

Table of contents

Akuvox EC33 Lift Control Administrator Guide

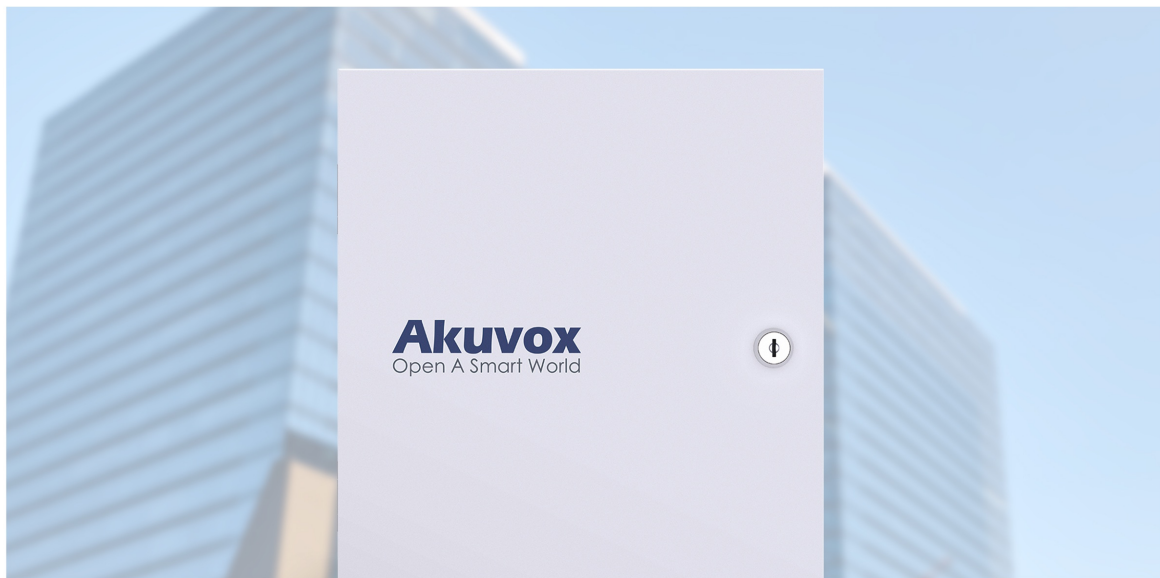
About This Manual	3
Product Overview	5
Changelog	6
Model Specification	7
Before You Start	9
Requirements	9
Indicators	9
Log in to Web Interface	10
Introduction to Configuration Menu	11
Status	12
Info	12
Alarm Log	12
Access Log	13
Network	15
Device Deployment in Network	16
Directory	18
User Management	18
Unlock by Private PIN	18
Unlock by RF Card	19
Access Setting	19
Device	21
Elevator Access Control and Fire Alarm	21
Relay Setting	21
Event-based Elevator Access Control	24
Wiegand	24
RS485	25
Mailbox Control	26
Settings	28
Time	28
Fire Alarm	28
Action URL	29
Schedule	31
HTTP API	32
Auto Provisioning	34
Provisioning Principle	34

Configuration Files for Auto-provisioning	35
AutoP Schedule	36
Static Provisioning	37
DHCP Provisioning	39
PNP Configuration	40
System	42
Upgrade	42
Reboot and Reset	42
Maintenance	43
System Log	43
Remote Debug Server	43
PCAP	44
Backup	45
IP Announcement	45
Security	45
Web Interface Password	45
Emergency Action	46
Web Interface Automatic Log-out	46

About This Manual



WWW.AKUVOX.COM



EC33

ACCESS CONTROLLER

Administrator Guide

Thank you for choosing the Akuvox EC33 lift controller. This manual is intended for administrators who need to properly configure the lift controller. This manual is written based on firmware version 33.30.1.18, and it provides all the configurations for the functions and features of the EC33 lift controller. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



The EC33 controls the elevator using its network-connected relays, providing a smart access control solution for the building. It integrates with Akuvox intercom products to manage access to the key-fobbed elevator. Administrators can configure comprehensive access control settings, including relay control, relay scheduling, card management, and emergency security measures. The device can be deployed, upgraded, configured, and maintained remotely via web-based or cloud-based operations. Additionally, it can be connected to third-party card readers through the Wiegand interface for card-based elevator entry control. Users can grant access to guests or visitors and guide them to the designated floor using the indoor monitor or the SmartPlus mobile app. Furthermore, users can access the building elevator on their current floor using an RFID card on the door phone.

Changelog

What's new in version 33.30.1.18:

- [Support the integration with the KonNaD Mailbox.](#)

Click [here](#) to view the device's previous changelog.

Model Specification

EC33	
CPU	SSD201 / SSD202
Touch Screen	X
Speaker (1W)	1 (For IP number announcement)
IP number announcement button	1
Mic	X
Power Input (12V)	1
Ethernet Port(10/100Mbps)	1
POE (IEEE802.3 af)	1
RS485	2 (1 for connecting the expansion board and the other for connecting with the floor sensors.)
Relay (24V2A 0.21W)	32
Power indicator	1
Network indicator	1
Relay indicator	32
Wiegand	1

Input	1
Reset Button	1
RTC	Capacitive
Power Supply	100~240VAC output, 12V 5A output
Stand by Power Consumption	<=5W
Operation Temperature	-10°C ~ +45°C
Operation Humidity	10% - 90%
Storage Temperature	-20°C~ +70°C
Certification	FCC

Before You Start

This section describes the basic instructions for the start-up operation of the E33 lift control.

Requirements

To deploy the EC33 lift control for the lift control application, make sure that:

- You have powered up the EC33.
- You have networked the EC33.
- You have connected the EC33 to the lift control panel.

