)”.
- Open Duration: Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255 seconds.

3. Tap a menu item and then edit the items

Platform Attendance

The Platform Attendance menu allows you to set the attendance mode as check-in, check-out, break-in, break-out, overtime-in, and overtime-out according to your actual situation.
NOTE: Local Time & Attendance will be disabled when using Platform Attendance.

1. On the main menu page, tap 📅 to access the Platform Attendance page



T & A Status

Attendance Mode: Manual

Attendance Status Required: ●

Check In / Check Out: Disable

Break Out / Break In: Disable

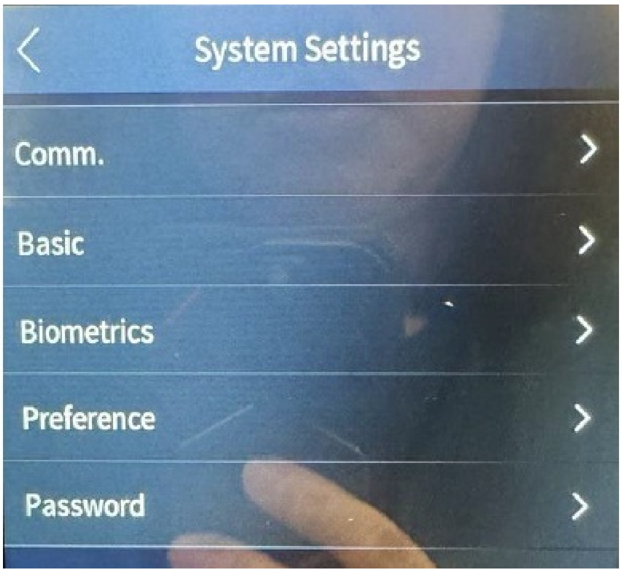
Overtime In / Overtime Out: Disable

2. Tap Attendance Mode and select:
   1. Manual: To manually set the attendace status.
   2. Auto: The system will automatically change the attendance status according to the configured schedule.
   3. Manual and Auto: The system will automatically change the attendance status according to the configured schedule and at the same time, you can manually change the status after the authentication.
3. Enable and disable Attendance Status Required.
4. Enable and disable the Check in/out, Break in/out, Overtime in/out, as needed.

System Settings

The System Settings menu allows you to configure system settings.

1. On the main menu page, tap ⚙ to access the System Settings page



2. Tap a submenu item to modify its settings.

Submenu	Description
Communication	Allows you to configure the network, RS-485, Wiegand, etc. See *Communication* Settings on page 28.
Basic	Allows you to configure sound, time, sleep, langauge, privacy, video standard, etc.
Biometrics	You can customize face parameters to improve the face recognition performance. S ee *Biometric Parameters* on page 29.
Preference	Allows you to select the screen theme and enable or disable shortcut keys.
Password	Allows you to modify the device password set during the initial setup.

Communication Settings

You can set the wired network, the Wi-Fi parameter, the RS-485 parameters, the Wiegand parameters, ISUP, and access to Hik-Connect on the communication settings page.

Set Wired Network

1. On the System Settings page, tap Comm. > Wired Network.
2. Enable DHCP for the system to automatically assign IP address, subnet mask, and gateway. Disabled DHCP to manually set the IP address, subnet mask, and gateway. NOTE: The device must be in the same network segment with the computer.
3. Set the DNS parameters. You can enable Auto Obtain DNS, set the preferred DNS server and the alternate DNS server.

Set RS-485 Parameters
The device can connect to an external access controller, secure door control unit or card reader via RS-485 connection.

1. On the System Settings page, tap Comm. > RS-485.
2. Enable RS-485.
3. Tap Peripherals, then according to your actual needs, select the type of external device to connect: Access Controller, Control Unit, Card Reader, or Elevator Module. NOTE: If Access Controller is selected:
    1. If the device is connected to a terminal, set the RS-485 address as 2
    2. If the device is connected to a controller, set the RS-485 address according to the door number.
4. Tap the back icon at the upper left corner to save the settings. If any changes are made, reboot the device.

Set Wiegand Parameters

1. On the System Settings page, tap Comm. > Wiegand.
2. Enable Wiegand.
3. Select a transmission direction:
    1. Input: To connect the device to a wiegand card reader.
    2. Output: To connect the device to an external access controller. The two devices will transmit the card number via Wiegand 34.
4. Select how the two devices will transmit the card no.: via Wiegand 26 or Wiegand 34.

