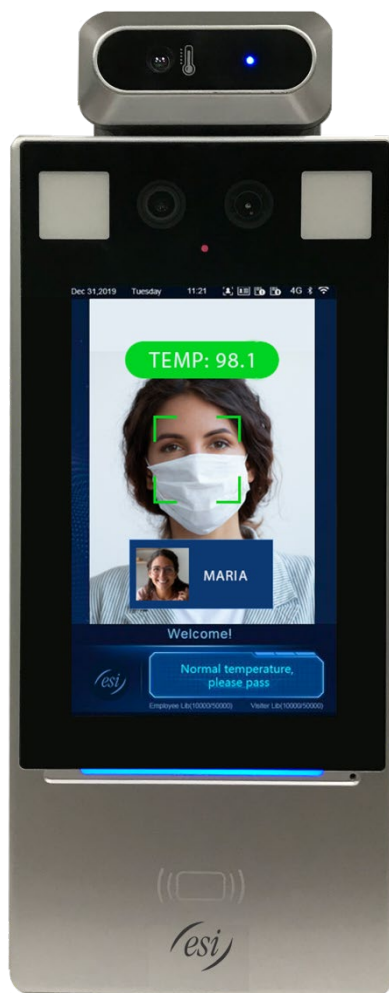


esi 5D Access Thermal Reader

User's Guide

This User Guide is intended to give users a basic understanding of how to use this device and how it operates. See Administrator Manual for more detailed setup information.



Contents

<i>Local Operations</i>	<i>6</i>
<i>Main Interface</i>	<i>6</i>
<i>Mask/Temperature Measurement Interface</i>	<i>9</i>
<i>Activation Config</i>	<i>15</i>
Basic Info	17
Device Location	17
Network Setting	19
User Management	20
Activation Password	24
Admin Password	25
Authentication Scene	26
<i>Door Opening Method</i>	<i>28</i>
Face Scan-based Door Opening	28
Card Swiping-based Door Opening	29
QR Code-based Door Opening	30
Remote Opening	30

Disclaimer

No part of this manual may be copied, reproduced, translated, or distributed in any form or by any means without prior written consent from Estech Systems, Inc. (ESI).

The manual may be updated from time to time due to version upgrade or other reasons.

The manual is for reference only. All the statements, information, and suggestions contained herein do not constitute warranties of any kind, express or implied.

Estech Systems, Inc. (ESI) shall not under any circumstances be liable for any special, consequential, incidental or indirect damages arising from the use of this manual or Estech Systems, Inc. (ESI)'s product, including but not limited to any loss of commercial profits, losses caused by missing data or documents, and anomalies during product running or information leakage due to cyber-attacks, hacker attacks, or virus attacks.

Before performing operations, be sure to carefully read through and observe safety specifications in this manual.

- Screenshots provided in this document are used as examples only and the UI layout varies with versions.
- Estech Systems, Inc. (ESI) (hereinafter referred to as "ESI") reserves the right to modify the content in this manual without prior notice or prompt, but ESI does not ensure that this manual is completely error-free.
- Subject to uncertain factors such as the physical environment, actual values of data may differ from the reference values described here. In case of any question or dispute, the right of final interpretation resides with ESI.
- Follow operational instructions in this manual when using the product. ESI is not responsible for problems caused by the violation of the instructions. Thank you for your cooperation.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

HIPPA Compliance

The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").¹ The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in the end notes. Visit our Privacy Rule section to view the entire Rule, and for other additional helpful information about how the Rule applies. In the event of a conflict between this summary and the Rule, the Rule governs.




[HHS.gov/HIPPA](https://www.hhs.gov/HIPPA)

Conventions

- The figures, charts or photos in this manual are used for illustration only, which may differ from the actual product.
- Subject to uncertain factors such as the physical environment, actual values of some data may differ from the reference values described here. In case of any question or dispute, the right of final interpretation resides with ESI.
- Follow this manual when using the product. Professional guidance is recommended.
- National conventions used in this document are described as follows:

Format	Description
Boldface	Indicates buttons, menus, tabs, window names, dialog names, and parameter names. For example, click OK or select Device Management .
" "	Indicates messages. For example, "Hanging Up" is displayed on the interface.
>	Directs you to go to a multi-level menu. For example, go to Device Management > Add Device . In this example, Add Device is a submenu under Device Management .

- The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.




Symbol	Description
 WARNING!	Contains important safety instructions and indicates situations that could cause bodily injury.
 CAUTION!	Means reader be careful and improper operations may cause damage or malfunction to product.
 NOTE!	Means useful or supplemental information about the use of product.

