

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



S560

INDOOR MONITOR

Administrator Guide

Thank you for choosing the Akuvox S560 series indoor monitor. This manual is intended for the administrators who need to properly configure the indoor monitor. This manual applies to the 560.30.10.10 version, and it provides all the configurations for the functions and features of the S560 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview















S560 series is a Linux SIP-based indoor device. It can be connected to the Akuvox door phone for audio communication and unlocking and can be deployed and maintained on the SmartPlus platform along with Akuvox door phones and SmartPlus app. It is economical, easy, and simple to use in such scenarios as small and medium-sized apartments.

Model Specifications

Model	S560
Speaker	Main unit: 8Ω1W Earpiece: 32Ω0.25W
MIC	-36dB
Card Reader	NA
Wi-Fi	NA
Bluetooth	NA
RJ45	x1, 10/100Mbps
Indicator light	x1
Power Supply	12VDC/1A or IEEE 802.3af PoE

Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio codecs, DTMF, etc.
- **Network:** This section mainly deals with DHCP & Static IP setting, RTP port setting, device deployment, etc.
- **Phone:** This section includes time and language management, call feature, audio control, light setting, key management, relay control, etc.
- **Contacts:** This section allows the user to check call logs.
- **Upgrade:** This section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.
- **Security:** This section is for password modification, account status & session time-out configuration, as well as high security mode switching.

 Status 	
Basic	Product Information
 Account 	Model
 Network 	Firmware Version
 Phone 	Network Information
 Contacts 	LAN Port Type
 Upgrade 	IP Address
 Security 	Gateway
	Backup DNS
	Account Information
	Account1

Access the Device

Within the same local network, you can enter the device IP address on the web browser to log into the device web interface where you can configure parameters.

Obtain Device IP Address

Note

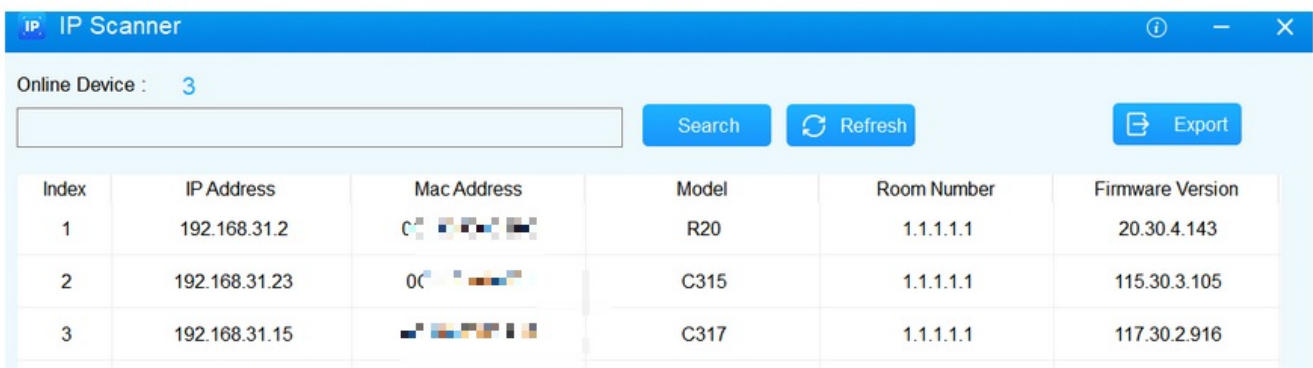
Ensure the device is connected to Ethernet and the handset is linked to the main unit; otherwise, it will be unable to obtain the IP address.

IP Broadcast Automatically

Press the # key for about 5 seconds and the device will automatically broadcast its IP address.

Use IP Scanner

You can use the IP scanner tool to check the device IP on the same local network.



