Visual Intercom Face Recognition Terminal

Quick Guide

V1.0.6

Contents

1 Product Overview

The visual intercom face recognition terminal ("the face recognition terminal" for short) is a face recognition access control product featuring high performance and high reliability. The face recognition technology is perfectly integrated into the access control device, which relies on deep learning algorithm, to support face authentication to open the door and achieve precise control of human. Moreover, using remote control to open the door is also supported via indoor monitor. And it can be widely applied to the scenarios of building systems, such as smart communities, public security, parks and other important areas.

The specification table below lists the major parameters of the device.

Parameters	**Description**
Operation System	Linux
Face Recognition Accuracy Rate	>99%
Face Recognition Time	200ms
Face Capacity	10,000
Card Capacity	100,000
Storage Capacity	4GB
Event Capacity	8,000 (with images)
Measurement Range	86℉ - 113℉
Measurement Deviation	≤0.54℉
Measurement Distance	3.28'
Authentication Mode	Face Whitelist: (1:N)
	Card: (1:N)
	Face + Body temperature

Parameters	Description
	Mask Detection
Door Opening Method	Face, Password, QR code, Card
Communication Mode	10/100Mbps adaptive network port
Card Type	Mifare 1 Card
User Management	Support user library addition, deletion, update
Record Management	Support local recording and real-time upload
Interface	LAN×1, Wiegand Input×1, Wiegand Output×1, RS485×1, Alarm Input×2, Alarm Output×1, USB2.0×1, Lock×1, Door Contact ×1, Exit Button×1
Power Supply	Input 12V±25% DC
Screen	Touch Screen, Size: 7 inches, Resolution: 600×1024
Camera	Dual Lens, 2MP, 1080P
Supplement Light	LED soft light and infrared light
Dimensions (L×W×H)	For terminal: 134.0mm×33.0mm×305.0mm
Working Environment	For terminal: -4℉-149℉, Relative Humidly < 95% (non-condensing)
	For module: 59℉-86℉
Protection Level	Both terminal and module: IP 54
Applicable Environment	Indoor, No wind

2 Device Installation

For the wiring and installation of the device, refer to *JXG-Face Recognition Access Control Terminal Quick Guide* and *JXG-Forehead Digital Detection Module Quick*

Guide.

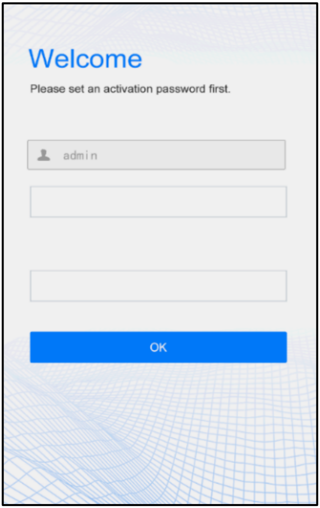
3 Local Configurations

3.1 Initial Interface

When the face recognition terminal is used for the first time or is restored to default factory settings, you need to set the activation password, which is used to log in to the Activation Configuration interface.

The activation 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).

Note: The password is consistent with the password for the admin to log in to the Web interface.



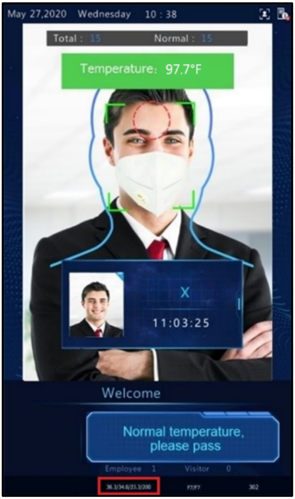
Welcome

Please set an activation password first.

admin

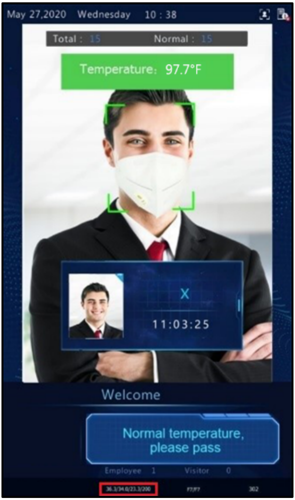
3.2 Main Interface

After you configure the activation password, the main interface of the visual intercom face recognition terminal displays.