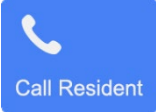



Local Operations

Main Interface

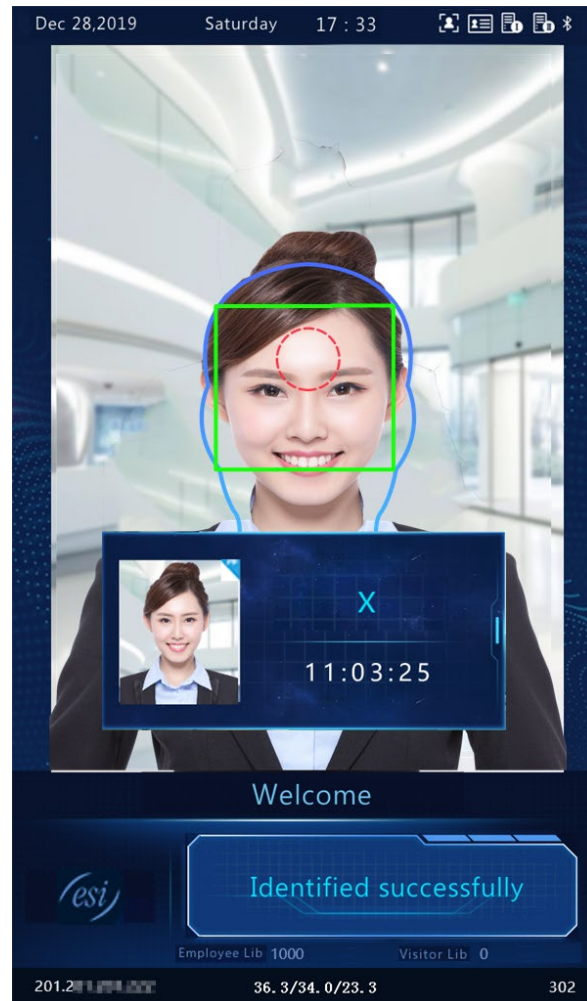
Main Interface (Video Intercom Mode)



No.	Description
1	<p>Displays the current date, time, and connection status of different services.</p>  <p>Indicates the following items from left to right:</p> <ul style="list-style-type: none"> • Whether to enable the face scan mode • Whether an ID card reader is connected properly • Whether server 1 is online • Whether server 2 is online <p> NOTE!</p> <p>An icon marked with  indicates "No".</p>

2	<ul style="list-style-type: none"> • Total : Total number of detected people • Normal : Number of people with normal temperature <p>This interface is only displayed when the temperature measurement function is enabled. For detailed operation descriptions, see Advanced Setting.</p>	
3	<p>Displays the photo and name of an identified person in the library. Refer to "Display" to enable the 5D Access Thermal Reader to display one or more registered face pictures.</p> <p>When Multiple Faces is selected, information about the latest person identified successfully is displayed on the left of the screen. The interface can display information about five recent people successfully identified.</p>	
4		Calls a resident. For detailed operation descriptions, see "Call Resident" .
		Enters a password to open the door. For detailed operation descriptions, see "Password-based Door Opening" .
		Calls the management center. For detailed operation descriptions, see "Call Management Center" .
		QR code used for door opening. For detailed operations, see "QR Code-based Door Opening" .
5	Title bar, which can be defined by users. For detailed operations, see "Custom Logo and Prompt" .	
6	Logo bar, which can be defined by users. For detailed operations, see "Custom Logo and Prompt" .	
7	Displays the identification result (such as identified successfully or unregistered person), authentication mode (such as face scan or card swiping), and other information.	
8	Displays the number of people in the employee library and in the visitor library.	
9	<p>Status bar at the bottom</p> <p>Displays the device IP address, real-time temperature, preset minimum temperature, ambient temperature, and match time.</p>	

Main Interface (Common Access Control Mode)



The main interface does not support Call or QR code based door opening in the common access control mode. The GUI displays the recognition result of only a single person.

Mask/Temperature Measurement Interface

In response to the current epidemic, companies, parks, and communities take temperatures and check mask wearing for people passing through the entrances and exits. The work is performed by people manually, which is exhausting and increases the risk of cross-infection. The 5D Access Thermal Reader is capable of checking whether people are wearing masks and taking their temperatures. An intelligent digital detection module is required, and the forehead temperature can be taken. For people with abnormal temperature (exceeding the preset maximum temperature threshold) or without masks, the 5D Access Thermal Reader displays an alarm on the GUI, plays a warning sound, and determines whether to open the door based on actual application scenes, thereby helping to achieve epidemic prevention and control. For detailed configuration, see “**Intelligent — Advanced Setting**” and “**Authentication Scene**”.



