Akuvox A05 Series Access Control Terminal Admin Guide_V2.0 202306

Akuvox
Open A Smart World

WWW.AKUVOX.COM

A05 ACCESS CONTROL TERMINAL

Administrator Guide

About This Manual

Thank you for choosing Akuvox A05 series access control terminal. This manual is intended for administrators who need to properly configure the access control terminal. This manual applies to 105.30.4.8 version, and it provides all the configurations for the functions and features of A05 series access control terminals. Please visit Akuvox forum or consult technical support for any new information or the latest firmware.

Introduction of Icons and Symbols

> **Note**
>
> - **Informative information and advice from the efficient use of the device.**

Related Documentation

You are advised to refer to the related documents for more technical information via the link below:

https://knowledge.akuvox.com

Product Overview

Akuvox A05 series is a Linux-based access control door phone with a display screen. It incorporates access control and video surveillance. Its finely tuned SmartPlus and AI-based communication technology allow featured customization to better suit your operation habit. A05 series has multiple ports, such as RS485 and Wiegand ports, which can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, helping to create a holistic control of building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, NFC, QR code and newly added door access in an accompaniment with body temperature measurement. A05 series access control terminal applies to residential buildings, office buildings, and their complex.

Change Log

The change log will be updated here along with the changes in the new software version.

Model Specification

Model **&** **Feature**	**A05S**

Display	5" IPS
Touch Screen	X
Button	X
Housing Material	Plastic
Relay Out	1
Alarm In	1
RS485	√
PoE	√
Resolution	1280x720
Brightness	500cd/m2
RAM	1GB
ROM	8GB
Card Reader	13.56MHz
Wi-Fi	X
Bluetooth	Optional

IP Rating	IP65
Temperature Detection	Optional
Face recognition	√
LTE	X
USB	X
External SD Card	X
Wall Mounting	√
Flush Mounting	X
Desk Mounting	X
POE Stand by Power	5.5W
POE Full Load Consumption	9.8W
Power Adapter Standby Power	5.5W
Power Adapter Full Load Consumption	10W
Color Option	Black

Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, Network Information, and log related configurations such as access log, temperature log, and so on.
- **Network**: this section mainly deals with DHCP&Static IP settings, and device deployment, etc.
- **Surveillance**: this section includes audio&video related settings such as Live stream, RTSP, ONVIF, and MJPEG.
- **Access Control**: this section includes input type setting, relay setting, door access control in terms facial recognition, RF card, and BLE setting, Body temperature.
- **Directory**: this section includes access schedule management and user management, adding cards, and upload face data and so on.
- **Device**: this section includes light, Wiegand, lift control, LCD, audio and so on.
- **Setting**: this section deals with relay schedule, security notification settings, web relay, time, action, and HTTP API settings.
- **System**: this section covers firmware upgrade, device reset, reboot, configuration file auto-provisioning, system log, remote debug server, PCAP, password modification as well as device backup.

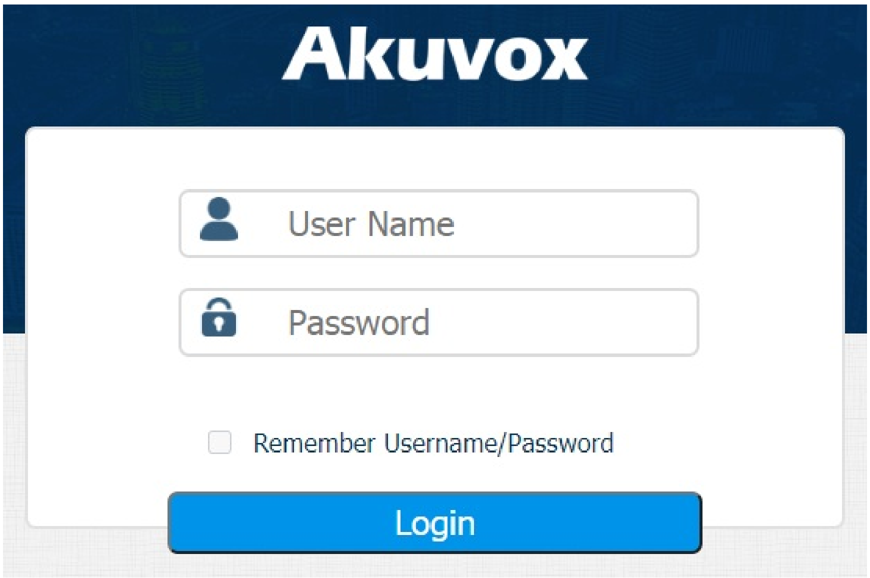
- **Tool selection**

Akuvox has many configuration tools for you to set up devices more conveniently. Here we list some common tools, please contact your administrator to get the tool if you need them.

1. **SDMC**: SDMC is suitable for the management of Akuvox access control devices in large communities for access control, resident information, and remote device control, etc.
2. **Akuvox Upgrade tool**: mainly used to reset the device password.
3. **IP scanner**: it is used to search Akuvox device IP addresses on a LAN.
4. **FacePro**: manage face data in batch for the access control terminal on a LAN.

Access the Device

Before configuring Akuvox A05, please make sure the device is installed correctly and connect to a normal network. Using Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to log in to the web browser by user name and password **admin** and **admin.**



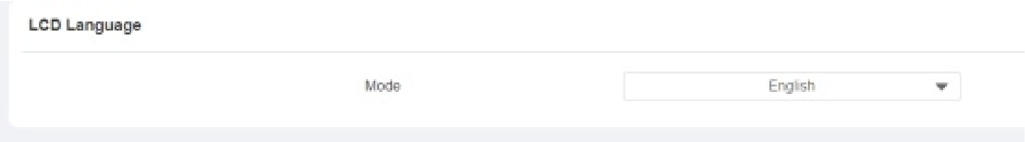
> **Note**
>
> - You can also obtain the device IP address using the Akuvox IP scanner to log into the device web interface. Please refer to the URL below for the IP scanner application:
>
> https://knowledge.akuvox.com/docs/how-to-obtain-ip-address-via-ip-scanner-1

> **Note**
>
> - **Google Chrome browser is strongly recommended.**
> - **The Initial user name and password are admin and please be case-sensitive to the user names and passwords entered.**

Time and Language Setting

Language Setting

To select the device language, go to **Setting** > **Time/Lang** > **LCD Language.**

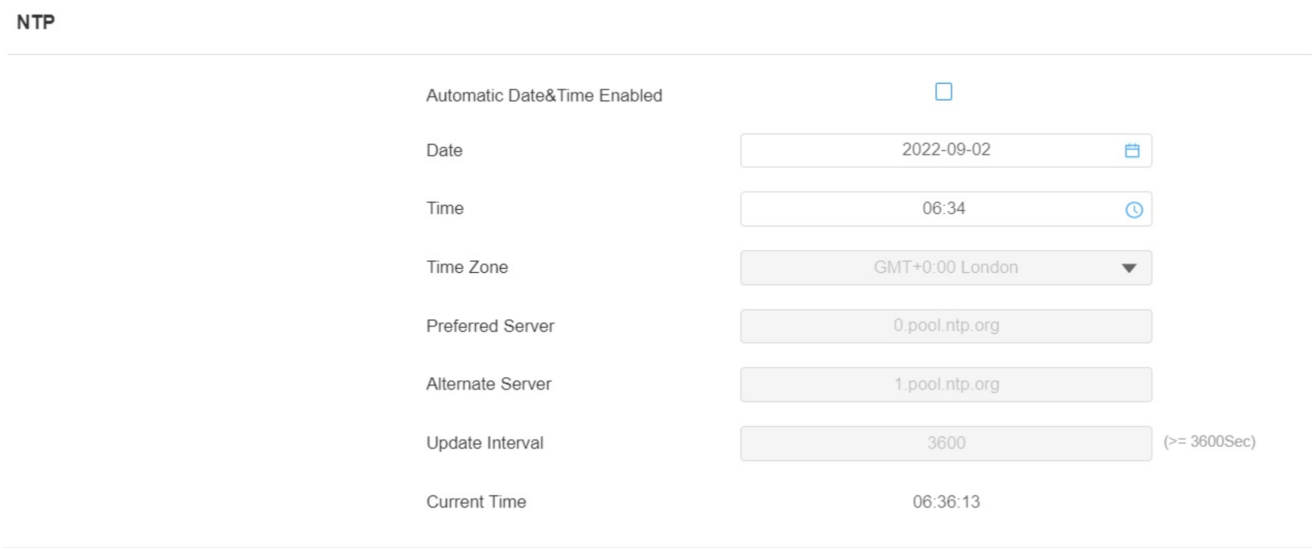


LCD Language

Mode	English ▾

Time Setting

Time setting on the web **Setting > Time/Lang > NTP** interface allows you to set up time and date manually while allowing you to use the NTP server address that you obtained to automatically synchronize your time and date. And when your time zone is selected, the device will automatically notify the NTP server of its time zone so that the NTP server can synchronize the time zone setting in your device.



NTP

Automatic Date&Time Enabled	□
Date	2022-09-02
Time	06:34
Time Zone	GMT+0:00 London ▾
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600Sec)
Current Time	06:36:13

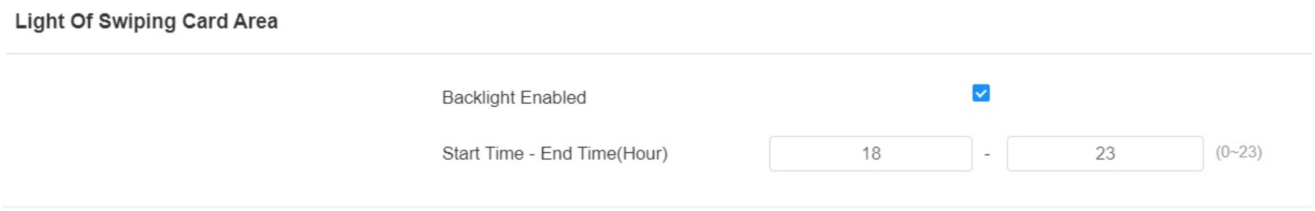
Parameter Set-up:

- **Automatic Date&Time Enabled:** enable the use of the NTP server for automatic time synchronization.
- **Time Zone:** select the specific time zone based on the device location. The default time zone is GMT+0:00.
- **Preferred Server**: enter the primary NTP server address you want to update the time with. The default NPT server address is 0.pool.ntp.org
- **Alternate Server**: enter the backup NPT server address you want to update the time with when the primary one failed.
- **Update Interval**: set the time update interval. For example, if you set it as 3600s, then the device will send a request to the NPT server for the time update once every 3600 second.
- **Current Time**: display the current device time.
- **Date/Time**: set the date and time for the device manually when you disable the automatic date and time service.

LED Setting

Configure Card Reader LED Setting

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want the card reader LED light to stay on, you can also set the timing for the exact time profile during which the LED light can be disabled to reduce electrical power consumption. To configure it, go to **Device > Light > LED Of Swiping Card Area**.



Light Of Swiping Card Area

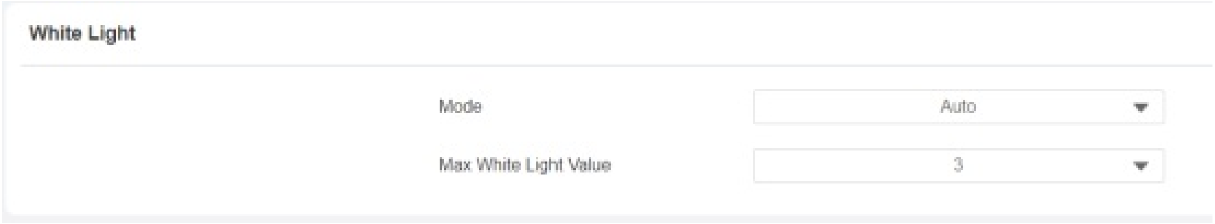
Backlight Enabled	☑			
Start Time - End Time(Hour)	18	-	23	(0~23)

Parameter Set-up:

- **Backlight Enabled**: tick the check box if you want to enable the card reader LED lighting.
- **Start Time- End Time (H)**: enter the time span for the LED lighting to be valid, eg. if the time profile is from **18-22**, it means the LED light will stay on during the time from **6:00 pm** to **10:00** pm during one day (24 hours).

Configure LED White Light Setting

LED White light is used to reinforce the lighting for facial recognition as well as for QR code door opening in the dark environment. To configure it, go to **Device > Light > White Light** interface.



White Light

Mode	Auto
Max White Light Value	3

Parameter Set-up:

- **Mode**: if you select **Auto**, then the white light will be turned on automatically for face recognition and QR code scan for door opening. If you select **Off**, then the white light will be disabled.
- **Max White Light Value**: set the white light value from**1-5**, and the default white light value is **3**. The greater value it is, the brighter the light will be.

Note

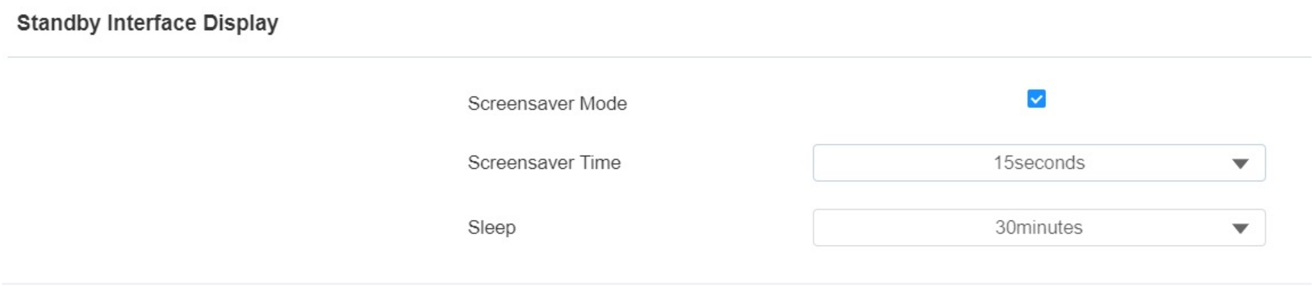
- IR LED light should be triggered first before the white light can be valid in the facial recognition, however, IR LED light does not need to be triggered for the white light function in the QR code scan.

Screen Display configuration

A05 series access control terminals allow you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

Configure Screensaver

A05 can turn on screen saver for a predefined time profile when there is no operation on the device, or no one is detected approaching. To configure it, go to **Device > LCD > Standby Interface Display**.



Standby Interface Display

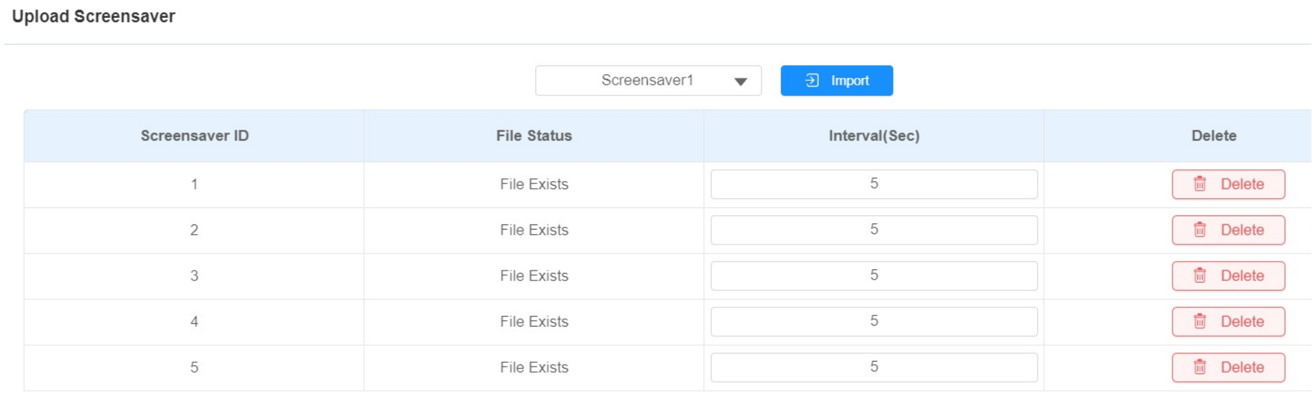
Screensaver Mode	☑
Screensaver Time	15seconds ▼
Sleep	30minutes ▼

Parameter Set-up:

- **ScreenSaver Mode:** tick the check box to enable the screen saver function.
- **Screensaver Time**: set the screen saver start time from 5 seconds up to 2 hours. For example, if you set the start time as 5 minutes, then the screen saver will start if there is no operation on the device or no one is approaching during the five minutes interval.
- **Sleep:** set how long you expect the screen saver to last before turning off the device's screen. You select the screen saver duration from 2 seconds to 30 min.

Upload Screensaver

To upload screen saver, go to **Device > LCD > Upload Screensaver.** You can upload a maximum of 5 pictures, and each picture will be displayed in rotation according to the ID order with the specific time duration (**Time Interval**) you set.



Upload Screensaver

Screensaver1 ▼ Import

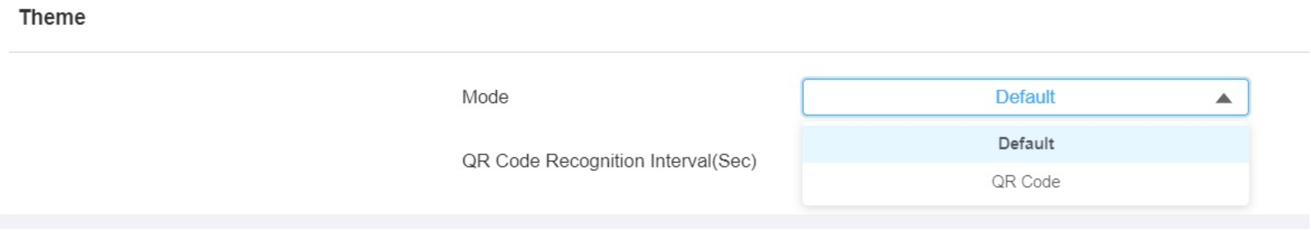
Screensaver ID	File Status	Interval(Sec)	Delete
1	File Exists	5	Delete
2	File Exists	5	Delete
3	File Exists	5	Delete
4	File Exists	5	Delete
5	File Exists	5	Delete

Note

- The pictures uploaded should be in **JPG format** with 2M pixels maximum.
- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurred.

Configure Access Screen Display Mode

You can select two types of access screen display modes on the home screen, namely, the Default mode for facial recognition and the QR code mode. To configure the configuration on web **Device > LCD > Theme** interface.



Theme

Mode: Default

QR Code Recognition Interval(Sec)

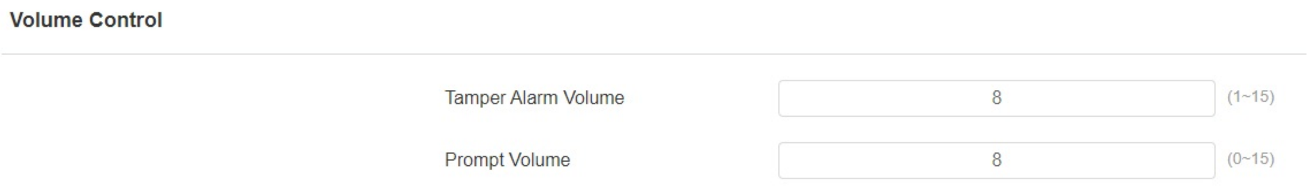
Parameter Set-up:

- **Mode:** there are two modes **Default** and **QR Code.** If you choose QR code, the main screen shows "**Please scan your QR code**" as default to remind you to unlock by QR code. If you choose Default, the main screen shows "**Please look at the screen**" as default to remind you to unlock by face recognition.
- **QR Code Recognition Interval(Sec):** this interval is only available when you choose **QR Code** mode. It is recognition of the interval between two QR codes.

