Akuvox
Open A Smart World

WWW.AKUVOX.COM

A05 ACCESS CONTROL TERMINAL

Administrator Guide

Version: 1.0 | Date: Jan.2021

About This Manual

Thank you for choosing Akuvox A05 series access control terminal. This manual is intended for the administrators who need to properly configure the access control terminal. This manual applies to 105.30.1.17 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 firmwares.

Introduction of Icons and Symbols

Warning:

- **Always abide by this information in order to prevent the persons from injury.**

Caution:

- **Always abide by this information in order to prevent the damages to the device.**

Note:

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

Tip:

- **Useful information for the quick and efficient use of the device.**

Related Documentation

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

http://wiki.akuvox.com

Table of Contents

1. Product Overview

Akuvox A05 series is an 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, 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.

2. Change Log

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

3. 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
Wall Mounting Dimension	√
Wall Mounting Dimension	√
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

4. Installation

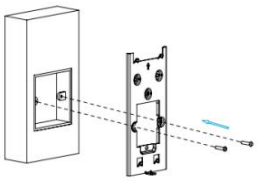
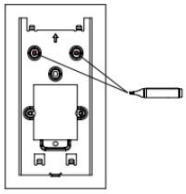
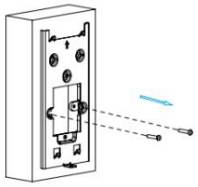
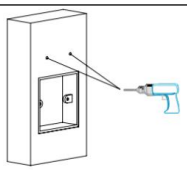
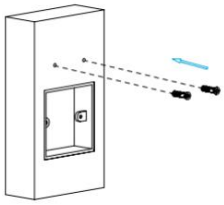
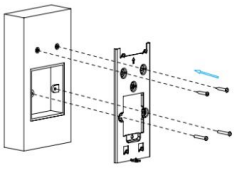
- **Universal Accessories**

No.	Accessories	Description	Quantity
1		A05	1
2		Wall-mounting bracket	1
3		Cable locking plate	1
4		Back cover	1
5		Rubber Plug	3
6		Allen Wrench	1
7		Torx Wrench	1
8		Plastic Wall Anchor	4
9		M3×6 Screw	4
10		M4×30 Screw	2
11		Torx Screw	1
12		M2.5×6 Screw	2
13		ST4×20 Screw	4

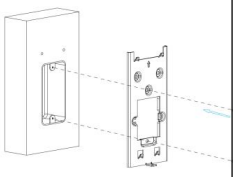
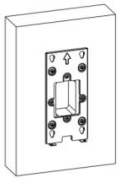
- **Digital Temperature Detector Accessories (Optional)**

No.	Accessories	Description	Quantity
1		Digital Forehead Temperature Detector	1
2		Digital Wrist Temperature Detector	1
3		M3x6 Screw	2
4		3×10.5 Screw	2

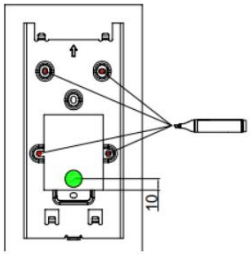
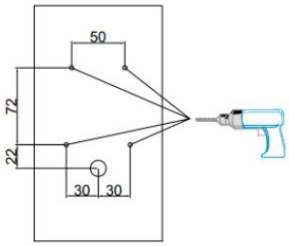
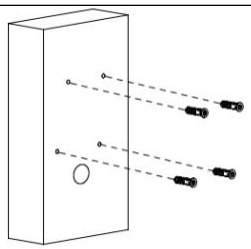
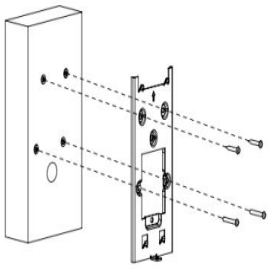
- **Wall-mounting bracket installation with 86x86 mm embedded junction box in the wall.**

Steps	Installation Picture	Installation Description
1		Fix the wall-mounting bracket on the embedded box with two M4x30 screws.
2		Mark the two positioning holes of the wall-mounting bracket on the wall.
3		Remove the two M4x30 screws and take off the wall-mounting bracket.
4		Use a hand drill with 5mm diameter bit to make two positioning holes with 5mm in depth in the marked positions.
5		Insert two plastic wall anchors into the two drilled holes.
6		Fix the wall-mounting bracket with two M4x30 screws and two ST4x20 screws.

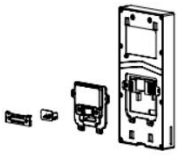
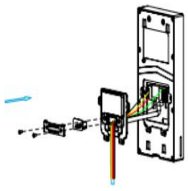
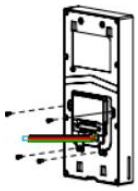
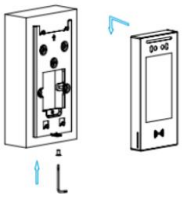
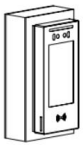
- **With 2x3 Inches Embedded Single-gang Box in the Wall**

Steps	Installation Picture	Installation Description
1		Fix the wall-mounting bracket on the single-gang junction box with the two M4x30 screws.
2		Finish the bracket installation.

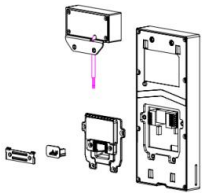
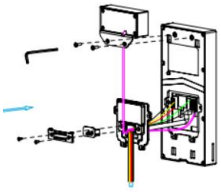
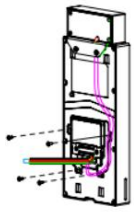
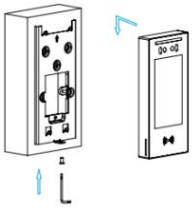
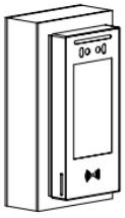
- **With Embedded Gang box in the Wall**

Steps	Installation Picture	Installation Description
1		According to the position of the cable, put the wall-mounting bracket closely on to the wall and mark the four positioning holes, while making sure that relative positions between wall-mounting bracket and wire hole are correct. **Note:** The positioning holes should be market in the center of the holes.
2		Take off the wall-mounting and drill the four marked positioning holes and the wire holes using 5mm hand drills.
3		Insert four plastic wall anchors into the holes.
4		Fix the wall-mounting bracket with four ST4x20 screws.

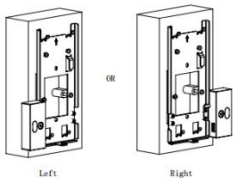
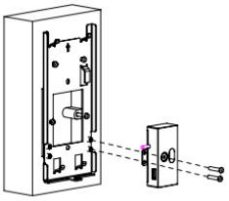
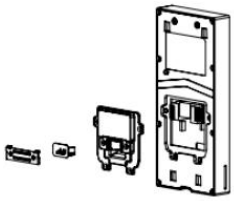
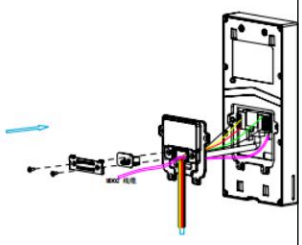
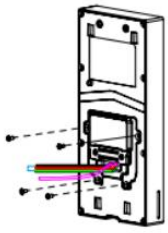
- **Device Installation without Digital Temperature Detector**

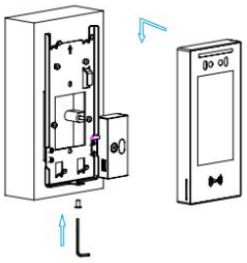
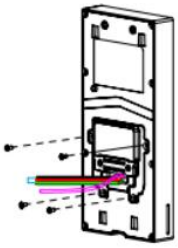
Steps	Installation Picture	Installation Description
1		Take out the device along with the back cover, cable locking plate , rubber plug and corresponding screws.
2		Lead the wires from the wall-mount bracket and the module through the square hole on the back cover, connecting them to the corresponding interface of the main board. Select a suitable size rubber plug to push all the cables into the back cover. Fix cable locking plate to the back cover with two M2.5x6 screws using the Allen wrench attached with.
3		Fasten the back cover with four M3x6 screws using the Allen wrench attached with.
4		Hang the device on to the square hanger on the wall mounting bracket, pull down the device to make it fall completely on to the square hanger on the wall-mounting bracket, then use the Torx Wrench attached with to tighten the device with the Torx screw.
5		Installation is completed.

- **Device Installation with Digital Forehead Temperature Detector**

Steps	Installation Picture	Installation Description
1		Take out the access control terminal and the digital forehead temperature detector and then take out back cover, cable locking plate and rubber plug.
2		Fasten the detector on to the nuts on the device's rear cover with two M3X10.5 screws using the Allen wrench attached with, and lead the wires from the wall-mount bracket and the detector through the square hole on the back cover, connecting them to the corresponding interface of the main board. And then select a suitable size rubber plug to push all the cables into the back cover. Fix cable locking plate to the back cover with two M2.5x6 screws using the Allen wrench attached with.
3		Fasten the back cover with four M3x6 screws using the Allen wrench attached with.
4		Hang the device on to the square hanger on the wall mounting bracket, pull down the device to make it fall completely on to the square hanger on the wall-mounting bracket, then use the Torx Wrench attached with to tighten the device with the Torx screw.
5		Installation is completed.

- **Device Installation with Digital Wrist Temperature Detector**

Steps	Installation Picture	Installation Description
1		Fix the the two holes of the detector onto the installation pins on the wall-bracket either on the left or right according to your preference.
2		Tighten the detector on to the inner threaded bolt with two M3x6 screw using the Allen wrench attached with in the same on both side.
3		Take out the device along with the back cover, cable locking plate , rubber plug and corresponding screws.
4		Fasten the module on to the nuts on the device’ s rear cover with two M3X6 screws using the Allen wrench attached with, then Lead the wires from the wall-mount bracket and the module through the square hole on the back cover, connecting them to the corresponding interface of the main board. And then Select a suitable size rubber plug to push all the cables into the back cover. Fix cable locking plate to the back cover with two M2.5x6 .
5		Fasten the back cover with four M2.5x6 screws.

6		Hang the device on to the square hanger on the wall mounting bracket, pull down the device to make it fall completely on to the square hanger on the wall-mounting bracket, then use the Allen Wrench attached with to tighten the device with two M3x6 screws.
7		Fasten the back cover with four M2.5x6 screws using the Allen wrench attached with.

5. Introduction to Configuration Menu

- **Status**: this sections gives you basic information such as product information, Network Information, and account information etc.

- **Network**: this section mainly deals with DHCP&Static IP setting, and device deployment etc.

- **Surveillance**: this section includes audio&video related settings such as Live stream, RTSP, ONVIF, MJPEG.

- **Access Control**: this section includes input type setting, relay setting, door access control in terms private PIN code, Facial recognition, RF card, and BLE setting as well log related configurations such as door log and temperature log.

- **Setting**: this second deals with time &language setting, security notification settings and door prompt text setting.

- **Upgrade**: this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, PCAP.

- **Security**: this section is for Password modification, tamper alarm, and web interface automatic-logout.

- **Device**: this section concerns LED light setting, ODSP Setting, screen saver setting, sound&volume setting and third-party integration in terms of integration via Wiegand, RS485.

- **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.

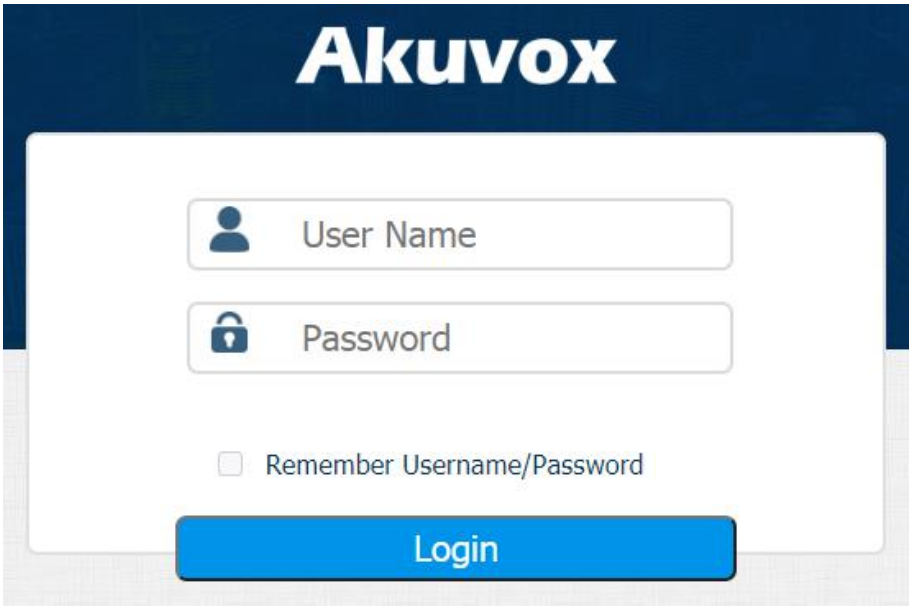
1. **SDMC**: SDMC is suitable for the management of Akuvox devices large communities, including access control, resident information, remote device control etc.,.
2. **Akuvox Upgrade tool**: Upgrade Akuvox devices in batch on a LAN (**Local**

Area Network).

3. **Akuvox PC Manager**: Distribute all configuration items in batch on a LAN.
4. **IP scanner**: it is used to search Akuvox device IP addresses on a LAN.
5. **FacePro**: Manage face data in batch for the access control terminal on a LAN.

6. Access the Device

1. Enter the IP address on the web browser.
2. Enter the **User Name** and **Password** of the device web interface.
3. Click **Login** tab to log in the web interface.



Tip:

- Please refer to the URL below for the IP scanner application instructions: http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s[]=ip&s[]=scanner

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.

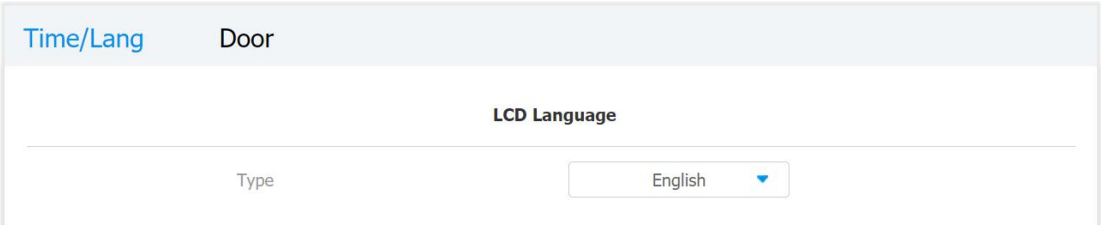
7. Time and Language Setting

7.1. Language Setting

When you first set up the device, you might need to set the language to your need. You can select the language display the device web interface.

To select the language, you can do as follows:

1. Click **Setting >Time/Lang > LCD Language**
2. Select the language you need and click **Submit** tab for validation.



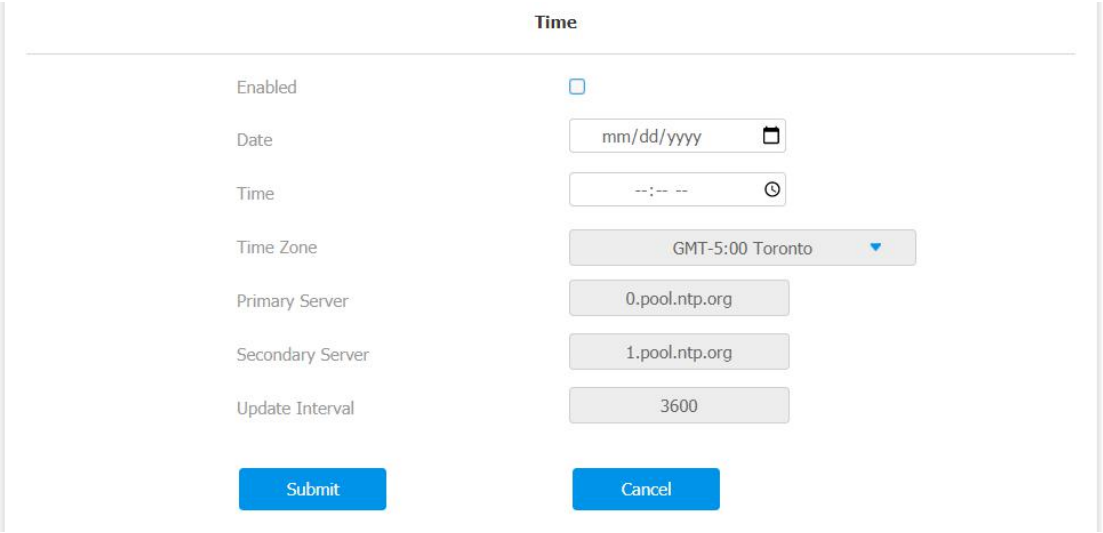
7.2. Time Setting

Time setting on the web interface allows you to set up time and date manually while allowing you to use 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.