The screenshot shows a web browser window titled "IP Scanner". At the top, it indicates "Online Device : 3". Below this is a search bar and three buttons: "Search", "Refresh", and "Export". The main content is a table with the following data:

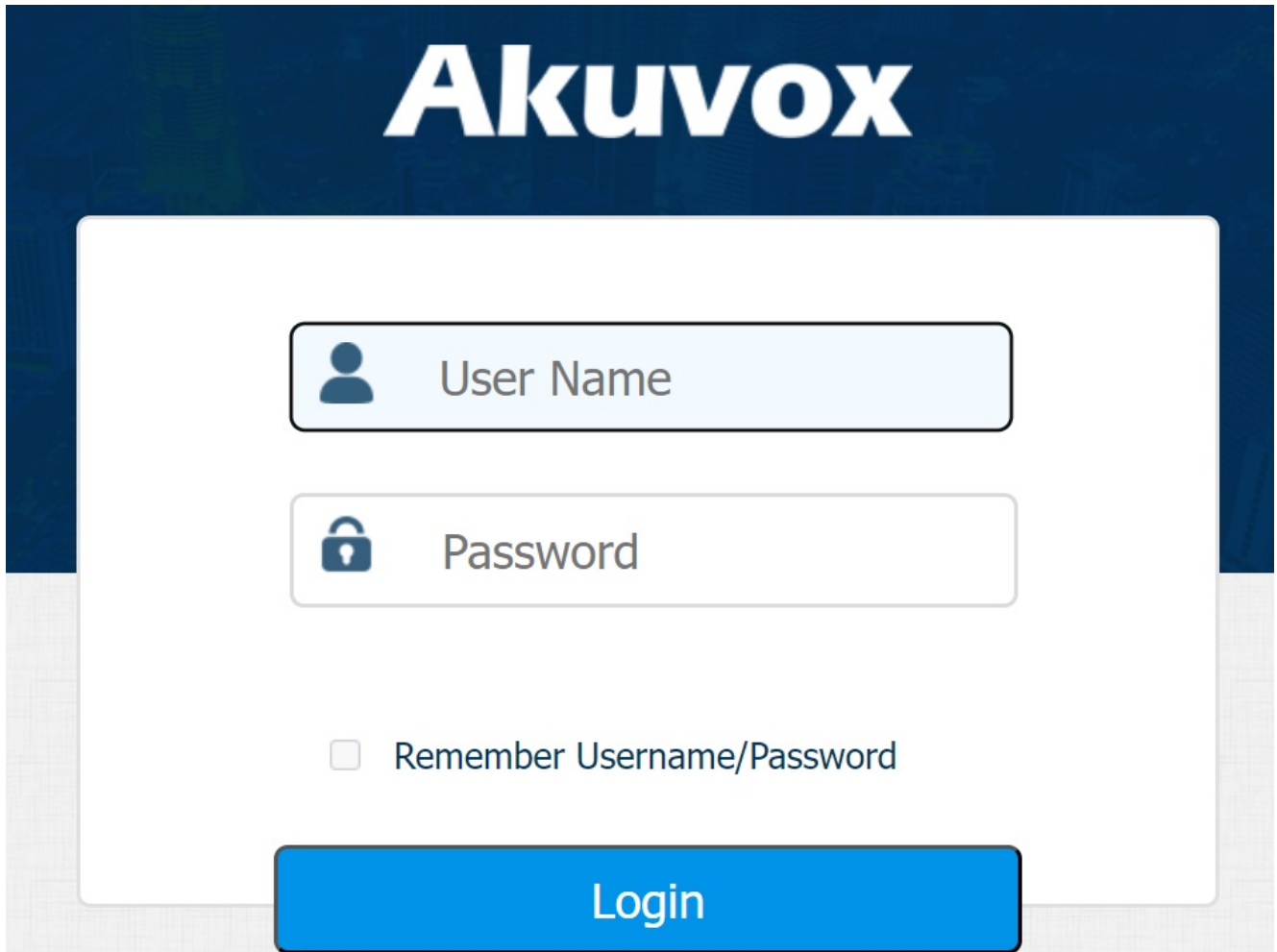
Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.31.2	C8:00:0A:00:00:00	R20	1.1.1.1.1	20.30.4.143
2	192.168.31.23	0C:00:0A:00:00:00	C315	1.1.1.1.1	115.30.3.105
3	192.168.31.15	08:00:0A:00:00:00	C317	1.1.1.1.1	117.30.2.916

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>

Log into the Device Setting Web Interface

To log into the device web interface where you can configure and change parameters, enter the device IP address on the browser. The default user name and password are both **admin**.



