AKUVOX ACCESS CONTROL TERMINAL ADMIN GUIDE

Version: 1.0 | Date: Jan.2022

About This Manual

Thank you for choosing Akuvox A01S, A02S access control terminal. This manual is intended for the administrators who need to properly configure the access control terminal. This manual applies to 101.30.1.24 version, and it provides all the configurations for the functions and features of A01S, A02S access control terminals. Please visit Akuvox forum or consult technical support for any new information or the latest firmware.

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:

https://knowledge.akuvox.com

FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

Table of Contents

1. Product Overview

Akuvox Access control terminals A01S, A02S,   incorporate door controller and a RIFD reader in one standalone device, thus saving your solution costs. Equipped with a card reader (125kHz and 13.5MHz) which is capable of handling a majority of cards in wide use currently. A0X is designed to provide you with greater flexibility and security than those traditional access control systems.A01S 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	A01S	A02S
Housing Material	Front panel: Toughened Glass Frame: Aluminum Alloy	
Relay Out	1	
Input	2	
Wiegand	√	
PoE	√	
RAM	128M	
ROM	128M	
Card Reader	13.56MHz&125KHz	
Wi-Fi	X	
Bluetooth	X	X
IP Rating	IP65	
LTE	X	
USB	X	
External SD Card	X	
Wall Mounting	√	
Flush Mounting	√	
Desk Mounting	X	

4. Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, Network Information etc. As well as log related configurations such as access log.

- **Directory**: this section includes access schedule management and user management.

- **Hardware**: this section includes input type setting, relay setting, card setting, Wiegand and LED setting, volume setting.

- **Services**: this section deals with security notification settings, web relay and HTTP API setting.

- **System**: this section covers network and time setting, firmware upgrade, device reset&reboot, configuration file auto-provisioning, system log and PCAP, password modification as well as device backup.

● Tool selection

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

1. **ACMS**: ACMS (Access Control Management System) is designed with an idea that personnel, device, access control, personnel attendance and shift schedule etc.

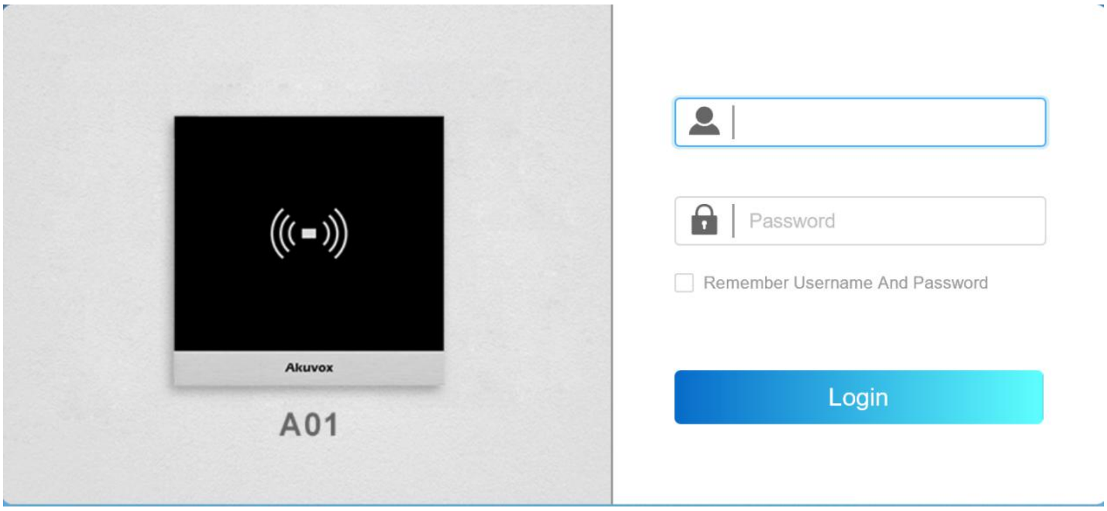
2. **Akuvox Upgrade tool**: Upgrade Akuvox devices in batch on a LAN (**Local Area Network**).

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. Access the Device

Before configuring Akuvox A01S, please make sure the device is installed correctly and connect a normal network. Using Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to login in the web browser by user name and password **admin** and **admin**.



Tip:

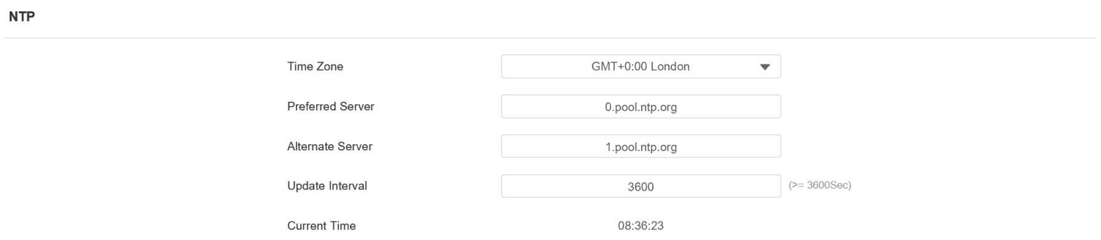
- Please refer to the URL below for the IP scanner application instructions: http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s[]=ip&s[]=scanner

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.

6. 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 configuration on the device web **System > Time** interface.



NTP

Time Zone	GMT+0:00 London	
Preferred Server	0.pool.ntp.org	
Alternate Server	1.pool.ntp.org	
Update Interval	3600	(>= 3600Sec)
Current Time	08:36:23	

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.

- **Alternate 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.

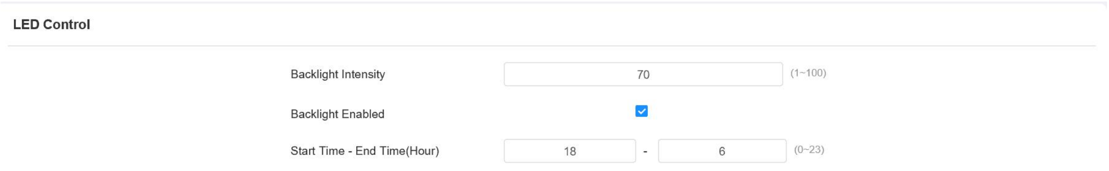
Note:

- When the check box is unticked, the parameters related to NTP server will become not editable.

7. LED Setting

7.1. Brightness Setting

If you want to brighten up the brightness in order to see the card reader at greater ease in an environment with higher light intensity, you need to set up the related parameters in web **Hardware > LED** interface.



LED Control

Backlight Intensity 70 (1~100)

Backlight Enabled ☑

Start Time - End Time(Hour) 18 - 6 (0~23)

Parameter Set-up:

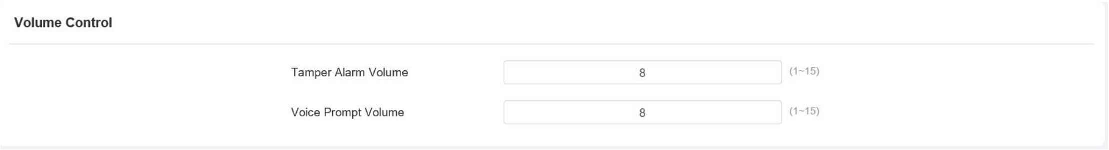
- **Backlight Intensity**: adjust the backlight intensity, the bigger value, the brighter backlight.
- **Backlight Enabled**: tick the check box if want to enable the card reader LED lighting and vice versa.
- **Start Time - End Time (H)**: enter the time span for the LED lighting to be valid, e.g., 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 in one day (24 hours).

8. Volume and Tone Configuration

Volume and tone configuration in A01S access control terminal refers to tamper alarm volume, voice prompt volume and open-door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

8.1.1. Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs. To configure the configuration on web **Hardware > Audio > Volume Control** interface.



Volume Control

Tamper Alarm Volume	8	(1~15)
Voice Prompt Volume	8	(1~15)

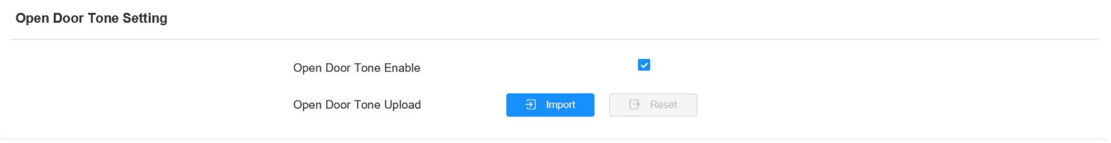
Parameter Set-up:

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

- **Voice Prompt Volume**: set the voice prompt volume from 0-15 according to your need. The default volume is **8**.