To configure the time setting on the web interface, you can do as follows:

1. Click **Setting >Time/Lang > Time**
2. Untick the check box to allow you to set the time and date manually.

3. Tick the check box to enable the NTP server function that allows you to synchronize your time setting via NTP server.
4. Enter the NTP server you obtained in the field of the primary and secondary NTP **server**.
5. Set up the update timing via NTP server.
6. Click the **Submit** tab for the validation and the **Cancel** tab for the cancellation.



Parameter Set-up:

- **Time Zone:** select the specific time zone depending on where the device is used and then press **Confirm** tab for the confirmation. The default time zone is GMT+0.00.

- **Primary Server**: enter the primary NTP server you obtained in the **NTP Server** field.

- **Secondary Server**: enter the secondary NTP server you obtained in the **NTP Server** field to be used as a backup.

- **Update Interval**: set the automatic time update via NTP server.

Note:

- When the check box is unticked , the parameters related to NTP server will become uneditable.

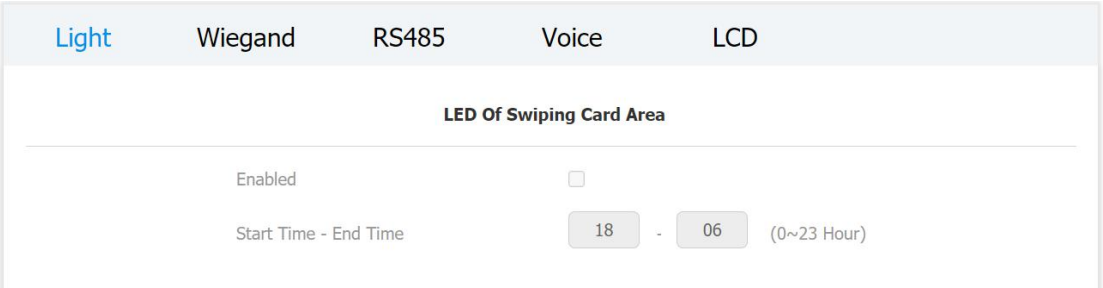
7.3. LED Setting

7.3.1. 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 to have the LED light on the card reader area to stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce the electrical power consumption.

To do the configuration, you can do as follows:

1. Click **Device > Light > LED of Swiping Card Area**
2. Set the parameter and click **Submit** tab for the validation.



Parameter set-up:

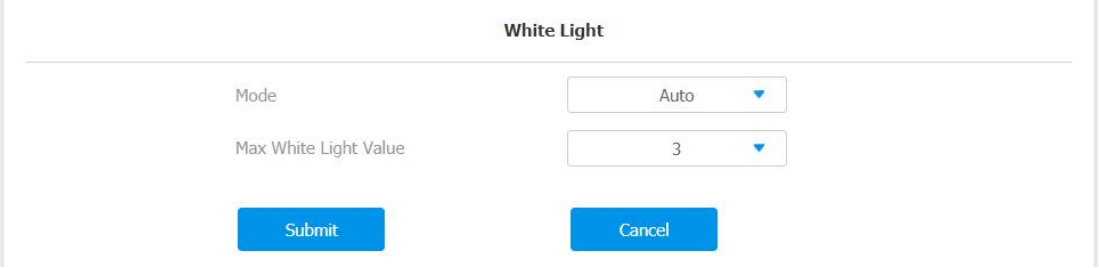
- **Enabled**: Tick the check box if want to enable the card reader LED lighting and vice versa.
- **Start Time - End Time (H)**: enter the time span for the LED lighting to be valid, e.g. if the time span is from **18-22** it means LED light will stay on during the time span from **6:00 pm** to **10:00**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

7.3.2. Configure LED White Light Setting

LED White light is used to reinforce the lighting for facial recognition as well as for the QR code access as needed in the dark environment. You can set the white light function properly on the device web interface.

To set up the white light function, you can do as follows:

1. Click **Device > Light > White Light**
2. Set up parameter properly.
3. Click **Submit** tab for the validation or cancel ta for the cancellation.



Parameter Set-up:

- **Mode**: select "**Auto**" or "**OFF**". If you select " **Auto**" then the white light will turn on for 5 minutes for facial recognition and QR code scan. And if you select "**Off**" then the white light will be turned off.

- **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.

7.4. 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.

7.4.1. Configure Screensaver

Await screen is mainly a function for the screen protection. You can make the device to go into idle status for a predefined time span when there is no operation on the device or no one is detected approaching.

Parameter set-up:

1. Click **Device > LCD > Standby Interface Display**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for the validation or cancel ta for the cancellation.

Parameter Set-up

- **ScreenSaver Mode:** tick the check box to enable the screen saver function.
- **Sleep:** set the screen saver start time range from "**5**" seconds to " **30**" minutes For example, if you set it as " 15 seconds" then the device will go into screen saver mode in 15 second when when there is no operation on the device or no one is detected approaching

7.5. Upload Screensaver

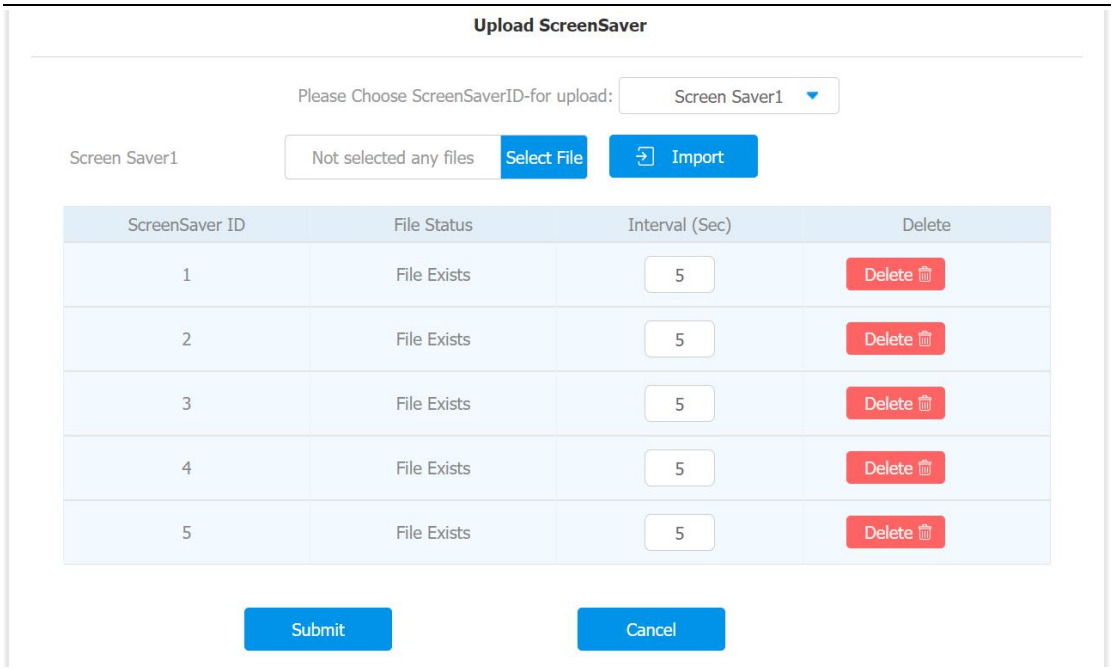
You can upload screensaver pictures separately or in batch to the device and to the device web interface for publicity purpose or for a greater visual experience.

To do so, you can do as follows:

1. Click **Device > LCD > Upload ScreenSaver**
2. Click **Select File** tab to choose the picture you want to upload to the device.
3. Click **Import** tab to start uploading the pictures (5 pictures maximum in total)
4. Click to designate the ID order number to the picture uploaded from image 1 to image 5 in the **Please Choose ScreenSaverID-for upload** field.
5. Set the display time of each individual picture you uploaded in **Interval (Sec.)** the display time range is from **"1-120"** seconds.
6. Click **Submit** tab or **Delete** tab for the confirmation or the cancellation of the pictures uploaded with the designated ID order number.

You are allowed to upload a maximum of 5 pictures, and each picture will be displayed in rotation according to the ID order with specific time duration (**Time Interval**) you set.

Please see the picture below:



Note:

- The pictures uploaded should be in **JPG format** with 2M pixel maximum.

7.6. Configure Access Screen Display Mode

You can select two types of access screen display mode on the home screen, namely, Default mode for facial recognition and QR code.

To do so, you can configure as follows:

1. Click **Device > LCD > Theme**
2. Set the mode to **Default** if you need to use facial recognition or set the mode to **QR code** if you need to use QR code for the door access
3. When in QR code mode, you can set QR code Recognition Interval.It ranges from 1 to 8 seconds.
4. Click **Submit** tab or **Delete** tab for the confirmation or the cancellation of theme modifications.

7.7. Volume and Tone Configuration

Volume and tone configuration in A05 access control terminal refers to Tamper alarm volume, Mic volume and open door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

7.7.1. Volume Configuration

You can configure the Mic volume according to your need for open door notification..More over, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

To set up the volumes on the device , you can do as follows:

1. Click **Device > Voice > Volume Control**
2. Set up Tamper alarm parameters according to your need.
3. Press Submit tab for the validation.

Parameter Set-up:

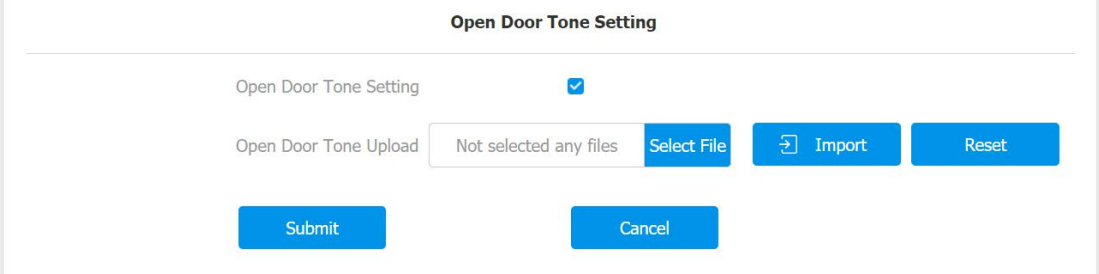
- **Ring Volume: s**et the ring volume from 0-15 according to your need. The default volume is "**8**".
- **Tamper Alarm Volume:** set the tamper alarm volume from 0-15 according to your need. The default volume is "**8**".

7.7.2. Upload Open Door Tone

You can upload the Open Door Tone on the device web interface.

To upload open door tone, you can do as follows:

1. Click **Device** >**Voice > Open Door Tone Setting**
2. Tick the check box in **Open Door Tone Setting** field to enable the open door time setting.
3. Click **Select File** tab to upload the .wav files you selected to the device.
4. Click **Import** tab to import the .wav files.
5. Click **Reset** tab if you want to reset the file uploaded.
6. Click the **Submit** tab for the validation or cancel ta for the cancellation.

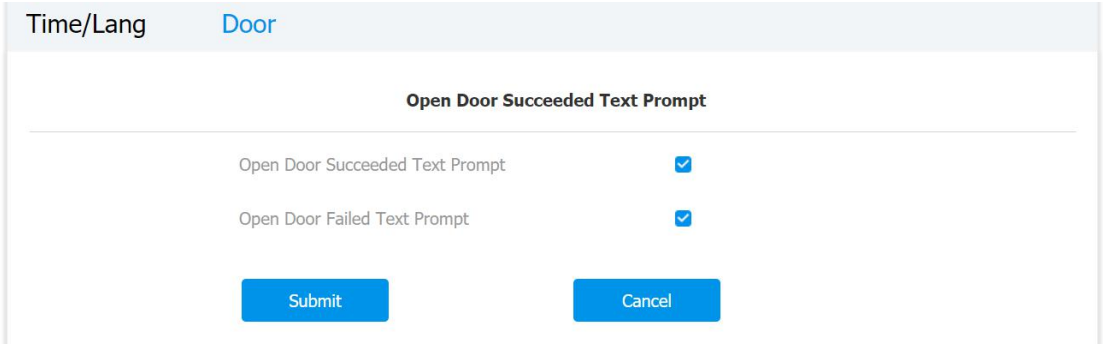


7.8. Configure Door Access Prompt Text

You can enable or disable the door access prompt to be shown on the access control terminal screen for door open failure and success.

To do the configuration, you can do as follows:

1. **Setting > Door > Open Door Succeeded Text Prompt**
2. Enable or disable the Prompt text for both open door failure and success.
3. Press **Submit** tab for the validation or cancel ta for the cancellation.



Parameter set-up:

- **Open Door Success:** Tick the check box if you want to see the text prompt after the door open success and vice versa.
- **Open Door Failed:** Tick the check box if you want to see the prompt words after the door open failure and vice versa.

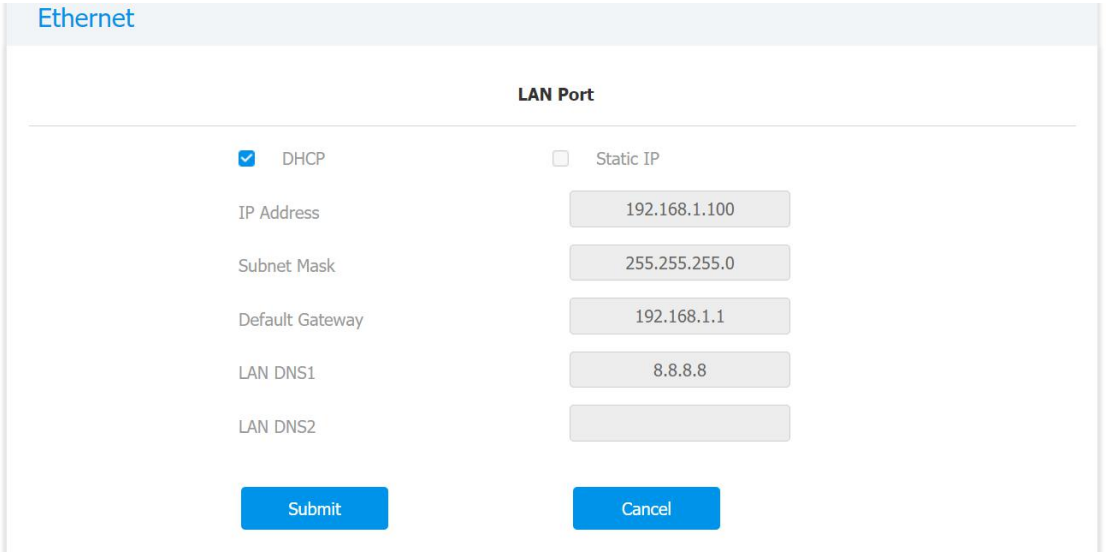
8. Network Setting

8.1. Configure Device Network

You can configure the default DHCP mode (**Dynamic Host Configuration Protocol**) and static IP connection. More over, you can set up IP address, Subnet Mask, Default Gateway, LAN DNS1 & LAN DNS2.

To configure the device network connection, you can do as follows:

1. Click **Network > Ethernet > LAN Port**
2. Select **DHCP** mode or **Static IP** mode by ticking off their respective check box.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



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 have to 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.