Indicators

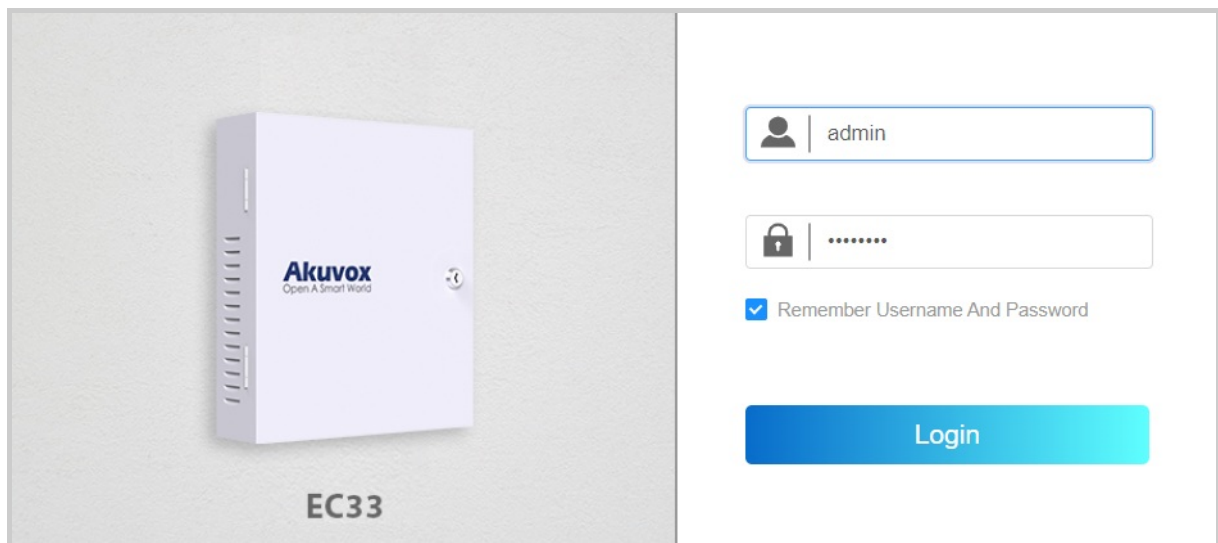
The following table describes the status of different indicators:

Indicator Type	Color	Status	Description
Power Indicator	Red	ON	The power is on
		OFF	The power is off
Network Indicator	Green	ON	The network (LAN Port) is connected
	Green	OFF	The network (LAN Port) is disconnected
	Yellow	ON	The data transmission is on
	Yellow	OFF	The data transmission is off
Relay Indicator	Blue	ON	The relay is on
		OFF	The relay is off.

Log in to Web Interface

You can log into the EC33 web interface to set up and manage device configurations. Open a browser, enter the EC33's IP address, and log in using the default username and password (both are **admin**).

To find the IP address, press the IP announcement button on the circuit board or use the Akuvox IP Scanner.

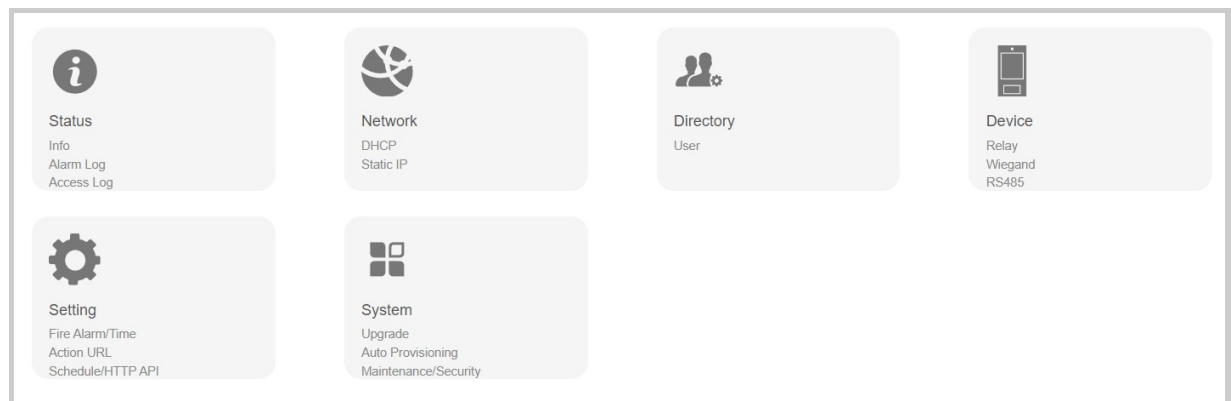


Note

- Download IP scanner:
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- See the 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 local network as the device.

Introduction to Configuration Menu

Akuvox EC33 lift control configuration includes 6 main menus: Status, Network, Directory, Device, Setting, and System.



Status

Info

This submenu displays the device's basic information and network settings.

Navigate to the web **Status> Info** interface.

Product Information		
	Model	EC33
	MAC Address	
	Firmware Version	33.30.0.82
	Hardware Version	33.0.0.0.0.0.0
	Server Mode	None
	Location	Access Control
	Uptime	00:04:53
Network Information		
	Port Type	DHCP Auto
	Link Status	Connected
	IP Address	192.168.36.125
	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

Alarm Log

The alarm log can store up to 100,000 logged alarm events. Every event contains time and date, event type, and alarm status. You can search for and delete the alarm event by date.

Navigate to the web **Status > Alarm Log** interface.

Alarm Log					
Select date		Select date		Q Search	
<input type="checkbox"/>	Index	Type	Date	Time	Status
<input type="checkbox"/>	1	Fire Alarm	2025-09-30	18:12:18	Disarm
<input type="checkbox"/>	2	Fire Alarm	2025-09-30	18:12:14	Turn On
<input type="checkbox"/>	3	Fire Alarm	2025-09-30	18:12:05	Disarm

- **Type:** Indicate alarm type. Currently, only with the fire alarm type.
- **Status:** Display the alarm status indicating if the alarm is on (Turn On) or off (Disarm).

Note

The logged event of a day is from 00:00:00 to 23:59:59 by default.

Access Log

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

Navigate to the web **Status> Access Log** interface.

Access Log								
Save Access Log Enable <input checked="" type="checkbox"/>								
All	Select date	Select date	Name/Code	Q Search		Export		
Index	User ID	Name	Code	Floor No.	Type	Date	Time	Status
1	-	Administrator	-	All	Server	2025-09-30	18:25:30	Success
2	-	-	-	All	HTTP	2025-09-30	18:12:06	Success
3	-	-	-	All	HTTP	2025-09-30	18:01:00	Success

- **Save Access Log Enable:** If enabled, the access log can be synchronized to the SmartPlus Cloud. If disabled, the access event will not be logged.
- **Name:** Display the name of the users for the access.
- **Code:** Display the access card number.
- **Floor No.:** Display the floor number where the door(s) are opened.

- **Type:** Display access method applied.
- **Status:** Display the door-opening result, success or failure.