8.1.2. Upload Open Door Tone

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

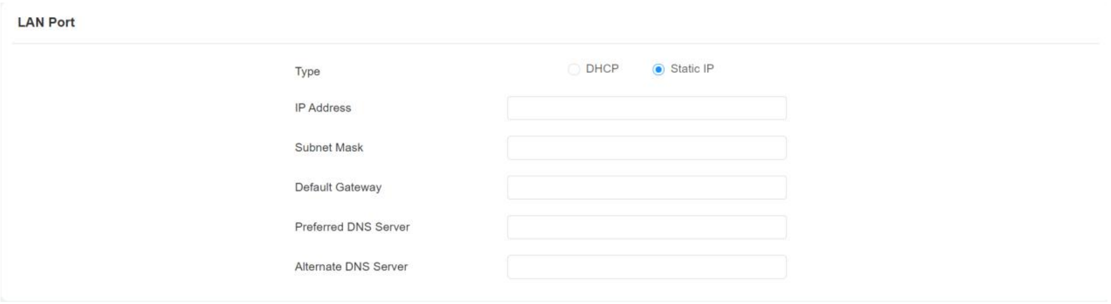


Open Door Tone Setting

Open Door Tone Enable	☑
Open Door Tone Upload	Import Reset

9. Network Setting

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



LAN Port

Type	○ DHCP ● Static IP
IP Address	
Subnet Mask	
Default Gateway	
Preferred DNS Server	
Alternate DNS Server	

Parameter Set-up:

- **DHCP**: select the **DHCP** mode by checking off the DHCP box. DHCP mode is the default network connection. If the DHCP mode is selected, then the access control terminal will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.

- **Static IP**: select the static IP mode by checking off the Static IP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address must be manually configured according to your actual network environment.

- **IP Address**: set up the IP Address if the static IP mode is selected.

- **Subnet Mask**: set up the subnet mask according to your actual network environment.

- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.

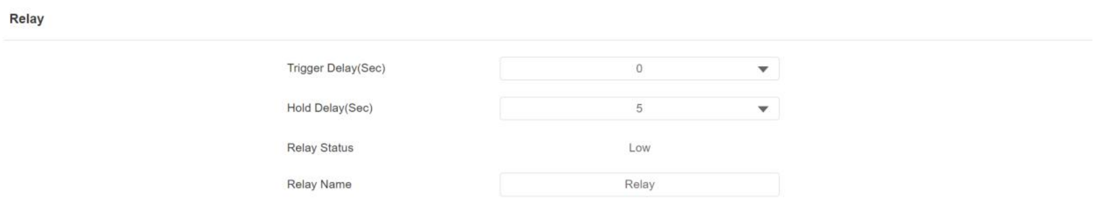
- **Preferred/Alternate DNS**: set up DNS1/ DNS2 (**Domain Name Server**) according to your actual network environment. DNS1 is the primary DNS server address while the DNS2 is the secondary server address, and the access control terminal connects to DNS2 server when the primary DNS server is unavailable.

10. Relay Setting

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

10.1.1.Relay switch setting

To configure the configuration on web **Hardware > Relay > Relay** interface.



Relay

Trigger Delay(Sec)	0
Hold Delay(Sec)	5
Relay Status	Low
Relay Name	Relay

Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (Ranging from 1-10 Sec.) For example, if you set the delay time as "**5**" sec. then the relay will not be triggered until 5 seconds after you press "**unlock**" tab.

- **Hold Delay (Sec):** set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as "**5**" Sec. then the relay will be delayed for 5 after the door is unlocked.

- **Relay Status:** relay status is low by default which means normally closed (NC) If the relay status is high, then it is in Normally Open status (NO).

- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for the convenience.

Note:

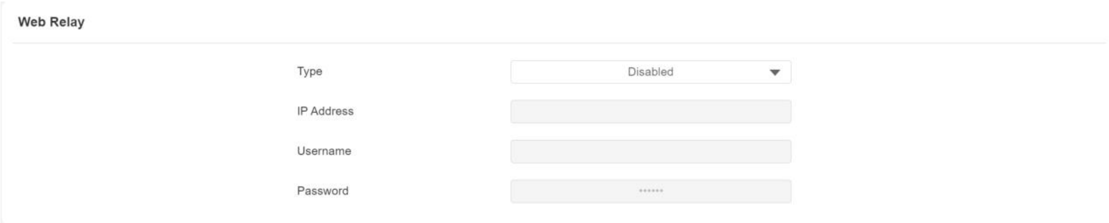
- Only the external devices connected to the relay switch needs to be powered by power adapters as relay switch does not supply power.

10.2.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.

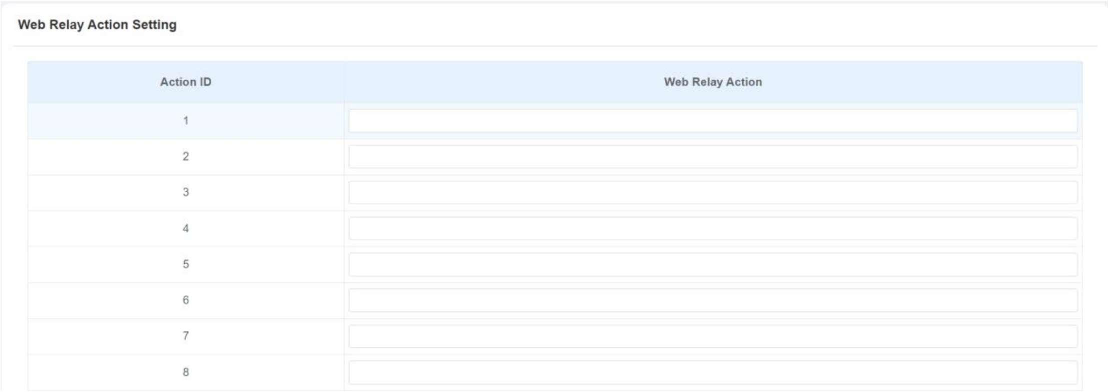
10.2.1.Configure Web Relay on the Web Interface

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 configure the configuration on web **Services > Web Relay** interface.



Web Relay

Type	Disabled
IP Address	
Username	
Password	******



Web Relay Action Setting

Action ID	Web Relay Action
1	
2	
3	
4	
5	
6	
7	
8	

Parameter Set-up:

- **Type:** select among three options **Disabled, WebRelay** and **Both**. Select **WebRelay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.

- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.

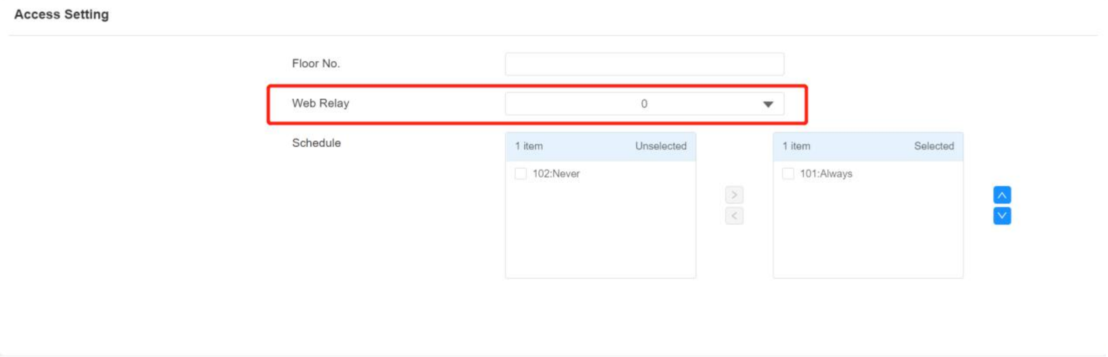
- **User Name**: enter the User name provided by the web relay manufacturer.

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

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

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

After the web relay is set up, you can configure the specific web relay to be triggered based on the relay location for the door access. To configure the configuration on web **Directory > User > Access Setting** interface. You need to click **+Add** tab to turn to **Access Setting** interface.



Access Setting

Floor No.