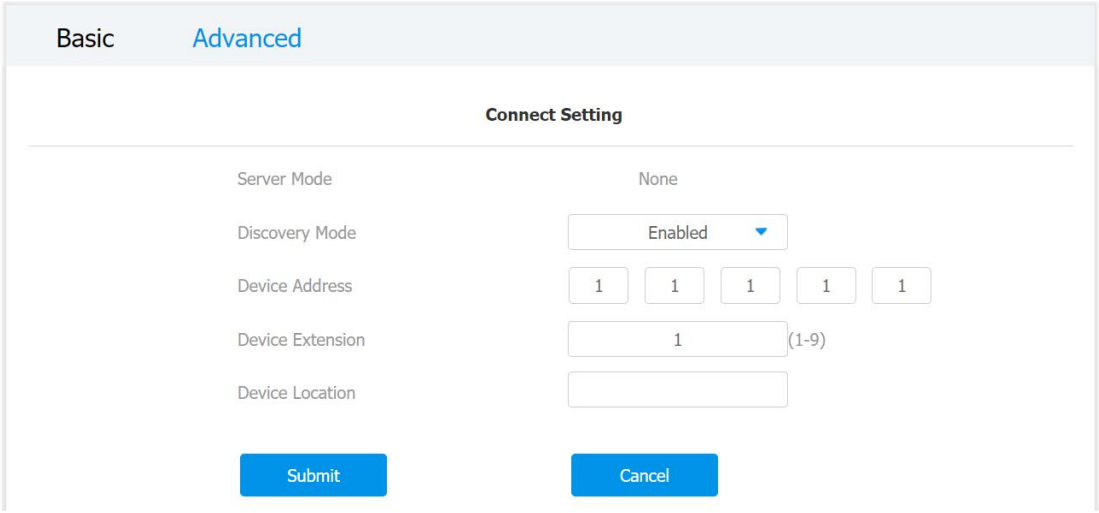
- **DNS1/DNS2**: set up DNS1/ DNS2 (**Domain Name Serve**r)according to your actual network environment. DNS1 is the primary DNS server address while the DNS2 is the secondary server address and the access control terminal connects to DNS2 server when the primary DNS server is unavailable .

8.2. 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 the device control and the convenience of the management.

To deploy the device in the network, you can do as follows:

1. Click **Network > Advanced > Connect Setting**
2. Set up correct parameters according to your actual application and deployment.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



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 **Cloud** 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, Room** in sequence.

- **Device extension**: enter the device extension number for the device you installed

- **Device Location**: enter the location in which the device is installed and used.

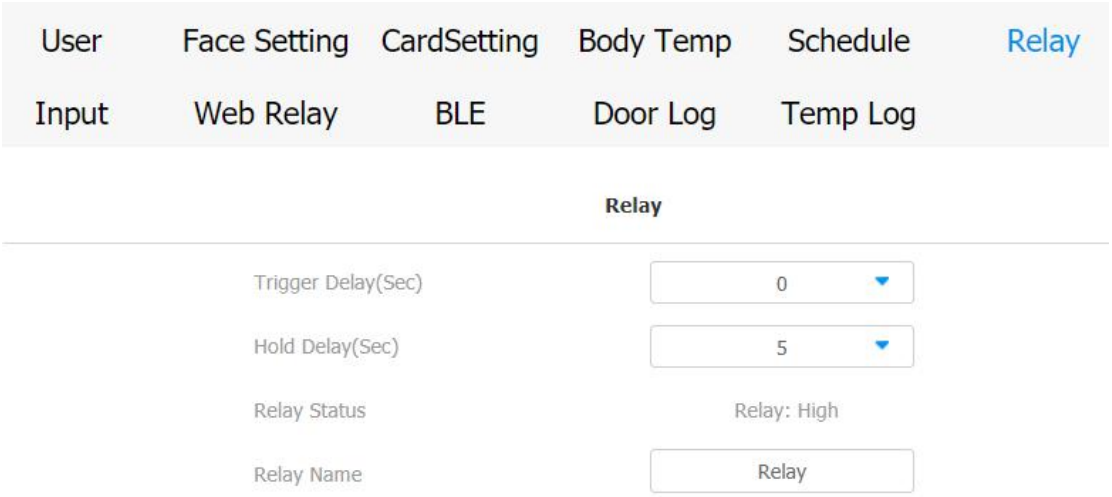
8.3. Relay Setting

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

Relay switch setting

To do the configuration, please do as follows:

1. Click **Access Control > Relay > Relay**
2. Set up relay related parameters properly according to your need.
3. Click **Submit** tab for the validation or cancel ta for the validation.



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 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 the convenience.

Note:

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

8.4. Web Relay Setting

In additional 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.

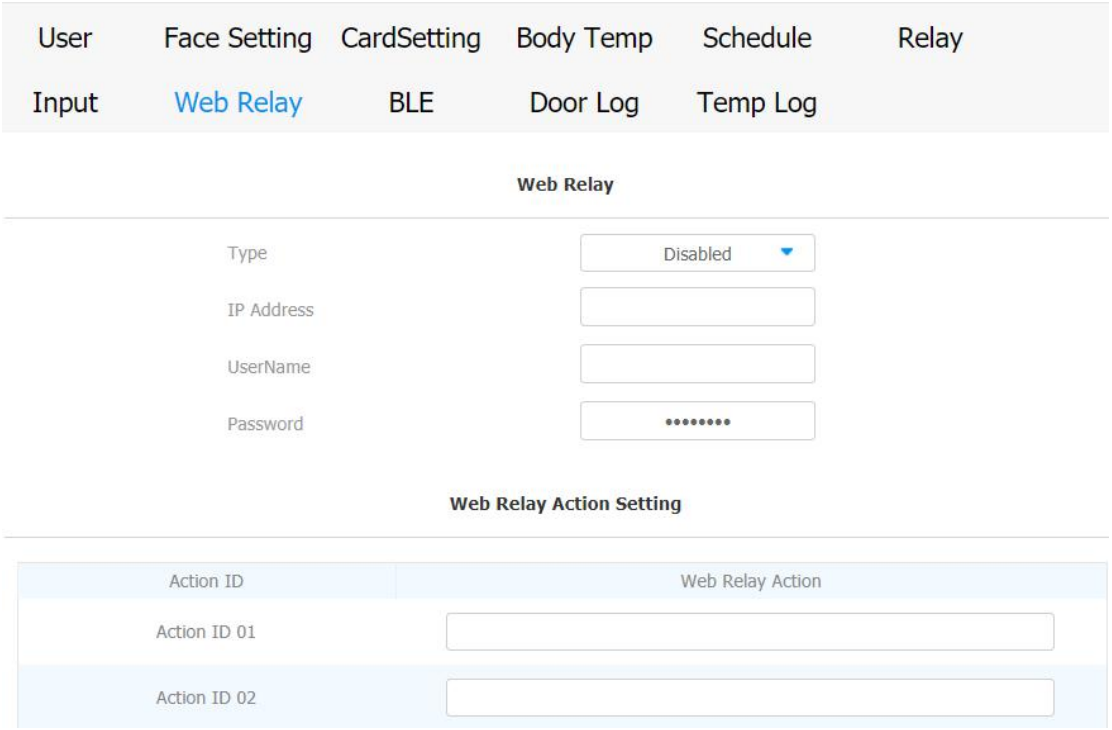
8.4.1. Configure Web Relay on the Web Interface

Web relay needs to 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 the door access via web relay.

To do the configuration , you can do as follows:

1. Click **Access Control > Web Relay**
2. Enter the parameters properly.

3. Go to the "**Web Relay Action Setting**" below in the same interface.
4. Configure the parameter properly.
5. Press the **Submit** tab for the validation or cancel ta for the cancellation.



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 we relay IP address provided by the web relay manufacturer.

- **User Name**: enter the User name provided by the web relay manufacturer.

- **Password:** enter the password provided by the web relay manufacturer.The passwords is authenticated via HTTP and you can define the passwords using "**http get**" in Action.

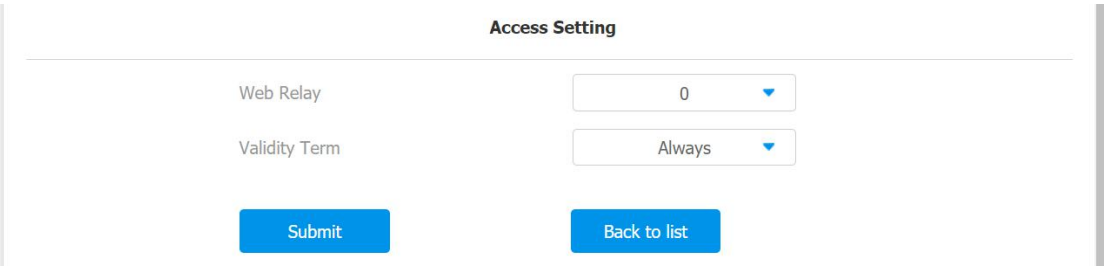
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.

  http://admin:admin@192.168.1.2/state.xml?relayState=2.

After the web relay is set up, you can configure the specific web relay to be triggered based on the relay location for the door access.

To configure the the web relay for the door access, you can do as follows:

1. Click **Access Control > User**
2. Click **Add** tab on the **User** Interface page.
3. Go to the **Access Setting** on the Bottom.
4. Click to select the specific web relay to be triggered at the corresponding location in the **Web Relay** field.
5. Click **Submit** tab for the validation.



9. Door Access Schedule Management

You are required to configure and make schedule for the user-based door access via RF card, Private PIN and Facial recognition.

9.1. Configure Door Access Schedule

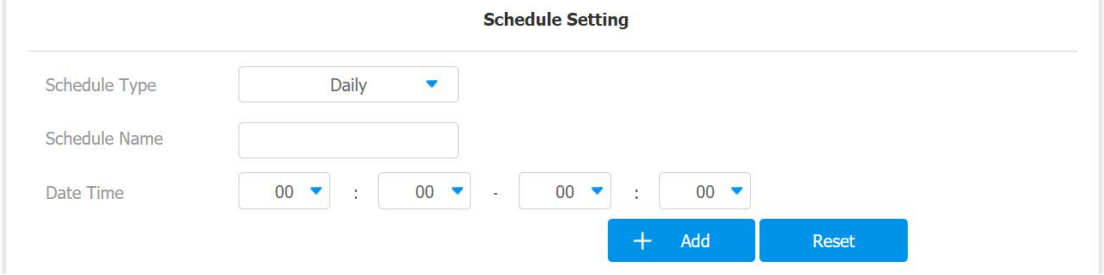
You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. More over, you can edit your door access schedule if needed.

9.1.1. Create Door Access Schedule

You can create the door access schedule on the daily or monthly basis and you can also create schedule that allows you to plan for a longer period of time in addition to running the door access schedule on the daily or monthly basis.

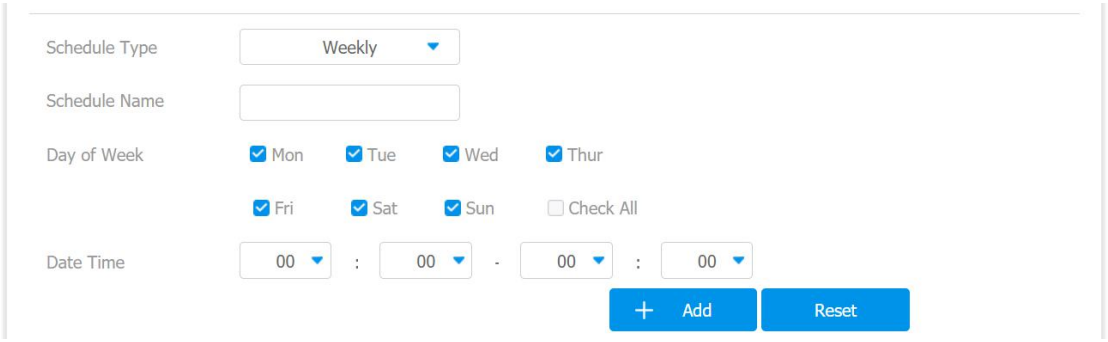
To create a daily schedule, you can do as follows:

1. Click **Access Control > Schedule Setting**
2. Click **Schedule Type** field to select "**Daily**" Type.
3. Enter the schedule name.
4. Set up the daily time schedule for the validity of the door access.
5. Click **Add** tab for the validation and **Reset** tab to clear the setting.



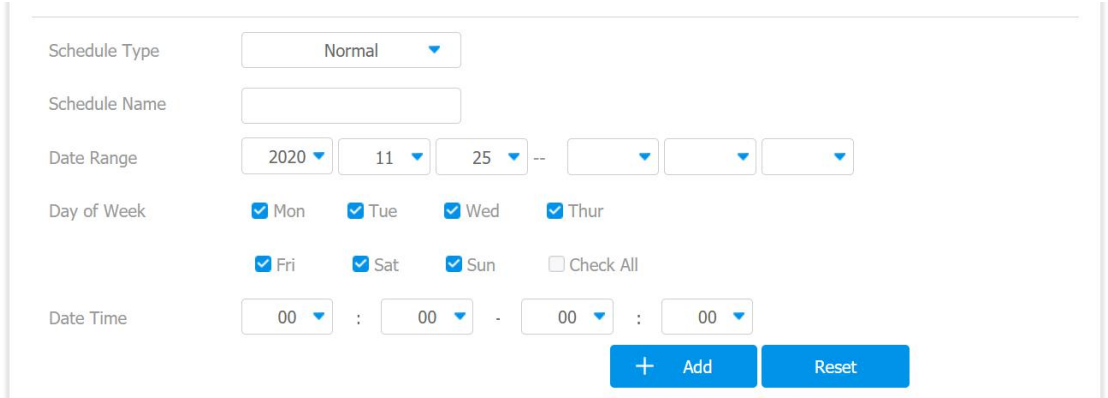
To create a weekly schedule, you can do as follows:

1. Click **Schedule Type** field to select "**Weekly**" Type.
2. Enter the schedule name according to your need.
3. Select the day (s) on which door access can be valid on monthly basis.
4. Set up the time schedule for the validity of the door access during a day.
5. Click **Add** tab for the validation and **Reset** tab to clear the setting.



To create a longer period schedule, you can do as follows:

1. Click **Schedule Type** field to select "**Normal**" Type.
2. Repeat the setting in the identical way as you do for the " Weekly" schedule.
3. Set the time period specifying year, month and date.
4. Click **Add** tab for the validation and **Reset** tab to clear the setting.

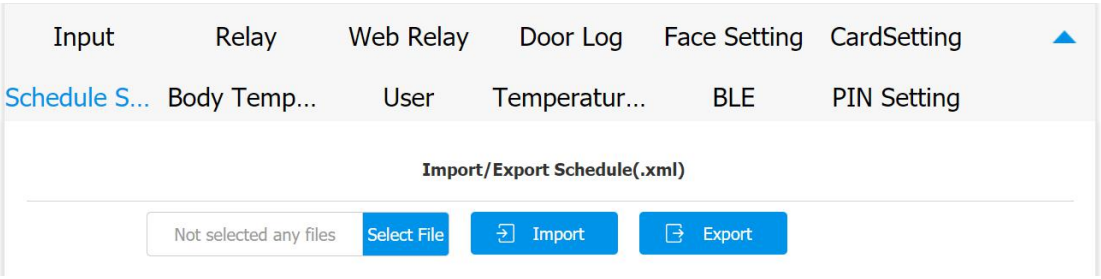


9.1.2.Import and Export Door Access Schedule

In addition to creating door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency.

To import and export the schedule, you can do as follows:

1. Click **Access Control > Schedule Setting> Import/Export Schedule(.xml)**
2. Click **Select file** Tab to upload your card data file.
3. Click **Import** tab to import the file to the device.
4. Click **Export tab** to export the file.



Note:

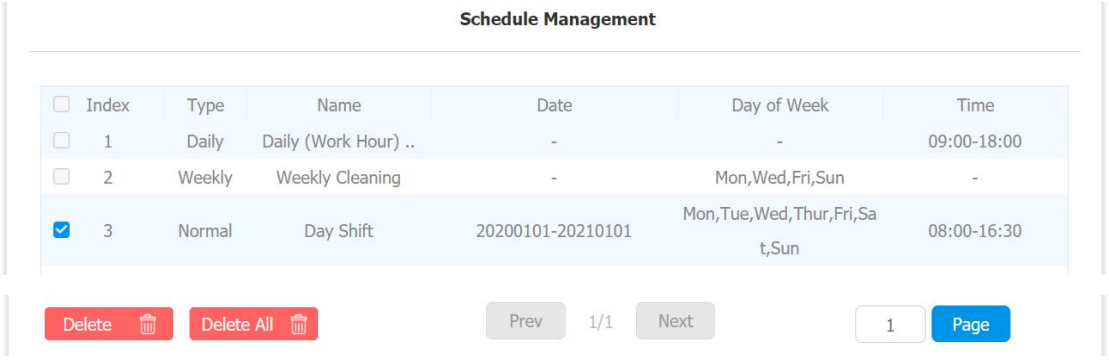
- It only supports .xml format file for importing and exporting the schedule.