The screenshot shows the login page for the Akuvox device web interface. At the top, the 'Akuvox' logo is displayed in white on a dark blue background. Below the logo, there is a white login form with a dark blue border. The form contains two input fields: 'User Name' with a person icon and 'Password' with a lock icon. Below these fields is a checkbox labeled 'Remember Username/Password'. At the bottom of the form is a large blue button labeled 'Login'.

Note

- Google Chrome browser is strongly recommended.
- Please be case-sensitive to the username and password entered.

Language and Time Setting

Language Setting

When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can be set up on the device web interface according to your preference.

Navigate to **Phone > Time/Lang** interface.

Web Language

Type

English

Parameter Set-up:

- **Type:** choose the desired web language from **English, Traditional Chinese, Portuguese, Spanish, German, Polish, Japanese, and Simplified Chinese.** Normally, English is the default web language.

Time Setting

Time setting on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

Navigate to **Phone > Time/Lang** interface.

NTP

Time Zone

GMT+0:00 London

Preferred Server

0.pool.ntp.org

Back Up Server

1.pool.ntp.org

Update Interval

3600

(>= 3600s)

Parameter Set-up:

- **Preferred/Backup Server:** enter the NTP server address. The backup server will take effect when the preferred server is invalid.
- **Update Interval:** to configure the interval between two consecutive NTP requests.

You can also set up time manually on the same interface, select the **Manual** checkbox and input time data.

Time Setting

Manual
 Auto

Date Year Mon Day

Time Hour Min Sec

Daylight Saving Time Setting

Daylight Saving Time is the practice of advancing clocks (typically by one hour) during warmer months so that darkness falls at a later clock time. You can modify the time parameters to achieve longer evenings or daytime, especially in summer.

Go to **Phone > Time/Lang** interface.

Daylight Saving Time

Daylight Saving Tim...

OffSet (-300~300Minutes)

By Date
 By Week

Start Time Mon Day Hour

End Time Mon Day Hour

Start Month Start Week Of Month

Start Day Of Week Start Hour (0~23)

End Month End Week Of Month

End Day Of Week End Hour (0~23)

Parameter Set-up :

- **Enabled:** to enable or disable daylight saving time. You can also configure it to make the device adjust the daylight saving time automatically.
- **Offset:** to set the offset value, it is 60 minutes as default, setting the clocks an hour ahead of the standard time.

Indicator Light Setting

Indicator Light Display Status

The device has an indicator light installed on the top surface. The light colors vary by the state the device is currently in. You can change light colors and states that represent the device status on the **Phone > Display** interface.

Light Settings		
Common	On ▼	Blue ▼
Ringing	Fastblink ▼	Blue ▼
Mic Mute	Slowblink ▼	Purple ▼
Talk/Dial	Slowblink ▼	Blue ▼
Phone Silent	Fastblink ▼	Purple ▼
Network Error	Fastblink ▼	Red ▼
DND	On ▼	Purple ▼
Device Upgrader	On ▼	Red ▼

The default indicator light status:

Color	Indicator Light Status	Color Code
Blue	A solid blue light	Normal status
	A fast blinking blue light	Ringling
	A slowly blinking blue light	During a call or calling
Purple	A solid purple light	Do Not Disturb is on
	A solid purple light	The handle is picked up
	A fast blinking purple light	Mute ringing
	A slowly blinking purple light	Mute MIC
Red	A solid red light	Rebooting or upgrading
	A fast blinking red light	Network error

Note

- The default indicator light priority:

DND > Network error > Mute ringing = Mute MIC > Ringling = During a call = Calling > The handle is picked up = Normal status

- Among the states with the same priority, the indicator light of the latest state will be on.

Sound and Volume Configuration

S560 provides you with various types of ringtones and volume configurations. You can configure them on the device web interface.

Volume Configuration

You can set up volumes on the device **Phone > Audio** interface.

Ring Volume

Volume

10

(0~15)

Talk Volume

Volume

10

(0~15)

Mic Volume

Volume

10

(1~15)



Key Volume

Volume

10

(0~15)

Note

- Ring volume and talk volume can also be adjusted on the device by pressing the  and  buttons.

Upload Tone Files

You can select and upload ringtones on the device **Phone > Audio** interface.

All Ringtones

Upload(Max Size: 25...

