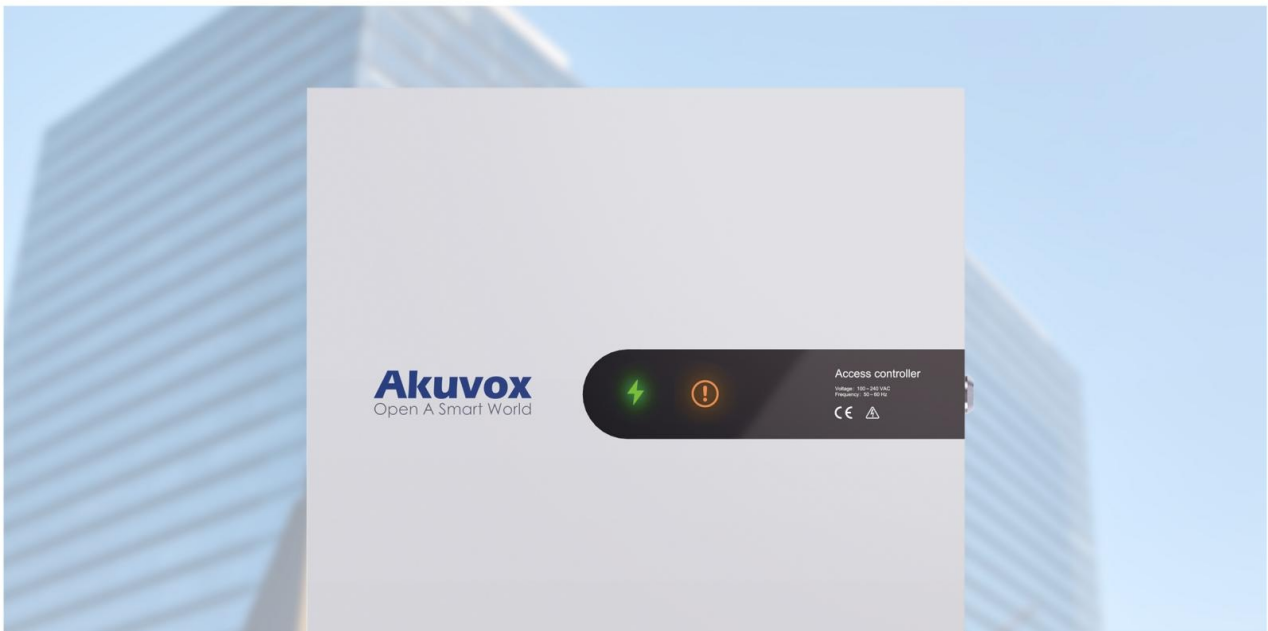


About This Manual



WWW.AKUVOX.COM



A094 SERIES ACCESS CONTROLLER


Administrator Guide

Thank you for choosing the Akuvox A094 access controller. This manual is intended for administrators who need to properly configure the access controller. This manual is written based on firmware version: 92.30.10.4, and it provides all the configurations for the functions and features of the access controller. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

The Akuvox A094 is a Linux-based access controller with multiple ports, including RS485 and Wiegand ports for seamless integration with external digital systems like card readers, elevator controllers, and fire alarm detectors. It features four built-in relays, allowing it to control a maximum of four doors and providing secure card access. The A094 is suitable for applications in commercial buildings, hospitals, and warehouses, offering comprehensive control of building entrances and surroundings.

Model Specification

Specification	A094
	
Operation System	Linux
Material	Galvanized steel
Installation	Wall-mounting
Relay	8 relays
Wiegand	4 Wiegand interface
Input	13 inputs
Ethernet	1x10/100M RJ45 interface
RS485	6 RS485 Interface
Working Power	12V
Power input	100-240VAC
Back Power Supply	Battery
Power output	12VDC 800mA x 4
Indicator	Power Indicator/ Ethernet indicator
Speaker	Inbuilt Speaker

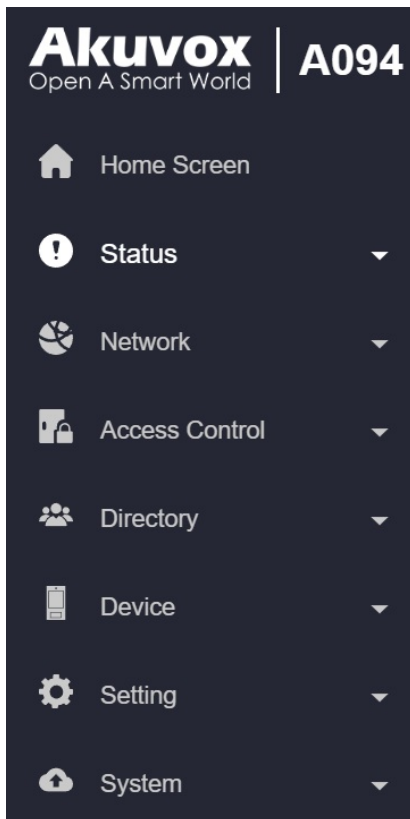
RAM	64MB
ROM	128MB
RTC	√
Reset	√
Work temperature	-10°C ~ +55°C
Storage temperature	-20°C ~ +70°C
Certification	CE/FCC

Indicator

Indicator Type	Color	Status	Description
Power Indicator	Green	ON	The power is on.
Warning Indicator	Orange	OFF	The power is off.
		ON	Failed to obtain the IP address.
		OFF	The device is in normal status.
		Flashing slowly	Device upgrade fails.
		Flashing quickly	The device is being upgraded.

Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, and access logs.
- **Network:** This section covers LAN port settings.
- **Access Control:** This section covers relay, input, web relay, card setting, etc.
- **Directory:** This section includes access schedule management and user management.
- **Device:** This section includes Wiegand and RS485 settings.
- **Setting:** This section deals with time, relay schedule, action, HTTP API settings, etc.
- **System:** This section covers firmware upgrade, device reset, reboot, configuration file auto-provisioning, system log and PCAP, password modification as well as device backup.

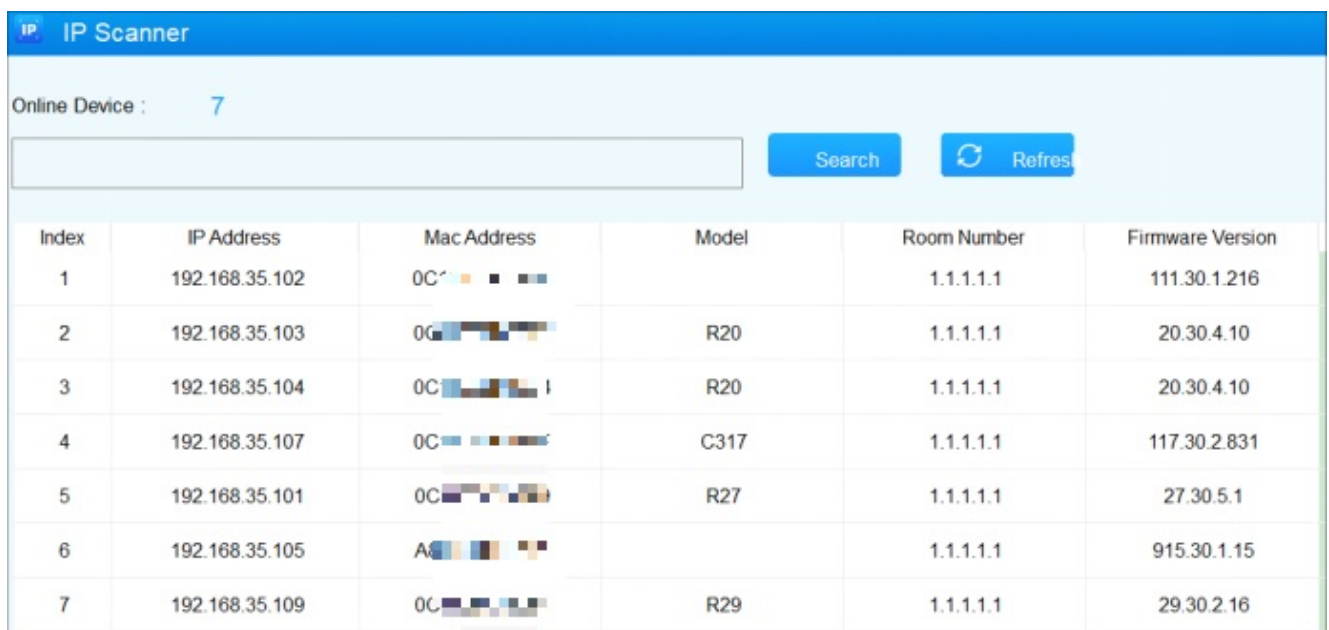


Access the Device

Akuvox A094 access controller system settings can be accessed on the device web interface.

