Akuvox

Table of contents

Akuvox A095S Access Controller Administrator Guide

About This Manual 6

Product Overview 8

Changelog 9

Model Specification 10

Indicator 12

Access the Device 14

- Obtain Device IP Address 14
- Access the Web Settings 15
- Set IP Announcement 16

Introduction to Configuration Menu 17

Language and Time 19

- Language 19
  - Custom Language 19
- Time 20

Volume Control 21

Network Setting 22

Network Status 22
Device Network Configuration 22
Wi-Fi Connection 24
LTE Wireless Connection 24
SNMP 26
TR069 27
Device Web HTTP Setting 28
Door Setting 29
Door Configuration 30
Auxiliary Output Configuration 32
Door Position Switch Configuration 35
Web Relay 36
Door Access Schedule Management 39
Create Access Schedule 39
Import and Export Door Access Schedule 40
Door Schedule 40
Holiday Schedule 41
Door-opening Configuration 44
Unlock by Public PIN Code 44
User-specific Access Methods 44

Unlock by Private PIN Code 45
Unlock by RF Card 45
Unlock by License Plate 46
Access Setting 47
Import and Export User Data 48
Unlock by HTTP Commands 48
Unlock by Exit Button 49
Unlock by Emergency Button 50
Security 53
Tamper Alarm 53
Disarm Setting 53
Security Notification 54
Action URL 55
High Security Mode 58
Web Interface Automatic Log-out 59
Real-time Monitoring 59
Emergency Action 60
Logs 62
Access Logs 63
Event Logs 63

Integration with Third-party Devices 65
Integration via Wiegand 65
Integration via RS485 69
Integration via HTTP API 70
Power Output Control 72
Lift Control 74
Firmware Upgrade 76
Auto-Provisioning via Configuration File 77
Provisioning Principle 77
Configuration Files for Auto-provisioning 78
Autop Schedule 79
Static Provisioning 80
Debug 83
System Log for Debugging 83
Remote Debug Server 83
PCAP for Debugging 84
Backup 86
Backup via SD Card 86
Account & Password 87
Modify Web Password 87

Modify Security Questions 88

System Reboot & Reset 90

Reboot 90

Reset 91

Akuvox

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

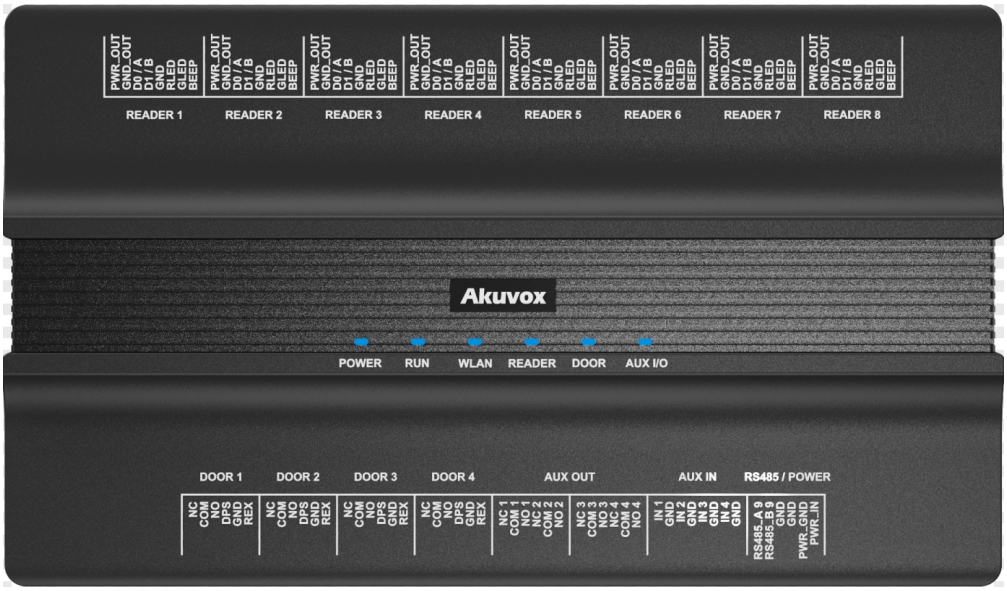


AKUVOX A095
ACCESS CONTROLLER
Administrator Guide

Akuvox

Thank you for choosing the Akuvox A095 access controller. This manual is intended for administrators who need to configure the access controller properly. This manual is written based on firmware version 95.30.11.9, 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 A095S 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 8 built-in relays, allowing it to control a maximum of four doors and providing secure card access. The A095S is suitable for applications in commercial buildings, hospitals, and warehouses, offering comprehensive control of building entrances and surroundings.

Changelog

What's new in version 95.30.11.9:

- Support the Reset Alarm When Door Closed and Relock When Door Closed features for door settings.
- Support the Door Keep Active While Card Present feature.

Click here to view the previous versions' changelog.

Akuvox

Model Specification

Model	A095S
Operation System	Linux
Flash	256MB
RAM	128MB
Ethernet	2xRJ45, 10/100 Mbps adaptive
Power Supply	PoE+ or 12VDC/5A power adapter
Power Output	x8 with a maximum of 500mA. Support power output when the device is powered by PoE+.
Relays	x8
I/O	x12
Reset Button	✓
Indicator Light	✓
Wiegand/RS458	x8
RTC	✓
Wi-Fi	✓, Wi-Fi 6
TF Card Slot	✓

Model	A095S
LTE	Optional

Indicator

Indicator Type	Color	Status	
Power	Blue	ON	
RUN	Blue	Flashing	
	Red	Flashing	The device finishes initialization, and some features malfunction.
WLAN	Blue	ON	
READER	Blue	Flashing	
DOOR	Blue	Flashing	
AUX I/O	Blue	Flashing	

Description
The device is powered on.
The device finishes initialization and all features function normally.

Description
The device connects to Wi-Fi or 4G network.
The device receives signals from the READER interface.
The device receives signals from the DOOR interface.
The device receives signals from the AUX I/O interface.

Access the Device

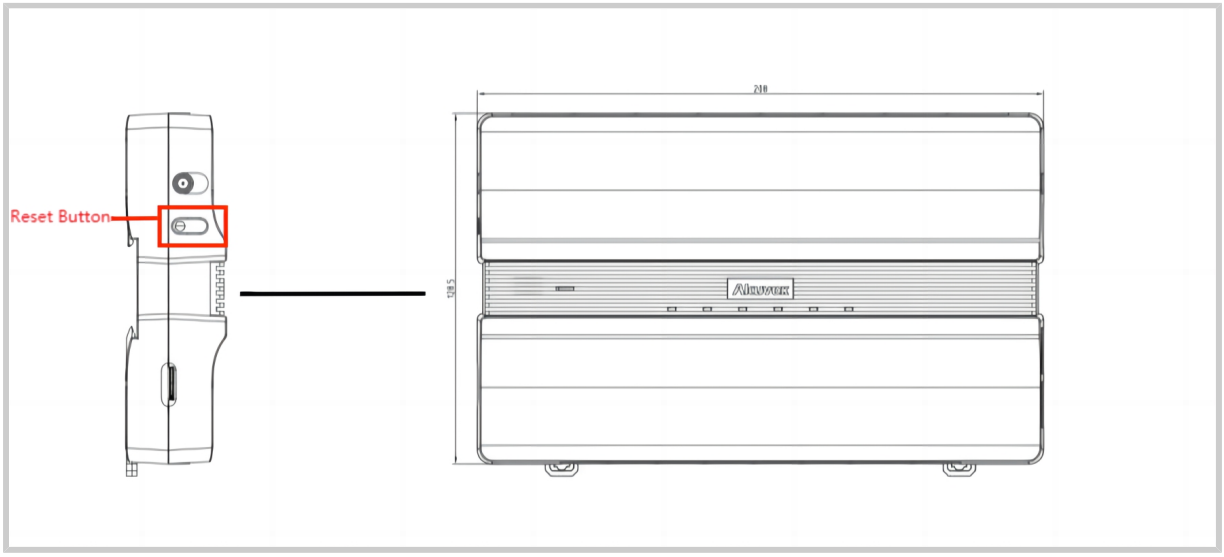
Access the device's settings by logging in to its web interface.

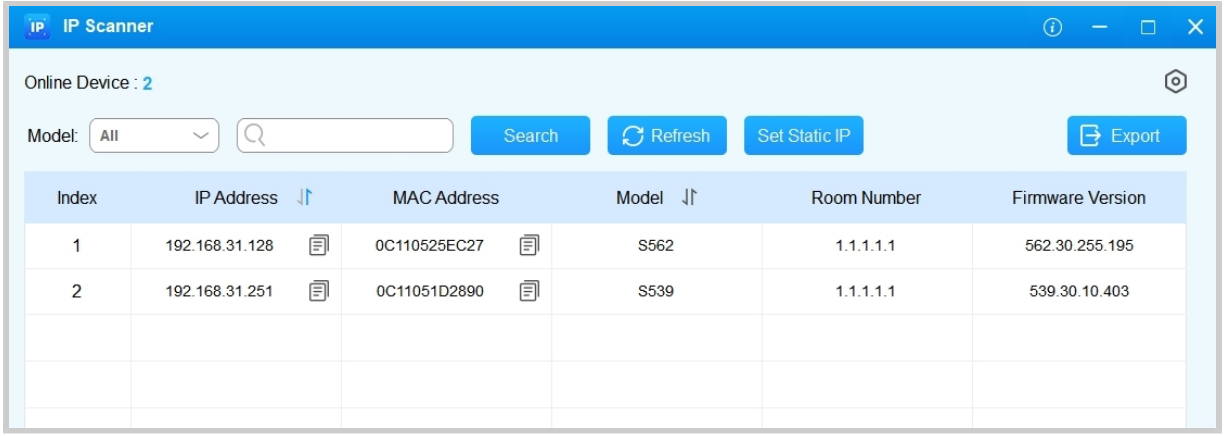
Obtain Device IP Address

Before configuring the device, please make sure the device is installed correctly and connected to a normal network.

You can obtain the device IP by:

- Pressing the reset button.
- Search for it with the IP scanner tool on the same local network(LAN).

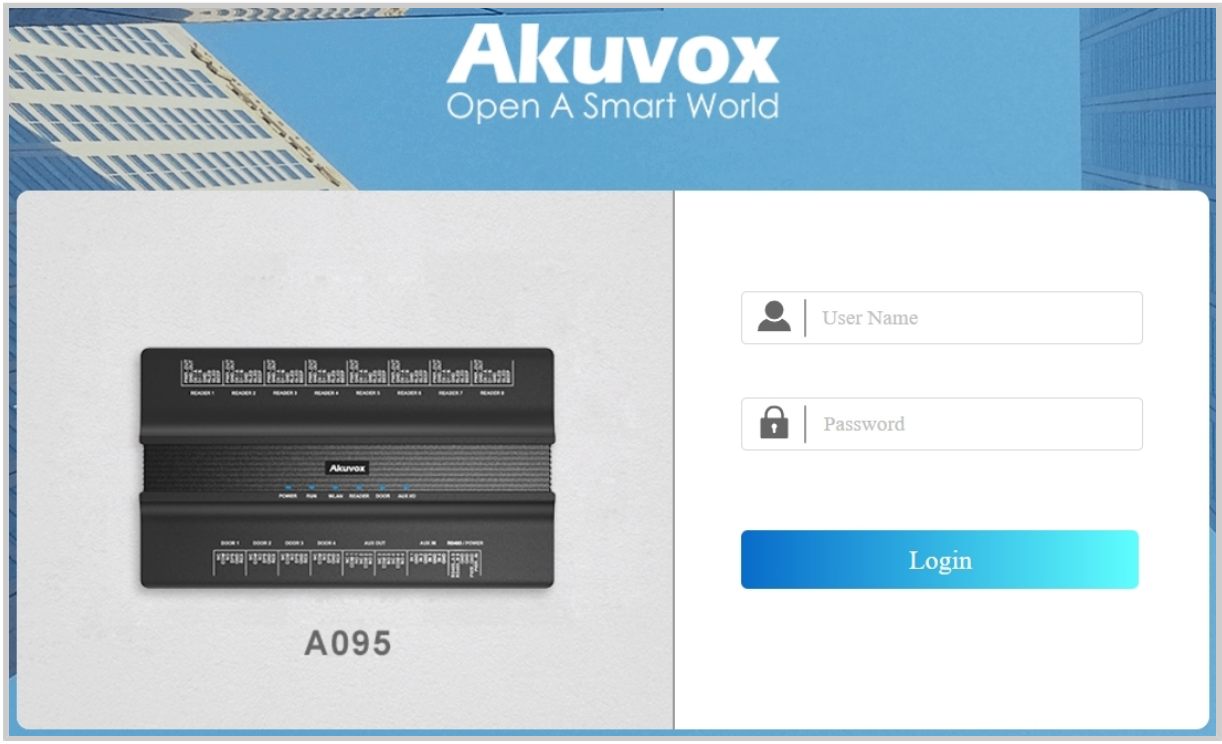




IP scanner

Access the Web Settings

Enter the device IP in a browser. The initial username and password(case-sensitive) are **admin**.

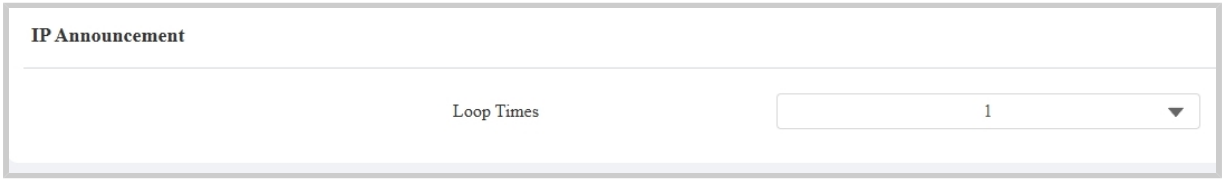


Note

- 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.
- Your computer should be on the same LAN as the device.

Set IP Announcement

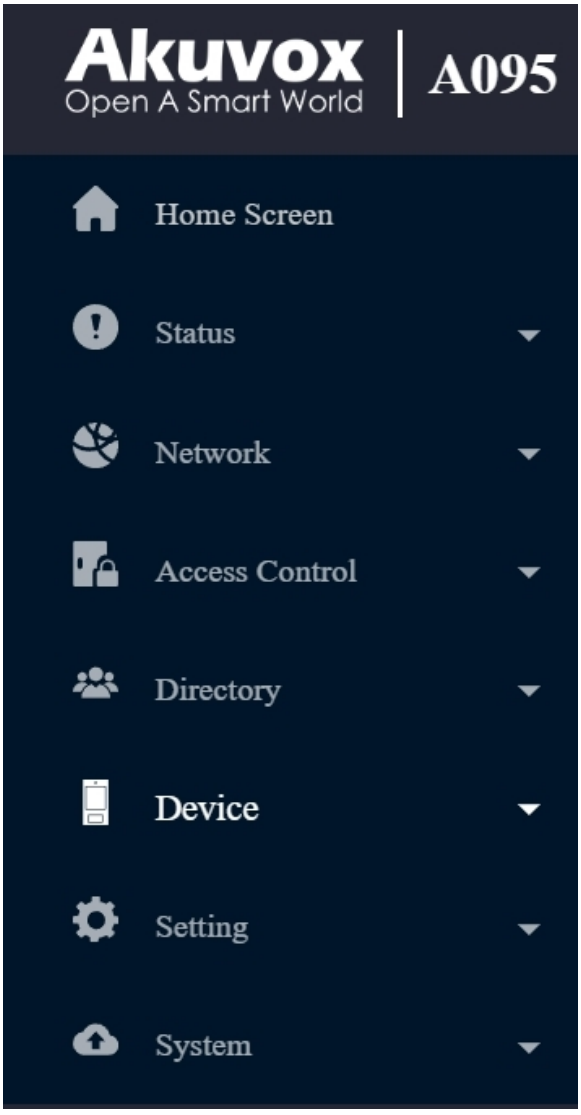
You can set up the IP announcement loop times on the **Device > Audio** interface.



- **Loop Times**: The value range is 1 to 5. The default is 1.

Introduction to Configuration Menu

- **Status**: This section gives you basic information, such as product information, network information, and access logs.
- **Network**: This section covers network settings.
- **Access Control**: This section covers relay, input, web relay, card setting, etc.
- **Directory**: This section is for user management.
- **Device**: This section includes the reader, lift control, audio, and SD card 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.


Akuvox
Open A Smart World
A095
Home Screen
Status
Network
Access Control
Directory
Device
Setting
System

Language and Time

Language

You can switch the web language in the upper-right corner.

Currently, English and Simplified Chinese are supported.



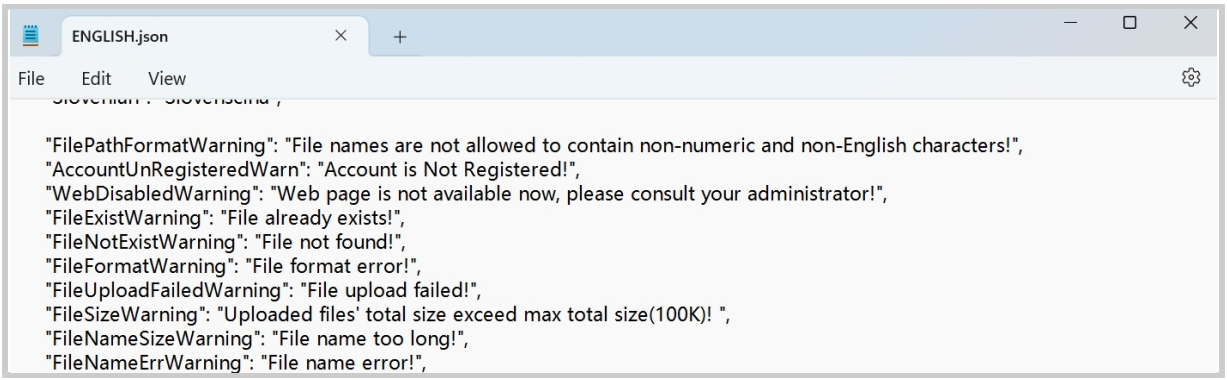
Custom Language

You can customize the configuration names and prompt texts on the device web portal, such as the file name error warning.