Not selected any files

Select File

Submit

Cancel

Ringtones

Ring1.wav

Delete



Note

- The uploaded file should be **.WAV** format within 250K.

Network Setting

Device Network Configuration

You can check the indoor monitor's network connection info and configure the default DHCP mode (Dynamic Host Configuration Protocol) and static IP connection for the device on the device's web interface.

Navigate to **Network > Basic** interface.

LAN Port

<input type="checkbox"/>	DHCP	<input checked="" type="checkbox"/>	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"/>		

Parameter Set-up:

- **DHCP:** DHCP mode is the default network connection. If the DHCP mode is turned on, then the device will be assigned by the DHCP server with IP address, subnet mask, default gateway and DNS server address automatically.
- **Static IP:** when static IP mode is selected, the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your 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 your actual network environment.
- **Default Gateway:** set up the gateway according to the IP address.
- **Preferred/Alternate DNS:** set up preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary one and the device will connect to the alternate server when the primary DNS server is unavailable.

Device Local RTP configuration

For the device network data transmission purpose, the device needs to be set up with a range of RTP ports (**Real-time Transport Protocol**) for establishing an exclusive range of data transmission in the network.

To configure it on the device **Network > Advanced > Local RTP** interface.

Local RTP

Starting RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

Parameters Set-up:

- **Starting RTP Port:** set the minimum start port that RTP stream can use. The default port is 11800.
- **Max RTP Port:** set the maximum end port that RTP stream can use. The default port is 12000.

Device Deployment in Network

Devices should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address, and extension numbers as opposed to other devices for device control and the convenience of the management.

You can do it on the web **Network > Advanced > Connect Setting** interface.

Connect Setting

Connect Mode	SDMC	Discovery Mode	<input type="text" value="Enabled"/>		
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"/>	(1-9)	Device Location	<input type="text" value="Indoor Monitor"/>	

Parameter Set-up:

- **Connect Mode:** it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type, therefore, you are allowed to choose **Cloud** or **SMDC** in discovery mode.

- **Discovery Mode:** select **Enabled** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and select **Disabled** if you want to conceal the device so as not to be discovered by other devices.
- **Device Node:** specify the device address by entering device location information from the left to the right: Community, Unit, Stair, Floor, 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 to distinguish it from other devices.

Intercom Call Configuration

SIP Call

Session Initiation Protocol(SIP) is a signaling transmission protocol used for initiating, maintaining, and terminating calls.

A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Account Registration

Each device needs a SIP account to make and receive SIP calls.

Akuvox intercom devices support the configuration of two SIP accounts, which can be registered under two independent servers.

To configure the SIP account, go to **Account > Basic > SIP Account** interface.

SIP Account			
Status	<input type="text" value="Disabled"/>	Account	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="text" value="Account 1"/>
Account Enabled	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="text" value="Disabled"/>	Display Label	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="text"/>
Display Name	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="text"/>	Register Name	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="text"/>
User Name	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="text"/>	Password	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; padding: 2px 10px;" type="password"/>

Parameter Set-up:

- **Status:** it displays the status of the SIP account.
- **Account:** select Account 1 or Account 2 to make the SIP call. Account 1 is the default option.
- **Account Enabled:** check to activate the registered SIP account.
- **Display Label:** configure the device label to be shown on the device screen.
- **Display Name:** configure the device's name to be shown on the device being called to.

- a. To register SIP account for Akuvox indoor monitors, obtain **Register Name, Username, and Password** from Akuvox indoor monitor PBX screen.
- b. To register SIP account for third-party devices, obtain **Register Name, Username, and Password** from third-party service provider.

SIP Server Configuration

SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

To configure it on the device **Account > Basic > SIP Server 1** interface.

SIP Server 1

SIP Server Address

SIP Server Port

5060

Registration Period

1800

(30~65535s)

Parameter Set-up:

- **SIP Server Address**: enter the server's IP address or its URL.
- **SIP Server Port**: set up SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is 1800, ranging from 30-65535s.

Outbound Proxy Server Configuration

An outbound proxy server receives and forwards all requests the designated server. It is an optional configuration, but if set it up, all future SIP requests get sent there in the first instance.

To configure the outbound proxy server on **Account > Basic > Outbound Proxy Server** interface.

