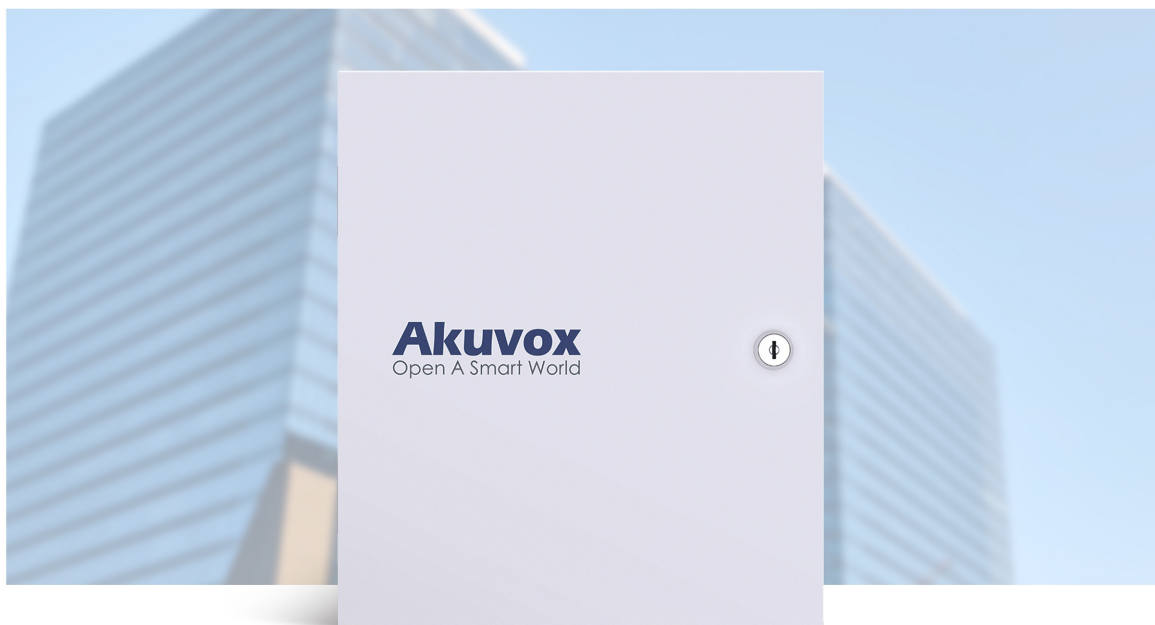


About This Manual



WWW.AKUVOX.COM



EC33

ACCESS CONTROLLER

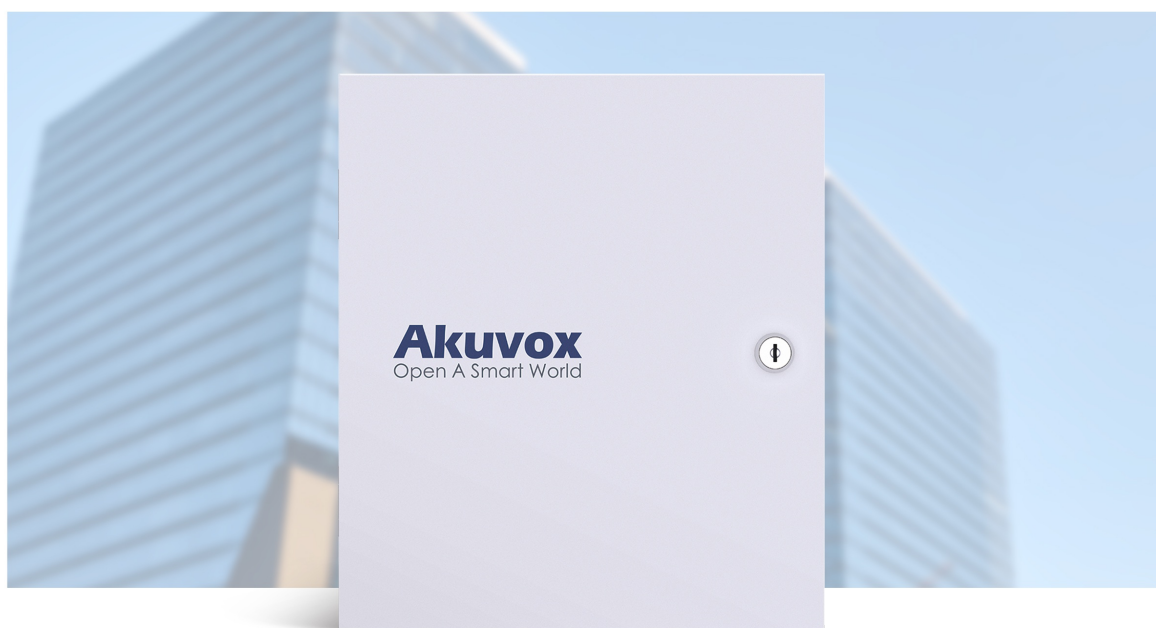
Administrator Guide

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 33.30.0.82, 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.

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 33.30.0.67, 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.

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 (IEEE802.3af)	1
RS485	2 (1 for connecting the expansion board and the other for connecting with 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.

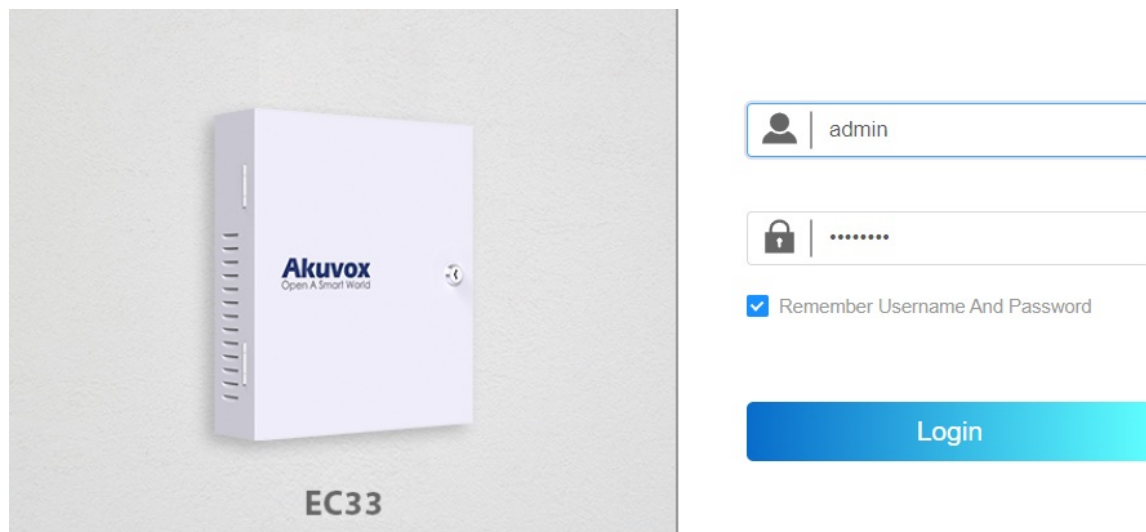