Export the .json file for editing. You may edit it with the notepad on your computer.

Import the .json file, and its size should be smaller than 1 MB.

File Example:



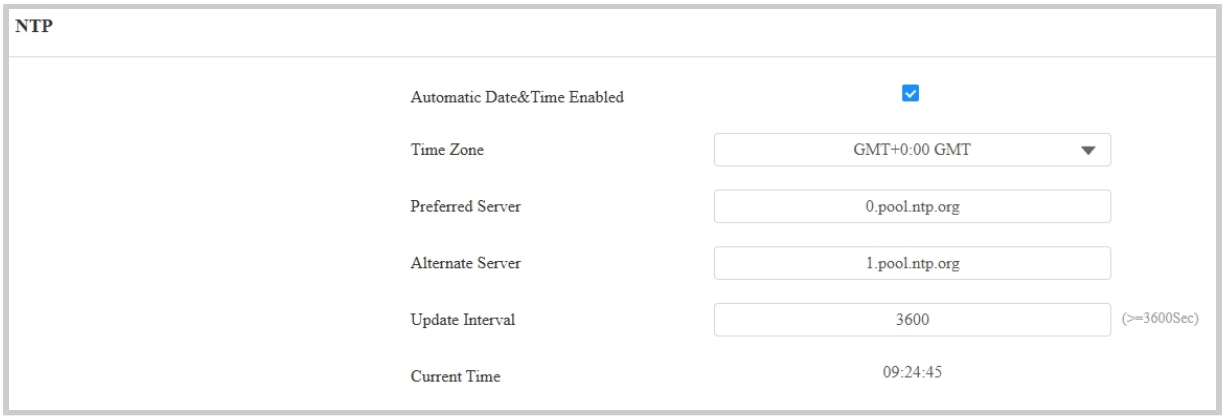
To set it up, go to the **Setting > Time/Lang** interface.



Time

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, go to the **Setting > Time/Lang** interface.



- **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 to 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.

Volume Control

You can set the volume level of the IP announcement and tamper alarm.

Set it up on the **Device > Audio** interface.

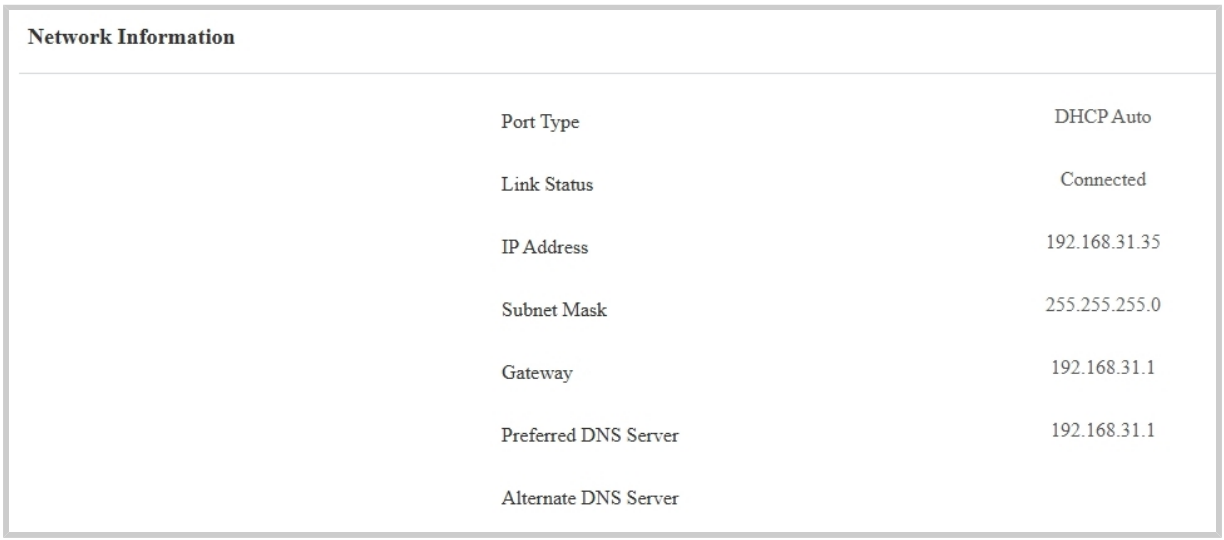


- **Level**: The default is 8. The value range is 1 to 15.

Network Setting

Network Status

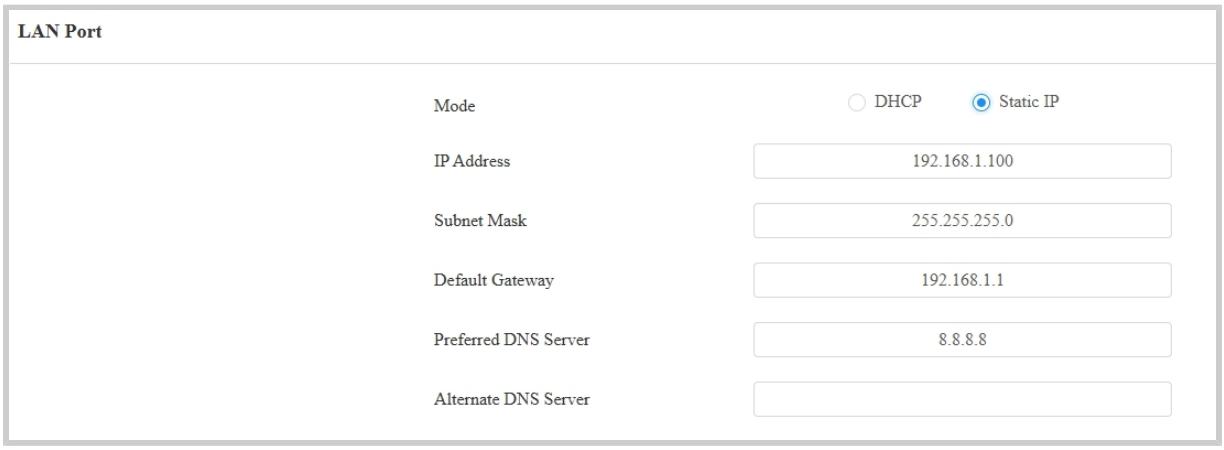
Check the network status on the web **Status > Info > Network Information** interface.



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.

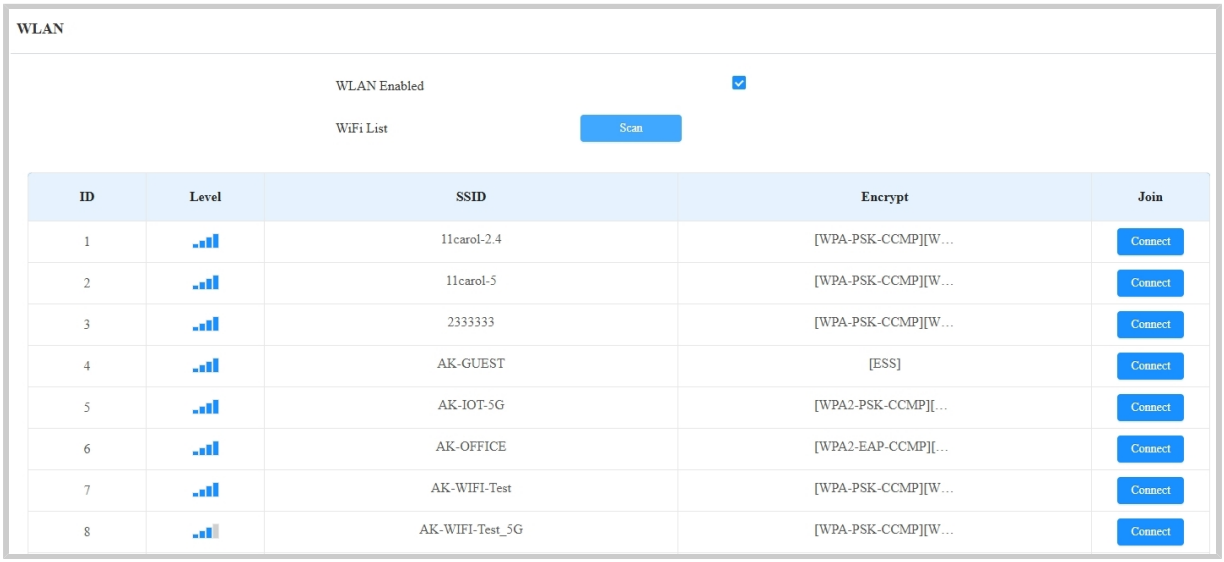


- **DHCP**: DHCP mode is the default network connection. In this mode, the device is assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: In this mode, the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings, your computer should be on the same local network as the device.
- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.
- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **Preferred/Alternate DNS Server**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The device connects to the alternate DNS server when the primary one is unavailable.

Wi-Fi Connection

The device supports connecting to the network via Wi-Fi. Set it up on the **Network > Basic** interface.

- Connect to the desired Wi-Fi by clicking **Connect** and entering the password.
- Refresh the Wi-Fi list by clicking **Scan**.



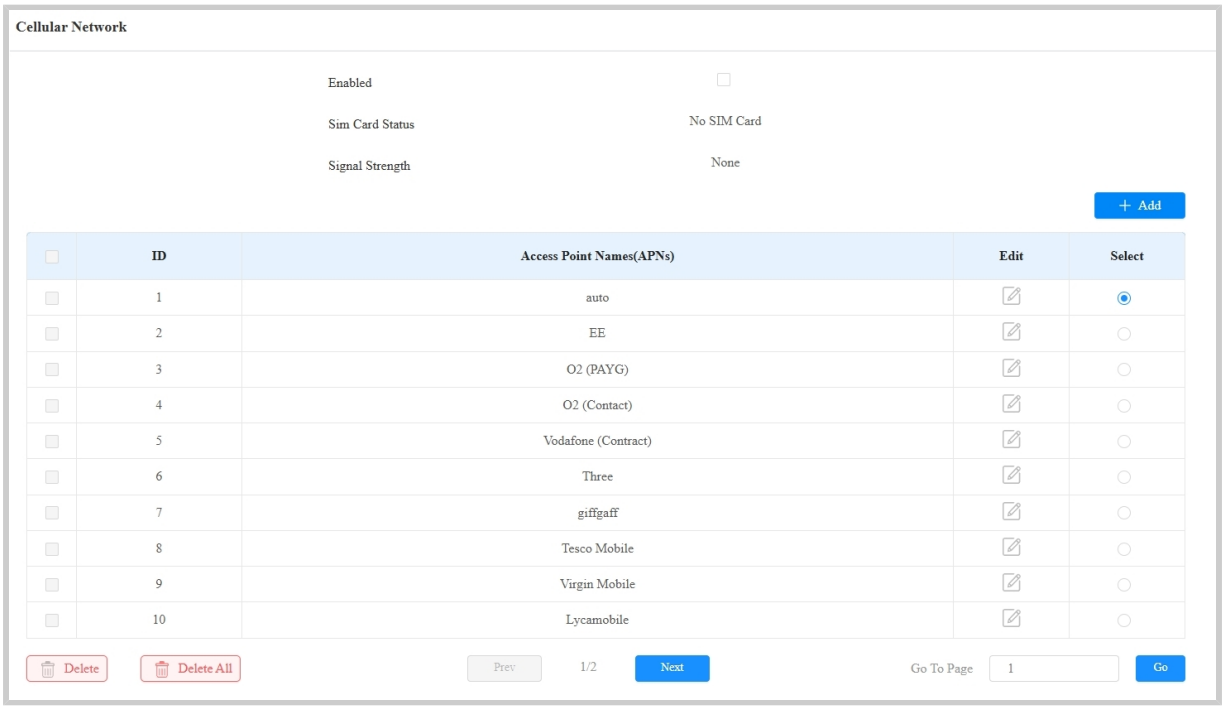
- **Level**: Display the signal strength.
- **SSID**: The Wi-Fi name.
- **Encrypt**: Display the Wi-Fi encryption method.

LTE Wireless Connection

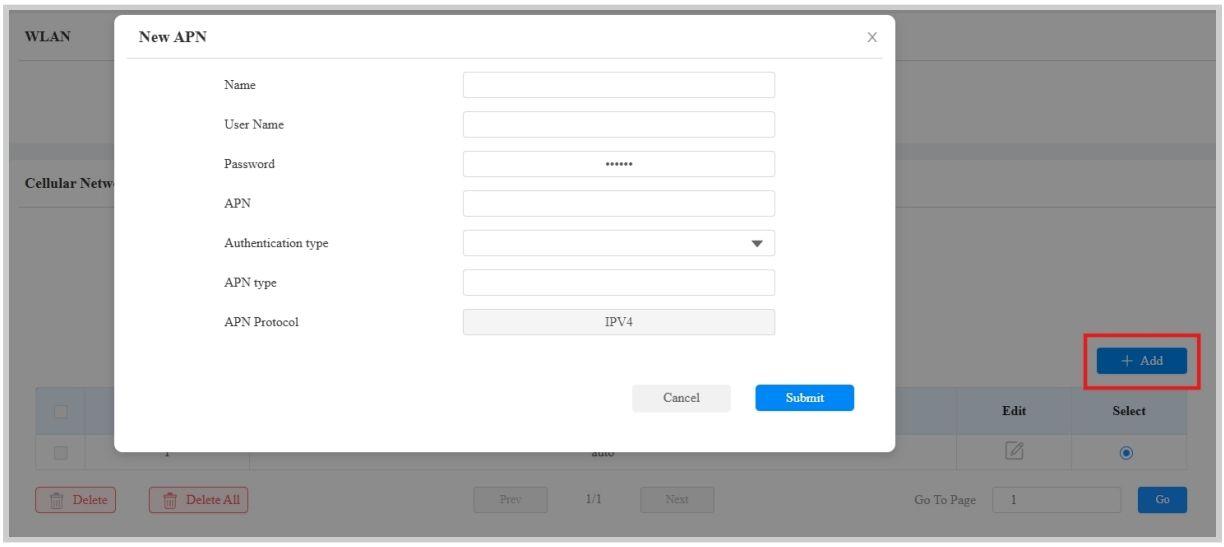
The LTE module enables cellular network connectivity for the device in areas where wired networks are unavailable, particularly beneficial for installations in older buildings.

The device supports the insertion of a SIM card for a 4G network connection. Please refer to the device's quick guide for instructions on installing the SIM card.

Set this feature up on the **Network > Basic** interface.



- **SIM Card Status**: Display whether a SIM card is inserted.
- **Signal Strength**: Indicate the network connection.
  - **None**: No SIM card inserted or the SIM card is not properly inserted, unable to detect signal.
  - **Weak**: The network signal is poor, typically when the signal strength is below -100 dBm.
  - **Fair**: The network signal is average, usually when the signal strength is between -90 and -100 dBm.
  - **Good**: The network signal is good, generally when the signal strength is between -70 and -90 dBm.
  - **Excellent**: The network signal is excellent, typically when the signal strength is between -50 and -70 dBm.
- **Access Point**: Select the access point or click **Add** to add a new one.
  Fill in the following information before clicking Submit. These can be found from the network provider of your SIM card.



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).

Set it up on the **Network > Advanced** interface.

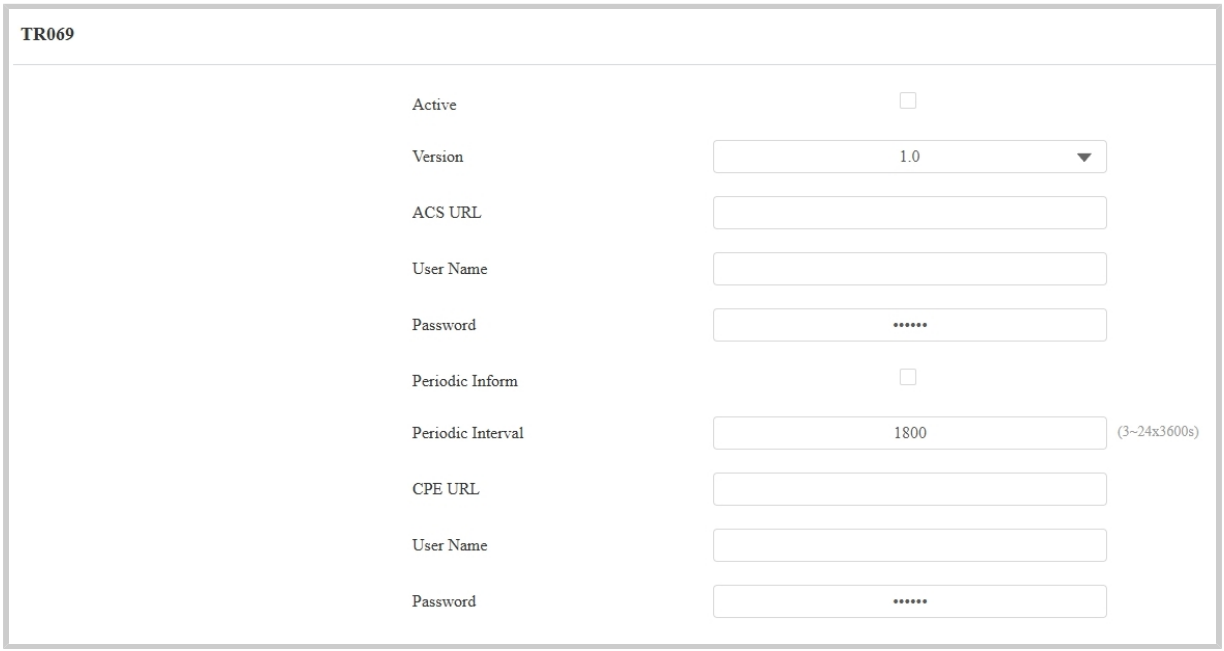


- **Port**: Set a specific port for the data transmission from 1024-65535.
- **Trusted IP**: Enter the third-party IP address.