Obtain Device IP Address

Before configuring the device, please make sure the device is installed correctly and connected to a normal network. Using the Akuvox IP scanner tool to search the device IP address in the same LAN.

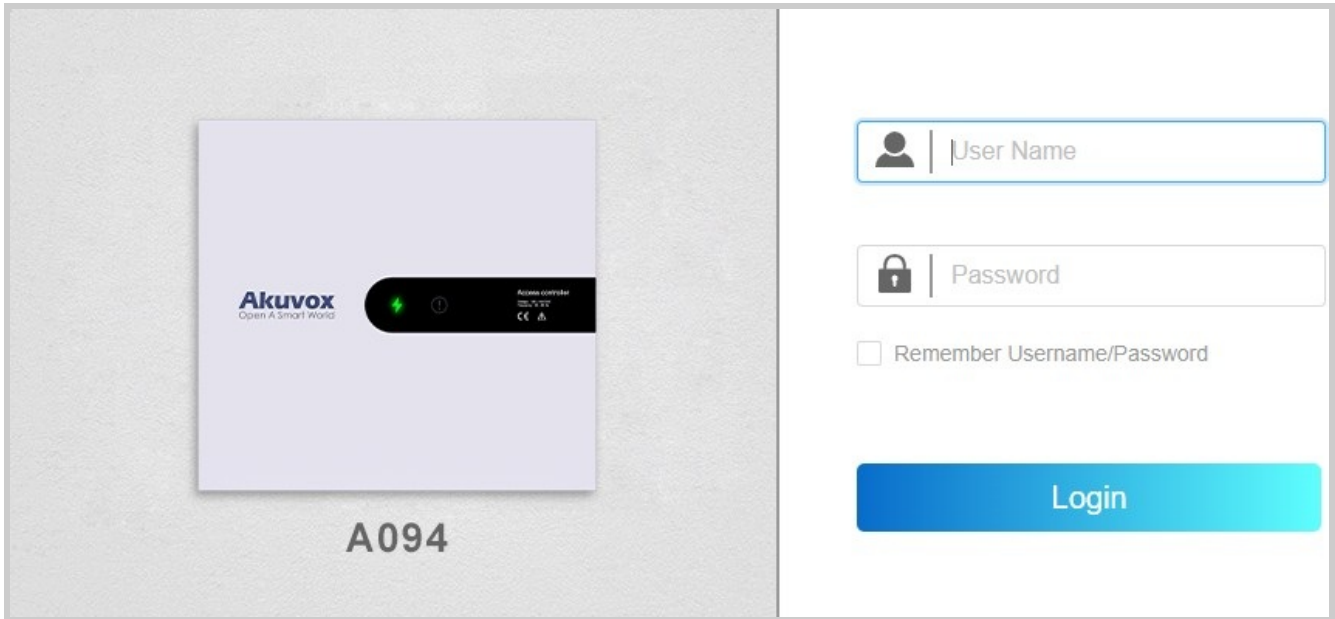


The screenshot shows the 'IP Scanner' web interface. At the top, it indicates 'Online Device : 7'. Below this is a search input field, a 'Search' button, and a 'Refresh' button. The main content is a table with the following columns: Index, IP Address, Mac Address, Model, Room Number, and Firmware Version. The table contains 7 rows of data.

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C...		1.1.1.1	111.30.1.216
2	192.168.35.103	0C...	R20	1.1.1.1	20.30.4.10
3	192.168.35.104	0C...	R20	1.1.1.1	20.30.4.10
4	192.168.35.107	0C...	C317	1.1.1.1	117.30.2.831
5	192.168.35.101	0C...	R27	1.1.1.1	27.30.5.1
6	192.168.35.105	A...		1.1.1.1	915.30.1.15
7	192.168.35.109	0C...	R29	1.1.1.1	29.30.2.16

Access the Device Web Interface

Enter the device IP address on the web browser to log in to the device web interface where you can set up features. The initial user name and password are **admin** and please be case-sensitive to the user names and passwords entered.



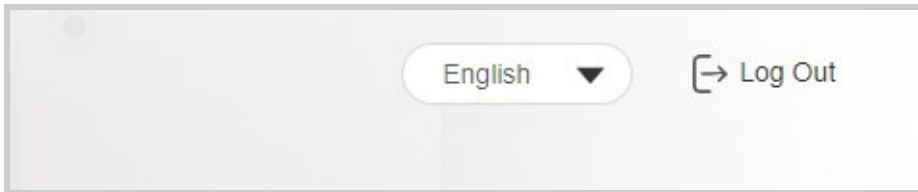
Note

- Download IP scanner:
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- See detailed guide:
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Google Chrome browser is strongly recommended.

Language and Time Setting

Language Setting

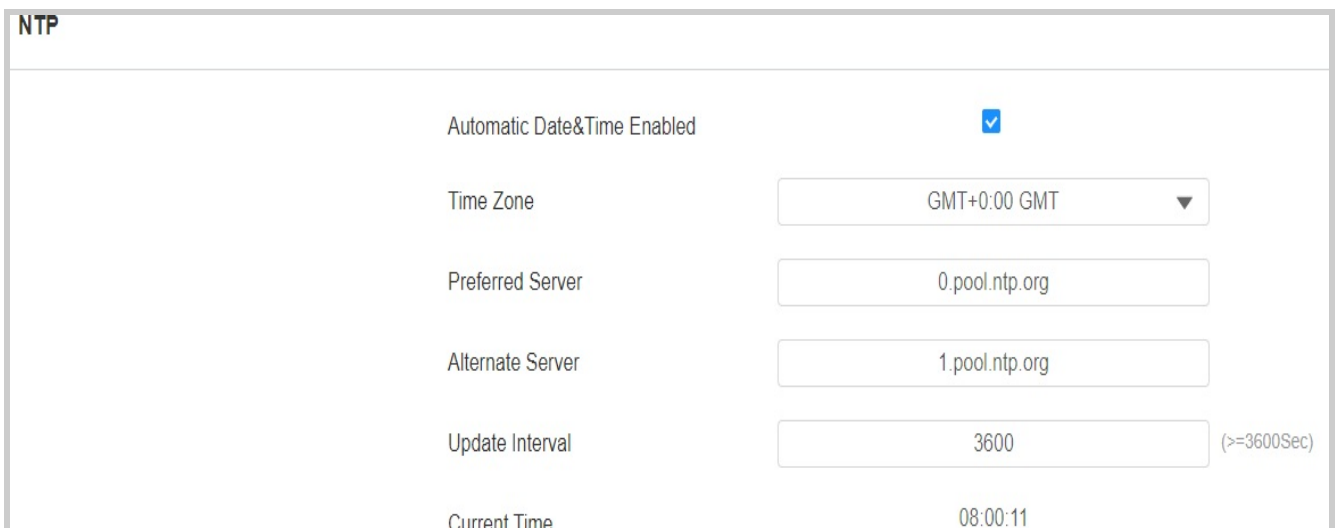
You can select the web language in the upper right corner. Currently, the A094 supports English and Simplified Chinese.