Volume & Tone Configuration

Configure Volume

You can set the temper alarm volume and prompt alarm volume. Go to **Device > Audio > Volume Control.**



Volume Control

Tamper Alarm Volume: 8 (1~15)

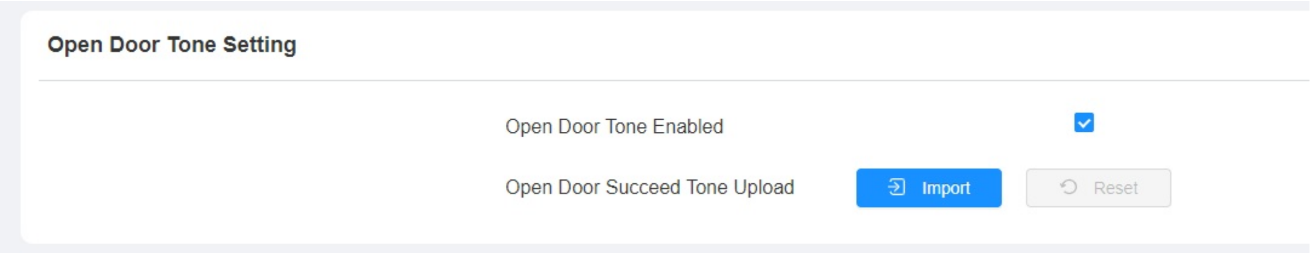
Prompt Volume: 8 (0~15)

Parameter Set-up:

- **Tamper Alarm Volume**: set the tamper alarm volume from 1-15 according to your need. The default volume is **8.**
- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sound for door opening success and failure, ringback, and temperature measurement sound, etc.

Upload Open Door Tone

You can upload the Open-Door Tone on the device web interface. To configure the configuration on web **Device >Audio > Open Door Tone Setting**



Open Door Tone Setting

Open Door Tone Enabled ☑

Open Door Succeed Tone Upload

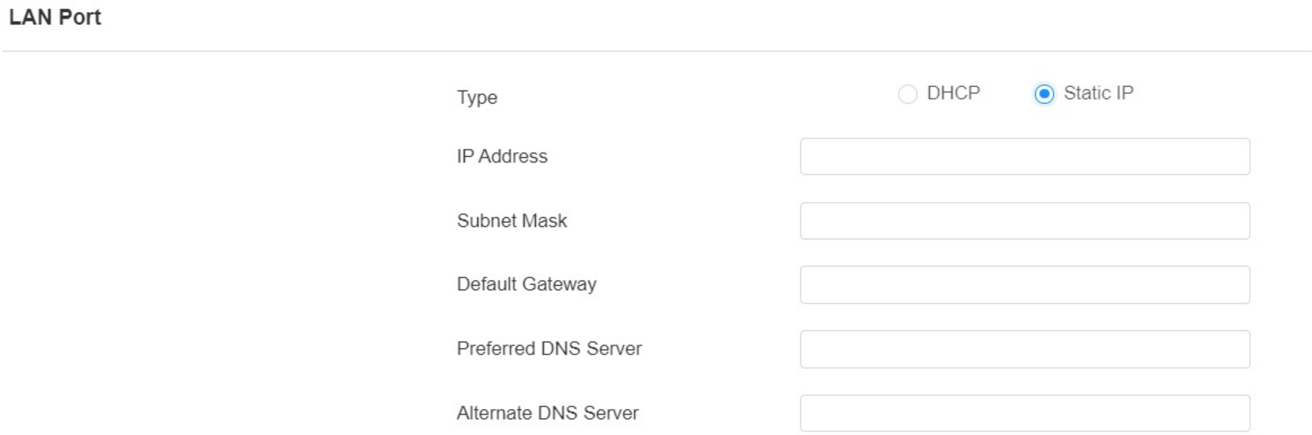
Note

- The open door tone file should be .wav format and the file size should be smaller than 200KB.

Network Setting

Configure Device Network

You can configure the default DHCP mode (**Dynamic Host Configuration Protocol**) and static IP connection. Moreover, you can set up IP address, Subnet Mask, Default Gateway, LAN DNS1 & LAN DNS2. To configure the configuration on web **Network** > **Basic** > **LAN Port** interface.



LAN Port

Type ○ DHCP ● Static IP

IP Address

Subnet Mask

Default Gateway

Preferred DNS Server

Alternate DNS Server

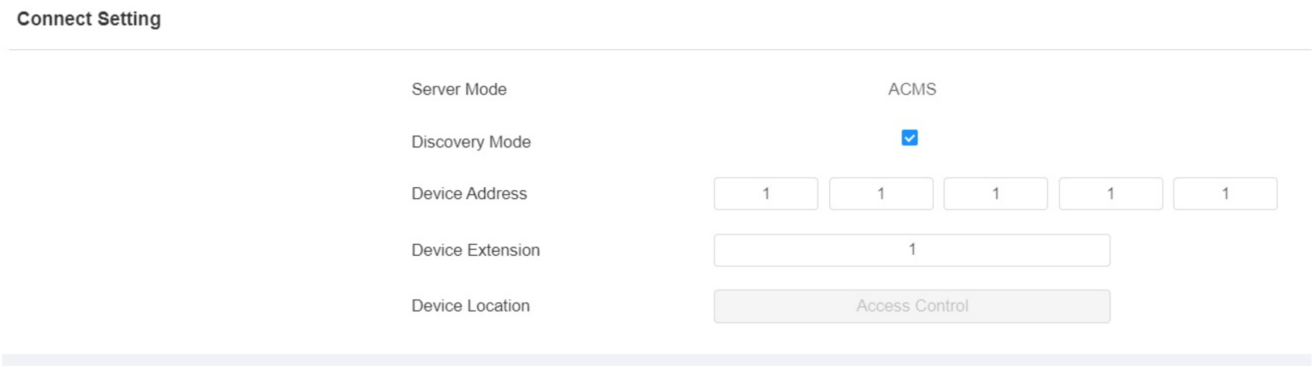
Parameter Set-up:

- **DHCP**: select the **DHCP** mode by checking off the DHCP box. DHCP mode is the default network connection. If the DHCP mode is selected, then the access control terminal will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: select the static IP mode by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address must be manually configured according to your actual network environment.
- **IP Address**: set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **Preferred DNS Server/Alternate DNS Server**: set up DNS server (**Domain Name Server**) according to your actual network environment. The access control unit will connect to the **Alternate DNS Server**

(backup server) if the preferred DNS server failed.

Configure Device Deployment in Network

Access control terminals should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address and extension numbers as opposed to other devices for device control and the convenience of the management. To configure the configuration on web **Network > Basic > Connect Setting** interface.



Connect Setting

Server Mode: ACMS

Discovery Mode: ☑

Device Address: 1 | 1 | 1 | 1 | 1

Device Extension: 1

Device Location: Access Control

Parameter Set-up:

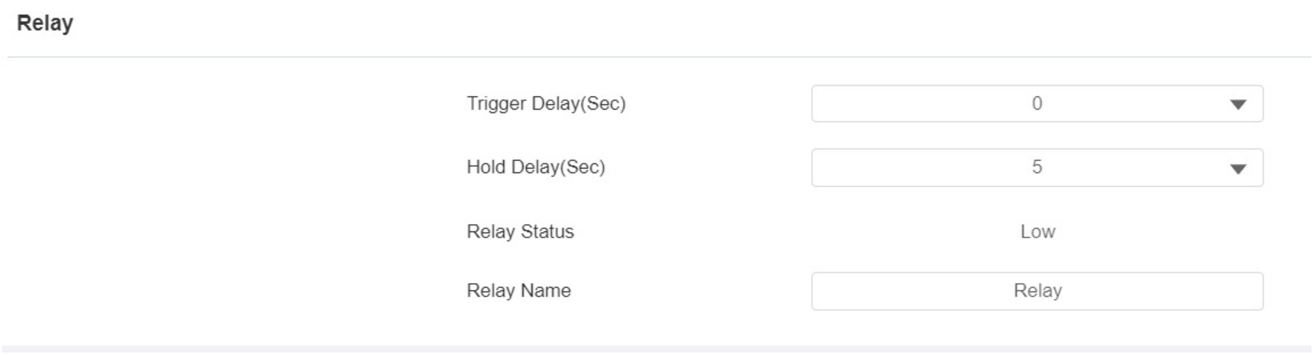
- **Server Mode:** it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC** or **Akuvox SmartPlus** and **None. None** is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **Discovery Mode:** click **Enabled** to turn on the discovery mode of the device so that it can be discovered by other devices in the network and click **Disabled** if you want to conceal the device so as not to be discovered by other devices.
- **Device Address:** specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor,** and **Room** in sequence.
- **Device extension**: enter the device extension number for device you installed
- **Device Location**: enter the location in which the device is installed and used.

Relay Setting

You can configure the relay switch(es) and DTMF for door access on the web interface.

Relay switch setting

To configure the configuration on web **Access Control > Relay > Relay** interface.



Relay

Trigger Delay(Sec): 0

Hold Delay(Sec): 5

Relay Status: Low

Relay Name: Relay

Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (ranging from 1-10 Sec.) For example, if you set the delay time as **5** sec. then the relay will not be triggered until 5 seconds after you press **unlock** tab.
- **Hold Delay (Sec):** set the relay hold delay timing (ranging from 1-10 Sec.) For example, if you set the hold delay time as **5** Sec. then the relay will be delayed for 5 after the door is unlocked.
- **Relay Status:** relay status is low by default which means normally closed (NC) If the relay status is high, then it is in Normally Open status (NO).
- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note

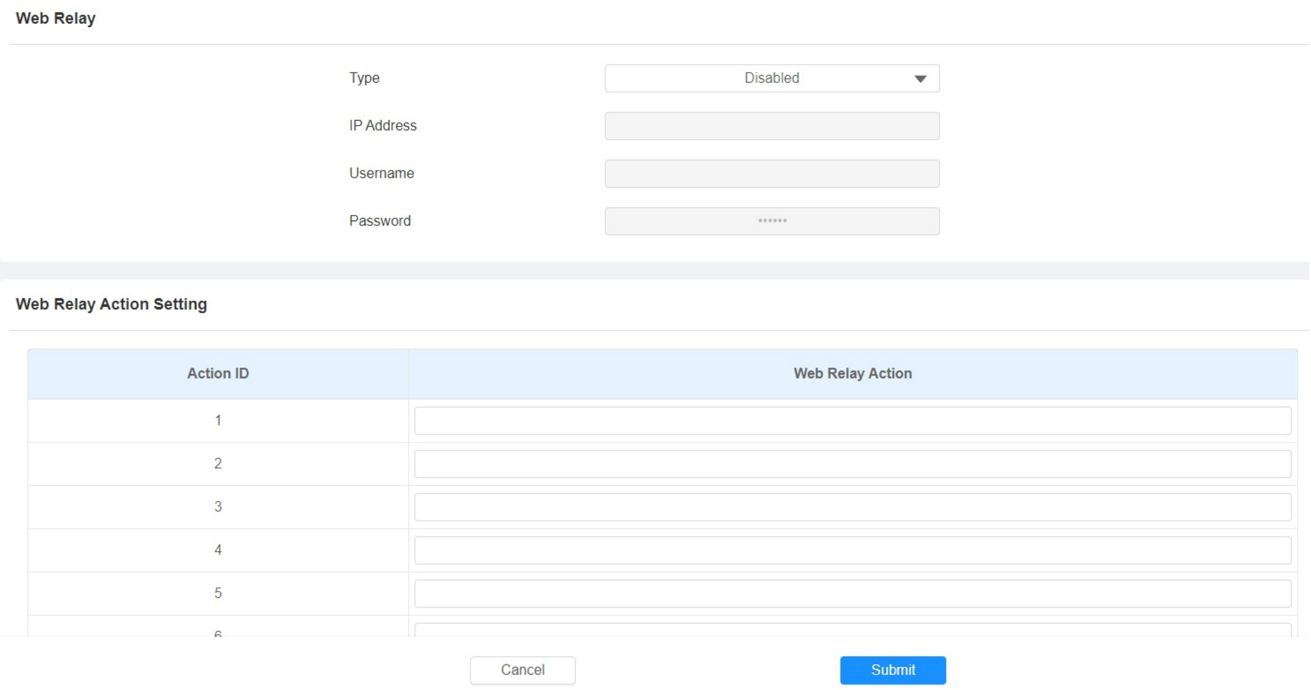
- Only the external devices connected to the relay switch need to be powered by power adapters as the relay switch does not supply power.

Web Relay Setting

In addition to the relay that is connected to the access control terminal, you can also control the door access using the network-based web relay on the device and on the device web interface.

Configure Web Relay on the Web Interface

Web relay needs to be set up on the web interface where you are required to fill in such information as relay IP address, password, web relay action, etc. Before you can achieve door access via web relay. To configure the configuration on web **Access Control > Web Relay** interface.



Web Relay

Type	Disabled
IP Address	
Username	
Password	••••••

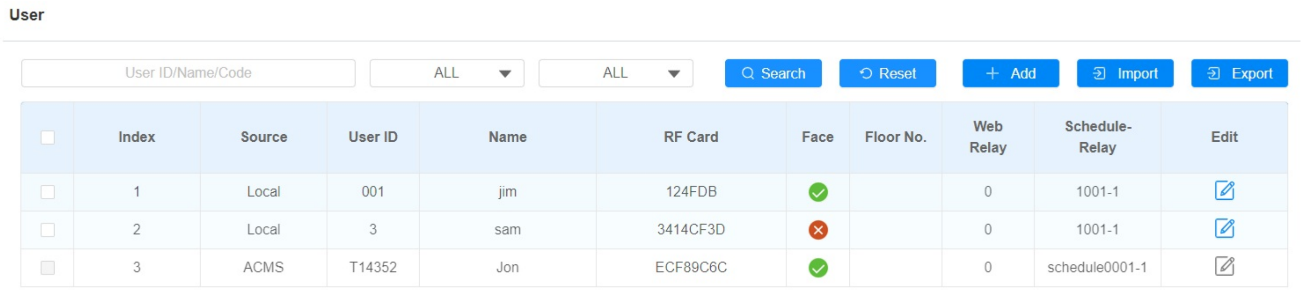
Web Relay Action Setting

Action ID	Web Relay Action
1	
2	
3	
4	
5	
6	

Parameter Set-up:

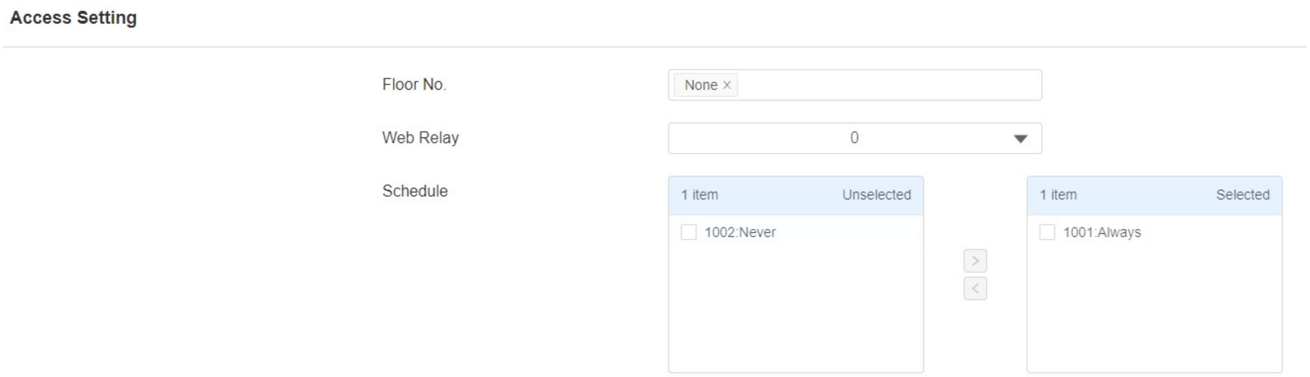
- **Type:** select among three options **Disabled**,**WebRelay** and **Both.** Select **WebRelay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.
- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.
- **Username**: enter the User name provided by the web relay manufacturer.
- **Password:** enter the password provided by the web relay manufacturer. The password is authenticated via HTTP and you can define the passwords using **http get** in Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. **http://admin:admin@192.168.1.2/state.xml?relayState=2.**

After the web relay is set up, you can select the specific web relay action to be carried out. You can go to **Directory** > **User,** then click + Add , then scroll down to **Access Setting**.



User

□	Index	Source	User ID	Name	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	001	jim	124FDB	✓		0	1001-1	✎
□	2	Local	3	sam	3414CF3D	✗		0	1001-1	✎
□	3	ACMS	T14352	Jon	ECF89C6C	✓		0	schedule0001-1	✎



Access Setting

Floor No. None ×

Web Relay 0

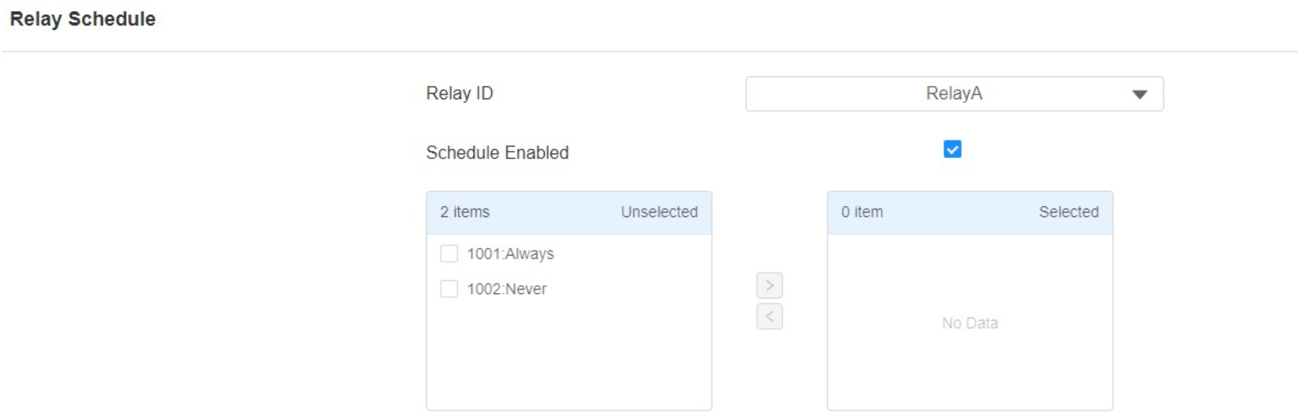
Schedule

1 item	Unselected
□ 1002:Never	

1 item	Selected
□ 1001:Always	

Relay Schedule

Set the corresponding relay always open at a specific time. This feature is designed for some specific scenarios, such as, the time after school, or for morning work time. To do the configuration, navigate to **Access Control > Relay > Relay Schedule** interface.



Relay Schedule

Relay ID RelayA

Schedule Enabled ☑

2 items	Unselected
□ 1001:Always	
□ 1002:Never	

0 item	Selected
No Data	

Parameter Set-up:

- **Relay ID:** choose the relay you need to set up.
- **Schedule Enabled:** it is disabled by default. Only choose to enable it, and you can select the schedule. For creating the schedule, please refer to the door access schedule configuration.

> **Note**
>
> - **You can refer to Create Door Access Schedule for the relay schedule setting.**

Door Access Schedule Management

You are required to configure and make schedule for the user-based door opening using RF card and facial recognition.