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.

Set it up on the **Network > Advanced** interface.



- **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.

Device Web HTTP Setting

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

Set it up on the **Network > Advanced** interface.



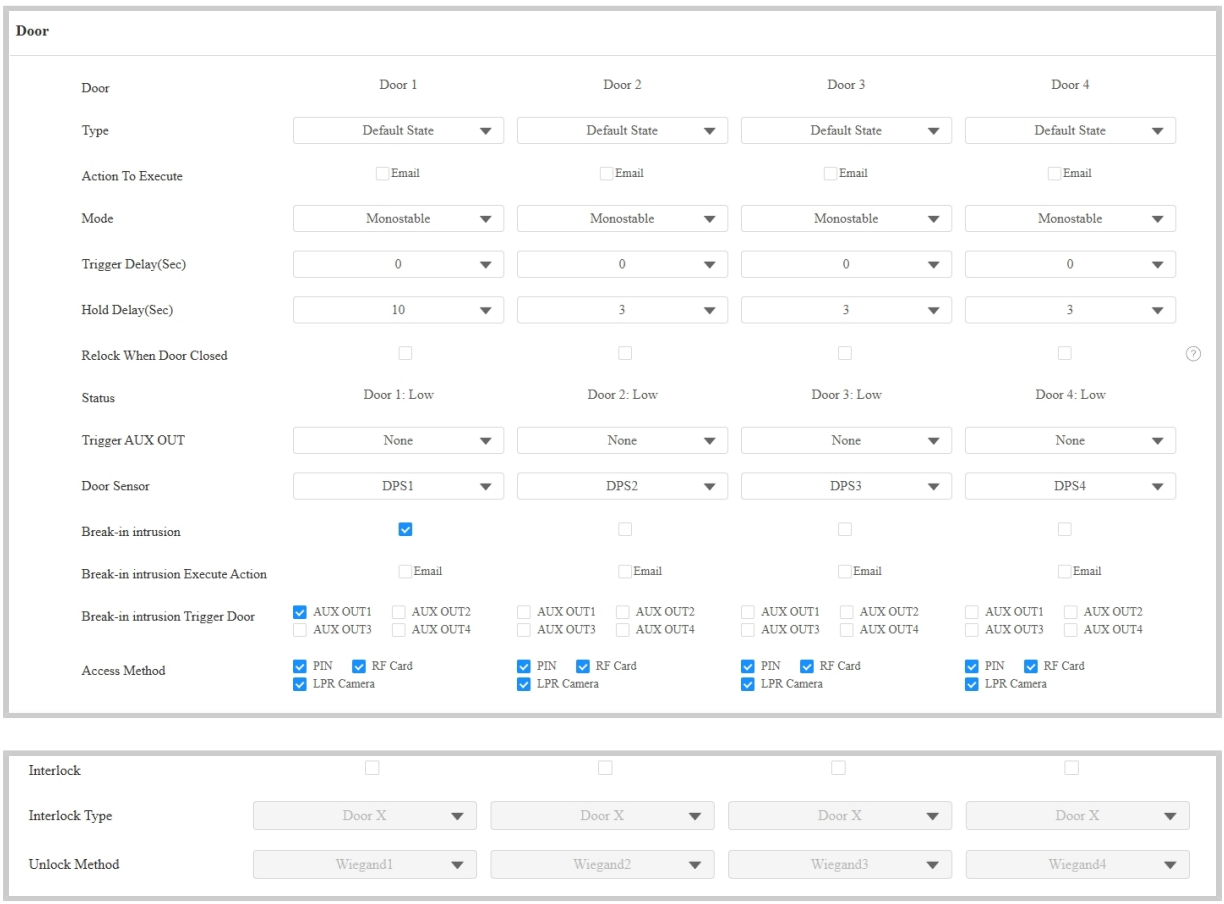
- **HTTP/HTTPS Enabled**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

Door Setting

Door Configuration

A095 has 8 built-in relays, which can be connected to electrical door locks for access controls. 4 of them are named door 1-4, and the others are auxiliary outputs.

Set up doors on the **Access Control > Door** interface.



- **Type**: Determine the interpretation of the door status:
  Default State: A “Low” status in the Door Status field indicates that the door is closed, while “High” indicates that it is open.
  - **Invert State**: A “Low” status in the Door Status field indicates an open 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 door status.

  - **Monostable**: The door status resets automatically within the trigger delay time after activation.
  - **Bistable**: The door status resets upon trigger again.
- **Trigger Delay(Sec):** Set the delay time before the door opens. For example, if set to 5 seconds, the door will not open until 5 seconds later when users use their credentials.
- **Hold Delay(Sec):** Determine the door-opening time. For example, if set to 5 seconds, the door stays open for 5 seconds.
- **Relock When Door Closed**: Specify whether the relay should be reset (door relocked) immediately when the door is physically closed.
  - If disabled(the default), the relay reset follows the configured **Hold Delay (Sec)**. The relay will remain active until the configured time expires, regardless of the door sensor status.
  - If enabled, the relay is reset immediately when the door sensor **Input** detects that the door is closed. The door will be relocked without waiting for the **Hold Delay** time to expire.
- **Status**: Indicate the state of the door, which is normally opened and closed. By default, it shows low for Normally Closed(NC) and high for Normally Open(NO).
- **Trigger AUX OUT**: A095 has four auxiliary outputs that can be connected to 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 doors.
- **Door Sensor**: Specify which input interface is connected to a door sensor.
- **Break-in intrusion**: Enable this option for detecting whether the door is forcibly or illegally opened. Click here to learn more information about this feature.
- **Break-in intrusion Execute Action**: Set whether to send a message to the preconfigured Email address when the break-in intrusion happens.
- **Break-in intrusion Trigger Door**: Specify the **AUX OUT** to be triggered by break-in intrusion.
- **Access Method**: Check the method(s) to open the door.

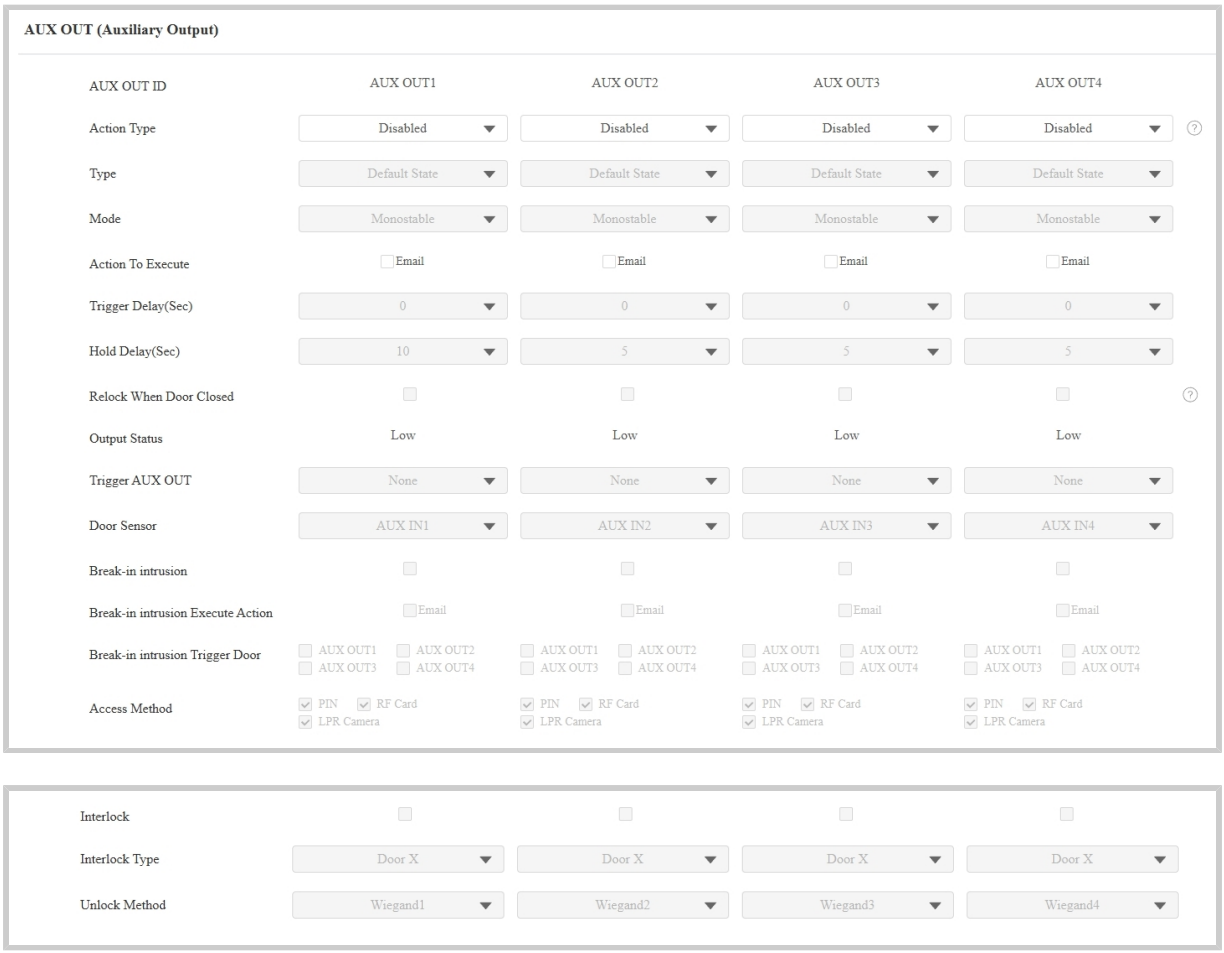
- **Interlock**: This feature limits the opening of other doors when one door is open. For example, enable Interlock for Doors 1, 2, and 4. When Door 1 is opened, Door 2 or 4 cannot be opened until Door 1 is closed. While Door 3 is not affected.
- **Interlock Type**: Available when **Interlock** is enabled. Set how to determine the door is closed, by door reset or REX(Request to Exit) reset.
- **Unlock Method**: Available when **Interlock** is enabled. Specify the method that opens the door. The settings of the corresponding Wiegand and DPS(Door Position Switch) will be overwritten.

> **Note**
>
> Click **here** to view the Interlock feature details.

Auxiliary Output Configuration

The 4 auxiliary outputs(AUX OUT) can be connected to door locks, sirens, or warning devices.

Set them up on the **Access Control > Auxiliary Output** interface.



- **Action Type**: Select the function of the AUX OUT.
  - **Disabled**: Disable the interface.
  - **Door**: It is connected to a door lock. Additional door-specific settings become available below.
  - **AUX OUT**: Control an external device such as a siren or indicator light.

Output Behavior (For **Door** and **AUX OUT** action types)

- **Mode**: Specify the conditions for automatically resetting the output status.
  - **Monostable**: The status resets automatically within the trigger delay time after activation.
  - **Bistable**: The status resets upon trigger again.

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

Door Settings (For **Door** action type)

- **Type**: Determine the interpretation of the door status:
  Default State: A "Low" status in the Door Status field indicates that the door is closed, while "High" indicates that it is open.
  - **Invert State**: A "Low" status in the Door Status field indicates an open door, while "High" indicates a closed one.
- **Trigger Delay(Sec):** Set the delay time before the door opens. For example, if set to 5 seconds, the door will not open until 5 seconds later when users use their credentials.
- **Trigger AUX OUT**: Set whether to trigger one of the other three AUX OUTs when this output is activated.
- **Door Sensor**: If the output is bound to a door sensor, specify which input interface is connected to the door sensor.
- **Break-in intrusion**: Enable this option for detecting whether the door is forcibly or illegally opened. Click here to learn more information about this feature.
- **Break-in intrusion Execute Action**: Set whether to send a message to the preconfigured Email address when the break-in intrusion event happens.
- **Break-in intrusion Trigger Door**: Specify the **AUX OUT** to be triggered by a break-in intrusion.
- **Access Method**: Check the method(s) to open the door.
- **Interlock**: This feature limits the opening of other doors when one door is open. For example, enable Interlock for Doors 1, 2, and 4. When Door 1 is opened, Door 2 or 4 cannot be opened until Door 1 is closed. While Door 3 is not affected.

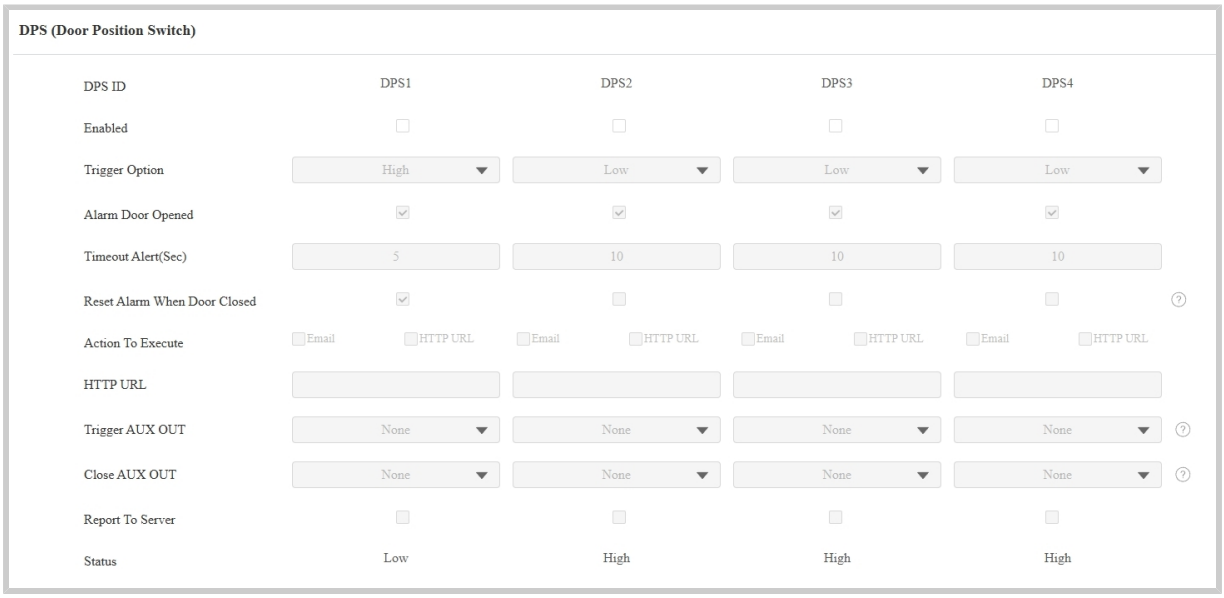
- **Interlock Type**: Available when **Interlock** is enabled. Set how to determine the door is closed, by door reset, DPS(Door Position Switch), or REX(Request to Exit) reset.
- **Unlock Method**: Available when **Interlock** is enabled. Specify the method that opens the door. The settings of the corresponding Wiegand and DPS(Door Position Switch) will be overwritten.

> **Note**
>
> Click **here** to view the Interlock feature details.

Door Position Switch Configuration

The device has 8 extra inputs. 4 of them can be connected to door position switches for detecting the open or closed status of doors.

To set up DPS, go to the **Access Control > Door > DPS(Door Position Switch)** interface.



- **Enabled**: Specify the input used.
- **Trigger Option**: Set the input interface to trigger at a low or high electrical level.
- **Alarm Door Opened**: This feature triggers an alarm when a door remains open longer than the configured duration.

- **Timeout Alert(Sec)**: The number of seconds a door can remain open before the alarm is triggered.
- **Reset Alarm When Door Closed**: Determine whether the door-open timeout alarm is automatically cleared when the door is closed.
  - If it is disabled(the default), when a timeout triggers the **Output** alarm, the alarm duration is determined by the **Hold Delay** configured for the Output, regardless of whether the door is closed.
  - If it is enabled, the **Output** alarm will be cleared automatically when the **Input** status is reset (for example, when the door is closed). In this case, the alarm stops immediately instead of waiting for the **Hold Delay** to expire.
- **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 URL**: 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. The format is *http://HTTP server's IP/Message content*.
- **Trigger AUX OUT**: Specify an auxiliary output to be activated when the timeout alert is triggered.
- **Close AUX OUT**: Specify an auxiliary output to be deactivated when the timeout alert is cleared. Please note that this feature does not work during the relay schedule time.
- **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.

