

Akuvox E12W Intercom

NOTE:

This guide makes the following assumptions

- You know how to/already created a site in the Akuvox Cloud
- You have already added the E12W via its MAC on the cloud

The navigation to settings may be different as updates are pushed out quite regularly. Features may be reworked or missing here.

The navigation will be different depending on the Hardware version.

Accessing the Intercom

The E12W Intercom can be accessed either via the cloud or IP address. It is recommended that you log into it via IP Address first for initial setup.

Devices can sometimes not immediately connect to the cloud until they've first been logged into via IP Address.

After you've added the E12 to the site:

- ❖ Use an IP Scanner to get the IP Addresses of the E12. Akuvox has its own IP Scanner for detecting its own products, so it might be best to use theirs if you can't detect it on your IP Scanner.
 - Link to IP Scanner: <https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP%20scanner>
- ❖ Paste the IP into your browser to get into the Web GUI
- ❖ Log into the E12 with the default username and password being admin.
- ❖ You might need to reset the E12 to get it to connect to the cloud, for a fresh new connection.

Account setup

When you add the E12 to the cloud, it should automatically pull its details for its Akuvox account and set as Account 1 by default.

Setting up Group Calls

Usually, it can pull from the cloud automatically the SIP numbers of monitors and apps in the site. But if there's specific numbers that are that you want called, you can manually put in the SIP numbers. There are 2 tables there, 1 for the cloud pulled numbers and 1 for the local numbers. The moment any number is added to the local numbers, it will override the cloud numbers and only call those in the local table. If local is empty, then it will call the cloud numbers.

Basic

Manager Dial

Call Type

Group Call

Call Timeout (Sec)

20

(If the local group is not blank, then only the local numbers will be called.)

Group Call Number (Local)

847006276			

Group Call Number (Cloud)

847116119/1	847116120/1		

- ❖ Log into the device either via IP Address or “Remote Control” in the cloud
- ❖ Go to Intercom > Basic and look at Group Call
- ❖ Enter the SIP numbers you want the E12 to call in the textboxes. You can add 1 or multiple SIP numbers. Be sure to double check you are putting the right SIP numbers.
- ❖ If you want the E12 to call phone line numbers, you’ll need a third-party SIP service like “2Talk” and add that as the second account.
- ❖ Submit

Setting Up Sequence Call

There is no way to set it up on the actual E12. You’ll need to do it through the cloud. Specifically, this can only be done in a **community site**.

Setting up Relay

The E12 has one in built relay

- ❖ Go to Access Control > Relays
- ❖ Here are all the settings that configure the Relay.

► Status

► Account

► Network

► Intercom

► Surveillance

▼ Access Control

Input

Relay

Web Relay

BLE

Card Setting

User

Access Allowlist

Door Log

Lift Control

► Device

► Setting

► Upgrade

► Security

Relay

Relay

TypeDefault state▼

ModeMonostable▼

Trigger Delay(Sec)0▼

Hold Delay(Sec)3▼

DTMF Mode1 Digit DTMF▼

1 Digit DTMF#▼

2~4 Digits DTMF

Relay StatusLow

Relay NameRelay1

Security Relay

Relay IDSecurity Relay A

Connect TypeRelay

Trigger Delay(Sec)0▼

Hold Delay(Sec)5▼

1 Digit DTMF2▼

2~4 Digits DTMF

Relay NameSecurity Relay A

Enabled☐

Test

Help

Note:
Max length of characters for input box:
255: Broadsoft Phonebook server
address
127: Remote Phonebook URL &
AUTOP Manual Update Server URL
63: The rest of input boxes

Warning:

Field Description:

Submit Shortcut

SubmitCancel

Open Relay via DTMF

- ❖ Go to Access Control > Relays and look at Open Relay via DTMF

Relay

Relay

TypeDefault state▼

ModeMonostable▼

Trigger Delay(Sec)0▼

Hold Delay(Sec)3▼

DTMF Mode1 Digit DTMF▼

1 Digit DTMF#▼

2~4 Digits DTMF

Relay StatusLow

Relay NameRelay1

Open Relay Via DTMF

Assigned The Authority For

Allowlist And Push Button ▼

Disable/Enable Tones

Open Door Tone Setting

Open Door Inside Tone Enabled ☒

Open Door Outside Tone Enabled ☒

Open Door Failed Tone Enabled ☒

- ❖ Go to Device > Audio and look at Open Door Tone setting
- ❖ Tick/Untick the checkboxes of the tone you want enabled/disabled
- ❖ Submit

Volume

Audio

Volume Control

Mic Volume	8	(1~15)
Volume Level	1	▼
Speaker Volume	15	(1~15)
Tamper Alarm Volume	15	(1~15)
Voice Prompt Volume	15	(0~15)

- ❖ Go to Device > Audio and look at Volume Control
- ❖ Adjust volume as needed by entering a volume level between 1 – 15.
- ❖ “Volume Level” will change the overall volume.
 - Level 1 range is 80 – 95
 - Level 2 range is 95 – 109

Upload Custom Audio for Tones

Tone Upload			
(File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16)			
Ringback	Choose File	No file chosen	Upload Delete
Open Door Inside Tone	Choose File	No file chosen	Upload Delete
Open Door Outside Tone	Choose File	No file chosen	Upload Delete
Open Door Failed Tone	Choose File	No file chosen	Upload Delete
Emergency Alarm Tone	Choose File	No file chosen	Upload Delete
Hang Up Tone	Choose File	No file chosen	Upload Delete

- ❖ Go to Device > Audio and look at Tone Upload
- ❖ The requirements your file needs to meet to be uploaded are:
 - File type needs to be WAV
 - Size must be < 200kb
 - Sample Rate 8/16k
 - Bits: 16
- ❖ Click choose file on the one you want to replace with your custom
- ❖ Select the file and click upload
- ❖ Submit

Change LED settings

LED Setting

LED Fill Light

Mode

Auto

Min Photoresistor

1500

(0~1800)

Max Photoresistor

1600

(0~1800)

Light Of The Button

Device Status	Color	Display Mode
Normal	Blue	Always On
OFFLINE	Red	Breathing Light
Calling	Blue	Breathing Light
TALKING	Purple	Always On
RECEIVING	Blue	Breathing Light
Emergency Alarm	Red & Blue	500/500 Blink

Light Of The Card Reader

LED Enabled

☐

Submit

Cancel

- ❖ Go to Device > Light
- ❖ Here you can change the light mode and status colours

Setting up Calls to phone numbers

Basic	
SIP Account	
Status	Unregistered
Account	Account 2 ▼
Account Enabled	☐
Display Label	
Display Name	
Register Name	
Username	
Password	*****

Preferred SIP Server	
Server IP	Port 5060
Registration Period	1800 (30~65535Sec)

Alternate SIP Server	
Server IP	Port 5060
Registration Period	1800 (30~65535Sec)

Rather than calling the Akuvox SIP numbers, you can have the device call phone numbers instead. This will require you to have a **Third-Party SIP** Service like **2Talk**.

You'll need to setup Account 2 with that Third Party SIP account.

- ❖ Go to Account > Basic and look at SIP Account
- ❖ Click the dropdown for Account 1
- ❖ Select Account 2
- ❖ Fill out the details using the Third-Party SIP account details

Save Configuration

- ❖ Go to System > Maintenance and look at Others
- ❖ You import or export a TGZ file with the configurations you made to the device on it. This is helpful for backing up configurations, in case any new changes start causing problems

Others

Config File(.tgz/.conf/.cfg)

Choose File

No file chosen

Export

(Encrypted)

Import

Cancel

Submit

Cancel

Third Party Device Integration

Wiegand

- ❖ Go to Access Control > Card Setting and look at Wiegand

With these settings, it all depends on the third-party device and what requirements it needs. You'll need to play around with the settings to find what works best for both your purpose and system needs.