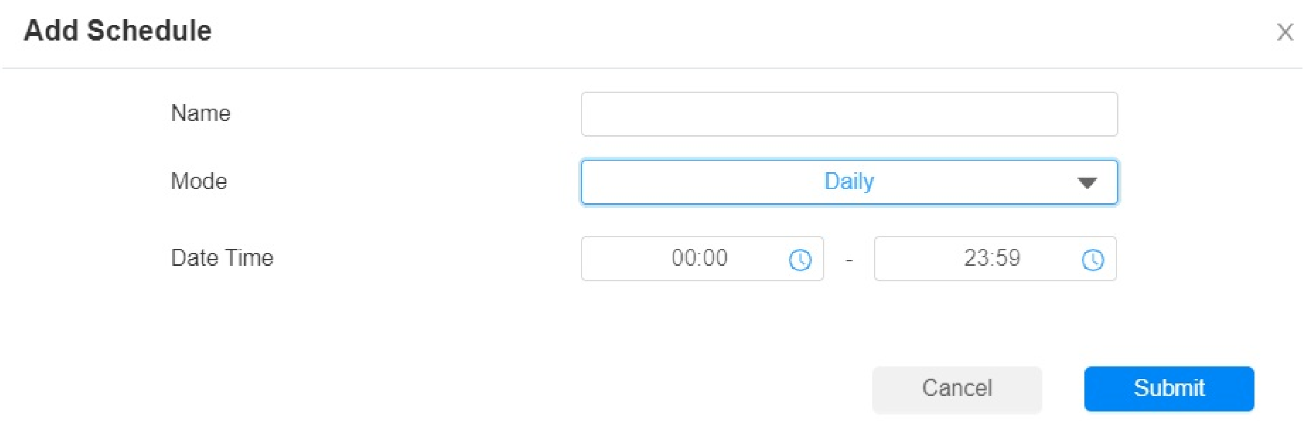
Configure Door Access Schedule

You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. Moreover, you can edit your door access schedule if needed.

Create Door Access Schedule

You can create the door access schedule on a daily or monthly basis, and you can also create schedules that allow you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis. To configure it, go to **Setting > Schedule**, then click **+ Add.**

To create daily schedule:



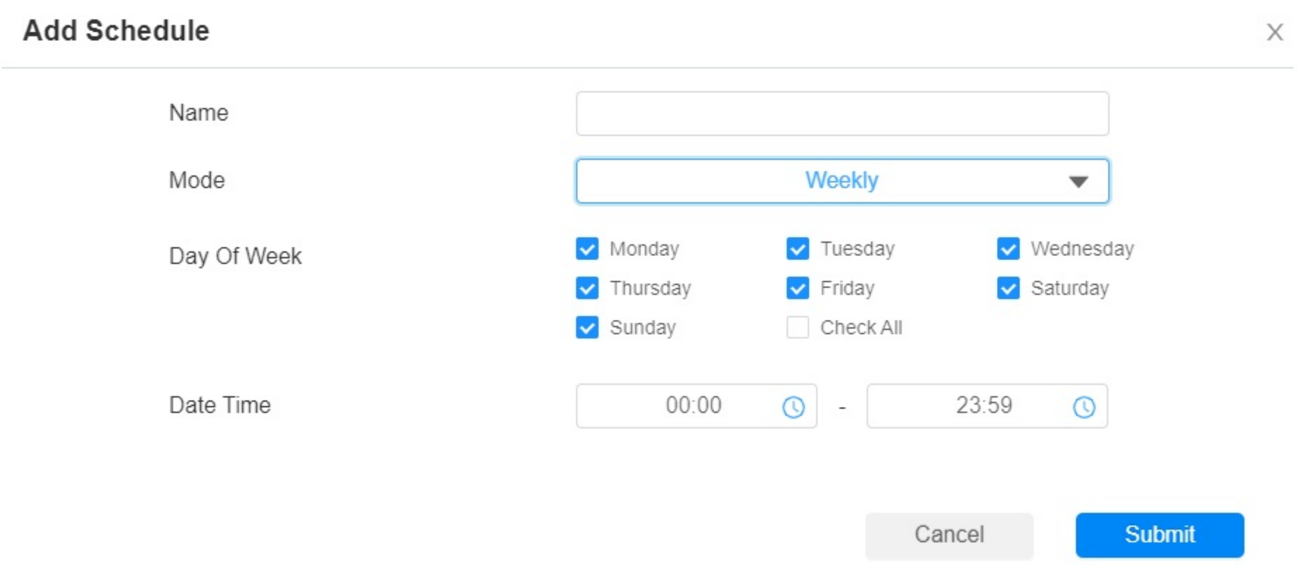
Add Schedule

Name:

Mode: Daily

Date Time: 00:00 - 23:59

To create a weekly schedule:



Add Schedule

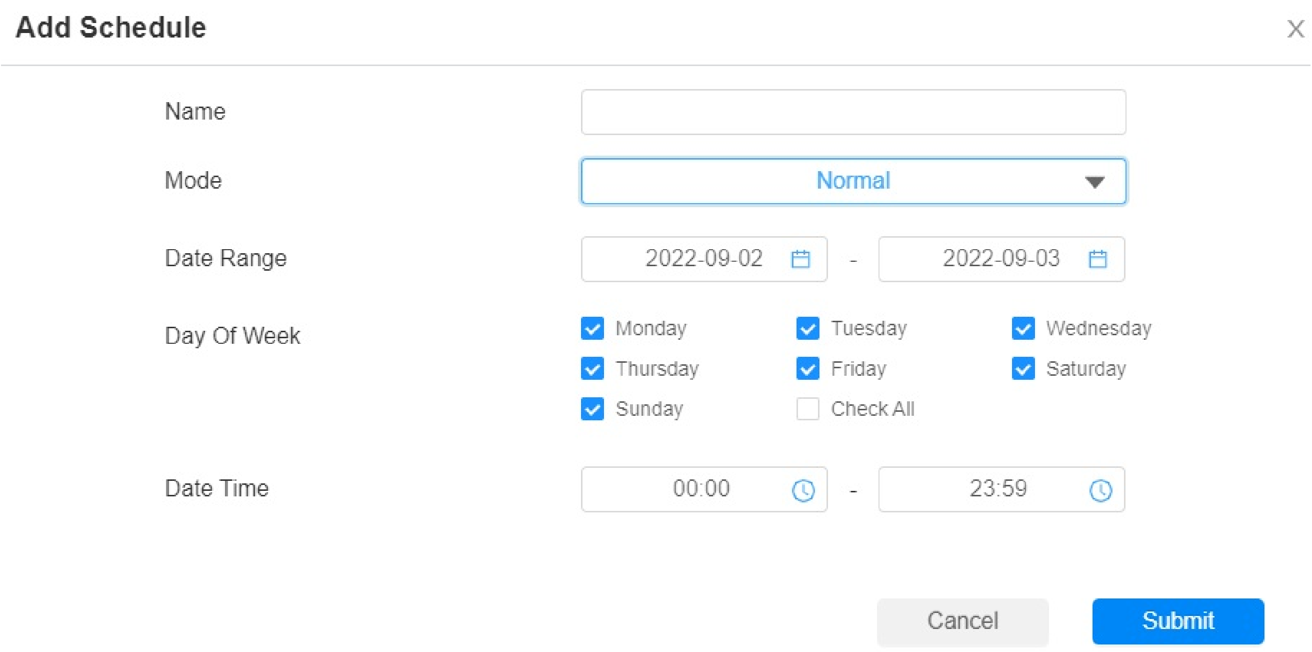
Name:

Mode: Weekly

Day Of Week: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday □ Check All

Date Time: 00:00 - 23:59

To create a longer period schedule:



Add Schedule

Name:

Mode: Normal

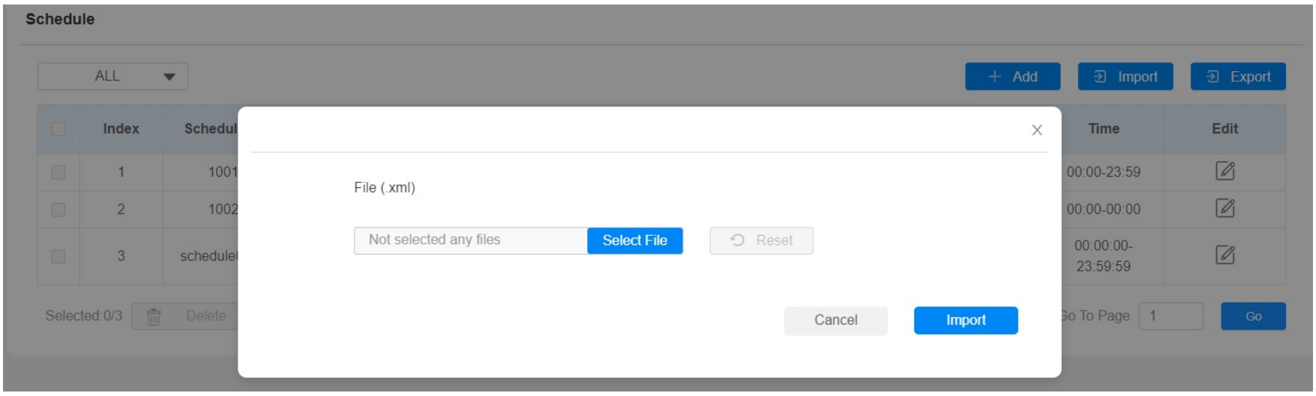
Date Range: 2022-09-02 - 2022-09-03

Day Of Week:
☑ Monday ☑ Tuesday ☑ Wednesday
☑ Thursday ☑ Friday ☑ Saturday
☑ Sunday □ Check All

Date Time: 00:00 - 23:59

Import and Export Door Access Schedule

In addition to creating door access schedules separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency. To configure the configuration on web **Access Control > Schedule,** then click Import .



Schedule

□	Index	Schedul	Time	Edit
□	1	1001	00:00-23:59	
□	2	1002	00:00-00:00	
□	3	schedule	00:00:00- 23:59:59	

Selected:0/3

File (.xml)

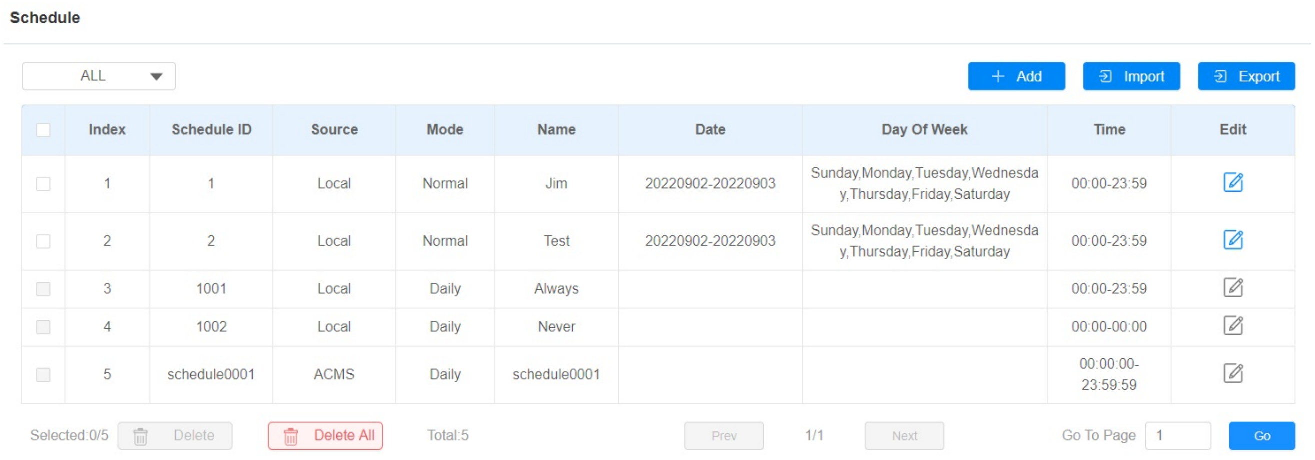
Not selected any files

Note

- It only supports .xml format files for importing and exporting the schedule.

Edit the Door Access Schedule

If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch on the web Setting>**Schedule.**



Schedule

ALL ▾ | + Add | Import | Export

□	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
□	1	1	Local	Normal	Jim	20220902-20220903	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	✎
□	2	2	Local	Normal	Test	20220902-20220903	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	✎
□	3	1001	Local	Daily	Always			00:00-23:59	✎
□	4	1002	Local	Daily	Never			00:00-00:00	✎
□	5	schedule0001	ACMS	Daily	schedule0001			00:00:00-23:59:59	✎

Selected:0/5 | Delete | Delete All | Total:5 | Prev | 1/1 | Next | Go To Page 1 | Go

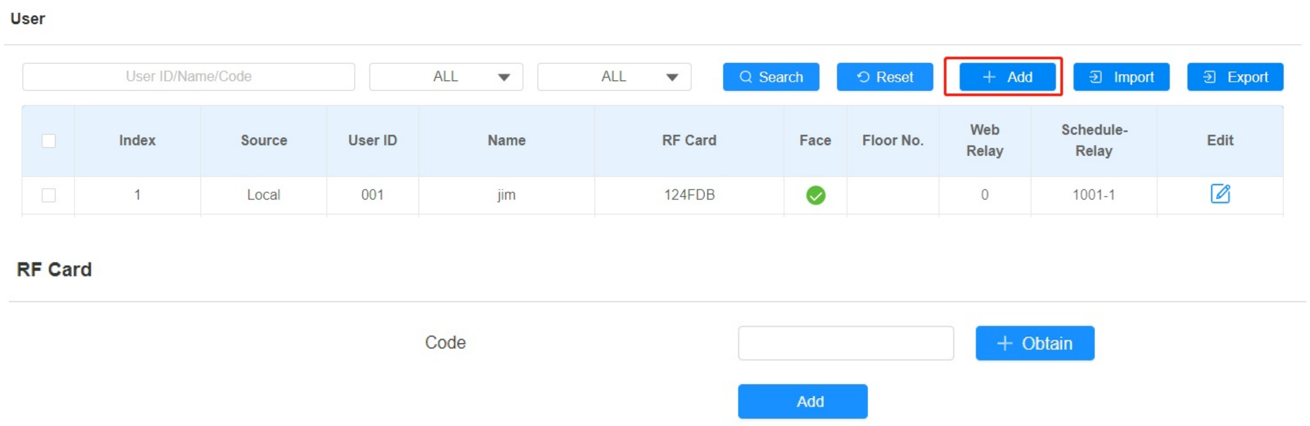
Door Unlock Configuration

A05 series access control terminal offers you three types of door access via QR code, RF card, and Facial recognition. You can configure them on web interface. Moreover, you can import or export the configured files to maximize your RF card configuration efficiency.

Configure RF Card for Door Unlock

Configure RF Card on the Web Interface

To configure the configuration on web **Directory > User**, click **+ Add**. Then click **+Obtain** and tap your card on the card reader.



User

User ID/Name/Code | ALL ▾ | ALL ▾ | Search | Reset | + Add | Import | Export

□	Index	Source	User ID	Name	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	001	jim	124FDB	✓		0	1001-1	✎

RF Card

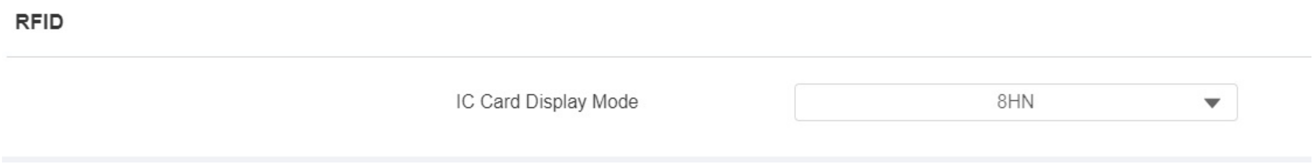
Code: | + Obtain

Add

> **Note**
>
> - Please refer to PIN code access schedule selection for the RF card user(s)-specific door access.
> - RF card with 13.56 MHz and 125 kHz can be applicable to the access control terminal for the door access.

Configure RF Card Code Format

If you want to integrate with the third-party intercom system in terms of RF card door access, you can change the RF card code format to be identical to that applied in the third-party system. To configure the configuration on web **Access Control > Card Setting > RFID** interface.



RFID

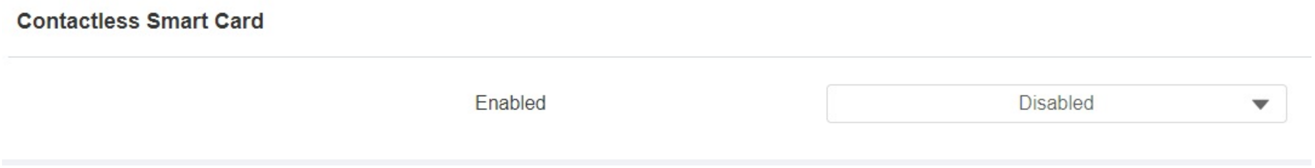
IC Card Display Mode: 8HN

Parameter Set-up:

- **IC Card Display Mode**: select the card format for the **ID Card** for the door access among five format options: 8HN,8H10D,6H3D5D,6H8D,8HN,8HR,8HD. The card code format is 8HN by default in the access control terminal.

Unlock by NFC

NFC(Near Field Communication) is a popular way for door access. It uses radio waves for data transmission interaction. A01 can be unlocked by NFC. You can keep the mobile phone closer to the door phone for door access. To configure the configuration on web **Access Control > Card Setting > Contactless Smart Card** interface.

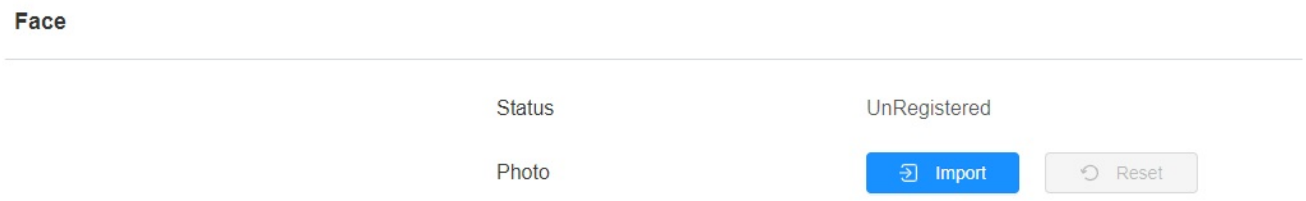


Contactless Smart Card

Enabled: Disabled

Configure Facial Recognition on Web Interface

To configure the configuration on web **Directory > User,** then click **+Add.**



Face

Status: UnRegistered

Parameter Set-up:

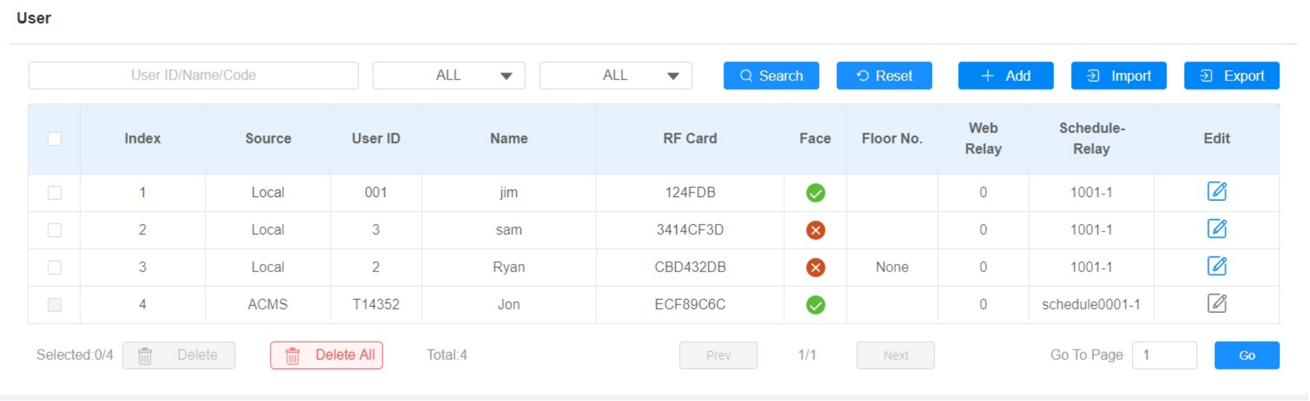
- **Status**: It will show **"Registered"** when the picture uploaded conforms to the format and standard otherwise it would show **"Unregistered"** as the default. However, the status will be changed back to **Unregistered** if the picture uploaded is cleared when you press the **Reset** tab.
- **Photo:** select the picture in jpg or png format to be uploaded to the device and press if you want to clear the picture uploaded.