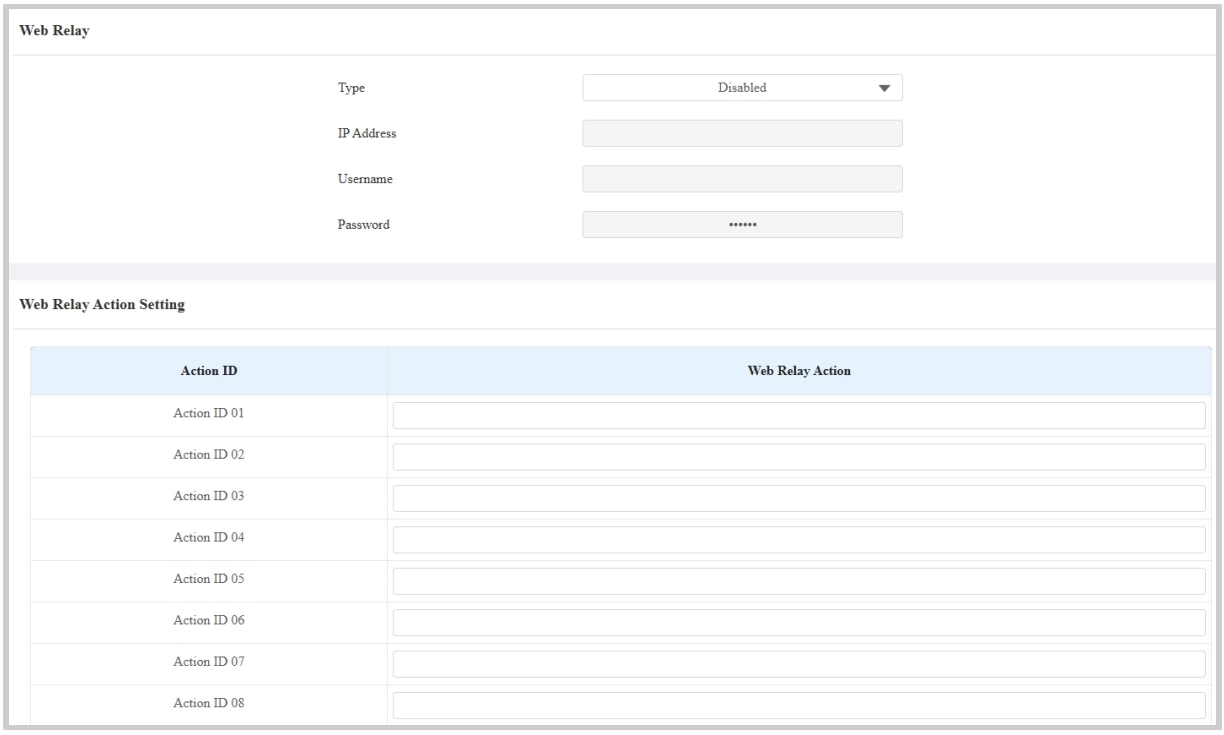
Web Relay

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.



Click here to view how to set up web relay.

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



- **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.
- **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.

> **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.

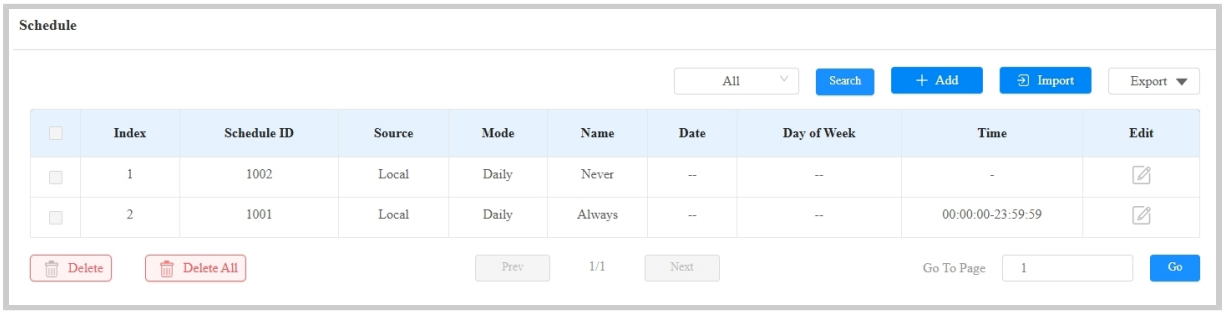
Door Access Schedule Management

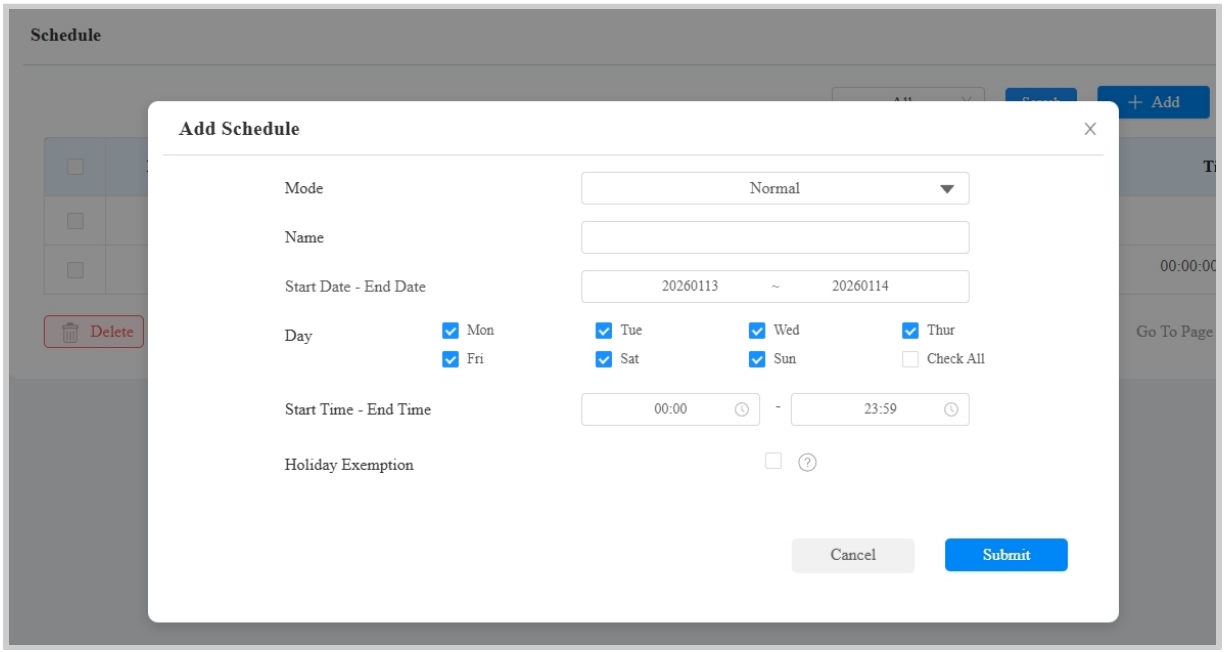
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Access Schedule

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

To set it up, go to the **Setting > Schedule** interface. Click **+Add**. The device supports 100 local schedules.





- **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.

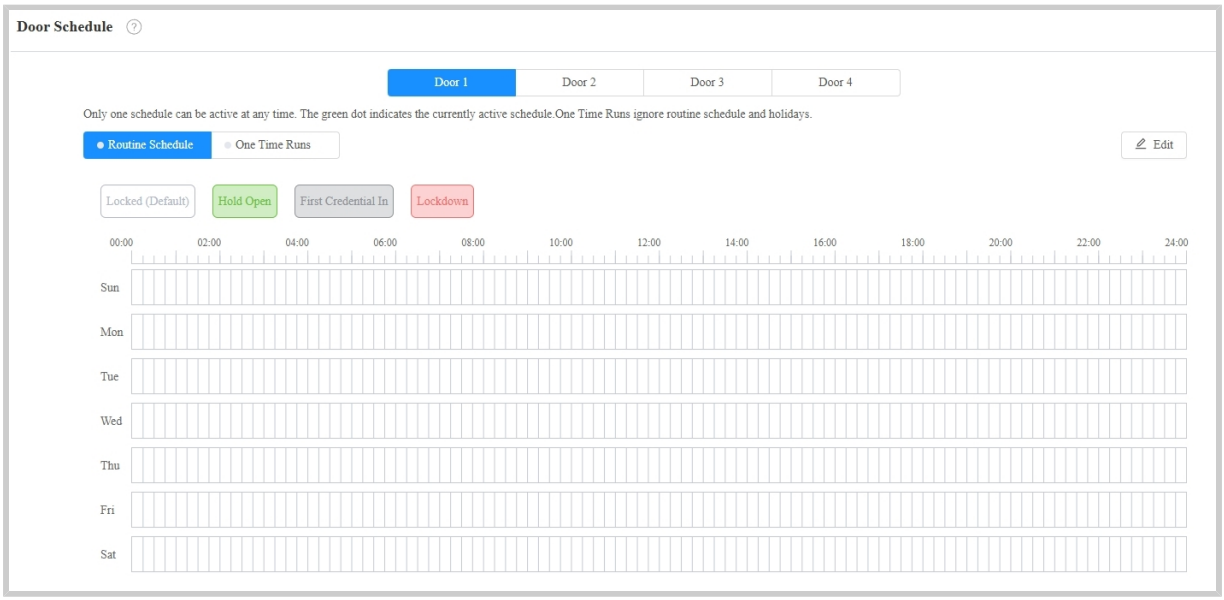
To set it up, go to the **Setting > Schedule** interface. The import and export files are in **XML** format.



Door Schedule

The door schedule allows you to set a specific door 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 > Door** interface.



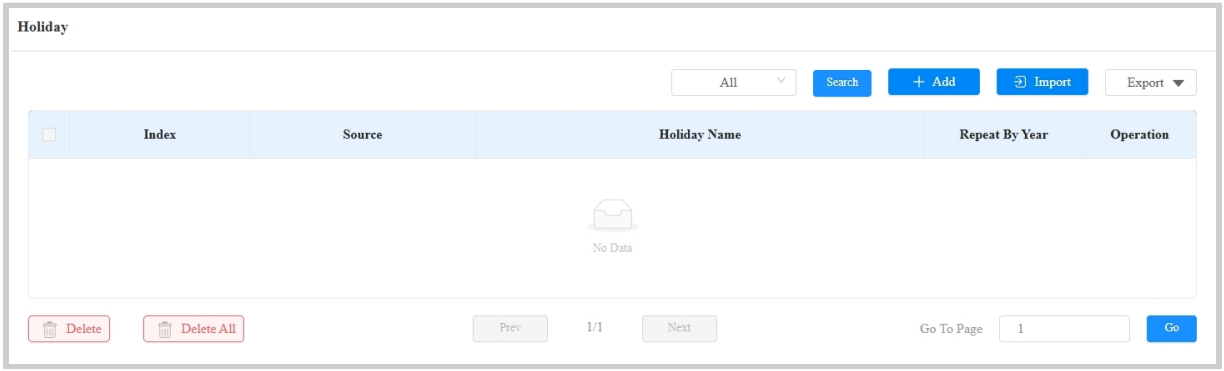
- **Door**: Specify which door uses the schedule.
- **Repeat Type**:
  - **Routine Schedule**: The schedule repeats every week. Click **Edit** on the right to configure.
  - **One-Time Runs**: Set the daily or weekly schedule that repeats during a defined period.
- **Schedule Mode:**
  - **Hold Open**: The door remains open during the scheduled time.
  - **First Credential In:** The door remains open during the scheduled time after users use their credentials for the first time.
  - **Lockdown**: The door remains closed during the scheduled time.

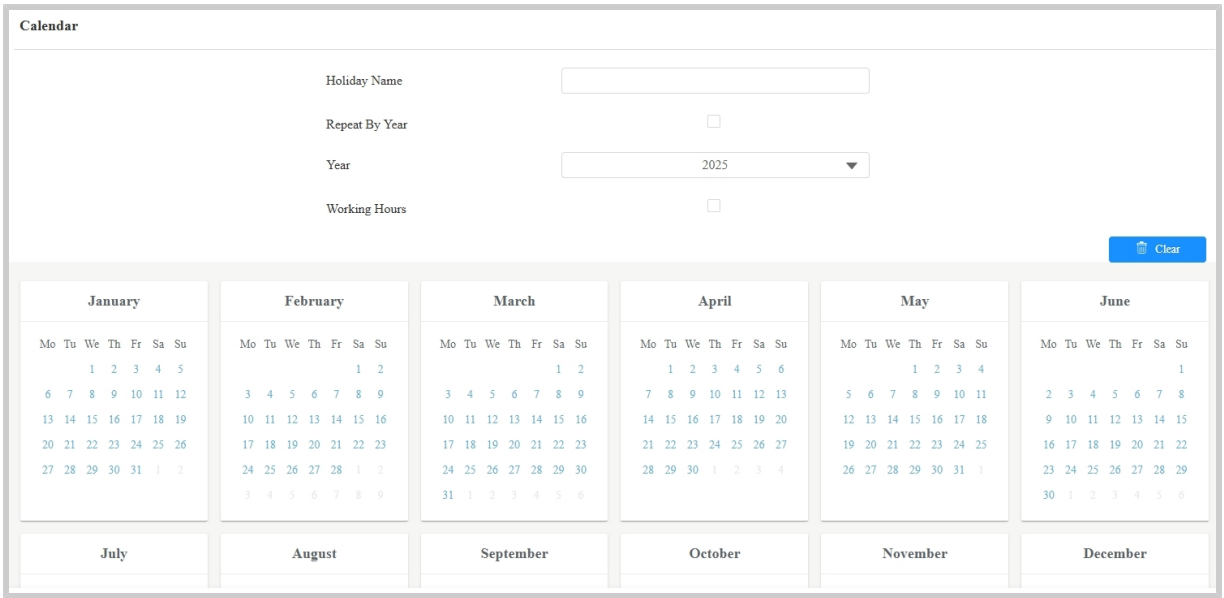
> **Note**
>
> Click here to view the detailed configuration of each schedule mode.

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.





- **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
All
Search
Add
Import
Export

Door-opening Configuration

Unlock by Public PIN Code

The device supports entering a public PIN code on a third-party reader to open the door.

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



- **PIN Code**: Set a 2-8 digit PIN code accessible for universal use. The default is 33333333.

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 door to open.

To add a user, go to **Directory > User** interface and click **+Add**. The device supports 100,000 users.



- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.
- **Role**: Define the user as a General User or an Administrator.
  - **Admin Permission**: If enabled, when the alarm is triggered, the admin can disarm by using his/her credentials twice within the disarm time, like swiping the card twice, or entering the PIN followed by swiping the card. Click here to view the detailed disarm settings.

Unlock by Private PIN Code

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



- **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.



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

> **Note**
>
> - Each user can have a maximum of 5 cards added.
> - The device supports 500,000 cards.
> - RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device 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.



- **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.

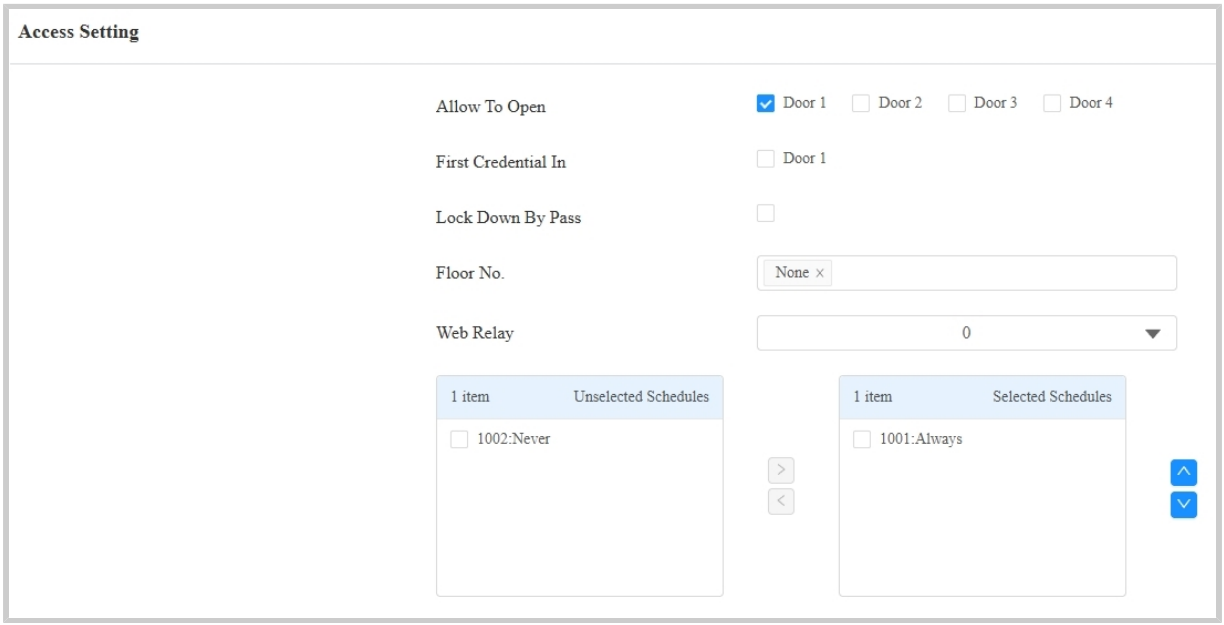


- **Add**: A user can have up to 5 license plates.
- **Duration**: Enable/disable Long-term Vehicle. It is enabled by default. If disabled, specify when the vehicle can enter or exit the parking lot.

Access Setting

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

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



- **Allow To Open**: Specify the door(s) to be opened using the credentials assigned to the user.
- **First Credential In:** This decides whether the user can keep the door open during the scheduled time after activating it.
- **Lockdown Bypass**: This decides whether the user can open the door when the door is locked during the scheduled time.
- **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 the number of door openings 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.



Unlock by HTTP Commands

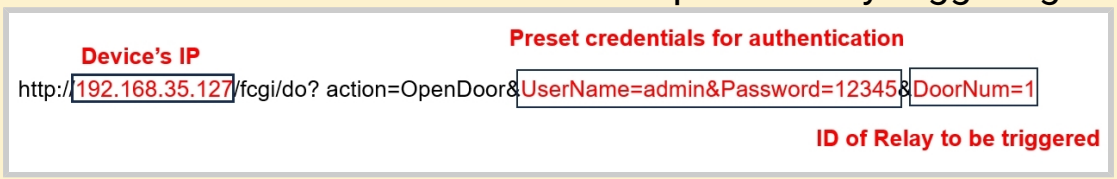
The device supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the device. This will trigger the relay and open the door, even if the users are away from the device.