Web Relay 0

Schedule

1 item	Unselected
□ 102:Never	

1 item	Selected
□ 101:Always	

11. Door Access Schedule Management

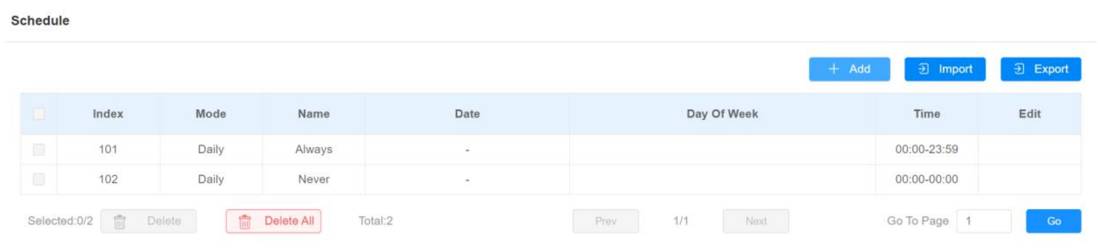
You are required to configure and make schedule for the user-based door access via RF card.

11.1. 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. Moreover, you can edit your door access schedule if needed.

11.1.1.Create Door Access Schedule

You can create the door access schedule on the daily or weekly 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 configure the configuration on web **Directory > Schedule** interface.

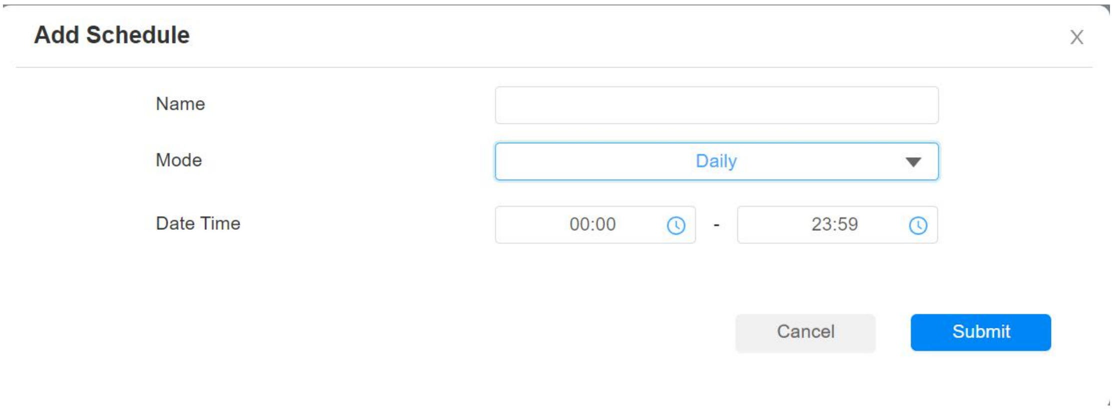


Schedule

□	Index	Mode	Name	Date	Day Of Week	Time	Edit
□	101	Daily	Always	-		00:00-23:59	
□	102	Daily	Never	-		00:00-00:00	

Selected:0/2 Delete Delete All Total:2 Prev 1/1 Next Go To Page 1 Go

Click **+ Add** to create a daily schedule, select **Schedule Mode** as **Daily**.



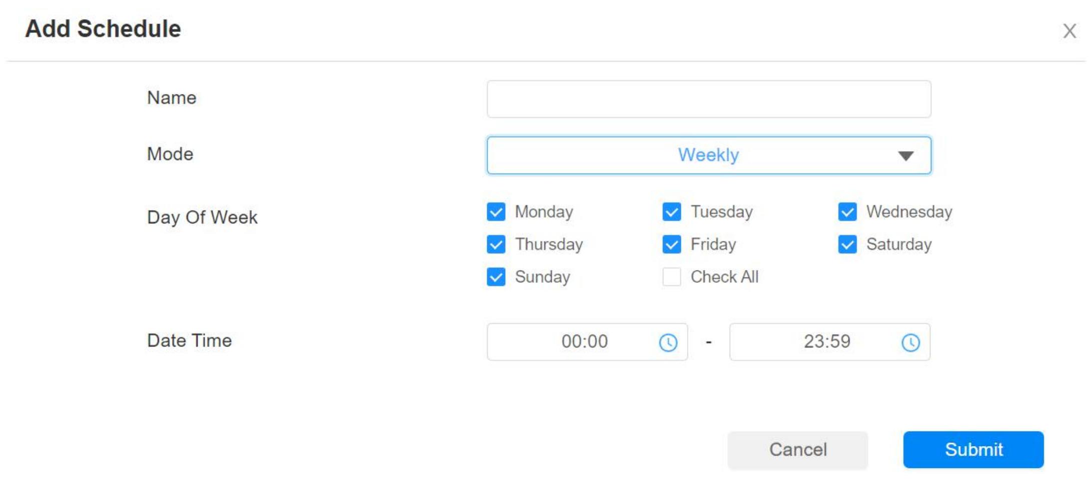
Add Schedule

Name

Mode: Daily

Date Time: 00:00 - 23:59

Click **+ Add** to create a weekly schedule, select **Schedule Mode** as **Weekly**.



Add Schedule

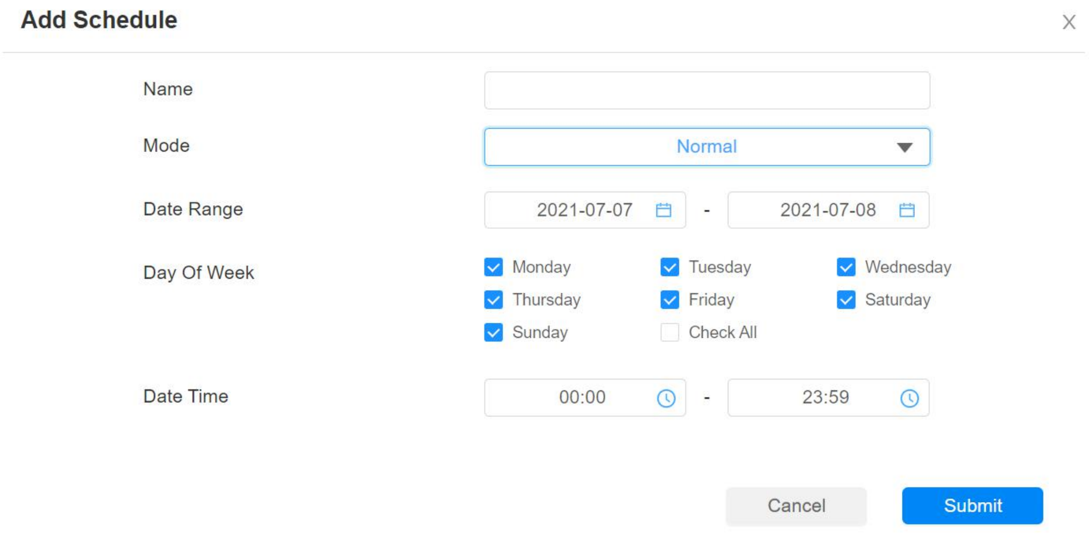
Name

Mode: Weekly

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

Date Time: 00:00 - 23:59

Click **+ Add** to create a longer period schedule, select **Schedule Mode** as **Normal**.



Add Schedule

Name

Mode: Normal

Date Range: 2021-07-07 - 2021-07-08

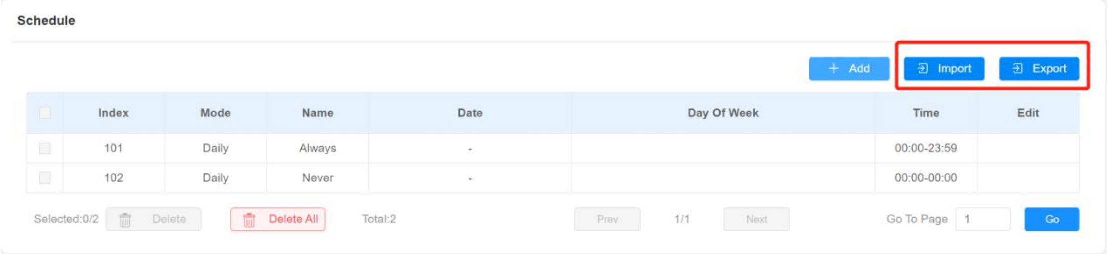
Day Of Week:
☑ Monday ☑ Tuesday ☑ Wednesday
☑ Thursday ☑ Friday ☑ Saturday
☑ Sunday □ Check All

Date Time: 00:00 - 23:59

Cancel Submit

11.1.2.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 configure the configuration on web **Directory > Schedule** interface.