Note

- Pictures to be uploaded should be in jpg or png format.

Configure Door Access Using Configured Files

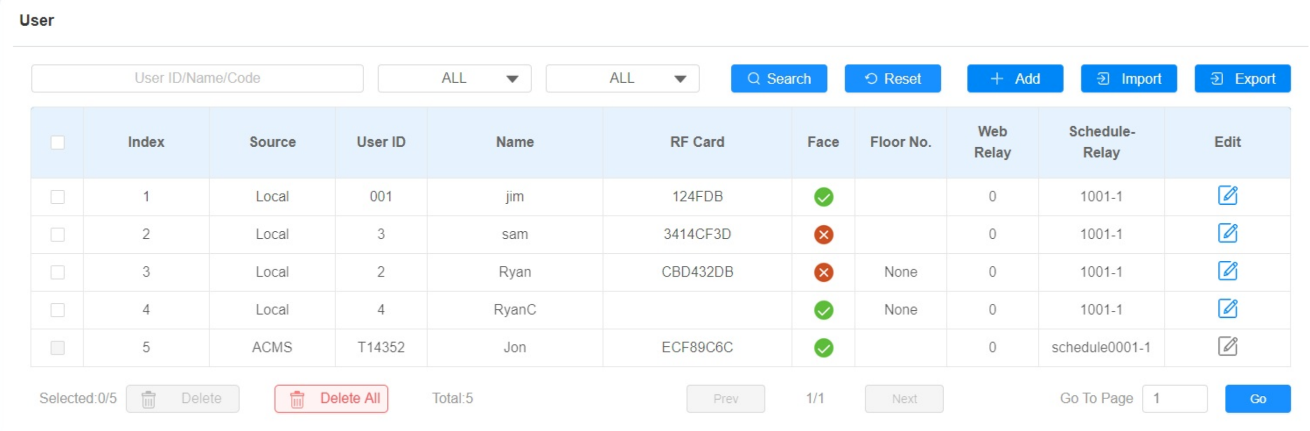
A05 series access control terminals allow you to speedily configure user(s)-specific door access in batch by importing the configured all-in-one door access control files incorporating user information, door access type, door access schedule, etc., thus all the door access setting can be done at one stop, saving your time and effort from configuring the door access for users separately when users are large in number. To configure the configuration on web **Access Control > User** interface.



□	Index	Source	User ID	Name	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	001	jim	124FDB	✓		0	1001-1	✎
□	2	Local	3	sam	3414CF3D	✗		0	1001-1	✎
□	3	Local	2	Ryan	CBD432DB	✗	None	0	1001-1	✎
□	4	ACMS	T14352	Jon	ECF89C6C	✓		0	schedule0001-1	✎

Editing the User(s)-specific door access data

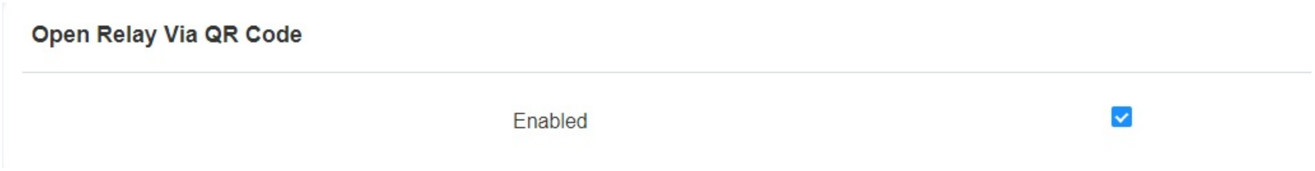
You can search user(s)-specific door access and edit the door access data on the web **Access Control > User** interface.



□	Index	Source	User ID	Name	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	001	jim	124FDB	✓		0	1001-1	✎
□	2	Local	3	sam	3414CF3D	✗		0	1001-1	✎
□	3	Local	2	Ryan	CBD432DB	✗	None	0	1001-1	✎
□	4	Local	4	RyanC		✓	None	0	1001-1	✎
□	5	ACMS	T14352	Jon	ECF89C6C	✓		0	schedule0001-1	✎

Unlock by QR Code

QR code is another option for door access. If you want to apply for QR code access, you need to enable the QR code function. To configure the configuration on web **Access Control > Relay > Open Relay via QR Code** interface.



Open Relay Via QR Code

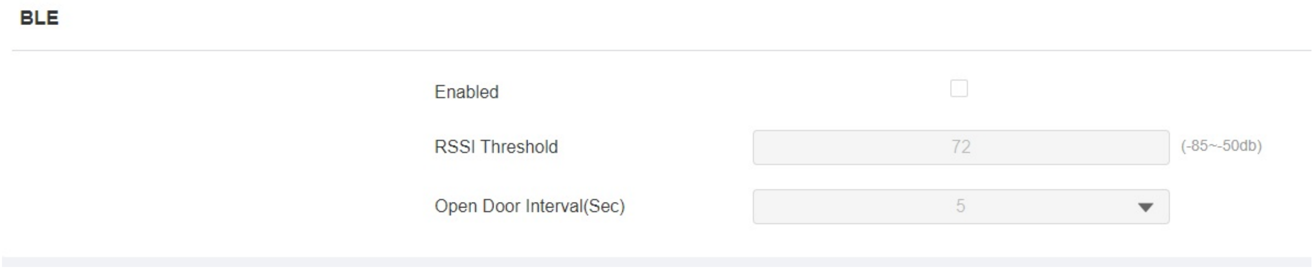
Enabled ☑

Note

- The function should work with Akuvox SmartPlus. For more information, please contact Akuvox technical support.

Unlock by Bluetooth

You can also gain door access by mobile phone with Bluetooth which is used together with Akuvox SmartPlus. You can shake the mobile phone closer to the access control terminal for door access. To configure the configuration on web **Access Control > BLE > BLE** interface.



BLE

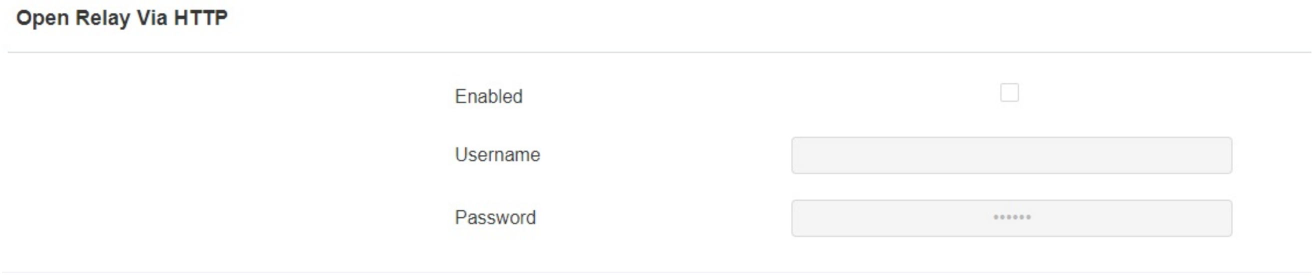
Enabled	□	
RSSI Threshold	72	(-85~-50db)
Open Door Interval(Sec)	5 ▾	

Parameter Set-up:

- **Enabled:** enable or disable the Bluetooth function. Bluetooth is turned off by default.
- **Rssi Threshold:** select the signal receiving strength from -85~-50db in absolute terms. The higher value it is, the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval(Sec):** select the time interval between every two Bluetooth door accesses.

Unlock by HTTP Command on Web Browser

You can unlock the door remotely without approaching the device physically for door access by typing in the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for door access. To configure the configuration on web **Access Control > Relay > Open Relay via HTTP** interface.



Open Relay Via HTTP

Enabled	□
Username	
Password	••••••

Parameter Set-up:

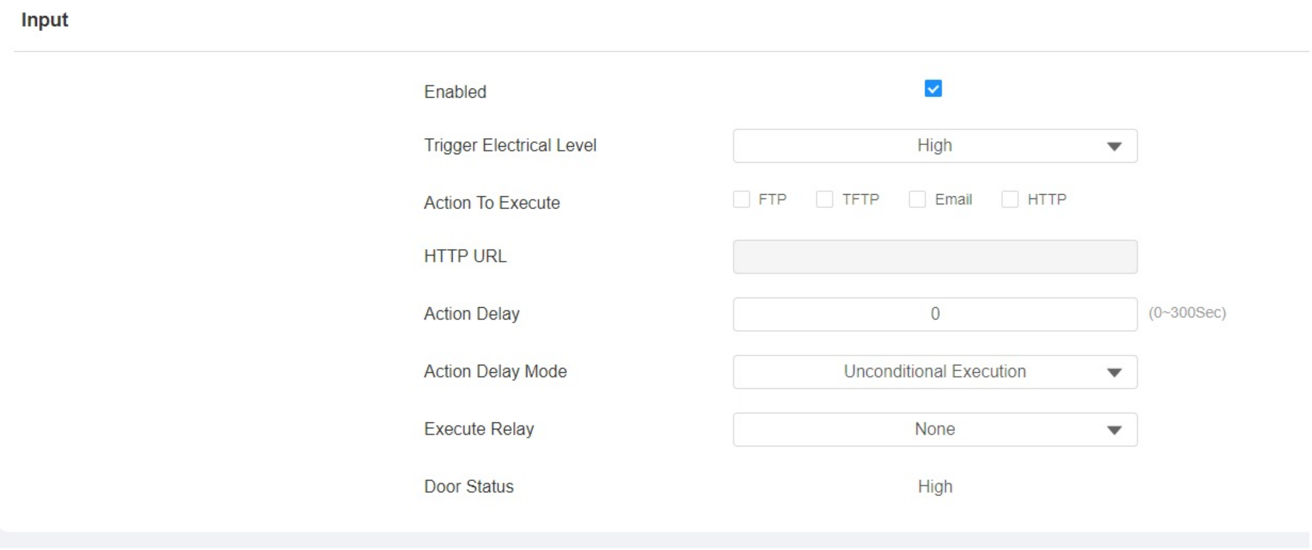
- **Enabled:** enable the HTTP command unlock function by clicking on **Enable** field.

- **Username:** enter the user name of the device web interface, for example: **Admin.**
- **Password**: enter the password for the HTTP command. For example: **12345. Please refer to the following example:** http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

> **Note**
>
> - **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

Unlock by Exit Button by the Door

When you need to open the door from inside using the exit button installed by the door, you can configure the access control terminal Input to trigger the relay for the door access. To configure the configuration on web **Access Control** > **Input** > **Input** interface.



Input

Enabled	☑
Trigger Electrical Level	High
Action To Execute	□ FTP □ TFTP □ Email □ HTTP
HTTP URL	
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution
Execute Relay	None
Door Status	High

Parameter Set-up:

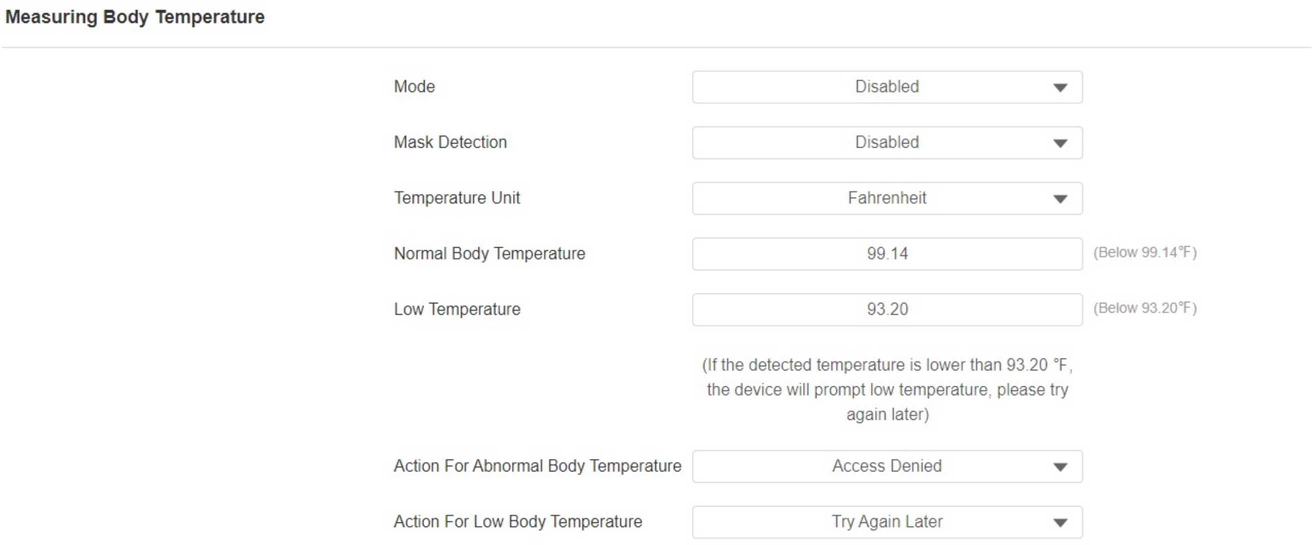
- **Trigger Electrical Level:** select the trigger electrical level options between **High** and **Low** according to the actual operation of the exit button.
- **Action to Execute:** set actions to be triggered by the input. FTP, TFTP, Email and HTTP URL actions are supported.
- **HTTP URL**: to set HTTP URL.
- **Action Delay:** set the action delay timing (ranging from 1-300 Sec.) For example, if you set the delay time as **5**. then the action will not be triggered until 5 seconds after the input status changes.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of the input signal.

Body Temperature Measurement for Door Access (Optional)

A05 series provides you with an optional body temperature measurement function designed to be applied in the situation where the measurement becomes necessary for the safety of the residents and visitors etc. Residents and visitors are required to go through temperature measurements along with an optional mask detection check before they are allowed door access.

Body Temperature Measurement Configuration

You can configure the body temperature measurement function in terms of defining the normal temperature as well as making schedule for the validity of the function etc. To configure the configuration on web **Access Control** > **Body Temperature** > **Measuring Body Temperature** interface.



Measuring Body Temperature

Mode	Disabled	
Mask Detection	Disabled	
Temperature Unit	Fahrenheit	
Normal Body Temperature	99.14	(Below 99.14℉)
Low Temperature	93.20	(Below 93.20℉)
	(If the detected temperature is lower than 93.20 ℉, the device will prompt low temperature, please try again later)	
Action For Abnormal Body Temperature	Access Denied	
Action For Low Body Temperature	Try Again Later	

Parameter Set-up:

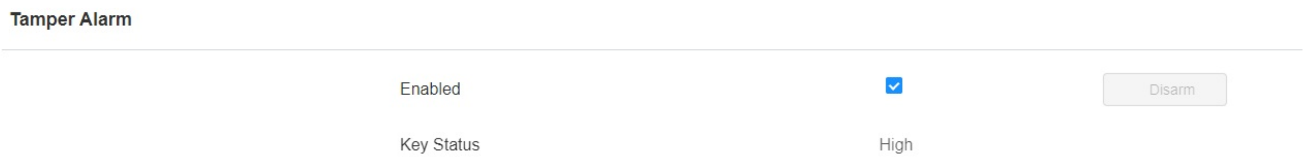
- **Mode**: select either **Disabled** Mode or **Wrist** Mode for temperature measurement according to your need. The device can be installed with a digital forehead temperature detector therefore you are required to set the mode properly according to your application.
- **Mask Detection**: select **Enable** or **Disable** to turn on or turn off the mask detection. When enabled, the device will check if the visitor is wearing a mask or not while reminding the visitor with the announcement **"Please wear a mask"** visitors wearing a mask will be prompted either **"Keep face in the frame"** or **"Keep wrist close to the sensor"** depending on the mode that is selected. Warning alarm will be triggered when the body temperature measured is detected higher than the defined normal body temperature.
- **Normal Body Temperature**: set the body temperature to the predefined body temperature as the measuring basis in either Fahrenheit or Celsius. For example, if you set the temperature 37.3 degrees Celsius as the normal temperature, then any body temperature measured higher than 37.3 degrees Celsius will be deemed as abnormal temperature, while a temperature lower than 34 degree Celsius will be deemed as low body temperature.
- **Low Temperature**: set the low temperature.
- **Action for Abnormal Body Temperature**: if you select the prompt **Access Denied** then you will be denied access for having a high body temperature. If you select **Just For Reminder**, you will still be granted access with high body temperature.
- **Action for Low Body Temperature**: if you select the prompt **Try Again later** you will not be given access

permission for the low body temperature. If you select **Just For Reminder** you will still be granted access with low body temperature.

Security

Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm on the device. To configure the configuration on web **System > Security > Temper Alarm** interface.



Tamper Alarm

Enabled ☑ Disarm

Key Status High

Parameter Set-up:

- **Enable**: tick the check box to enable the temper alarm function. When the temper alarm goes off, you can press the **Disarm** tab beside the check box to clear the alarm.
- **Key Status**: temper alarm will not be triggered unless the key status is shifted from **Low** to **High** status.

Note

- **Disarm** tab will turn gray when the temper alarm is cleared.
- The round rubber button at the back of the device must be in press-down status otherwise the alarm will not be fired.