Indicators

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 into Web Interface

You can log into the EC33 web interface, which allows you to set up and manage the device configurations. You can open a browser and enter the IP address of EC33, then enter the username and password to log in to the web interface (The default username and password are both Admin). You can obtain the IP address by holding the IP announcement button on the circuit board or using the Akuvox IP Scanner.

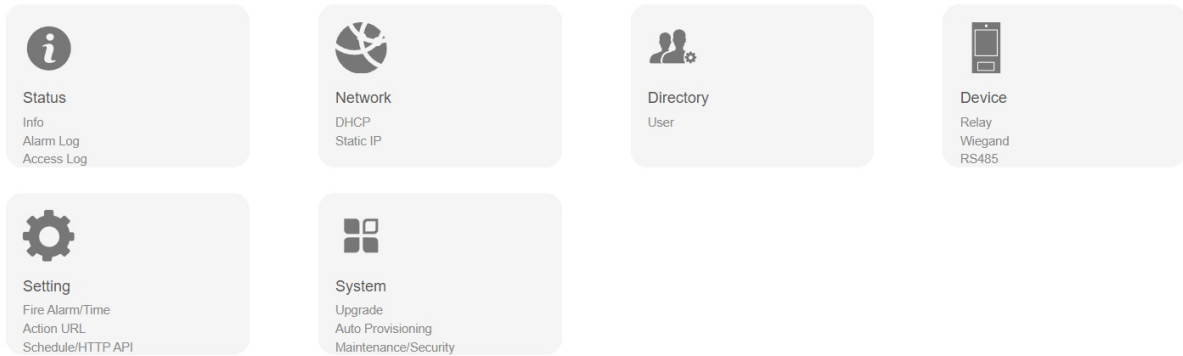


Note

- 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.
- Please be case-sensitive to the user names and passwords entered.