Set ISUP Parameters
Set the ISUP parameter for the device to upload data via the ISUP protocol.

1. On the System Settings page, tap Comm. > ISUP.
2. Enable the ISUP function and set the ISUP server parameters:

Submenu	**Description**
Central Group	Enabled the central group to upload the data to the center group.
Main Channel	Supports N1 or none.
IS UP	Enable ISUP and set the ISUP parameters like, protocol version, address type, IP address, etc. where data will be uploaded.

Biometric Parameters

You can customize the face parameters to improve face recognition performance.

1. On the System Settings page, tap Biometrics.
2. Tap a submenu item to modify its settings.

Submenu	Description
Face Liveliness Level	Set the matching security level when performing live face authentication.
Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Face Recognition Interval (sec)	The interval time between two continuous face recognitions when authenticating. Allowable range from 1 to 10 seconds.
Wide Dynamic	Use the Wide Dynamic Range function to balance the brightness of the whole image to provide clear images with details. It is recommended to enable WDR function if the device is installed outdoors or when there are both very dark and very bright areas simultaneously in view.
Face 1:N Security Level	Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
Face 1:1 Security Level	Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate, and the larger the false rejection rate
Eco Mode	After enabling the ECO mode, the device will use the IR camera

Settings	to authenticate faces in the low-light or dark environments. You can set the ECO mode threshold, ECO mode (1:N), ECO mode (1:1), Face with mask & face (1:1 ECO), and Face with mask & face (1:N ECO). **ECO Threshold:** When enabling the ECO mode, you can set the ECO mode's threshold.The larger the value, the easier the device entering the ECO mode. **ECO Mode (1:1)**: Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. **ECO Mode (1:N):** Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate
Hard Hat Detection	If needed, enable this setting and then set the reminder strategy: **Reminder of Wearing:** If a person is not wearing the hard hat during authentication, the device will pop up a prompt reminder and the door will open. **Must Wear:** If the person is not wearing the hard had during authentication, the device will pop up a prompt reminder, and the door will remain close. **None:** Even If the person is not wearing the hard had, no notification will be done.
Mask Settings	When enabled, the system will recognize the captured face with mask picture. You can set face with mask & face 1:N level and the strategy. **Face with Mask & Face (1:1):** Set the matching value when authenticating with face mask via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. **Face with Mask & Face (1:N):** Set the matching value when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. **Prompt**: Set the **None**, **Reminder of Wearing** and **Must Wear** prompt. · **Reminder of Wearing:** If the person does not wear a face mask when authenticating, the device displays a notification, and the door will open. · **Must Wear:** If the person does not wear a face mask when authenticating, the device displays a notification, and the door remains closed. · **None:** If the person does not wear a face mask when authenticating, the device will not prompt a notification.
Multiple Faces **Authentication**	If enabled, authentication of multiple faces will be supported.

Preference Settings
You can set some preferences like shortcut key behavior, call type, etc.

Set Shortcut Key

1. On the System Settings page, tap Preference > Shortcut Key.
2. Choose the shortcut key to display on the authentication page:
    1. Password: Enable to display password entry shortcut.
    2. Call: Enable to display of the call function shortcut key on the authentication page.

Then, select the type of call to make when the call button is pressed on the authentication page:

- Call Room: To dial a room number to call.
- Call Center: To call the center directly.
- Call Specified Room Number: To call the room number directly.
- Call APP: Call the mobile client where the device is added.

Set Theme Mode
On the System Settings page, tap Preference > Theme Mode. Then select:

- Authentication: Live view of the authentication page will be disabled on the screen.
- Advertisement: The advertising area and identification area (bottom of the screen) of the device will be displayed on the screen. Video and advertising information playback and welcome speech display are supported.

Password Settings
To change the password, go to the System Settings page, then tap Password. Follow the on-screen instructions to change the password.