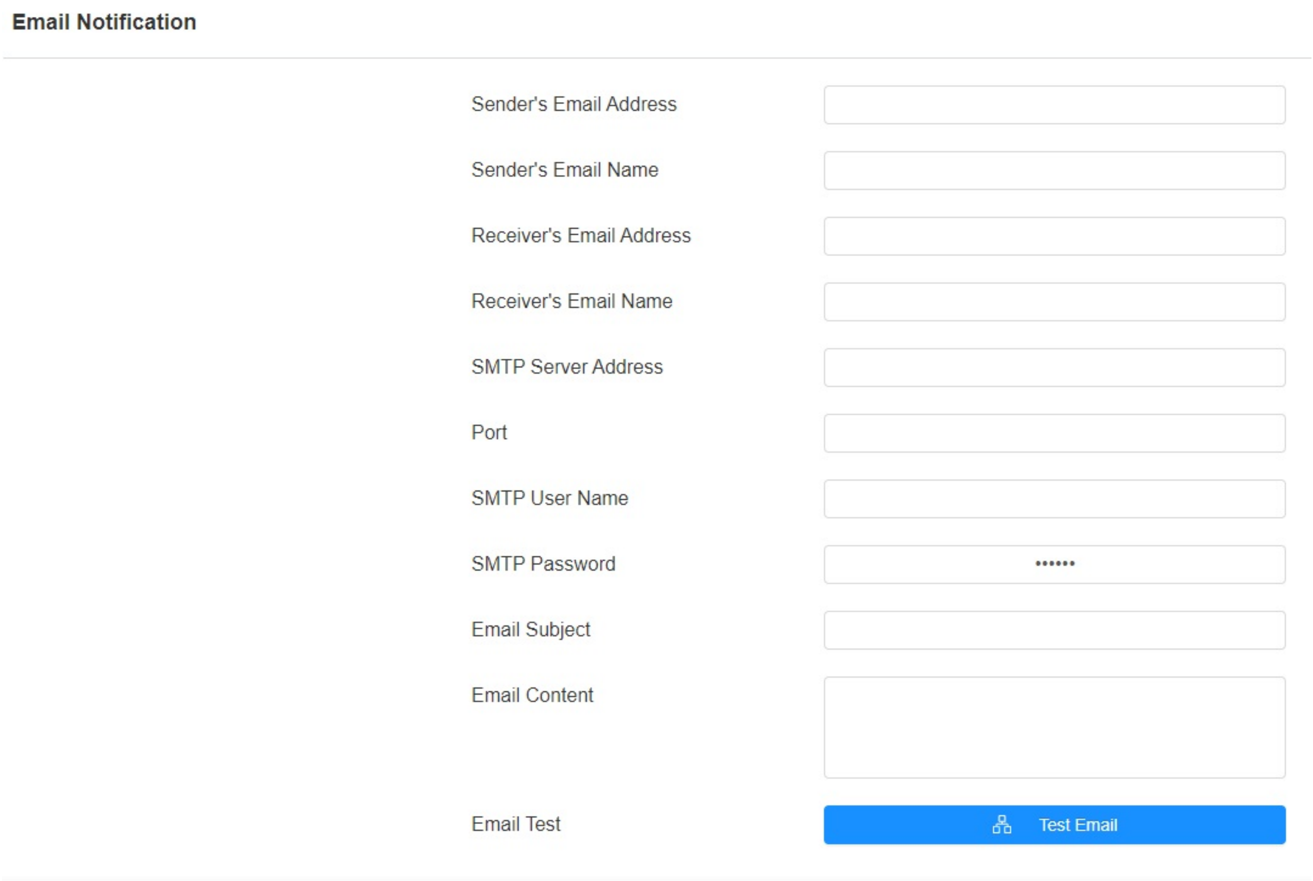
Note

- **The round rubber button at the back of the device must be in press-down status otherwise the alarm will not be fired.**

Security Notification Setting

Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web interface properly. To configure the configuration on web **Setting > Action > Email Notification** interface.



Email Notification

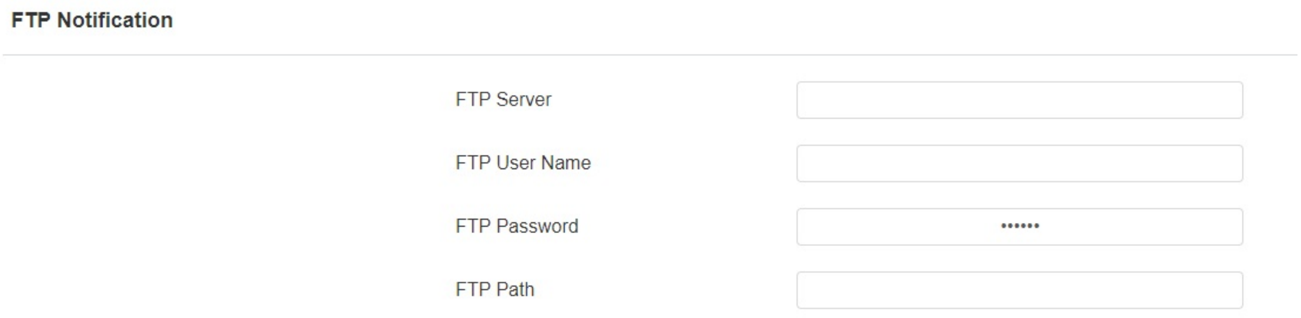
Sender's Email Address	
Sender's Email Name	
Receiver's Email Address	
Receiver's Email Name	
SMTP Server Address	
Port	
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	
Email Test	Test Email

Parameter Set-up:

- **Sender's Email Name:** enter the name of the email sender.
- **Sender's Email address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's Email address:** enter the receiver's email address.
- **Receiver's Email Name:** enter the name of the email receiver.
- **SMTP server address:** enter the SMTP server address of the sender.
- **Port:** enter the port number from which the email is sent out.
- **SMTP user name:** enter the SMTP user name, which is usually the same with sender's email address.
- **SMTP password:** configure the password of SMTP service, which is same with sender's email address.
- **Email subject:** enter the subject of the email.
- **Email content:** compile the email contents according to your need.
- **Email Test**: click to test if the email can be sent and received.

FTP Notification setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the web interface properly. To configure the configuration on web **Setting > Action > FTP Notification** interface.



FTP Notification

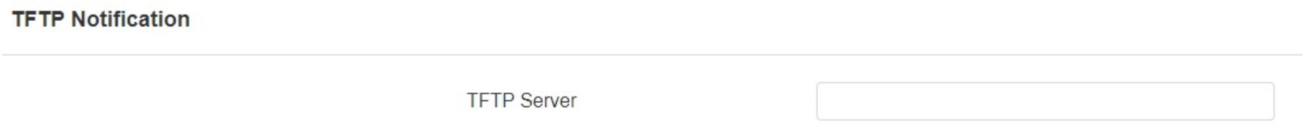
FTP Server	
FTP User Name	
FTP Password	••••••
FTP Path	

Parameter Set-up:

- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name**: enter the FTP server user name.
- **FTP Password**: enter the FTP server password.
- **FTP Path**: enter the folder name you created in FTP server.

TFTP Notification Setting

If you want to receive the security notification via TFTP, you can configure the FTP notification on the web interface properly. To configure the configuration on web **Setting > Action > TFTP Notification** interface.



TFTP Notification

TFTP Server	

Parameter Set-up:

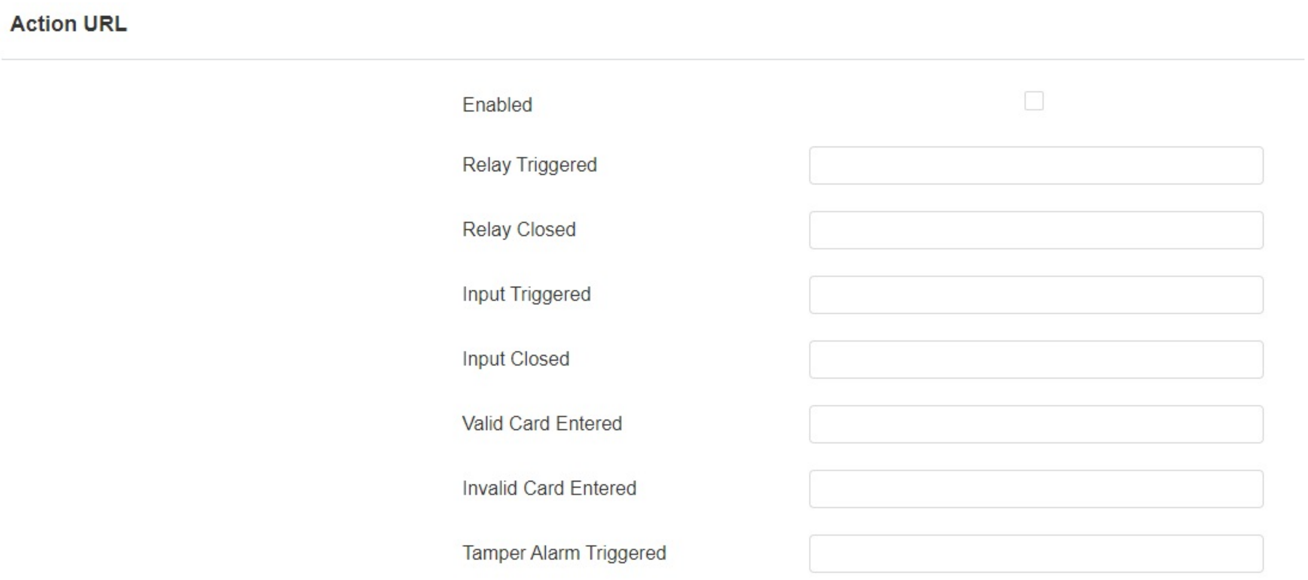
- **TFTP Server**: enter the address (URL) of the TFTP server for the TFTP notification

Action URL

A05 allows you to set up specific HTTP URL commands that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occurs any changes in the relay status, input status, PIN code, and RF card access for security purpose. You can navigate to **Setting > Actions URL**.

Note

- Action URL and format are provided by third party manufacturer, Akuvox door phone only sends the URL to third party devices.



Action URL

Enabled	□
Relay Triggered	
Relay Closed	
Input Triggered	
Input Closed	
Valid Card Entered	
Invalid Card Entered	
Tamper Alarm Triggered	

Akuvox Action URL:

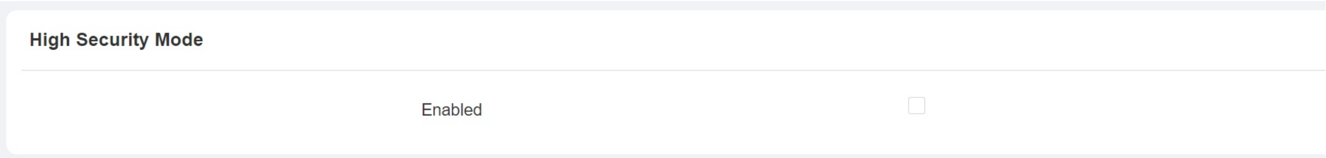
No	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/Callnumber=$remote
2	Hang Up	$remote	Http://server ip/Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/relaytrigger=$relay1status
5	Relay Closed	$relay1status	Http://server ip/relayclose=$relay1status
6	Input Triggered	$input1status	Http://server ip/inputtrigger=$input1status
7	Input Closed	$input1status	Http://server ip/inputclose=$input1status
8	Valid Code Entered	$code	Http://server ip/validcode=$code
9	Invalid Code Entered	$code	Http://server ip/invalidcode=$code
10	Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
11	Invalid Car Entered	$card_sn	Http://server ip/invalidcard=$card_sn
12	Tamper Alarm Triggered	$alarm status	Http://server ip/tampertrigger=$alarm status

High Security Mode

High security mode is designed to enhance the security, for example, it optimizes the password storage method.

Please note that once the mode is enabled, it is not allowed to downgrade the device from the version with the mode to an old one without it.

To configure this feature on the web: **System>Security>High Security Mode**



High Security Mode

Enabled ☐

Important Notes

1. This mode is disabled by default when the device is upgraded to a new version with high security from an older version without the mode. However, if the device is reset to its factory settings, the mode is enabled by default.

2. Enabling this mode will make the old version tools unusable. To continue using them, you must upgrade them to the following versions.

- PC Manager: 1.2.0.0
- IP Scanner: 2.2.0.0
- Upgrade Tool: 4.1.0.0
- SDMC: 6.0.0.34

3. The supported HTTP format varies depending on whether high secure mode is enabled or disabled.

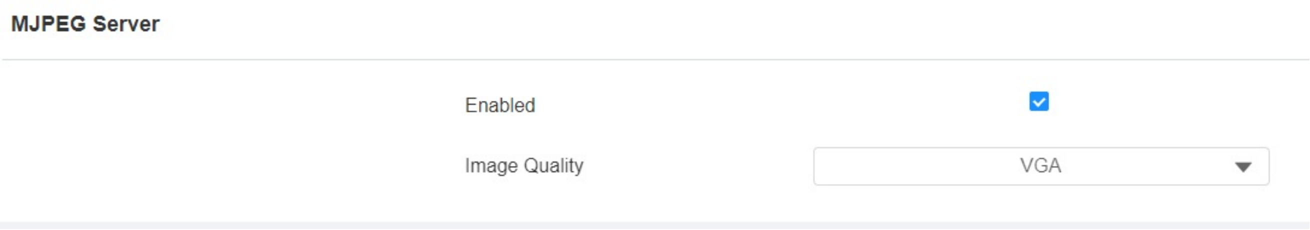
- When the mode is turned on, the device only supports new HTTP formats for door opening.
    - http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
    - http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- When the mode is off, the device supports the above two new formats as well as the old one:
    - http://deviceIP/fcgi/do?ction=OpenDoor&UserName=username&Password=password&DoorNum=1

4. It is not allowed to import/export tgz. format configuration files between a new version device and an old version device without high security mode.

Monitor and Image

MJPEG Image Capturing

A05 series allows you to capture the Mjpeg format monitoring image if needed. You can enable the MJPEG function and set the image quality on the web interface. To configure the configuration on web **Surveillance** > **MJPEG** > **MJPEG Server** interface.



MJPEG Server

Enabled ☑

Image Quality: VGA

Parameter Set-up:

- **Enabled**: tick the check box to enable or disable the MJPEG service.
- **Image Quality**: select the quality for the image capturing among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P,** and **1080P.**

After the MJPEG service is enabled, you can capture the image from the access control terminal using the following three types of URL format:

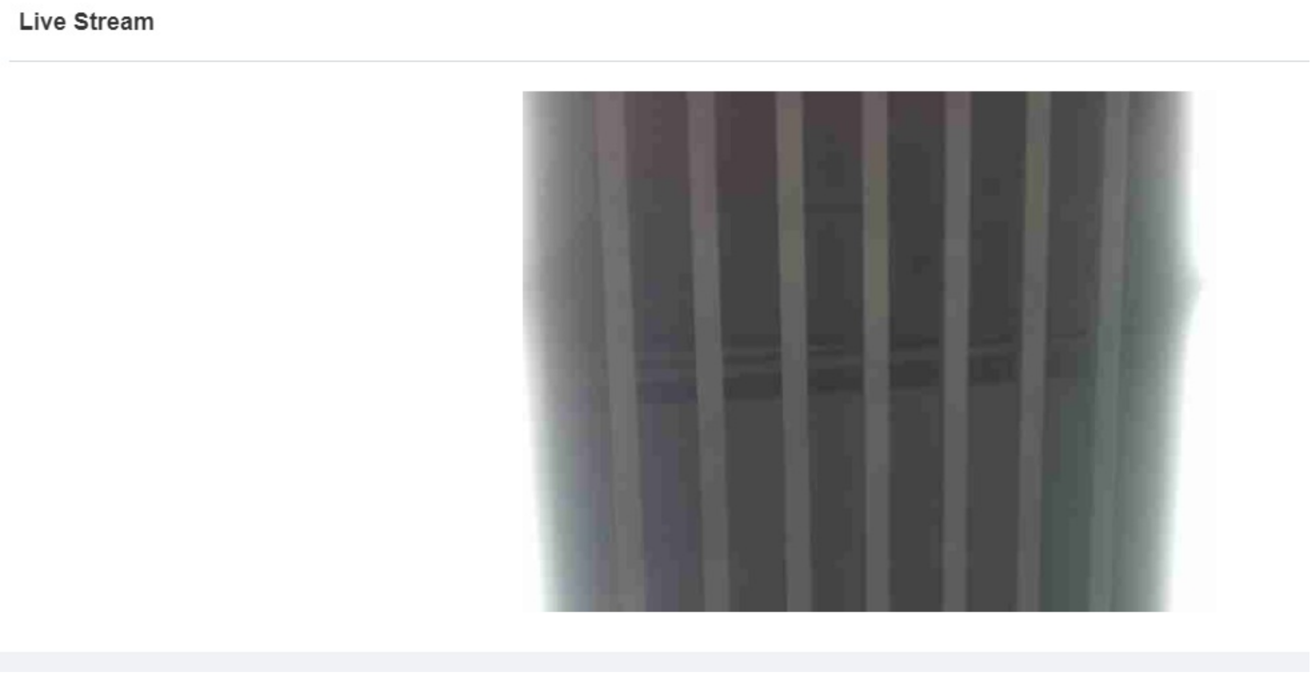
- http:// device ip:8080/picture.cgi
- http://device ip:8080/picture.jpg
- http://device ip:8080/jpeg.cgi

For example, if you want to capture the jpg format image of the access control terminal with the IP address: 192.168.1.104, you can enter “http://192.168.1.104:8080/picture.jpg” on the web browser.

Live Stream

If you want to check the real-time video from the A05 series access control terminal, you can go to the device web interface to obtain the real-time video or you can also enter the correct URL on the web browser to obtain it directly.

To see the live stream on web **Surveillance** > **Live Stream** interface.



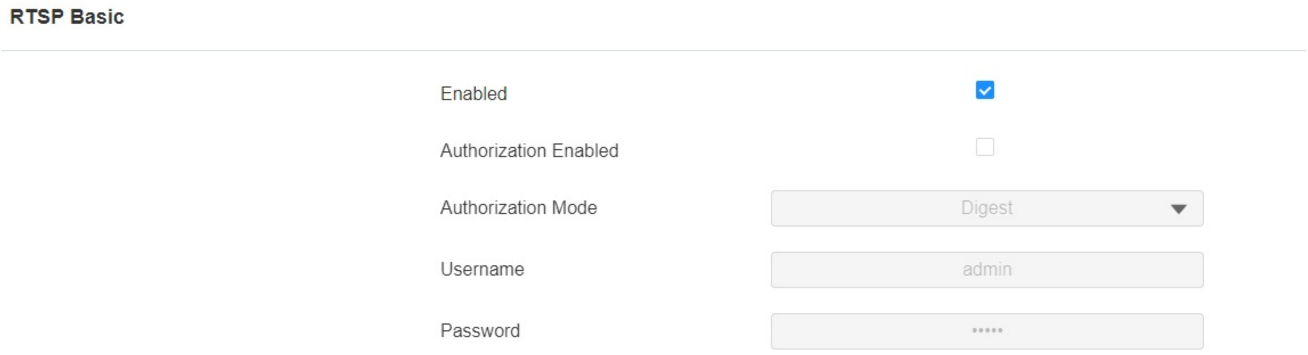
To check the real time video using URL, you can enter the correct URL (http://IP_address:8080/video.cgi) on the web browser if you want to obtain the real-time video directly by going to the web interface.

RTSP Stream Monitoring

A05 series access control terminal support RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or obtain the real time audio/ video (RTSP stream) from the access control terminal using the correct URL.

RTSP Basic Setting

You are required to set up the RTSP function in terms of RTSP authorization, authentication, and password, etc., before you are able to use the function. To configure it, go to **Surveillance** > **RTSP** > **RTSP Basic** interface.