Network

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

Navigate to the web **Network > Basic** interface.

LAN Port

Type

☐ DHCP
 ☒ Static IP

IP Address

Subnet Mask

Default Gateway

Preferred DNS Server

Alternate DNS Server

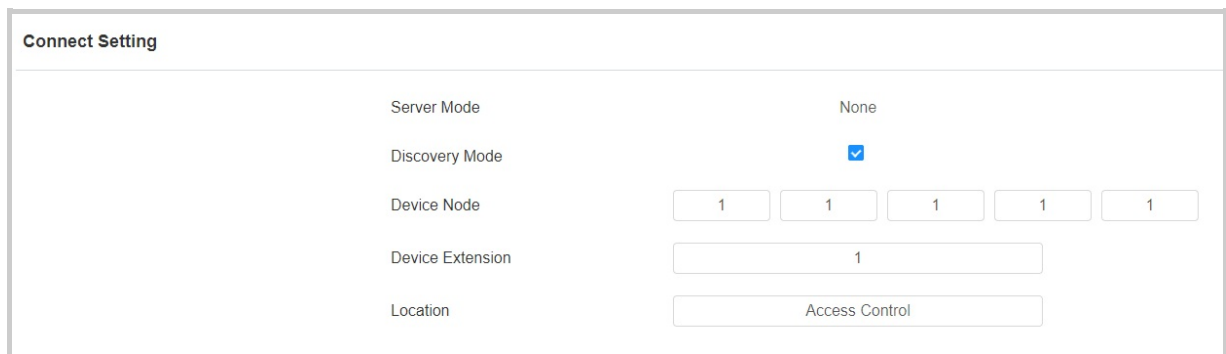
- **DHCP:** DHCP mode is the default network connection. If the DHCP mode is selected, then the device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP:** When static IP mode is selected, the IP address, subnet mask,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

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

Navigate to the web **Network > Advanced** interface.



The screenshot shows the 'Connect Setting' interface with the following fields and values:

Setting	Value
Server Mode	None
Discovery Mode	<input checked="" type="checkbox"/>
Device Node	1 1 1 1 1
Device Extension	1
Location	Access Control

- **Server Mode:** It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None. You can also change it manually.
- **None:** None is the default factory setting indicating the device is not in any server type. Devices connect directly to each other or within a local area network (LAN) without relying on external servers.
- **Cloud:** The device is connected to the SmartPlus Cloud, a cloud-based system simplifying property access management. The Cloud mode allows devices to interact intelligently with one another and the mobile SmartPlus App, backing up data daily and on different hosts. It suits projects requiring smart, flexible, and secure deployment and management.

- **SDMC:** The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.

- **Discovery Mode:** Enabled by default. Available for the **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not discovered by other devices.
- **Device Address:** Available for the **None** server mode. It can be used to call the device. Specify the device address by entering device location information from left to right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension:** Available for the **None** server mode. The device extension number ranges from 0 to 10.
- **Location:** The location in which the device is installed and used. Available for the **None** server mode.

Directory

The directory section lists all the user's information and the access controls you have set up for them. You can search, delete, and edit the users.

User Management

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

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

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

User

ALL

Q Search

Reset

+ Add

Import

Export

	Index	Source	User ID	Name	PIN	RF Card	Schedule ID	Floor No.	Edit
	1	Cloud		8852 123			11528	6	

User Info

User ID

1

Name

- **User ID:** The unique identification number assigned to the user.
- **Name:** The name of this user.

Unlock by Private PIN

The device can be connected to an external keypad. Users can open doors by entering their private PINs on the keypad.

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

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

The device can be connected to an external card reader. Users can open doors by swiping their cards on the reader.

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

RF Card

Code

+ Obtain

Add

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

Note:

- Each user can have a maximum of 5 cards added.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device for access.

Access Setting

Access Setting

Floor No.

None x

Schedule

1 Item

Unselected

☐ 1002:Never

1 Item

Selected

☐ 1001:Always

>

<

- **Floor No.:** **Floor No. :** Specify the floor(s) that are accessible to the user via the elevator.

- **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.

Device

Elevator Access Control and Fire Alarm

You can manage elevator access control through the web interface.

- Click a specific floor number (relay-based) to grant access to that floor.
- Click **Open All** to allow access to all floors.
- Click **Close All** to deny access to all floors.
- In emergencies, such as a fire, click **Turn On Fire Alarm** to trigger the alarm and enable access to all floors.

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

Relay Status

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

32

Open All

Close All

Turn On Fire Alarm

- **Open All:** All relays will stay activated (doors stay open). All relay tabs turn blue.
- **Close All:** All relays will stay deactivated (doors stay closed).
- **Turn On Fire Alarm:** By clicking it, the fire alarm will be triggered and activate all relays at the same time. All relays tab here turns green.

Relay Setting

You can configure the relay activation with a predefined delay and duration. You can also specify the starting floor (relay number). For example, if you set -1 (basement floor 1) as the starting floor, the floor count will begin from -1 as the first floor.

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

Relay Setting	
Startup Validity Check	<input checked="" type="checkbox"/>
Type	Default State ▼
Trigger Delay	0 (0~10Sec)
Hold Delay	5 (1~300Sec)
Floor Starts From	1 ▼
Ground Floor	None ▼
Additional Rules	<input type="checkbox"/>

- **Startup Validity Check:** The device will check whether the relay is functioning normally after rebooting or resetting.
- **Type:**
 - **Default State:** In this state, the relay either remains open or closed based on its configuration. For example, if the relay is normally open (NO), it will be open until activated.
 - **Invert State:** In this state, a normally open relay would be closed (conducting), and a normally closed relay would be open (not conducting). This state is useful for applications where you want to toggle the relay's behavior based on specific conditions.
- **Trigger Delay (Sec):** Set the relay activation delay time (0-10 seconds). The default delay time is 0, meaning immediately activated after triggering.
- **Hold Delay (Sec):** Specify how long the relay stays activated before the door is closed.
- **Floor Starts From:** Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **Ground Floor:** If there are ground floors between the -1 and 1 floors, configure this option.

- **Additional Rules:** Check this option if you want to set up the relay type, trigger delay, and hold delay of a specific relay. Then, click **Add** to add rules.
 - **Relay ID:** Choose the relay(s) to be configured.