Temperature: 97.7°F

Normal temperature, please pass



Temperature: 97.7°F

Normal temperature, please pass

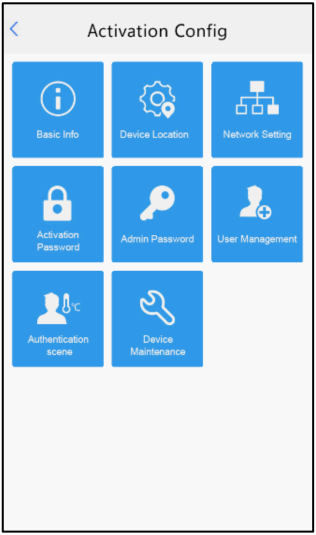
Measure Forehead Temperature

Measure Wrist Temperature

Tips: As shown in the figures above, the numbers in highlighted in the red circles indicate temperatures. If you see these numbers, it means that the forehead temperature measurement module or the wrist temperature measurement module has been connected successfully and working normally.

3.3 Activation Config

Press the main interface of the face recognition terminal for a long period of time (longer than 3 seconds). On the displayed password input interface, enter the configured activation password to go to the Activation Config interface.



3.3.1 Adding Personnel Information

1. On the **Activation Config** interface, tap to go to the **User Management** interface.
2. Configure personnel information by referring to the table below.

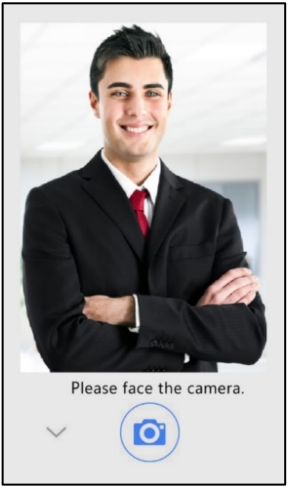
Parameter	Parameter Description and Configuration	Remarks
Name	Mandatory. Enter the name of a person.	/

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.
Face Picture	Collect and input face photos. After successful input, the person can have the face scanned for access.	

3. Perform the following steps to collect a person's face photo:

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

   2) Tap 📷 to collect the face snapshot.



Please face the camera.

3) On the photo confirmation interface, tap ✓ to confirm the photo.

4. On the **User Management** interface, tap **Save** to save the personnel information.

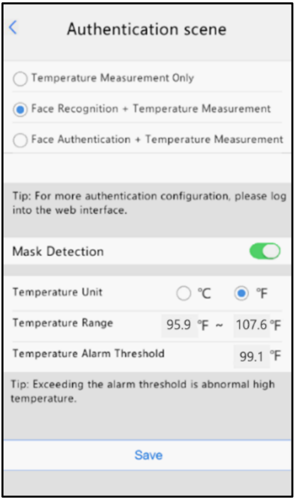
3.3.2 Changing Activation Password

1. On the **Activation Config** interface, tap 🔒 to go to the Activation Password interface.
2. Enter the old password, new password, and confirm the new password as required.
3. Tap **Save** to complete the activation password change.

3.3.3 Configuring Authentication Scene

This interface allows you to configure terminal authentication scenes, temperature measurement range, temperature alarm value, and other data.

1. On **the Activation Config** interface, tap Authentication scene to go to the 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 Unit ○ ℃ ● ℉

Temperature Range 95.9 ℉ ~ 107.6 ℉

Temperature Alarm Threshold 99.1 ℉

Tip: Exceeding the alarm threshold is abnormal high temperature.

2. Change the authentication method by selecting the radio button, as required.
3. To detect whether a person is wearing a mask, enable the **Mask Detection** button.
4. To change the **Temperature Unit** to Fahrenheit or Celsius, tap the °F or °C radio button.
5. Set the **Temperature Range**, if required. The valid range is 30°C (86°F) to 45°C

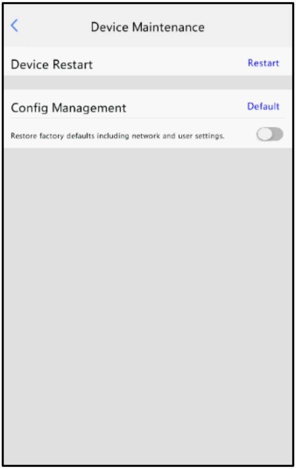
(113°F).

