About This Manual

Akuvox
Open A Smart World

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 configure the access controller properly. This manual is written based on firmware version 92.30.10.213, 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.

Changelog

What’s new in version 92.30.10.213:

- Added the holiday exemption option for users to open doors during holidays.
- Optimized event log.

Click here to view the changelog of the device’s previous versions.

Model Specification

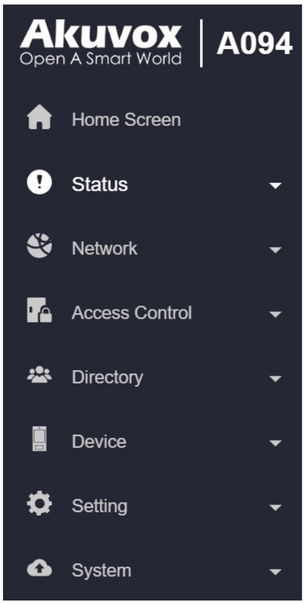
Specification	A094
Operation System	Linux
Material	Galvanized steel
Installation	Wall-mounting
Relay	8 relays
Wiegand	4 Wiegand interface
Input	13 inputs
Ethernet	1x10/100M RJ45 interface
RS485	6 RS485 Interface
Working Power	12V
Power input	100-240VAC
Back Power Supply	Battery
Power output	12VDC 800mA x 4
Indicator	Power Indicator/ Ethernet indicator
Speaker	Inbuilt Speaker
RAM	64MB
ROM	128MB
RTC	√
Reset	√
Work temperature	-10℃ ~ +55℃
Storage temperature	-20℃ ~ +70℃
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.

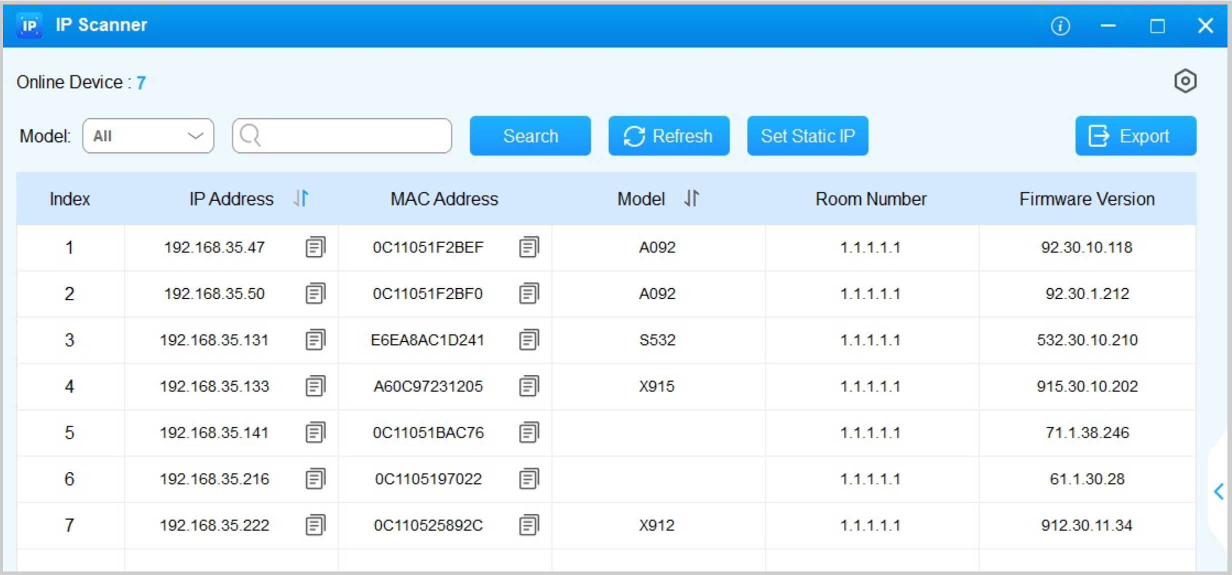


Access the Device

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.

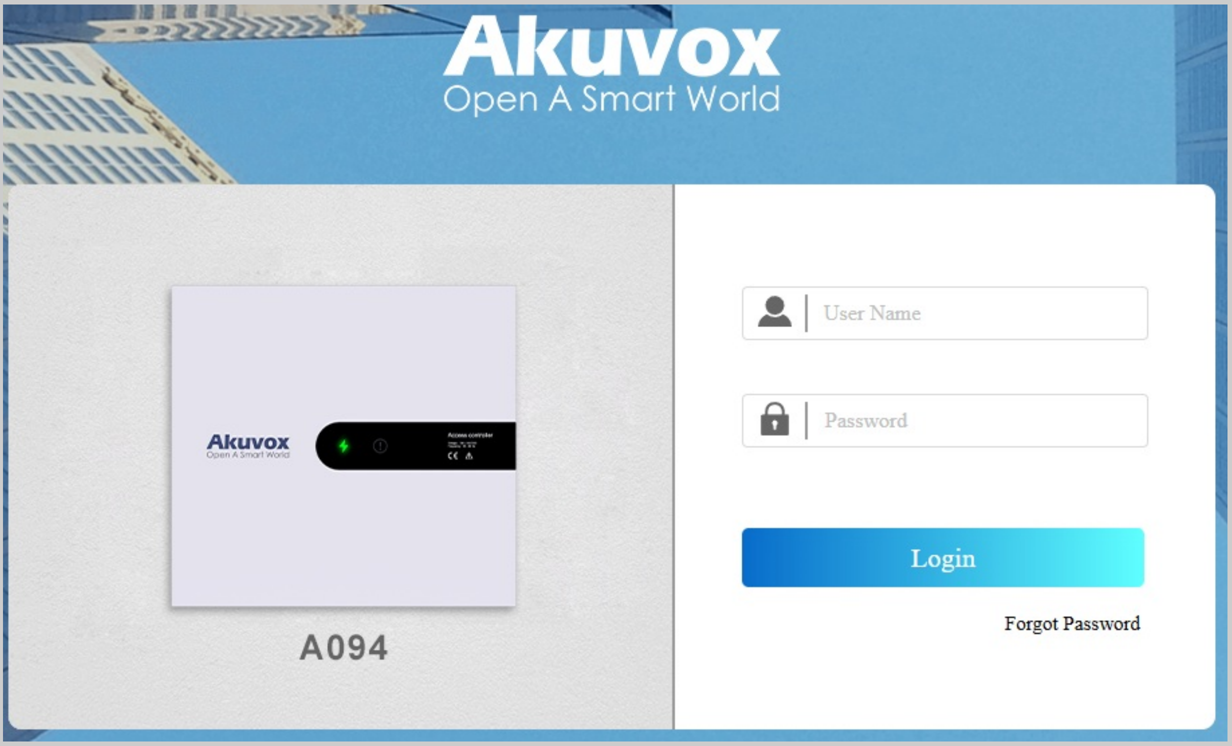


Online Device : 7

Index	IP Address	MAC Address	Model	Room Number	Firmware Version
1	192.168.35.47	0C11051F2BEF	A092	1.1.1.1.1	92.30.10.118
2	192.168.35.50	0C11051F2BF0	A092	1.1.1.1.1	92.30.1.212
3	192.168.35.131	E6EA8AC1D241	S532	1.1.1.1.1	532.30.10.210
4	192.168.35.133	A60C97231205	X915	1.1.1.1.1	915.30.10.202
5	192.168.35.141	0C11051BAC76		1.1.1.1.1	71.1.38.246
6	192.168.35.216	0C1105197022		1.1.1.1.1	61.1.30.28
7	192.168.35.222	0C110525892C	X912	1.1.1.1.1	912.30.11.34

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.



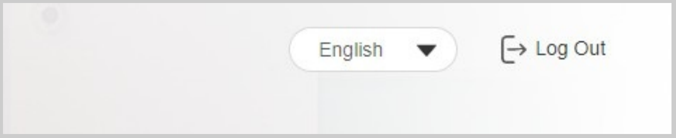
Note

- 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

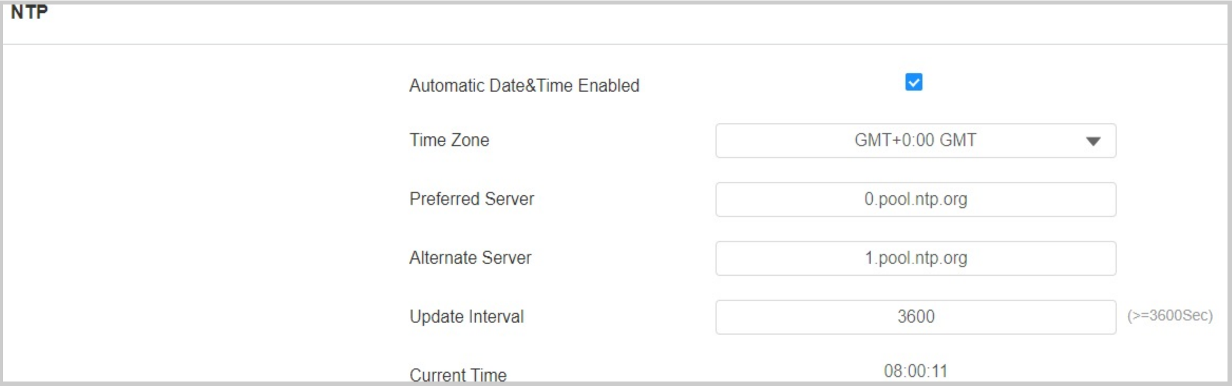
You can select the web language in the upper right corner. Currently, the A094 supports English and Simplified Chinese.



Time Setting

The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on your device.

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



NTP

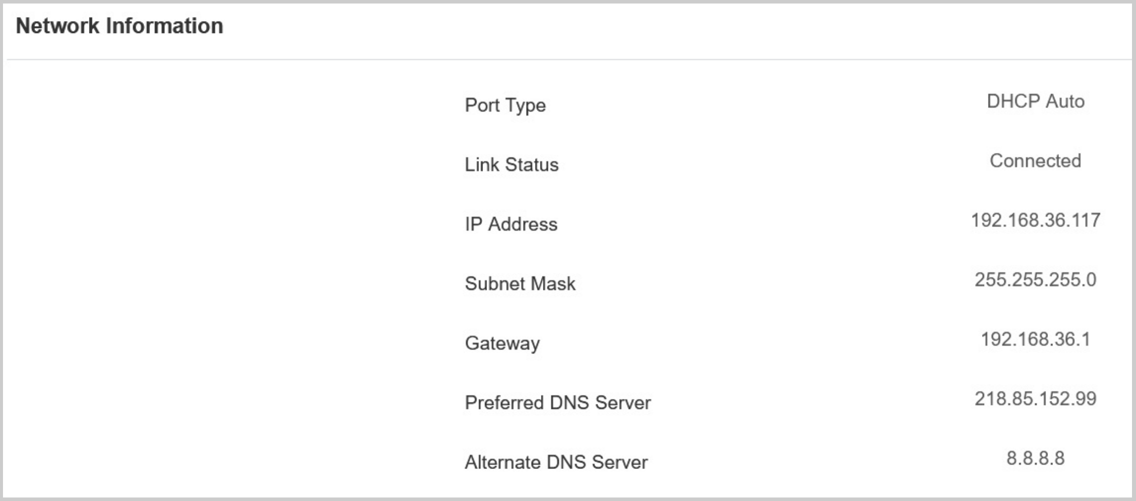
Automatic Date&Time Enabled	☑	
Time Zone	GMT+0:00 GMT	
Preferred Server	0.pool.ntp.org	
Alternate Server	1.pool.ntp.org	
Update Interval	3600	(>=3600Sec)
Current Time	08:00:11	

- **Automatic Date&Time Enabled**: Set whether the device updates the time automatically via the Network Time Protocol(NTP) server.
- **Time Zone**: Select the time zone.
- **Primary/Alternate Server:** Enter the primary NTP server address for updating the time. The default NTP 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.



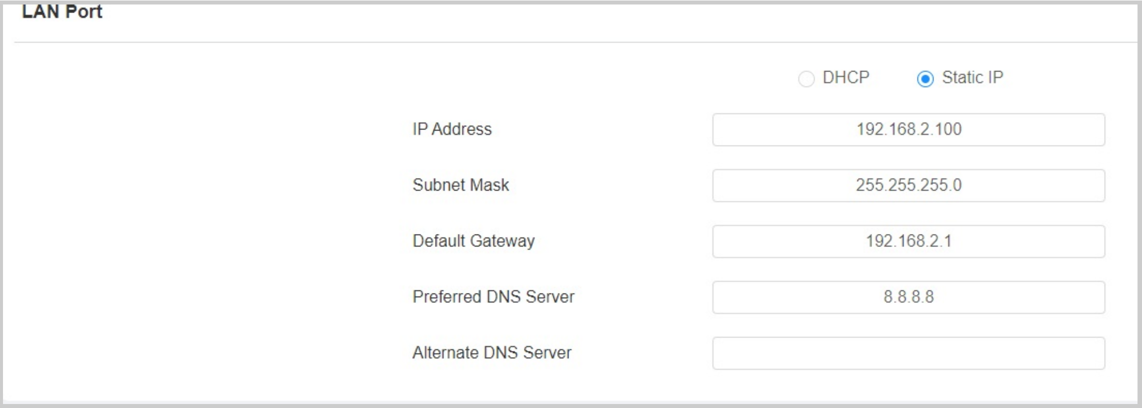
Network Information

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

○ DHCP ● Static IP

IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
Preferred DNS Server	8.8.8.8
Alternate DNS Server	

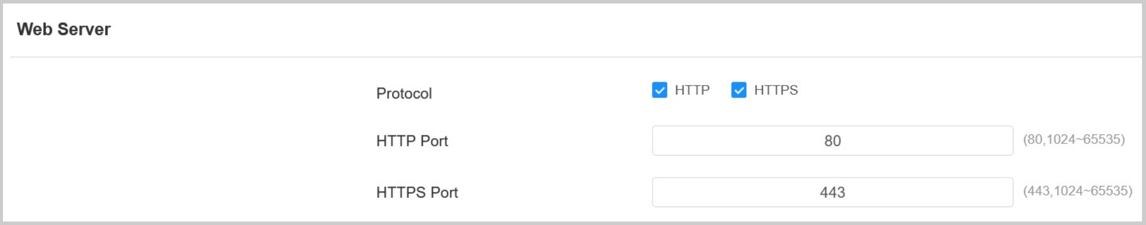
- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the access control terminal will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: When static IP mode is selected, the IP address, 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

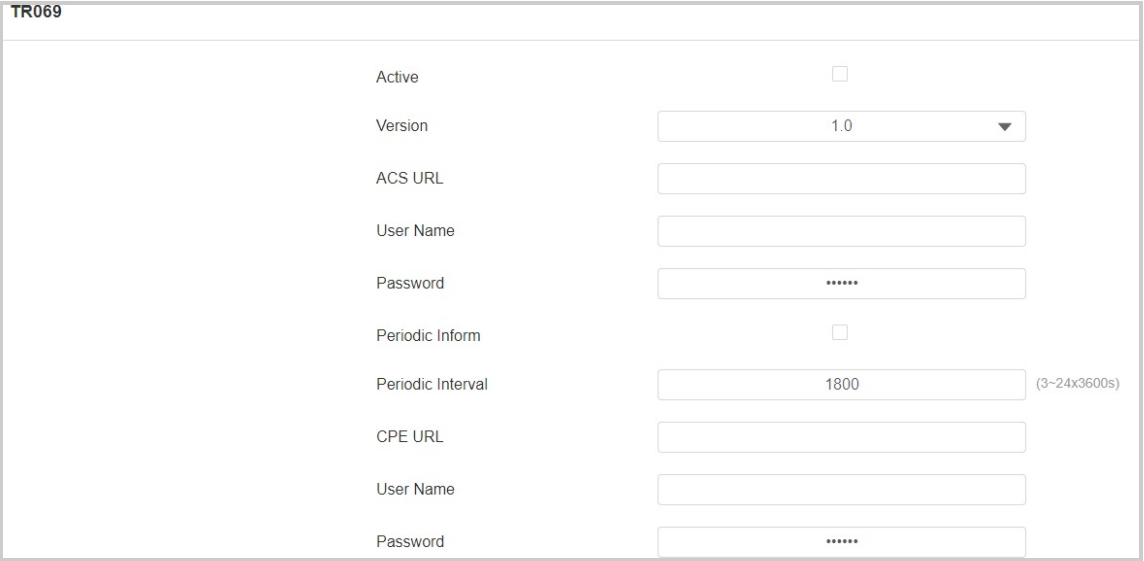
Protocol	☑ HTTP ☑ HTTPS	
HTTP Port	80	(80,1024~65535)
HTTPS Port	443	(443,1024~65535)

- **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.