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



Tip

Here is an HTTP command URL example for relay triggering.



Note

The HTTP format for relay triggering varies by 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.

To set it up, go to the **Access Control > Door > REX(Request to Exit)** interface.

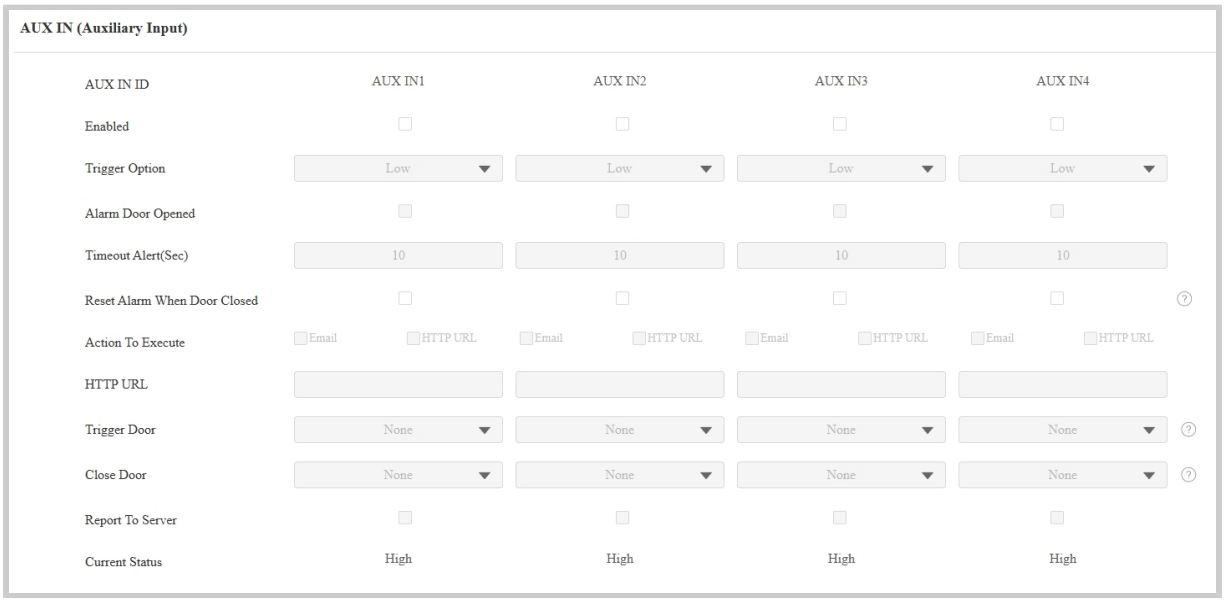


- **Enabled**: Specify the specific input(s) interface used.
- **Trigger Option**: Set the input interface to trigger at a low or high electrical level.
- **Open Door**: Specify the door to be opened.
- **Close Door**: Specify the door to be closed.
- **Status**: Display the status of the input signal.

Unlock by Emergency Button

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

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



- **Enabled**: Specify the input used.
- **Trigger Option**: Set the input interface to trigger at a low or high electrical level.
- **Alarm Door Opened**: This feature triggers an alarm when a door remains open longer than the configured duration.
- **Timeout Alert(Sec)**: The number of seconds a door can remain open before the alarm is triggered.
- **Reset Alarm When Door Closed**: Determine whether the door-open timeout alarm is automatically cleared when the door is closed.
  - If it is disabled(the default), when a timeout triggers the **Output** alarm, the alarm duration is determined by the **Hold Delay** configured for the Output, regardless of whether the door is closed.
  - If it is enabled, the **Output** alarm will be cleared automatically when the **Input** status is reset (for example, when the door is closed). In this case, the alarm stops immediately instead of waiting for the **Hold Delay** to expire.
- **Action to Execute**: Set the desired actions that occur when this input interface is triggered.
  - **Email**: Send a message to the preconfigured Email address .

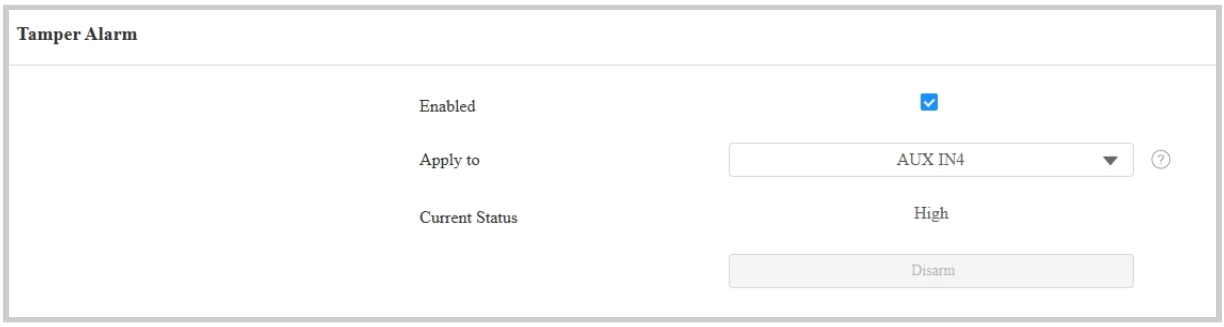
  - **HTTP URL**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below. The format is *http://HTTP server's IP/Message content*.
- **Trigger Door**: Specify a door to be opened along with the input.
- **Close Door:** Specify a door to be closed when the input is triggered. Please note that this feature does not work during the relay schedule time.
- **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.
- **Current Status**: Display the status of the input signal.

Security

Tamper Alarm

The tamper alarm function prevents anyone from removing the device without permission. The device's AUX IN can be connected to a sensor, detecting illegal movement of the device.

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



- **Disarm**: When the tamper alarm goes off, you can press the **Disarm** tab to clear the alarm.
- **Apply To**: The input that is connected to the detection sensor. The default is AUX IN4. When applying AUX IN to the tamper alarm, its settings will be unavailable.
- **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.

Disarm Setting

You can set the automatic disarm time and the time for users to disarm manually when alarms are triggered.

Set it up on the **Access Control > Auxiliary Input > Disarm Setting** interface.



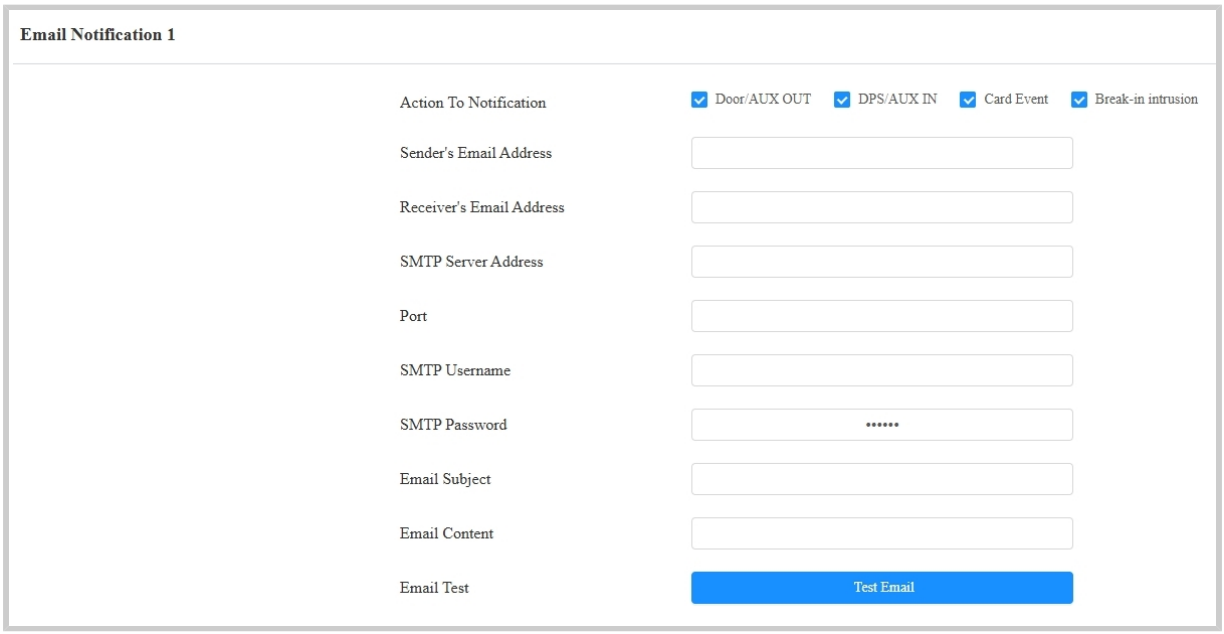
- **Enabled**: The disarm feature is disabled by default.
- **Reset Time**: Define the time(10-240 minutes) to clear the alarm automatically after the alarm is triggered.
- **Disarm Time**: Admin users can use their credentials twice within the time to clear the alarm, like swiping the card twice, or entering the PIN followed by swiping the card.

Security Notification

A security notification informs users or security personnel of any breach or threat that the device detects. For example, if the device detects something unusual, the system sends a notification to users or security through email.

Click here to view how to set this feature up.

Set up email notifications on the **Setting > Action** interface.



- **SMTP Server Address**: The SMTP server address of the sender.
- **Port**: SMTP server port.
- **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, RF card access changes, etc.

Akuvox Action URL:

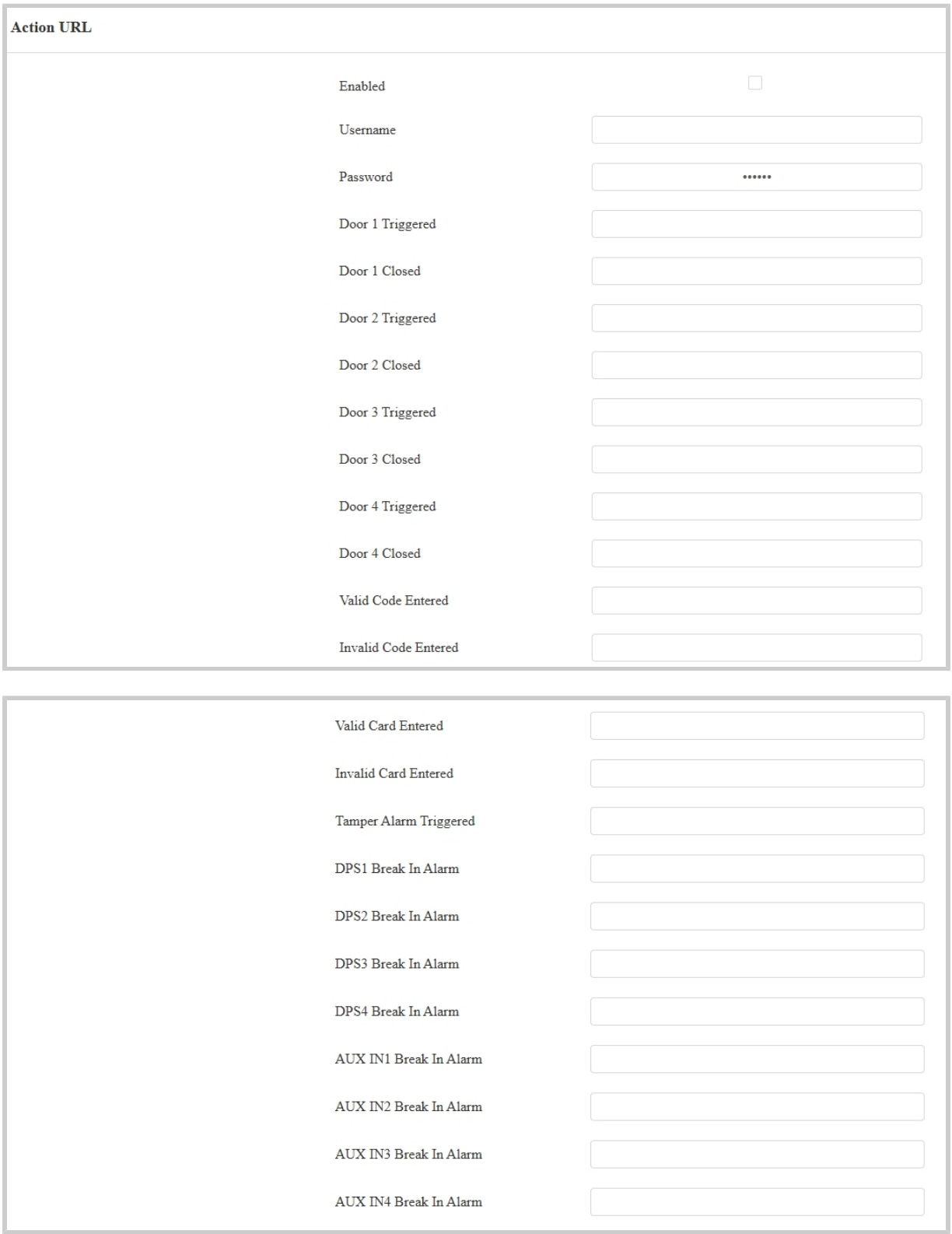
No	Event	Parameter format
1	Door Triggered	$relay1status
2	Door Closed	$relay1status

3	Valid Code Entered	$code
4	Invalid Code Entered	$code
5	Valid Card Entered	$card_sn
6	Invalid Card Entered	$card_sn
7	Tamper Alarm Triggered	$alarmstatus
8	DPS Break-in Alarm	$relay1status
9	AUX IN Break-in Alarm	$relay1status

Example
Http://server ip/relaytrigger=$relay1status
Http://server ip/relayclose=$relay1status
Http://server ip/validcode=$code
Http://server ip/invalidcode=$code
Http://server ip/validcard=$card_sn
Http://server ip/invalidcard=$card_sn
Http://server ip/tampertrigger=$alarmstatus
Http://server ip/inputtrigger=$relay1status
Http://server ip/inputtrigger=$relay1status

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, go to the **Setting > Action URL** interface. You can set up the username and password for authentication.



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.

Disable High Security Mode on the **System > Security** interface. It is enabled by default.



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.



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** interface.

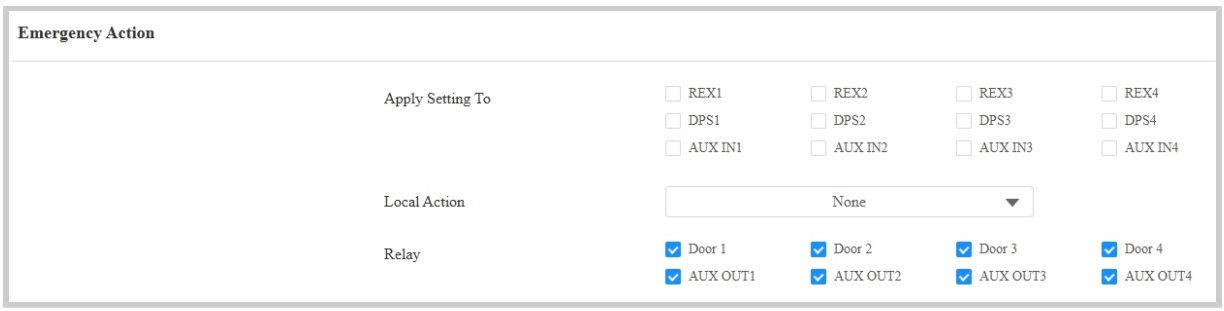


- **Apply Setting To**:
  - **None**: Not display door status.
  - **REX**: The door is opened by triggering the input(pressing the exit button).
  - **Door**: The door is opened by triggering the relay.

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.



- **Local Action**: Set whether to open doors with the input trigger. An option called “End Now” will be available when the door is opened. You can click it to close it.
  - **None**: Disable the feature.
  - **Time**: Set the duration time of the door opening.
  - **Always**: The door keeps open.

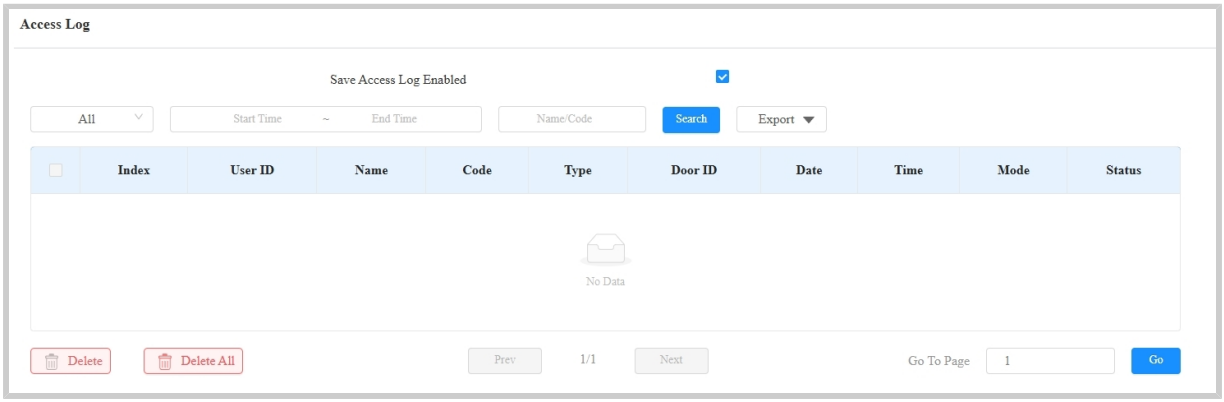
> **Note**
>
> When the device is deployed on the SmartPlus Cloud, property managers can apply emergency actions and the local action will be overwritten. For example, when the door is set to be activated for 5 minutes. At 3 minutes, the Cloud issues the Emergency Unlock action, the door will not be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

Logs

Access Logs

The access log displays up to 200,000 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 XML or CSV format.