6. Set the **Temperature Alarm Threshold**, if required. By default, this field is set to 37.3°C per medical recommendations. If you change the temperature unit to Fahrenheit, it will change to 99.1°F automatically.

7. Tap **Save** to save the changes.

3.3.4 Device Maintenance

On the **Device Maintenance** interface, you can restart the visual intercom face recognition terminal and restore it to default factory settings.



Device Maintenance

Device Restart Restart

Config Management Default

Restore factory defaults including network and user settings.

To restart the device, tap **Restart**. On the pop-up window, tap **OK** to restart the device.

To restore the device to default configurations:

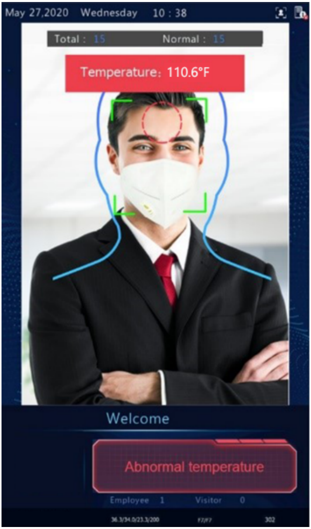
- Tap **Default**. On the pop-up window, tap **OK** to restore default configuration. All parameters expect network setting, system time, admin password and activation password will be restored to default configuration.

- First tap , then tap **Default**, On the pop-up window, tap **OK**. All parameters will be restored to default factory settings.

3.4 Device Operations

When measuring forehead temperature, a person needs to get close to the device, to fit the human shape on the screen and aim the forehead center at the red circle. When measuring wrist temperature, a person needs to aim the wrist at the temperature-measuring point of the digital detection module.

The following pictures show the abnormal temperatures detected by the forehead temperature measurement module and the wrist temperature measurement module.



May 27,2020 Wednesday 10 : 38

Total : 15 Normal : 15

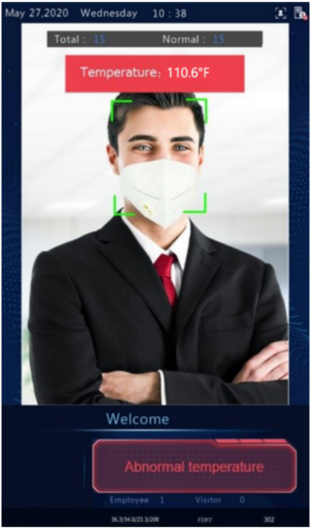
Temperature: 110.6°F

Welcome

Abnormal temperature

Employee 1 Visitor 0

36.3/34.0/23.3/200 F7/F7 302



May 27,2020 Wednesday 10 : 38

Total : 15 Normal : 15

Temperature: 110.6°F

Welcome

Abnormal temperature

Employee 1 Visitor 0

36.3/34.0/23.3/200 F7/F7 302

4 Web Configurations

You can manage and maintain the visual intercom face recognition terminal using the Web browser. It is recommended to use the Internet Explorer 10.0 running on a Windows 7.0 or Windows 10.0 Operating System.

By default, the device static IP address is 192.168.1.13. If you have changed the IP address, please use the actual IP address. Before you start, please make sure the network connection between the computer and the device is in a good condition, and your computer IP address is in the same IP segment as the device.

For more detailed information, please refer to the *Visual Intercom Face Recognition Terminal User Manual.*

4.1 Logging in to the Web Interface

1. Enter the IP address in the address bar of the browser and press **Enter**.

   Note: You may need to install a plug-in at the first login. Download and install it as prompted.

2. Enter the username and password, and then click **Login**.

   Note: The default username is ***admin*** and the default password is ***123456***. The password for admin to log in to the Web interface is the same as the activation password. If the activation password has been changed on the device, enter the new password here.

4.2 Viewing Real-Time Video

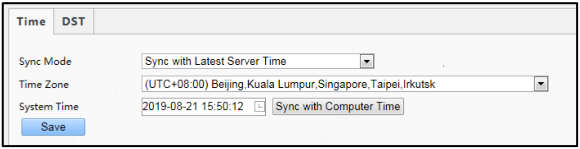
In Live View, you can view real-time audio and video received from the camera of the device.

If you log in with the **Live View** check box selected, live video appears by default when you are logged in. You may double-click the window to enter or exit full screen mode.