TR069

Active	□	
Version	1.0	
ACS URL		
User Name		
Password	••••••	
Periodic Inform	□	
Periodic Interval	1800	(3~24x3600s)
CPE URL		
User Name		
Password	••••••	

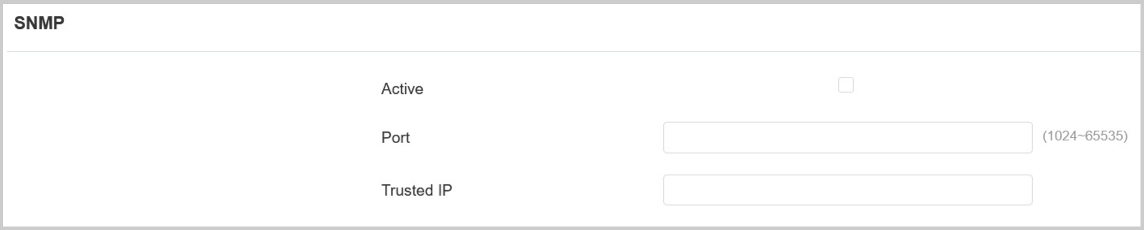
- **Version:** Select the TR069 version.
- **ACS URL**: Set the URL of the ACS server, for example, http://192.168.1.47:8080/openacs/acs
- **User Name**: Set the ACS server username for authentication.

- **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 □

Port (1024~65535)

Trusted IP

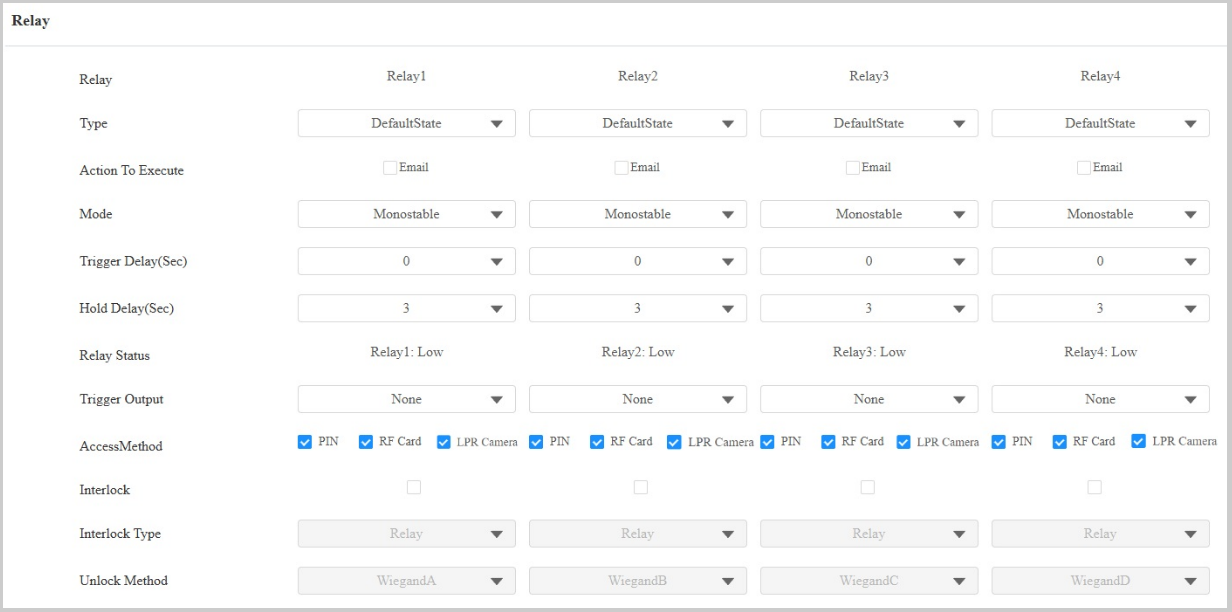
- **Port**: Set a specific port for the data transmission from 1024-65535.
- **Trusted IP**: Enter the third-party IP address.

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

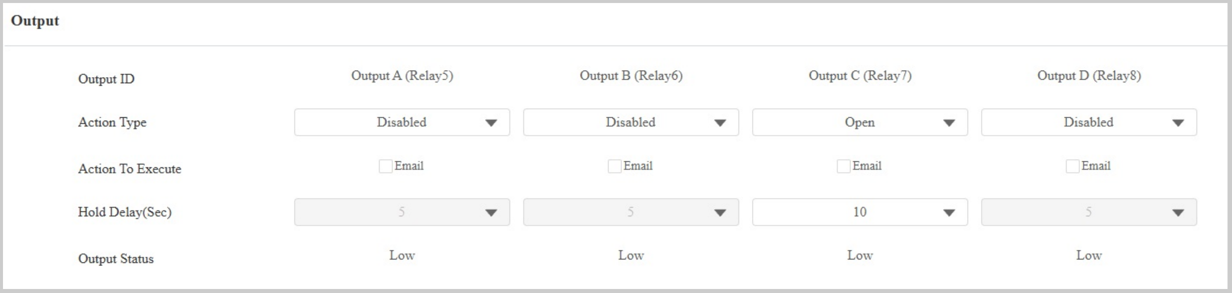
Relay	Relay1	Relay2	Relay3	Relay4
Type	DefaultState	DefaultState	DefaultState	DefaultState
Action To Execute	□Email	□Email	□Email	□Email
Mode	Monostable	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0	0
Hold Delay(Sec)	3	3	3	3
Relay Status	Relay1: Low	Relay2: Low	Relay3: Low	Relay4: Low
Trigger Output	None	None	None	None
AccessMethod	☑ PIN ☑ RF Card ☑ LPR Camera	☑ PIN ☑ RF Card ☑ LPR Camera	☑ PIN ☑ RF Card ☑ LPR Camera	☑ PIN ☑ RF Card ☑ LPR Camera
Interlock	□	□	□	□
Interlock Type	Relay	Relay	Relay	Relay
Unlock Method	WiegandA	WiegandB	WiegandC	WiegandD

- **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 open.
  - **Invert State**: A "Low" status in the Relay Status field indicates an opened door, while "High" indicates a closed one.
- **Action to Execute**: Send an email notification to the preconfigured email address.
- **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).
- **Trigger Output**: A094 has four extra relays which can be connected to some devices, such as a smoke sensor, to carry out preset actions like setting off alarms or turning on the light. They can be triggered with specific relays.
- **Access Method**: Check the method(s) to trigger the relay.

- **Interlock**: This feature limits the opening of other doors when one door is open. For example, enable Interlock for Relays 1, 2, and 4. When Relay 1 is opened, Relay 2 or 4 cannot be opened until Relay 1 is closed. While Relay 3 is not affected.
- **Interlock Type**: Available when Interlock is enabled. Set how to determine the door is closed, by relay reset or input reset.
- **Unlock Method**: Available when Interlock is enabled. Specify the method that opens the relay. The settings of the corresponding Wiegand and Input will be overwritten.

> **Note**
>
> Click here to view the detailed explanation of the Interlock feature.

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



Output

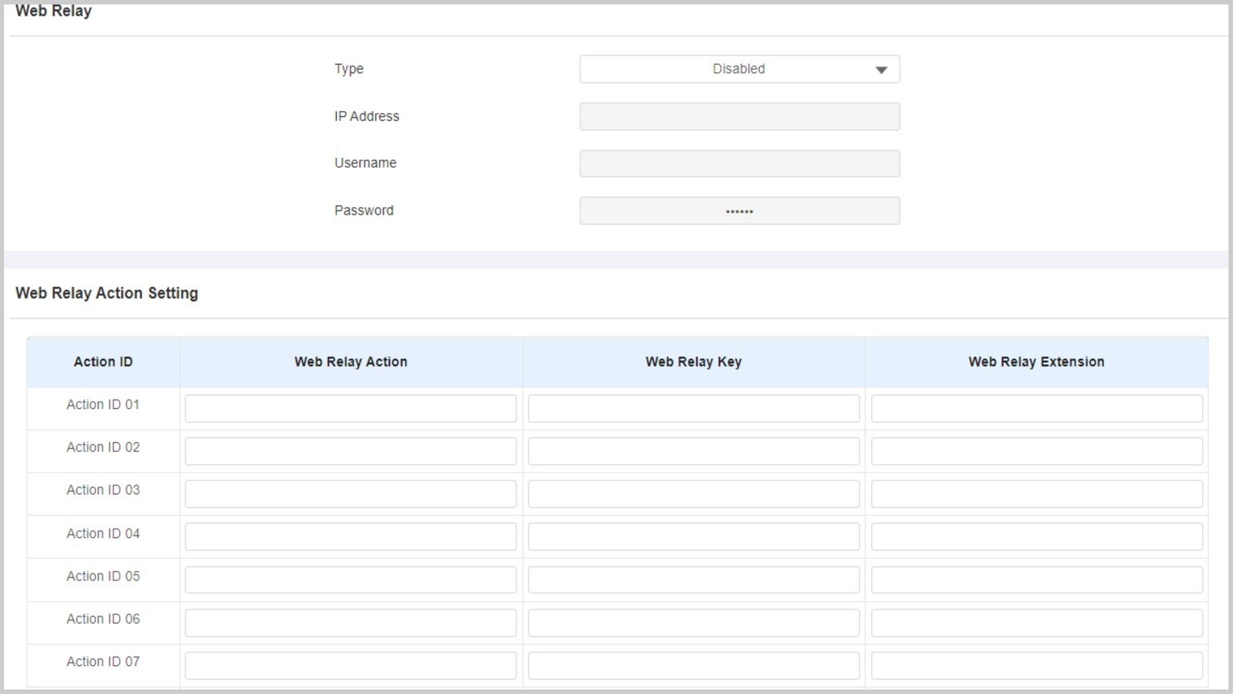
Output ID	Output A (Relay5)	Output B (Relay6)	Output C (Relay7)	Output D (Relay8)
Action Type	Disabled	Disabled	Open	Disabled
Action To Execute	☐ Email	☐ Email	☐ Email	☐ Email
Hold Delay(Sec)	5	5	10	5
Output Status	Low	Low	Low	Low

- **Action**: Set whether to use the Output. When **Open** is selected, Hold Delay option can be configured.
- **Action to Execute**: Send an email notification to the preconfigured email address.
- **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	Disabled
IP Address	
Username	
Password	......

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01			
Action ID 02			
Action ID 03			
Action ID 04			
Action ID 05			
Action ID 06			
Action ID 07			

- **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.

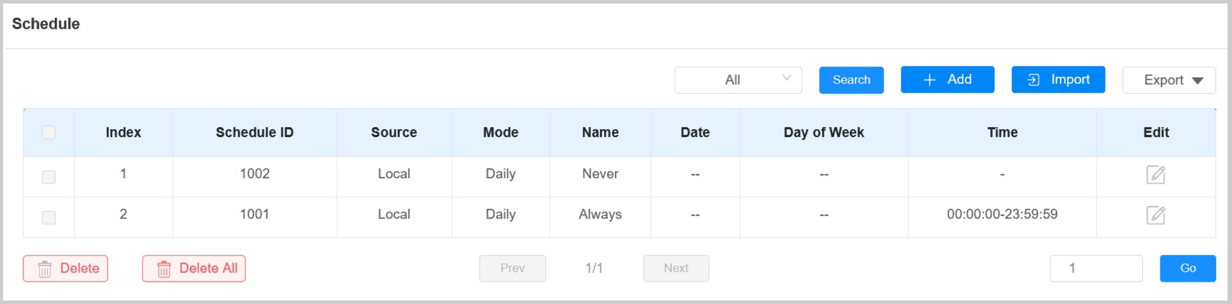
Door Access Schedule Management

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

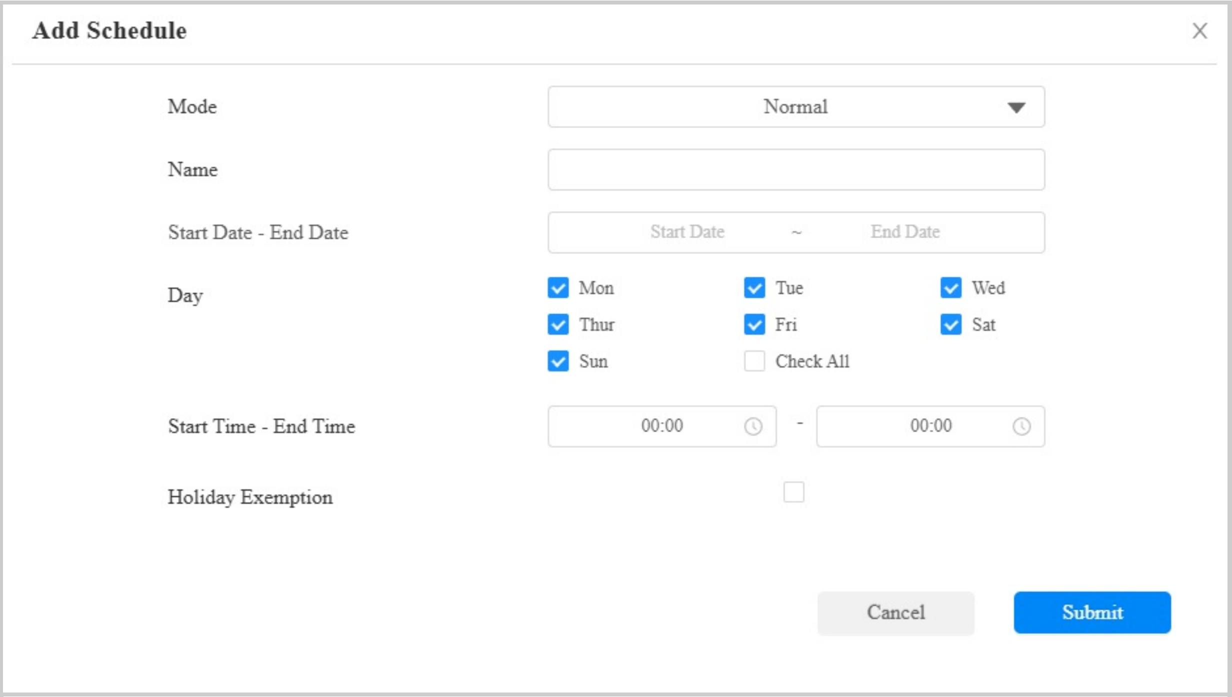
You can create door access schedules for daily, weekly, or custom time periods.

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



Schedule

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



Add Schedule

Mode: Normal

Name:

Start Date - End Date: Start Date ~ End Date

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun □ Check All

Start Time - End Time: 00:00 - 00:00

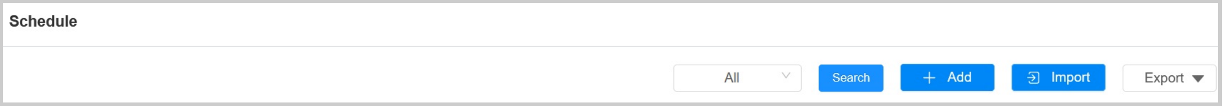
Holiday Exemption: □

- **Name**: Name the schedule.
- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long-term schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Holiday Exemption**: The holiday schedule has higher priority over the access schedule, which limits users from opening doors. If users want to open doors during holidays within the access schedule, you need to check this option.

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.