9.1.3.Edit the Door Access Schedule

If you want to edit or delete your door access schedule you created, you can edit or delete the configured schedule separately or in batch on the web interface.

To edit or delete the schedule , you can do as follows:

1. Click **Access Control > Schedule Setting> Schedule Management**
2. Tick ☑ the schedule you wish to edit or delete .
3. Go to **Schedule Setting** section above in the same interface page.
4. Edit the schedule according to your need.
5. Click **Edit** tab for validation or **Reset** tab to go back to your previous setting



10. Door Unlock Configuration

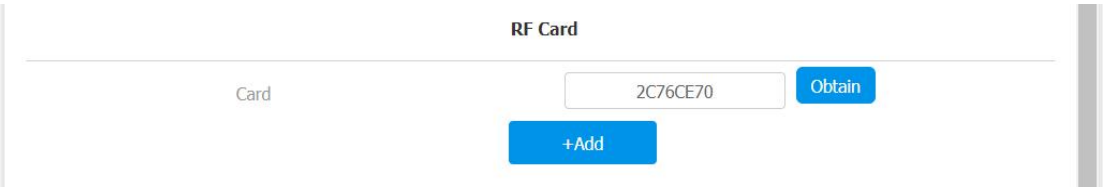
A05 series access control terminal offer you three types of door access via QR code code, RF card and Facial recognition. You can configure them on web interface. More over, you can import or exporting the configured files to maximize your RF card configuration efficiency.

10.1.Configure RF Card for Door Unlock

10.1.1. Configure RF Card on the Web Interface

To configure RF card , you can do as follows:

1. **Click Access Control > User**
2. Click the **Add** tab.
3. Go to **User Basic** section.
4. Enter the **user's name** and **floor number**.
5. Go to **RF Card** section.
6. Click and **Obtain** tab and place the card on the card reader area.



Note:

- Please refer to PIN code access schedule selection for the RF card user(s)-specific door access.

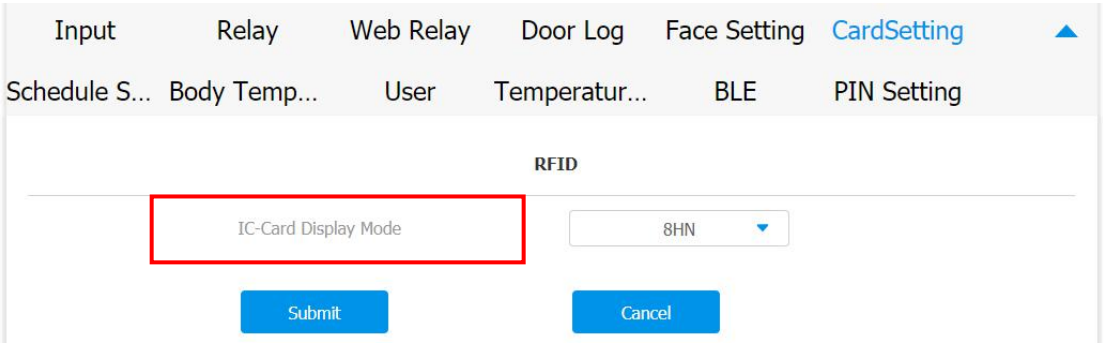
Note:

- RF card with 13.56 MHz and 125 KHz can be applicable to the access control terminal for the door access.

10.1.1.1. 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 with that applied in the third party system.

To select the RF card format, you can do as follows:



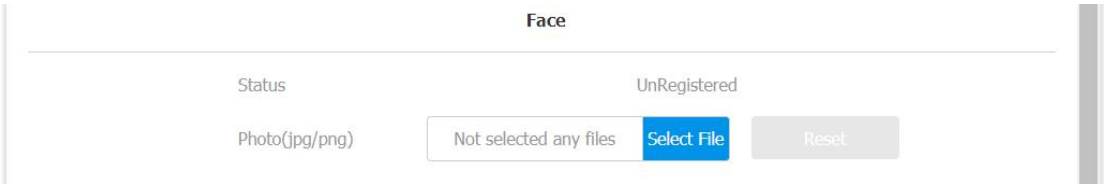
Parameter Set-up:

IC-Card Display Mode: select the card format for the **ID Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR.** The card code format is 8HN by default in the access control terminal.

10.1.2. Configure Facial Recognition on Web Interface

To configure PIN code , you can do as follows:

7. **Click Access Control > User**
1. Click the **Add** tab.
2. Go to **User Basic** section.
3. Enter the **user's name** and **floor number**
4. Click **Select File** tab to upload the picture from PC for facial recognition.
5. Click **Reset** tab if you want to cancel the picture.
6. Click **Submit** tab on the bottom for the validation.



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(jpg/png):** select the picture with jpg or png format to be uploaded to the device and press if you want to clear the picture uploaded.

Note:

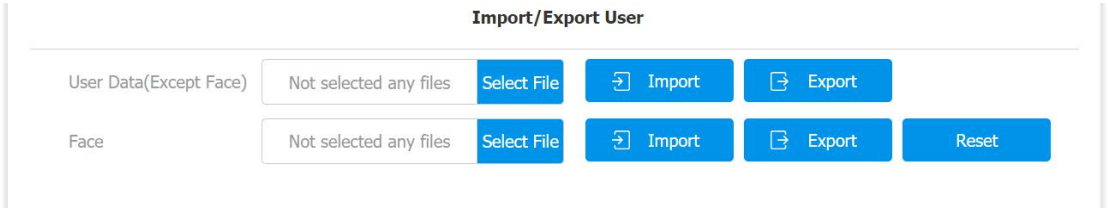
- Pictures to be uploaded should be in jpg or png format.

10.2. 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 import the configured door access files, you can do as follows:

1. Click **Access Control > User**
2. Click **Select File** tab in **User Data (except Face)** field to upload the configured file for the door access not inclusive of the access by facial recognition.
3. Click **Import** tab to start uploading the files and Export to export the file.
4. Click **Select File** tab in **Face** field to upload configured file for the door access by facial recognition.
5. Click **Import** tab to start uploading the files and Export to export the file.
6. Click **Reset** tab if your want to clear the configured file (facial recognition) you selected.



Note:

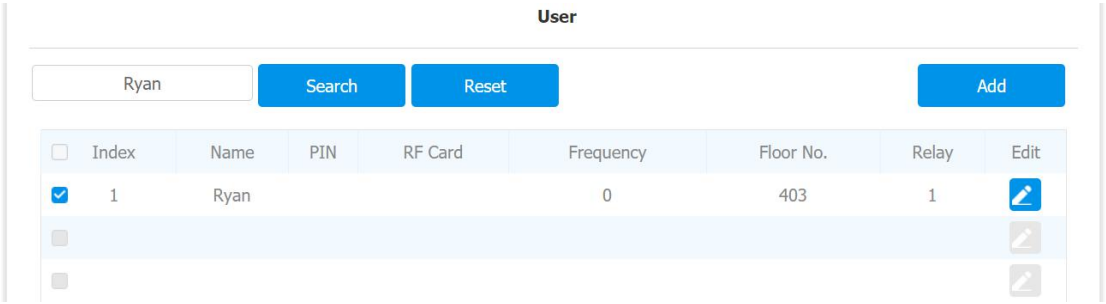
- Configured file for facial recognition and the other types of configured door access file are separated with different file forms.

10.3.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 interface.

To search and edit the user data, you can do as follows:

1. Click **Access Control > User**
2. Enter the search information in the **Search** field and press **Reset** tab if you want to clear the information entered.
3. Click **Edit** tab to add the user data.
4. Tick the check box of the specific user if you want to delete the user or ticket the the check box by the the **Index** to delete all the user data.

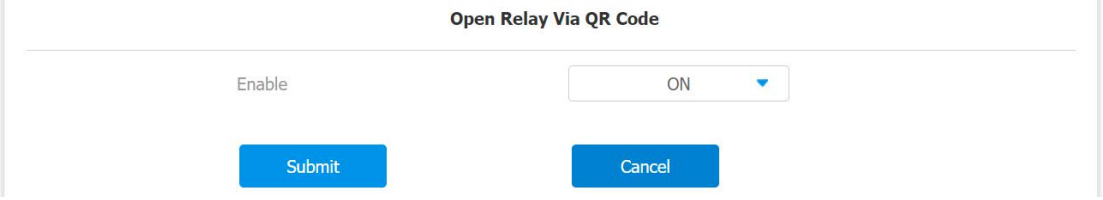


10.3.1. Unlock by QR Code

QR code is another option for door access. If you want to apply QR code access, you need to enable the QR code function.

To enable the QR code function , you can do as follows:

1. Click **Access Control > Relay > Open Relay via QR Code**
2. Enable the QR code function by clicking "**On**"in the **Enable** field.
3. Click **Submit** tab for validation or cancel ta for cancellation.



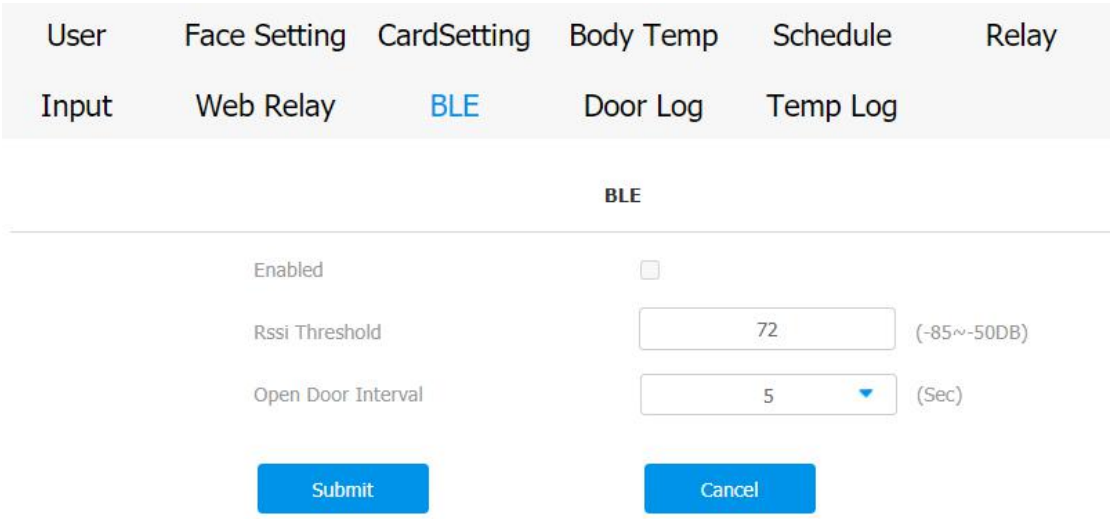
Note:

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

10.3.2. Unlock by Bluetooth

You can also gain the 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 the door access.

1. Click **Access Control > BLE > BLE**
2. Set up parameter according to your need.
3. Click on **Submit** tab for the validation or cancel ta for the cancellation.



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:** select the time interval between the every two Bluetooth door accesses.

10.3.3. Unlock by HTTP Command on Web Browser

You can unlock the door remotely without approaching the device physically for the door access by typing in the created the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access.

To do the configuration, you can do as follows:

1. Click **Access Control > Relay > Open Relay via HTTP**
2. Set up parameters properly.
3. Click **Submit** tab for the validation or cancel ta for the cancellation.

Parameter Set-up:

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

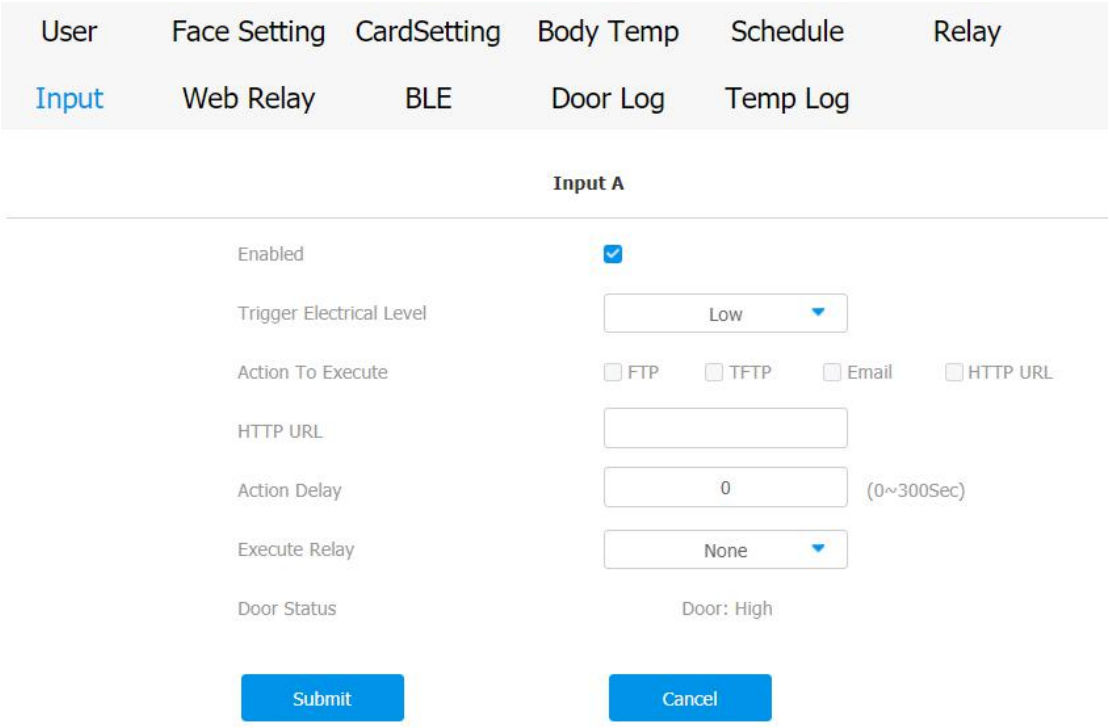
- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

10.3.4. 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 do the configuration, you can do as follows:

1. Click **Access Control > Input > Input**
2. Tick **Enabled** to enable the Input function.
3. Set up the parameters according to your need.
4. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



Parameter set-up:

- **Trigger Electrical Level:** select the trigger electrical level options between "**High**" and "L**ow**" according the actual operation on 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" sec. then the action will not triggered until 5 seconds after input status changed.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

10.3.5. Body Temperature Measurement for Door Access（Optional）

A05 series provide 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 measurement along with optional mask detection check before they are allowed for the door access.

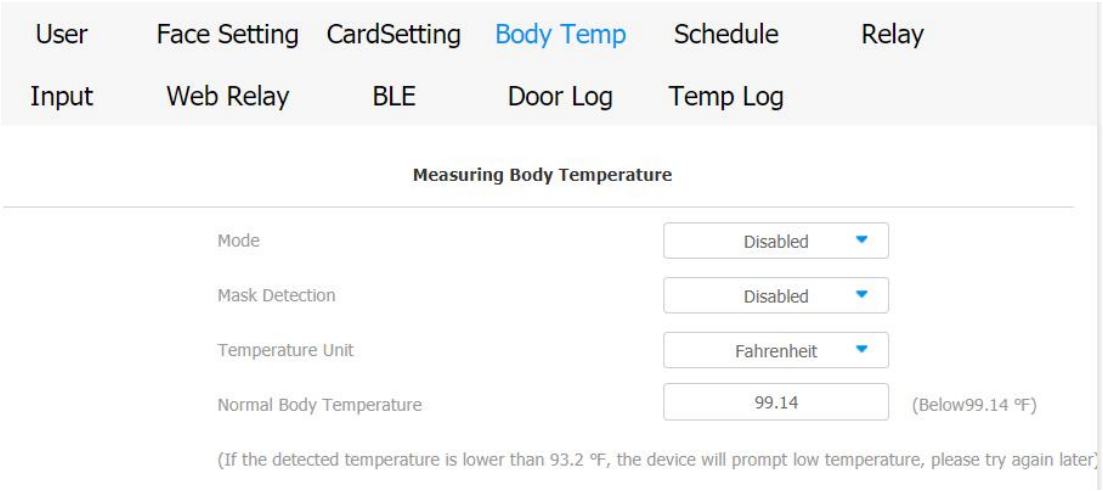
10.3.5.1. Body Temperature Measurement Configuration

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 do the configuration, you can do as follows:

1. Click **Access Control > Body Temperature > Measuring Body Temperature**
2. Set up parameters properly.
3. Set the schedule for the validity of the body temperature measurement.