Time Setting

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

To set it up, navigate to the web **Setting > Time > NTP** interface.



- **Time Zone:** Set whether the device updates the time automatically via the Network Time Protocol(NTP) server.
- **Primary/Alternate Server:** Enter the primary NTP server address for updating the time. The default NPT server address is 0.pool.ntp.org. The alternate server is for backup.

- **Update Interval:** Set the time update interval. For example, if you set it as 3600s, the device will send a request to the NTP server for the time update every 3600 seconds.
- **Current Time:** Display the current device time.

Network Configuration

Network Status

Check the network status on the web **Status > Info** interface.

Network Information	
Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.117
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8

Device Network Configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the DHCP server.

To set it up, go to **Network > Basic** interface.

LAN Port	
	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text" value="192.168.2.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.2.1"/>
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Alternate DNS Server	<input type="text"/>

- **DHCP:** DHCP mode is the default network connection. If the DHCP mode is selected, 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**: When static IP mode is selected, the IP address, subnet mask, default gateway, and DNS server address should be configured according to the network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected.
- **Subnet Mask**: Set up the subnet mask according to the actual network environment.
- **Default Gateway**: Set up the correct gateway according to the IP address.
- **Preferred/Alternate DNS Server**: Set up the preferred or alternate Domain Name Server(DNS) server according to the actual network environment. The preferred DNS server is the primary server while the alternate DNS server is the secondary one. The secondary server is for backup.

Web Server

This function manages device website access. The access controller supports two remote access methods: HTTP and HTTPS (encryption).

Set it up on the web **Network > Advanced > Web Server** interface.

Web Server		
Protocol	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> HTTPS
HTTP Port	<input type="text" value="80"/>	(80,1024~65535)
HTTPS Port	<input type="text" value="443"/>	(443,1024~65535)

- **Protocol**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

TR069

TR-069 (Technical Report 069) provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. For door phones, the administrators can manage all the devices on a common TR-069 Platform. IP phones can be easily and securely configured on the TR-069 platform to make mass deployment more efficient.

To set it up, navigate to the web **Network > Advanced > TR069** interface.

The screenshot shows the TR069 configuration page with the following fields:

Active	<input type="checkbox"/>
Version	1.0
ACS URL	
User Name	
Password	*****
Periodic Inform	<input type="checkbox"/>
Periodic Interval	1800 (3~24x3600s)
CPE URL	
User Name	
Password	*****

- **Version:** Select the TR069 version.
- **ACS URL:** Set the URL of the ACS server, for example, <http://192.168.1.47:8080/openacs/acs>
- **User Name:** Set the ACS server username for authentication.
- **Password:** Set the ACS server password for authentication.
- **Periodic Inform:** Allow the device to send requests to the ACS server for automatic configuration and update.
- **Periodic Interval:** Set the time interval for the device to send the request to the ACS server for the automatic configuration and update.
- **CPE URL:** Set the device URL, for example, <http://192.168.1.48:8882/>
- **User Name:** Set the device authentication username.
- **Password:** Set the device authentication password.

SNMP

Simple Network Management Protocol(**SNMP**) is a protocol for managing IP network devices. It allows network administrators to monitor devices and receive alerts for attention-worthy conditions. SNMP provides variables describing system configuration, organized in hierarchies and described by Management Information Bases (MIBs).

To set it up, navigate to the web **Network > Advanced> SNMP** interface.

SNMP	
Active	<input type="checkbox"/>
Port	<input type="text" value="1024-65535"/>
Trusted IP	<input type="text"/>

- **Port:** Set a specific port for the data transmission from 1024-65535.
- **Trusted IP:** Enter the third-party IP address.

Relay Setting

Built-in Relays

The A094 access controller has eight built-in relays in total. Two of the first four relays are on the mainboard and the other two are on the expanded board. And the rest of the four auxiliary relays(Output A, B, C, D) are on the expanded board. You can connect relays to electrical door locks for the door access control.

Set up relays on the web **Access Control > Relay** interface.

Relay	Relay1	Relay2	Relay3	Relay4
Type	DefaultState	DefaultState	DefaultState	DefaultState
Mode	Monostable	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0	0
Hold Delay(Sec)	3	3	3	3
Relay Status	Relay1: Low	Relay2: Low	Relay3: Low	Relay4: Low
Trigger Output	None	None	None	None

- **Type:** Determine the interpretation of the Relay Status regarding the state of the door:
 - **Default State:** A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.
 - **Invert State:** A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.
- **Mode:** Specify the conditions for automatically resetting the relay status.
 - **Monostable:** The relay status resets automatically within the relay delay time after activation.
 - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec):** Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after it is triggered.
- **Hold Delay(Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.

- **Relay Status:** Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).

A094 has four extra relays which can be triggered by some devices such as a smoke sensor to carry our preset actions like setting off alarms or turning on the light.

Set up the extra relays on the web **Access Control > Auxiliary Output** interface.

Output				
Output ID	Output A (Relay5)	Output B (Relay6)	Output C (Relay7)	Output D (Relay8)
Action Type	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼
Hold Delay(Sec)	5 ▼	5 ▼	5 ▼	5 ▼
Output Status	Low	Low	Low	Low

- **Hold Delay (Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **Output Status:** Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).

Web Relay

A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.



To set it up, navigate to the web **Access Control > Web Relay** interface.

Web Relay

Type	<input style="width: 100%;" type="text" value="Disabled"/>
IP Address	<input style="width: 100%;" type="text"/>
Username	<input style="width: 100%;" type="text"/>
Password	<input style="width: 100%;" type="password"/>

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 02	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 03	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 04	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 05	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 06	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 07	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

- **Type:** Determine the type of relay activated when employing door access methods for entry.
 - **Disabled:** Only activate the local relay.
 - **Web Relay:** Only activate the web relay.
 - **Both:** Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.

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

- **Username:** The user name provided by the web relay manufacturer.

- **Password:** The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.

- **Web Relay Action:** Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.
- **Web Relay Key:** The configured DTMF code. When the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.

Note

If the URL includes full HTTP content (e.g., `http://admin:admin@192.168.1.2/state.xml?relayState=2`), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., `state.xml?relayState=2`), the relay uses the entered IP address.

- **Web Relay Key:** Determine the methods to activate the web relay based on whether the DTMF code is filled.
 - Filling with the configured DTMF code restricts activation to card swiping and DTMF.
 - Leaving it blank enables all door-opening methods.
- **Web Relay Extension:** Specify the intercom device and the methods it can use to activate the web relay during calls.
 - When an intercom device's IP/SIP is specified, only that device can trigger the web relay (except for via card swiping or DTMF) during calls.
 - If left blank, all devices can trigger the relay during calls.

Door Access Schedule Management

A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Door Access Schedule

You can create door access schedules for daily, weekly, or custom time periods.

To set it up, navigate to the web **Setting > Schedule** interface. Click **+Add**.

The screenshot displays the 'Schedule' management interface. At the top, there are buttons for 'Search', '+ Add', 'Import', and 'Export'. Below this is a table with the following data:

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
1	1002	Local	Daily	Never	--	--	-	[Edit]
2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	[Edit]

Below the table are 'Delete' and 'Delete All' buttons, and pagination controls showing '1/1' items.