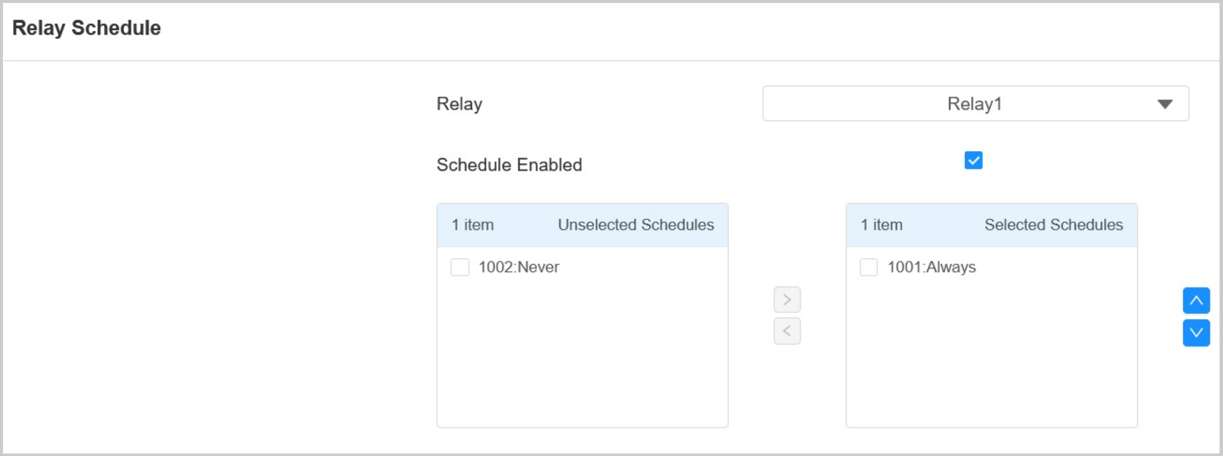
To set it up, go to the **Setting > Schedule** interface. The import and export files are in **XML** format.



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 Schedule

Relay: Relay1

Schedule Enabled: ☑

1 item	Unselected Schedules
□ 1002:Never	

1 item	Selected Schedules
□ 1001:Always	

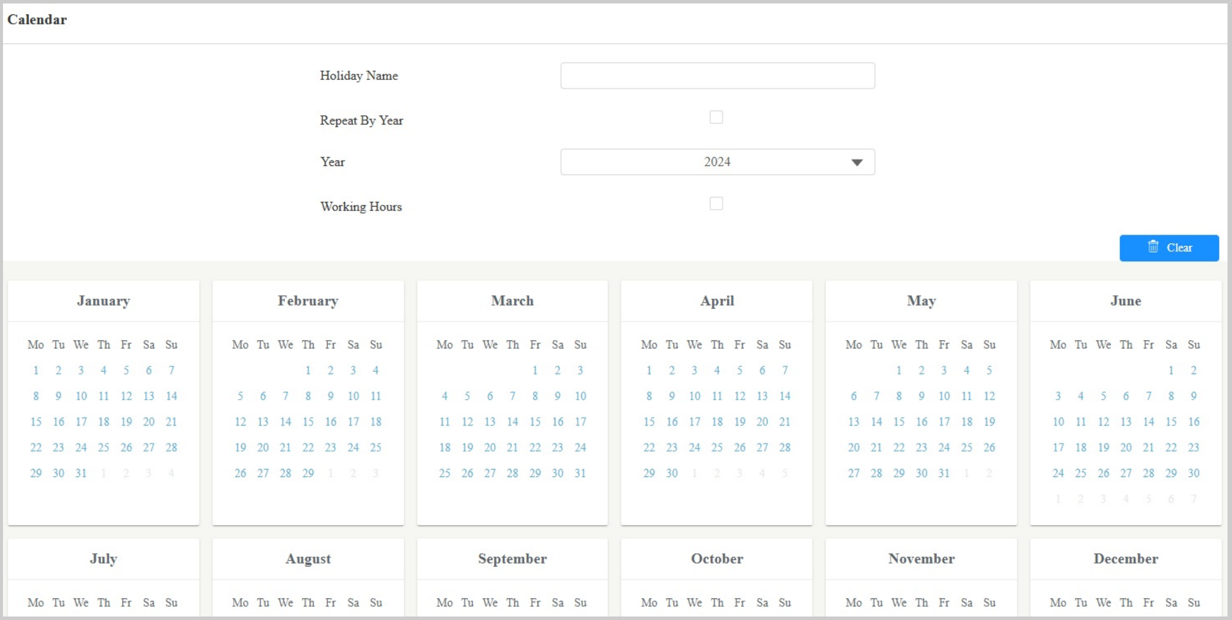
- **Relay ID**: Specify the relay you need to set up.
- **Schedule:** Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

For instructions on creating schedules, kindly consult the Create Door Access Schedule section.

Holiday Schedule

You can define the holidays when users cannot open doors to enhance access control security. You can also set the Working Hours to allow authorized users to open doors.

Set it up on the web **Setting > Holiday** interface. Click **+Add** to add a holiday and click **+Clear** to clear the selection of all dates.



Calendar

Holiday Name

Repeat By Year □

Year 2024

Working Hours □

January

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

February

Mo	Tu	We	Th	Fr	Sa	Su
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	1	2	3

March

Mo	Tu	We	Th	Fr	Sa	Su
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

April

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

May

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

June

Mo	Tu	We	Th	Fr	Sa	Su
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

July

Mo	Tu	We	Th	Fr	Sa	Su

August

Mo	Tu	We	Th	Fr	Sa	Su

September

Mo	Tu	We	Th	Fr	Sa	Su

October

Mo	Tu	We	Th	Fr	Sa	Su

November

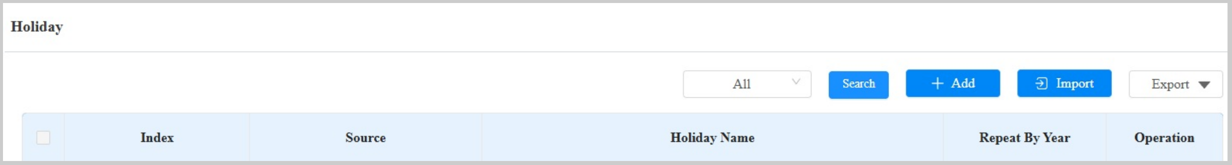
Mo	Tu	We	Th	Fr	Sa	Su

December

Mo	Tu	We	Th	Fr	Sa	Su

- **Holiday Name**: Name the schedule.
- **Repeat By Year**: Set whether to repeat the schedule every year.
- **Year**: Select the year.
- **Working Hours**: During working hours, users are allowed to open doors with their credentials.

You can also import and export schedule files on the same interface. The import/export file is in XML format.



Holiday

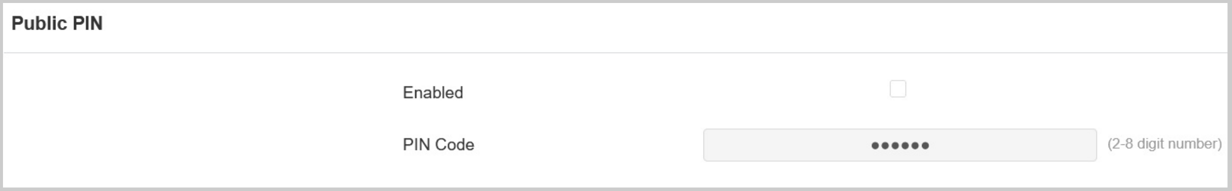
□	Index	Source	Holiday Name	Repeat By Year	Operation

Door-opening 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)

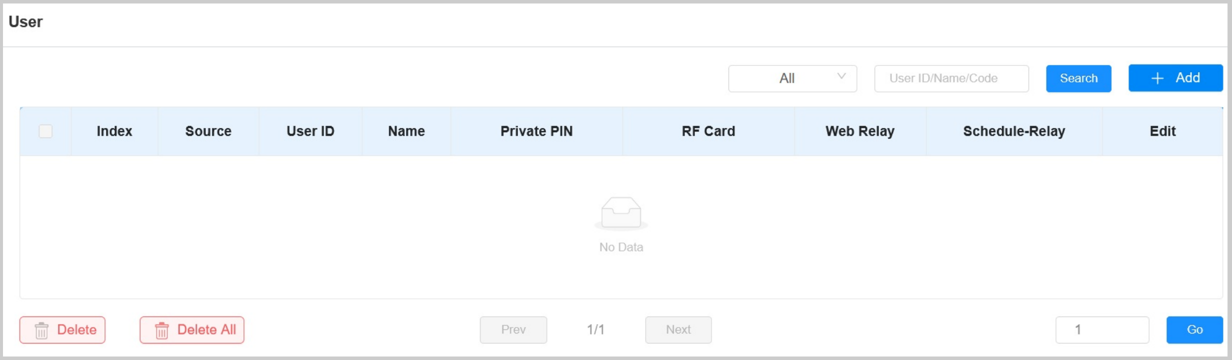
- **PIN Code**: Set a 2-8 digit PIN code accessible for universal use.

User-specific Access Methods

The private PIN code, RF card, and license plate should be assigned to a particular user for opening doors.

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.

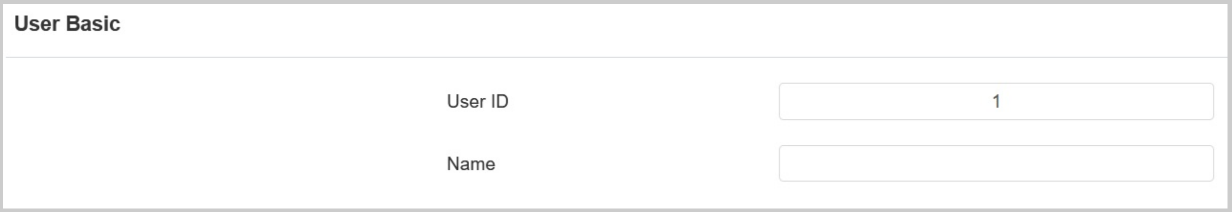
To add a user, go to **Directory > User** interface and click **+Add**.



User

□	Index	Source	User ID	Name	Private PIN	RF Card	Web Relay	Schedule-Relay	Edit

No Data



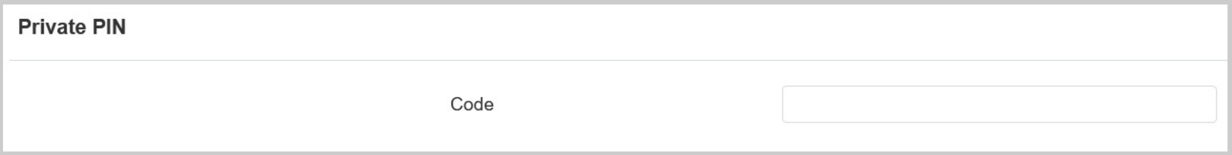
User Basic

User ID	1
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.



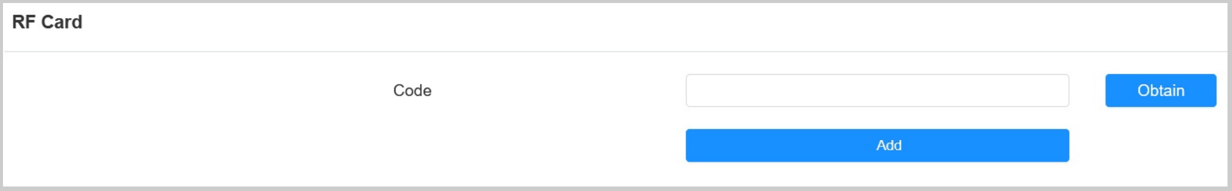
Private PIN

Code

- **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.



RF Card

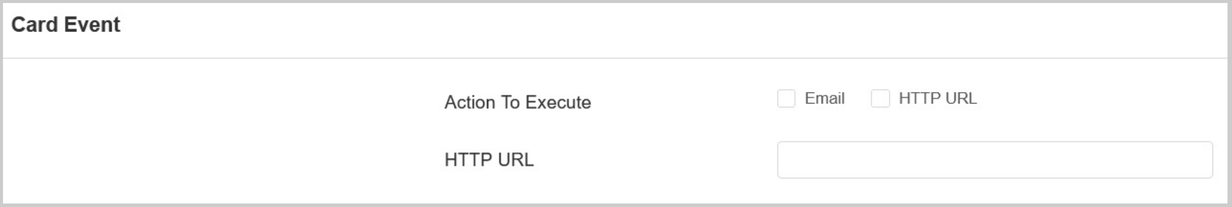
Code

- **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.



Card Event

Action To Execute □ Email □ HTTP URL

HTTP URL

- **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.

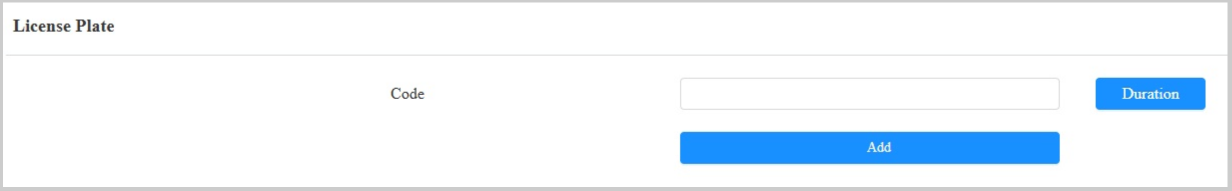
Unlock by License Plate

Akuvox offers two main ways to identify vehicles and open gates.

- Use a third-party LPR(License Plate Recognition) camera to recognize the license plate of the vehicle.

- Use the Akuvox long-range card reader ACR-CPR12 to recognize the UHF card attached to the vehicle's windshield.

To assign the license plate to a user, find the **License Plate** part on the **Directory > User > +Add** interface.



License Plate

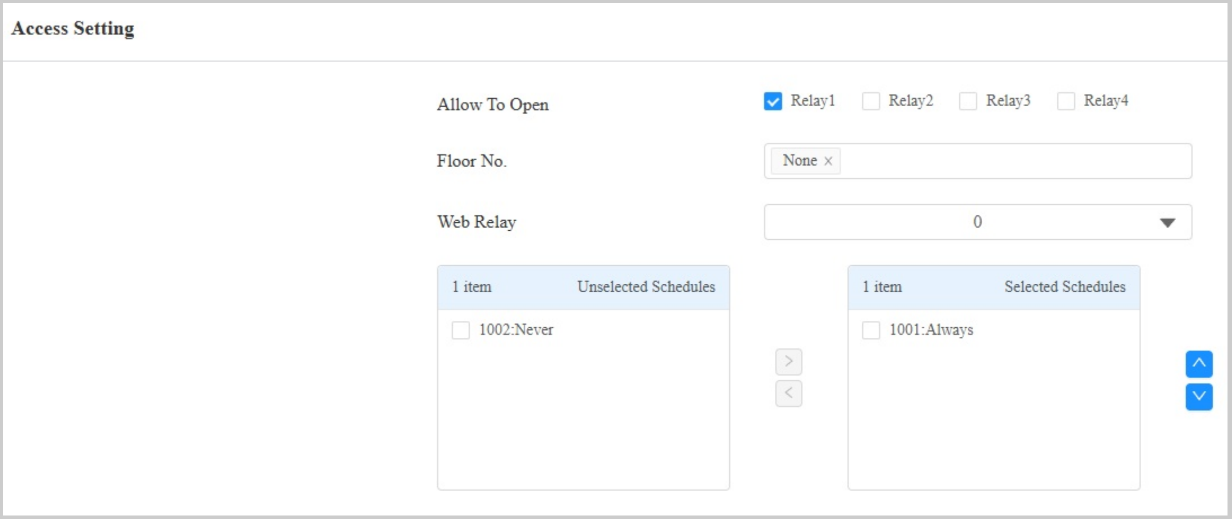
Code:

- **Add**: A user can have up to 5 license plates.
- **Duration**: Enable/disable Long-term Vehicle. It is enabled by default. If disabled, specify when the vehicle can enter or exit the parking lot.

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.



Access Setting

Allow To Open: ☑ Relay1 □ Relay2 □ Relay3 □ Relay4

Floor No.: None ×

Web Relay: 0

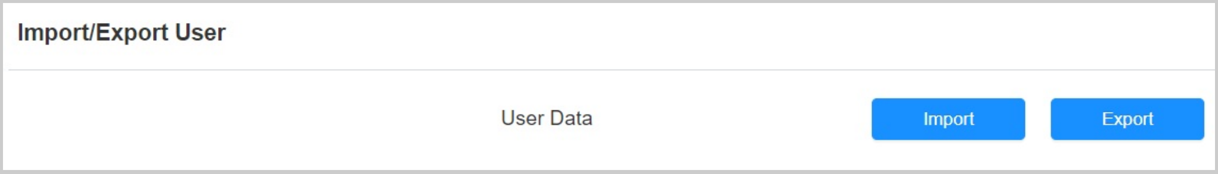
1 item Unselected Schedules
□ 1002:Never

1 item Selected Schedules
□ 1001:Always

- **Allow To Open**: Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **Floor No.**: Specify the accessible floor(s) to the user via the elevator.
- **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.