4. Click on **Submit** tab for the validation or cancel ta for the cancellation.



Parameter set-up:

- **Mode**: select either "**Disabled"** Mode or "**Wrist**" Mode for temperature measurement according to your need. The device can be installed with digital forehead temperature detector therefore you can 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**" while visitors wearing 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.

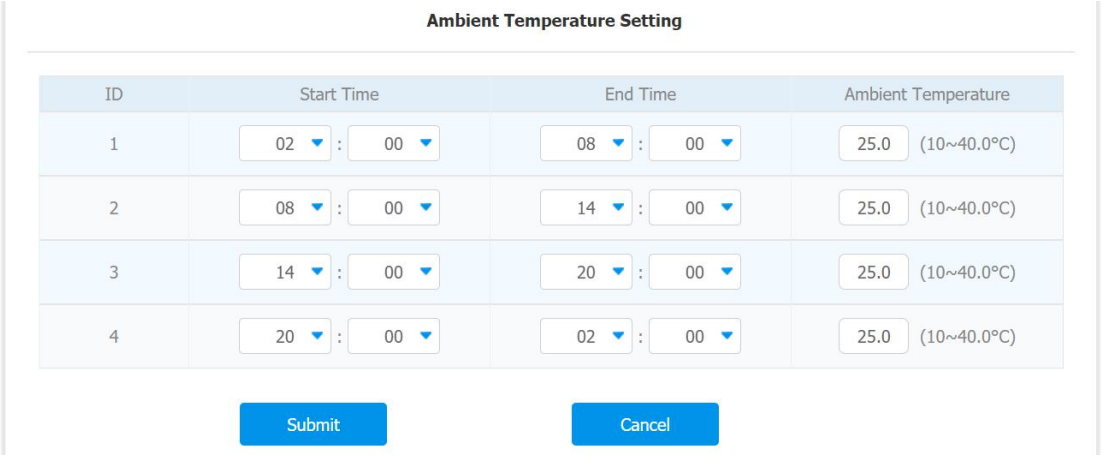
- **Normal Body Temperature**: set the body temperature to the predefined body temperature as the measuring basis in either Fahrenheit or Celsius. For example if you set the temperature 37.3 degree Celsius as the normal temperature, then any body temperature measured higher than 37.3 degree Celsius will be deemed as abnormal temperature, while the temperature lower than 34 degree Celsius will be deemed as low body temperature.

10.3.5.2. Ambient Temperature Configuration

In order to offset the minor variations on the temperature as affected by the ambient temperature in the different places where the device is installed or in the different time of a day, you are required to configure the temperature setting on the basis of time segments during a day.

To do the configuration, you can do as follows:

1. Click **Access Control > Body Temperature > Ambient Temperature Setting**
2. Set up parameters properly.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



Parameter Set-up:

- **Start Time/End Time:** select the start time and end time temperature by referring to the actual temperature measured at the time segments ranging from 10- 40℃degree Celsius. For example, when you divide the time into four time segments, then each of the time segments will be six hours (24 hours a day), while the end time of one segment should be the start time of the next time segment. You can divide the time segments according to your need.

- **Ambient Temperature**: enter the ambient temperature degree. Accuracy can be ensured for the actual temperature value within the range from 10- 40 degree Celsius .

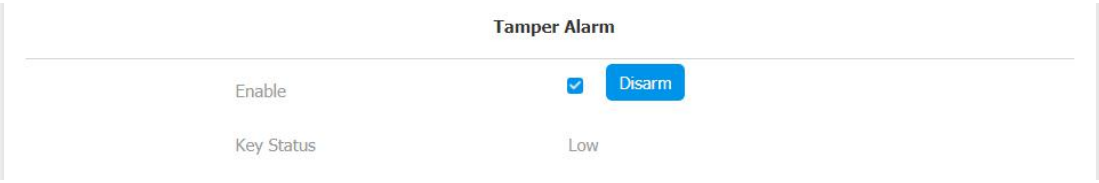
Security

10.4. 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 set up the temper alarm , you can do as follows:

1. Click **Security > Basic > Temper Alarm**
2. Tick the check box to enable the temper alarm function.



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.

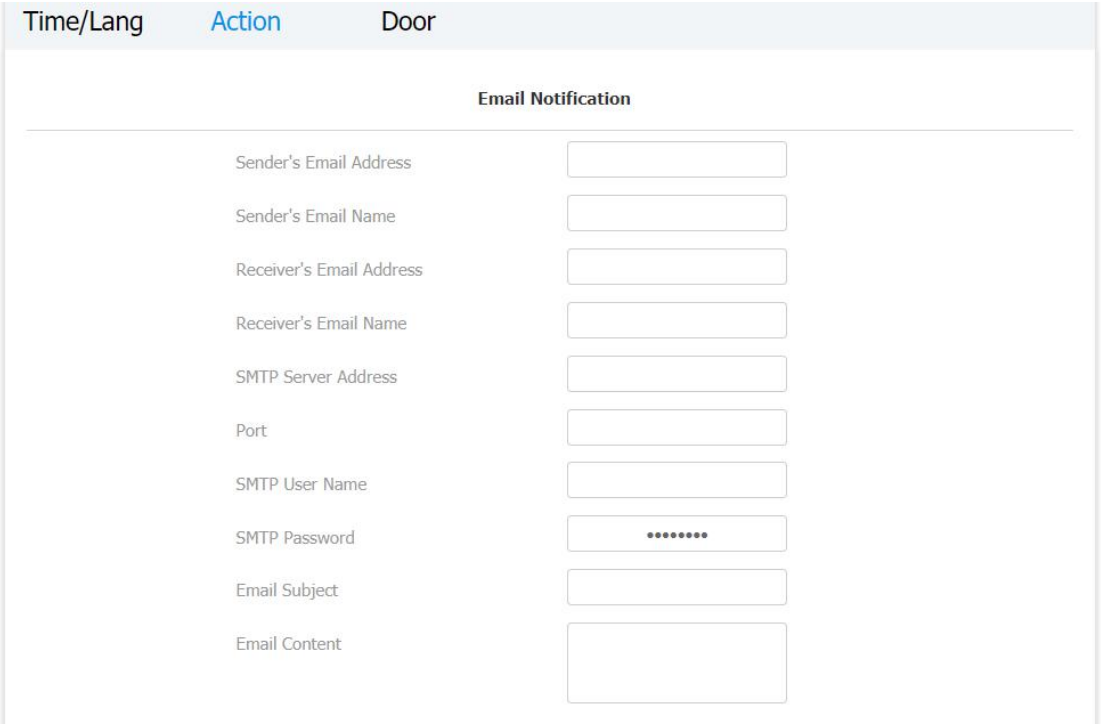
10.5.Security Notification Setting

10.5.1. 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 do the configuration, you can do as follows:

1. Click **Setting > Action > Email Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for validation or cancel ta for cancellation.



Parameter set-up:

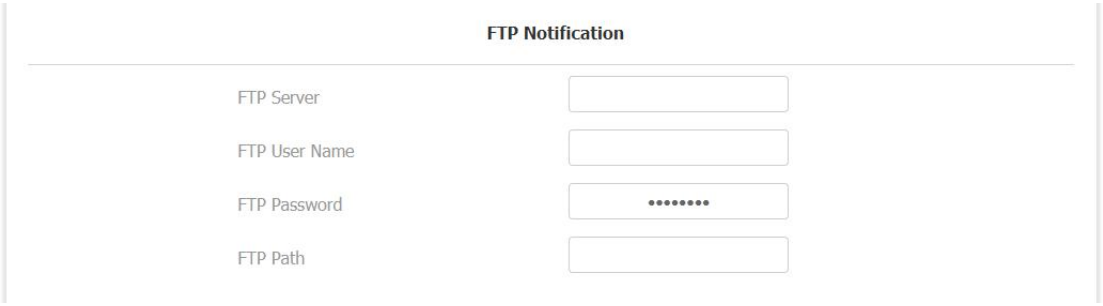
- **Sender's Email Name:** enter the name of the email sender.
- **Sender's email address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's email address:** enter the receiver's email address.
- **Receiver's Email Name:** enter the the name of the 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 emails contents according to your need.

10.5.2. 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 do the configuration, you can do as follows:

1. Click k **Setting > Action > FTP Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for validation or cancel ta for cancellation.



Parameter set-up:

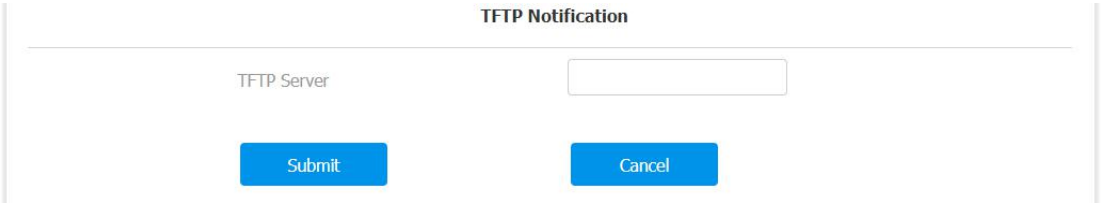
- **FTP server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name**: enter the FTP server user name.
- **FTP Password**: enter the FTP server password.
- **FTP Path**: enter the folder name you created in FTP server.

10.5.3. 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 do the configuration, you can do as follows:

1. Click **Setting > Action > TFTP Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for validation or cancel ta for cancellation.



Parameter set-up:

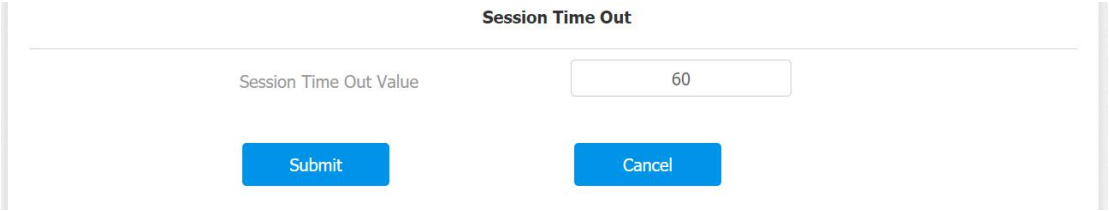
- **TFTP Server**: enter the address (URL) of the TFTP server for the FTP notification

10.6.Web Interface Automatic Log-out

You can set up the web interface automatic log-out timing, requiring re-login by entering the user name and the passwords for the security purpose or for the convenience of operation.

To configure the web interface time-out, you can do as follows:

1. Click **Security > Basic > Session Time Out**
2. Enter the time-out value in the **Session Time Out Value** field.
3. Click Submit tab for the validation or cancel ta for the cancellation.



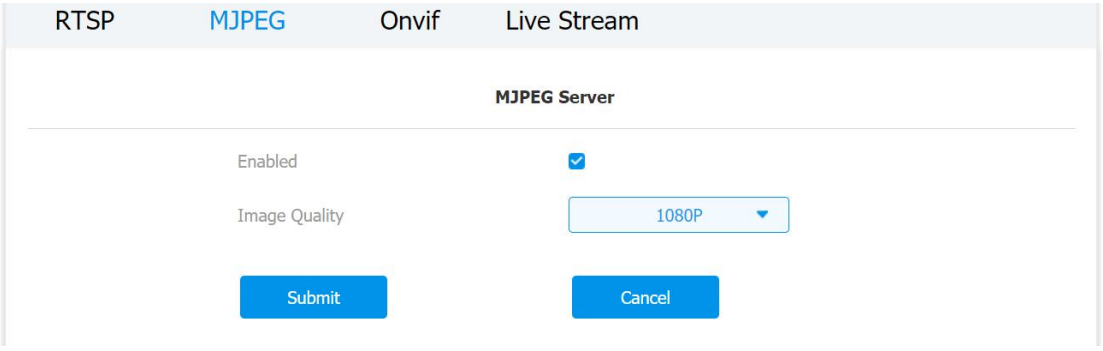
11. Monitor and Image

11.1.Mjpeg Image Capturing

A05 series allow 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 do the configuration, you can do as follows:

1. Click **Surveillance > MJPEG > Mjpeg Server**
2. Set the parameters properly according to your need.
3. Click **Submit** tab for the validation or cancel ta for the cancellation.



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, 1080P**

After the Mjpeg service is enabled, you can capture the image from the access control terminal using 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 access control terminal with the IP address:192.168.1.104, you can do as follows:

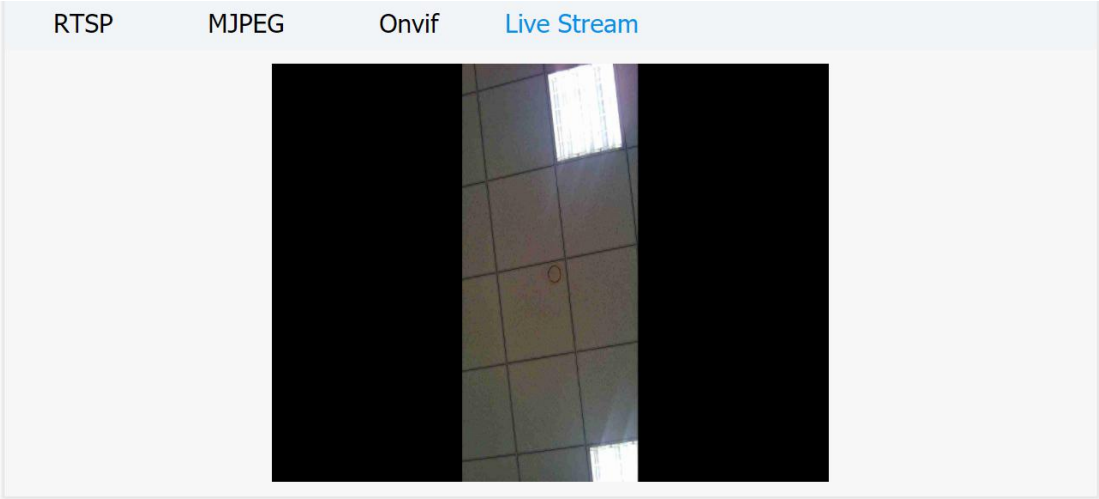
1. Enter "http://192.168.1.104:8080/picture.jpg" on the web browser
2. Ppress Enter key in your keyboard to capture the image.

11.2.Live Stream

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

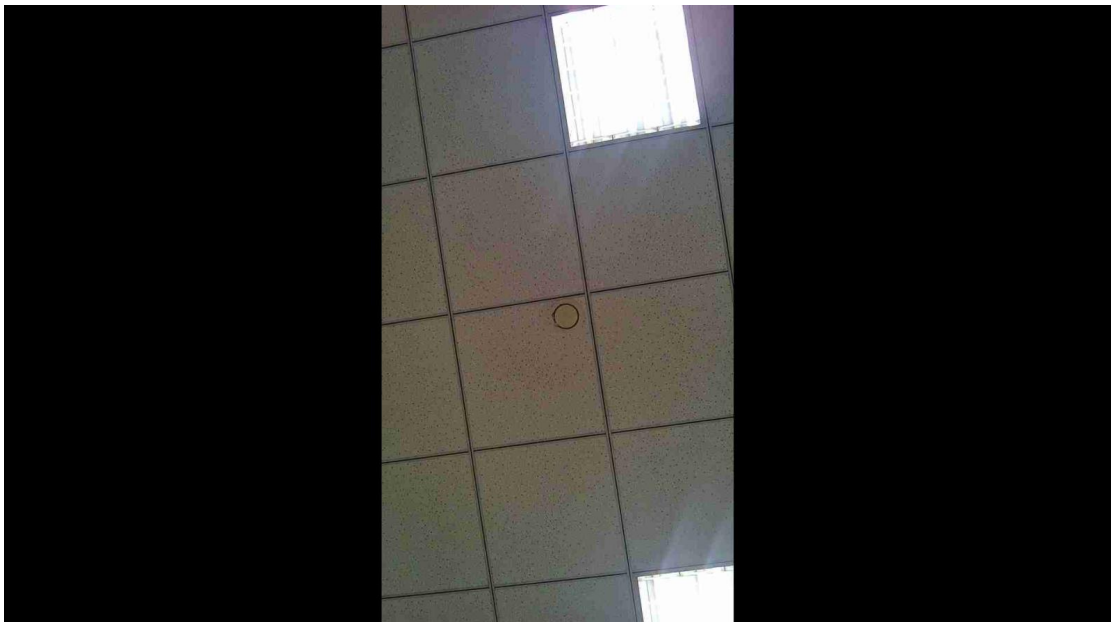
To check the real time video on the web interface, you can do as follows:

1. Click **Surveillance > Live Stream**
2. Check the real time video on the web interface.



To check the real time video using URL, you can do as follows:

1. Enter the correct URL (**http://IP_address:8080/video.cgi**) on the web browser if you want to obtain the real-time video directly with going to the web interface.
2. Check the real time video.