RTSP Basic

Enabled	☑
Authorization Enabled	☐
Authorization Mode	Digest
Username	admin
Password	•••••

Parameter Set-up:

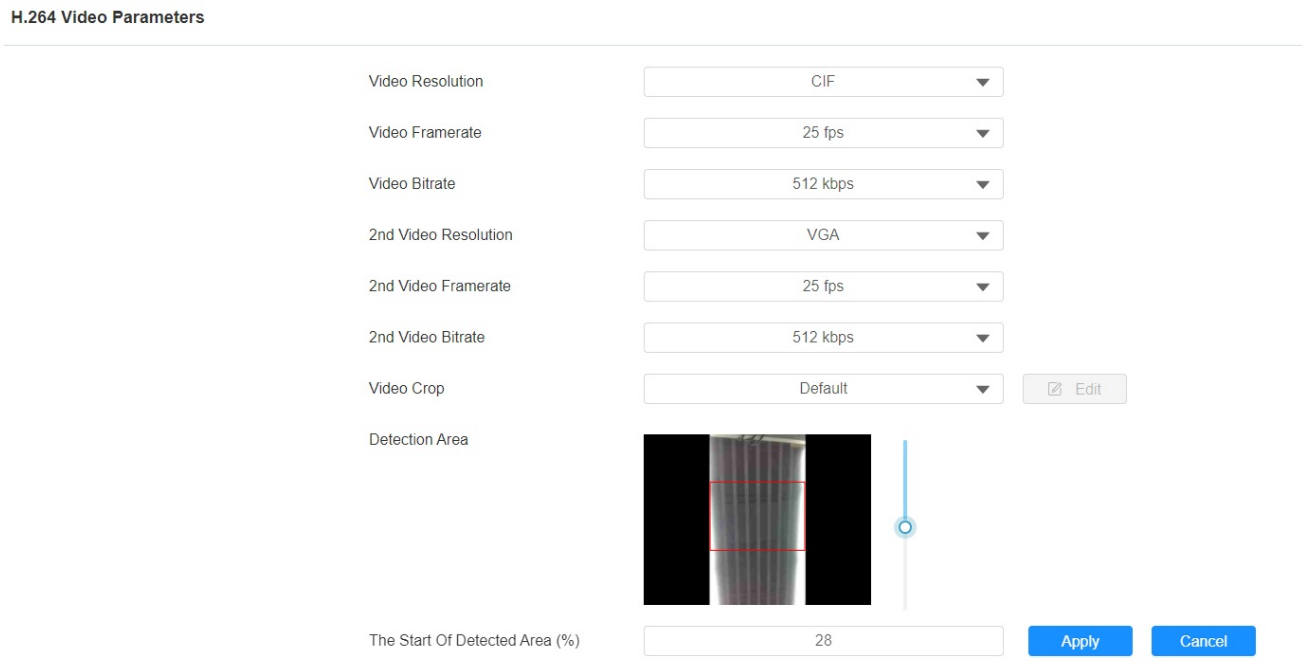
- **Enabled:** tick the check box to turn on or turn off the RTSP function.
- **AuthorizationEnabled**: tick the check box to enable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, and RTSP Password on

the intercom device such as indoor monitor for authorization.

- **RTSP Authentication Type**: select RTSP authentication type between **Basic** and **Digest. Basic** is the default authentication type. This is applicable when the authorization is enabled.
- **Username**: enter the name used for RTSP authorization.
- **Password**: enter the password for RTSP authorization.

RTSP Stream Setting

You can select the video codec format for the RTSP stream for the monitoring and you can also configure video resolution and bitrate, etc. based on your actual network environment on the web interface. To configure the configuration on web **Surveillance > RTSP > H.264 Video Parameters** interface.



H.264 Video Parameters

Video Resolution	CIF
Video Framerate	25 fps
Video Bitrate	512 kbps
2nd Video Resolution	VGA
2nd Video Framerate	25 fps
2nd Video Bitrate	512 kbps
Video Crop	Default
Detection Area	
The Start Of Detected Area (%)	28

Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: **QCIF**, **QVGA**, **CIF**, **VGA**, **4CIF**, **720P**, and **1080P**. The default video resolution is **720P**, and the video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than **720P**.
- **Video Framerate**: **25fps** is the video frame rate by default.
- **Video Bitrate**: select video bit-rate among six options: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps** according to your network environment. The default video bit rate is **2048 kbps**.
- **2nd Video Resolution2**: select the video resolution for the second video stream channel. While the default video solution is **VGA**.
- **2nd Video Framerate**: select the video framerate for the second video stream channel. **25fps** is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate**: select video bit rate among the six options for the second video stream channel. While the second video stream channel is **512 kbps** by default.
- **Video Crop**: select **Original** for the full-screen video display. And select **Default** if you only want to select

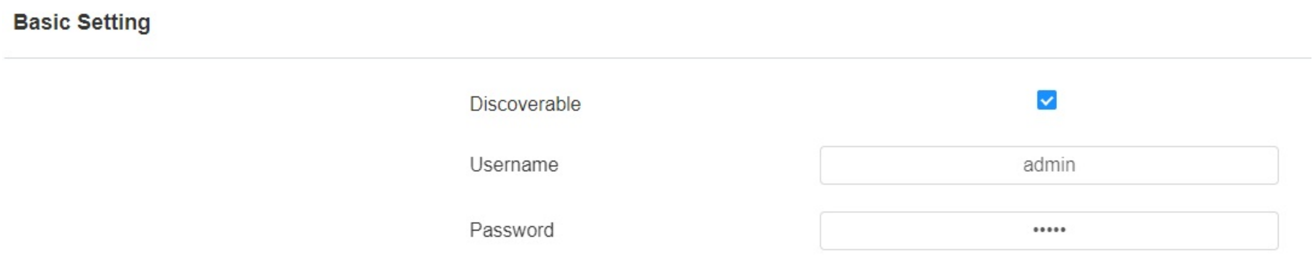
the specific area on the video to be displayed. You can click **Edit** to start video cropping.

Note

- A05 series supports two video stream channels for H.264 codec video stream.

ONVIF

Real-time video from the A05 series access control terminal camera can be searched and obtained by the Akuvox indoor monitor or by third-party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function in the access control terminal so that other devices will be able to see the video from the access control terminal. To configure the configuration on web **Intercom** > **ONVIF** interface.



Basic Setting

Discoverable ☑

Username admin

Password •••••

Parameter Set-up:

- **Discoverable:** tick the check box to turn on the ONVIF mode. If you select video from the access control terminal camera can be searched by other devices. ONVIF mode is **Discoverable** by default.
- **UserName:** enter the user name. The user name is **admin** by default.
- **Password**: enter the password. The password is **admin** by default.

After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream.

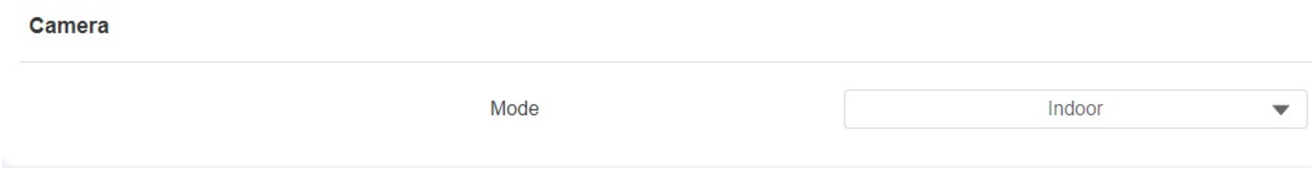
For example: http://IP **address:80/onvif/device_service**

Note

- Fill in the specific IP address of the access control terminal in the URL.

Camera Mode

You can select the camera mode for better video quality depending on where the door phone is located. You can select **Indoor mode** for better video image (RTSP, ONVIF, and Mjpeg) if the door phone is placed indoors. On the contrary, you can select **Outdoor mode** if the door phone is placed outdoors. To set it up, go to **Surveillance** > **ONVIF** > **Camera.**



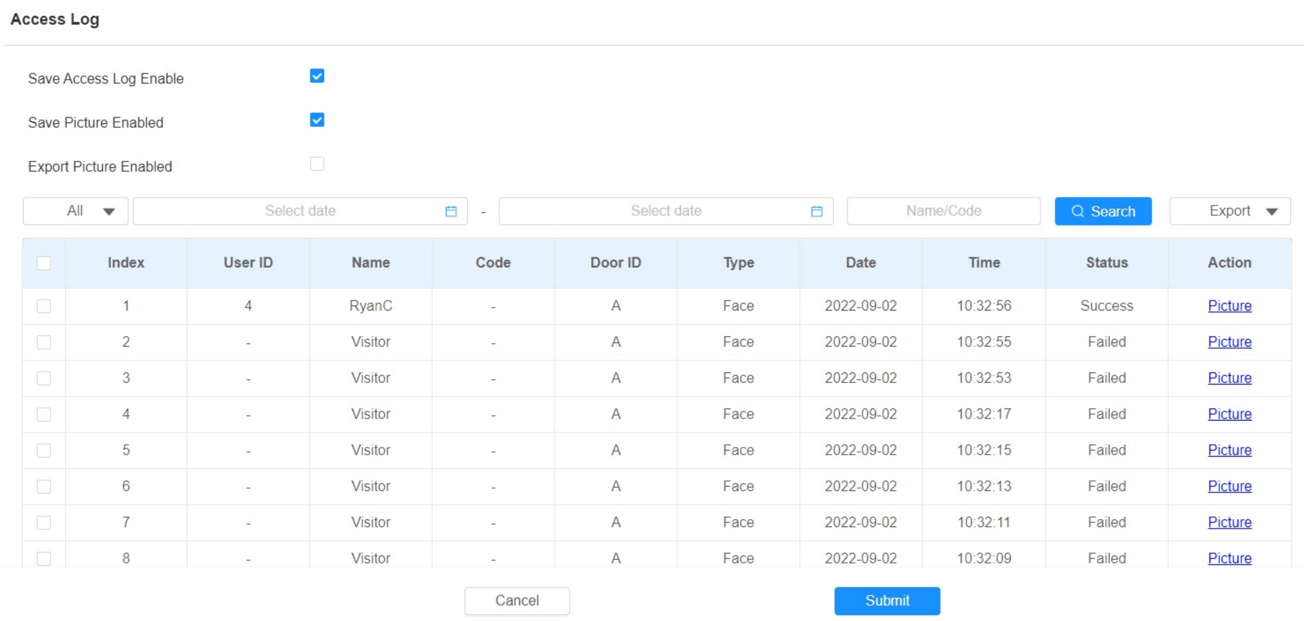
Camera

Mode: Indoor

Logs

Door Logs

If you want to search and check on door access history, you can search and check the door logs on the device web **Status > Access Log** interface.



Access Log

Save Access Log Enable ☑

Save Picture Enabled ☑

Export Picture Enabled □

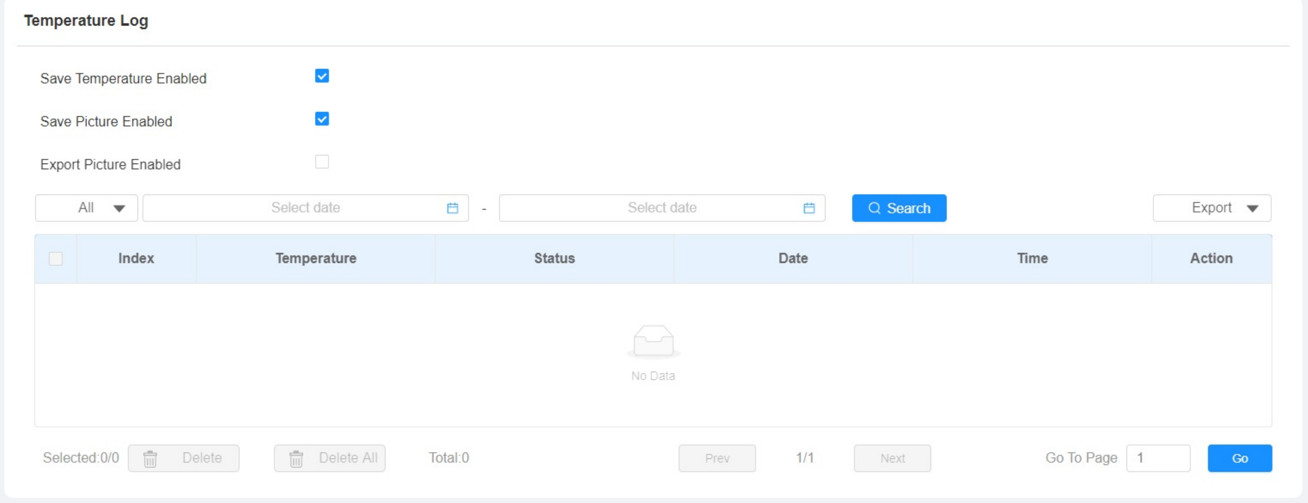
□	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status	Action
□	1	4	RyanC	-	A	Face	2022-09-02	10:32:56	Success	Picture
□	2	-	Visitor	-	A	Face	2022-09-02	10:32:55	Failed	Picture
□	3	-	Visitor	-	A	Face	2022-09-02	10:32:53	Failed	Picture
□	4	-	Visitor	-	A	Face	2022-09-02	10:32:17	Failed	Picture
□	5	-	Visitor	-	A	Face	2022-09-02	10:32:15	Failed	Picture
□	6	-	Visitor	-	A	Face	2022-09-02	10:32:13	Failed	Picture
□	7	-	Visitor	-	A	Face	2022-09-02	10:32:11	Failed	Picture
□	8	-	Visitor	-	A	Face	2022-09-02	10:32:09	Failed	Picture

Parameter Set-up:

- **Save Access Log Enabled:** tick the check box to turn on or turn off the door log function.
- **Status:** select between **Success** and **Failed** options to search for successful door accesses or Failed door accesses.
- **Time:** select the specific time span of the door logs you want to search, check or export.
- **Name/Code**: select the **Name** and **Code** options to search the door log by the name or by the PIN code.
- **Door ID:** displays the door name.
- **Type**: display the access type like card or HTTP.

Temperature Log

To check the temperature log on web **Access Control > Temperature Log** interface.



Temperature Log

Save Temperature Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled □

□	Index	Temperature	Status	Date	Time	Action

No Data

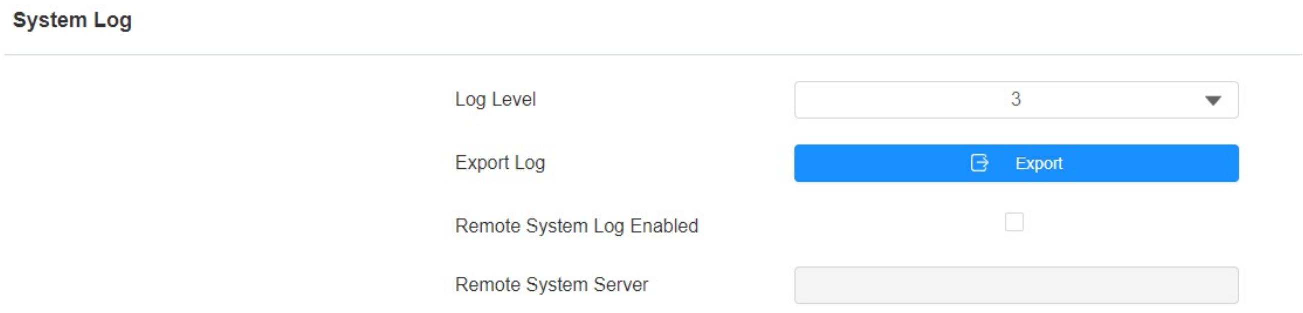
Selected:0/0 Delete Delete All Total:0 Prev 1/1 Next Go To Page 1 Go

- **Save Temperature Enabled:** tick the check box to turn on or turn off the temperature Log.
- **Save Picture Enabled**: enable it if you want to save the temperature measuring snapshot.
- **Export Picture Enabled**: enable it if you want to export the temperature log with a snapshot picture captured.
- **Time:** select the specific time span of the temperature log you want to search, check, or export.
- **Action**: click to display the picture captured.

Debug

System Log for Debugging

System log in the access control terminal can be used for debugging purpose. If you want to export the system out to a local PC or to a remote server for debugging, you can set up the function on the web **System > maintenance > System Log** interface.



System Log

Log Level: 3

Export Log: Export

Remote System Log Enabled □

Remote System Server

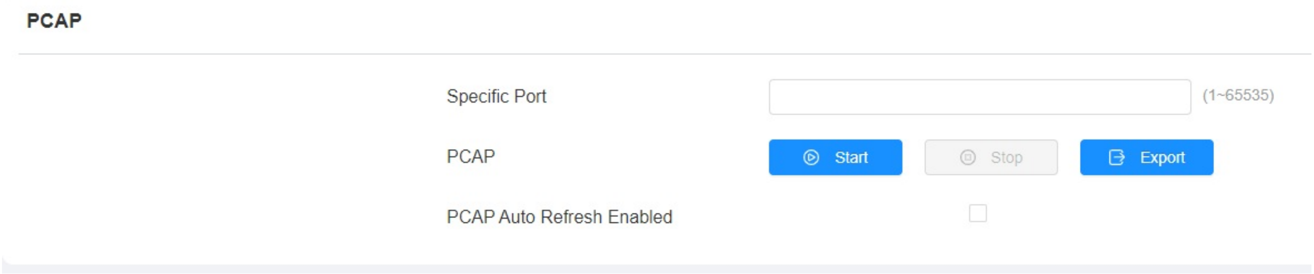
Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is **3**. The higher the level is, the more complete the log is.
- **Export Log**: click the **Export** tab to export the temporary debug log file to a local PC.
- **Remote System Log**: select **Enable** or **Disable** if you want to enable or disable the remote system log.
- **Remote System Server**: enter the remote server address to receive the device log. And the remote server

address will be provided by Akuvox technical support.

PCAP for Debugging

PCAP in A05 series access control terminal is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **System > maintenance> PCAP** interface properly before using it.



PCAP

Specific Port (1~65535)

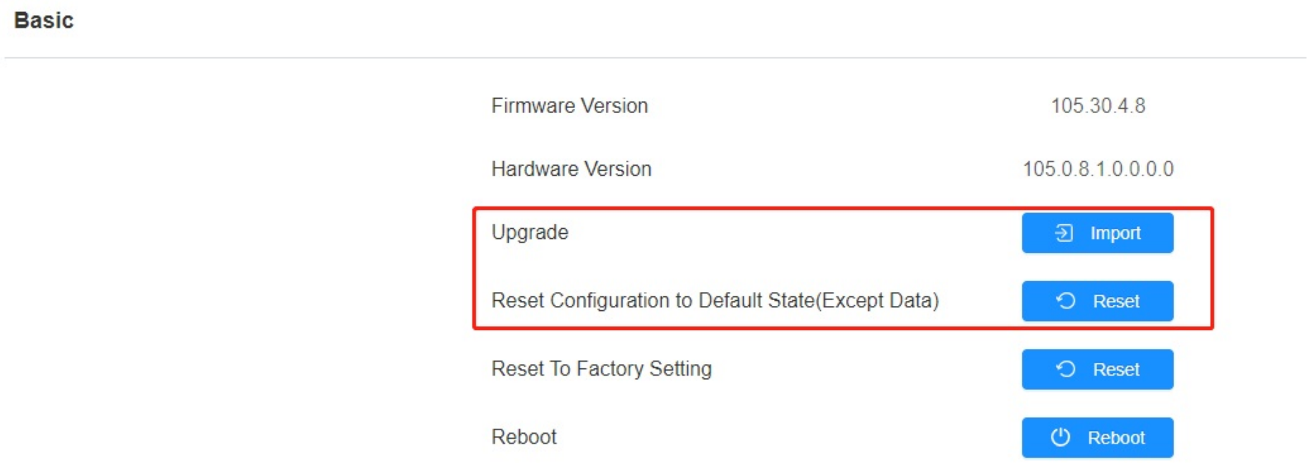
PCAP Auto Refresh Enabled □

Parameter Set-up:

- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: select **Enable** or **Disable** to turn on or turn off the PCAP auto fresh function. If you set it as **Enable** then the PCAP will continue to capture data packet even after the data packets reached its 50M maximum capacity. If you set it as **Disable** the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

Firmware Upgrade

Firmware of different versions for A05 series access control terminal can be upgraded on the device web **System > Upgrade > Basic** interface.