4.3 Synchronizing Time

In most cases, it is recommended that you synchronize the device time with the computer time.

1. Go to **Setup** > **Common** > **Time**.

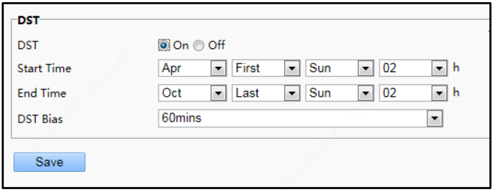


Sync Mode: Sync with Latest Server Time

Time Zone: (UTC+08:00) Beijing,Kuala Lumpur,Singapore,Taipei,Irkutsk

System Time: 2019-08-21 15:50:12

2. From the **Sync Mode** drop-down list, select **Sync with System Configuration**.
3. From the **Time Zone** drop-down list, select your time zone.
4. Click **Sync with Computer Time**.
5. Click **Save**.
6. If Daylight Saving Time is applicable to your time zone, click the **DST** tab.



DST: ● On ○ Off

Start Time: Apr First Sun 02 h

End Time: Oct Last Sun 02 h

DST Bias: 60mins

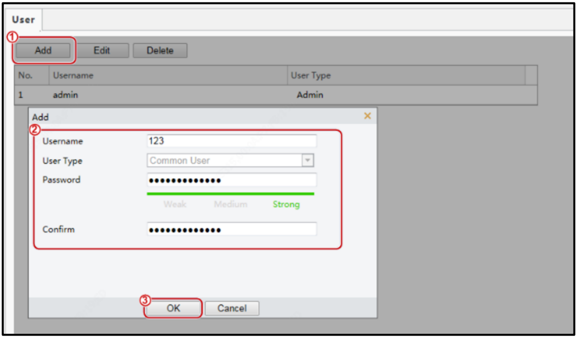
7. Select the **On** radio button and complete other settings as needed.
8. Click **Save**.

4.4 Managing Users

As the only administrator of the device, you can add up to 32 common users who only have the live view permission to the device.

1. Go to **Setup > Common > User**.

2. Follow the steps shown in the figure below to add a common user.



No.	Username	User Type
1	admin	Admin

Add

Username: 123

User Type: Common User

Password: ••••••••••••••

Confirm: ••••••••••••••

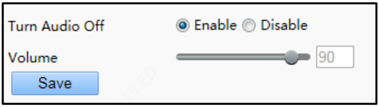
Note: To edit the password of a user, including the admin account of yourself, from the user list, select the user to be edited, click **Edit**.

4.5 Configuring Audio

On the Audio page, you can turn on or off the device audio, and also adjust the volume of the device audio.

1. Go to **Setup > Common > Ports & Devices**.

2. Click the **Audio** tab.



Turn Audio Off ● Enable ○ Disable

Volume 90

3. To turn off the audio, select the **Enable** radio button of the **Turn Audio Off** field.

4. To turn down the audio, set the **Volume** by typing a proper number in the text

box or dragging the slider.

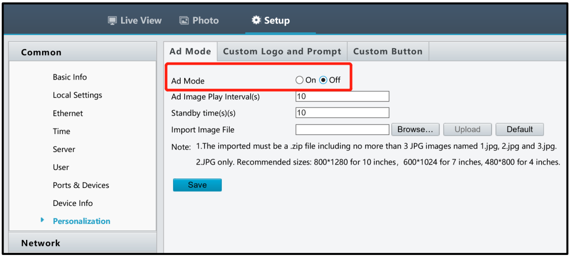
5. Click **Save**.

4.6 Turning Off Device Lights in Darkness

By default, the device lights will always be turned on in darkness as a supplement light for face recognition. You can perform the following steps to turn off the lights.

Before you start, please make sure the **Smart Illumination** is turned on in the **Setup > Image > Image > Smart Illumination** settings.

1. Go to **Setup > Personalization > Ad Mode**, turn off the Ad Mode by selecting the **Off** radio button, click **Save**.