11.3.RTSP Stream Monitoring

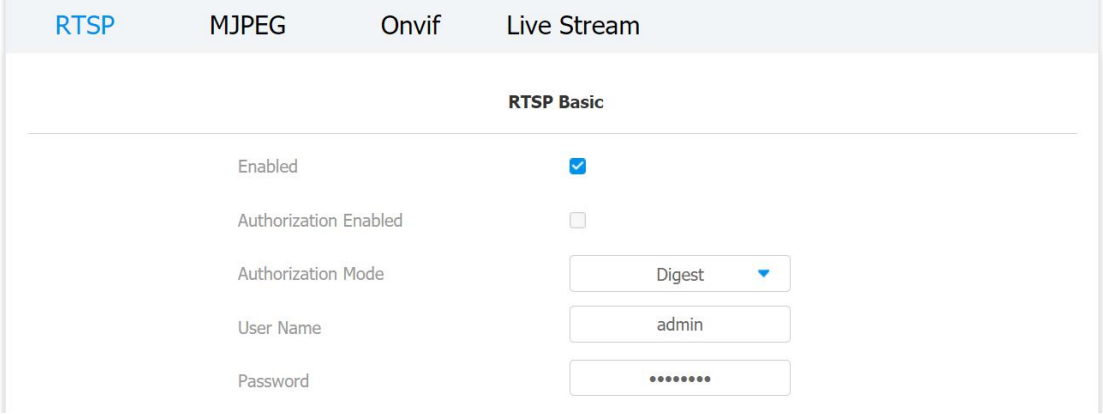
A05 series access control terminal support RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or obtain the the real time audio/ video (RTSP stream) from the access control terminal using the correct URL.

11.3.1. RTSP Basic Setting

You are required to set up RTSP function in terms of RTSP Authorization, authentication and password etc., before you are able to use the function.

To do the configuration, you can do as follows:

1. Click **Surveillance > RTSP > RTSP Basic**
2. Set up parameters properly.
3. Click **Submit** tab for validation or cancel ta for cancellation.



Parameter Set-up:

- **Enabled:** Tick the check box to to turn on or turn off the RTSP function.

- **Authorization Enabled**: 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, 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.

- **User Name**: enter the name used for RTSP authorization.

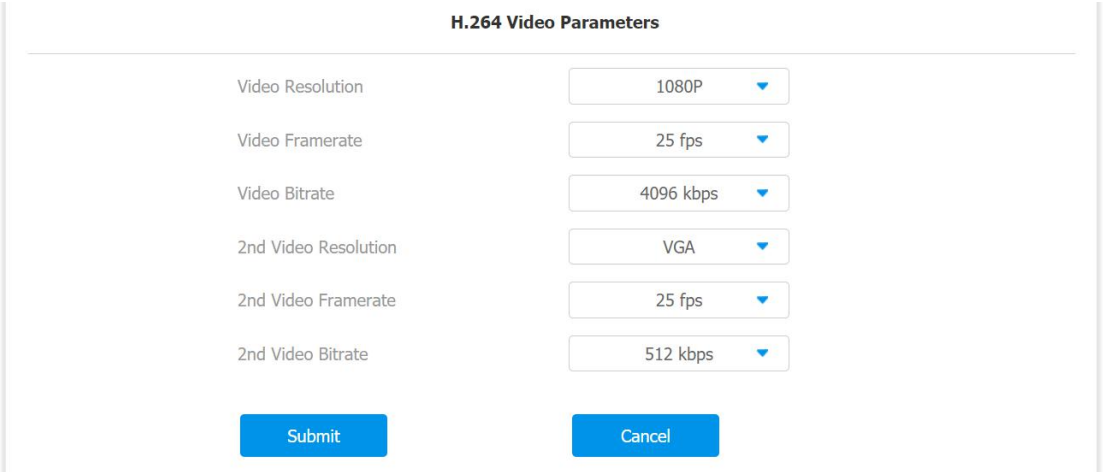
- **Password**: enter the password for RTSP authorization.

11.3.2. 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 bit-rate etc.which based on your actual network environment on the web interface.

To configure the parameters, please do as follows:

1. Click **Surveillance > RTSP > H.264 Video Parameters**
2. Set up video parameters according to your need.
3. Click **Submit** tab for validation or cancel ta for cancellation.



Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: "**QCIF**", **"QVGA**","**CIF**","**VGA**","**4CIF**","**720P**,""**1080P**". The default video resolution is "**720P.** and the video from the access control terminal might not be able to be shown in 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", "4096 kpbs"** according to your network environment. The default video bit-rate is " **2048 kpbs**".

- **2nd Video Resolution2**: select 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 kpbs**" by default.

Note:

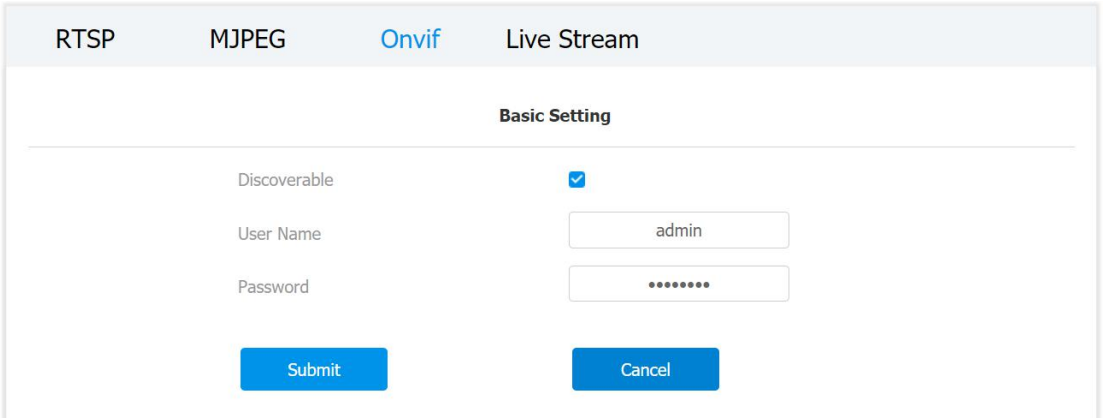
- A05 series supports two video stream channels for H.264 codec video stream.

11.4. ONVIF

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

To do the configuration, you can do as follows:

1. Click **Intercom > ONVIF**
2. Set up parameters properly.
3. Click **Submit** tab for validation or cancel ta for cancellation.



Parameter Set-up:

- **Discoverable:** Tick the check box to turn on the 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.
- **User Name:** 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.

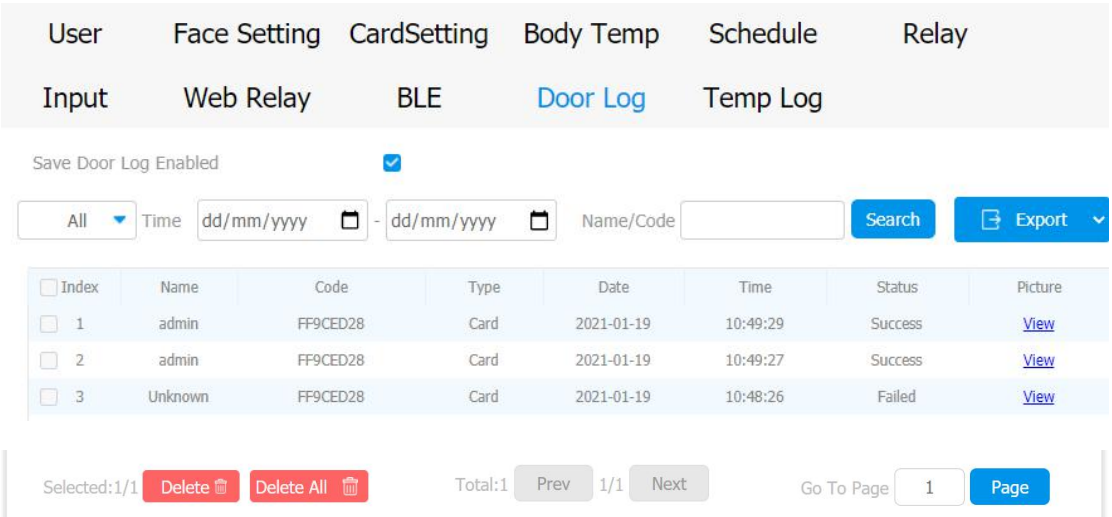
12. Logs

12.1.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 interface.

To access the door logs , you can do as follows:

1. Click **Access > Door log**
2. Tick the the check box of **Save Door Log Enabled** if you want to save the log.
3. Click icon if you want to search door access by “ All” “ Success” and“failed “.
4. Click on **“View”** on each door log if you want to see the picture captured for the door log.
5. Check on the specific door log check box and click **Delete** tab to delete.
6. Click **Delete all** tab if you want to delete all of the door logs.



Parameter set-up:

- **Save Door Log Enabled:** Tick the check box to turn on or turn off the door log function.

- **Status: s**elect between **"Success" and "Failed"** options to search for successful door accesses or Failed door accesses.

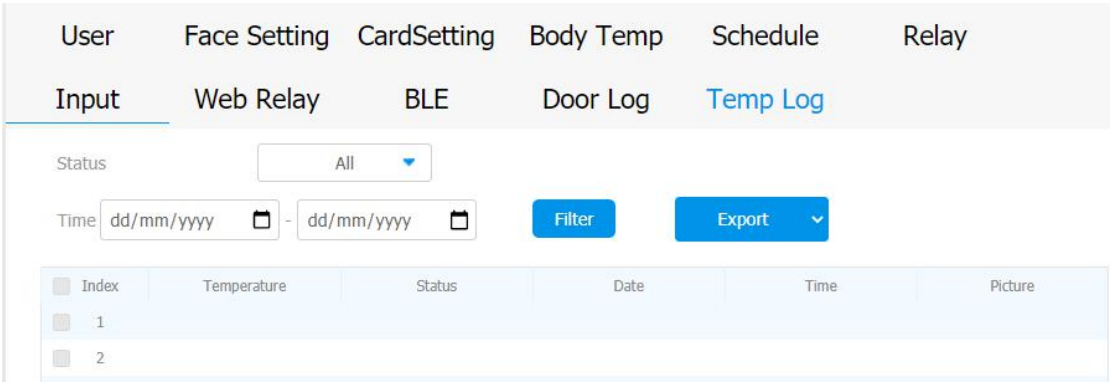
- **Time:** select the specific time select the specific time span of the door logs you want to search, check or export.

- **Name/Code**: select the "**Name**" and " **Code**" options to search door log by the name or by the PIN code.

12.2. Temperature Log

To check temperature log, you can do as follows:

1. Click **Access Control > Temperature Log**
2. Click **Status** field to select the range and category of temperature log check among four options:"**All**", "**Normal**", "**Abnormal**", "**Low Temperature**".
3. Click **Filter** tab to see the specific category of temperature log selected.
4. Click **Export** tab to export the the temperature log.
5. Click the specific check box and click **Delete** tab to delete the temperature log you want to delete.
6. Tick the the check box by **Index** to delete all the temperature log.



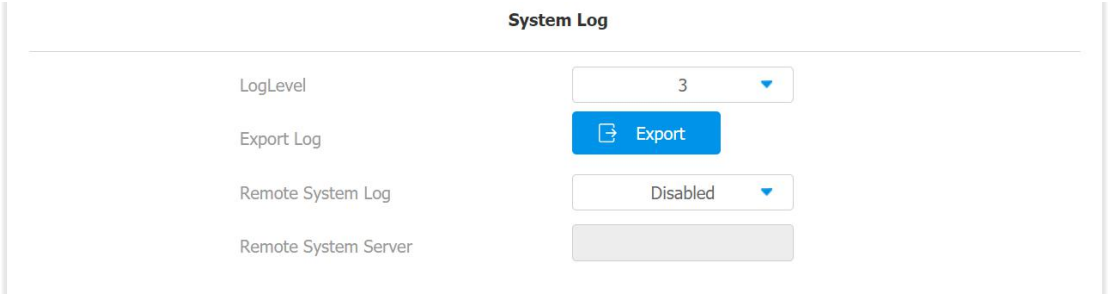
13. Debug

13.1.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 interface.

To do the configuration, you can do as follows:

1. Click **Upgrade > Advanced > System Log**
2. Enter the parameters properly.
3. Reproduce the problem occurred.
4. Click **Export** tab to export logs.
5. Click **Submit** tab for validation and **Cancel** for cancellation.



Parameter Set-up:

- **LogLevel**: 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 "**5**", the more complete the log is "**7**".

- **Export Log**: click the **Export** tab to export temporary debug log file to a local PC.

- **Remote System Log**: select "**Enable**" or " **Disable**" if you wan to enable or disable the remote system log.

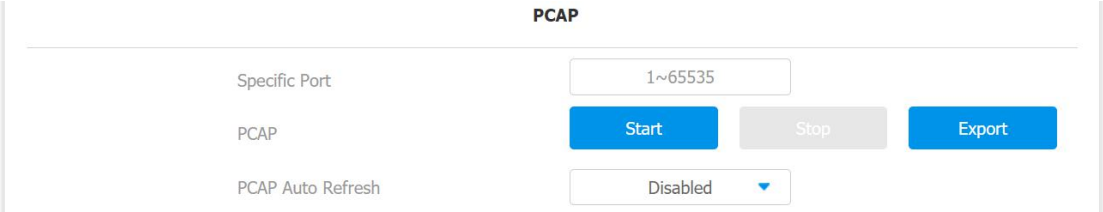
- **Remote System Server**: enter the remote server address to receive the the device log**.** And the remote server address will be provide by Akuvox technical support.

13.2.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 interface properly before using it.

To do the configuration, you can do as follows:

1. Click **Upgrade > Advanced > PCAP**
2. Set up parameters properly.
3. Start PCAP data packets capturing by clicking on **Start** tab.
4. Stop PCAP data packets capturing by clicking on the **Stop** tab.
5. Export the data packets captured by PCAP by clicking on **Export** tab.



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 the a certain range of data packets before clicking **Export** tab to export the data packets to you

Local PC.

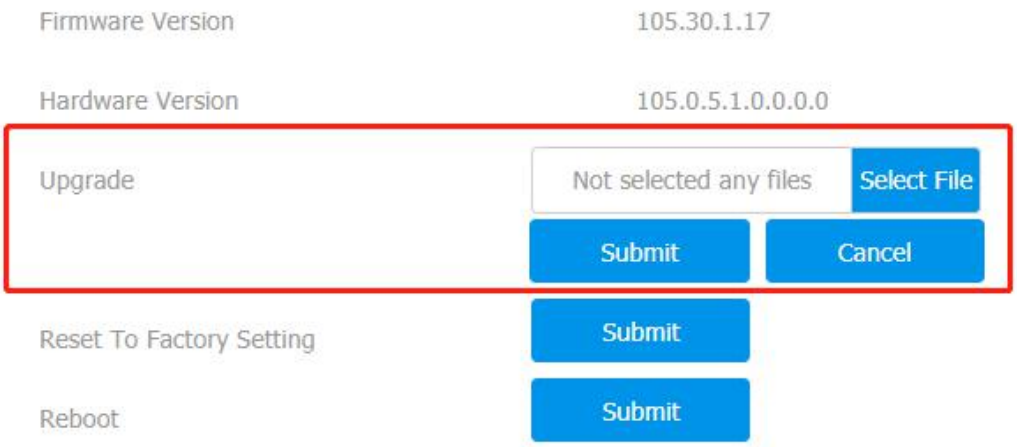
- **PCAP Auto Refresh**: select "**Enable**" or " **Disable**" to turn on or turn off the PCAP auto fresh function. If you set it as " Enable" then the PCAP will continue to capture data packet even after the data packets reached its 50M maximum in capacity. If you set it as " **Disable**" the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

14. Firmware Upgrade

Firmwares of different versions for A05 series access control terminal can be upgraded on the device web interface.