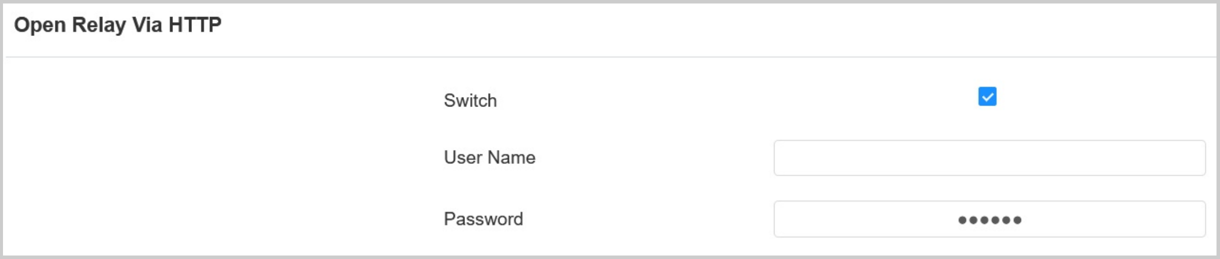
Import/Export User

User Data

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.



Open Relay Via HTTP

Switch ☑

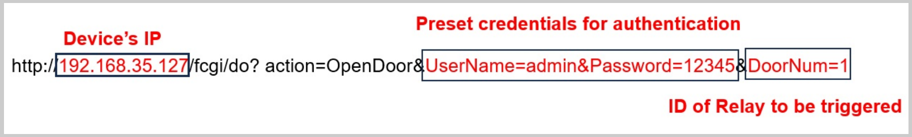
User Name

Password ●●●●●●

- **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.



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

Device's IP
Preset credentials for authentication
ID of Relay to be triggered

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.

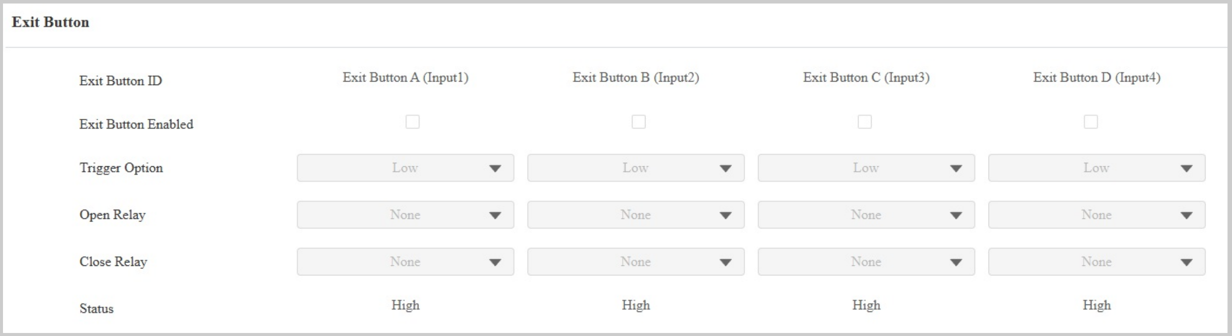
Unlock by Exit Button

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.

Click here to watch the instruction video.

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

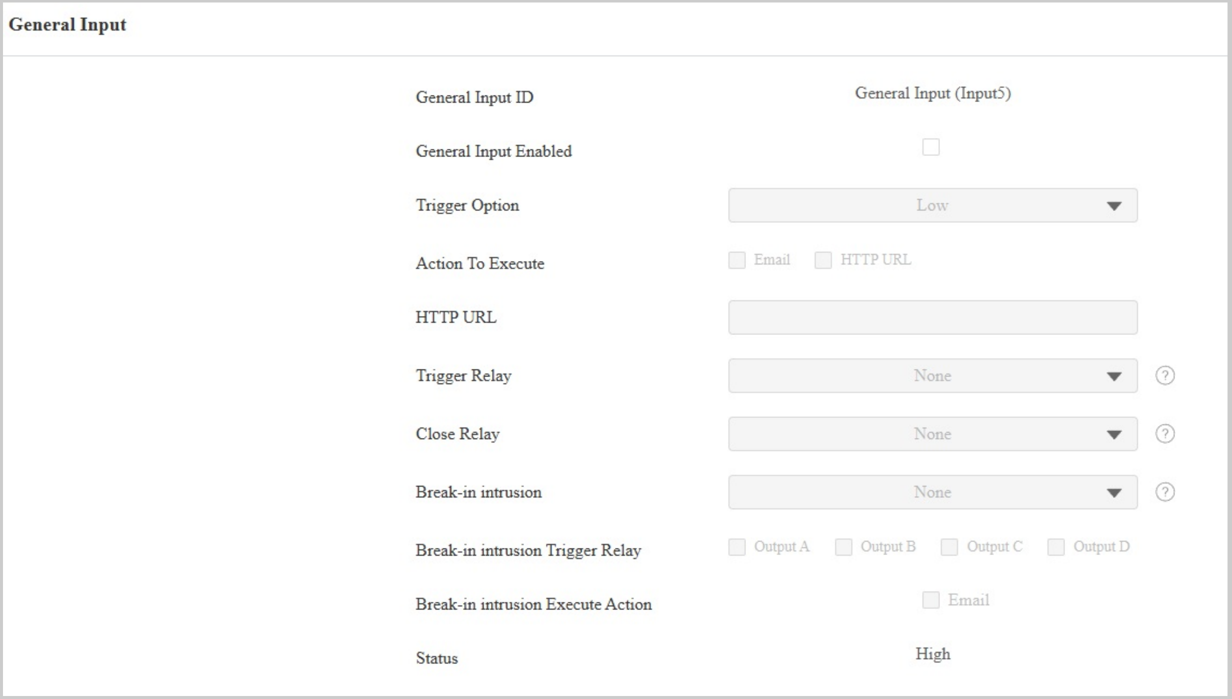
Exit Button ID	Exit Button A (Input1)	Exit Button B (Input2)	Exit Button C (Input3)	Exit Button D (Input4)
Exit Button Enabled	□	□	□	□
Trigger Option	Low	Low	Low	Low
Open Relay	None	None	None	None
Close Relay	None	None	None	None
Status	High	High	High	High

- **Exit Button Enabled**: Specify a specific input interface used.
- **Trigger Option**: Set the input interface to trigger at a low or high electrical level.
- **Open Relay**: Specify the relay to be opened.
- **Close Relay**: Specify the relay to be closed.
- **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

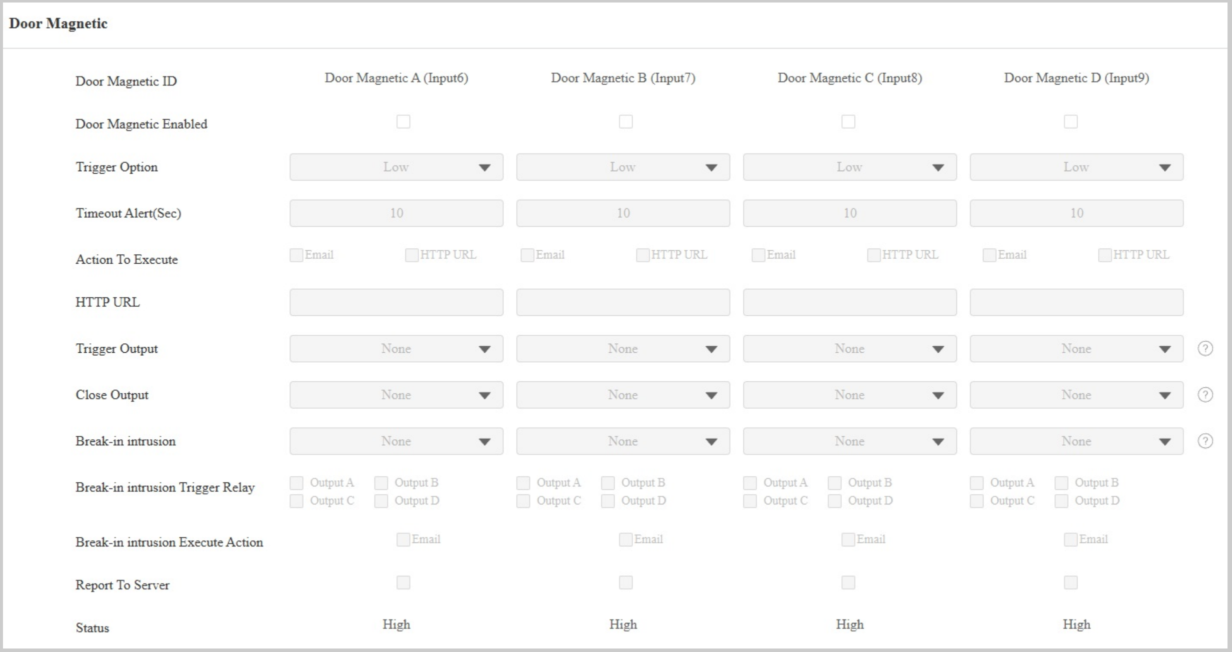
General Input ID	General Input (Input5)
General Input Enabled	□
Trigger Option	Low
Action To Execute	□ Email □ HTTP URL
HTTP URL	
Trigger Relay	None
Close Relay	None
Break-in intrusion	None
Break-in intrusion Trigger Relay	□ Output A □ Output B □ Output C □ Output D
Break-in intrusion Execute Action	□ Email
Status	High

- **Trigger Option**: Set the input interface to trigger at a 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.
- **Close Relay**: Specify the relay to be closed when the input is triggered. Please note this feature does not work during the relay schedule time.
- **Break-in intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. This feature is not compatible with the Trigger Relay and Close Relay functions.
  Click here to learn more information about this feature.
- **Break-in intrusion Trigger Relay**: Specify the relay(relay 5~8) to be opened.
- **Break-in intrusion Execute Action**: Set whether to send a message to the preconfigured Email address when the break-in intrusion happens.
- **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.



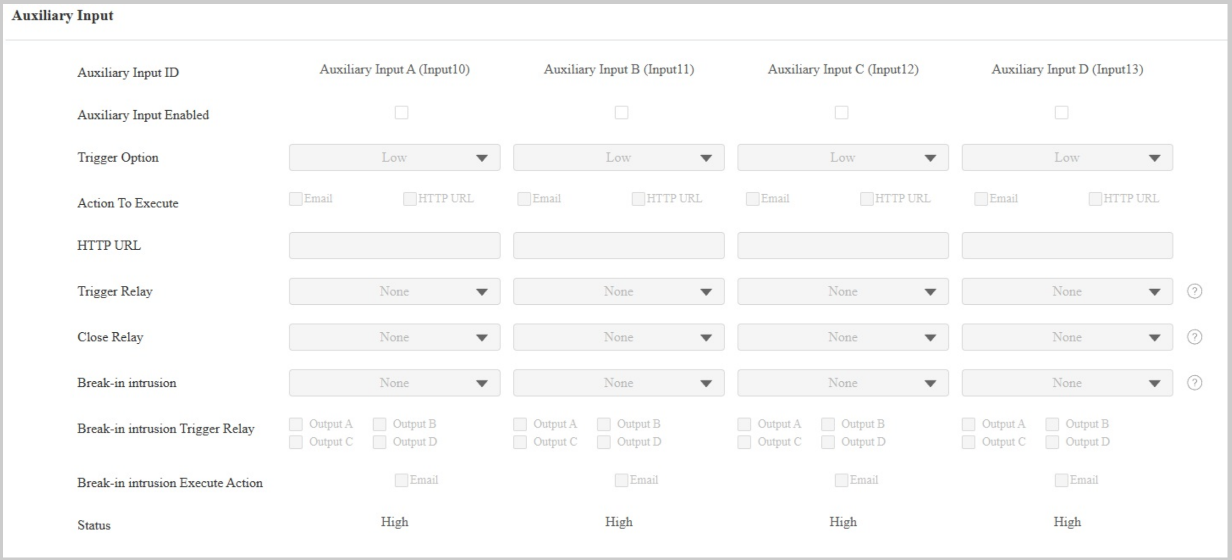
Door Magnetic

Door Magnetic ID	Door Magnetic A (Input6)	Door Magnetic B (Input7)	Door Magnetic C (Input8)	Door Magnetic D (Input9)
Door Magnetic Enabled	□	□	□	□
Trigger Option	Low ▼	Low ▼	Low ▼	Low ▼
Timeout Alert(Sec)	10	10	10	10
Action To Execute	□Email □HTTP URL	□Email □HTTP URL	□Email □HTTP URL	□Email □HTTP URL
HTTP URL				
Trigger Output	None ▼	None ▼	None ▼	None ▼
Close Output	None ▼	None ▼	None ▼	None ▼
Break-in intrusion	None ▼	None ▼	None ▼	None ▼
Break-in intrusion Trigger Relay	□ Output A □ Output B □ Output C □ Output D	□ Output A □ Output B □ Output C □ Output D	□ Output A □ Output B □ Output C □ Output D	□ Output A □ Output B □ Output C □ Output D
Break-in intrusion Execute Action	□Email	□Email	□Email	□Email
Report To Server	□	□	□	□
Status	High	High	High	High

- **Door Magnetic Enabled**: Specify the input used.
- **Trigger Option**: Set the input interface to trigger at a low or high electrical level.
- **Timeout Alert(Sec)**: When the input trigger time exceeds this limit, an alert will be triggered.
- **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 Output**: Specify a relay output to be triggered along with the input.
- **Close Output**: Specify a relay output to be closed when the input is triggered. Please note this feature does not work during the relay schedule time.
- **Break-in intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. This feature is not compatible with the Trigger Output and Close Output functions.
  Click here to learn more information about this feature.

- **Break-in intrusion Trigger Relay**: Specify the relay to be opened.
- **Break-in intrusion Execute Action**: Set whether to send a message to the preconfigured Email address when the break-in intrusion happens.
- **Report to Server**: Set whether to report the alarm logs to ACMS or SmartPlus Cloud where the device is deployed when the timeout alert is triggered.
- **Status:** Display the status of the input signal.

> **Note**
>
> Outputs A, B, C, and D correspond to Relay 5, 6, 7, and 8.



Auxiliary Input

Auxiliary Input ID	Auxiliary Input A (Input10)	Auxiliary Input B (Input11)	Auxiliary Input C (Input12)	Auxiliary Input D (Input13)
Auxiliary Input Enabled	□	□	□	□
Trigger Option	Low	Low	Low	Low
Action To Execute	□ Email □ HTTP URL	□ Email □ HTTP URL	□ Email □ HTTP URL	□ Email □ HTTP URL
HTTP URL				
Trigger Relay	None	None	None	None
Close Relay	None	None	None	None
Break-in intrusion	None	None	None	None
Break-in intrusion Trigger Relay	□ Output A □ Output B □ Output C □ Output D	□ Output A □ Output B □ Output C □ Output D	□ Output A □ Output B □ Output C □ Output D	□ Output A □ Output B □ Output C □ Output D
Break-in intrusion Execute Action	□ Email	□ Email	□ Email	□ Email
Status	High	High	High	High

- **Auxiliary Input Enabled**: Specify the input used.
- **Trigger Option:** Set the input interface to trigger at a 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.
- **Close Relay**: Specify the relay to be closed when the input is triggered. Please note this feature does not work during the relay schedule time.
- **Break-in intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. This feature is not compatible with the Trigger Relay and Close Relay functions.
  Click here to learn more information about this feature.
- **Break-in intrusion Trigger Relay**: Specify the relay to be opened.
- **Break-in intrusion Execute Action**: Set whether to send a message to the preconfigured Email address when the break-in intrusion happens.
- **Status:** Display the status of the input signal.

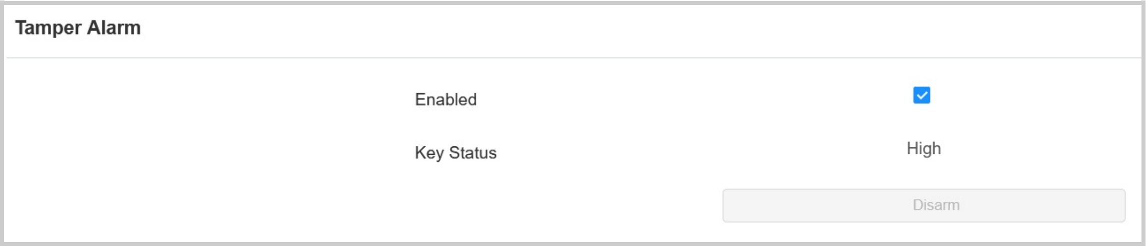
Security

Tamper Alarm

The tamper alarm function prevents anyone from removing the device without permission. Akuvox devices support two types of tamper proof: gravity detection and button status detection.