NOTE!

- When the temperature measurement function is enabled to take the forehead temperature, a person needs to get close to occupy the human shape on the screen, and aim their forehead center at the red circle .
- Ensure that the forehead is at a proper distance from the Intelligent Digital Detection Module. The recommended distance is 0.5–0.7m.
- When the forehead temperature needs to be taken, the forehead cannot be covered by fringes, hats, sunglasses, or other objects.
- The temperature measurement function requires an Intelligent Digital Detection Module, which can be connected to the 5D Access Thermal Reader through the RS485 connection. For the configuration, see “**Serial Port**”.
- Do not use the Temperature Measurement Function together with the Safety Helmet/Safety Module Function.

Mask detection and temperature measurement

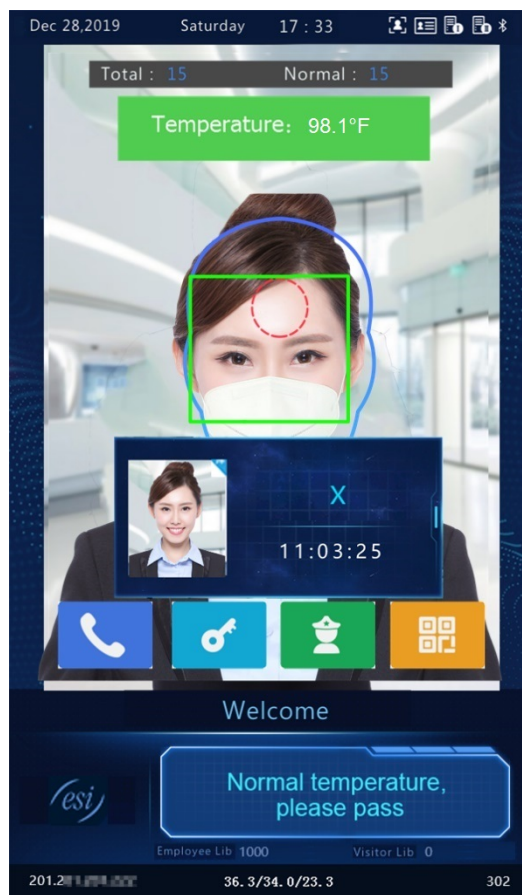
Enable both the Mask Detection and Temperature Measurement functions on the 5D Access Thermal Reader. When a person (whose information is stored in the library) passes through the terminal, the GUI displays the detection result.



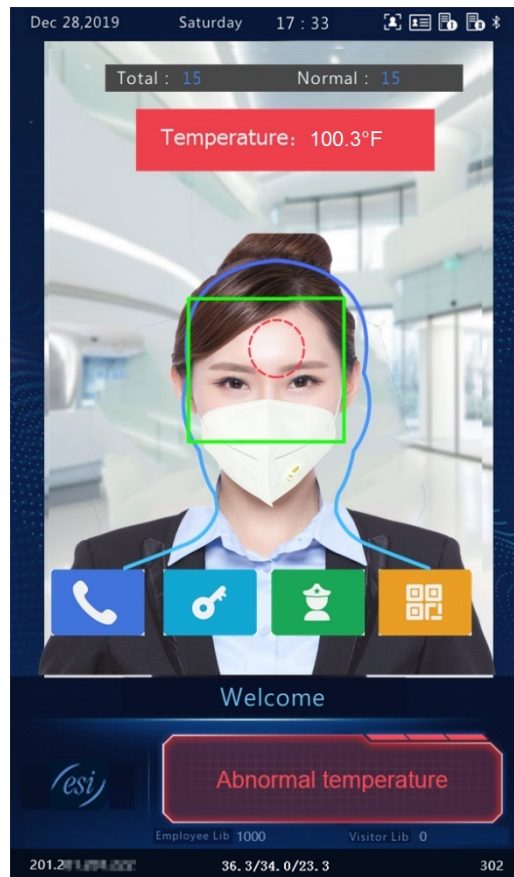
NOTE!

The following figures show examples of interfaces of forehead temperature measurement.