An 'Add Schedule' modal is open, showing the following fields:

- Mode:** Normal (dropdown)
- Name:** (text input)
- Start Date - End Date:** 20240401 ~ 20240402
- Day:**
 - Mon
 - Tue
 - Wed
 - Thur
 - Fri
 - Sat
 - Sun
 - Check All
- Start Time - End Time:** 00:00 - 23:59

Buttons for 'Cancel' and 'Submit' are at the bottom of the modal.

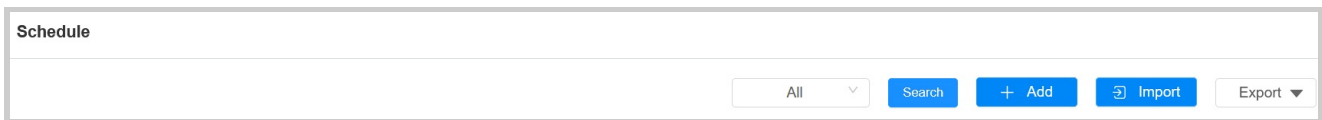
- **Name:** Name the schedule.
- **Mode:**
 - **Normal:** Set the schedule based on the month, week, and day. It is used for a long period schedule.

- **Weekly:** Set the schedule based on the week.
- **Daily:** Set the schedule based on 24 hours a day.

Import and Export Door Access Schedule

You can create door access schedules one by one or in bulk. You can export the current schedule file, edit it or add more schedules following the format, and import the new file to the desired devices. This helps you manage your door access schedules easily.

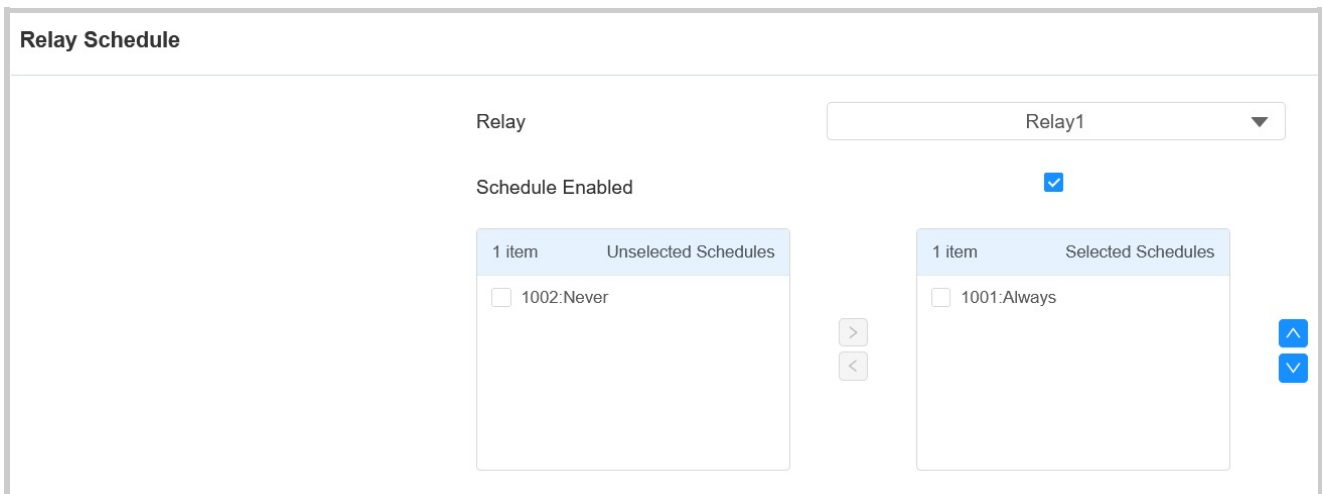
To set it up, go to the **Setting > Schedule** interface. The import and export files are in **XML** format.



Relay Schedule

The relay schedule allows you to set a specific relay to always open at a certain time. This is helpful for situations like keeping the gate open after school or keeping the door open during work hours.

To set it up, go to **Access Control > Relay > Relay Schedule** interface.



- **Relay ID:** Specify the relay you need to set up.
- **Schedule:** Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

For instructions on creating schedules, kindly consult the [Create Door Access Schedule](#) section.

Door Unlock Configuration

Unlock by Public PIN Code

The device supports public pin codes for administrators or cleaners to open the door.

To set up the public PIN code, go to **Access Control > Relay > Public PIN** interface.

Public PIN

Enabled

PIN Code (2-8 digit number)

- **PIN Code:** Set a 2-8 digit PIN code accessible for universal use.

User-specific Access Methods


The private PIN code and RF card should be assigned to a particular user for opening the elevator door.

When adding a user, you can also customize settings such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

To add a user, go to **Directory > User** interface and Click **+Add**.

User

All

<input type="checkbox"/>	Index	Source	User ID	Name	Private PIN	RF Card	Web Relay	Schedule-Relay	Edit
 No Data									

1/1

User Basic

User ID

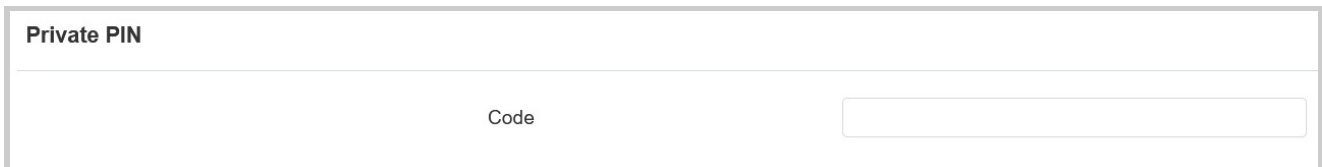
Name

- **User ID:** The unique identification number assigned to the user.

- **Name:** The name of this user.

Unlock by Private PIN Code

On the **Directory > User > +Add** interface, scroll to the **Private PIN** section.

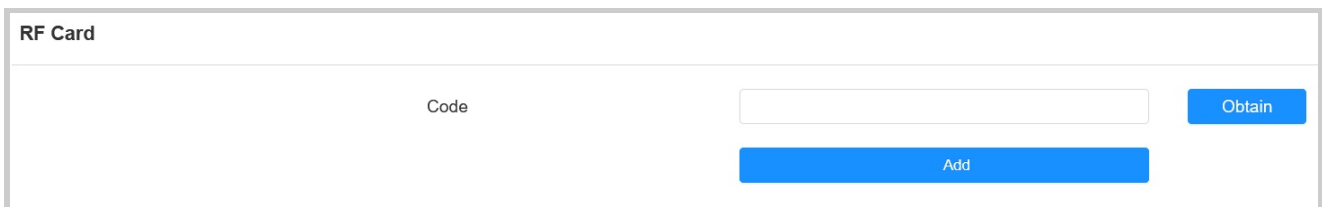


The screenshot shows a form titled "Private PIN". Below the title is a label "Code" followed by a text input field.

- **Code:** Set a 2-8 digit PIN code solely for the use of this user. Each user can only be assigned a single PIN code.

Unlock by RF Card

On the **Directory > User > +Add** interface, scroll to the **RF Card** section.



The screenshot shows a form titled "RF Card". Below the title is a label "Code" followed by a text input field. To the right of the input field is a blue button labeled "Obtain". Below the input field is a blue button labeled "Add".

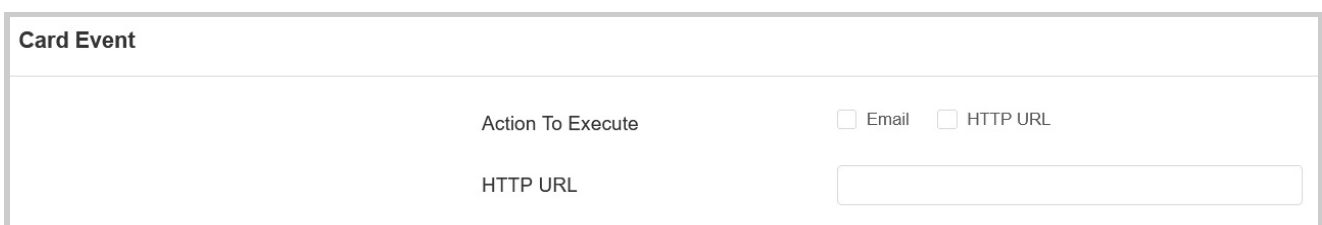
- **Code:** The card number that the card reader reads.