Click here to view which type is supported by the device and learn the function details.

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



Tamper Alarm

Enabled ☑

Key Status High

- **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.

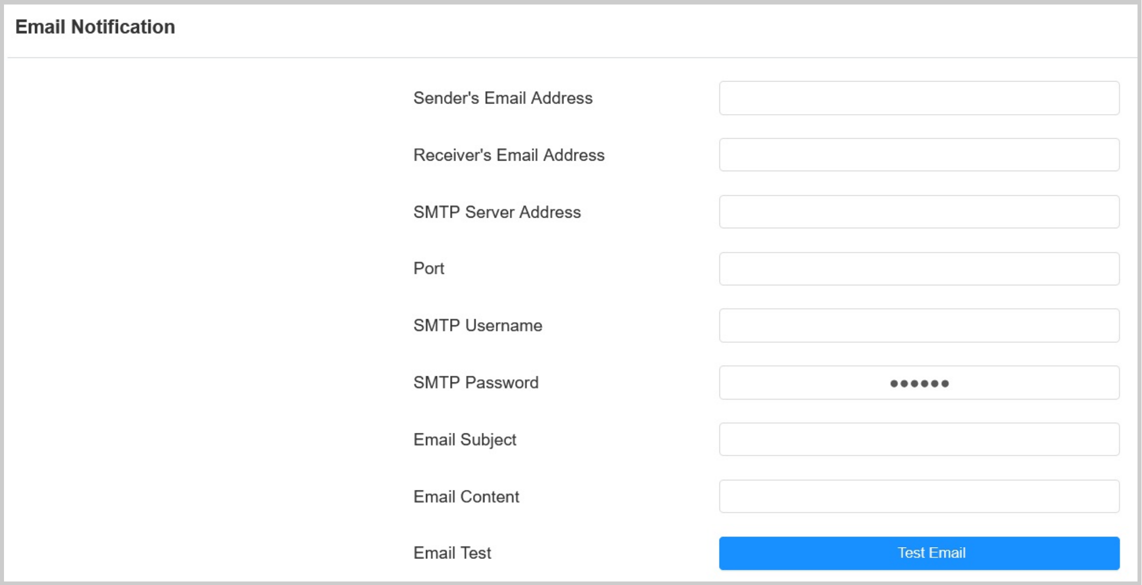
> **Note**
>
> The disarm tab will turn grey when the tamper alarm is cleared.

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

Receiver's Email Address

SMTP Server Address

Port

SMTP Username

SMTP Password ••••••

Email Subject

Email Content

Email Test

- **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

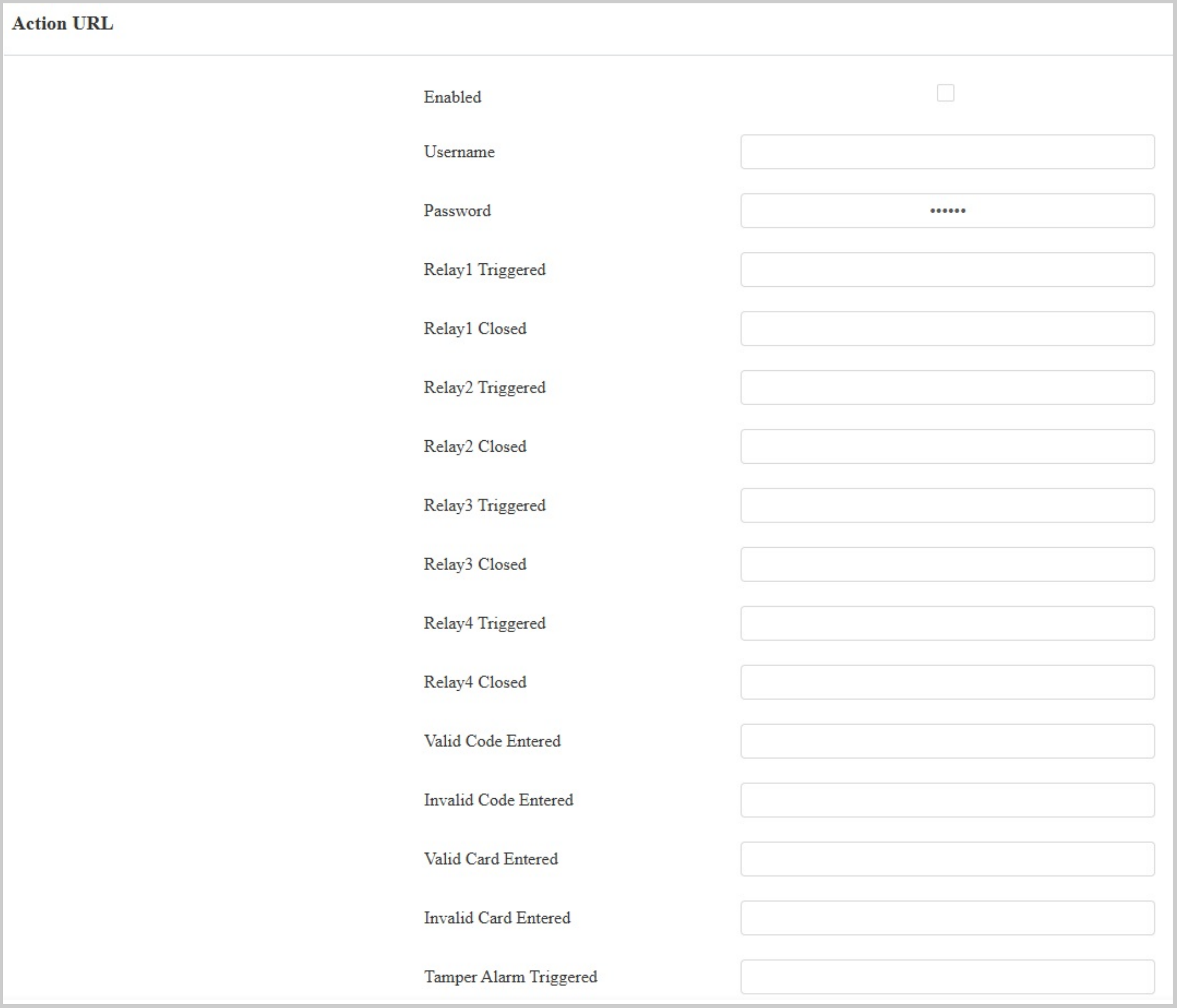
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, PIN code, or RF card access changes.

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?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

To set it up, navigate to the web **Setting > Action URL** interface. You can set up the username and password for authentication.



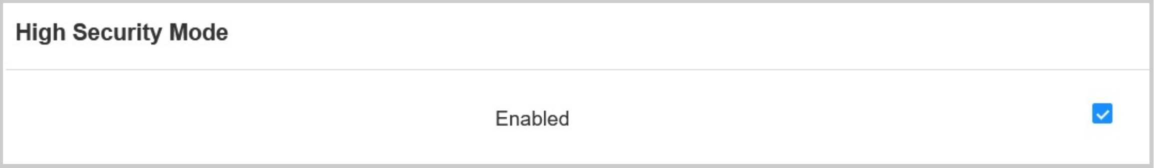
Action URL

Enabled	□
Username	
Password	••••••
Relay1 Triggered	
Relay1 Closed	
Relay2 Triggered	
Relay2 Closed	
Relay3 Triggered	
Relay3 Closed	
Relay4 Triggered	
Relay4 Closed	
Valid Code Entered	
Invalid Code Entered	
Valid Card Entered	
Invalid Card Entered	
Tamper Alarm Triggered	

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	☑

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:

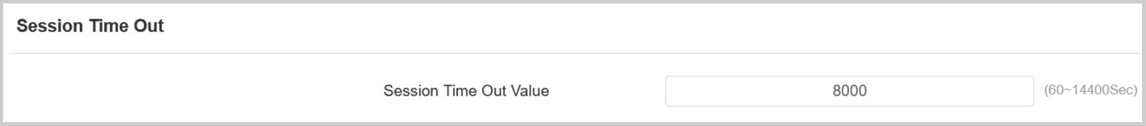
- http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

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.



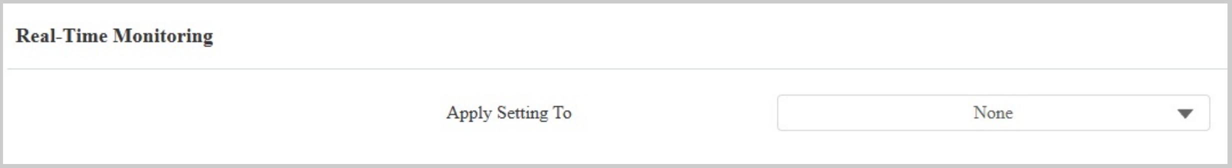
Session Time Out

Session Time Out Value: 8000 (60~14400Sec)

Real-time Monitoring

This feature displays the door status when the device is connected to the SmartPlus Cloud. Property managers and end users can check the door status respectively on the SmartPlus Property Manager platform and SmartPlus App.You need to specify the relay(s) or input(s) that apply this feature. Click here to see the detailed configuration.

Set it up on the **System > Security > Real-time Monitoring** interface.



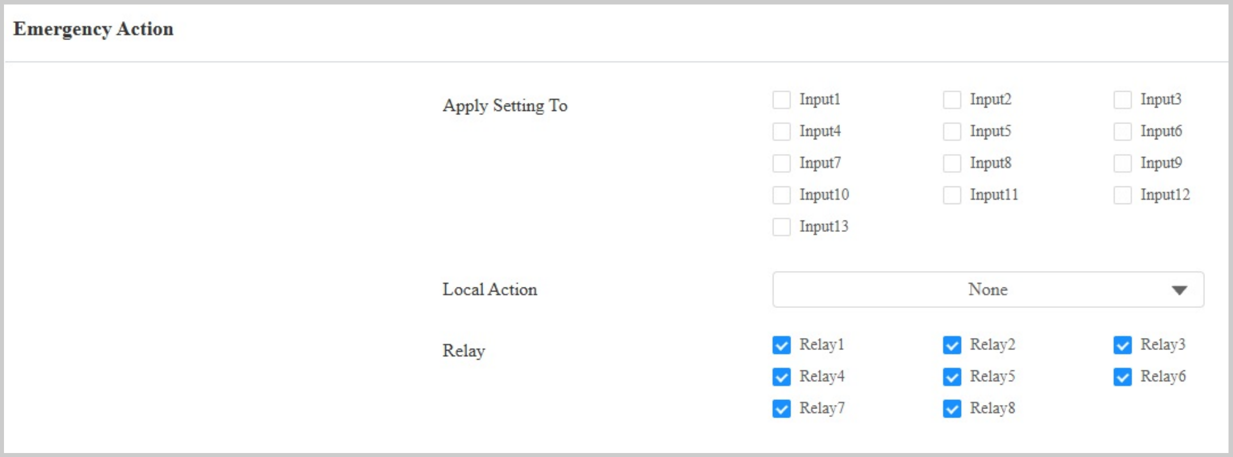
Real-Time Monitoring

Apply Setting To: None

Emergency Action

This feature can keep the door(s) open when an emergency happens(the input is triggered). You need to specify the Input that applies the feature.

Set it up on the **System > Security > Emergency Action** interface.



Emergency Action

Apply Setting To

□ Input1	□ Input2	□ Input3
□ Input4	□ Input5	□ Input6
□ Input7	□ Input8	□ Input9
□ Input10	□ Input11	□ Input12
□ Input13		

Local Action: None

Relay

☑ Relay1	☑ Relay2	☑ Relay3
☑ Relay4	☑ Relay5	☑ Relay6
☑ Relay7	☑ Relay8	

- **Local Action**: Set whether to trigger the local relays with the input trigger. An option called “End Now” will be available when the relay is activated. You can click it to close the relay.
  - **None**: Disable the feature.
  - **Time**: Set the duration time of the relay activation.
  - **Always**: The relay keeps activated once it is triggered.

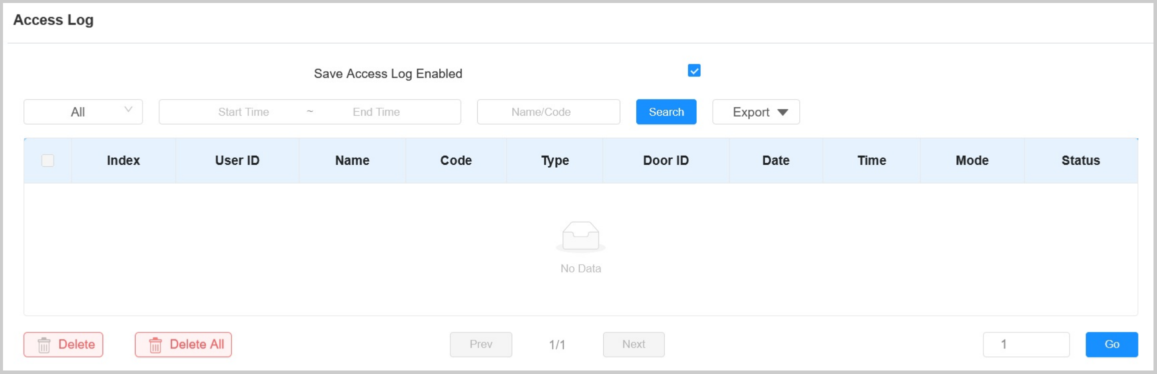
> **Note**
>
> When the device is deployed on the SmartPlus Cloud, property managers can apply emergency actions and the local action will be overwritten. For example, when the local relay is set to be activated for 5 minutes. At 3 minutes, the Cloud issues the Emergency Unlock action, the relay will not be closed after 5 miniutes but only closed when the Cloud issues the Emergency Close action.

Logs

Access Logs

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.



Access Log

Save Access Log Enabled ☑

All | Start Time ~ End Time | Name/Code | Search | Export

□	Index	User ID	Name	Code	Type	Door ID	Date	Time	Mode	Status

No Data

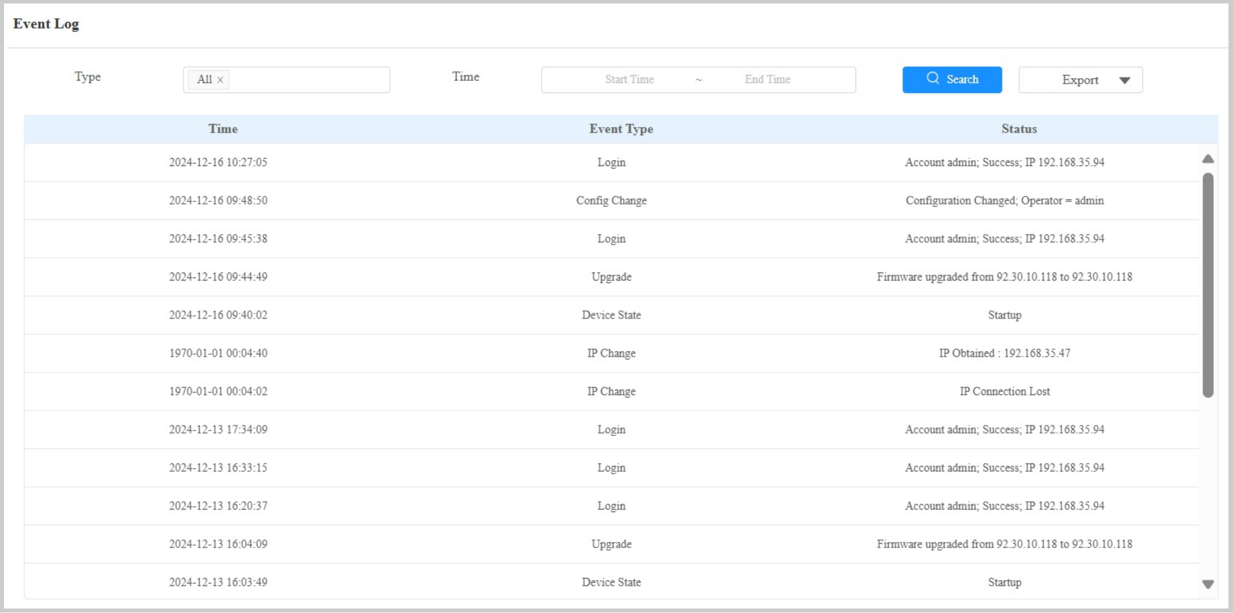
Delete | Delete All | Prev | 1/1 | Next | 1 | Go

- **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.