Ad Mode ○ On ● Off

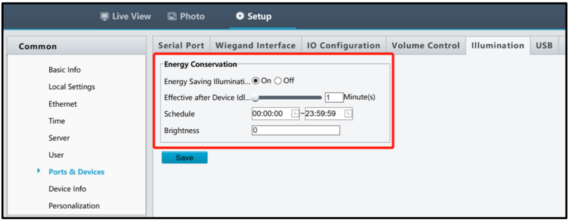
Ad Image Play Interval(s) 10

Standby time(s)(s) 10

Import Image File

Note: 1.The imported must be a .zip file including no more than 3 JPG images named 1.jpg, 2.jpg and 3.jpg.
2.JPG only. Recommended sizes: 800*1280 for 10 inches, 600*1024 for 7 inches, 480*800 for 4 inches.

2. Go to **Setup > Personalization > Ports & Devices > Illumination**.



Energy Conservation

Energy Saving Illuminati... ● On ○ Off

Effective after Device Idl... 1 Minute(s)

Schedule 00:00:00 ~23:59:59

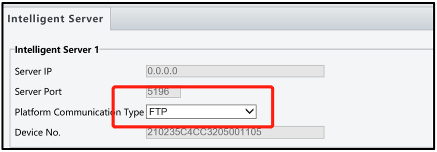
Brightness 0

3. Select the **On** radio button for the **Energy Saving Illumination** field.
4. In the **Effective after Device Idle For** field, set the time to enter the energy saving mode. E.g., 1 minute, the screen will be off one minute after a detecting a face.
5. Optionally, in the **Schedule** field, set the time range that the energy saving mode applies to.
6. In the **Brightness** field, set the value to adjust the brightness of the light when the screen is off. E.g. 0.
7. Click **Save**.

4.7 Configuring FTP Server

You can back up the captured photos to your FTP server.

1. Go to **Setup > System > Server**.



Intelligent Server 1

Server IP 0.0.0.0

Server Port 5196

Platform Communication Type FTP

Device No. 210235C4CC3205001105

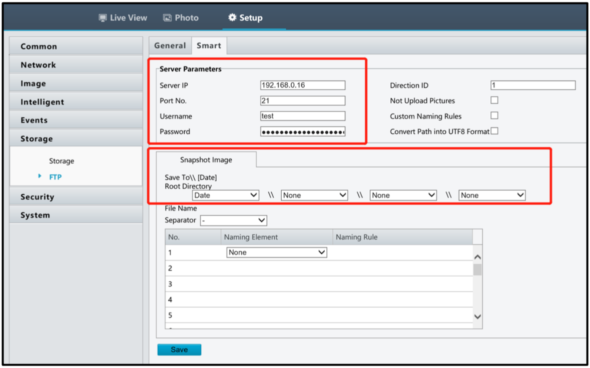
2. In the **Intelligent Server 1** section, select *FTP* from the **Platform Communication Type** drop-down list.
3. Click **Save**.

4. Go to **Setup > Storage > FTP > Smart**.

   Note: The General tab is not applicable to this device and will be removed. Any settings on the General tab have no impact to settings on the Smart tab.

5. In the **Server Parameters** section, enter the Server IP, Port, Username, and Password, as required.

6. In the **Snapshot Image** section, set the Root Directory, if necessary.



Server Parameters

Server IP 192.168.0.16

Port No. 21

Username test

Password ••••••••••••••••••

Direction ID 1

Not Upload Pictures □

Custom Naming Rules □

Convert Path into UTF8 Format □

Snapshot Image

Save To\\ [Date]

Root Directory Date \\ None \\ None \\ None

File Name

Separator -

No.	Naming Element	Naming Rule
1	None	
2		
3		
4		
5		

7. Click **Save**. The captured photos will automatically be saved to the directory on the FTP server.

4.8 Configuring OSD Parameters

On Screen Display (OSD) is the text displayed on the screen with video images. You can configure the content and the position to be displayed on the screen. For example, Date & Time.

1. Go to **Setup > Image > OSD**.

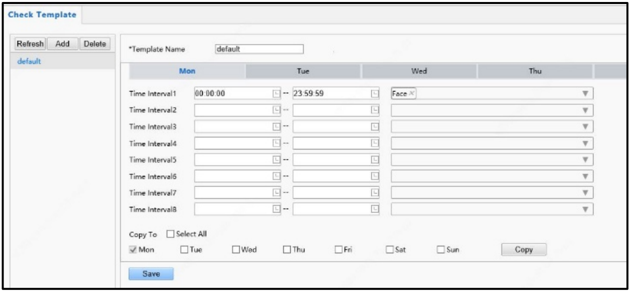
2. Select the position and content to be displayed on the screen.