Basic

Firmware Version 105.30.4.8

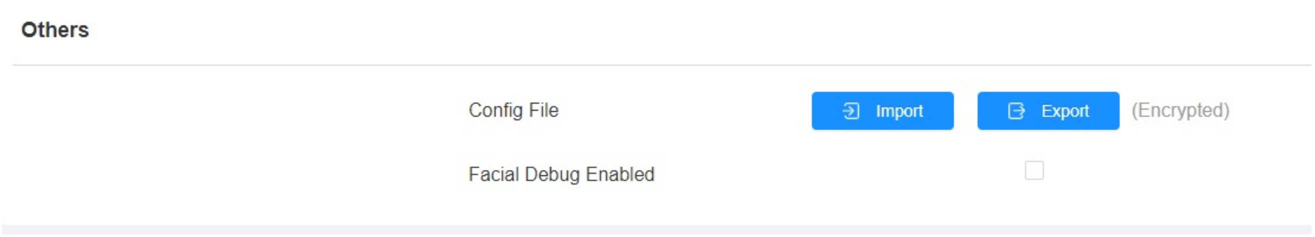
Hardware Version 105.0.8.1.0.0.0.0

Note

- Firmware files should be .rom format for the upgrade.

Backup

Configuration files can be imported to or exported out of the device to your local PC on the device web **Upgrade > Maintenance > Others** interface if needed.



Others

Config File

(Encrypted)

Facial Debug Enabled □

Parameter Set-up:

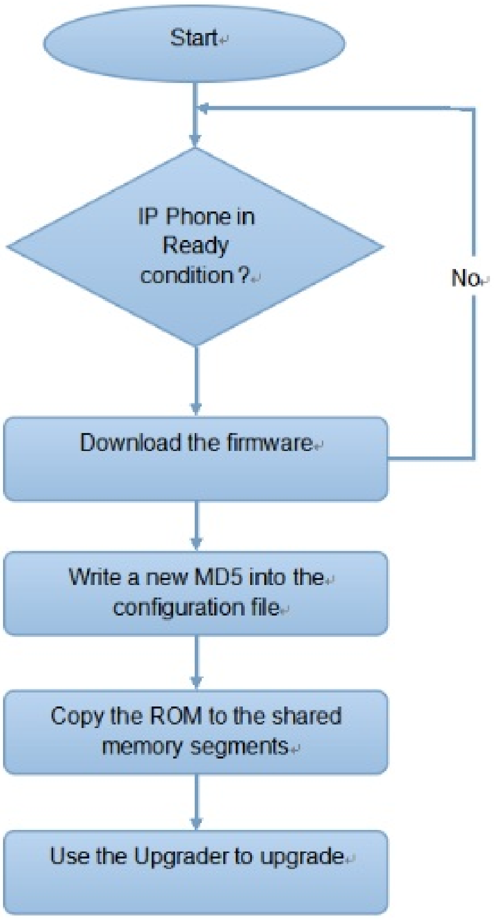
- **Facial Debug Enabled**: enable it for facial recognition debugging.

Auto-provisioning via Configuration File

Configurations and upgrading on A05 series access control terminal can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the access control terminal.

Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade devices in batch via third party servers. **DHCP, PNP, TFTP, FTP,** and **HTTPS** are the protocols used by the Akuvox intercom devices to access the URL of the address of the third-party server which stores configuration files and firmware, which will then be used to update the firmware and the corresponding parameters on the access control terminal.


Start
IP Phone in Ready condition ?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments
Use the Upgrader to upgrade

Configuration Files for Auto-provisioning

Configuration files have two formats for auto-provisioning. one is the general configuration files used for general provisioning and another one is MAC-based configuration provisioning.

The difference between the two types of configuration files is shown below:

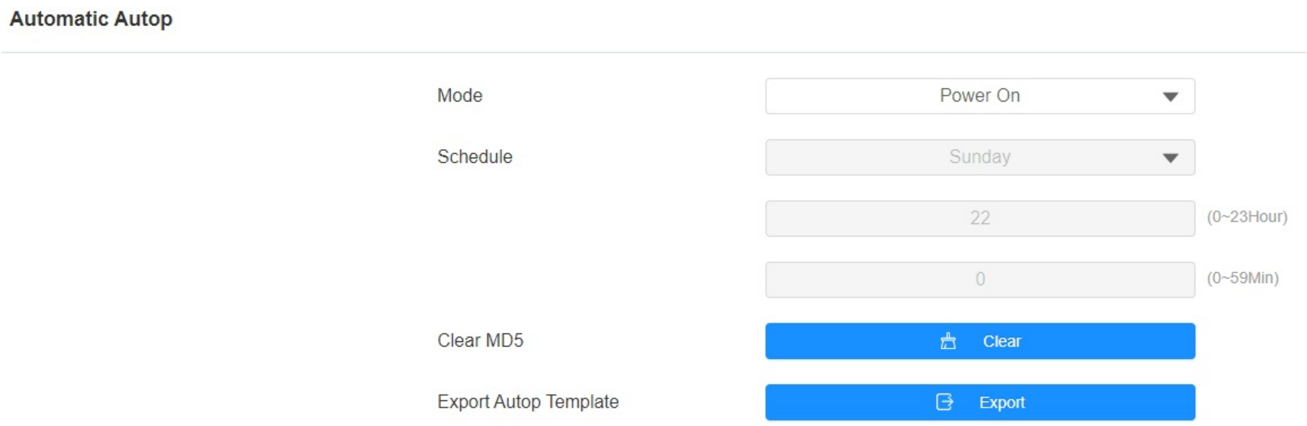
- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example: r000000000083.cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

AutoP Schedule

Akuvox provides you with different Autop methods that enable the access control terminal to perform provisioning for itself at a specific time according to your schedule. To configure the configuration on web **System > Auto Provisioning > Automatic Autop** interface.



Automatic Autop

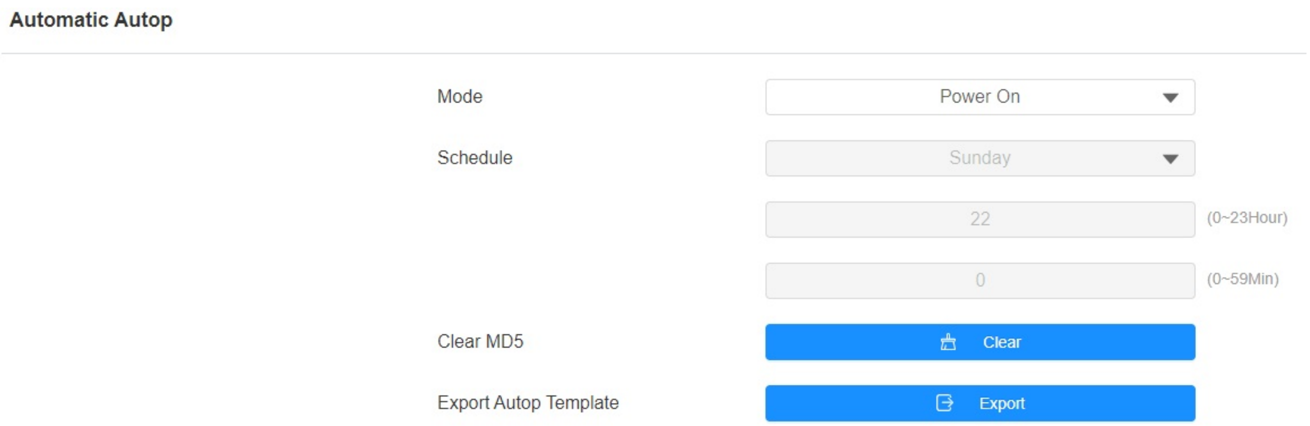
Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

Parameter Set-up:

- **Power On:** select **Power on** if you want the device to perform Autop every time it boots up.
- **Repeatedly:** select **Repeatedly** if you want the device to perform autop according to the schedule you set up.
- **Power On + Repeatedly:** select **Power On + Repeatedly** if you want to combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
- **Hourly Repeat:** select **Hourly Repeat** if you want the device to perform Autop every hour.

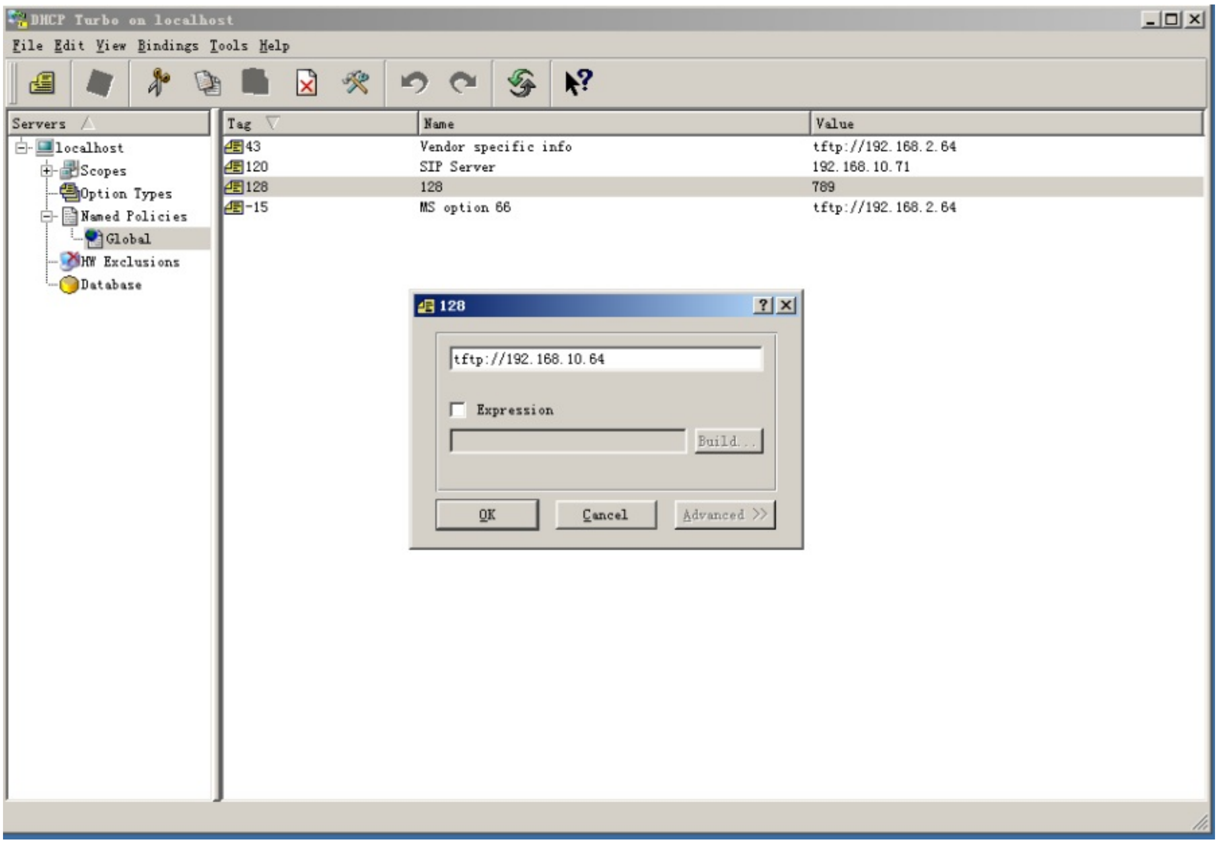
DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option code (ranging from 128-255), you are required to configure DHCP Custom Option on the web interface. To set up DHCP AutoP with **Custom Option** and **Power on** mode, on web **System > Auto Provisioning > Automatic Autop** interface. Click **Export** tab in Export Autop Template to export the Autop template. Then set up DHCP Option on DHCP server.



Automatic Autop

Mode	Power On	
Schedule	Sunday	
	22	(0~23Hour)
	0	(0~59Min)
Clear MD5	Clear	
Export Autop Template	Export	



Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

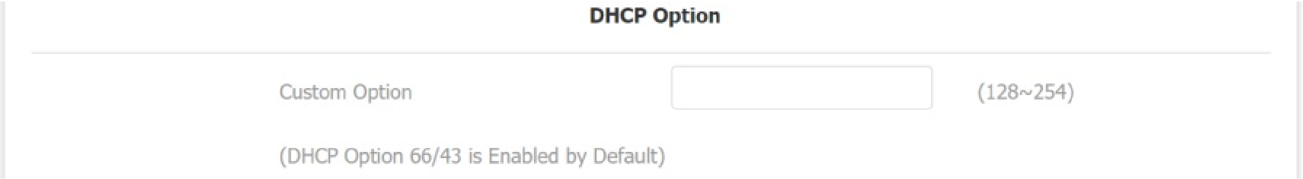
128

tftp://192.168.10.64

□ Expression

Note

- The custom Option type must be a string. The value is the URL of TFTP server.



DHCP Option

Custom Option		(128~254)

(DHCP Option 66/43 is Enabled by Default)

Parameter Set-up:

- **Custom Option**: enter the DHCP code that matched with the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.

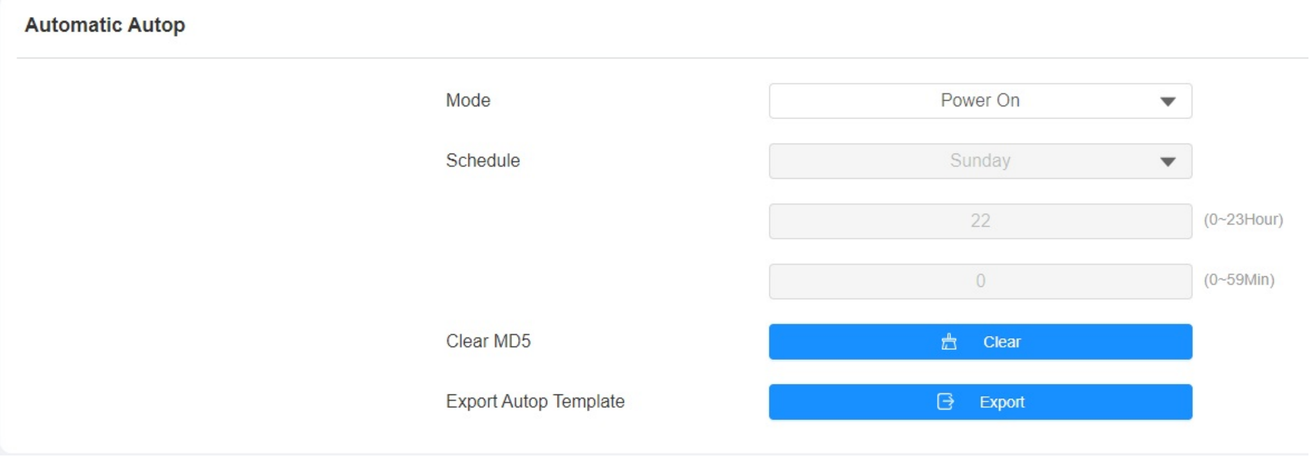
- **DHCP Option 66:** If none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.
- **DHCP Option 43:** If the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

Note

- The general configuration file for the in-batch provisioning is with the format "**r0000000000xx.cfg**", taking A05 as an example, "**r000000000105.cfg**" (10 zeros in total). While the MAC-based configuration file for the specific device provisioning is with the format, MAC_Address of the device.cfg, for example "**0C110504AE5B.cfg.**"

Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the access control terminal will perform the auto provisioning at a specific time according to the autop schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration. Download the Autop template on **System > Auto Provisioning > Automatic Autop,** and set up Autop server on **System > Auto Provisioning > Automatic Autop** interface.



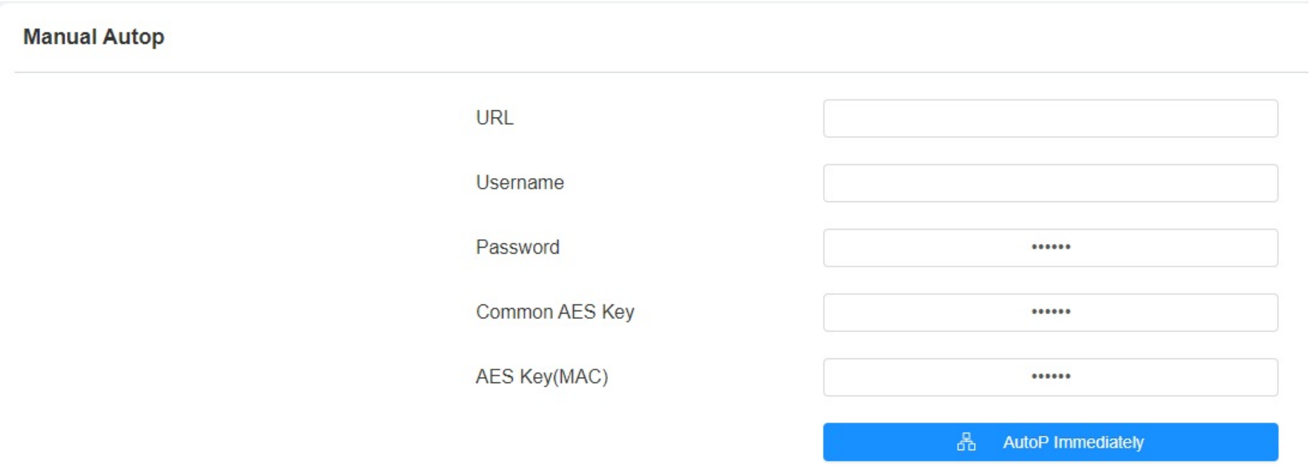
Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)



Manual Autop

URL	
Username	
Password	••••••
Common AES Key	••••••
AES Key(MAC)	••••••

Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
- **User Name**: set up a user name if the server needs a user name to be accessed otherwise leave it blank.
- **Password**: set up a password if the server needs a password to be accessed otherwise leave it blank.
- **Common AES Key**: set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

- AES is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

Note

Server Address format:

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
- ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/ (use the default port 80)
- http://192.168.0.19:8080/ (use other ports, such as 8080)
- HTTPS: https://192.168.0.19/ (use the default port 443)

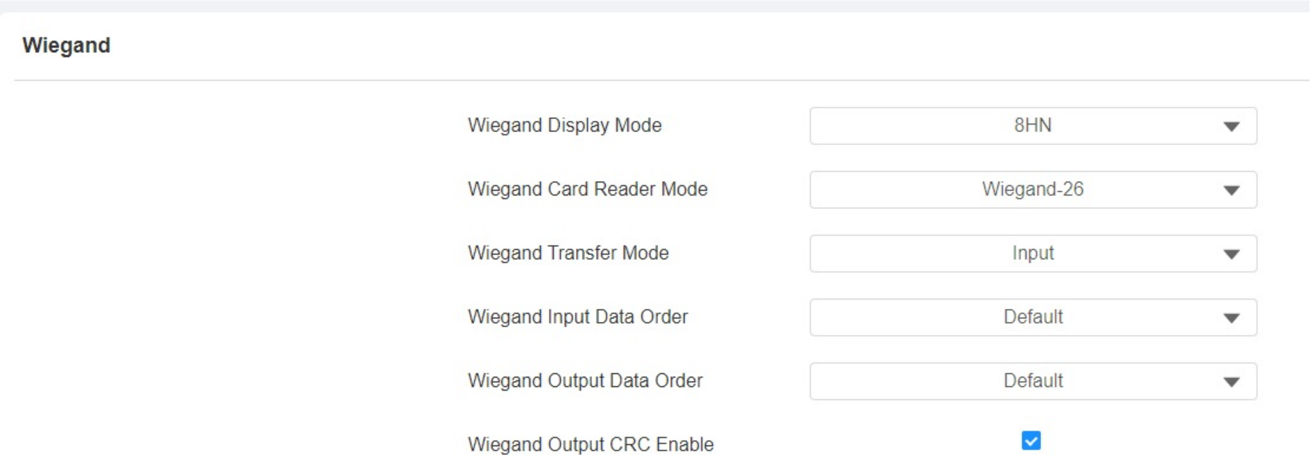
Note

- **Akuvox does not provide user specified server.**
- **Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.**

Integration with Third Party Device

Integration via Wiegand

If you want to integrate the A05 series access control terminal with the third-party devices via Wiegand, you can configure the Wiegand on the web **Device > Wiegand > Wiegand** interface.