Event Logs

The event logs record the key events such as the status change of input, relay, tamper alarm, etc. This helps track the status and changes of the device.

Check event logs on the **Status > Event Log** interface. You can export the log in CSV format.



Event Log

Type: All ×

Time: Start Time ~ End Time

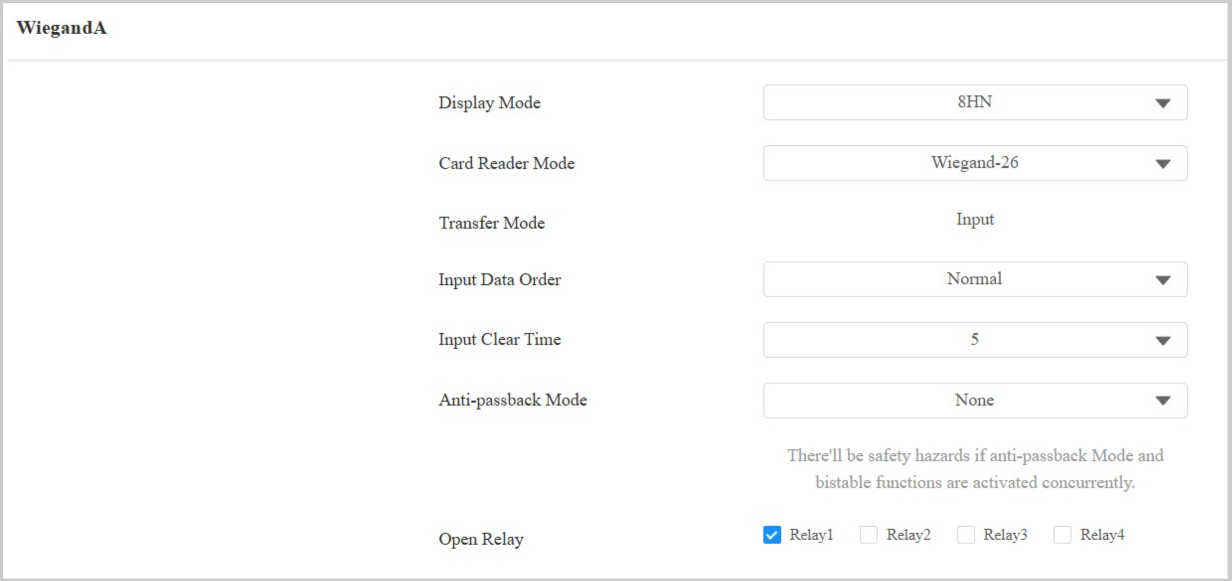
Time	Event Type	Status
2024-12-16 10:27:05	Login	Account admin; Success; IP 192.168.35.94
2024-12-16 09:48:50	Config Change	Configuration Changed; Operator = admin
2024-12-16 09:45:38	Login	Account admin; Success; IP 192.168.35.94
2024-12-16 09:44:49	Upgrade	Firmware upgraded from 92.30.10.118 to 92.30.10.118
2024-12-16 09:40:02	Device State	Startup
1970-01-01 00:04:40	IP Change	IP Obtained : 192.168.35.47
1970-01-01 00:04:02	IP Change	IP Connection Lost
2024-12-13 17:34:09	Login	Account admin; Success; IP 192.168.35.94
2024-12-13 16:33:15	Login	Account admin; Success; IP 192.168.35.94
2024-12-13 16:20:37	Login	Account admin; Success; IP 192.168.35.94
2024-12-13 16:04:09	Upgrade	Firmware upgraded from 92.30.10.118 to 92.30.10.118
2024-12-13 16:03:49	Device State	Startup

Integration with Third-Party Device

Integration via Wiegand

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

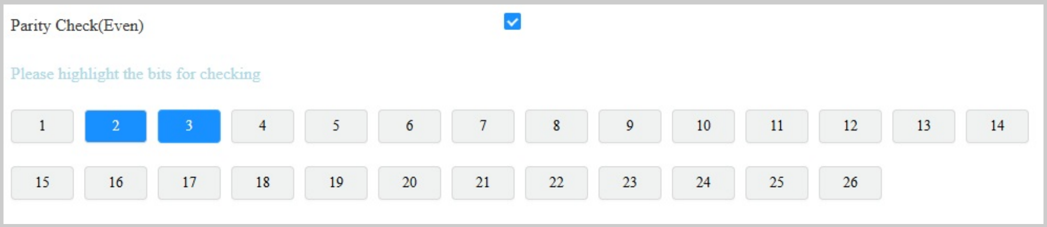
To set it up, navigate to the web **Device > Wiegand** interface.



WiegandA

Display Mode	8HN
Card Reader Mode	Wiegand-26
Transfer Mode	Input
Input Data Order	Normal
Input Clear Time	5
Anti-passback Mode	None
	There'll be safety hazards if anti-passback Mode and bistable functions are activated concurrently.
Open Relay	☑ Relay1 □ Relay2 □ Relay3 □ Relay4

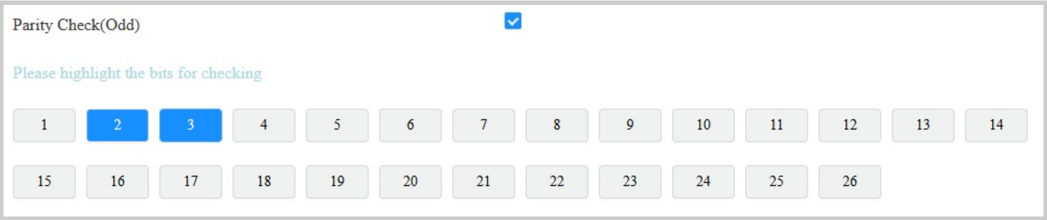
- **Display Mode**: Select the Wiegand card code format from the provided options.
  - **Ignore Facility Code**: This option is available when 6H3D5D(WG26) is selected. When enabled, the first three bits of cards will be ignored for successful card reading.
- **Card Reader Mode**: The transmission format should be identical between the access control terminal and the third-party device. It is Wiegand 26 by default.
  When **Customize** is selected, further set up the following options:
  - **Display Mode**:
    - **HEX(Hexadecimal)**: The default option. Base-16 numbering system that uses digits from 0 to 9 and letters from A to F.
    - **DEC(Decimal)**: The base-10 numbering system that uses digits 0-9 only.
  - **Total Number of Bits**: Define the bit number of the card data for processing. The range is from 1 to 128. The default is 26.
  - **Card Number Length**: Specify the bits used to store card number, limited by the **Total Number of Bits**. For example, when the total bit number is 26, you can specify a length between 1 and 26 to be read as card code.
  - **Use Site Code**: Set whether to use the site code. You may need to enable it when third-party access control system requires the site code for processing the card's information.
    When enabled, specify the bits read by the device, limited by the **Total Number of Bits**. For example, when the total bit number is 26, the range is from 1 to 26.
  - **Parity Check(Even)**: When enabled, the sum of selected bits must be even to pass verification. For example, when the second and third bits are selected and their sum is even, the parity check passes.



Parity Check(Even) ☑

Please highlight the bits for checking

- **Parity Check(Odd)**: When enabled, the sum of selected bits must be odd to pass verification. For example, when the second and third bits are selected and their sum is odd, the parity check passes.



Parity Check(Odd) ☑

Please highlight the bits for checking

Tip

- Parity check is a simple error detection mechanism used to ensure that data has not been corrupted during transmission or storage.
- When it is enabled, the device will first perform the check. Only if the check passes will it read the card number.
- Card Reading Example:
  Suppose total number of bits is 32 and the card data is 0011 1000 0101 1100 0010 0100 0011 1110.

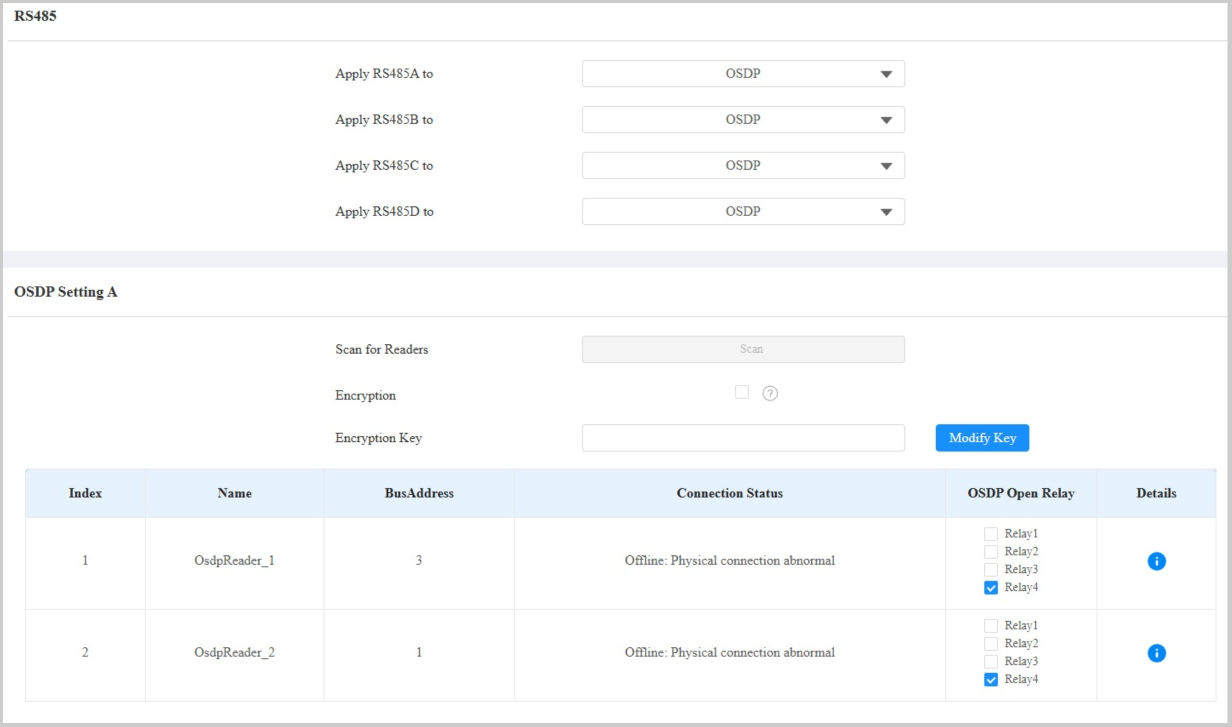
Display Mode	Card Number Length	Site Code	Parity Check
HEX: 385C243E	13-32 Bits: C243E	1-12 Bits: 385	• 2-15 bits(Even): The s is 7, fail to pass the check. • 16-31 bits(Odd): The s is 7, successfully pass the check.

- **Transfer Mode**: It is **Input** by default. It means the device serves as a receiver, which allows users to open doors by swiping an RF card or entering a PIN code on the third-party card reader.
- **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. For example, the card code is 00345678.
  - **Normal**: The code is 00345678 displayed on the device’s carding adding interface.
  - **Reversed**: The code is 00785634 displayed on the device’s carding adding interface.
- **Input Clear Time**: When the interval of entering passwords exceeds the time, all entered passwords will be cleared.
- **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.
- **Open Relay**: Select the relay triggered by Wiegand.

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.

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



RS485

Apply RS485A to: OSDP

Apply RS485B to: OSDP

Apply RS485C to: OSDP

Apply RS485D to: OSDP

OSDP Setting A

Scan for Readers: Scan

Encryption: □

Encryption Key: Modify Key

Index	Name	BusAddress	Connection Status	OSDP Open Relay	Details
1	OsdpReader_1	3	Offline: Physical connection abnormal	□ Relay1 □ Relay2 □ Relay3 ☑ Relay4	ⓘ
2	OsdpReader_2	1	Offline: Physical connection abnormal	□ Relay1 □ Relay2 □ Relay3 ☑ Relay4	ⓘ

- **Apply RS485 To**: OSDP card readers can be connected to A094 via RS485 A/B/C/D interfaces. One interface can support up to 4 readers. When the card reader is connected via RS485A/B, A094 can scan it and display its status on the web interface.

> **Tip**
>
> It is suggested to use RS485A/B for card reader connection. Using RS485C/D may lead to connection failure.

- **OSDP Setting A/B**: The settings are available when OSDP is enabled.
  - **Scan for Readers**: Click **Scan** to detect the connected card reader.
  - **Encryption**: Check this option when the OSDP protocol is encrypted.
  - **Encryption Key:** Fill in the key when **Encryption** is checked. Please confirm the key with the card reader service provider.
  - **Modify Key**: Click to modify the encryption key, which must be 32 bits long and can include numbers (0-9) and letters (a-f, A-F).
  - **Connection Status**: Display whether the reader is online and connected properly.
  - **OSDP Open Relay**: Check the relay to be opened.
  - **Details**: Click to view the card reader's information.
- **OSDP Setting C/D**: The settings are available when OSDP is enabled.
  - **Encryption**: Check this option when the OSDP protocol is encrypted.
  - **Key Value**: Fill in the key when **Encryption** is checked. Please confirm the key with the card reader service provider.
  - **OSDP Open Relay**: Check the relay to be opened.
- **Virtual Door Mode**:
  - It is disabled by default. Users can ONLY open relays that are checked on both the OSDP setting and Access Setting interfaces.

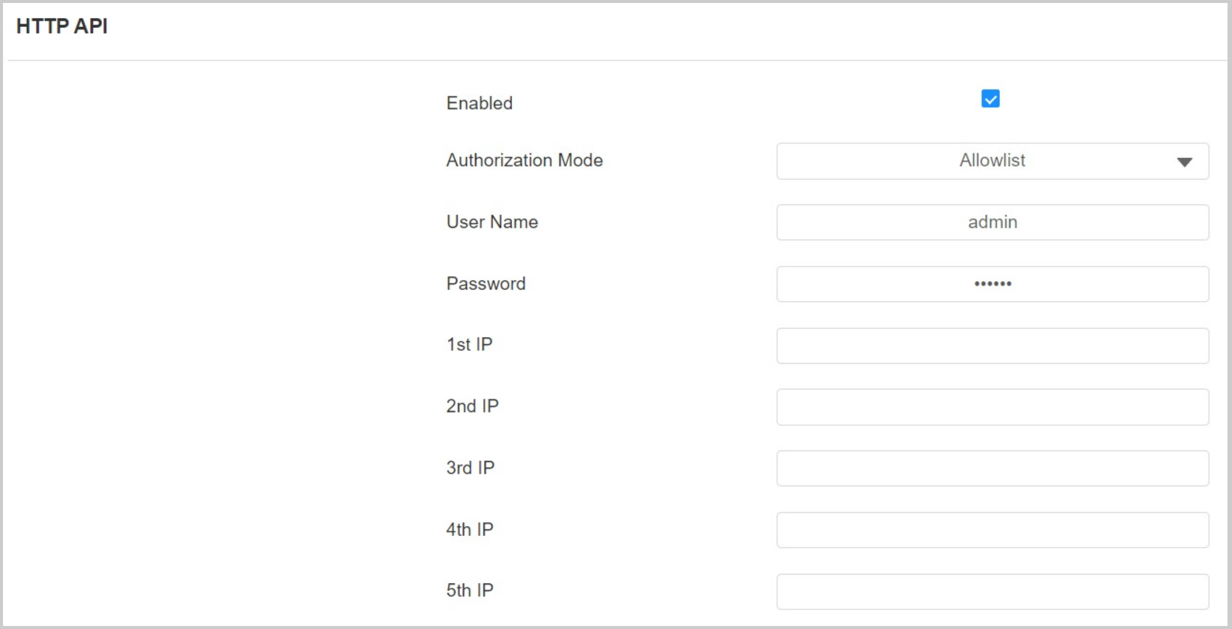
- If it is enabled, users can open relays that are checked on the OSDP setting interface with their credentials, regardless of whether they are checked on the Access Setting interface.

> **Note**
>
> Click here to view the detailed configuration of the OSDP feature.