Note: After you have set the position and OSD content, the ✓ symbol appears in the Status column, which means that the OSD is set successfully. You may set multiple lines of contents for each area and use ∧ and ∨ to adjust the display sequence.

3. After completing the settings, a message displays to indicate the successful settings.
4. To cancel OSD for an area, clear the OSD content in the Overlay OSD Content column or select **None** in the Position column.

4.9 Configuring Check Templates

The check template is applicable when the device is used together with a door control system. With the check template, you can configure the authentication modes that are applicable to different periods of time in a day, so people must match the authentication modes before they can open the door. The authentication mode can be configured separately for each day or copied to all days. Up to 16 check templates can be configured.



*Template Name: default

Time Interval1: 00:00:00 -- 23:59:59 Face

Time Interval2 --

Time Interval3 --

Time Interval4 --

Time Interval5 --

Time Interval6 --

Time Interval7 --

Time Interval8 --

Copy To □ Select All

☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

1. Go to **Setup > Intelligent > Check Template** and click **Add**.
2. Set parameters in the right panel of the interface.
   - Template Name: Enter the name of a check template. The value is a string of 1–63 characters.

- Set the authentication mode for each time range in a week based on actual conditions. There are four authentication modes available:
    - IC Card: People will need to swipe a card with valid card number to open the door.
    - Face: People will need to pass face authentication to open the door.
    - IC Card+Face: People will need to swipe a valid card and then pass face authentication to open the door.

  Note: When multiple authentication modes are selected, the authentication modes are in an "OR" relationship, that is, people can open the door if they pass any of the configured authentication modes.

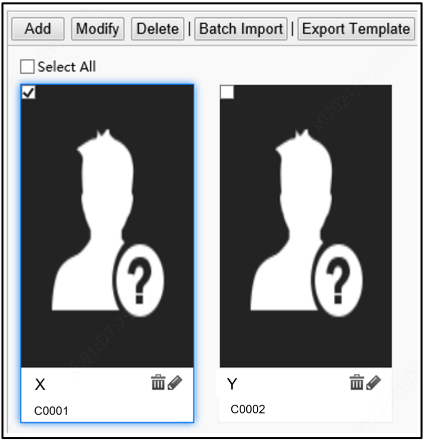
3. After setting time ranges and authentication modes for Monday, if the settings also apply to any other days of the week, select the relevant check boxes. You can select the **Select All** check box to copy them to all days. Click **Copy**.
4. Click **Save**.

4.10 Adding Personnel Information to Face Libraries

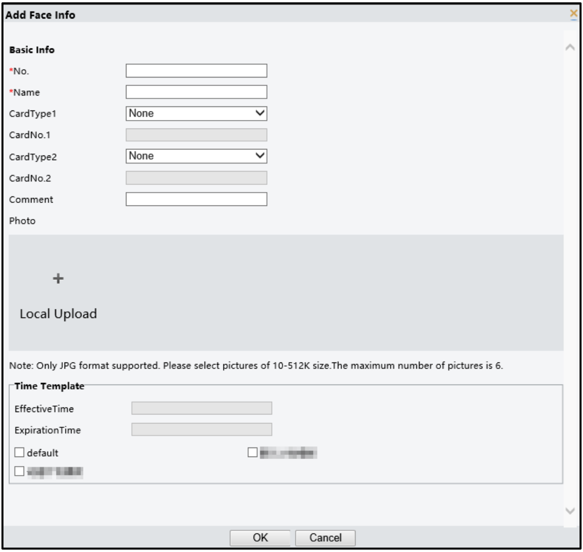
A face library is where you save personnel information, such as Name, Staff ID, Face Pictures etc. By default, there is one DefaultEmployeeLib and one DefaultVisitorLib. While you can add more libraries, please do not rename or delete these two libraries.

4.10.1 Adding One Person

1. Go to **Setup > Intelligent > Face Library** and select the face library to which persons are to be added. E.g., DefaultEmployeeLib.



2. On the personnel list bar, click **Add**. The Add Face Info interface displays.



Add Face Info

Basic Info

*No.	
*Name	
CardType1	None
CardNo.1	
CardType2	None
CardNo.2	
Comment	

Photo

Note: Only JPG format supported. Please select pictures of 10-512K size.The maximum number of pictures is 6.