Add Additional Rules

Relay ID	<div>1 x</div> <div>2 x</div>
Type	<div>Default State</div>
Trigger Delay	<div>0</div> <div>(0~10Sec)</div>
Hold Delay	<div>5</div> <div>(1~300Sec)</div>

Open Door 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.

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

Open Relay Via HTTP

Enabled	<input type="checkbox"/>
Username	<input type="text"/>
Password	<input type="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:

EC33's IP
http://192.168.35.127/fcgi/do?action=OpenDoor&
Preset credentials for authentication
UserName=admin&Password=12345&
ID of Relay to be triggered
DoorNum=1

Note

Click [here](#) to view how to set up door opening by HTTP commands.

Event-based Elevator Access Control

You can set access control schedules based on events. Choose from your customized schedules and assign them to the relays (floors) for elevator access control. For example, you might [create a schedule](#) for house cleaning in a building or for controlling a school gate (open or closed during specific time intervals).

Set it up on the **Device > Relay** interface. Click **Add** to apply schedules to relays.

The image shows two screenshots of the Akuvox web interface. The top screenshot, titled "Relay Schedule", displays a table with columns for Index, Relay, Schedule ID, and Edit. Above the table is a search bar labeled "Relay ID" with a "Search" button and an "Add" button. The bottom screenshot, titled "Add Scheduled Relay", shows a form for assigning schedules to a relay. It includes a "Relay ID" field, a "Schedule" dropdown menu, and two boxes: "Unselected" (containing "1002:Never") and "Selected" (containing "1001:Always"). Arrows between the boxes allow for moving items between the two states.

- **Relay ID:** Select relay-based floor number. The floor number can be up to 128 if extra control boards are added.
- **Schedule Enabled:** Make the desired schedule effective by moving it from the left to the right box.

Wiegand

EC33 can be connected to third-party devices such as card readers via Wiegand. You set the Wiegand setting based on the technical specification of the third-party device for the integration.

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

Wiegand

Wiegand Display Mode

8HN

Wiegand Card Reader Mode

Wiegand-26

Wiegand Transfer Mode

Input

Wiegand Input Data Order

Normal

Wiegand Input Clear Time

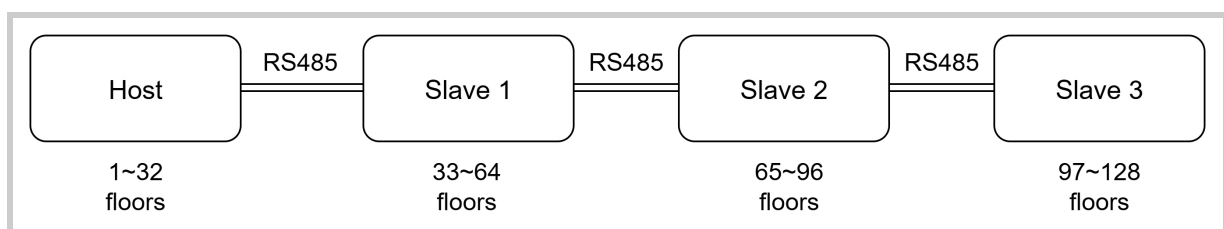
5

- **Wiegand Display Mode:** Select the same Wiegand card code display format as that of the third-party device (8H10D; 6H3D5D; 6H8D; 8HN; 8HR; RAW, 8HR10D).
- **Wiegand Card Reader Mode:** Select the same Wiegand data transmission format as that of the third-party device (Wiegand 26,34,58).
- **Wiegand Transfer Mode:** It is invariably input because E33 receives the data from the third-party card reader.
- **Wiegand Input Data Order:** Select the Wiegand input data sequence: **Normal** for the normal data sequence, and **Reversed** for the reversed order.
- **Wiegand Input Clear Time:** When the interval of entering passwords exceeds the time. All entered passwords will be cleared.

RS485

EC33 is scalable from 32 floors to 128 floors by enhancing it with extra control boards via the RS485 interface. You can either choose the RS485A or B interface for the application.

It supports a maximum of 4 boards connected in series, with the main board supporting configurations for floors of 32, 64, 96, or 128. The first slave board's relays correspond to 33~64 floors.



Set this up on the **Device > RS485** interface. Specify which RS485 interface is used for connection before configuration.

RS485A List

Apply To

Expanding Board(As Host) ▼

Please ensure that only one board is set as the host.

Expanding Board Status

Disconnected

RS485B List

Apply To

None ▼

- **Apply To:**
 - **None:** Disable the feature.
 - **Expanding Board(As Host):** The device works as the main board that can be connected to a slave board. The floor number changes occur on this device's web interface.
 - **Expanding Board(As Slave):** The device works as the slave board that can be connected to another slave board.
- **Expanding Board Status:** Display whether the expanding board is connected.

Mailbox Control

The device supports the integration with KonNaD mailboxes. When the mail carrier delivers the letter, the device receives the message and sends a notification to the resident's SmartPlus App and/or indoor monitor.

Click [here](#) to view the detailed configuration.

Set this feature up on the **Device > Mailbox** interface.

Mailbox Setting

Enabled

☒

Detect Interval

60

(10~3600s)

Notificaiton Title

New Letter

Notification Text Content

Hello, your letter is in the mailbox. Please check it promptly.

Mailbox

Add

Mailbox1 IP Address

Delete

Mailbox 1

Mailbox Status

Disconnect

Fill in the building number and room number in the order of the mailbox. Example: 3#201