To upgrade the firmware, you can do as follows:

1. Click **Upgrade > Basic**
2. Select firmware files from your local PC.
3. Press **Submit** tab for the validation or cancel ta for the cancellation.



Note:

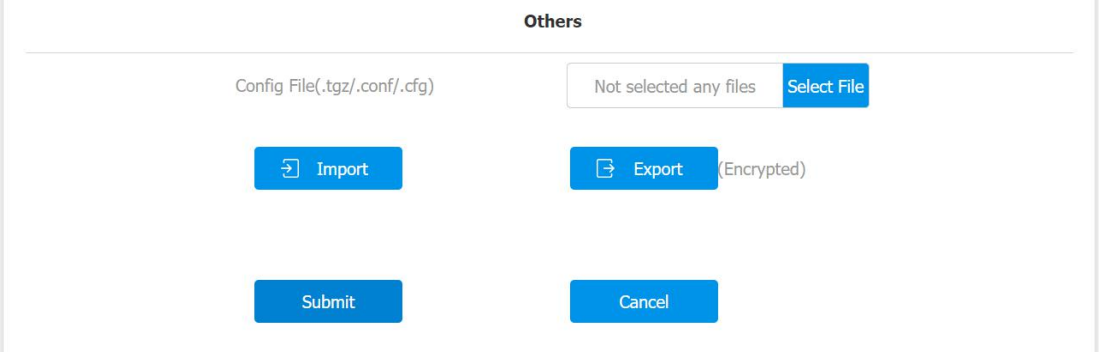
- Firmware files should be .rom format for upgrade.

15. Backup

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

To do so , you can do as follows:

1. Click **Upgrade > Advanced > Others**
2. Click **Select File** to select the file from your local PC.
3. Click **Import** tab if you want to import the selected config file.
4. Click **Export** tab if you want to export the existing config files to you local PC.
5. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.

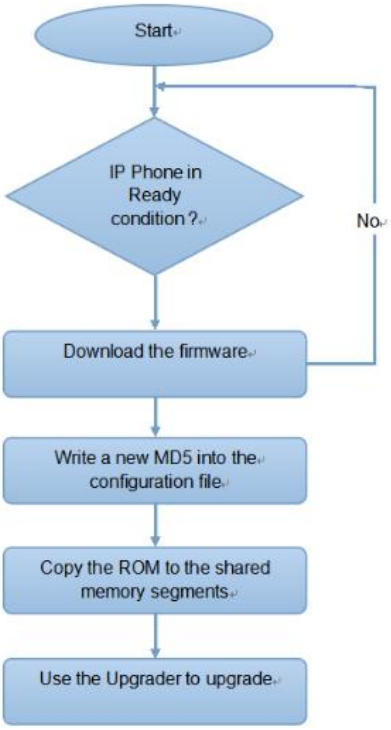


16. Auto-provisioning via Configuration File

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.

16.1.Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade the devices in batch via third party servers. **DHCP, PNP, TFTP, FTP, 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 firmwares, which will then be used to to update the firmware and the corresponding parameters on the access control terminal.



16.2. Configuration Files for Auto-provisioning

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

The difference between the two types of configuration files is shown as 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 is used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.

Note:

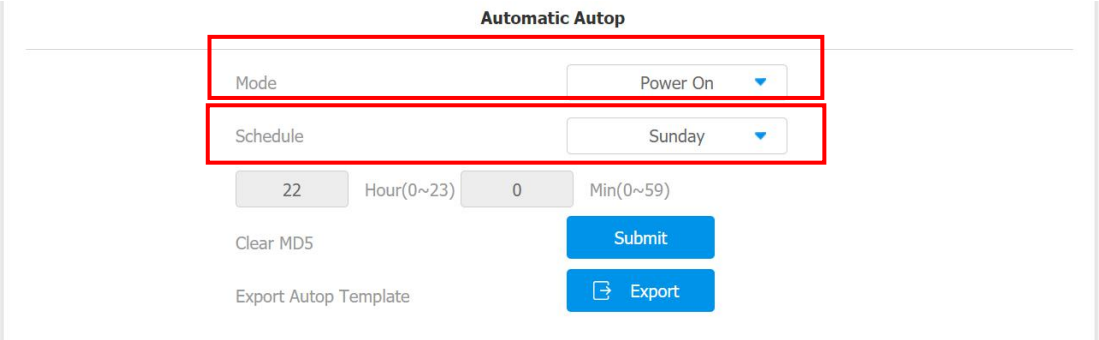
- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

16.3.AutoP Schedule

Akuvox provides you with different Autop methods that enable the access control terminal to perform provisioning for itself in a specific time according to your schedule.

To set up the schedule, you can do as follows:

1. Click **Upgrade > Advanced > Automatic Autop**
2. Set up mode and schedule according to your need.
3. Click **Submit** tab for the validation or cancel ta for the cancellation.



Parameter Set-up:

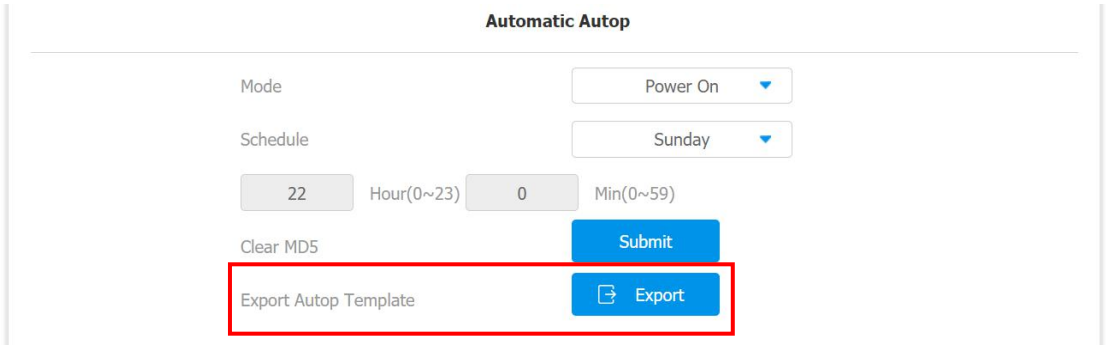
- **Power On:** select "**Power on**", if you want the device to perform Autop every time it boots up.
- **Repeatedly:** select " **Repeatedly**", if you want the device to perform autop according to the schedule you set up.
- **Power On + Repeatedly:** select "**Power On + Repeatedly**" if you want 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.

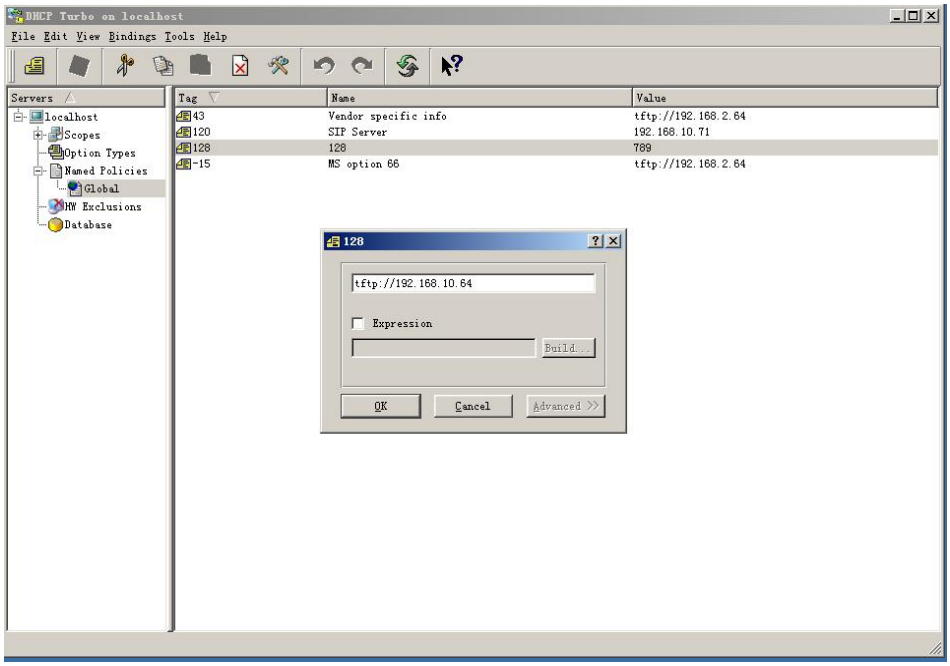
16.4.DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using DHCP option which allows device to send a request to a DHCP server for a specific DHCP option code. If you wan to use **Custom Option** as defined by users with option code range 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, you can do as follows:

1. Click **Upgrade > Advanced > Automatic Autop**
2. Click **Export** tab in **Export Autop Template** to export Autop template.
3. Set up DHCP Option on DHCP server.

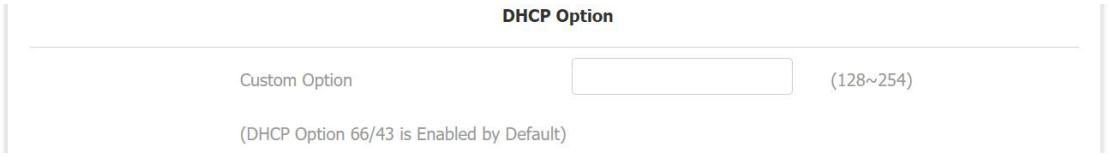




Note:

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

4. Rename the AutoP config template.
5. Select general provisioning configuration file for the device in-batch provisioning or the MAC-based configuration file for the specific device provisioning.
6. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server.
7. Edit AutoP config template.
8. Go to **Upgrade > Advanced > DHCP Option** on the device web interface.
9. Enter the DHCP code in the **Custom Option field** for the URL to the config file server.
10. Click **Submit** tab for the validation or cancel ta for the cancellation.



Parameter set-up:

- **Custom Option**: enter the DHCP code that matched with corresponding URL so that 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 the option 66 with the update 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 the option 43 with the update server URL in it.

Note:

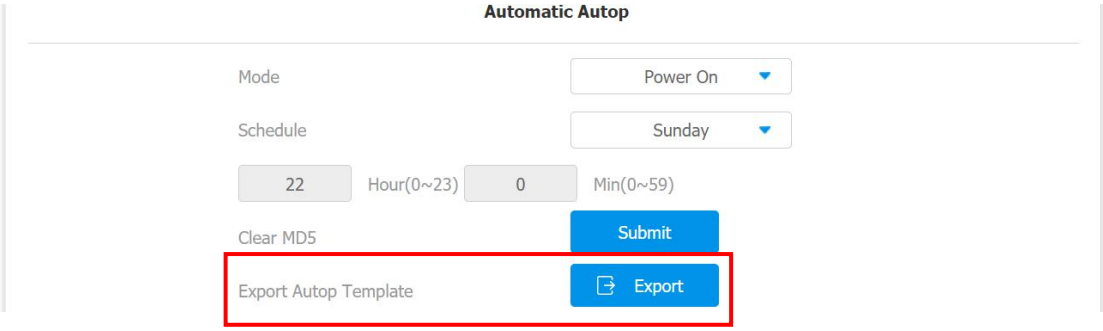
- The general configuration file for the in-batch provisioning is with the format "r**0000000000xx.cfg**" taking A05 as an example "r000000000105.cfg (10 "zeros" in total while the MAC-based configuration file for the specific device provisioning is with the format "MAC_Address of the device.cfg, for example "**0C110504AE5B.cfg.**"

16.5.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 on a specific timing according to 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.

To set up static provisioning autop, you can do as follows

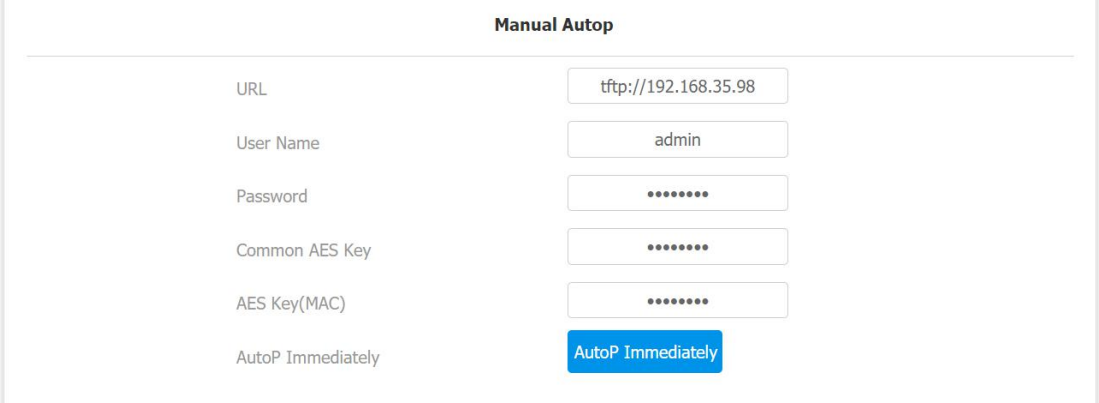
1. Click **Upgrade > Advanced > Automatic Autop**
2. Click **Export** tab in **Export Autop Template** to export Autop template.



3. Rename the AutoP config template.
4. Select general provisioning configuration file for the device in-batch

provisioning or the MAC-based configuration file for the specific device provisioning. (for example: r**000000000016** for A05 access control terminal and **r000000000115** for C315 in door monitor)

5. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server.
6. Edit AutoP config template.
7. Upload the AutoP config template to DHCP/TFTP/FTP/HTTP/HTTPS server.
8. Go to **Upgrade > Advanced > Manual Autop** on the web interface.
9. Enter TFTP URL into the box(under the path "Upgrade-Advanced") and click AutoP Immediately.



Parameter set-up:

- **URL**: set up tftp，http，https，ftp server address for the provisioning.
- **User Name**: set up a user name if the server needs an user name to be accessed to otherwise leave it blank.
- **Password**: set up a password if the server needs a password to be accessed to otherwise leave it blank.
- **Common AES Key**: set up AES code for the intercom to decipher 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)

Tip:

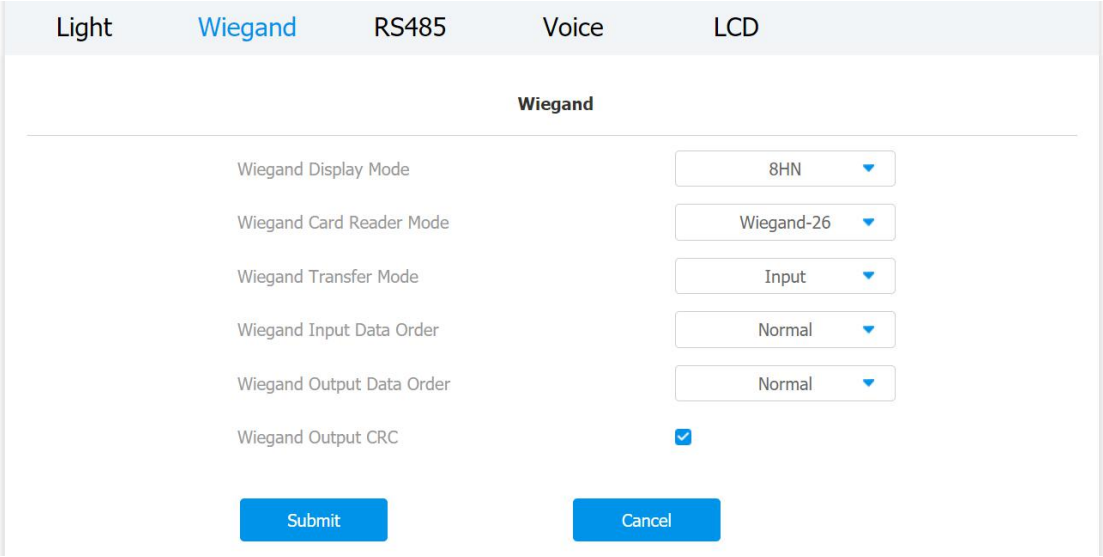
- Akuvox do not provide user specified server.
- Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

17. Integration with Third Party Device

17.1. 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 interface.