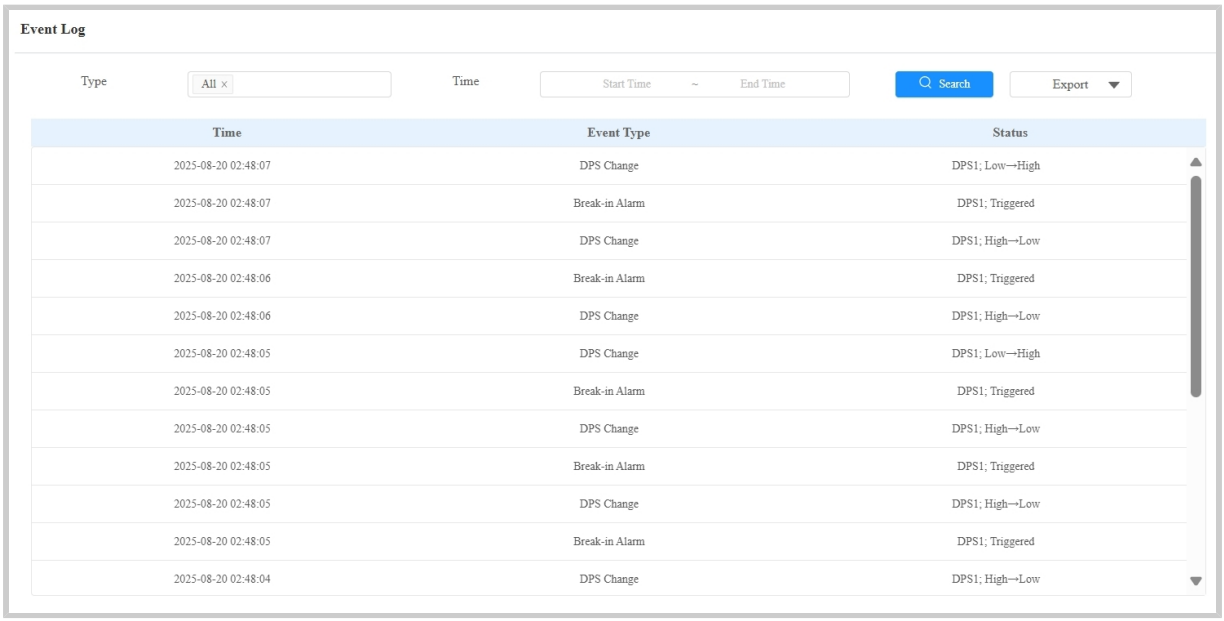


- **Save Access Log Enabled**: Decide whether to save the door-opening records.
- **Time**: Select the specific period of the door logs you want to search, check, or export.
- **Name/Code**: Search the log by the username or the PIN code.
- **Type**: Display the access type, such as RF Card.
- **Door 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. The device supports up to 100,000 logs, which can be exported in CSV format.

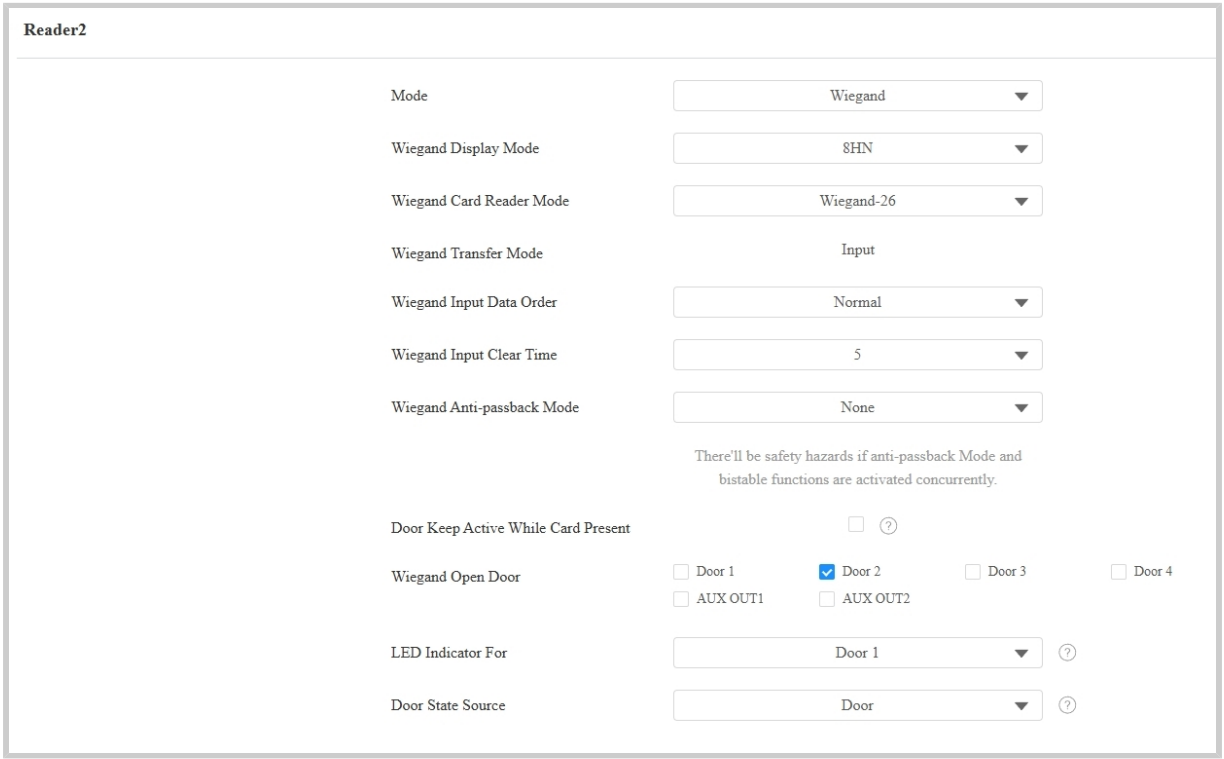

Event Log
Type
All ×
Time
Start Time
~
End Time
Search
Export
Time
Event Type
Status
2025-08-20 02:48:07
DPS Change
DPS1; Low→High
2025-08-20 02:48:07
Break-in Alarm
DPS1; Triggered
2025-08-20 02:48:07
DPS Change
DPS1; High→Low
2025-08-20 02:48:06
Break-in Alarm
DPS1; Triggered
2025-08-20 02:48:06
DPS Change
DPS1; High→Low
2025-08-20 02:48:05
DPS Change
DPS1; Low→High
2025-08-20 02:48:05
Break-in Alarm
DPS1; Triggered
2025-08-20 02:48:05
DPS Change
DPS1; High→Low
2025-08-20 02:48:05
Break-in Alarm
DPS1; Triggered
2025-08-20 02:48:05
DPS Change
DPS1; High→Low
2025-08-20 02:48:05
Break-in Alarm
DPS1; Triggered
2025-08-20 02:48:04
DPS Change
DPS1; High→Low

Integration with Third-party Devices

Integration via Wiegand

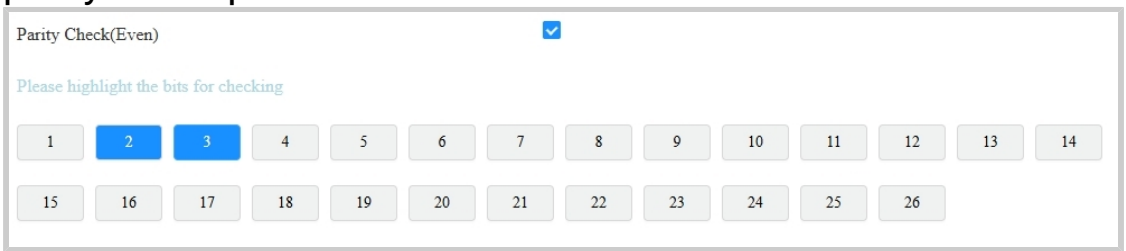
The device has 8 readers, which can work in Wiegand or OSDP mode. The Wiegand feature enables the Akuvox device to act as a controller.

To set it up, go to the **Device > Reader** interface. Set the reader mode to **Wiegand**.



- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options: 8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26), 8HR10D, and RAW.
  - **Ignore Facility Code**: This option is available when 6H3D5D(WG26) is selected. When enabled, the first three bits of the cards will be ignored for successful card reading.

- **Wiegand 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 the 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 a card code.
  - **Use Site Code**: Set whether to use the site code. You may need to enable it when a 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(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.



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
HEX: 385C243E	13-32 Bits: C243E	1-12 Bits: 385

Parity Check	Card Code
• 2-15 bits(Even): The sum is 7, fail to pass the check. • 16-31 bits(Odd): The sum is 7, successfully pass the check.	C243E

- **Wiegand 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.

- **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. 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.
- **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.
- **Door Keep Active While Card Present**: This feature keeps the relay triggered continuously while a valid card stays within the reader's detection range. The relay will deactivate automatically when the card is moved away.

  > **Note**
  >
  > - Upon detecting a valid card, the device generates a **Card Present Access Log** and activates the relay.
  > - While continuously reading the card, the relay remains active. No additional Access Logs are generated.
  > - Upon detecting the card leaving the reading area, the device generates a **Card Removed Access Log**.

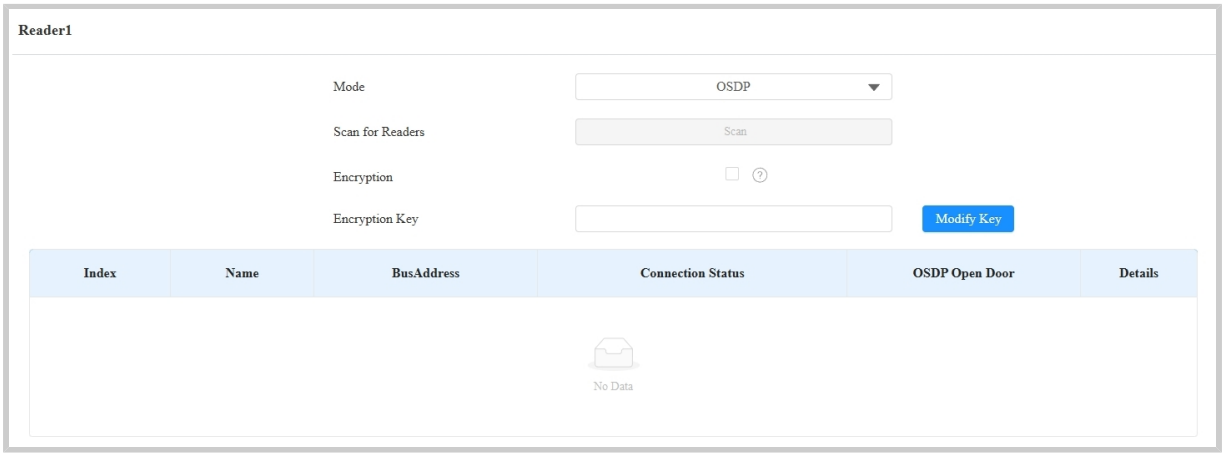
- **Wiegand Open Door**: Select the door to be opened by Wiegand.
- **LED Indicator For:** Each reader has GLED and RLED interfaces to control the indicator lights of the Wiegand card reader.
  - **If None is selected:** GLED and RLED do not show the real-time status of the door. They only indicate whether a door opening action was successful.
  - **If a specific door is selected**: GLED and RLED show the real-time status of that door.

  - When the door is open, GLED stays lit, and RLED turns off.
  - When the door is locked down, RLED stays lit, and GLED turns off.
- **Door State Source**: Available when **LED Indicator For** is configured. It determines whether the door's status is defined by **Door** or by **Input(Door Sensor)**.

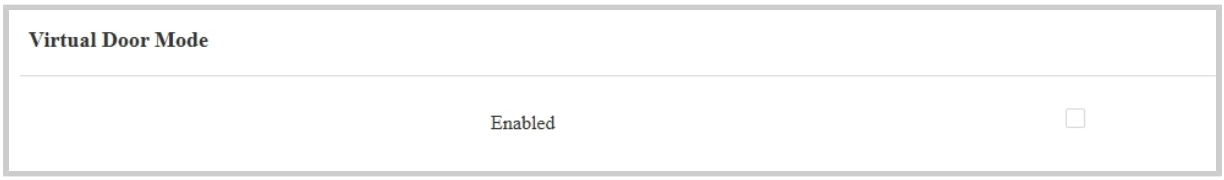
Integration via RS485

The device has 8 readers, which can work in Wiegand or OSDP mode.

Set it up on the web **Device > RS485** interface. Set reader mode to **OSDP**.



- **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 Door**: Check the door to be opened.
- **Details**: Click to view the card reader's information.



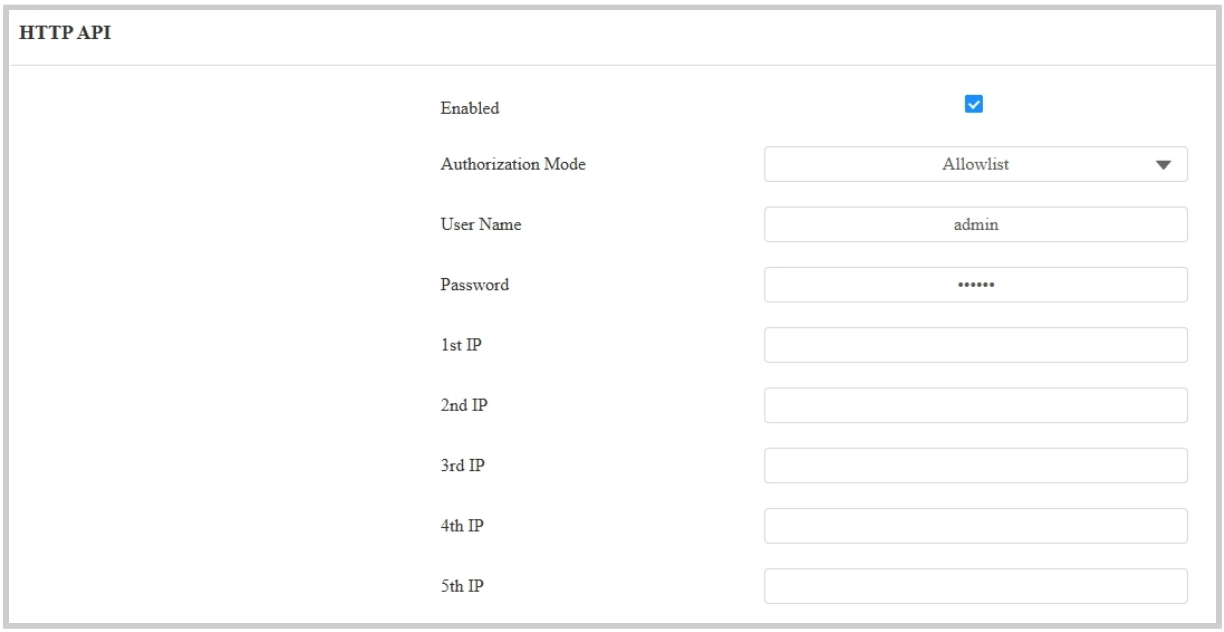
- **Virtual Door Mode**:
  - It is disabled by default. Users can ONLY open doors that are checked on both the Reader setting and Access Setting interfaces.
  - If it is enabled, users can open doors that are checked on the Reader setting interface with their credentials, regardless of whether they are 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, go to **Setting > HTTP API** interface.



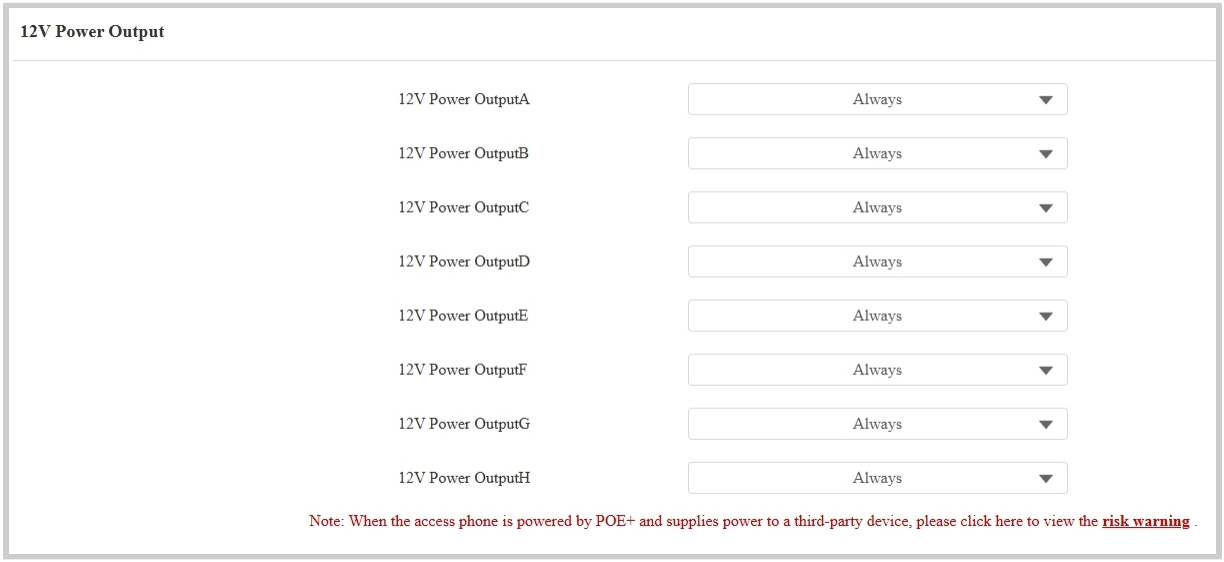
- **HTTP API Enable:** Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode:**
  - **None**: No authentication is required for the HTTP API, 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 addresses 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. Click here to view power output requirements.