The following are the available settings in the Wiegand section:

Wiegand

Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	wiegand-26 ▼
Wiegand Transfer Mode	Input ▼
Wiegand Input Data Order	Normal ▼
Wiegand Output Data Order	Normal ▼
Wiegand Output Basic Data Order	Normal ▼
Wiegand Output CRC Enabled	☒

- ❖ **Wiegand Display Mode:** Select the Wiegand card code format from the provided options.
- ❖ **Wiegand Card Reader Mode:** The transmission format should be identical between the door phone and the third-party device.
- ❖ **Wiegand Transfer Mode:**
 - **Input:** The device serves as a receiver.
 - **Output:** The device serves as a sender and can directly output the data, such as a card code.

- **Convert To Card No. Output:** The device serves as a sender and cannot directly output the data.
- ❖ **Wiegand Input Data Order:** Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- ❖ **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
 - For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion (e.g., Wiegand 26). If Reversed is selected, the card data is 0x55 0x44 0x33.
- ❖ **Wiegand Output Basic Data Order:** Set the sequence of the card data before going through Wiegand conversion and outputting the card code.
 - For example, if the card data is 0x11 0x22 0x33 0x44 and the Reversed option is selected, the data will be 0x44 0x33 0x22 0x11.
- ❖ **Wiegand Output CRC Enabled:** It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.

HTTP

- ❖ Go to Security > HTTP API

The HTTP command format depends on the third-party device you use.

The following are the modifiable settings you can change here:

- ❖ **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:** It is Digest by default. 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 the username and password.
- ❖ **Username:** Enter the username for authentication. The default is admin.
- ❖ **Password:** Enter the password for authentication. The default is admin.
- ❖ **1st IP-5th IP:** Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

Authorization Types:

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 the username and password.
Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) in 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.
-------	--

Factory Reset

You can reset the E12 from either the cloud, logging into the E12 or by doing a physical reset.

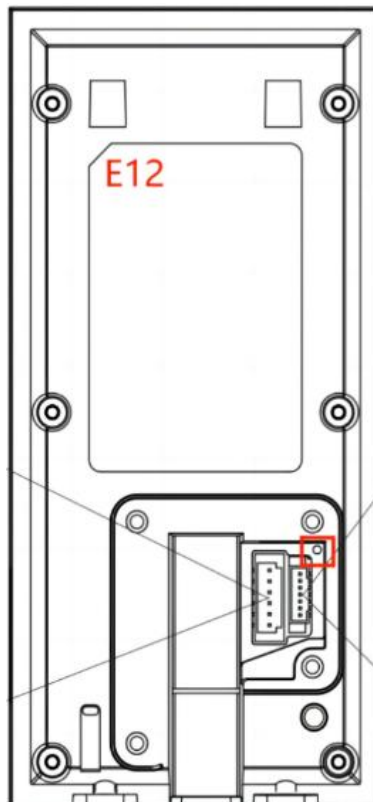
Cloud Reset

- ❖ Navigate to your cloud and find your site
- ❖ Go into the device information of your device
- ❖ Click Settings
- ❖ Click Reset

In the Device Web GUI

- ❖ Log into the E12
- ❖ Go to System > Upgrade
- ❖ Click Reset next to Reset to Factory Setting

Physical Reset



- ❖ Take the back cover off then power it on
- ❖ Insert a PIN in the area marked and hold for 10 seconds
- ❖ The E12 will light up and go into factory reset. After reboot, the LED stays blue

Firmware Upgrade

You'll need to download the firmware from the Akuvox Knowledge site.

1. Go to <https://knowledge.akuvox.com/>
2. Search for the model of device followed by "firmware"
3. Find the article for your model of firmware
4. Download from the link in the firmware (If it asks you which version of firmware, choose Asia)

On the Device:

- ❖ Go to Upgrade > Basic and look at Upgrade
- ❖ Click Choose File and select the firmware upgrade file
- ❖ Then click the Upgrade button.
- ❖ The device will begin upgrading and reboot.