Time Template

EffectiveTime	
ExpirationTime	

☐ default ☐ [redacted]

☐ [redacted]

3. On the **Add Face Info** interface, complete person information as required.

4. Click **OK**.

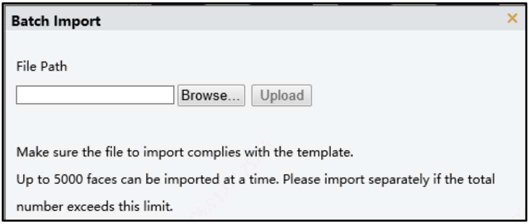
4.10.2 Importing Personnel Information in Batch

1. Go to **Setup > Intelligent > Face Library** and select the face library to which persons are to be added. E.g., DefaultEmployeeLib.

2. Click **Export Template** to download an import template to the local device.

3. Decompress the template. In the import table, enter information according to requirements.

4. Click **Batch Import** to upload the import table.



Batch Import

File Path

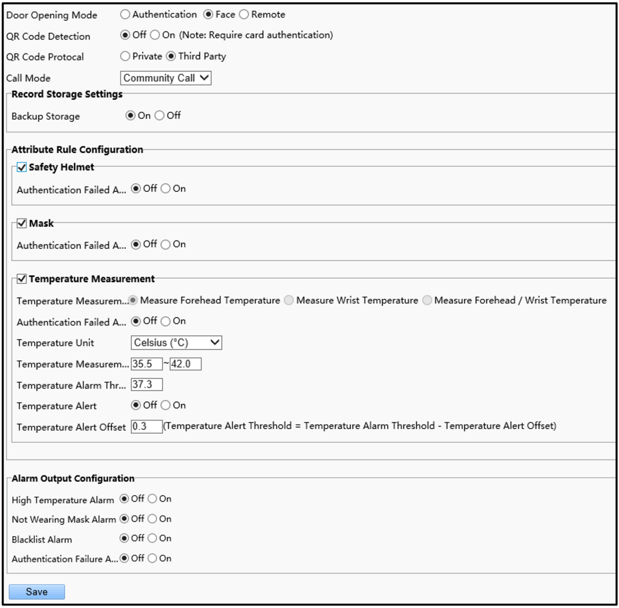
Make sure the file to import complies with the template.

Up to 5000 faces can be imported at a time. Please import separately if the total number exceeds this limit.

Note: If information about a person fails to be imported, check the failure reason in the description column, modify information and then import the person information again.

4.11 Advanced Settings

On the Advanced Setting page, you can set parameters like Door Opening Mode, Mask Detection, Temperature Measurement Unit, Alarm Temperature Threshold etc. On the web page, go to **Setup** > **Intelligent** > **Advanced Setting**. For more detailed information, please refer to the *Visual Intercom Face Recognition Terminal User Manual.*



Door Opening Mode ○ Authentication ● Face ○ Remote

QR Code Detection ● Off ○ On (Note: Require card authentication)

QR Code Protocal ○ Private ● Third Party

Call Mode Community Call

Record Storage Settings

Backup Storage ● On ○ Off

Attribute Rule Configuration

☑ **Safety Helmet**

Authentication Failed A... ● Off ○ On

☑ **Mask**

Authentication Failed A... ● Off ○ On

☑ **Temperature Measurement**

Temperature Measurem... ● Measure Forehead Temperature ○ Measure Wrist Temperature ○ Measure Forehead / Wrist Temperature

Authentication Failed A... ● Off ○ On

Temperature Unit Celsius (°C)

Temperature Measurem... 35.5 ~ 42.0

Temperature Alarm Thr... 37.3

Temperature Alert ● Off ○ On

Temperature Alert Offset 0.3 (Temperature Alert Threshold = Temperature Alarm Threshold - Temperature Alert Offset)

Alarm Output Configuration

High Temperature Alarm ● Off ○ On

Not Wearing Mask Alarm ● Off ○ On

Blacklist Alarm ● Off ○ On

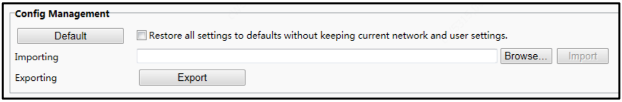
Authentication Failure A... ● Off ○ On

4.12 Maintenance Configurations

4.12.1 Restoring Default Factory Settings

Where necessary, for example, after you upgrade the firmware, you can restore the device to default settings on the Maintenance page.