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



- **12V Power Output ID:** Specify the output(4 Door interfaces and 4 AUX OUT interfaces) for supplying power.
- **Power Output Type**: Select the power output type.
  - **Always:** The device will provide a continuous power supply. The device's door status will be changed from NC to NO status after the door interface is triggered, thus cutting off the power. The power supply will be resumed after the door is reset.
  - **Triggered by Open Door**: It is generally for the GND and NO connection.
    After triggering, the door status switches from NO to NC, initiating the power supply.

The power supply is cut off after the door interface is reset. The door interface can be reset automatically after the pre-selected timeout(3, 5, or 10 seconds).

- **Time Out(Sec)**: This option is available when **Triggered by Open Door** is selected. Set the door interface reset time.

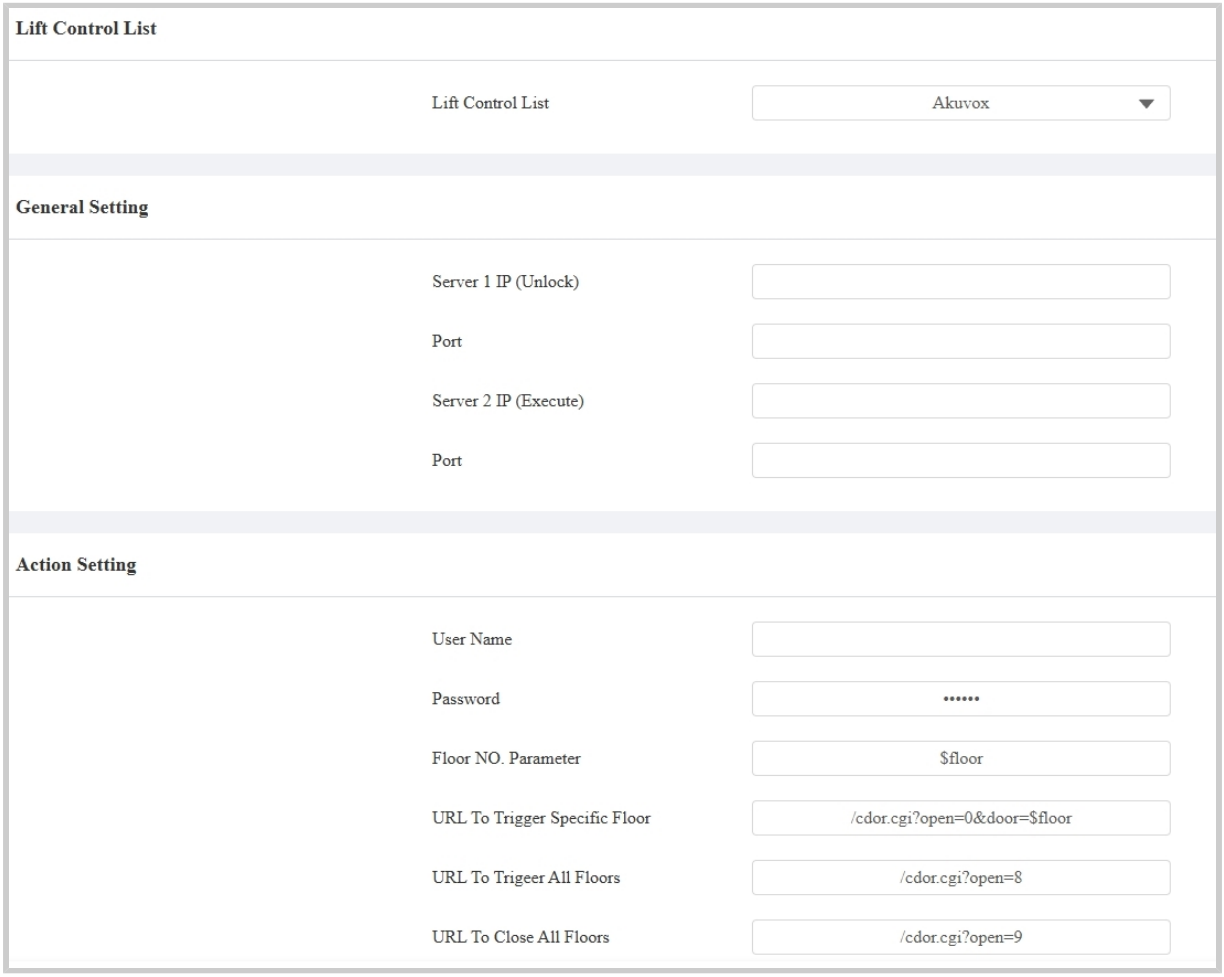
Note

- Powered by PoE+, A095 provides 12V power with a maximum per-port current of 0.2A if the device's READER interfaces are connected fully to 8 devices. It provides 12V power with the per-port current between 0.2A and 0.4A if the device's READER interfaces are connected to 4 devices or fewer.
- Powered by a 12V/5A DC power connector, A095 provides 12V/500mA per port.

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. Select **Akuvox** in the Lift Control List.

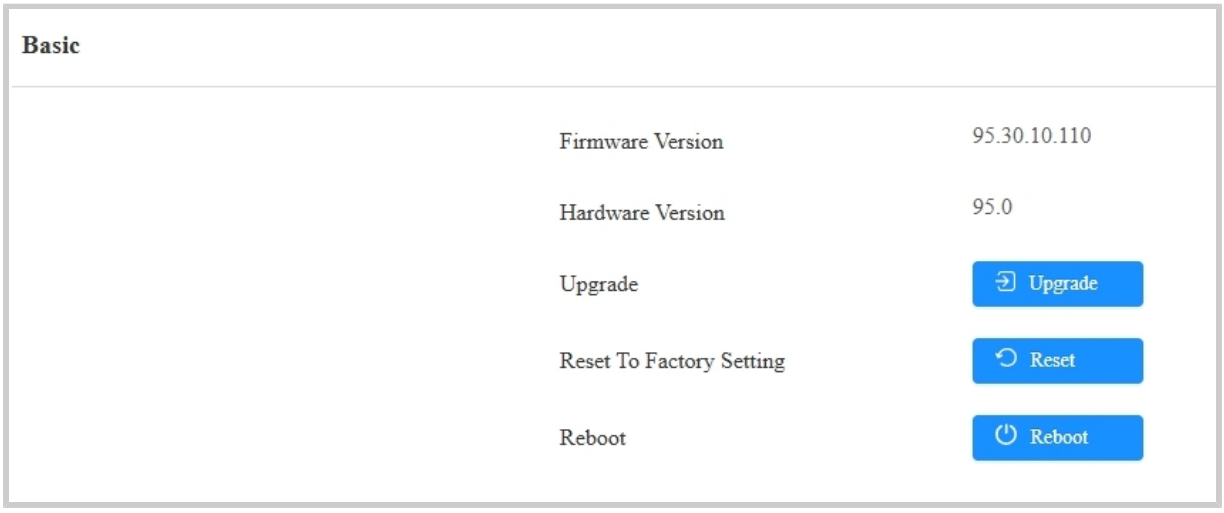


- **Server 1 IP(Unlock)**: The IP address of the Akuvox lift control server. It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute)**: The IP address of the server that triggers lift control.
- **Port**: The server port of the lift controller server.
- **User Name**: The username 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.



Note

Firmware files should be in .rom format for upgrade.

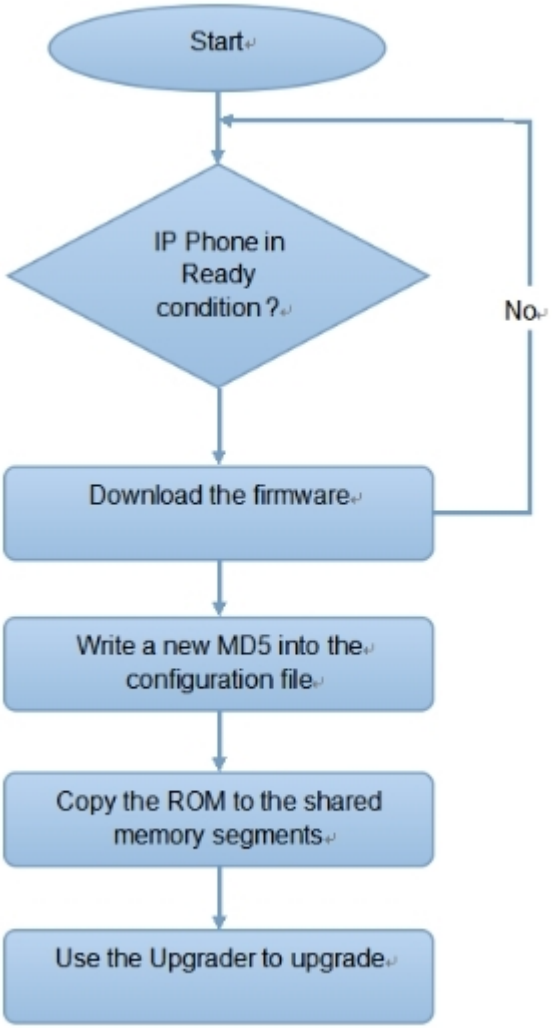
Auto-Provisioning via Configuration File

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:



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

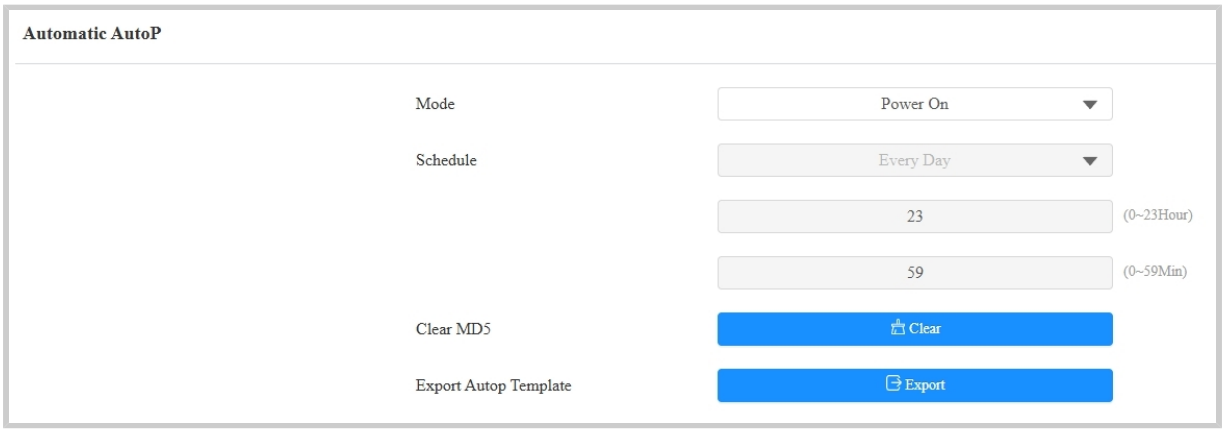
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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.

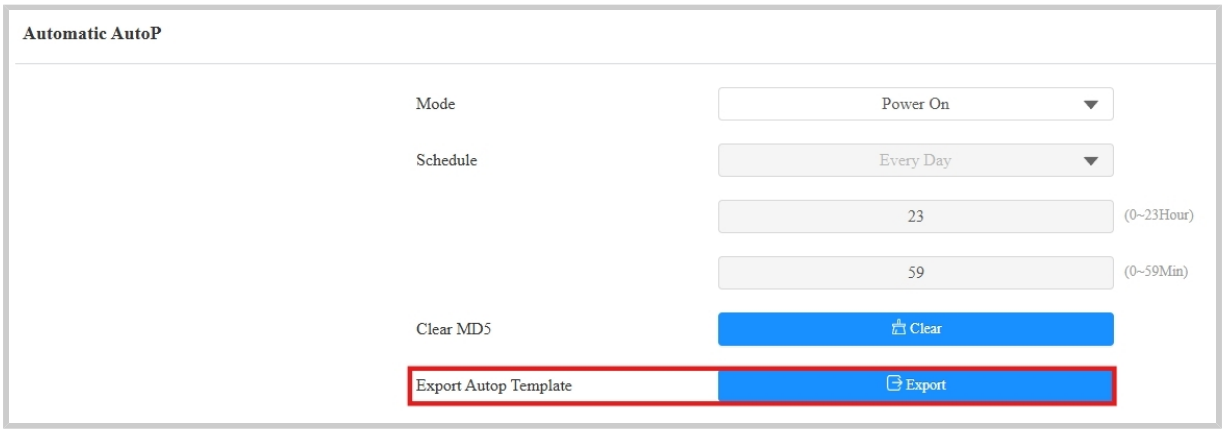


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode, which will enable the device to perform Autop every time it boots up or according to the schedule you set up.
  - **Hourly Repeat**: The device will perform Autop every hour.

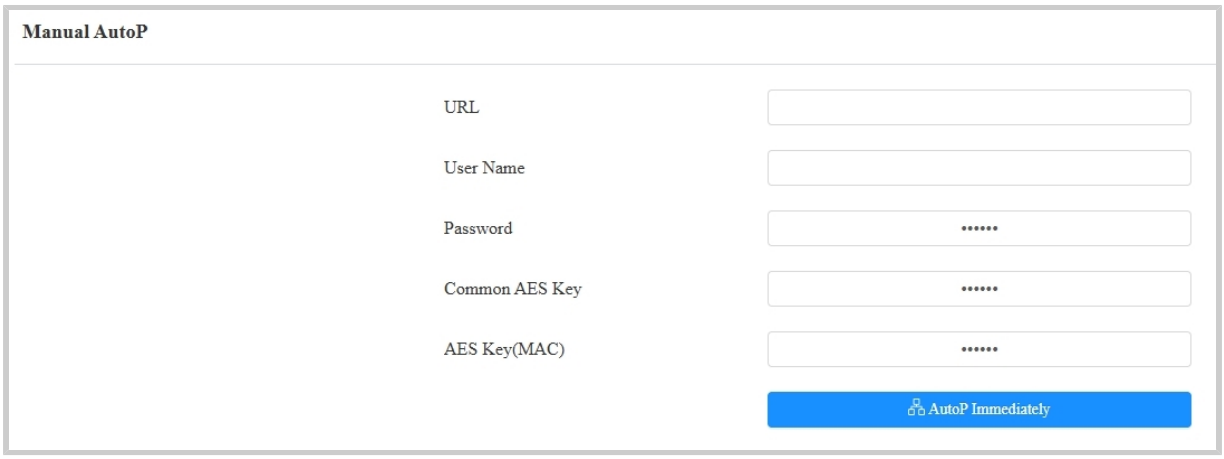
Static Provisioning

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.



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



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server requires a username to be accessed.
- **Password**: Enter the password if the server requires 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

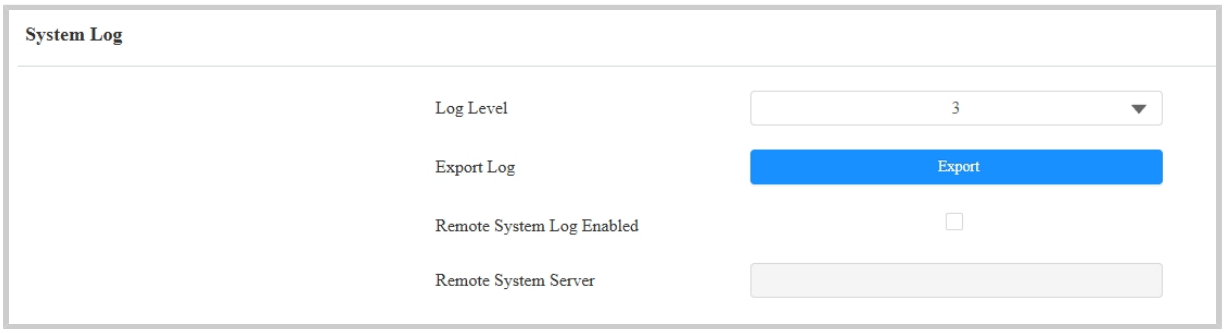
Akuvox do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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

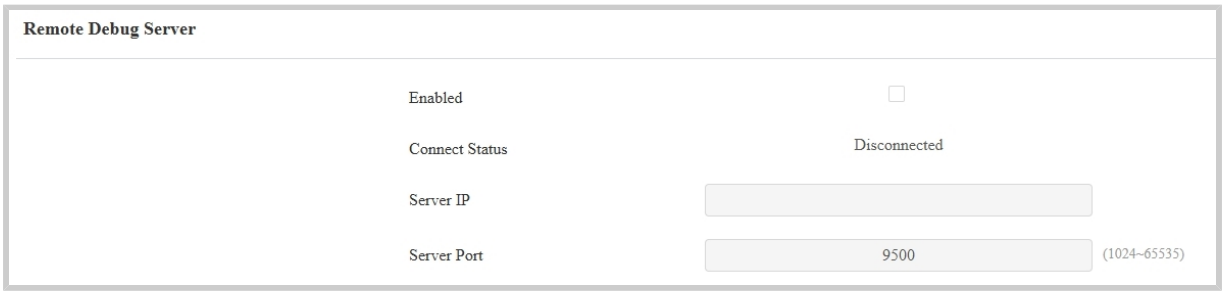


- **Log Level**: Log levels range from 1 to 7. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export the 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.