Normal Temperature and Mask Worn



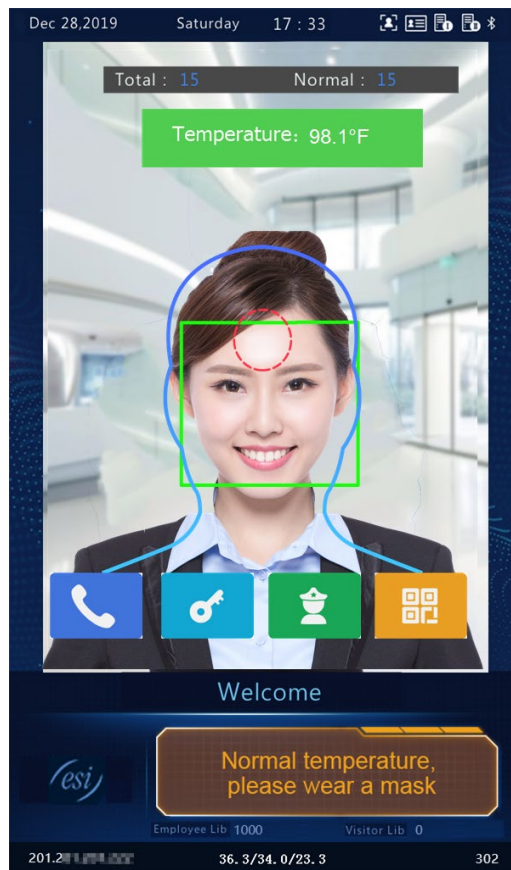
Mask Worn but Abnormal Temperature



NOTE!

When both the temperature measurement and mask detection functions are enabled, temperature measurement is prior to mask detection. Once an abnormal temperature is detected, an "abnormal temperature" alarm is reported on the GUI and the warning sound is played no matter whether the person wears a mask or not.

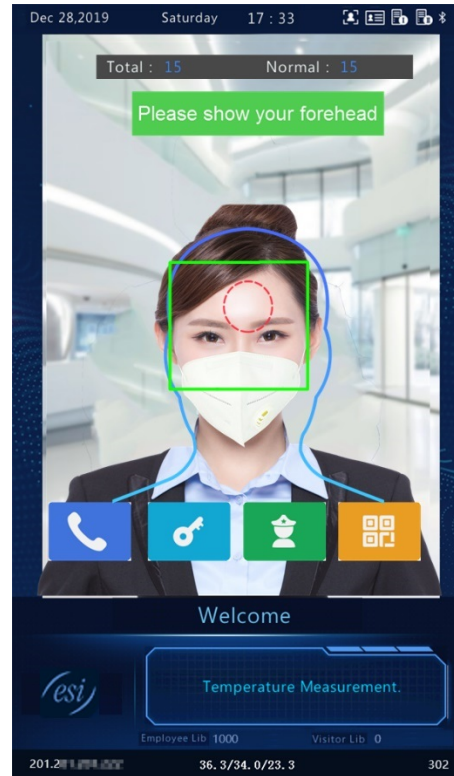
Normal Temperature but Mask Not Worn



Temperature measurement mode

The 5D Access Thermal Reader supports pure temperature measurement mode, in which the temperature measurement function is enabled, but no authentication mode is configured in the face library (for details, see **“Face Library Management”**). In this mode, the 5D Access Thermal Reader determines whether to open the door based on actual scenes for people with abnormal temperatures. For detailed configuration, see **“Intelligent — Advanced Setting”**.

Temperature Measurement Mode

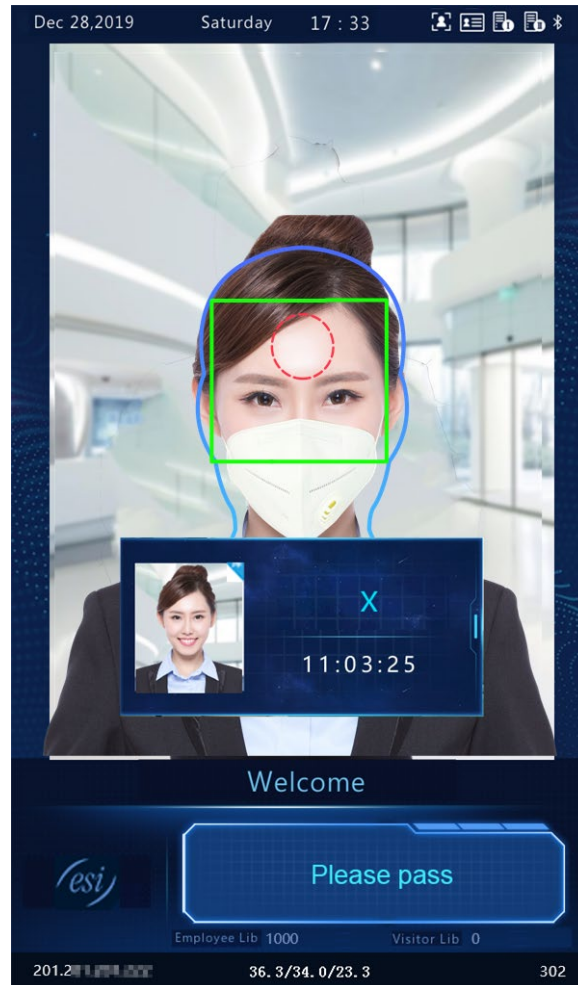


- Normal Temperature: The temperature of a detected person is normal. For the prompt on the GUI and voice prompt.
- Abnormal Temperature: The temperature of a detected person is abnormal. For the prompt on the GUI and voice prompt.