Main board

DI1

DI2

DI3

DI4

DI5

DI6

DI7

DI8

DI9

DI10

DI11

DI12

DI13

DI14

DI15

DI16

DI17

DI18

DI19

DI20

DI21

DI22

DI23

DI24

DI25

DI26

DI27

DI28

DI29

DI30

DI31

DI32

Expansion Board

+ Add

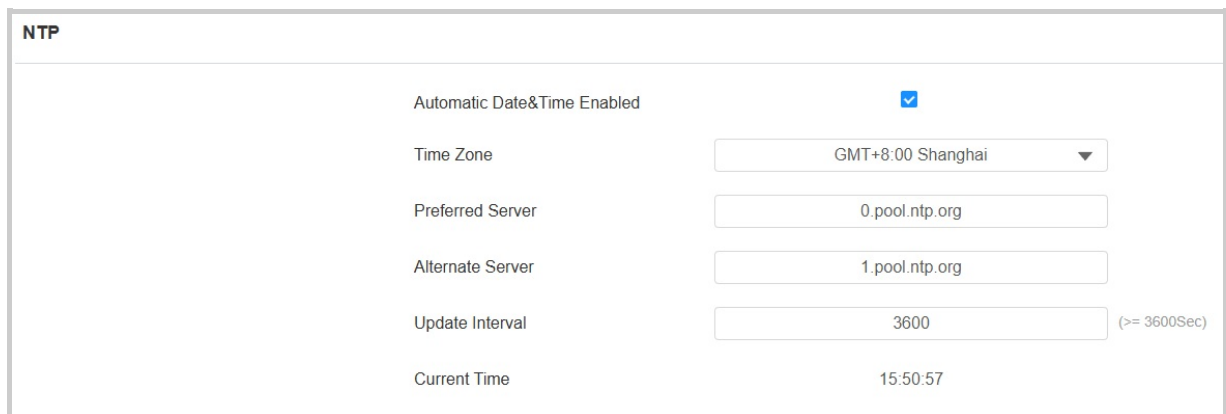
- **Detect Interval:** Define the interval for the device to detect the mailbox. The default is 60 seconds.
- **Notification Title:** Customize the notification title displayed on the SmartPlus App and/or indoor monitor.
- **Notification Text Content:** Customize the notification content displayed on the SmartPlus App and/or indoor monitor.
- **Mailbox IP Address:** Click **Add** to input the mailbox's IP address.
- **Mainboard:** Specify which DI to trigger when the mail is delivered. And fill in the **Building Name#APT Number** where the resident lives in the target DI field. For example, Building A#203.
- **Expansion Board:** If the mailbox's mainboard is connected to an expansion board, click **+Add** to configure it.

Settings

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.

Set it up on the **Setting > Time** interface.



NTP	
Automatic Date&Time Enabled	<input checked="" type="checkbox"/>
Time Zone	GMT+8:00 Shanghai ▼
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600Sec)
Current Time	15:50:57

- **Automatic Date & Time Enabled:** Enable it for NTP-based automatic time update; disable it to manually set up the time and date.
- **Preferred Server:** Set the primary NTP server, which will update the device time periodically.
- **Alternate Server:** Set the backup NTP server. This will be used when the primary NTP server fails.
- **Update Interval:** Set the time interval that the device sends the request to the NTP server for the time update automatically.
- **Current Time:** Display the current device time.

Fire Alarm

When EC33 is triggered by a fire alarm event, it can respond to it with a preset action by sending a preset HTTP command (URL) to a third-party HTTP server for the pre-defined action.

Set it up on the **Setting > Fire Alarm** interface.

Fire Alarm

Enabled

☒

Trigger Electrical Level

Low

Action To Execute

☐ HTTP

HTTP URL

Action Delay

0

(0~300Sec)

Current Status

High

- **Triggered Electrical Level:** Select the trigger electrical level options between High and Low according to the actual operation of the fire alarm switch. The default setting is Low.
- **Action to Execute:** Enable it so that you can type in the HTTP command for the pre-defined action.
- **HTTP URL:** Enter the HTTP URL. The command includes 512 characters at a maximum.
- **Action Delay:** Set the action delay time (0-300 seconds) when the alarm is triggered. The default is 0.

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 alarm status or RF card access changes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Turn on Fire Alarm	\$input1status	Http://server ip/inputtri=\$input1status
2	Disarm Fire Alarm	\$input1status	Http://server ip/inputclose=\$input1status
3	Valid Card Entered	\$card_sn	Http://server ip/validcard=\$card_sn
4	Invalid Card Entered	\$card_sn	Http://server ip/invalidcard=\$card_sn

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

Set it up on the **Setting > Actions URL** interface.

Action URL

Active

☐

Turn On Fire Alarm

Disarm Fire Alarm

Valid Card Entered

Invalid Card Entered

- **Active:** Enable it if you want the Action URL to be sent to the preset server for predefined actions.
- **Turn On Fire Alarm:** The URL will be sent to the preset HTTP server when the fire alarm is triggered.
- **Disarm Fire Alarm:** The URL will be sent when the fire alarm is cleared.
- **Valid Card Entered:** The URL will be sent whenever an access attempt is made by using a valid RFID card.
- **Invalid Card Entered:** The URL will be sent whenever an access attempt is made by using an invalid RFID card.

Schedule

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.

You can add, import, edit, and search the access control schedule. Click **+Add** to add a schedule manually.

Set it up on the **Setting > Schedule** interface. You can add 100 local schedules.

The screenshot shows the 'Schedule' management interface. At the top, there's a dropdown menu set to 'Local' and three buttons: '+ Add', 'Import', and 'Export'. Below is a table with columns: Index, Schedule ID, Source, Mode, Name, Date, Day Of Week, Time, and Edit. There are three rows of schedules. At the bottom, there are pagination controls: 'Selected: 0/3', 'Delete', 'Delete All', 'Total: 3', 'Prev', '1/1', 'Next', 'Go To Page 1', and a 'Go' button.

Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
1	1001	Local	Daily	Always			00:00-23:59	
2	1002	Local	Daily	Never			00:00-00:00	
3	1	Local	Normal	Office Cleaning	20221101-20221130	Monday,Tuesday,Wednesday,Thursd ay, Friday	00:00-23:59	