1. Go to **Setup > System > Maintenance**.


Config Management

Default ☐ Restore all settings to defaults without keeping current network and user settings.

Importing Browse... Import

Exporting Export

2. In the **Config Management** section:

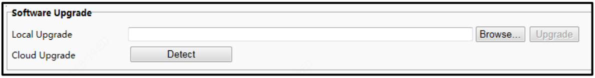
    - When **Default** is clicked, all parameters are restored to default factory settings, except the administrator login password, network port parameters, system time, admin password, and activation password.

    - If the **Restore all settings to defaults without keeping current network and user settings** checkbox is selected, when **Default** is clicked, all parameters are restored to default factory settings. After this, a prompt asking you to change the activation password is displayed on the GUI.

4.12.2 Upgrading the Firmware

Once a new firmware is available, you can upgrade the firmware of the device. Make sure that the power supply is normal during the upgrade process. The device will restart after the upgrade process is completed.

1. Go to **Setup > System > Maintenance**.


Software Upgrade

Local Upgrade Browse... Upgrade

Cloud Upgrade Detect

2. In the **Software Upgrade** section, click **Browse** and select the correct upgrade file.

3. Click **Upgrade** and then confirm to start.

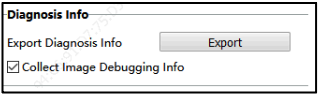
4. In some cases, you may need to restore the device to default settings after upgrading it. On the Maintenance page, in the **Config Management** section, click **Default** to start the process.

    Note: Do not select the **Restore all settings …** checkbox.

4.12.3 Exporting Diagnosis Information

Diagnosis information includes logs and system configurations. In case your device encounters malfunctions, you can export diagnosis information and send it to technical support for troubleshooting.

1. Go to **Setup > System > Maintenance**.



2. Click **Export**. In the displayed dialog box, select the local directory for storing the information.

Note: ⍰By selecting the **Collect Image Debugging Info** checkbox, you can display video with debugging information at the same time, which makes troubleshooting easier.

Disclaimer and Safety Warnings

Copyright Statement

No part of this manual may be copied, reproduced, translated or distributed in any form by any means without prior content in writing from our company (referred to as us hereafter).

The product described in this manual may contain proprietary software owned by our company and its possible licensors. Unless permitted, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form by any means.

Export Compliance Statement

Our company complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, our company asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Privacy Protection Reminder

Our company complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc., in this manual may be different from the actual appearances, functions, features, etc., of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Our company cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.

- Our company reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will our company be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. Our company disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will our company and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if our company has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change default password and set strong password**: You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.

- **Keep firmware up to date**: It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly**: Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL**: Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering**: Allow access only from the specified IP addresses.
- **Minimum port mapping**: Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features**: If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely**: Avoid using the username and password of your social media, bank, email account, etc., as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions**: If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP**: When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP**: Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast**: Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs**: Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection**: Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network**: Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting our company first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Installation and use of the device must be in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Use Caution

- When battery is used, avoid:
  - High or low extreme temperatures during use, storage and transportation;
  - Extremely low air pressure, or low air pressure at high altitude.
  - Battery replacement.
- Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
  - Replace battery with an incorrect type;
  - Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;
- Dispose the used battery according to your local regulations or the battery manufacturer's instructions.

Avertissement de l’utilisation de la batterie

- Lorsque utiliser la batterie, évitez:
  - Températures extrêmement élevées ou basses pendant l’utilisation, le stockage et le transport;

  - Pression d’air extrêmement basse, ou pression d’air basse à haute altitude.
  - Remplacement de la batterie.
- Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme celles mentionnées ici, peut entraîner des risques d’incendie, d’explosion ou de fuite liquide de gaz inflammables.
  - Remplacer la batterie par un type incorrect;
  - Disposer d’une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;
- Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.

Regulatory Compliance

FCC Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.

NOTE: This device has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the device is operated in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

LVD/EMC Directive

This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU.

WEEE Directive–2012/19/EU

The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EC

Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.

🌐 www.cssinco.com

✉ support@cssinco.com