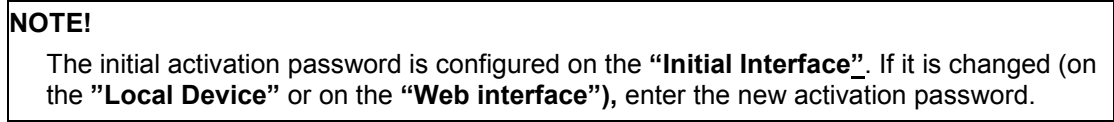
Mask detection

The 5D Access Thermal Reader supports mask detection. When a person (whose information is stored in the library) does not wear a mask, an alarm is reported on the GUI and a warning sound is played. For those who do not wear masks, the terminal determines whether to open the door based on actual scenes. For detailed configuration, see **“Intelligent — Advanced Setting”**.

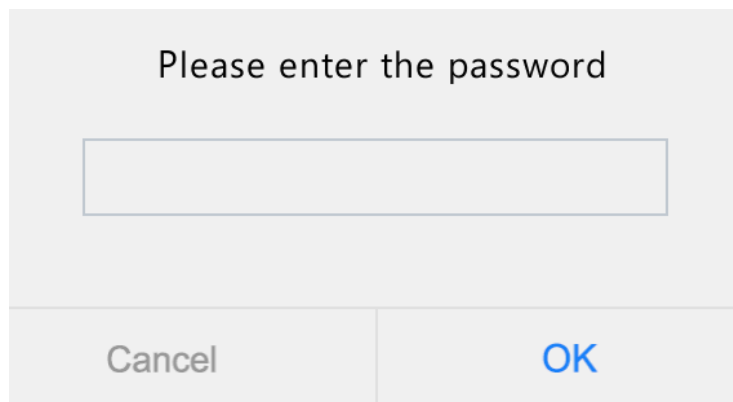
Mask Worn



Press and hold your finger on the main interface of the 5D Access Thermal Reader (longer than 3 seconds) until the password input interface appears. In the displayed password input interface, enter the configured activation password to go to the “**Activation Config**” interface. If you forget the password, contact ESI to seek help.



Activation Password Input Interface

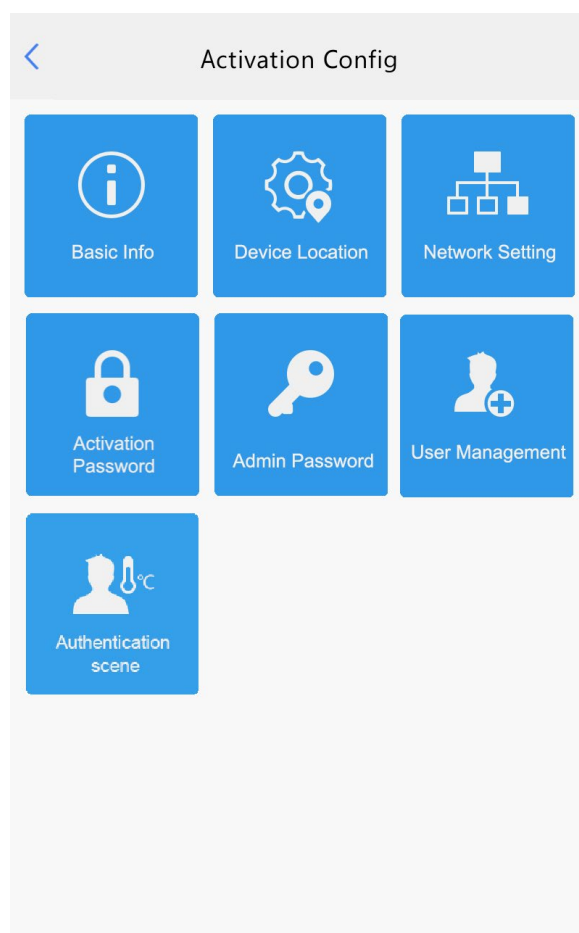


Please enter the password

Cancel OK

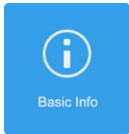
On the “**Activation Config**” interface, you can view basic information about the 5D Access Thermal Reader, configure the device location, network and password and input personnel information and authentication scene.