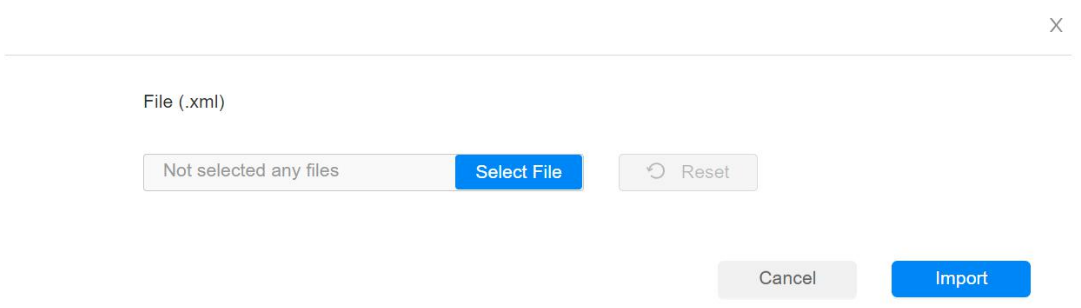


Schedule

+ Add Import Export

□	Index	Mode	Name	Date	Day Of Week	Time	Edit
□	101	Daily	Always	-		00:00-23:59	
□	102	Daily	Never	-		00:00-00:00	

Selected:0/2 Delete Delete All Total:2 Prev 1/1 Next Go To Page 1 Go



File (.xml)

Not selected any files Select File Reset

Cancel Import

Note:

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

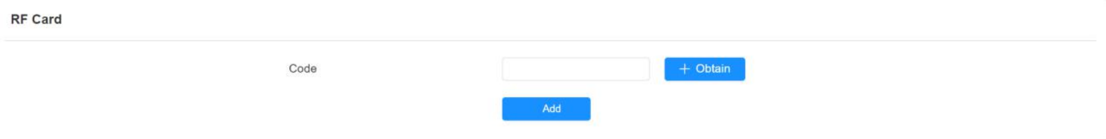
12. Door Unlock Configuration

A01S access control terminal offer you three types of door access via RF card. You can configure them on web interface. Moreover, you can import or exporting the user configured files including access control information.

12.1.Configure RF Card for Door Unlock

12.1.1.Configure RF Card on the Web Interface

To configure the configuration on web **Directory > User > RF Card** interface. You need to click **+Add** tab to turn to **RF Card** interface.

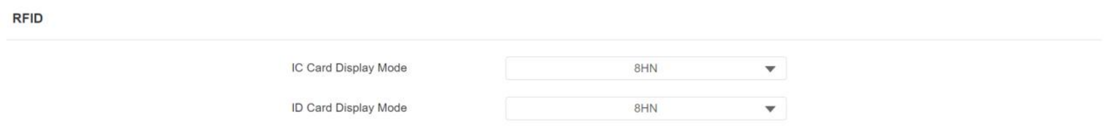

RF Card

Code

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

12.1.1.1. 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 configure the configuration on web **Hardware > Card Reader** interface.


RFID

IC Card Display Mode: 8HN

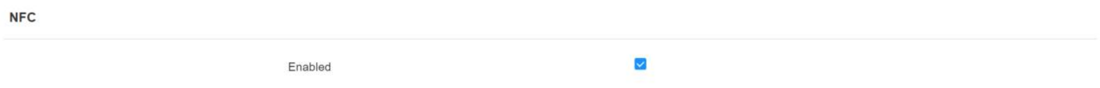
ID Card Display Mode: 8HN

Parameter Set-up:

- **IC/ID 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.

12.1.2. Unlock by NFC

NFC(Near Field Communication) is popular way for door access. It uses radio waves for data transmission interaction. A0X supports to be unlocked by NFC. You can keep the mobile phone closer to the door phone for the door access. To configure the configuration on web **Hardware > Card Reader > NFC** interface.



NFC

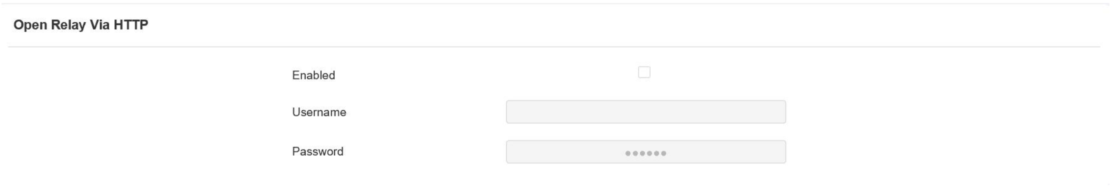
Enabled ☑

Note:

- NFC feature is only supported by Android telephone.

12.1.3. 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 configure the configuration on web **Hardware > Relay > Open Relay Via HTTP** interface.



Open Relay Via HTTP

Enabled □

Username

Password ••••••

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:

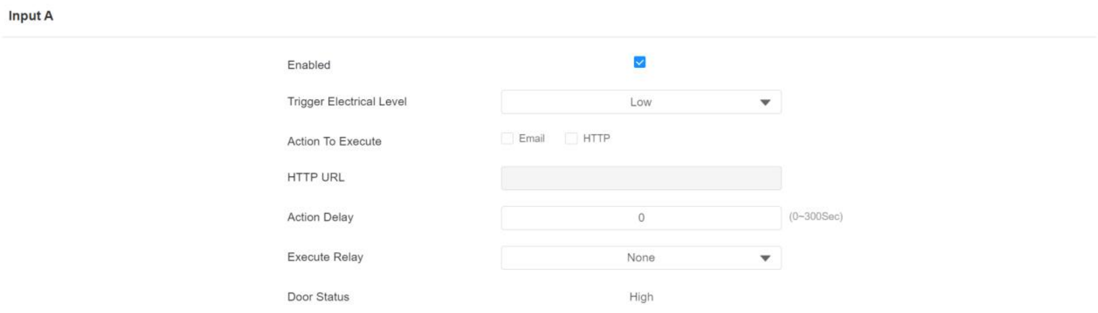
http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note:

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

12.1.4. Unlock by Exit Button

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



Input A

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

Parameter Set-up:

- **Trigger Electrical Level:** select the trigger electrical level options between “**High**” and “**Low**” according to the actual operation on the exit button.

- **Action to execute:** set actions to be triggered by the input. Email and HTTP URL actions are supported.

- **HTTP URL**: to set HTTP URL.

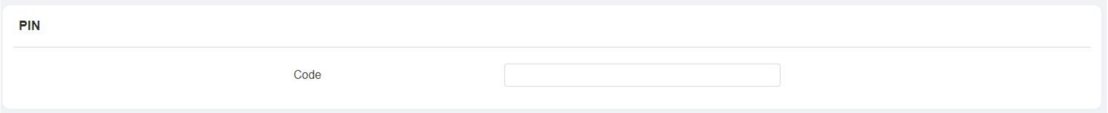
- **Action Delay:** set the action delay timing (Ranging from 1-300 Sec.) For example, if you set the delay time as "5". then the action will not be triggered until 5 seconds after input status changed.

- **Execute Relay:** set up relays to be triggered by the input.

- **Door Status:** display the status of input signal.

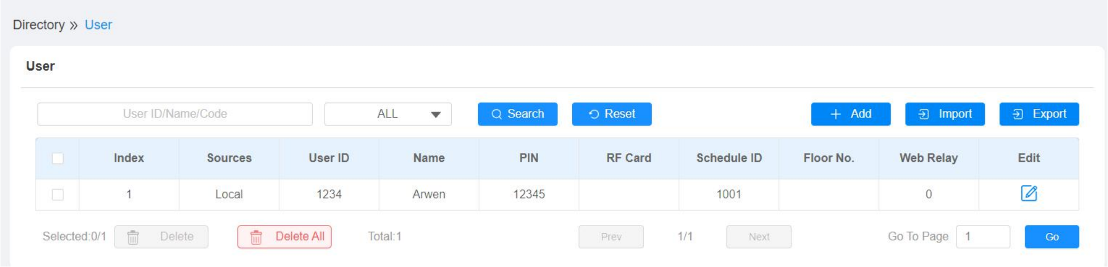
12.1.5. Unlock by PIN Code

A02S supports open the door via pin code.You can set up PIN code on the **Directory>User,** click **Add**, then input the private code.