Note

- Each user can have a maximum of 5 cards added.
- The device allows to add 50,000 users.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the door phone for access.

Events Triggered by Using RF Cards

You can set up the events triggered by swiping the RF cards on the **Access Control > Card Setting** interface.



The screenshot shows a form titled "Card Event". Below the title is a label "Action To Execute" followed by two radio buttons: "Email" and "HTTP URL". Below the radio buttons is a label "HTTP URL" followed by a text input field.

- **Action to Execute:** Set the desired actions that occur when the door is opened by swiping the RF card.
 - **Email:** Send a message to the preconfigured [Email address](#).
 - **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL:** Enter the HTTP message if selecting HTTP as the action to execute. The format is [http://HTTP server's IP/Message content](#).

Access Setting

You can customize access settings such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

On the **Directory > User > +Add** interface, scroll to the **Access Setting** section.

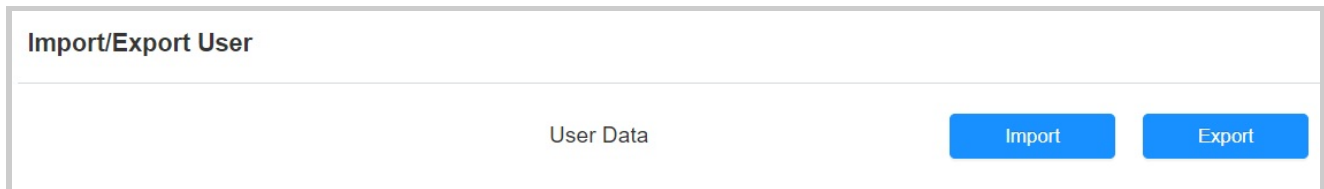
The screenshot shows the 'Access Setting' configuration page. At the top, there's a title 'Access Setting'. Below it, the 'Allow To Open' section has four radio buttons: 'Relay1' (checked), 'Relay2', 'Relay3', and 'Relay4'. Underneath is the 'Web Relay' section with a dropdown menu currently showing '0'. The bottom part of the interface features two list boxes. The left box, titled 'Unselected Schedules', contains one item: '1002:Never'. The right box, titled 'Selected Schedules', contains one item: '1001:Always'. Between the boxes are left and right arrow buttons, and on the right side of the 'Selected Schedules' box are up and down arrow buttons.

- **Allow To Open:** Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **Web Relay:** Specify the ID of web relay action commands that you've configured on the [Web Relay](#) interface. A default value of 0 indicates that the web relay will not be triggered.
- **Schedule:** Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
 - **Always:** Allows door opening without limitations on door open counts during the valid period.

- **Never:** Prohibits door opening.

Import and Export User Data

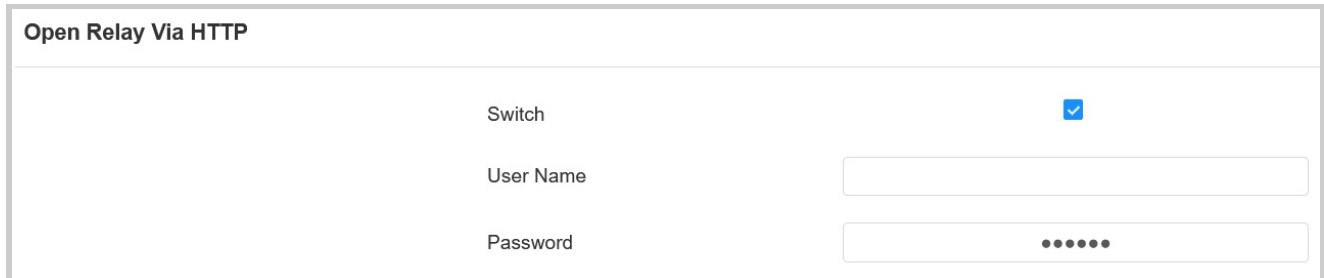
You can import and export the user data on the **Directory > User > Import/Export User** interface. The files are in TGZ format.



Open Doors via HTTP Command

The device supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the device. This will trigger the relay and open the door, even if the users are away from the device.

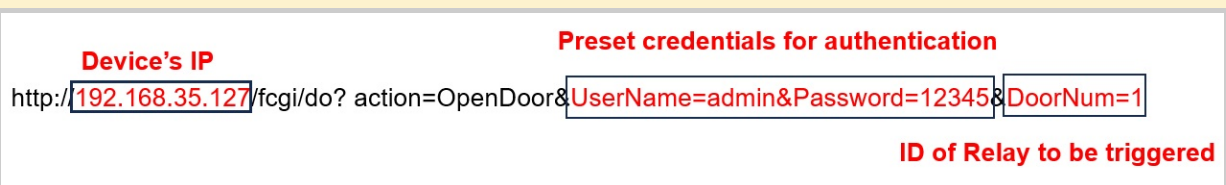
To set it up, go to **Access Control > Relay > Open Relay Via HTTP** interface.



- **Username:** Set a username for authentication in HTTP command URLs.
- **Password:** Set a password for authentication in HTTP command URLs.

Tip:

Here is an HTTP command URL example for relay triggering.



Note

The HTTP format for relay triggering varies depending on whether the device's high secure mode is enabled. Please refer to this how-to guide [Opening the Door via HTTP Command](#) for more information.

Unlock by Exit Button

When users need to open the door from inside by pressing the Exit button, you need to set up the Input terminal that matches the Exit button to activate the relay for the door access.

The device has 13 inputs, and 4 of them can be connected to the exit button.

To set it up, go to **Access Control > Input** interface.

Exit Button				
Exit Button ID	Exit Button A (Input1)	Exit Button B (Input2)	Exit Button C (Input3)	Exit Button D (Input4)
Exit Button Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Trigger Option	Low ▼	Low ▼	Low ▼	Low ▼
Open Relay	None ▼	None ▼	None ▼	None ▼
Status	High	High	High	High

- **Exit Button Enabled:** To use a specific input interface.
- **Trigger Option:** Set the input interface to trigger at low or high electrical level.
- **Open Relay:** Specify the relay to be triggered.
- **Status:** Display the status of the input signal.

Unlock by Emergency Button

It is recommended to use general input for fire emergency applications as it facilitates organizing input connections and prevents miswiring. When the fire emergency button is activated, it will initiate predefined actions like opening doors and activating alarm sirens.

To set it up, navigate to the web **Access Control > Input > General Input** interface.

General Input	
General Input ID	General Input (Input5)
General Input Enabled	<input type="checkbox"/>
Trigger Option	Low ▼
Action To Execute	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL
HTTP URL	
Trigger Relay	None ▼
Status	High

- **Trigger Option:** Set the input interface to trigger at low or high electrical level.
- **Action To Execute:** Set the desired actions that occur when this Input interface is triggered.
 - **Email:** Send a message to the preconfigured [Email address](#).
 - **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL:** Enter the HTTP message if selecting HTTP as the action to execute. The format is [http://HTTP server's IP/Message content](#).
- **Trigger Relay:** Specify the relay to be triggered.
- **Status:** Display the status of the input signal.

In addition to the above five inputs, the device has 8 extra inputs. Four of them can be connected to the door sensor for door-opening security. The rest can be connected to door sensors, smoke sensors, fire sensors, and IR motion detection sensors based on the actual application.

To set it up, navigate to the web **Access Control > Auxiliary Input** interface.