Activation Config Interface



Basic Info

The “**Basic Info**” interface allows you to view the status of the current device in real time so as to rapidly know about the device condition and better maintain the device.



- On the “**Activation Config**” interface, tap  to go to the “**Basic Info**” interface.

Basic Info Interface

Basic Info	
Model	OET-213H
Firmware Version	PTS_Q2101-80000001_0007
Hardware Version	A
Boot Version	V1.2
Serial No.	210235C3VC4821600063
Network	204.41.128.178/255.255.255.0/24-4.1.1
MAC Address	48:9e:8b:8b:8b:8b
System Time	2019/9/27 17:09:18
Operation Time	0Day(s)0Hour(s)53Minute(s)
Management Server	Offline(0.0.0.0:5060)
Edge Storage	Normal

Device Location

On the “**Device Location**” interface, you can configure the community, unit, and management center to which the device belongs.




- On the “**Activation Config**” interface, tap  to go to the “**Device Location**” interface.

Device Location Interface

Configure device location information by referring to the table below.

Parameter Description and Configuration

Parameter	Parameter Description and Configuration
Management Center IP	<p>Enter the IP address of the management center.</p> <p>After configuration, a user can tap “Call Management Center” on the GUI to call the management center.</p> <p> NOTE!</p> <p>The management center IP address must be in the same network segment as the device and <u>cannot</u> begin with 127.</p>
Community	<p>Enter the name of the community to which the device belongs.</p> <p>A string of 1 to 35 characters can be entered.</p>
Building	<ul style="list-style-type: none"> Enter the No. of the building where the device is located. The value must be an integer in the valid range of 1 to 99.
Configurable Units	<p>Select the quantity of units that can be served by the device from the drop-down list.</p> <p>The options include 1, 2, and 3.</p>
Unit	<p>Enter the No. of the unit where the device is located.</p> <p>The value is an integer in the valid range of 1 to 9.</p>

- Tap **“Save”** to complete the device location information configuration.

Network Setting

On the “**Network Setting**” interface, you can modify the device IP address and other communication parameters so that the device can communicate with external devices.



On the “**Activation Config**” interface, tap  to go to the “**Network Setting**” interface.

Network Setting Interface

A screenshot of a mobile application interface titled "Network Setting". It features a back arrow on the top left. Below the title, there are three rows of configuration fields: "IP Address" with the value "204.4.1.249", "Subnet Mask" with "255.255.255.0", and "Default Gateway" with "204.4.1.1". Each field has a small icon to its right. Below these fields is a large, empty grey rectangular area. At the bottom of the interface is a white bar with a blue "Save" button.

Set network parameters by referring to the table below.

Parameter	Parameter Description and Configuration
IP Address	Enter the IP address of the device. The IP address of the device must be unique across the network.
Subnet Mask	Enter the subnet mask of the device.
Default Gateway	Enter the default gateway of the device.

Tap “**Save**” to complete network setting.

User Management

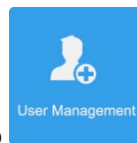
The 5D Access Thermal Reader allows you to input personnel information. Personnel whose information has been input to the device successfully can swipe cards or credentials, or have their faces scanned for access.

Face photo collection requirements

When adding a person to the whitelist, collect the face photo by strictly observing the following requirements:

- General requirement: bareheaded full-face photo. Only the face photo of the person under collection is displayed on the screen of the terminal during collection and face photos of other people cannot be contained.
- Range requirement: The photo should show the outline of a person's ears and cover the range from the top of the head (including all hair) to the bottom of the neck.
- Position requirement: The face must be positioned within the limit box on the interface of the terminal during collection.
- Makeup requirement: There should be no cosmetic color that affects the true appearance during collection, such as eyebrow makeup and eyelash makeup.
- Background requirement: The white, blue, or other pure color background is acceptable.
- Light requirement: Light with appropriate brightness is required during collection. Too dark photos, too bright photos, and light- and dark-colored face photos should be avoided.

Personnel information input operation process



On the “**Activation Config**” interface, tap to go to the “**User Management**” interface.

User Management Interface

A screenshot of the "User Management" interface on a mobile device. The interface has a light gray background. At the top, there is a blue header bar with a white back arrow on the left and the text "User Management" in the center. Below the header, there are several input fields: "Name" with a text input box, "Gender" with two radio buttons labeled "Male" (selected) and "Female", "Card No." with a text input box, and "ID No." with a text input box. Below these fields is a section labeled "Face Picture" with a counter "0/1". Under "Face Picture", there is a large gray square with a white plus sign in the center, indicating where to tap to add a face picture. At the bottom of the interface, there is a blue button labeled "Save".