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	0C3305000031
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 and delete the alarm event by date.

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

AlarmLog

-

	Index	Type	Date	Time	Status
 No Data					

Selected: 0/15

Total: 15

1/1

Go To Page

- **Type** indicates 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 ☒

-

	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status
 No Data									

Selected: 0/0

Total: 0

1/1

Go To Page

- **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.
- **Door ID:** display the relay (relay number) that has been triggered for the elevator door opening.
- **Type:** display access method applied. Currently only with card and HTTP commands.
- **Status:** display the door opening 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	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Preferred DNS Server	<input type="text"/>
Alternate DNS Server	<input type="text"/>

- **DHCP** is the default network connection. The device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: 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 if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to the actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **Preferred/Alternate DNS Server**: set up the primary Domain Name Server(DNS). The preferred server is the primary server address while the alternate one is for backup. The device will connect to the alternate server when the primary server 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.

Connect Setting

Server Mode	None
Discovery Mode	<input checked="" type="checkbox"/>
Device Node	<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Location	<input type="text" value="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** or **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type.
- **Discovery Mode:** the discovery mode makes the device be discovered by other devices in the network. Disable it if you want to conceal the device so as not to be discovered by other devices. After turning off the discovery mode, you need to restart the device to take effect.
- **Device Node:** specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, and Room** in sequence.
- **Device Extension:** enter the device extension number for the device you installed.
- **Device Location:** enter the location in which the device is installed and used.

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

When adding users, you need to set up their unique user information, and the access control to allow them to access the elevator in the building. To add users, click Import to upload the users and access control using .tgz files or you can click +Add to add users one by one.

Navigate to the web **Directory > Users** interface.

User Info

User ID

2

Name

- **User ID:** it is automatically generated by the system. The number will be in descending order, for example, 1234.
- **Name:** enter the username.

PIN

Code

RF Card

Code

+ Obtain

Add

- **PIN:** the PIN code users can use to open the door.
- **Code:** place the RFID card on the card reader area and click Obtain to acquire the code.

Access Control Setting

Access Setting

Floor No.	<input type="text" value="None x"/>	
Schedule	<div><div>1 Item</div><div>Unselected</div><div><input type="checkbox"/> 1002:Never</div></div>	<div><div>1 Item</div><div>Selected</div><div><input type="checkbox"/> 1001:Always</div></div>

- **Floor No.:** the floor the users can access by elevator.
- **Schedule:** select the elevator access control schedule. **1001: Always** means users can always open the elevator door via RF cards. **1002: Never** means users cannot open the elevator door via RF cards.

Device

Elevator Access Control and Fire Alarm

You can conduct elevator access control on the web interface. You can click a specific floor number (the relay-based number) to allow access to the specific floor, click **Open All** to allow all floor access by the elevator and click **Close All** to deny elevator access to all the floors. In certain emergencies such as a fire accident occurring, you can click **Turn On Fire Alarm** which allows you to trigger the fire alarm while turning on all relays for all-floor access.

Navigate to the web **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 relays tab here turns 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 set the relay activation with a predefined delay time, and the relay duration time. Here, you can also decide on the first floor that floor (relay number) starts from. For example, if you set -1 (basement floor 1) as the first floor, then the floor count will start from -1 floor, the first floor.

Navigate to the web **Device > Relay** interface.

Relay Setting

Startup Validity Check	<input checked="" type="checkbox"/>
Trigger Delay(Sec)	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>
Floor Starts From	<input type="text" value="1"/>

- **Startup Validity Check:** the device will check whether the relay is functioning normally after rebooting or resetting.
- **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.
- **Relay Floor Start 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).

HTTP Door Unlock

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

Navigate to the web **Device > Relay** interface.

Open Relay Via HTTP

Enabled	<input checked="" type="checkbox"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>

- **Username:** enter the user name for the HTTP command authentication, for example, **admin**.
- **Password:** enter the password for the HTTP command authentication, for example, **12345**.