Outbound Proxy Server

Outbound Enabled	<input type="text" value="Disabled"/>		
Preferred Outbound ...	<input type="text"/>	Preferred Outbound ...	<input type="text" value="5060"/>
Backup Outbound Pr...	<input type="text"/>	Backup Outbound Pr...	<input type="text" value="5060"/>

Parameter Set-up:

- **Preferred/Backup Outbound Proxy Server:** set up preferred/backup server IP for the outbound proxy server.
- **Preferred/Backup Outbound Proxy Server Port:** enter the port number to establish a call session via the outbound proxy server or the backup one.

DND

The Do Not Disturb(DND) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

Go to **Phone > Call Feature > DND** interface.

DND

Whole Day	<input type="text" value="Enabled"/>	Return Code When ...	<input type="text" value="486(Busy Here)"/>
Schedule	<input type="text" value="Disabled"/>	DND Start Time	<input type="text" value="00:00"/>
DND End Time	<input type="text" value="00:00"/>		

Parameter Set-up:

- **Whole Day/Schedule:** check **Whole Day** or **Schedule** to enable the DND function. DND function is disabled by default.
- **Schedule:** when **Schedule** is enabled, you can configure DND specific time by selecting the **Start Time** and **End Time**.
- **Return Code When DND:** select what code should be sent to the calling device via the SIP server. 404 for Not found; 480 for Temporarily Unavailable; 486 for Busy Here; 603 for Decline.

Data Transmission Type Configuration

Akuvox intercom devices support four data transmission protocols: **User Datagram Protocol(UDP)**, **Transmission Control Protocol(TCP)**, **Transport Layer Security(TLS)**, and **DNS-SRV**.

To configure it on the device **Account > Basic > Transport Type** interface.

Transport Type

Type

UDP



Parameter Set-up:

- **UDP**: select UDP for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select TCP for reliable but less-efficient transport layer protocol.
- **TLS**: select TLS for secured and reliable transport layer protocol.
- **DNS-SRV**: select DNS-SRV to obtain DNS record for specifying the location of services. And SRV not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

SIP Hacking Protection

Internet phone eavesdropping is a network attack that allows unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls from being compromised on the Internet.

Navigate to **Account > Advanced > Call** interface.

Call

Min Local SIP Port

5062

(1024~65535)

Max Local SIP Port

5062

(1024~65535)

Prevent SIP Hacking

Disabled



Call Setting




Direct IP Call

IP calls and SIP calls can be made directly on the intercom device by entering the IP number on the device.

Press Button to Make a Call

You can quickly make a call with the preset number by pressing  on the device.

To set up the feature on the device **Phone > Function Key** interface.

Function Key		
Key	Type	Value
DSS Key A	Call Manager 	<input type="text"/>
DSS Key B	NA 	<input type="text"/>
DSS Key OpenDoor	NA 	<input type="text"/>

Parameter Set-up:

- **Type:** in DDS Key A or DDS Key B field, select **Call Manager** from **NA, Unlock, Action URL, Transfer, and Call Manager**.
- **Value:** when **Call Manager** is selected, enter the desired SIP/IP number you want to call.

Speed Dial

Speed dial is a function that allows you to make speedy calls by long pressing the specific tabs without entering any dial numbers.

To set up speed dial on the device **Phone > Function Key > Speed Dial List** interface.

Speed Dial List(Long Press To Dial)

Key	Name	Value
DSS Key 1	<input type="text"/>	<input type="text"/>
DSS Key 2	<input type="text"/>	<input type="text"/>
DSS Key 3	<input type="text"/>	<input type="text"/>
DSS Key 4	<input type="text"/>	<input type="text"/>

Parameter Set-up:

- **Key:** each DDS Key corresponds to the numeric key on the device from 1-9.
- **Name:** name the key. It supports up to 63 bytes.
- **Value:** enter the device SIP/IP number to be called.

Call Forwarding

Call Forward is a feature used to redirect an incoming call to a specific third party. Users can redirect the incoming call based on different scenarios. Typically, call forward has three modes: **Always Forward/ No Answer Forward/Busy Forward**.

To set up the function on web Phone > Call Feature > Forward Transfer interface.