Wiegand

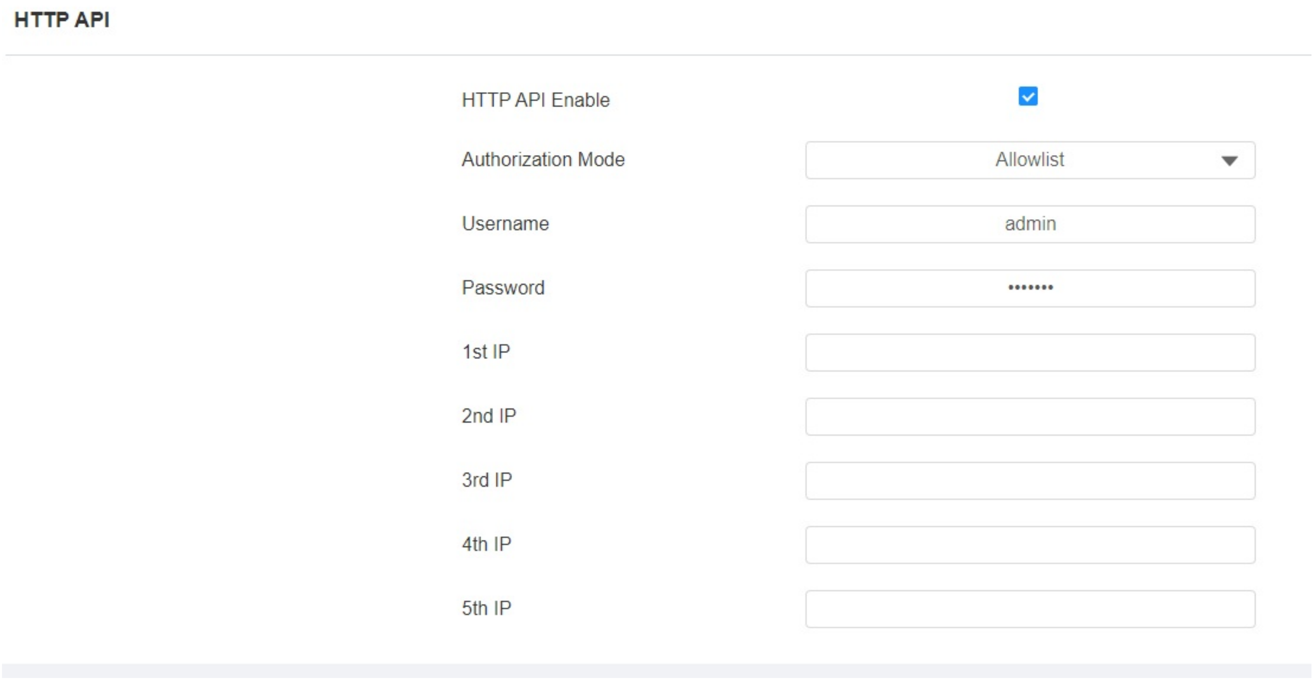
Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Wiegand-26
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Default
Wiegand Output Data Order	Default
Wiegand Output CRC Enable	☑

Parameter Set-up:

- **Wiegand Display Mode**: select Wigand Card code format among **8H10D**; **6H3D5D**; **6H8D**; **8HN**; **8HR**; **RAW**.
- **Wiegand Card Reader Mode:** set the Wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **and Wiegand 58**. The transmission format should be identical between the access control terminal and the device to be integrated.
- **Wiegand Transfer Mode:** set the transfer mode between **Input** or **Output** if the access control terminal is used as a receiver, then set it as Input for the access control terminal and vice versa.
- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Normal** and **Reversed** if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Normal** and **Reversed** if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output CRC:** tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.

Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third party device with the Akuvox intercom device. You can configure the HTTP API function on the web **Setting > HTTP API** interface for the integration.



HTTP API

HTTP API Enable ☑

Authorization Mode: Allowlist

Username: admin

Password: •••••••

1st IP

2nd IP

3rd IP

4th IP

5th IP

Parameter Set-up:

- **HTTP API Enable** enable or disable the HTTP API function for third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned to HTTP 403 forbidden status.
- **Authorization Mode:** select among four options: **None, WhiteList, Basic, Digest** for authorization type, which will be explained in detail in the following chart.
- **Username:** enter the user name when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **Password:** enter the password when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **1st IP- 5th IP:** enter the IP address of the third party devices when the WhiteList authorization is selected for the integration.

Lift Control

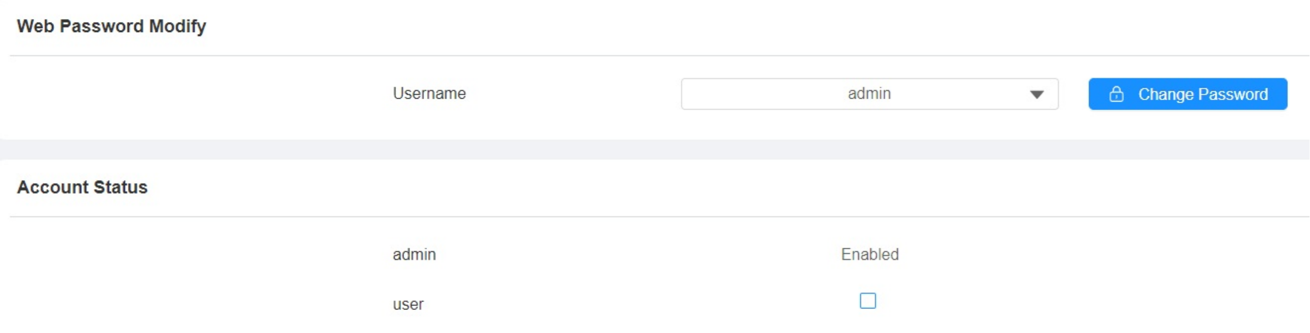
You can connect A05 with AKuvox EC32 lift controller and third-party lift controllers for the lift control. You can summon the lift to go down to the ground floor when you are granted various types of access methods on the door phone. To set up the lift control, go to **Device > Lift Control.**

NO.	Integration Mode	Description
1	**None**	If you select **None** then the RS485 integration will be disabled.
3	**Akuvox EC32**	Select **Akuvox EC32** if you want to connect the device with Akuvox EC32 lift controller.

Password Modification

Modify the Password

To change the default web password, navigate to **System > Upgrade > Web Password Modify.** Select **admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password. You can also disable User account permission to log in to the web.



Web Password Modify

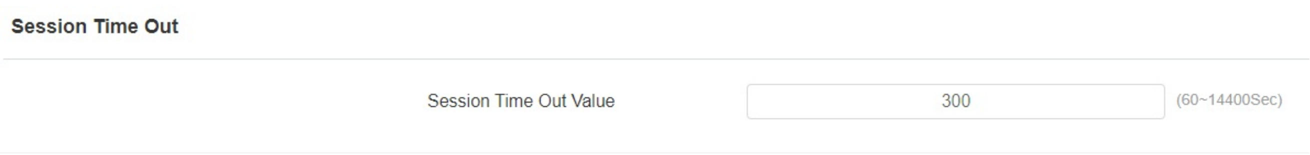
Username	admin	Change Password

Account Status

admin	Enabled
user	□

Web Interface Automatic Log-out

You can set up the web interface automatic log-out timing, requiring re-login by entering the username and the password for security purpose. To set it up, go to **System** > **Security > Session Time Out** interface.



Session Time Out

Session Time Out Value	300	(60~14400Sec)

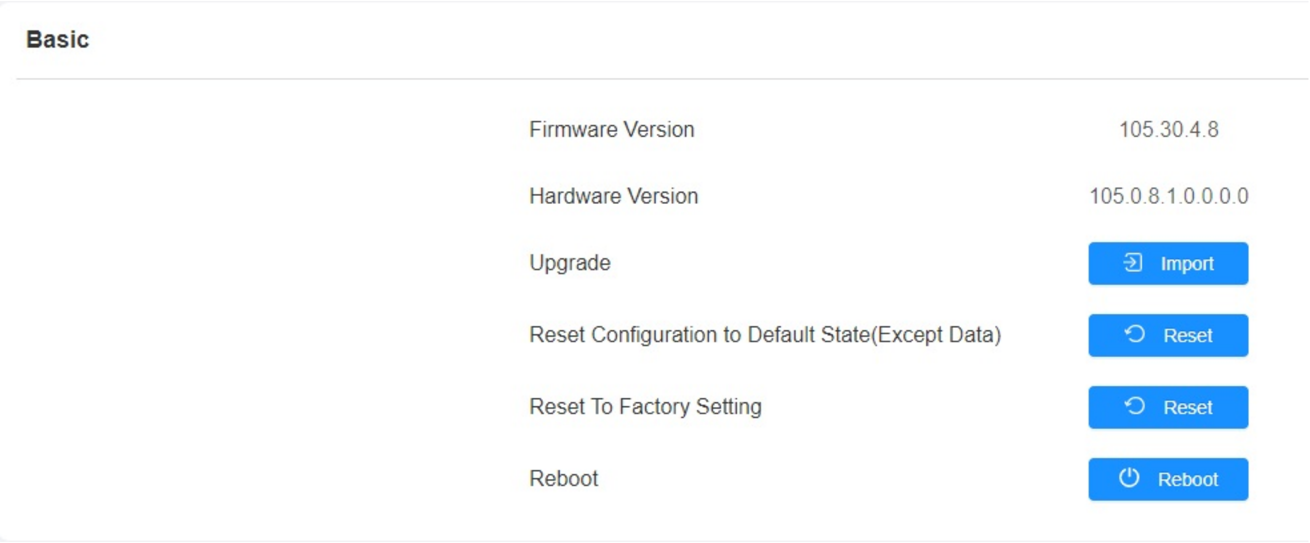
Parameters Set-up:

- **Session Time Out Value:** set the automatic timeout. For example, if you set it as 500, then the web page will be automatically logged out if the web page is left with no operation for 500 seconds. The default is 300 seconds.

System Reboot and Reset

Reboot

If you want to restart the device, you can operate it on the device web **System > Upgrade > Basic** interface as well. Moreover, you can set up a schedule for the device to be restarted.



Basic

Firmware Version 105.30.4.8

Hardware Version 105.0.8.1.0.0.0.0

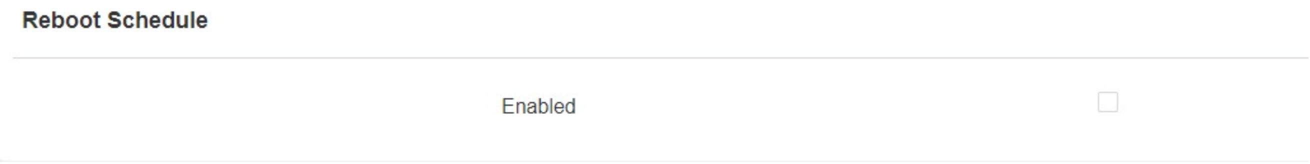
Upgrade

Reset Configuration to Default State(Except Data)

Reset To Factory Setting

Reboot

To set up the device restart schedule on web **System > Auto Provisioning > Reboot Schedule** interface.

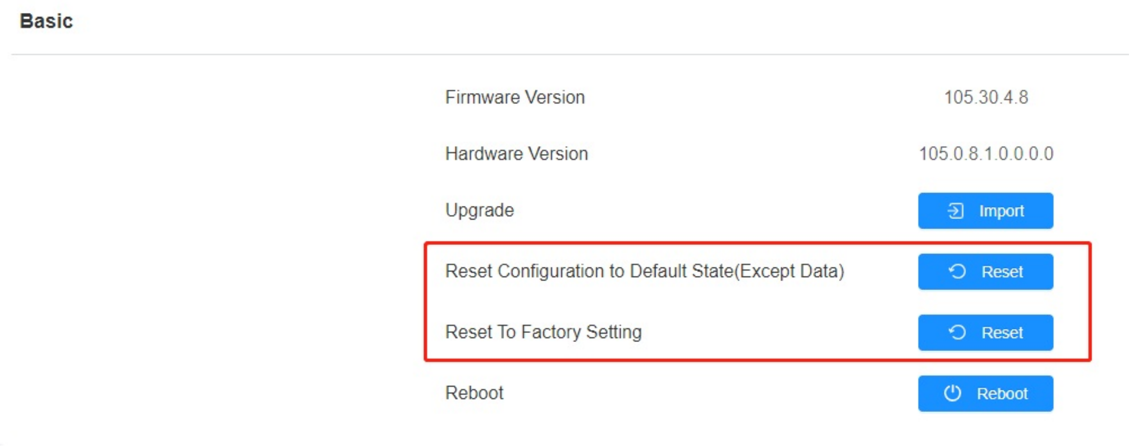


Reboot Schedule

Enabled □

Reset

You can select **Reset To Factory Setting** if you want to reset the device (deleting both configuration data and user data such as RF cards, face data, and so on). Or, select **Reset Configuration to Default State (Except Data) Reset**, if you want to reset the device (retaining the user data). To reset the device, go to **System > Upgrade.**



Basic

Firmware Version 105.30.4.8

Hardware Version 105.0.8.1.0.0.0.0

Upgrade

Reset Configuration to Default State(Except Data)

Reset To Factory Setting

Reboot

Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatic Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation μ-Law

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation μ-Law

PCAP: Packet Capture

PNP: Plug and Play

RFID: Radio Frequency Identification

RTP: Real-time Transport Protocol

RTSP: Real Time Streaming Protocol

MPEG: Moving Picture Experts Group

MWI: Message Waiting Indicator

NO: Normal Opened

NC: Normal Connected

NTP: Network Time Protocol

NAT: Network Address Translation

NVR: Network Video Recorder

ONVIF: Open Network Video Interface Forum

SIP: Session Initiation Protocol

SNMP: Simple Network Management Protocol

STUN: Session Traversal Utilities for NAT

SNMP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

WG: Wiegand

FAQ

Q1: How to obtain the IP address of R2X?

A1: ✔ For devices with a single button - E21/ R20/ R23/ R26:

While E21/ R20/ R23/ R26 power up normally, hold the call button for 5 seconds after the statue LED turns blue and it will enter into IP announcement mode. In announcement mode, the IP address will be announced repeatedly. Press the call button again to quit the announcement mode.

✔ For devices with multiple numeric keyboards - R27:

While R27 power up normally, press *2396# to enter the home screen and press 1 to go to the System Information screen to check the IP address.

✔ For devices with touch screen - X915/R29:

While it powers up normally, in the dial interface, press 9999, Dial key, 3888, and OK to enter the system setting screen. Go to the info screen to check the IP address.

✔Common method:

Using Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: Do Akuvox devices support opus codec?

A2: For now, only Akuvox Android video IP phone R48G can support Opus audio codec.

Q3: What is the supported temperature range for the Akuvox door phone?

A3: R20/E21/R26/R23/Standard R27/Standard X915 – 14° to 112°F (-10° to 45°C)

R27/X915 with heating supporting — 40 degrees

R28 – (-40°C~55°C)

Indoor monitor – 14° to 112°F (-10° to 45°C)

IP Phone – 32º~104ºF(0~40ºC)

Q4: Do Akuvox devices support Modbus protocol?

A4: No.

Q5：Failure in importing the X915 face data to another X915 using the exported face data.

A5：Please confirm the following steps：

The import format is zip;

After you export, you need to unzip the .tgz folder, then make the unzipped folder into .zip again.

Q6: Which version of ONVIF do R20 and X915 support?

A6: Onvif 18.04 profiles

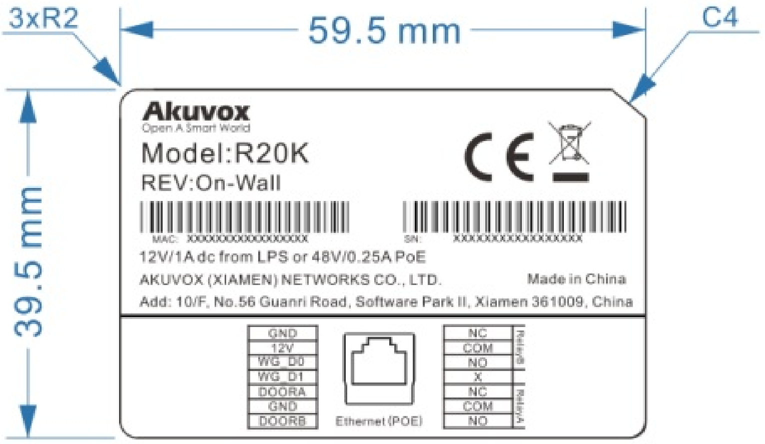
Q7: Do door phones support these card types? Prox, Legacy iClass, iClassSE, HID Mifare, HID DESFire, HID SEOS.

A7: Sorry, they are not supported. They need to be implemented via hardware modifications.

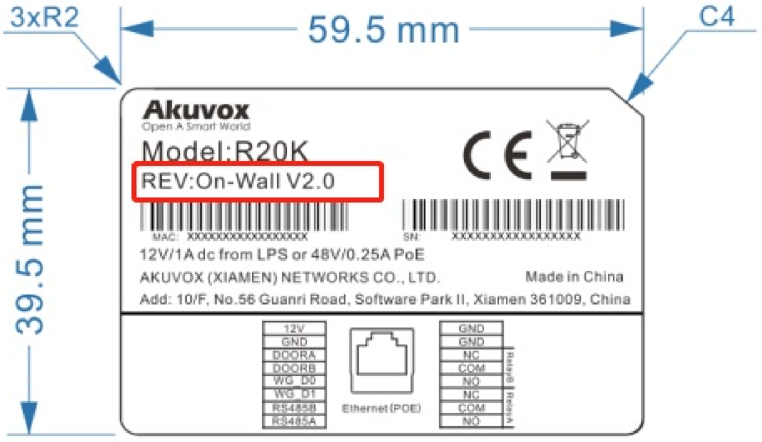
Q8: How to confirm whether my device is hardware version 1 or hardware version 2?

A8: 1.Label

- **Hardware version 1**



- **Hardware version 2**



- **Firmware Version**

The firmware is different between hardware version1 and hardware version 2.

Go to Web-Status -Firmware Version.

20.X.X.X is hardware version 1.

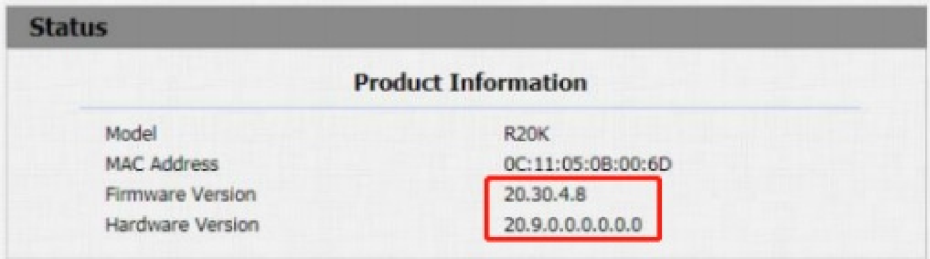
220.X.X.X is hardware version 2.

- **Hardware version**

The firmware is different between hardware version1 and hardware version 2.

Go to Web-Status -Firmware Version.

If the hardware version is 220.x, then the device is hardware version 2.



Status

Product Information

Model	R20K
MAC Address	0C:11:05:0B:00:6D
Firmware Version	20.30.4.8
Hardware Version	20.9.0.0.0.0.0.0

Contact Us

For more information about the product, please visit us at www.akuvox.com or feel free to contact us by

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

Telephone: +86-592-2133061 ext.7694/8162

We highly appreciate your feedback about our products.