Please refer to the example: <http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1>

Event-based Elevator Access Control

You can set the access control schedule on an event basis. You can select from your customized access control schedules and assign them to the relays (floors) you need for elevator access control. For example, a customized event can be house-cleaning in a building or the school gate control (staying open or closed during certain time intervals).

Navigate to the web **Device > Relay** interface.

Relay Schedule

Relay ID: All

Schedule Enabled: ☒

3 items	Unselected		0 item	Selected
<input type="checkbox"/> 1001:Always		>		
<input type="checkbox"/> 1002:Never		<		
<input type="checkbox"/> 1:Office Cleaning				
			No Data	

- **Relay ID:** select relay-based floor number (All, 1-32 floors). The floor number can be up to 64 if an extra control board is added.
- **Schedule Enabled:** select the schedule you need for your event. 1001 Always means to stay open, and 1002 Never means to stay closed.

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.

Navigation to the web **Device > Wiegand** interface.

Wiegand

Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	Wiegand-26 ▼
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal ▼

- **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, Reversed). Select **Normal** for the normal data sequence, and Reversed for the reversed order.

RS485

EC33 is scalable from 32 floors to 64 floors by enhancing it with an extra control board via the RS485 interface. You can either choose RS485A or B interface for the application. When you select **Expansion Board**, then the selectable floor range will be changed from 32 to 64 in the access control schedule. **None** is the default setting you choose to disable the function.

Navigate to the web **Device > RS485** interface.

RS485AList

Apply To

None ▼

RS485BList

Apply To

Expanding Board ▼



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.

Navigate to the web **Setting > NTP** interface.

NTP

Automatic Date&Time Enabled	<input type="checkbox"/>
Date	<input type="text" value="2022-11-06"/> 
Time	<input type="text" value="13:13"/> 
Time Zone	<input type="text" value="GMT+0:00 London"/> ▼
Preferred Server	<input type="text" value="0.pool.ntp.org"/>
Alternate Server	<input type="text" value="1.pool.ntp.org"/>
Update Interval	<input type="text" value="3600"/> ($\geq 3600\text{Sec}$)
Current Time	13:24:38

- **Automatic Date & Time Enabled:** enable it for NPT-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.

Navigate to the web **Setting > Fire Alarm** interface.

Fire Alarm

Enabled	<input checked="" type="checkbox"/>
Trigger Electrical Level	Low ▼
Action To Execute	<input type="checkbox"/> HTTP
HTTP URL	<input type="text"/>
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 (Command). The command includes 512 characters 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. `http://server ip/inputclose=$input1status`

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

Navigate to the web **Setting > Actions URL** interface.

Action URL

Active	<input type="checkbox"/>
Turn On Fire Alarm	<input type="text"/>
Disarm Fire Alarm	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<input type="text"/>

- **Active:** enable it if you want the Action URL to be sent to the preset server for predefined actions.
- **Turn On Fire Alarm:** type in the corresponding action URL that will be sent to the preset HTTP server when the fire alarm is triggered.
- **Disarm Fire Alarm:** type in the corresponding action URL that will be sent to the preset HTTP server when the fire alarm is cleared.

- **Valid Card Entered:** type in the action URL that will be sent to the preset HTTP server whenever an access attempt is made by using a valid RFID card.
- **Invalid Card Entered:** type in the action URL that will be sent to the preset HTTP server 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.

Navigate to the web **Setting > Schedule** interface.

Schedule

Local ▼

+ Add

📄 Import

📄 Export

<input type="checkbox"/>	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
<input type="checkbox"/>	1	1001	Local	Daily	Always			00:00-23:59	
<input type="checkbox"/>	2	1002	Local	Daily	Never			00:00-00:00	
<input type="checkbox"/>	3	1	Local	Normal	Office Cleaning	20221101-20221130	Monday, Tuesday, Wednesday, Thursday, Friday	00:00-23:59	

Selected: 0/3

Delete

Delete All

Total: 3

Prev

1/1

Next

Go To Page

1

Go

Add Schedule

X

Name

Mode

Date Range

 -

Day Of Week

☒ Monday
 ☒ Tuesday
 ☒ Wednesday
☒ Thursday
 ☒ Friday
 ☒ Saturday
☒ Sunday
 ☐ Check All

Date Time

 -

Cancel

Submit

- **Name:** name the schedule.
- **Mode:** select schedule type(Normal, Weekly, Daily). Select Normal for a longer period of access control schedule.