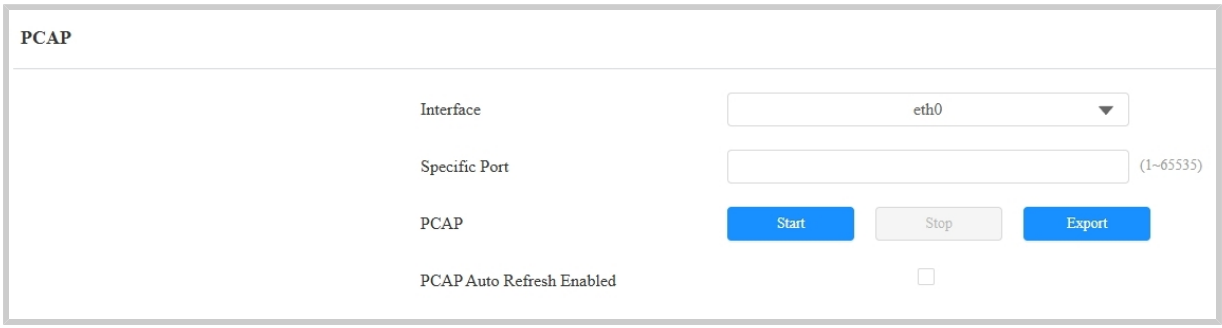


- **Connect Status**: Display the remote debug server connection status.
- **Server IP**: Set the remote debug server IP address. Please ask the Akuvox technical team for the server IP address.
- **Server Port**: Set the remote debug server port.

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.



- **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 50 MB maximum 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. The supported file format is TGZ and CFG.



Backup via SD Card

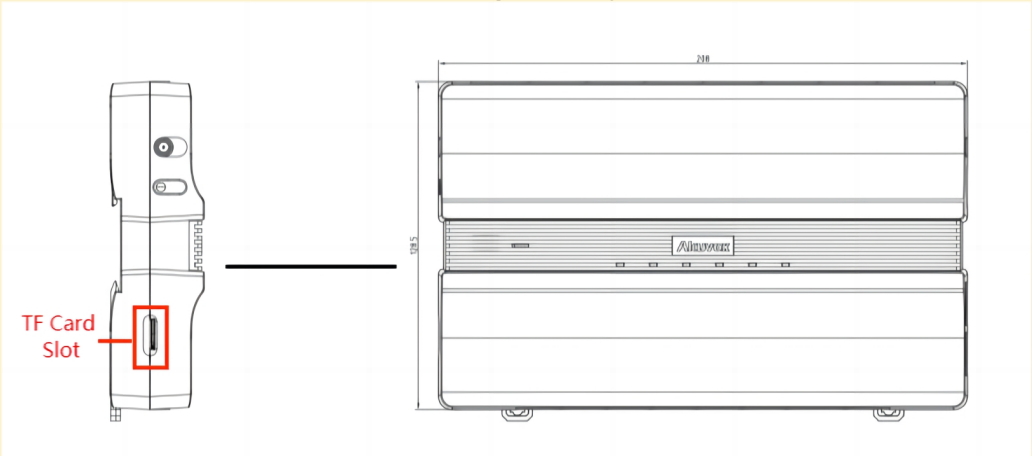
The device supports inserting an SD card for importing and exporting configuration files.

To set it up, go to the **Device > SD Card** interface.



Tip

To install an SD card, remove the rubber plug with the removal tool in the device's package.



Account & Password

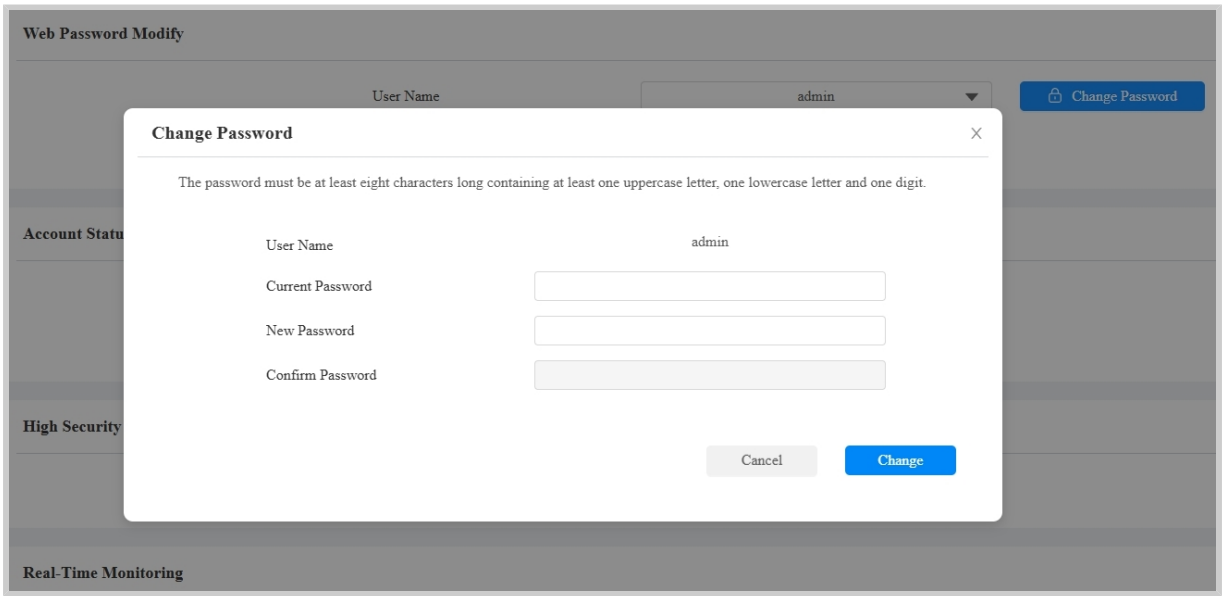
Modify Web Password

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

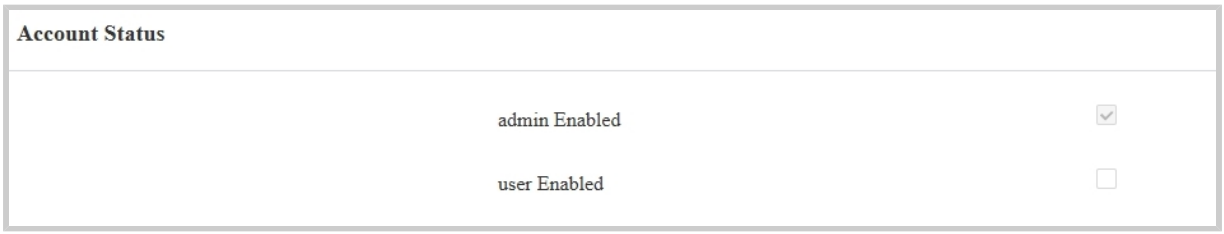
To set it up, go to **System > Security > Web Password Modify** interface.



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



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



Modify Security Questions

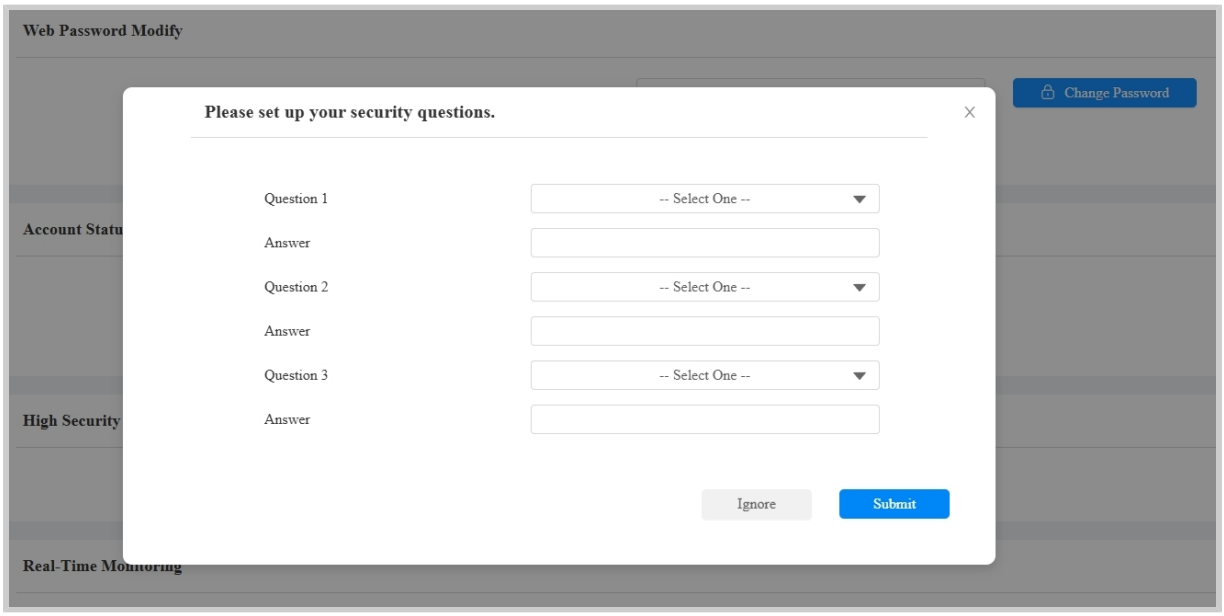
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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**.



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


Web Password Modify
Change Password
Account Statu
High Security
Real-Time Monitoring
Please set up your security questions.
Question 1
-- Select One --
Answer
Question 2
-- Select One --
Answer
Question 3
-- Select One --
Answer
Ignore
Submit

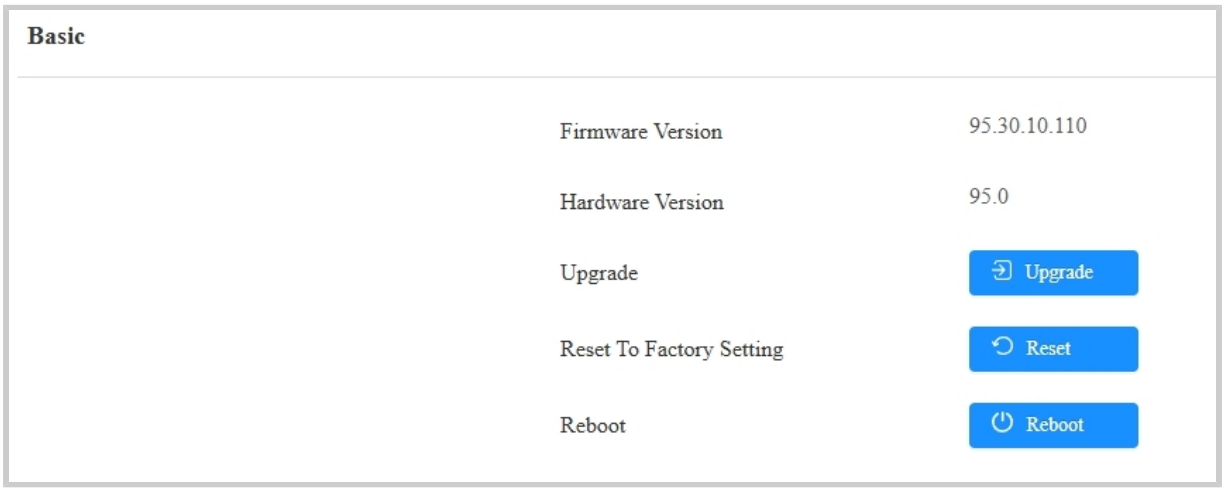
System Reboot & Reset

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.

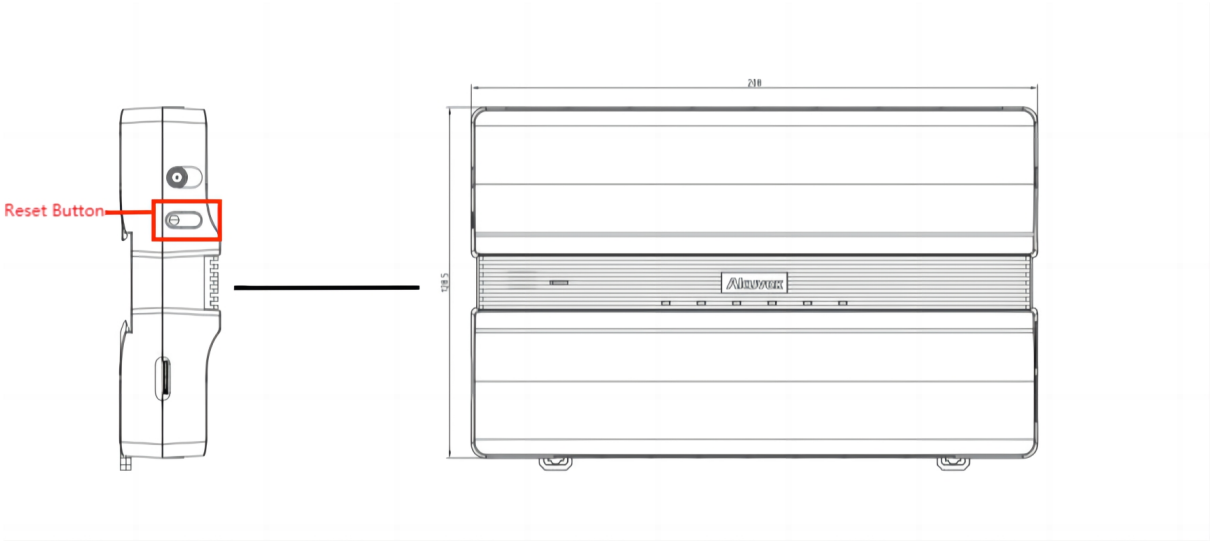


- To set up the device reboot schedule

Navigate to the web **System > Auto Provisioning** interface. Set the time when the device reboots.

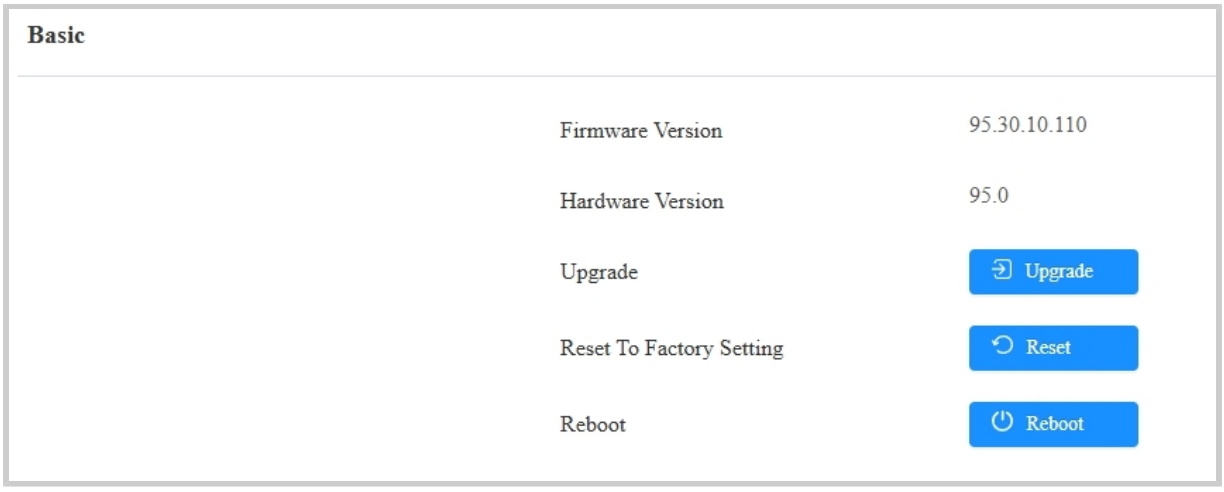


The device can also be rebooted by holding the reset button for 6 seconds.

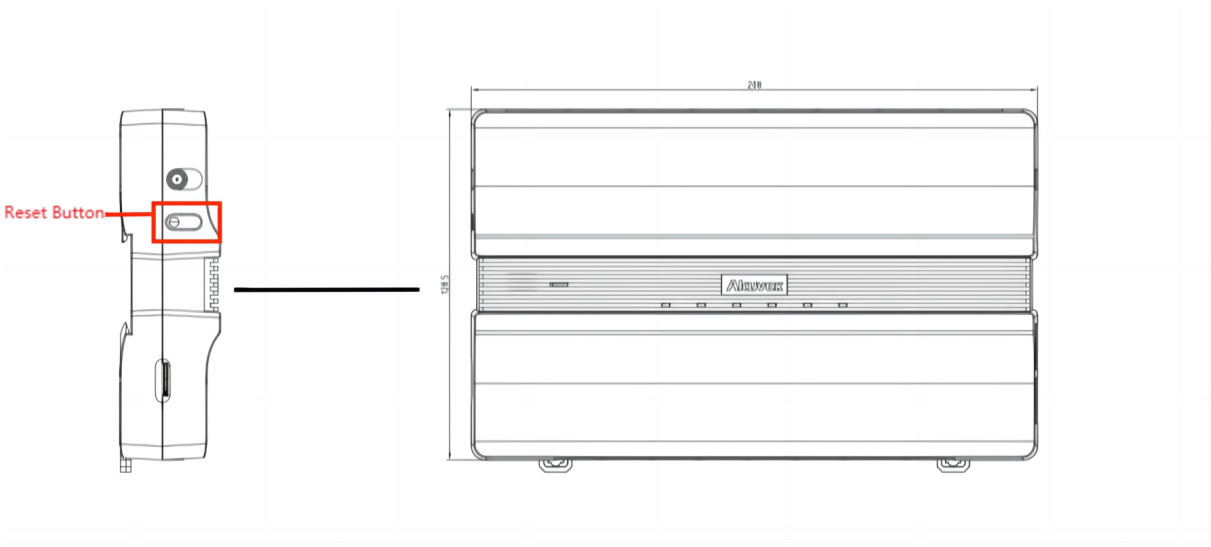


Reset

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



The device can also be reset by holding the reset button for about 15 seconds until the RUN indicator light stops flashing. Then, the device will automatically reset and restart.


Reset Button