- Configure personnel information input by referring to the table below.

Parameter	Parameter Description and Configuration	Remarks
Name	Mandatory. Enter the name of a person.	/
Gender	Enter the gender of the person. Select Male or Female from the drop-down list. The default value is Male .	/
Card No.	Enter the card No. of the person. After successful input, the person can swipe the card for access.	At least one of the parameters needs to be set so that personnel information can be input successfully.
ID No.	Enter the ID card No. of the person. After successful input, the person can swipe the ID card for access.	
Face Picture	Collect and input face photos by referring to the “face photo collection process” . After successful input, the person can have their face scanned for access.	

Perform the following operations to collect and input a person's face photo.

- Follow the prompt on the interface and ask the person to face the camera.


- When the photo displayed on the GUI meets **“face photo collection requirements”**, tap  to collect the face snapshot.



is the back button.

Collecting and Inputting a Face Photo



On the photo confirmation interface, tap  to confirm the collected photo.


 is the back button.

Photo Confirmation Interface



On the “**User Management**” interface, tap “**Save**” to complete the personnel information input.

Save Interface

<

User Management

Name

Jack

Gender

☒ Male ☐ Female


Card No.

123

ID No.

Face Picture

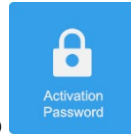
1/1



Save

Activation Password

To change the configured activation password, do as follows:



On the “**Activation Config**” interface, tap to go to the “**Activation Password**” interface.

Activation Password Interface

< Activation Password

Please enter the old password

Please enter the new password

Confirm

At least two from the following are required:
uppercase letter(A-Z), lowercase letter(a-z), digit(0-9), underscore(_) and
hyphen(-).

Save

Enter the old password, new password, and confirm the new password as required.



NOTE!

- The password must contain at least eight characters (including at least two of the following types: upper case letters, lower case letters, digits, underscores, and hyphens).
- The confirmation password must be consistent with the new password.
- The activation password is consistent with the password for the **admin** to log in to the Web interface. If the activation password is changed, use the new password to “**log in to the Web interface**”.

Tap **Save** to complete the activation password change.

Admin Password

On the “**password-based door opening interface**”, users can enter an admin password to open the door. The admin password is applicable to device managerial personnel (such as people in the management center).

The admin password is disabled by default. If you need to enable the admin password, tap “**Yes**” and enter passwords in “**Password**” and “**Confirm**”.



NOTE!

- The password must be a string of eight characters.
- The confirmation password must be consistent with the password.

Admin Password Configuration Interface

Password Configuration

Enable ☐ Yes ☒ No

Password

Confirm

Tip: Please enter a 8-character password.

Save

Authentication Scene

This interface allows you to configure terminal authentication scenes, temperature measurement range, temperature alarm value, and other data. The table below describes the detailed configuration.

Authentication Scene Interface

<

Authentication scene

☒

Temperature Measurement Only

☐

Face Recognition + Temperature Measurement

☐

Face Authentication + Temperature Measurement

Tip: For more authentication configuration, please log into the web interface.

Mask Detection

Temperature Range

95.9 °F ~ 107.6 °F

Temperature Alarm Threshold

99.1 °F

Tip: Exceeding the alarm threshold is abnormal high temperature.

Save

Parameter		Description and Configuration
Authentication Scene	Temperature Measurement Only	<p>The 5D Access Thermal Reader only measures people's temperatures and does not conduct another authentication. For the prompt on the GUI, see “Temperature Measurement Mode”.</p> <p>Note: In this scene, the authentication modes of all libraries configured in the 5D Access Thermal Reader will be cleared.</p>
	Face Scan + Temperature Measurement	<p>A person is allowed to pass only after the face authentication is successful and the temperature is normal. For the prompt on the GUI, see “Mask Detection and Temperature Measurement”.</p>
	Face Authentication + Temperature Measurement	<p>The face whitelist mode + temperature measurement mode is adopted.</p> <p>A person (whose information is stored in the library) is allowed to pass only after the face authentication is successful and the temperature is normal. For the prompt on the GUI, see “Mask Detection and Temperature Measurement”.</p> <p>Note: This scene can be configured only when the default employee library exists under “Face Library Management”.</p>
Mask Detection		Enable or disable it based on actual application scenes.
Temperature Configuration	Temperature Measurement Range	<p>Value range: [86.0F – 113.0F] - [30C–45C];</p> <p>Default range: [95.0F – 107.6F] - [34C–42C]</p> <p>Configure the range based on actual application scenes.</p>
	Temperature Alarm Threshold	<p>When the digital detection module detects a temperature higher than the threshold configured here, the "abnormal temperature" alarm is displayed on the GUI and the warning sound is played.</p> <p>Value range: [86.0F – 113.0F] - [30C–45C];</p> <p>Default value: [99.14F] – [37.3C]</p>