HTTP API

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

Navigate to the web **Setting > HTTP API** interface.

HTTP API

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

- **HTTP API Enable:** if it is disabled, the request from the third-party products will be denied and returned with HTTP 403 Forbidden.
- **Authorization Mode :**
 - None: No authentication is required for HTTP API as it is only used for demo testing.
 - Allowlist: this mode requires you to enter the IP address of the devices that you allow for the integration via HTTP API.
 - Basic: this mode requires you to fill in the User name and the password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode the username and password.
 - Digest: password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx",opaque="xx".
 - Token: this mode is used by Akuvox developers only.
- **Username:** customize the username for authentication.
- **Password:** customize the password for authentication.

- **IP(1-5):** type in the IP address of the third-party device allowed for the integration. This is applied only for Allowlist mode.

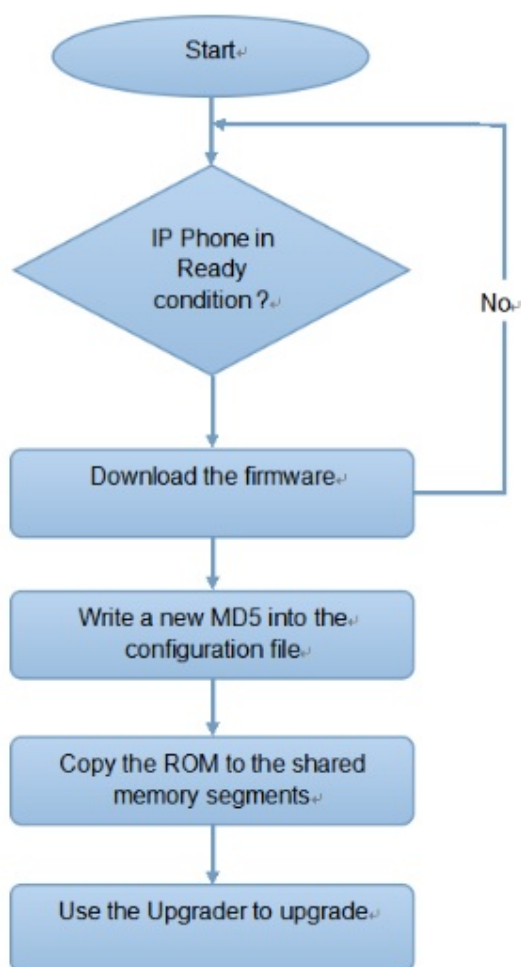
Auto Provisioning

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 at a specific time according to your schedule.

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

Automatic Autop

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

- **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 you set up.
 - **Power On + Repeatedly:** combine **Power On** and **Repeatedly** modes that will enable the device to perform Autop every time it boots up or according to the schedule you set up.

- **Hourly Repeat:** allow the device to perform Autop every hour.

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.