PIN

Code:



□	Index	Sources	User ID	Name	PIN	RF Card	Schedule ID	Floor No.	Web Relay	Edit
□	1	Local	1234	Arwen	12345		1001		0	✎

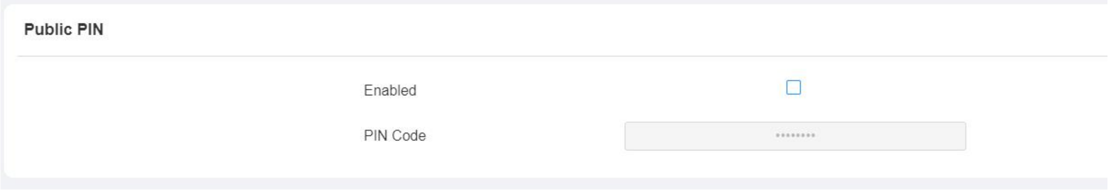
Parameter Set-up:

- **Code:** input the private code.(The code should contain 2-8 digits.)

After the configuration, PIN will be displayed on the user interface.

12.1.6. Unlock by Public Code

A02S supports public pin code for administrators or cleaners to open the door.You can set up public pin code on **Hardware>Relay>Public PIN interface.**



Public PIN

Enabled □

PIN Code ••••••••

Parameter Set-up:

- **Enabled:** click the checkbox to enable the public pin code.
- **PIN Code:** input the public pin code.(The code should contain 2-8 digits.)

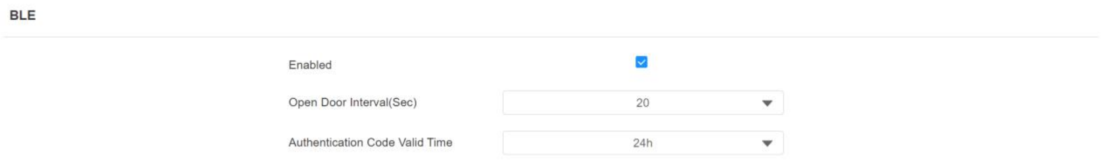
12.1.7. Unlock by Bluetooth

You can also gain door access by mobile phone with Bluetooth which is used together with Akuvox MobileKey App now. You can use the mobile phone closer to the access control terminal with hand-free mode for the door access..

Note:

- Only supports this feature.
- You can download the App from Google Play or App Store.
- Please refer to https://youtu.be/2ji9fQfxu2M and https://youtu.be/GvBvyXRDhh4 about using this feature.

You can enable BLE on **Hardware>BLE.**



BLE

Enabled ☑

Open Door Interval(Sec) 20

Authentication Code Valid Time 24h

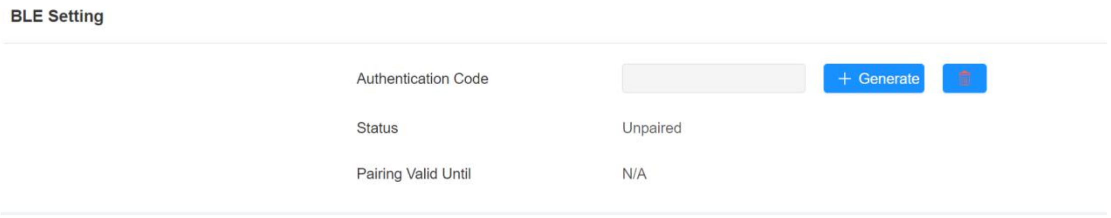
Parameter Set-up:

- **Enabled:** this feature is enabled by default. You can disabled it if it is unnecessary.
- **Open Door Interval(Sec):** select the time interval between the every two

Bluetooth door accesses.

- **Authentcation Code Valid Time:** for the security, you can setup the authentication code valid time to avoid codes being paired indefinitely. The time can be set up from 1h to 24h.

You can set up on **Directory>User,** click **Add** to enter BLE Setting interface.



BLE Setting

Authentication Code

Status: Unpaired

Pairing Valid Until: N/A

Parameter Set-up:

- **Authentication Code:** click **Generate** to create a paring code for the App. The app will using this code to match with .

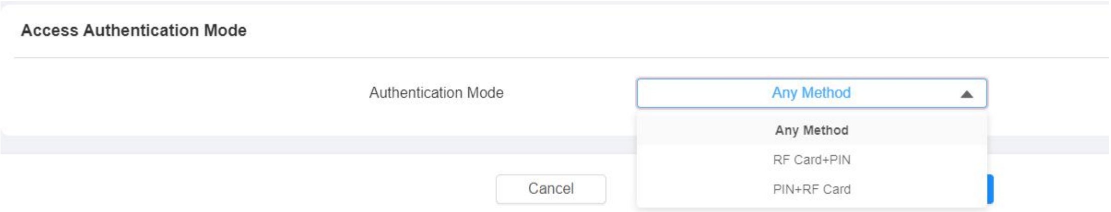
- **Status:** Shows whether the current authentication code has been paired with the app.

- **Paring Valid Until:** display the current pairing validity period of this code.

12.2. Access Authentication Mode

12.2.1. Access Authentication Mode Configuration

A02S supports dual access authentication mode. You can set up the dual access authentication mode on **Hardware > Relay> Access Authentication Mode interface.**



Access Authentication Mode

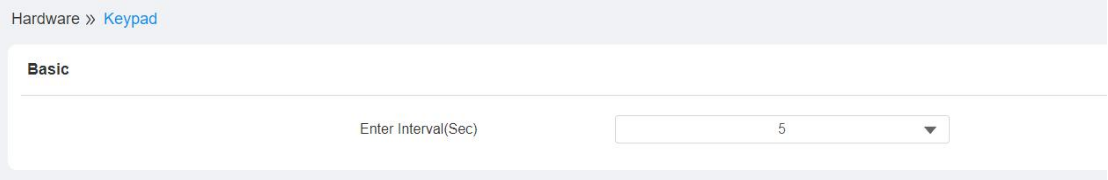
Authentication Mode: Any Method

Parameter Set-up:

- **Authentication Mode**: “Any Method” indicates RF card or PIN code.”RF Card+PIN” means swiping the card first then input the PIN code. “PIN+RF Card” means input the PIN code, then swipe the card.

12.2.2. Dual Authentication Interval

You can set up the interval time for dual access authentication on **Hardware > Keypad > Basic** interface.



Enter Interval(Sec) 5

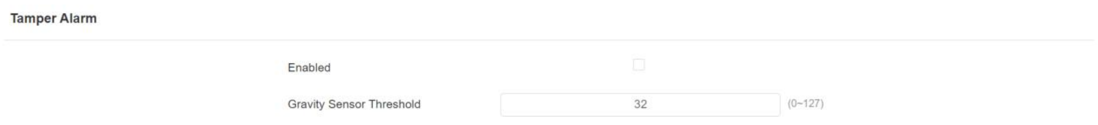
Parameter Set-up:

- **Enter Interval(Sec):** set up the interval time from 1 to 10 seconds.For example, if you set the interval time as 5 seconds, then the interval between the two access authentication must be limited within 5 seconds.

13. Security

13.1.Tamper Alarm Setting

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



Tamper Alarm

Enabled □

Gravity Sensor Threshold 32 (0~127)

Parameter Set-up:

- **Enable**: tick the check box to enable the tamper alarm function. When the tamper 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.

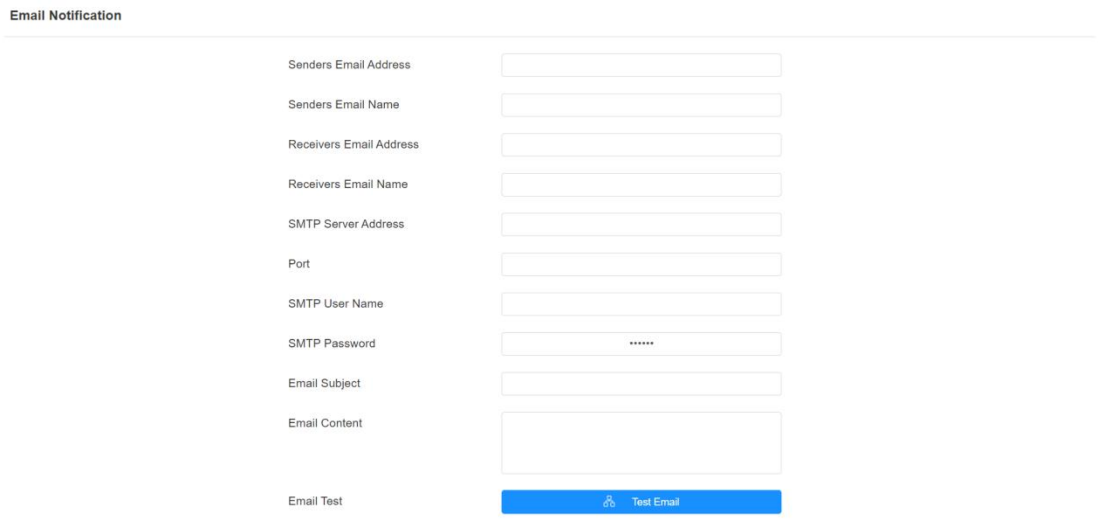
Note:

- **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.