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	☑
Authorization Mode	Allowlist
User Name	admin
Password	••••••
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

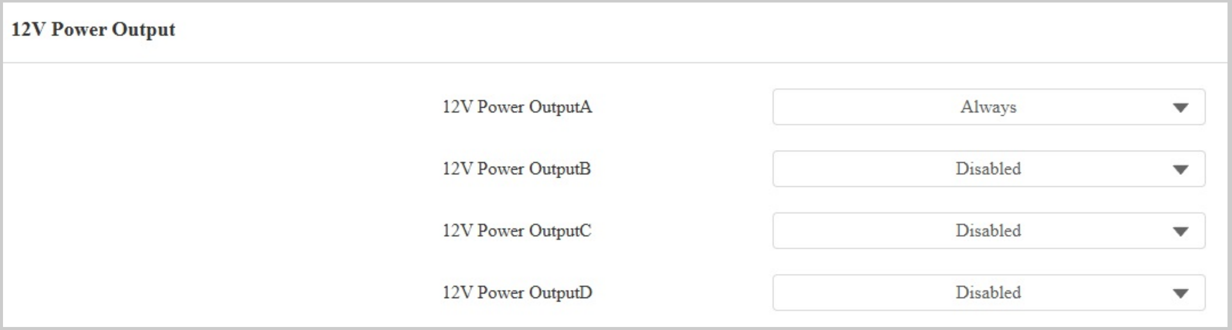
- **HTTP API Enable:** Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode:**
  - **None**: No authentication is required for HTTP API as it 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 only used by Akuvox developers.
- **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	Always
12V Power OutputB	Disabled
12V Power OutputC	Disabled
12V Power OutputD	Disabled

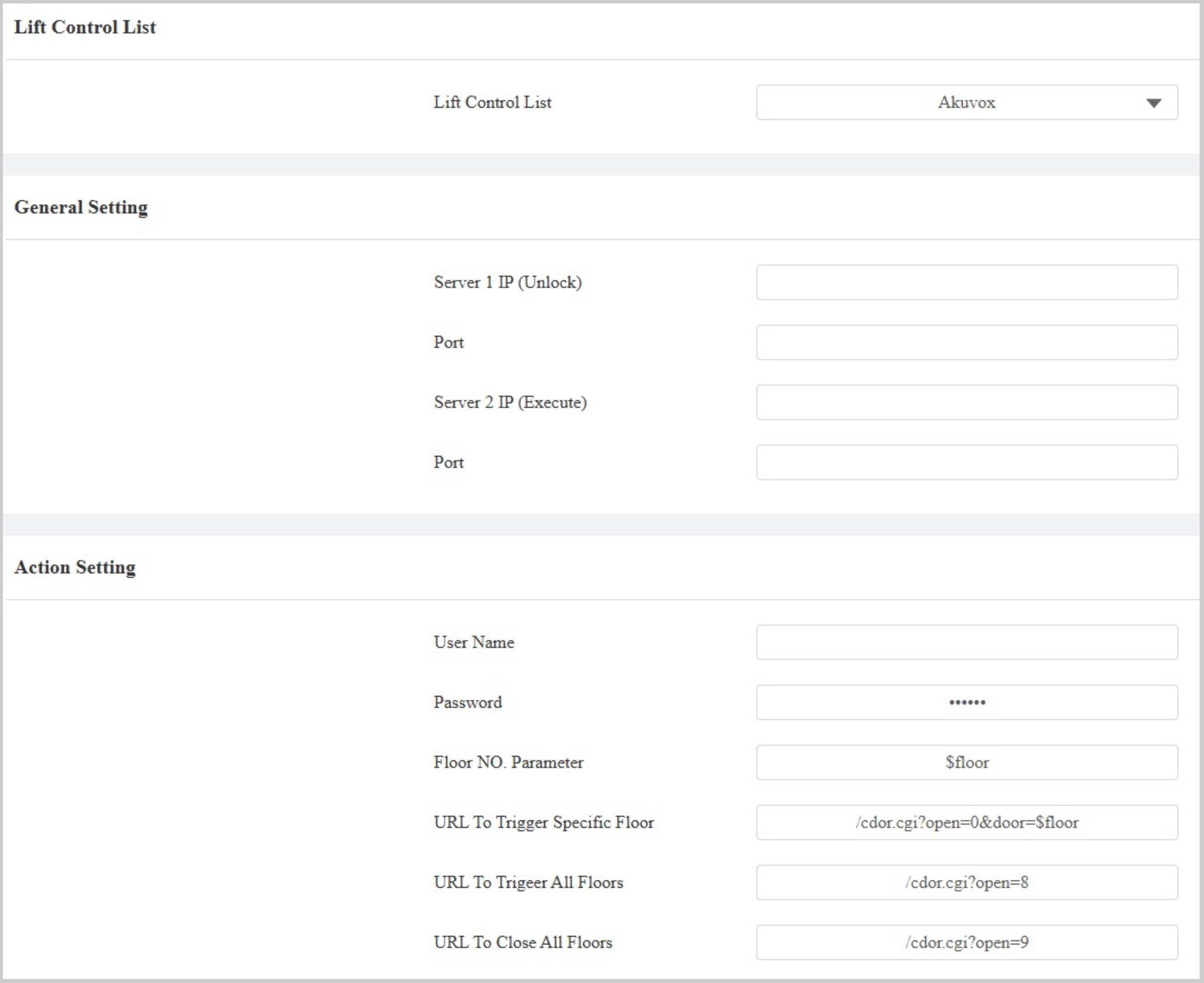
- **Relay ID:** Specify the relay for the power supply output.
- **Power Output Type**: Select the power output type.
  - **Always:** The device will provide a continuous power supply. The device's relay status will be changed from NC to NO status after the relay is triggered, thus cutting off the power 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, or 10 seconds). 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)**: This option is available when **Triggered by Open Relay** is selected. Set the relay reset time.

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

Lift Control

The device can be connected to the Akuvox lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through various types of access methods.

Set it up on the **Device > Lift Control** interface.



Lift Control List

Lift Control List	Akuvox

General Setting

Server 1 IP (Unlock)	
Port	
Server 2 IP (Execute)	
Port	

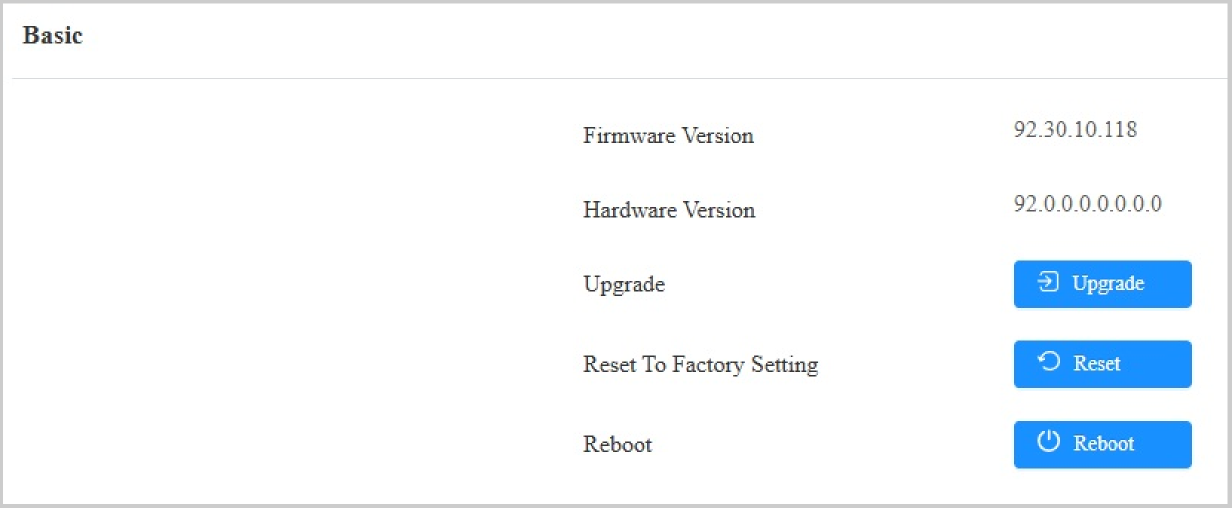
Action Setting

User Name	
Password	••••••
Floor NO. Parameter	$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=$floor
URL To Trigeer All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9

- **Server 1 IP(Unlock)**: The IP address of the Akuvox lift control server. It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute)**: The IP address of the server that triggers lift control.
- **Port**: The server port of the lift controller server.
- **User Name**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.

Firmware Upgrade

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



Basic

Firmware Version	92.30.10.118
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.

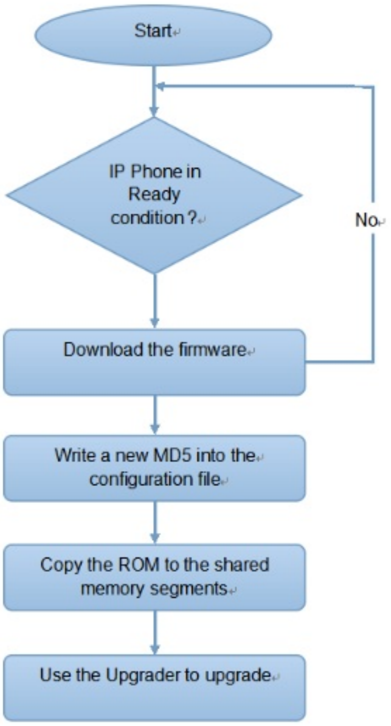
Auto-Provisioning via Configuration File

You can configure and upgrade the device through the web interface using one-time or scheduled auto-provisioning with configuration files. This eliminates the need to set up configurations manually, saving you time and effort.

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:


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

Configuration Files for Auto-provisioning

Configuration files for auto-provisioning come in two formats: general configuration files and MAC-based configuration files.

Differences:

- **General Configuration Provisioning**:

A general configuration file is stored on a server, allowing all related devices to download the same file to update parameters.

- **MAC-Based Configuration Provisioning**:

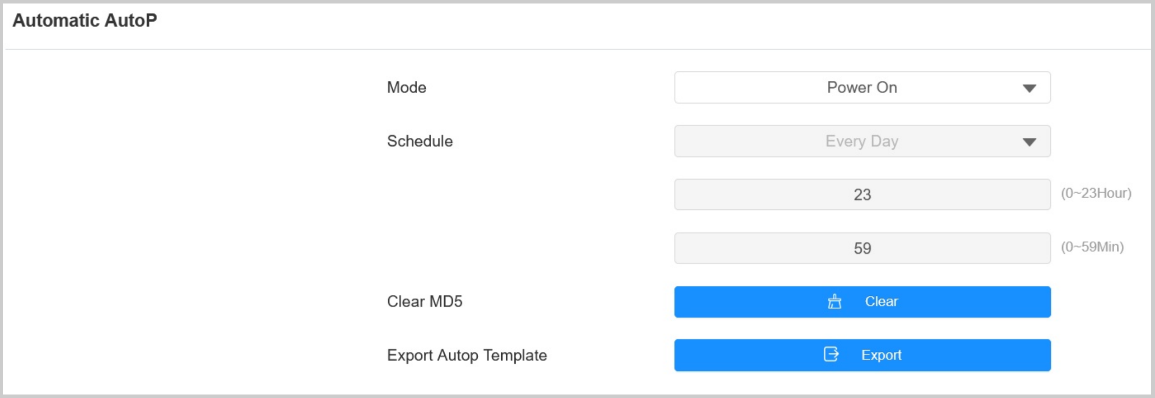
MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

> **Note**
>
> - Configuration files must be in CFG format.
> - The name of the general configuration file for batch provisioning varies by model.
> - The MAC-based configuration file is named after its MAC address.
> - Devices will first access general configuration files before the MAC-based ones if both types are available.
>
> 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: Power On

Schedule: Every Day

23 (0~23Hour)

59 (0~59Min)

Clear MD5: Clear

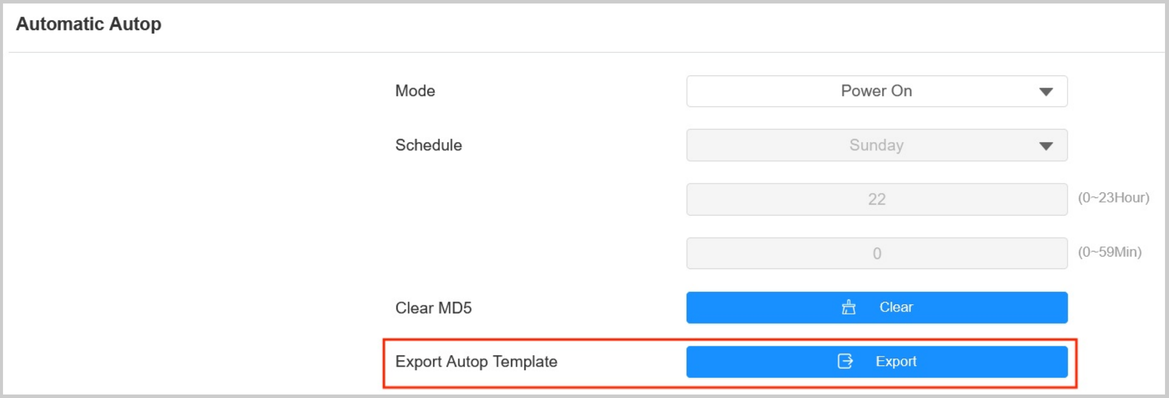
Export Autop Template: Export

- **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: Power On

Schedule: Sunday

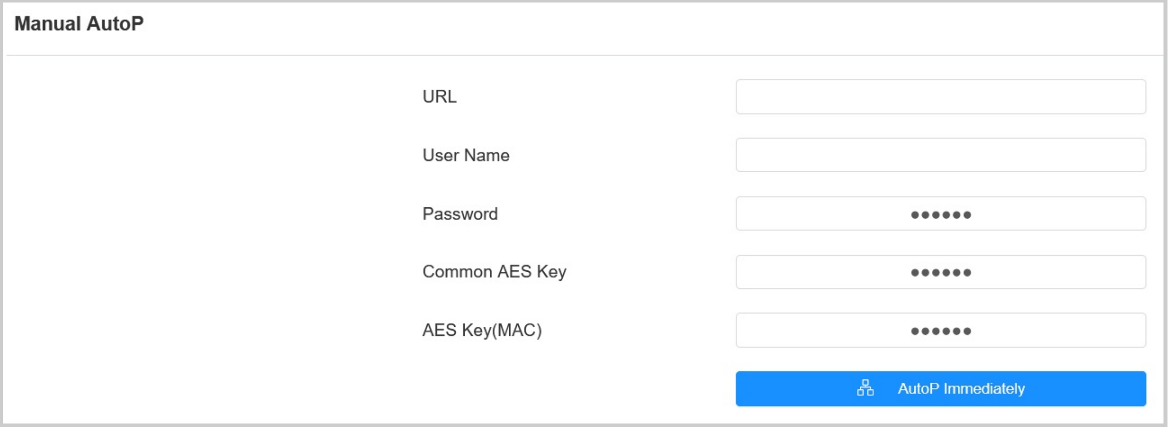
22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

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



Manual AutoP

URL:

User Name:

Password: ••••••

Common AES Key: ••••••

AES Key(MAC): ••••••

- **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

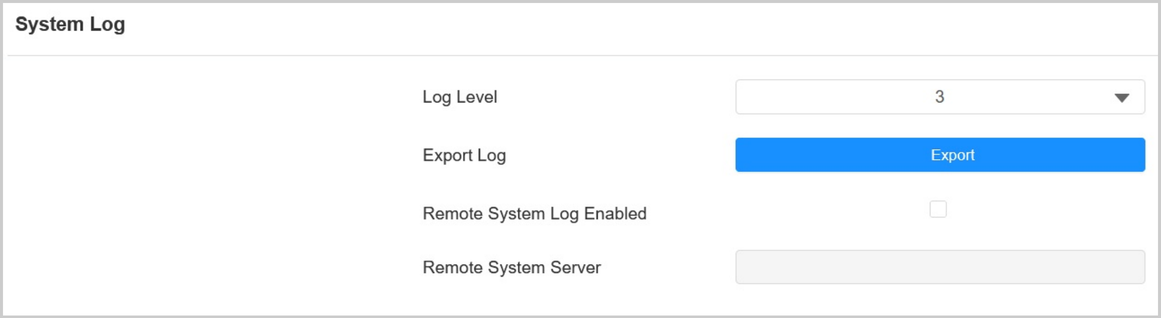
- Akuvox do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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



System Log

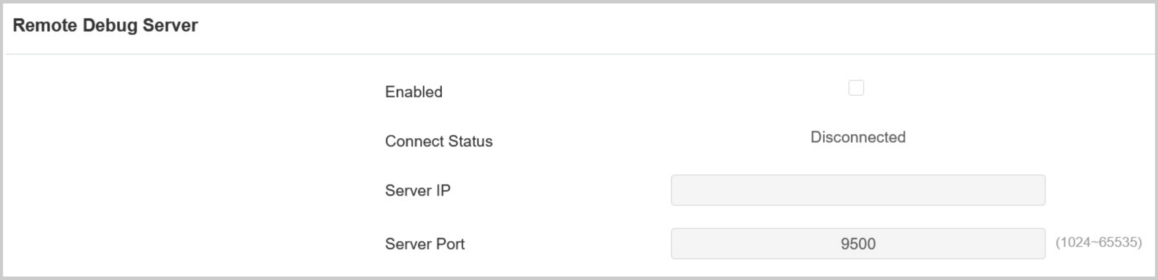
Log Level	3
Export Log	Export
Remote System Log Enabled	□
Remote System Server	

- **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.