Door Magnetic				
Door Magnetic ID	Door Magnetic A (Input6)	Door Magnetic B (Input7)	Door Magnetic C (Input8)	Door Magnetic D (Input9)
Door Magnetic Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Trigger Option	Low ▼	Low ▼	Low ▼	Low ▼
Timeout Alert(Sec)	10 ▼	10 ▼	10 ▼	10 ▼
Action To Execute	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL
HTTP URL	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Trigger Output	None ▼	None ▼	None ▼	None ▼
Status	High	High	High	High

Auxiliary Input				
Auxiliary Input ID	Auxiliary Input A (Input10)	Auxiliary Input B (Input11)	Auxiliary Input C (Input12)	Auxiliary Input D (Input13)
Auxiliary Input Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Trigger Option	Low ▼	Low ▼	Low ▼	Low ▼
Action To Execute	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL	<input type="checkbox"/> Email <input type="checkbox"/> HTTP URL
HTTP URL	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Trigger Relay	None ▼	None ▼	None ▼	None ▼
Status	High	High	High	High

- **Trigger Option:** Set the input interface to trigger at low or high electrical level.
- **Timeout Alert(Sec):** The alarm will be triggered if the door opening duration exceeds the time.
- **Status:** Display the status of the input signal.
- **Action To Execute:** Set the desired actions that occur when this Input interface is triggered.
 - **Email:** Send a message to the preconfigured Email address.
 - **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL:** Enter the HTTP message if selecting HTTP as the action to execute. The format is <http://HTTP server's IP/Message content>.
- **Trigger Relay:** Specify the relay to be triggered.
- **Status:** Display the status of the input signal.

Security

Tamper Alarm

The tamper alarm function prevents anyone from removing the devices without permission. It will set off the tamper alarm when the device detects a change in its gravity value from the original one.

To set it up, navigate to the web **System > Security** interface.

Tamper Alarm	
Enabled	<input checked="" type="checkbox"/>
Key Status	High
<input type="button" value="Disarm"/>	

- **Disarm:** When the tamper alarm goes off, you can press the **Disarm** tab to clear the alarm.
- **Key Status:** The tamper alarm will not be triggered unless the key status is shifted from Low to High status.

Note

The disarm tab will turn grey when the tamper alarm is cleared.

Security Notification Setting

Email Notification Setting

Set up email notifications to receive messages of unusual motion from the device.

Go to **Setting > Action > Email Notification** interface.

Email Notification

Sender's Email Address	<input type="text"/>
Receiver's Email Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
Port	<input type="text"/>
SMTP Username	<input type="text"/>
SMTP Password	<input type="password"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
Email Test	<input type="button" value="Test Email"/>

- **SMTP Server Address:** The SMTP server address of the sender.
- **SMTP Username:** The SMTP username is usually the same as the sender's email address.
- **SMTP Password:** The password of the SMTP service is the same as the sender's email address.
- **Email Test:** Used to test whether the email can be sent and received.

Action URL

You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, PIN code, or RF card access changes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Relay Triggered	\$relay1status	Http://server ip/relaytrigger=\$relay1status
2	Relay Closed	\$relay1status	Http://server ip/relayclose=\$relay1status
3	Valid Code Entered	\$code	Http://server ip/validcode=\$code
4	Invalid Code Entered	\$code	Http://server ip/invalidcode=\$code
5	Valid Card Entered	\$card_sn	Http://server ip/validcard=\$card_sn
6	Invalid Card Entered	\$card_sn	Http://server ip/invalidcard=\$card_sn
7	Tamper Alarm Triggered	\$alarm status	Http://server ip/tampertrigger=\$alarm status

For example: [http://192.168.16.118/help.xml?](http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

[mac=\\$mac:ip=\\$ip:model=\\$model:firmware=\\$firmware:card_sn=\\$card_sn](http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

To set it up, navigate to the web **Setting > Action URL** interface.

Action URL	
Enabled	<input type="checkbox"/>
Relay1 Triggered	<input type="text"/>
Relay1 Closed	<input type="text"/>
Relay2 Triggered	<input type="text"/>
Relay2 Closed	<input type="text"/>
Relay3 Triggered	<input type="text"/>
Relay3 Closed	<input type="text"/>
Relay4 Triggered	<input type="text"/>
Relay4 Closed	<input type="text"/>
Valid Code Entered	<input type="text"/>
Invalid Code Entered	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<input type="text"/>
Tamper Alarm Triggered	<input type="text"/>

High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods, and more.

Enable High Security Mode on the **System > Security > High Security Mode** interface.

High Security Mode
Enabled <input checked="" type="checkbox"/>

Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.
2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

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

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

If the mode is on, the device only accepts the new HTTP formats below for door opening.

- | http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- | http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is off, the device can use both the new formats above and the old format below:

- | http://deviceIP/fcgi/do?
action=OpenDoor&UserName=username&Password=password&DoorNum=1

4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Web Interface Automatic Log-out

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

To set it up, navigate to the web **System > Security** interface.

Session Time Out	
Session Time Out Value	<input type="text" value="8000"/> (60~14400Sec)

Door Log

The access log displays up to 100,000 access records on applied cards and HTTP commands. Each record includes time and date, user information, card number, and so on.

Check the access log on the web **Status > Access Log** interface. You can export the access log file in **CSV** or **XML** format.

The screenshot shows the 'Access Log' interface. At the top, there is a toggle for 'Save Access Log Enabled' which is checked. Below this are search filters: a dropdown menu set to 'All', input fields for 'Start Time' and 'End Time', an input field for 'Name/Code', a blue 'Search' button, and an 'Export' dropdown menu. The main area contains a table with the following headers: Index, User ID, Name, Code, Type, Door ID, Date, Time, Mode, and Status. The table body is empty and displays a 'No Data' message with a folder icon. At the bottom, there are two red 'Delete' buttons, navigation buttons for 'Prev', '1/1', and 'Next', a page number '1' in a box, and a blue 'Go' button.

- **Save Access Log Enabled:** Decide whether to save the door-opening records.
- **Time:** Select the specific period of the door logs you want to search, check, or export.
- **Name/Code:** Search the log by the username or the PIN code.
- **Type:** Display the access type such as RF Card.
- **Door ID:** Display the door name.
- **Status:** **Success** and **Failed** options represent successful door accesses and failed door accesses respectively.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

To set it up, go to **System > Maintenance > System Log** interface.

The screenshot shows the 'System Log' configuration page. It features four settings: 'Log Level' is a dropdown menu set to '3'; 'Export Log' is a blue button labeled 'Export'; 'Remote System Log Enabled' is a checkbox that is currently unchecked; and 'Remote System Server' is a text input field that is currently empty.

- **Log Level:** Log levels range from 1 to 7. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the **Export** tab to export the temporary debug log file to a local PC.
- **Remote System Server:** Set the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.

Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

Navigate to the web **System > Maintenance** interface.

The screenshot shows the 'Remote Debug Server' configuration page. It features four settings: 'Enabled' is a checkbox that is currently unchecked; 'Connect Status' is a text label showing 'Disconnected'; 'Server IP' is a text input field that is currently empty; and 'Server Port' is a text input field set to '9500' with a range indicator '(1024-65535)' to its right.

- **Connect Status:** Display the remote debug server connection status.

- **Server IP:** Set the remote debug server IP address. Please ask the Akuvox technical team for the server IP address.
- **Server Port:** Set the remote debug server port.

PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

Navigate to the web **System > Maintenance** interface.