Forward Transfer

Account	<input type="text" value="Account 1"/>		
Always Forward	<input type="text" value="Disabled"/>	Target Number	<input type="text"/>
Busy Forward	<input type="text" value="Disabled"/>	Target Number	<input type="text"/>
No Answer Forward	<input type="text" value="Disabled"/>	Target Number	<input type="text"/>
No Answer Ring Tim...	<input type="text" value="30"/>		



Parameter Set-up:

- **Account:** to choose from **Direct IP, Account 1** or **Account 2** to implement the call forwarding feature.
- **Always Forward:** all incoming calls will be automatically forwarded to a specific number.
- **Busy Forward:** incoming calls will be forwarded to a specific number if the device is busy.

- **No Answer Forward:** incoming calls will be forwarded to a specific number if the device is not picked up within no answer ring time.
- **Target Number:** to enter the specific forward number if the indoor monitor enables **Always Forward / Busy Forward / No Answer Forward**.
- **No Answer Ring Time (Sec):** to set no answer time interval from 0-120 seconds before the call is transferred to a designated number.

You can also press  to transfer a call to a designated number. To set it up on the **Phone > Function Key** interface.

Function Key

Key	Type	Value
DSS Key A	Call Manager 	<input type="text"/>
DSS Key B	Transfer 	<input type="text"/>

Parameter Set-up:

- **Type:** in DDS Key A or DDS Key B field, select **Transfer** from **NA, Unlock, Action URL, Transfer, and Call Manager**.
- **Value:** when transfer is selected, enter the transfer SIP number.

Multicast

Multicast is a one-to-many communication within a range. The device can act as a listener and receive audio from the broadcasting source.

Go to the web **Phone > Multicast** interface.

Multicast Setting

Multicast Group ▼

Multicast List

Multicast Group	Multicast Address
Multicast Group 1	<input type="text" value="224.1.6.11:51230"/>
Multicast Group 2	<input type="text" value="224.1.6.11:51231"/>
Multicast Group 3	<input type="text" value="224.1.6.11:51232"/>

Listen List

Listen Group	Listen Address	Label
Listen Group 1	<input type="text"/>	<input type="text"/>
Listen Group 2	<input type="text"/>	<input type="text"/>
Listen Group 3	<input type="text"/>	<input type="text"/>

Parameter Set-up:

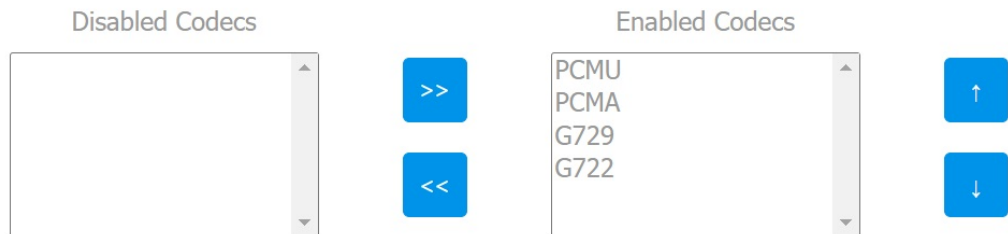
- **Multicast Group:** set the device in one of the groups or disable this function.
- **Multicast List:** to fill in the parameters of the multicast group. Indoor monitor will establish multicast calls to other indoor monitors which are set in the multicast group.
- **Listen List:** to fill in the parameters of listen group. Indoor monitor will receive multicast calls if some indoor monitors call the listening group.
- **Label:** to show the label name on the calling interface if users establish all calls.

Audio Codec Configuration

The device supports four types of Codec (PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To do the configuration on web **Account > Advanced > Audio Codecs** interface.

Audio Codecs



Please refer to the bandwidth consumption and sample rate for the codec types below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz

Door Access Control Configuration

Remote Relay Switch Setting

You can use the unlock tab during the call to open the door. And you are required to set up the same DTMF code in the door phone and indoor monitor.

Go to the web Phone > Relay > Remote Relay interface.

Remote Relay

DTMF Code1

#

DTMF Code2

#

DTMF Code3

#

Parameter Set-up:

- **DTMF Code:** to set the DTMF code for the remote relay, which is # by default.

Web Relay Setting

A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.