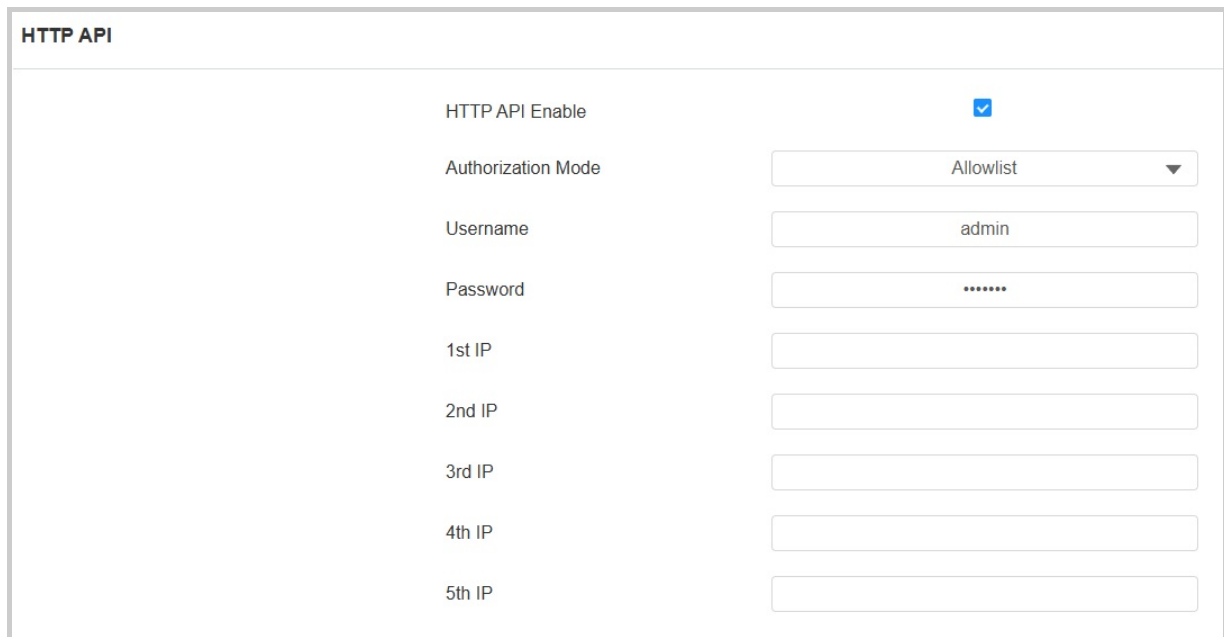
The screenshot shows the 'Add Schedule' modal form. It has fields for Name, Mode (set to 'Normal'), Date Range (2025-10-09 to 2025-10-10), Day Of Week (checkboxes for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, and a 'Check All' option), and Date Time (00:00 to 23:59). There are 'Cancel' and 'Submit' buttons at the bottom.

- **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.

HTTP API

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

Set it up on the **Setting > HTTP API** interface.



HTTP API	
HTTP API Enable	<input checked="" type="checkbox"/>
Authorization Mode	Allowlist ▼
Username	admin
Password	*****
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

- **HTTP API Enabled:** 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:** Select among the following options: None, Allowlist, Basic, Digest, and Token for authorization type, which will be explained in detail in the following chart.
- **User Name:** 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.

Please refer to the following description for the authentication mode:

Authorization Mode	Description
None	No authentication is required for HTTP API as it is only used for demo testing.
Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication. The allowlist is suitable for operation in the LAN.
Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode of username and password.
Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
Token	This mode is used by Akuvox developers only.

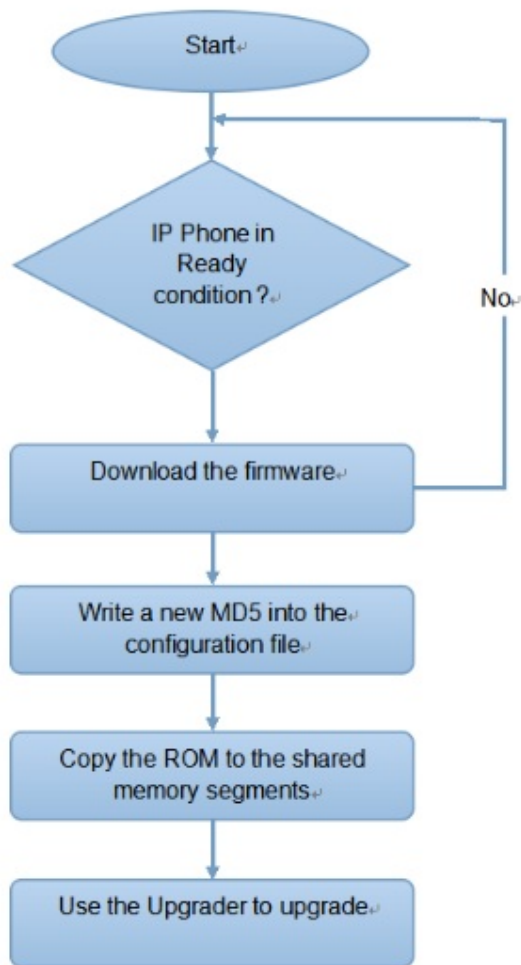
Auto Provisioning

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

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.

Set it up on the **System > Auto Provisioning** interface.

Automatic Autop

Mode	Power On ▼
Schedule	Sunday ▼
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

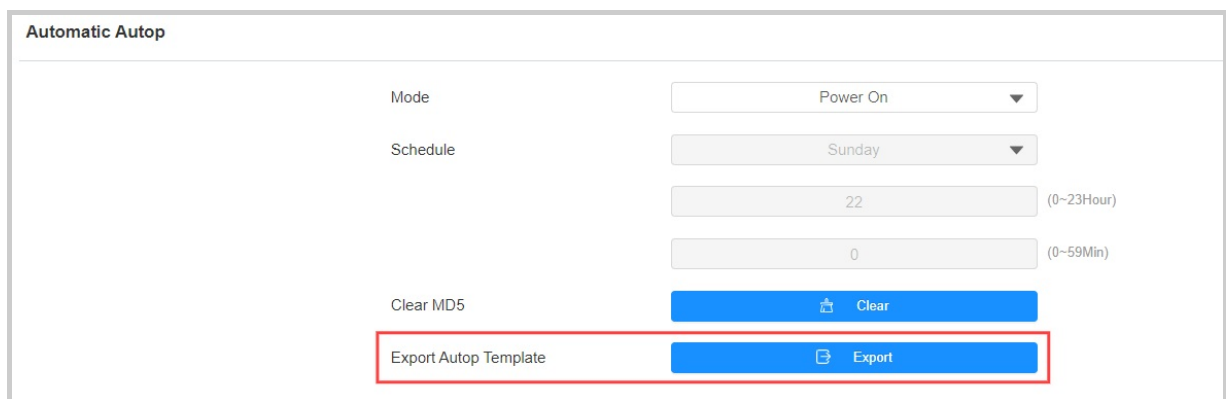
- **Mode:**
 - **Power On:** Allow the device to perform Autop every time it boots up.