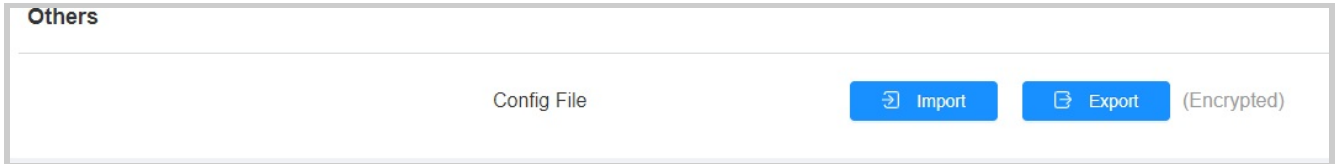
The screenshot shows a web interface for PCAP configuration. At the top left, the word 'PCAP' is displayed. Below it, there is a 'Specific Port' label followed by an empty text input field and a '(1-65535)' range indicator. Underneath, the 'PCAP' label is positioned above three buttons: 'Start' (blue), 'Stop' (grey), and 'Export' (blue). At the bottom, the 'PCAP Auto Refresh Enabled' label is followed by an unchecked checkbox.

- **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 the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh Enabled:** When enabled, the PCAP will continue to capture data packets even after the data packets reach their 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets captured reach the maximum capacity of 1MB.

Backup




You can import or export encrypted configuration files to your Local PC.

Navigate to the web **System > Maintenance > Others** interface.



Firmware Upgrade

Upgrade the device on the web **System > Upgrade** interface.

Basic	
Firmware Version	92.30.10.4
Hardware Version	92.0.0.0.0.0.0.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reboot	 Reboot

Note

Firmware files should be in .rom format for upgrade.

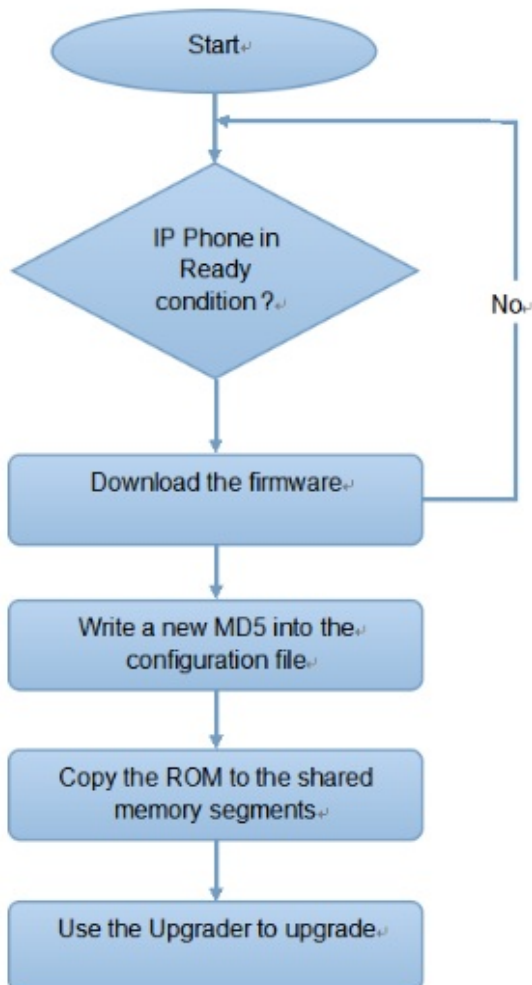
Auto-Provisioning via Configuration File

You can configure and upgrade the door phone on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade devices in batch via third-party servers. DHCP, PNP, TFTP, FTP, and HTTPS are the protocols used by the Akuvox 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 device.

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

The difference between the two types of configuration files:

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

Note

- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

You may click [here](#) to see the detailed format and steps.

Autop Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself according to the schedule.

To set it up, go to **System > Auto Provisioning > Automatic Autop** interface.

Automatic AutoP

Mode	<input style="width: 100%;" type="text" value="Power On"/>
Schedule	<input style="width: 100%;" type="text" value="Every Day"/>
	<input style="width: 80%;" type="text" value="23"/> (0~23Hour)
	<input style="width: 80%;" type="text" value="59"/> (0~59Min)
Clear MD5	<input style="width: 100%;" type="button" value="Clear"/>
Export Autop Template	<input style="width: 100%;" type="button" value="Export"/>

• **Mode:**

- **Power On:** The device will perform Autop every time it boots up.
- **Repeatedly:** The device will perform Autop according to the schedule you set up.
- **Power On + Repeatedly:** 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:** The device will perform Autop every hour.

Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device will perform the auto-provisioning at a specific time according to the auto provision 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 it up, download the template on **System > Auto Provisioning > Automatic Autop** first.


Automatic Autop

Mode	<input style="width: 100%;" type="text" value="Power On"/>
Schedule	<input style="width: 100%;" type="text" value="Sunday"/>
	<input style="width: 80%;" type="text" value="22"/> (0~23Hour)
	<input style="width: 80%;" type="text" value="0"/> (0~59Min)
Clear MD5	<input style="width: 100%;" type="button" value="Clear"/>
Export Autop Template	<input style="width: 100%;" type="button" value="Export"/>

Set up the Autop server on **System > Auto Provisioning > Manual Autop** interface.

Manual AutoP

URL	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Common AES Key	<input type="password"/>
AES Key(MAC)	<input type="password"/>

 AutoP Immediately

- **URL:** Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username:** Enter the username if the server needs a username to be accessed.
- **Password:** Enter the password if the server needs a password to be accessed.
- **Common AES Key:** It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC):** It is used for the intercom to decipher the MAC-based Autop configuration file.

Note

- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- **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.

Integration with Third Party Device

Integration via Wiegand

The Wiegand feature enables the Akuvox device to act as a controller or a card reader.

To set it up, navigate to the web **Device > Wiegand** interface.

WiegandA

WiegandA Display Mode	8HN
WiegandA Card Reader Mode	Wiegand-26
WiegandA Transfer Mode	Input
WiegandA Input Data Order	Normal
WiegandA Input Clear Time	5
WiegandA Anti-passback Mode	None

There'll be safety hazards if anti-passback Mode and bistable functions are activated concurrently.

WiegandA Open Relay Relay1 Relay2 Relay3 Relay4

- **Wiegand Display Mode:** Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode:** The transmission format should be identical between the access control terminal and the third-party device. It is automatically configured.
- **Wiegand Transfer Mode:**
 - **Input:** The device serves as a receiver.
 - **Output:** The device serves as a sender.
- **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.
- **Wiegand Input Clear Time:** When the interval of entering passwords exceeds the time. All entered passwords will be cleared.

- **Wiegand Anti-passback Mode:** Select from Entry and Exit. This mode restricts users from entering the door by following others.

For example, if the user follows someone else through the door, the next time he/she cannot swipe his/her card to pass the Entry/Exit door.

- **Wiegand Open Relay:** Select the relay triggered by Wiegand.

Note

Click [here](#) to see detailed configuration steps.

Integration via RS485

The device has six RS485 ports, 2 of which are used for the connection with the expanded access control board. The rest four are used for third-party integration, for example, you can connect A094 to the third-party RS485 card readers for access control. You can select the type of card reader for any of the RS485 interfaces.

Set it up on the web **Device > RS485** interface.

RS485	
Apply RS485A to	Disabled ▼
Apply RS485B to	Disabled ▼
Apply RS485C to	Disabled ▼
Apply RS485D to	Disabled ▼

Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device and the Akuvox device.

To set it up, navigate to the web **Setting > HTTP API** interface.

HTTP API

Enabled	<input checked="" type="checkbox"/>
Authorization Mode	<input type="text" value="Allowlist"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
1st IP	<input type="text"/>
2nd IP	<input type="text"/>
3rd IP	<input type="text"/>
4th IP	<input type="text"/>
5th IP	<input type="text"/>

- **HTTP API Enable:** Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.