13.2.Security Notification Setting

13.2.1.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 configure the configuration on web **Services > Action > Email Notification** interface.



Email Notification

Senders Email Address	
Senders Email Name	
Receivers Email Address	
Receivers Email Name	
SMTP Server Address	
Port	
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	
Email Test	Test Email

Parameter Set-up:

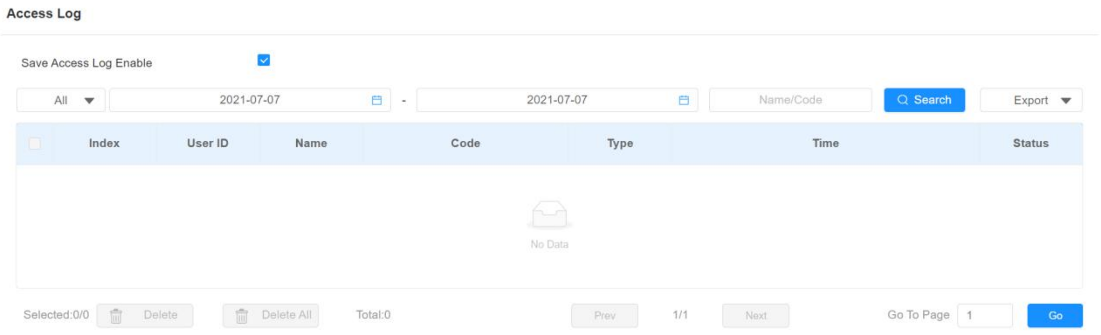
- **Sender's Email Name:** enter the name of the email sender.
- **Sender's email address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's email address:** enter the receiver's email address.
- **Receiver's Email Name:** enter the name of the email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

- **SMTP server address:** enter the SMTP server address of the sender.
- **Port:** enter the port number from which the email is sent out.
- **SMTP user name:** enter the SMTP user name, which is usually the same with sender's email address.
- **SMTP password:** configure the password of SMTP service, which is same with sender's email address.
- **Email subject:** enter the subject of the email.
- **Email content:** compile the emails contents according to your need.

14. Logs

14.1.Access Log

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



Access Log

Save Access Log Enable ☑

All ▾ | 2021-07-07 - 2021-07-07 | Name/Code | Search | Export ▾

□	Index	User ID	Name	Code	Type	Time	Status

No Data

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

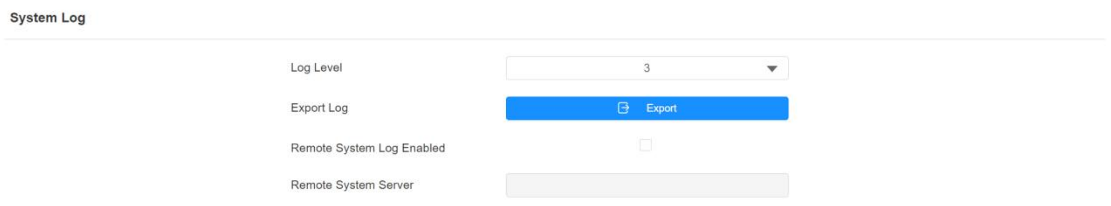
Parameter Set-up:

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

15. Debug

15.1.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 **System > Maintenance > System Log** interface.



System Log

Log Level	3
Export Log	Export
Remote System Log Enabled	□
Remote System Server	

Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is **3**, the higher the level is **5**, the more complete the log is **7**.

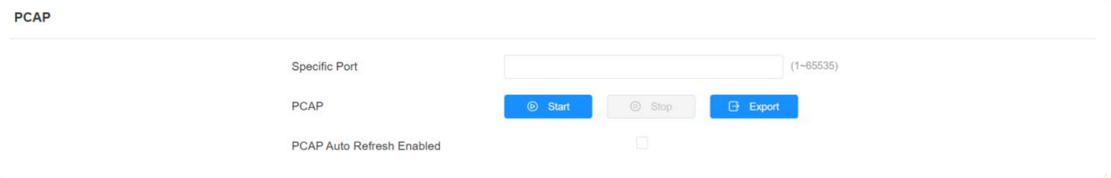
- **Export Log**: click the **Export** tab to export temporary debug log file to a local PC.

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

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

15.2.PCAP for Debugging

PCAP in A01S access control terminal is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **System > Maintenance > PCAP** interface properly before using it.



Parameter Set-up:

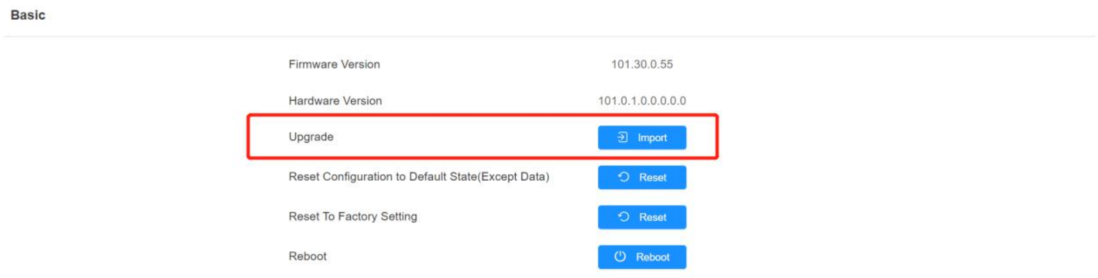
- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.

- **PCAP**: click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.

- **PCAP Auto Refresh Enabled**: 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.

16. Firmware Upgrade

Firmware of different versions for A01S access control terminal can be upgraded on the device web **System > Upgrade** interface.



Basic

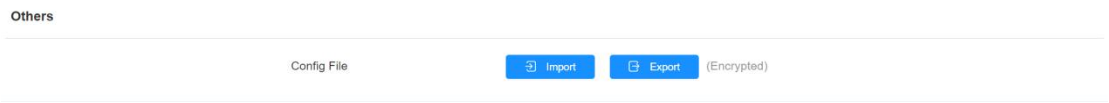
Firmware Version	101.30.0.55
Hardware Version	101.0.1.0.0.0.0.0
Upgrade	Import
Reset Configuration to Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

Note:

- Firmware files should be .rom format for upgrade.

17. Backup

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

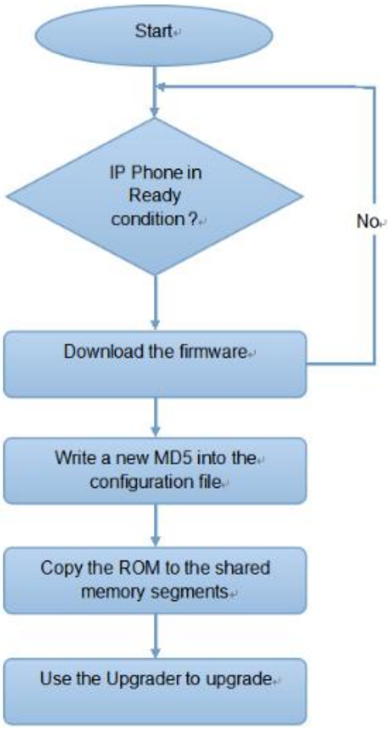


18. Auto-provisioning

Configurations and upgrading on A01S 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.

18.1.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 firmware, which will then be used to update the firmware and the corresponding parameters on the access control terminal.


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

18.2. 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.

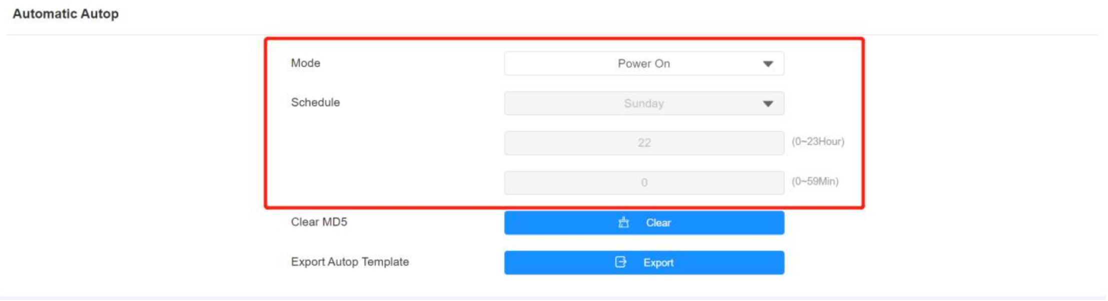
- **MAC-based configuration provisioning**: MAC-based configuration files is used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded 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.