Remote Debug Server

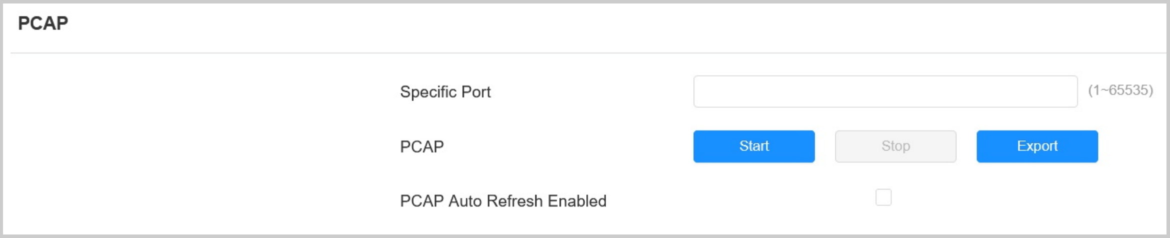
Enabled	□
Connect Status	Disconnected
Server IP	
Server Port	9500 (1024~65535)

- **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.



PCAP

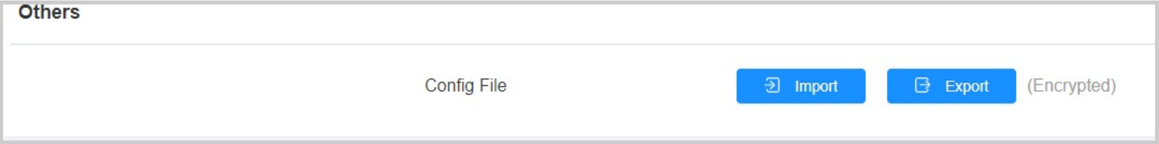
Specific Port		(1~65535)
PCAP	Start Stop Export	
PCAP Auto Refresh Enabled	□	

- **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.



Others

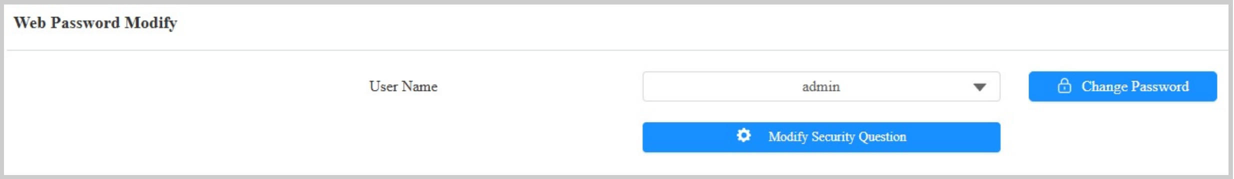
Config File

Account & Password

Modify Web Password

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

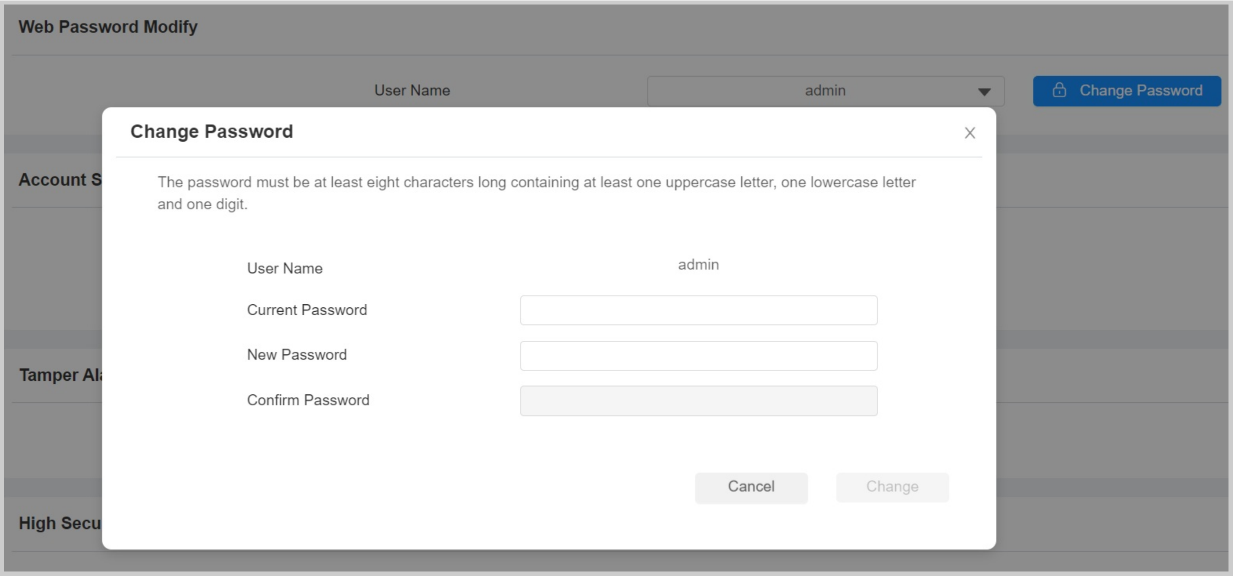
To set it up, go to **System > Security > Web Password Modify** interface.



Web Password Modify

User Name: admin

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



Change Password

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

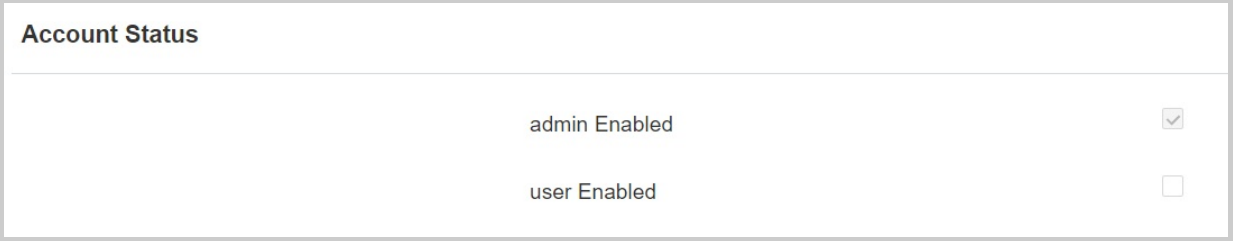
User Name: admin

Current Password:

New Password:

Confirm Password:

To enable or disable the user account, scroll to the **Account Status** section. The default password for the user account is **user**.



Account Status

admin Enabled ☑

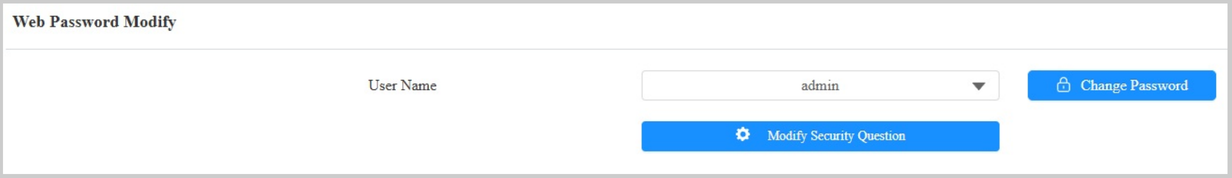
user Enabled ☐

Modify Security Questions

Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

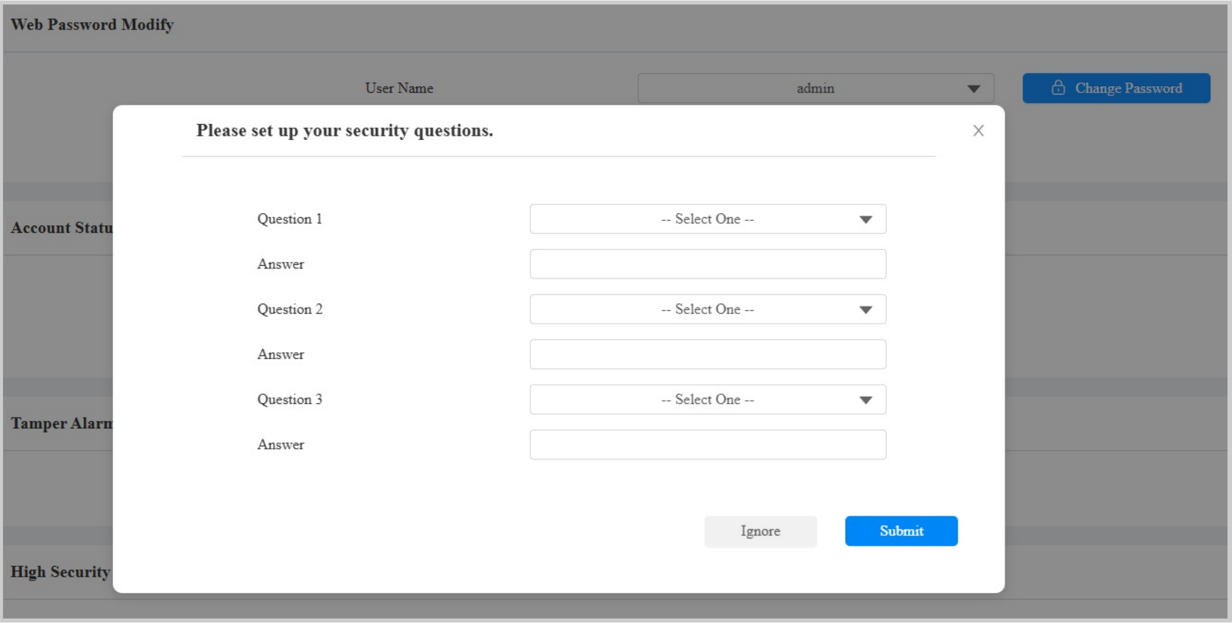
If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

Set it up on the **System > Security** interface. Click **Modify Security Question**.


Web Password Modify

User Name: admin

You need to first enter the right password for verification and then set up the security questions.


Web Password Modify

User Name: admin

Please set up your security questions.

Question 1: -- Select One --

Answer:

Question 2: -- Select One --

Answer:

Question 3: -- Select One --

Answer:

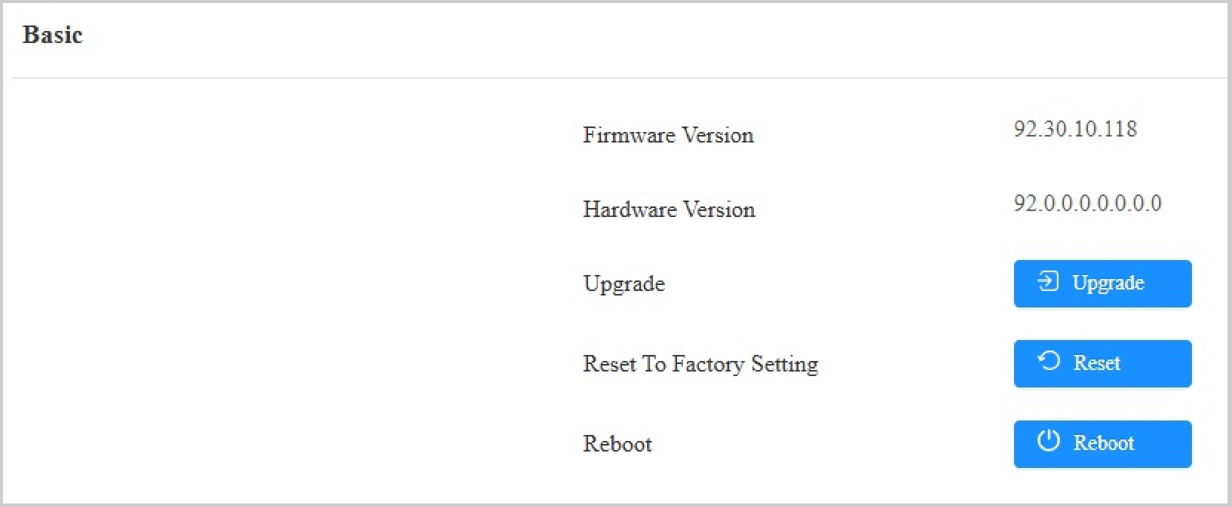
System Reboot & Reset

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.

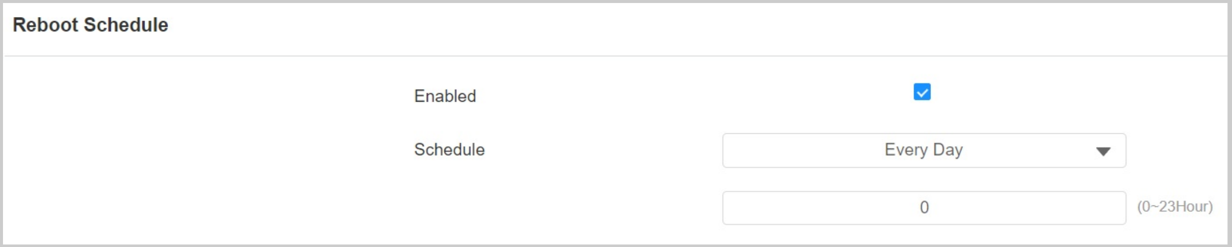


Basic

Firmware Version	92.30.10.118
Hardware Version	92.0.0.0.0.0.0
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reboot	Reboot

- To set up the device reboot schedule

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

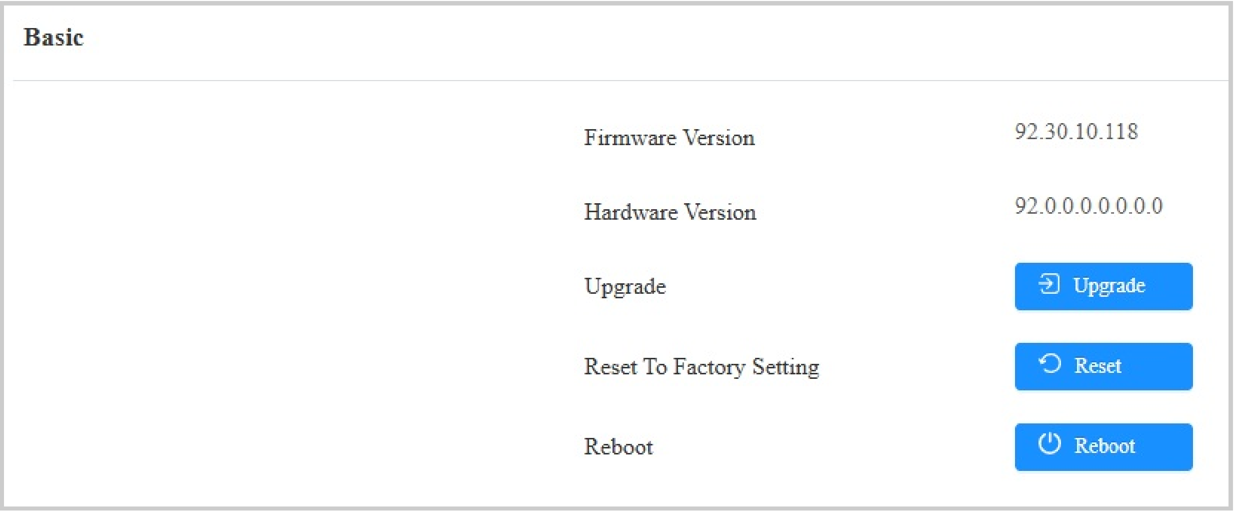


Reboot Schedule

Enabled	☑
Schedule	Every Day
	0 (0~23Hour)

Reset

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



Basic

Firmware Version 92.30.10.118

Hardware Version 92.0.0.0.0.0.0

Upgrade

Reset To Factory Setting

Reboot