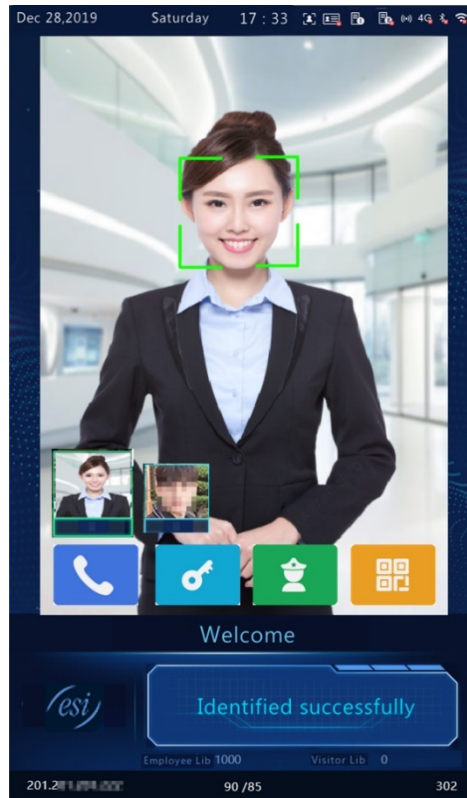
Door Opening Method

Face Scan-based Door Opening

The 5D Access Thermal Reader matches a collected face photo with photos in the face photo library.

- If the match is successful, an interface as shown in the figure below is displayed, the audio **"Recognized successfully"** is played, and the door is successfully opened.

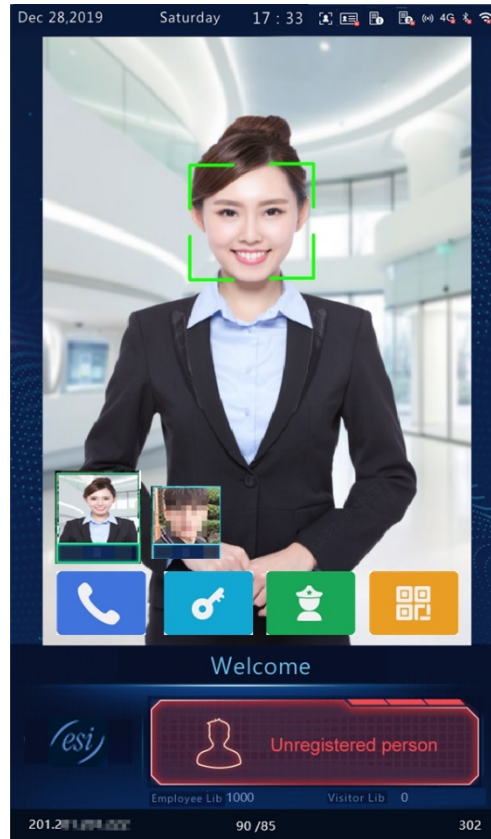
Successful Recognition Interface



- If the match fails, an interface as shown in the figure below is displayed and the audio **"Unregistered person"** is played. You can try other methods to open the door.

Note: Only applies when Digital Thermal Detection Module not installed.

Unregistered Person Interface



- Other face scan-based door opening failures

Some failures may arise during face scan-based door opening. The prompts displayed on the interface are as follows and the effect is similar to the “**Unregistered Person**” interface.

- Not a real person.
- Unscheduled access.
- Please face the camera.

Note: Only applies when Digital Thermal Detection Module not installed.

Card Swiping-based Door Opening

- People can swipe their cards on the 5D Access Thermal Reader to open the door.
- When a card reader is connected to the 5D Access Thermal Reader, people can swipe their cards in the card scan area to open the door.




NOTE!

People's card information needs to be sent to the 5D Access Thermal Reader in advance.

QR Code-based Door Opening

The 5D Access Thermal Reader supports QR code-based door opening.

- Tap  on the main interface to go to the QR code interface.
- Aim the generated QR code towards the camera of the 5D Access Thermal Reader or a connected QR code scan device. The recognition will be successful, and the door will be open.



NOTE!

If no operation is performed on the QR code interface within 30 seconds, the 5D Access Thermal Reader automatically switches to the live view interface.

Remote Opening

After the door is opened remotely, the 5D Access Thermal Reader notifies the user of the door opening by displaying and playing a prompt.

After the 5D Access Thermal Reader is connected to an indoor monitor, and the configuration is complete, operations can be performed on the indoor monitor to open the door remotely.

Door Opening Success Interface