- **Repeatedly:** Allow the device to perform Autop according to the schedule.
- **Power On + Repeatedly:** Combine Power On and Repeatedly modes, allowing the device to perform Autop every time it boots up or according to the schedule.
- **Hourly Repeat:** Allow the device to perform Autop every hour.
- **Schedule:** When Power On + Repeatedly mode is selected, you can select the specific day and time for the Autop.
- **Clear MD5:** Used to compare the existing autop file with the autop file in the server; if the files are the same, then the provisioning will be stopped, thus avoiding unnecessary auto-provisioning.

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.

Download the Autop template on the **System > Auto Provisioning > Automatic Autop** interface.




The screenshot shows the 'Automatic Autop' configuration page. It includes a 'Mode' dropdown set to 'Power On', a 'Schedule' dropdown set to 'Sunday', and two time input fields: '22' (0~23Hour) and '0' (0~59Min). Below these are two buttons: 'Clear MD5' and 'Export Autop Template'. The 'Export Autop Template' button is highlighted with a red rectangular box.

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

Manual Autop

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

 AutoP Immediately

- **URL:** The TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username:** Set up a username if the server requires a username to be accessed.
- **Password:** Set up a password if the server requires a password to be accessed.
- **Common AES Key:** Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key(MAC):** Set up the AES code for the intercom to decipher the MAC-based auto-provisioning configuration file.

Note

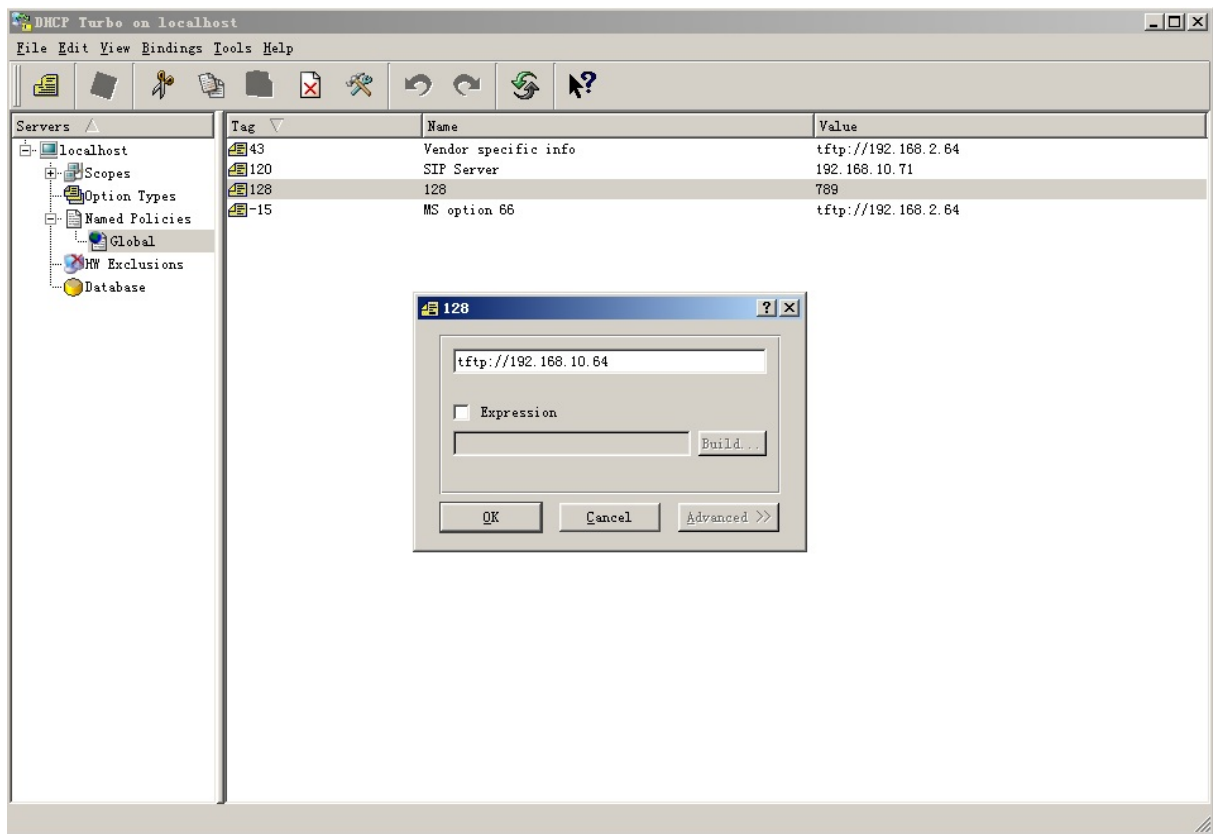
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/(use 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 does not provide a user-specified server. Please prepare the TFTP/FTP/HTTP/HTTPS server by yourself.

DHCP Provisioning

Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **CustomOption** as defined by users with option codes ranging from 128-255, you are required to configure DHCP Custom Option on the web interface.

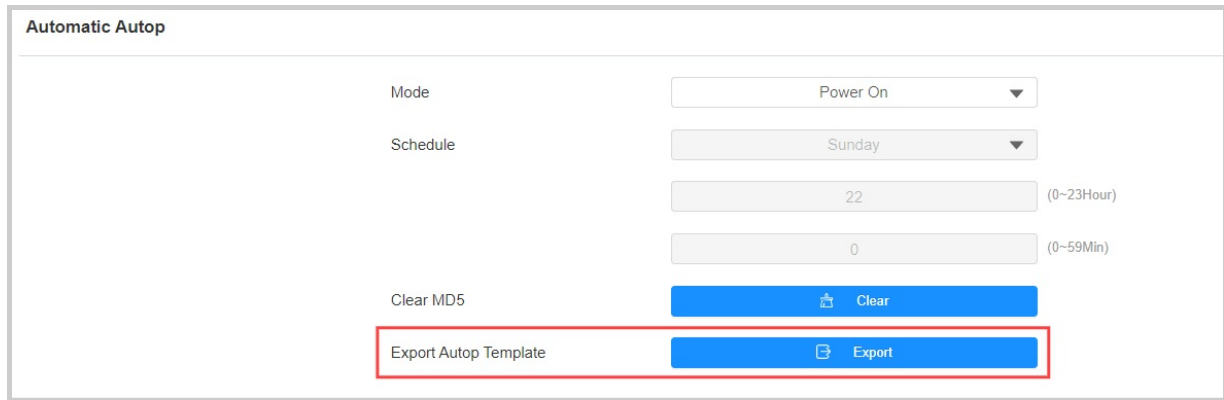


Note

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

Set up DHCP Autop with Power On mode and export Autop Template to edit the configuration.