Data

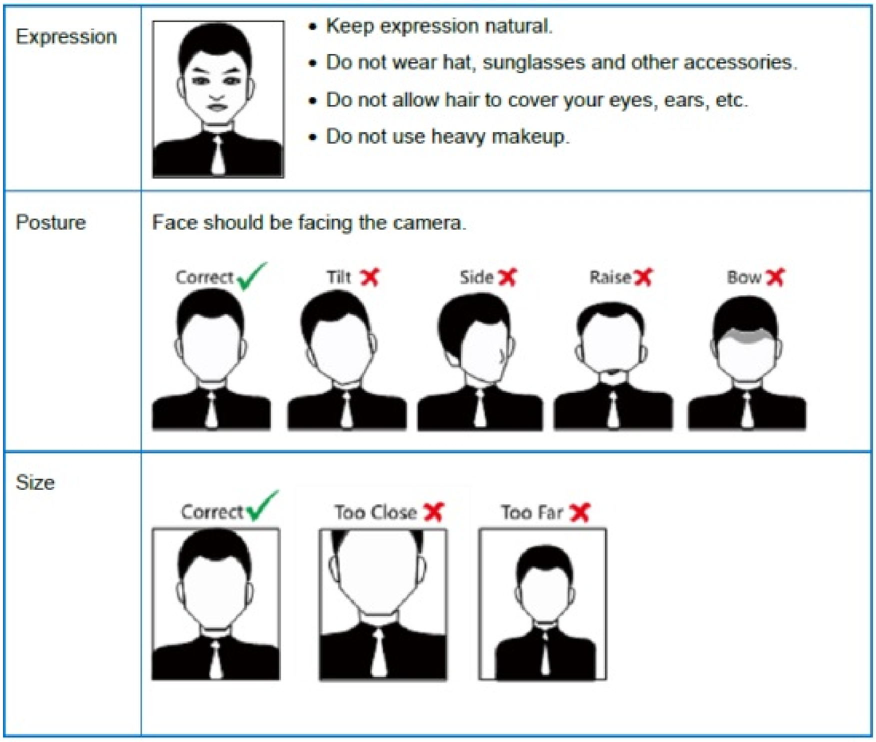
The Data menu allows you to import, export, and delete user data on the device. For importing and exporting data, an external USB flash drive is required. Then follow the on-screen instructions to import / export data. On the main menu page, tap ◔ to access the Data page

Maintenance

The Maintenance menu allows you to view the system information, and device capacity, reset or restore factory default settings, and reboot device. On the main menu page, tap 🔧 to access the Maintenance page.

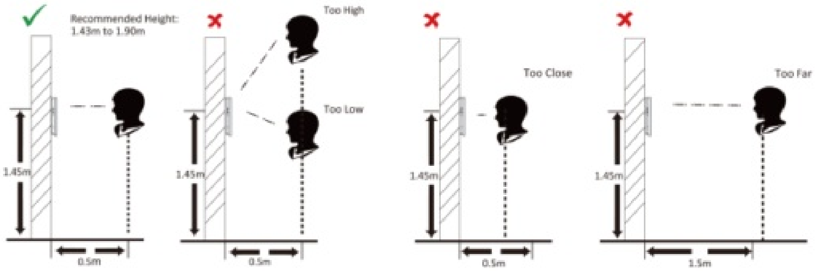
Tips in Picture Taking

Take note of the correct expression, posture, and size of the face when taking the face photo to ensure recognition accuracy.



Expression	- Keep expression natural. - Do not wear hat, sunglasses and other accessories. - Do not allow hair to cover your eyes, ears, etc. - Do not use heavy makeup.
Posture	Face should be facing the camera. Correct ✓ Tilt ✗ Side ✗ Raise ✗ Bow ✗
Size	Correct ✓ Too Close ✗ Too Far ✗

Positions When Taking or Authenticating Face



CONTACT

- 7F, No. 1, Alley 20, Lane 407, Sec. 2, Ti-Ding Blvd., Neihu District, Taipei, Taiwan 114, R.O.C.
- TEL : +886-2-2656-2588
- FAX: +886-2-2656-2599
- Email: sales@acti.com

Documents / Resources

 Face Recognition Reader & Controller User's Manual R71CF-313 ACTi	ACTi R71CF-313 Face Recognition Reader and Controller [pdf] User Manual R71CF-313 Face Recognition Reader and Controller, R71CF-313, Face Recognition Reader and Controller, Reader and Controller, and Controller, Controller

References