18.3.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 configure the configuration on web **System > Auto Provisioning > Automatic Autop** interface.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

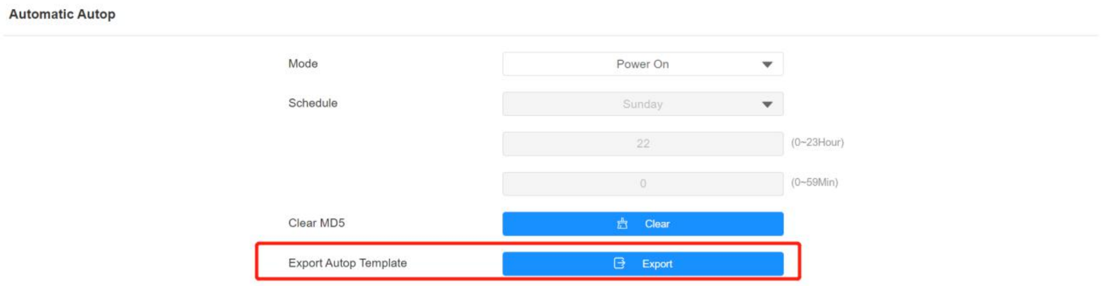
Export Autop Template: Export

Parameter Set-up:

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

18.4.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 want 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. And export Autop Template to edit the configuration. Then set up DHCP Option on **System > Auto Provisioning > DHCP Option** interface.



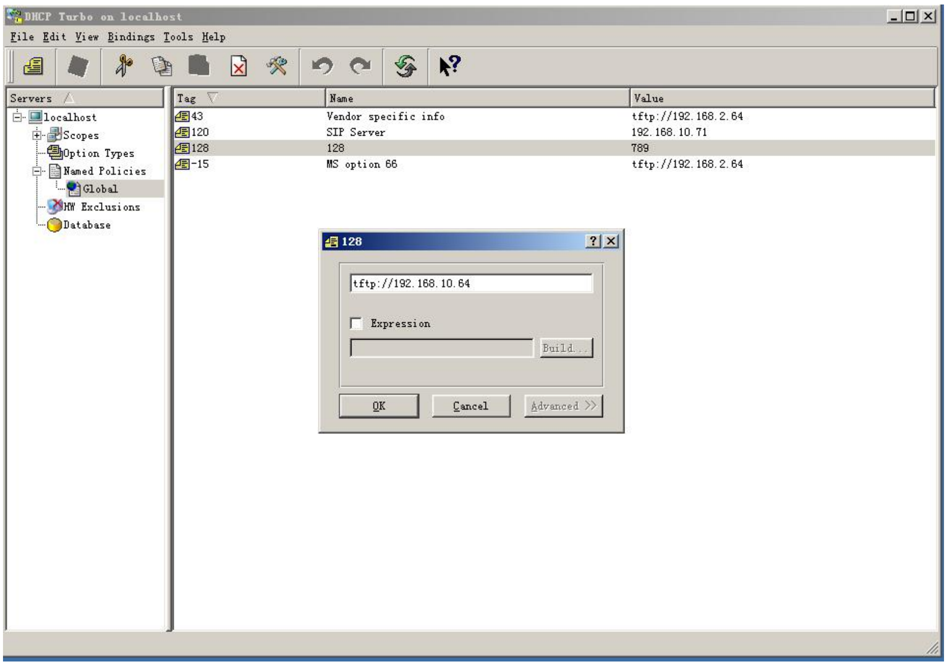
Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)



DHCP Turbo on localhost

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

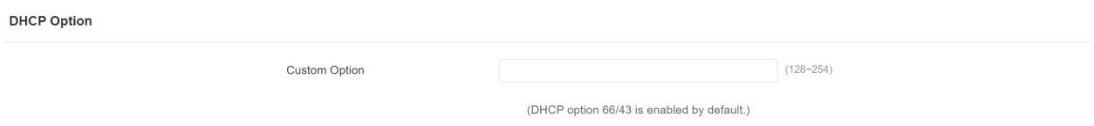
128

tftp://192.168.10.64

□ Expression

Note:

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


DHCP Option

Custom Option (128~254)

(DHCP option 66/43 is enabled by default.)

Parameter Set-up:

- **Custom Option**: enter the DHCP code that matched with 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.

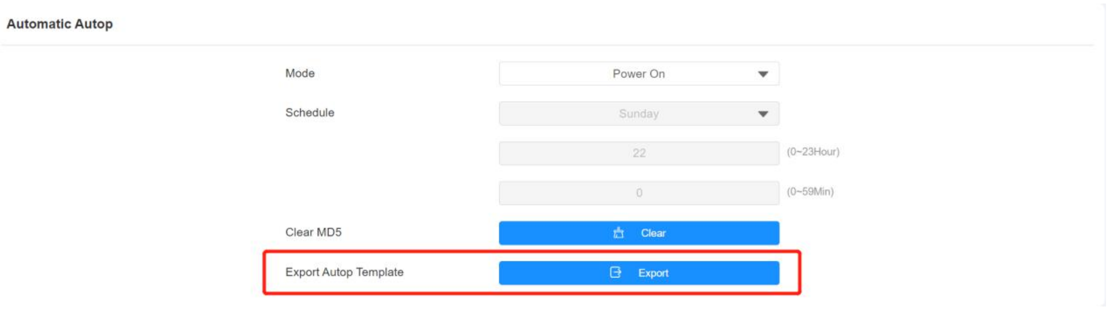
- **DHCP Option 43:** If the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for the option 43 with the update server URL in it.

Note:

- The general configuration file for the in-batch provisioning is with the format "r**0000000000xx.cfg**" taking A01S as an example "r000000000101.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."**

18.5.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 download the Autop template first and setup Autop server on **System > Auto Provisioning > Manual Autop** interface.



Automatic Autop

Mode: Power On

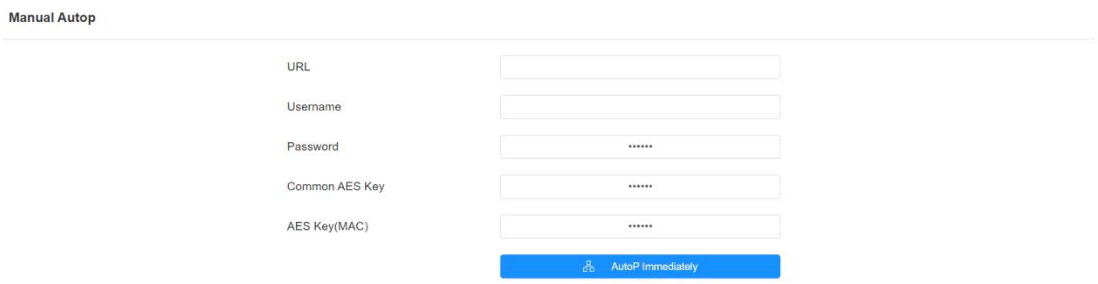
Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export



Manual Autop

URL:

Username:

Password: ••••••

Common AES Key: ••••••

AES Key(MAC): ••••••

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)

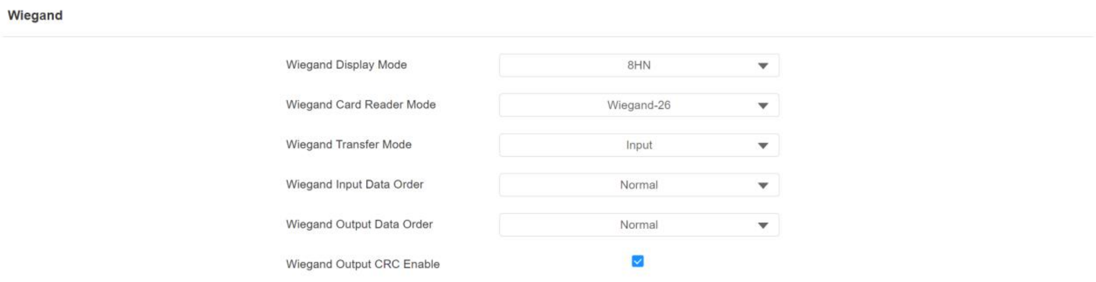
Tip:

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

19. Integration with Third Party Device

19.1.Integration via Wiegand

If you want to integrate the A01S access control terminal with the third-party devices via Wiegand, you can configure the Wiegand on the web **Hardware > Wiegand** interface.