To do this configuration on web Phone > Relay > WebRelay Setting interface. IP Address, User Name and Password are provided by the web relay manufacturer.

WebRelay Setting

IP Address UserName

Password

WebRelay Action Setting

ActionId	IP	SIP	WebRelay Action
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>

Parameter Set-up:

- **Password:** the passwords are authenticated via HTTP and you can define the passwords using HTTP get in Action.
- **IP/SIP:** the relay extension information, which can be an IP address or SIP account of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device. This setting is optional.
- **Web Relay Action:** the specific web relay action command provided by the web manufacturer for different actions by the web relay. The example format: **state.xml?relayState=2.**

-If you have not entered the IP address, username, and password, you need to enter the complete HTTP command in such a format: **http://Username:Password@IP address/state.xml?relayState=2.**

Door Unlock Configuration

Door Unlock by DTMF Code

In order to achieve door access via DTMF code or some other applications, you are required to properly configure DTMF in order to establish a DTMF-based data transmission between the door phone and other intercom devices for third-party integration.

Go to **Account > Advanced > DTMF** interface.

DTMF

Type

RFC2833

DTMF Code Transpo...

Disabled

DTMF Payload

101

(96~127)

Parameter Set-up:

- **Type:** select DTMF type among **RFC2833**, **Info**, and **Info+RFC2833** according to your need.
- **DTMF Code Transport Format:** select it only when the third-party device that receives the DTMF code adopts Info transport format. Info transfers the DTMF code via signaling while other transport format does it via RTP audio packet transmission. You can select the DTMF transferring format according to the third-party device. For example, select Telephone-Event if the third-party device adopts the telephone-event. Select among four options: **Disabled**, **DTMF**, **DTMF-Relay**, and **Telephone-Event** according to your need.
- **Payload:** select payload 96-127 for data transmission identification.

Door Unlock via HTTP Command

You can unlock the door remotely without approaching the device physically for door access by typing the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for door access.

To do this configuration on web **Phone > Relay > Remote Relay by HTTP** or **HTTPs** interface.

Remote Relay By HTTP or HTTPS

Index	IP/SIP	Remote Relay IP	UserName	Door Num
<input type="checkbox"/> 1				
<input type="checkbox"/> 2				
<input type="checkbox"/> 3				
<input type="checkbox"/> 4				
<input type="checkbox"/> 5				

1/1

IP/SIP Remote Relay IP
 UserName Password
 Door Num 1 2 3 4

Parameter Set-up:

- **IP/SIP**: enter IP address or SIP account to trigger a certain remote relay of doorphone by sending HTTP message.
- **Username**: enter the device username to be used as a part of HTTP command to trigger the relay.
- **Password**: enter the device password to be used as part of HTTP command to trigger the relay.
- **Door Num**: it refers to the relay number.
Please refer to the following example: `http://192.168.35.127/cgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1`
- **Remote Relay IP**: enter the IP address of the device to be unlocked.

HTTP or HTTPS Command Import/Export

You can import and export HTTP or HTTPS commands on the device **Phone > Relay > Remote Relay by HTTP or HTTPS** interface.

HTTP or HTTPS Command Import/Export

Import(.xml)

Export

Unlock Key Configuration

You can also set the DDS keys as the unlock key and select the desired relay trigger type. To set it up on the **Phone > Function Key** interface.

Function Key

Key	Type	Value
DSS Key A	Unlock ▼	Remote Relay By HTTP ▼
DSS Key B	Unlock ▼	Remote Relay By HTTP ▼
DSS Key OpenDoor	Unlock ▼	Remote Relay By HTTP1 ▼

Parameter Set-up:

- **Type:** select **Unlock**.
- **Value:** select the relay trigger type (Remote Relay By HTTP, Remote Relay By DTMF 1-3, and Web Relay for DSS Key A/B; Remote Relay By HTTP 1-5 for DSS Key OpenDoor).

Security

Voice Encryption

The encryption function provides you with greater security for the intercom call. And Akuvox indoor monitors support three modes of voice encryption: **SRTP(Compulsory)**, **SRTP(Optional)**, **ZRTP(Optional)**.

To configure this feature on web **Account > Advanced > Encryption** interface.