Download the Autop template on the **System > Auto Provisioning > Automatic Autop**.



Automatic Autop

Mode: Power On

Schedule: Sunday

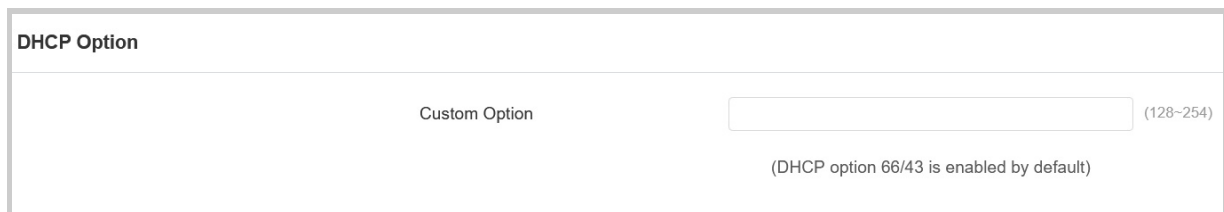
22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

Set it up on **System > Auto Provisioning > DHCP Option** interface.



DHCP Option

Custom Option: (128-254)

(DHCP option 66/43 is enabled by default)

- **Custom Option:** Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66:** If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL. This is done within the software, and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.
- **DHCP Option 43:** If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software, and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user.

Click [here](#) to watch the configuration video.

Enable/disable it on the web **System > Auto Provisioning > PNP Option** interface.





PNP Option
PNP Config Enabled
<input checked="" type="checkbox"/>

System

Upgrade

Upgrade the device on the **System > Upgrade** interface. Click **Import** to select and upload the file.

Basic

Firmware Version	33.30.0.82
Hardware Version	33.0.0.0.0.0.0
Upgrade	 Import
Reset Configuration to Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

Tip

Click [here](#) to download the latest firmware and view changelogs.





Reboot and Reset

Reboot and reset the device on the **System > Upgrade** interface.

The device provides two reset options:

- **Reset to Factory Setting:** Reset all data to the factory default.
- **Reset Configuration to Default State(Except Data):** Retain the user data, such as the RF cards and schedules.

Basic

Firmware Version	33.30.0.82
Hardware Version	33.0.0.0.0.0.0.0
Upgrade	 Import
Reset Configuration to Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot


Maintenance

System Log

System logs can be used for debugging purposes.

Export system logs on the **Maintenance > System Log** interface.

System Log

Log Level	<div>3</div>
Export Log	 Export
Remote System Log Enabled	<input type="checkbox"/>
Remote System Server	<div></div>

- **Log Level:** Select log levels 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:** Export the system log file to a local PC before you send it to the Akuvox technical support team.
- **Remote System Server:** Enter the remote server address to which the system log will be sent. The remote server address is provided by the Akuvox technical team.

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.

Set it up on the **System > Maintenance > Remote Debug Server** interface.

Remote Debug Server

Enabled	<input type="checkbox"/>
Connect Status	Disconnected
IP Address	<input type="text"/>
Port	<input type="text"/> (1024~65535)

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

PCAP

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

Set it up on the **System > Maintenance > PCAP** interface.

PCAP

Specific Port	<input type="text"/> (1~65535)
PCAP	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Export"/>
PCAP Auto Refresh Enabled	<input type="checkbox"/>

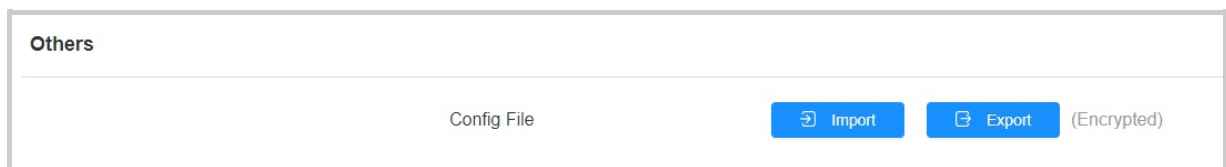
- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the port can be captured. You can leave the field blank by default.
- **PCAP:** Pick a certain data packet range by clicking Start and Stop. Then export the data packet captured during the time interval to your local PC.

- **PCAP Auto Refresh Enabled:** If you enable it, the PCAP will continue to capture data packets even after the data packets reach their maximum capacity. If you disable it, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing 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 formats are TGZ, CONF, and CFG.



Others

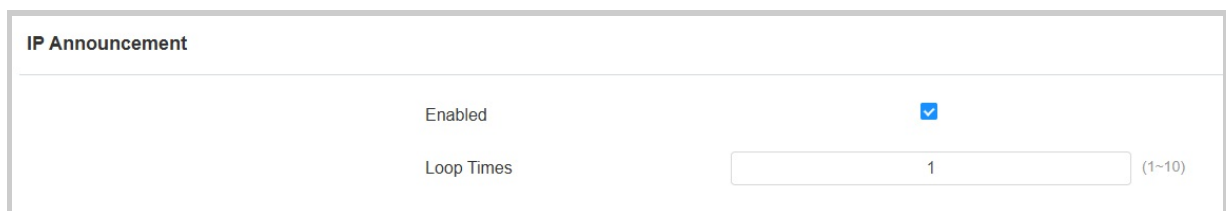
Config File

Import Export (Encrypted)

IP Announcement

With IP announcement enabled, you can easily obtain the EC33's IP address by holding the physical button on the control board during deployment. You can also set the number of IP announcements.

Set it up on the **System > Maintenance > IP Announcement** interface. This feature is enabled by default.



IP Announcement

Enabled ☒

Loop Times (1~10)

Security

Web Interface Password

The web password is used to access the device's web settings. You can change it on the **System > Security** interface.

Select **admin** for the administrator account and **user** for the user account. Then, click the **Change Password** tab.

Web Password Modify

Username

admin

Change Password

You can also enable or disable the user account.

Account Status

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

Emergency Action

This feature works with Akuvox SmartPlus Cloud. It keeps the door open when an emergency happens.

Click [here](#) to view the detailed configuration of this feature.

Enable this feature on the **System > Security** interface.

Emergency Action

Enabled

☐

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.

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

Session Time Out

Session Time Out Value

300

(60~14400Sec)