Wiegand

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

Parameter Set-up:

- **Wiegand Display Mode：** select Wigand Card code format among **8H10D**; **6H3D5D**; **6H8D**; **8HN**; **8HR**; **RAW**.

- **Wiegand Card Reader Mode:** set the Wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **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.

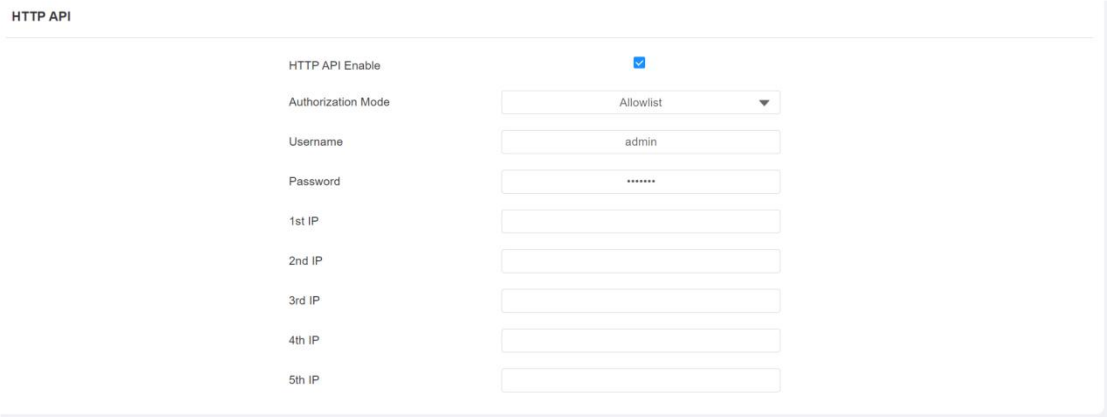
- **Wiegand Input Data Order**：set the Wiegand input data sequence between **Normal** and **Reversed** if you select **Reversed** then the input card number will be reversed an vice versa**.**

- **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 Enable:** tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.

19.2. Integration via HTTP API

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



HTTP API

HTTP API Enable	☑
Authorization Mode	Allowlist
Username	admin
Password	•••••••
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

Parameter set-up:

- **HTTP API:** select “**Enable**” or “ **Disable** “ to enable or disable the HPTT API function for the third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.

- **Auth Mode:** select among four options: **“None” “ WhiteList” “ Basic”,**

" **Digest"** for authorization type, which will be explained in detail in the following chart.

- **User Name:** enter the user name when "**Basic**" and **"Digest**" authorization mode is selected. The default user name is "Admin".

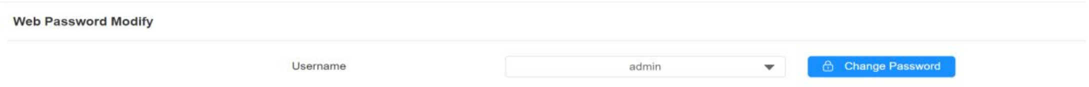
- **Password:** enter the password when "**Basic**" and **"Digest**" authorization mode is selected. The default user name is "Admin".

- **IP01-IP05:** enter the IP address of the third party devices when the "WhiteList" authorization is select for the integration.

20. Password Modification

20.1.Modify the Password

On the device web interface, you can set and change password for accessing the web **System > Security > Web Password Modify** interface. In addition, you can also select the user role when setting passwords.

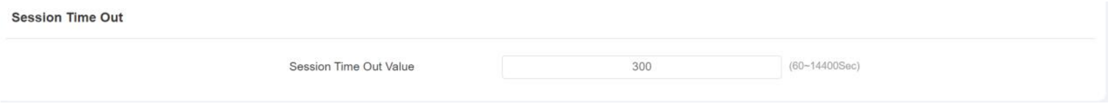


Web Password Modify

Username: admin

20.2.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 configuration on web **System > Security > Session Time Out** interface.



Session Time Out

Session Time Out Value: 300 (60~14400Sec)

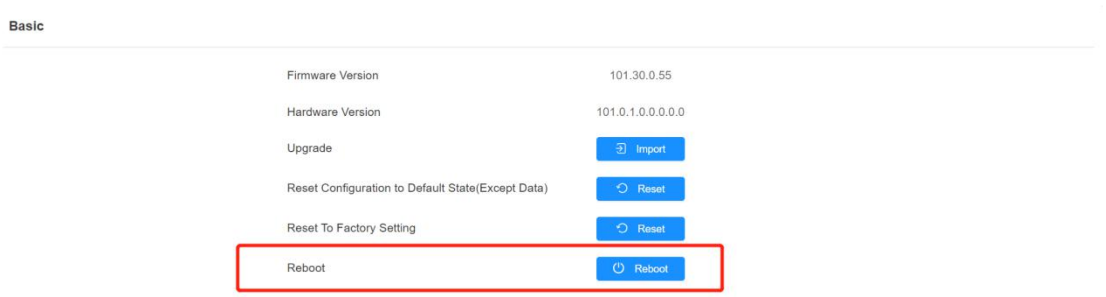
Parameters Set-up:

- **Session Time Out Value:** if there is no operation over the time, you need to login the website again.

21. System Reboot and Reset

21.1.Reboot

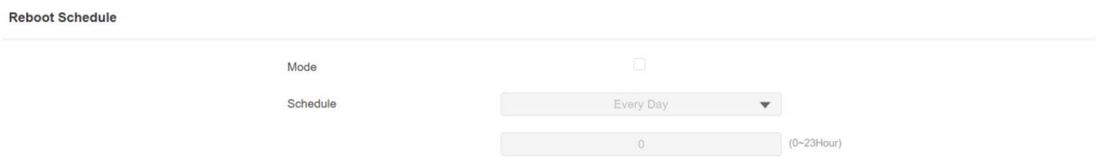
If you want to restart the device, you can operate it on the device web **System > Upgrade > Basic** interface as well. Moreover, you can set up schedule for the device to be restarted.



Basic

Firmware Version	101.30.0.55
Hardware Version	101.0.1.0.0.0.0.0
Upgrade	Import
Reset Configuration to Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

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

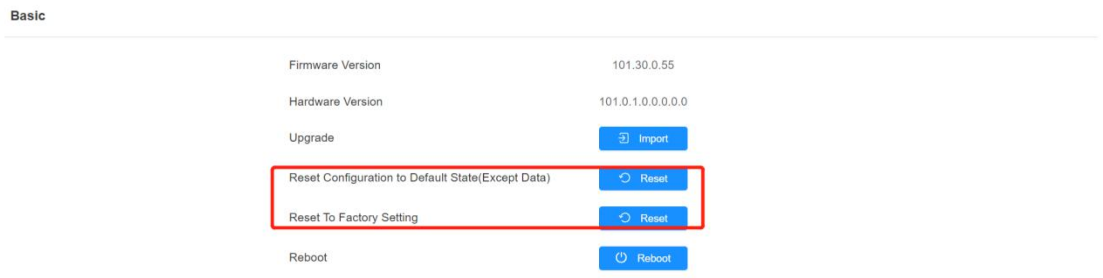


Reboot Schedule

Mode	□
Schedule	Every Day
	0 (0~23Hour)

21.2.Reset

If you want to reset the device system to the factory setting, you can it on the web **System > Upgrade** interface. You can also hold the reset button 12s on the back of A01S to reset.



Basic

Firmware Version	101.30.0.55
Hardware Version	101.0.1.0.0.0.0.0
Upgrade	Import
Reset Configuration to Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

22. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatic Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation µ-Law

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

23. FAQ

Q1: How to obtain IP address of access control terminal?
A1: Using Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: What is the supported temperature range for A01S ?
A2: Working Temperature: -20°C ~ +55°C
Storage Temperature: -30° C ~ +70° C

Q3: Do Akuvox devices support Modbus protocol?
A3: No.

Q4: Do access control terminals support these card types? Prox, Legacy iClass, iClassSE, HID Mifare, HID DESFire, and HID SEOS
A4: Sorry, they are not supported. They need to be implemented via hardware modifications.

24. 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.