1. Click **Device > Wiegand > Wiegand**
2. Set up parameters according to your need.
3. Click **Submit** tab for the validation or cancel ta for the cancellation.



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", " 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 an 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 an vice versa.

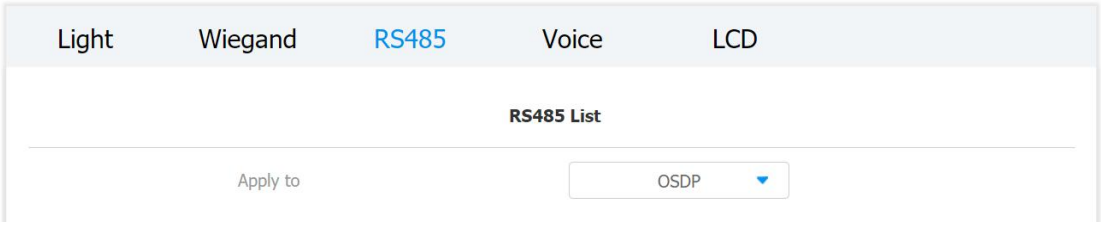
- **Wiegand Output CRC:** Tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.

17.2. Integration via RS485

RS485 Integration mode should be configured properly on the access control terminal's web interface before you can implement the integration between the access control terminal and the third party devices.

To do the configuration, you can do as follows:

1. Click **Device > RS485 > RS485 List**
2. Set up parameter properly.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



Parameter Set-up:

- **RS485 List**: select integration mode between two options: " **None**" ," **OSDP**", the detail for the two options will be provided in the following chart.

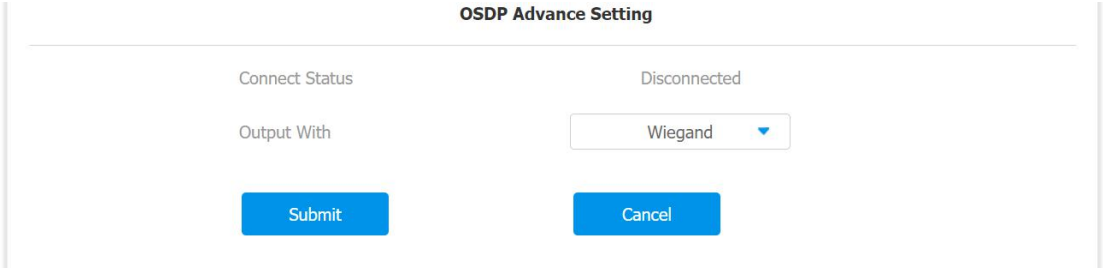
NO.	Integration Mode	Description
1	**None**	If you select "**None**" then the RS485 integration will be disabled.
2	**OSDP**	If you Select "**OSDP**" Mode, then the integration communication between the A05 series access control terminal and the third party device is via OSDP protocol. You are required to check for the device integration protocol and make sure if that they use the same integration protocol.

17.3. OSDP Setting

If you choose OSDP integration mode, you can not only check for OSDP status but also obtain the authentication from the third party devices for various applications such as door access etc.

To do the configuration, please do as follows:

1. Click **Device > RS485 > OSDP Advance Setting**
2. Set up parameter properly.
3. click **Send** tab if you want to send the Dummy Card number to be authenticated by the third party device.
4. Click **Submit** tab for the validation or cancel ta for the cancellation.



Parameter Set-up:

- **Connect Status:** indicate OSDP based communication status.

- **Send by:** select in what way you want to send out the card number among three options: "**OSDP", "Wiegand**" and " **None**". if you select **"OSDP"** then the card number will be sent out to the third party devices via RS485. if you select **"Wiegand"** then the card number will be sent out via wiegand. If you select **"None"** then the card number will not be sent out but retained in the system.

Note:

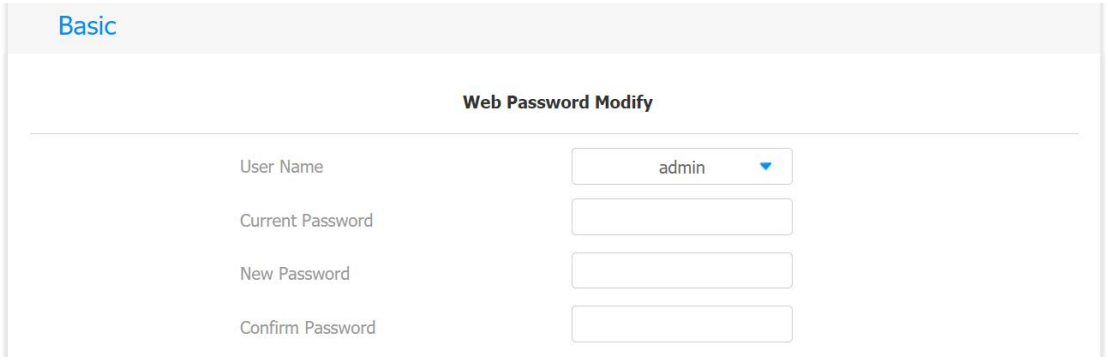
- Dummy card numbers can not be sent if "**OSDP**" is not selected in the RS485 list field.

18. Password Modification

On the device web interface, you can set and change password for accessing the web interface. In addition, you can also select the user role when setting passwords.

To set and change the web interface passwords, you can do as follows:

1. Click **Security > Basic > Web Password Modify**
2. Select **User Name** between **"admin"**.



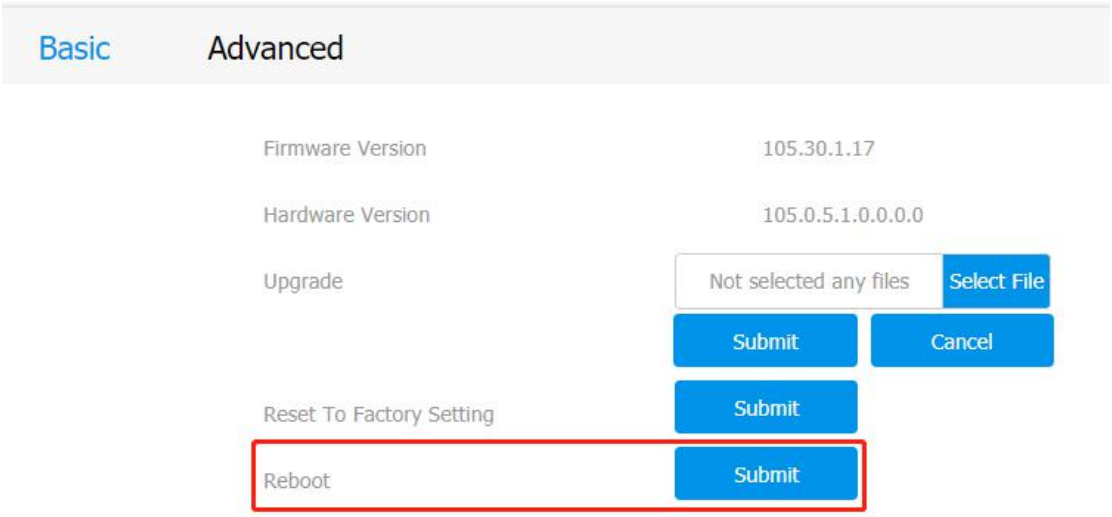
19. System Reboot and Reset

19.1.Reboot

If you want to restart the device, you can operate it on the device web interface as well. More over, you can set up schedule for the device to be restarted.

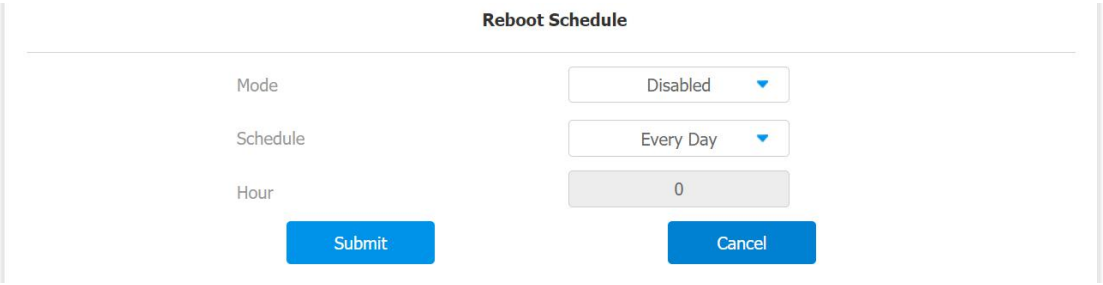
To restart the system setting on the web interface, you can do as follows:

1. Click **Upgrade > Basic**
2. Click on **Submit** tab for restarting the device.



To set up the device restart schedule, you can do as follows:

1. Click **Upgrade > Advanced > Reboot Schedule**
2. Enable the scheduled Reboot mode.
3. Set up the device restart day and timing (0-23).
4. Click **Submit tab** for the validation or cancel ta for the cancellation.

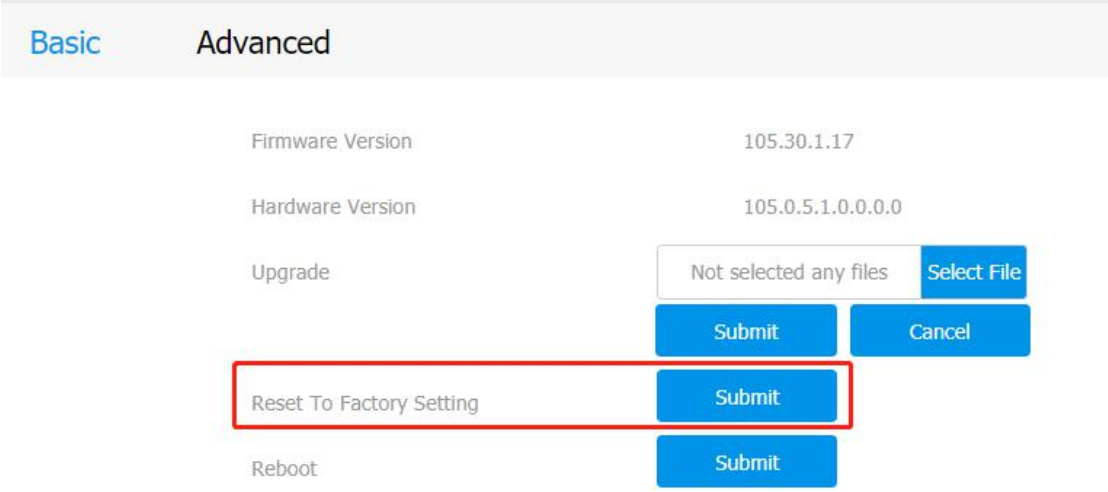


Reset

If you want to reset the device system to the factory setting, you can it on the web interface.

To reset to the factory setting, you can do as follows:

1. Click **Upgrade > Basic**
2. Click on **Submit** tab for **Reset to Factory Setting.**



20. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical 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

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

21. FAQ

Q1: How to obtain IP address of R2X
A1: ✔ For devices with 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 call button again to quit the announcement mode.

✔ For devices with multiple numeric keyboard - R27:
While R27 power up normally, press "*2396#" to enter home screen and press "1" to go to system Information screen to check the IP address.

✔ For devices with touch screen - R29:
While R29 power up normally, in the dial interface, press "9999", "Dial key", "3888" and "OK" to enter the system setting screen. Go to 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 akuvox door phone?
A3: R20/E21/R26/R23/Standard R27/Standard R29 -- 14° to 112°F (-10° to 45°C)
R27/R29 with heating supporting --- 40 degrees
R28 -- (-40°C~55°C)
Indoor phone -- 14° to 112°F (-10° to 45°C)
IPPhone -- 32º~104ºF(0~40ºC)

Q4: Do Akuvox devices support Modbus protocol?
A4: No.

Q5：Failure in importing the R29 face data to another R29 using the exported face data .
A5：Please confirm the following steps：
The import format is zip;
3. After you export , you need to unzip the .tgz folder , then make the unziped

folrder into .zip again.

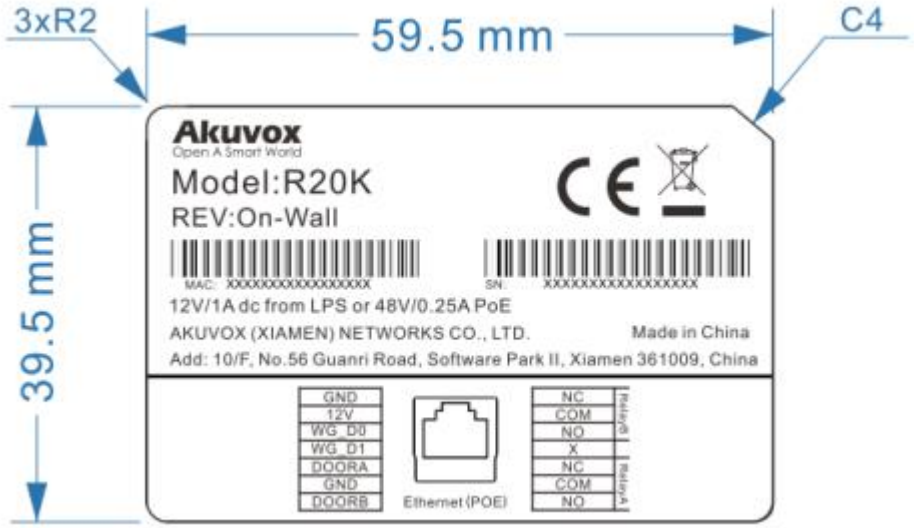
Q55: Which version of ONVIF does R20 and R29 support?
A55: Onvif 18.04 profiles

Q6: Do access control terminals support these card types? Prox, Legacy iClass,iClassSE,HID Mifare, HID DESFire,HID SEOS
A6: Sorry, they are not supported. They need to be implemented via hardware modifications.

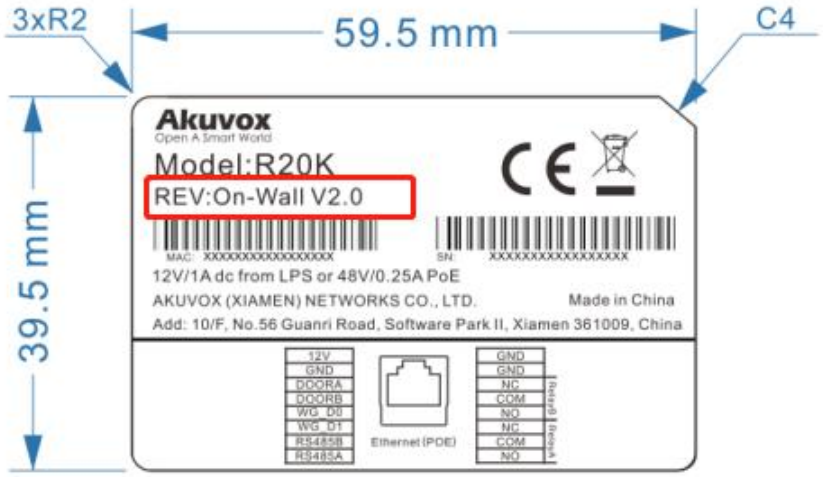
Q7: How to confirm whether my device is hardware version 1 or hardware version 2?

A7: 1.Label

- **Hardware version 1**



- **Hardware version 2**

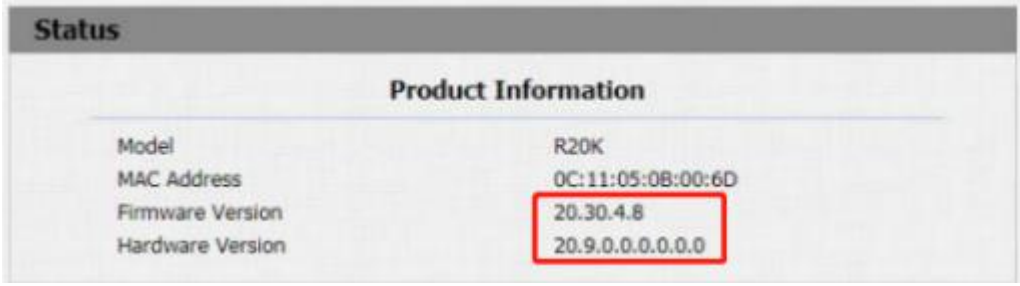


- **Firmware Version**

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.



22. 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.