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

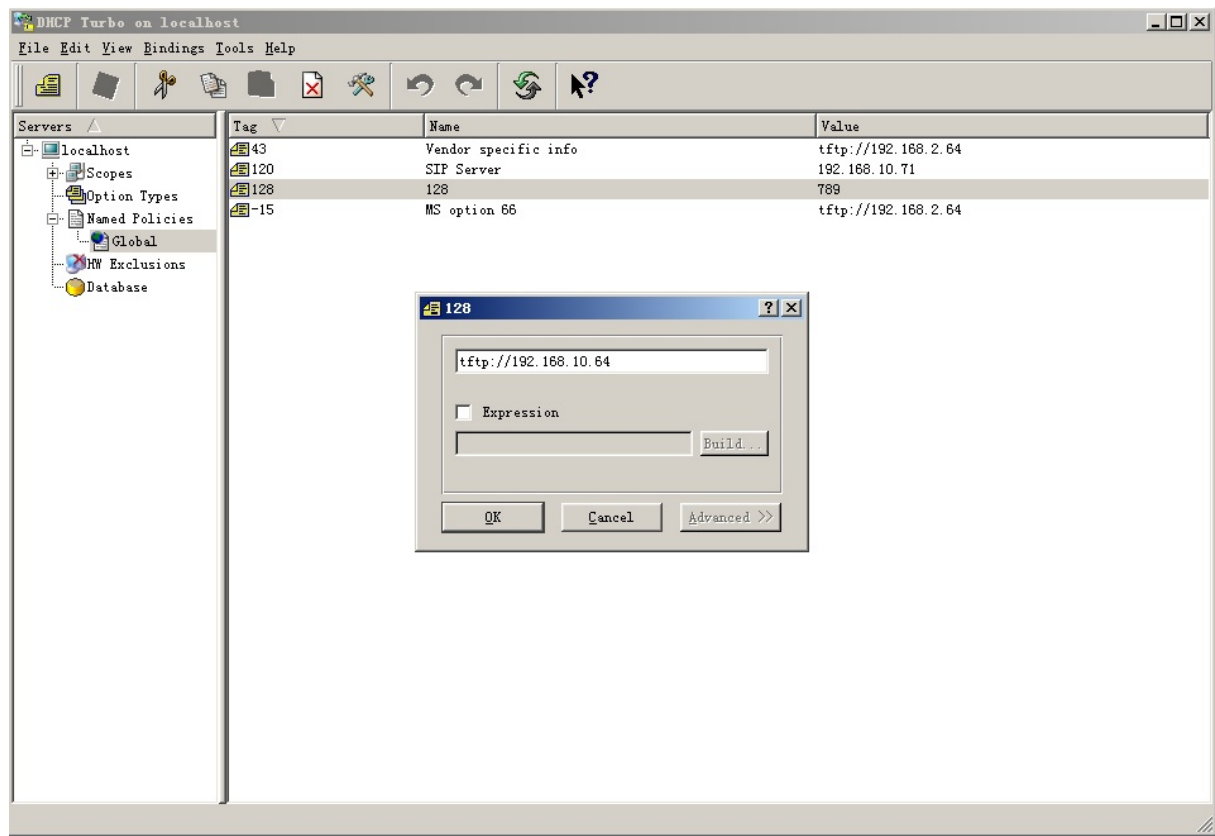
PNP Option

PNP Config Enabled



DHCP Provisioning Configuration

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 **Custom Option** 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.

To set up DHCP AutoP with Custom Option and Power on mode, on web **System > Auto Provisioning > Automatic Autop** interface. Click the **Export** tab in **Export Autop Template** to export the Autop template. Then set up the DHCP Option on the DHCP server.

Automatic Autop

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

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.

Note

- The general configuration file for the in-batch provisioning is with the **cfg** format, taking E16 as an example r000000000116.cfg (9 zero in total while the MAC-based configuration file for the specific device provisioning is with the format MAC_Address of the device. cfg), for example, **0C110504AE5B.cfg**.

Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device will perform the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.

Download the Autop template on **System > Auto Provisioning > Automatic Auto**, and set up the provisioning server on **System > Auto Provisioning > Manual Autop** interface.

Automatic Autop

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

Manual Autop

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Common AES Key	<input type="password" value="*****"/>
AES Key(MAC)	<input type="password" value="*****"/>
	<input type="button" value="AutoP Immediately"/>

- **URL:** set up TFTP, HTTP, HTTPS, and FTP server addresses for the provisioning.
- **User Name:** set up a user name if the server needs a user name to be accessed.
- **Password:** set up a password if the server needs the password to be accessed.
- **Common AES Key:** set up AES code for the intercom to decipher the general Auto Provisioning configuration files.
- **AES Key (MAC):** set up 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 do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

System

Upgrade

You can select **Reset To Factory Setting** if you want to reset the device (deleting both configuration data and user data such as RF cards, face data, and so on). Or, select **Reset Configuration to Default State (Except Data)**, if you want to reset the device (retaining the user data).

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

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.

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

System Log

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

- **Log Level:** select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging 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.

Navigate to the web **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.

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

PCAP

Specific Port

(1~65535)

PCAP
 Start
Stop
Export

PCAP Auto Refresh Enabled
 ☐

- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the 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.

Others

Config File
 Import
Export
(Encrypted)

IP Announcement

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

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

IP Announcement

Enabled



Loop Times

1

(1~10)

Security

Web Interface Password

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

To change the default web password, select **admin** for the administrator account and **user** for the user account. Click the **Change Password** tab to change the password.

Web Password Modify

Username

admin



Change Password

You can also enable or disable the user account.

Account Status

admin

Enabled

user



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.

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

Session Time Out

Session Time Out Value

300

(60~14400Sec)