- **Authorization Mode:**
 - **None:** no authentication is required for HTTP API as it is only used for demo testing.
 - **Normal:** this mode is for Akuvox developers only.
 - **Allowlist:** this mode requires you to enter the IP address of the devices you allow for the integration via HTTP API.
 - **Basic:** this mode requires you to fill in the authentication username and password. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode the username and password.
 - **Digest:** The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx",opaque="xx".
 - **Token:** this mode is used by Akuvox developers only.

- **Username:** Enter the user name when **Basic** or **Digest** authorization mode is selected. The default username is admin.

- **Password:** Enter the password when **Basic** or **Digest** authorization mode is selected. The default password is admin.
- **1st IP-5th IP:** Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

Power Output Control

The device can serve as a power supply for the external relays.

To set it up, navigate to the web **Access Control > Relay** interface.

12V Power Output

12V Power OutputA	Disabled ▼
12V Power OutputB	Disabled ▼
12V Power OutputC	Disabled ▼
12V Power OutputD	Disabled ▼
Time Out (Sec)	3 ▼

- **Relay ID:** Specify the relay for the power supply output.
- **Power Output Type:** Select the power output type.
 - **Always:** The device will provide a continuous power supply. The device relay status will be changed from NC to NO status after the relay is triggered, thus cutting off the power out. The power supply will be resumed after the relay is reset.
 - **Triggered by Open Relay:** The device relay will be changed from NO to NC status after the relay is triggered, thus starting the power supply. The power supply will be cut off after the relay is reset. The relay can be reset automatically by the relay timeout(3, 5, 10 Sec.). For example, if you want the relay to be automatically reset 10 seconds after triggering, you can select 10 seconds, meaning 10 seconds of power output. It is 3 seconds by default.
- **Time Out(Sec):** Set the relay reset time.

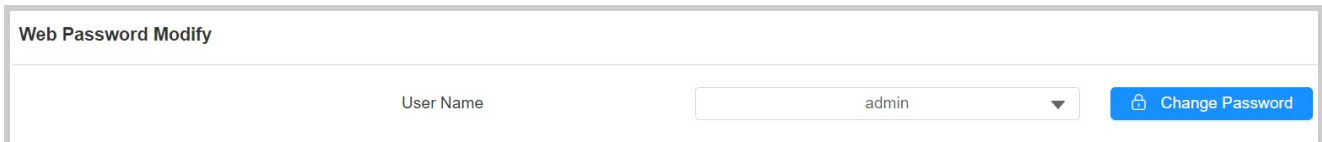
Tip

The power output is 12V, and the maximum output amperage is 0.8A.

Account & Password

You can modify the device web password for both the administrator account and the user account.

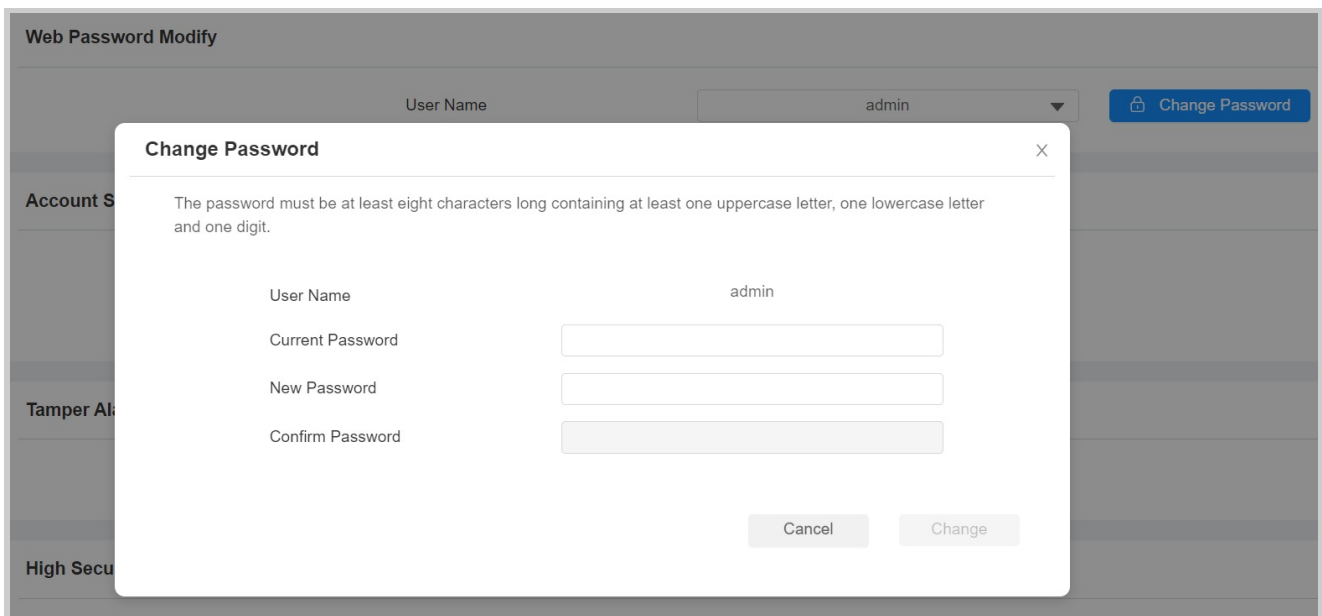
To set it up, go to **System > Security > Web Password Modify** interface.



Web Password Modify

User Name

Click **Change Password** to modify the password.



Web Password Modify

User Name

Change Password [X]

The password must be at least eight characters long containing at least one uppercase letter, one lowercase letter and one digit.

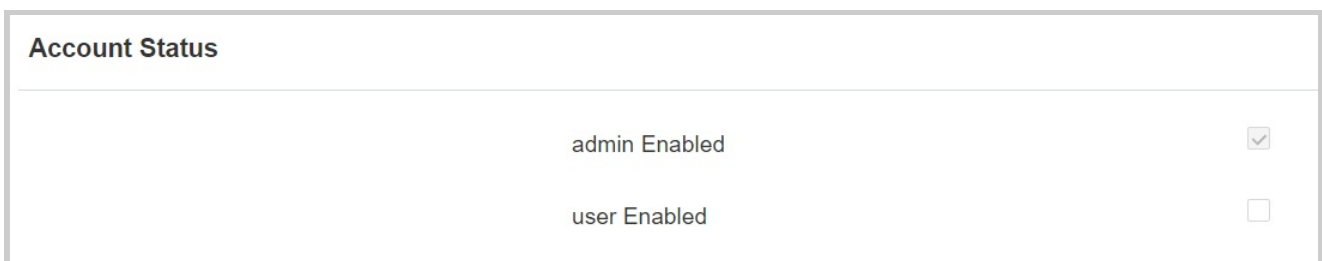
User Name

Current Password

New Password

Confirm Password

To enable or disable the user account, scroll to the **Account Status** section.



Account Status

admin Enabled	<input checked="" type="checkbox"/>
user Enabled	<input type="checkbox"/>

System Reboot & Reset




Reboot

The access controller can be rebooted manually or with a reboot schedule on the web interface.

- To reboot the system manually

Navigate to the web **System > Upgrade** interface.


Basic

Firmware Version	92.30.10.4
Hardware Version	92.0.0.0.0.0.0.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reboot	 Reboot

- To set up the device reboot schedule

Navigate to the web **System > Auto Provisioning** interface.

Reboot Schedule

Enabled	<input checked="" type="checkbox"/>
Schedule	<input type="text" value="Every Day"/> 
	<input type="text" value="0"/> (0~23Hour)

Reset

Reset the device on the web **Upgrade > Basic** interface.

Basic

Firmware Version 92.30.10.4

Hardware Version 92.0.0.0.0.0.0.0

Upgrade [↗ Upgrade](#)

Reset To Factory Setting [↻ Reset](#)

Reboot [🔌 Reboot](#)