Encryption

Voice Encryption(SR...

Disabled



Parameter Set-up:

- **Voice Encryption(SRTP):** select encryption mode from four options. If you select to disable it, the call will not be encrypted. **SRTP(Compulsory)**, all audio signals (technically speaking, it is RTP streams) will be encrypted to improve security. **SRTP(Optional)**, encrypts voice from the called party, if the called party also enables SRTP, the voice signals will also be encrypted. **ZRTP(Optional)** is the protocol that the two parties use to negotiate the SRTP session key.

Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation.

To configure it on the web **Security > Basic** interface.

Session Time Out

Session Time Out Va...

8000

(60~14400s)

Parameter Set-up:

- **Session Time Out Value:** set the automatic web interface log-out timing ranging from 60

seconds to 14400 seconds. The default value is 300.

Action URL

The device allows you to set up specific HTTP URL commands that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occur any changes in the relay status, input status, and PIN code for security purposes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Make Call	\$remote	Http://server ip/ Callnumber=\$remote
2	Hang Up	\$remote	Http://server ip/ Callnumber=\$remote
3	Relay Triggered	\$relay1status	Http://server ip/ relaytrigger=\$relay1status
4	Relay Closed	\$relay1status	Http://server ip/ relayclose=\$relay1status
5	Input Triggered	\$input1status	Http://server ip/ inputtrigger=\$input1status
6	Input Closed	\$input1status	Http://server ip/ inputclose=\$input1status
7	Valid Code Entered	\$code	Http://server ip/ validcode=\$code
8	Invalid Code Entered	\$code	Http://server ip/ invalidcode=\$code
9	Valid Card Entered	\$card_sn	Http://server ip/ validcard=\$card_sn
10	Invalid Car Entered	\$card_sn	Http://server ip/ invalidcard=\$card_sn
11	Tamper Alarm Triggered	\$alarm status	Http://server ip/tampertrigger=\$alarm status

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

[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)

To configure it on the **Phone > Function Key** interface.

Function Key

Key	Type	Value
DSS Key A	Action URL ▼	<input type="text"/>
DSS Key B	NA ▼	<input type="text"/>
DSS Key OpenDoor	NA ▼	<input type="text"/>

Parameter Set-up:

- **Type:** select Action URL.
- **Value:** enter the HTTP command triggered by pressing the corresponding key.

High Security Mode

High security mode is designed to enhance the security, for example, it optimizes the password storage method.

Please note that once the mode is enabled, it is not allowed to downgrade the device from the version with the mode to an old one without it.

To configure it on the device **Security > Basic** interface.

High Security Mode

Enable

Disabled ▼

Important Notes

1. This mode is disabled by default when the device is upgraded to a new version with high security from an older version without the mode. However, if the device is reset to its factory settings, the mode is enabled by default.

2. Enabling this mode will make the old version tools unusable. To continue using them, you must upgrade them to the following versions.

- PC Manager: 1.2.0.0
- IP Scanner: 2.2.0.0
- Upgrade Tool: 4.1.0.0
- SDMC: 6.0.0.34

3. The supported HTTP format varies depending on whether high secure mode is enabled or disabled.

- When the mode is turned on, the device only supports new HTTP formats for door opening.
 - `http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1`
 - `http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1`
- When the mode is off, the device supports the above two new formats as well as the old one:
 - `http://deviceIP/fcgi/do? action=OpenDoor&UserName=username&Password=password&DoorNum=1`

4. It is not allowed to import/export tgz. format configuration files between a new version device and an old version device without high security mode.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Navigate to **Upgrade > Basic** interface and click **Select File**.

Firmware Version	560.30.10.10	Hardware Version	560.0.0.0.0.0.0
Upgrade	<input type="text" value="Not selected any files"/> <input type="button" value="Select File"/>	<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Submit"/>		
Reboot	<input type="button" value="Submit"/>		

Note

- The file uploaded should be in **.rom** format.

Backup

You can import or export encrypted configuration files to your Local PC.

Go to **Upgrade > Advanced > Others** interface if needed.

Others

Config File(.tgz/.con...

Not selected any files

Select File

 Export

(Encrypted)

 Import

 Cancel

Note

- The file imported should be in .tgz, .conf, or .cfg format.

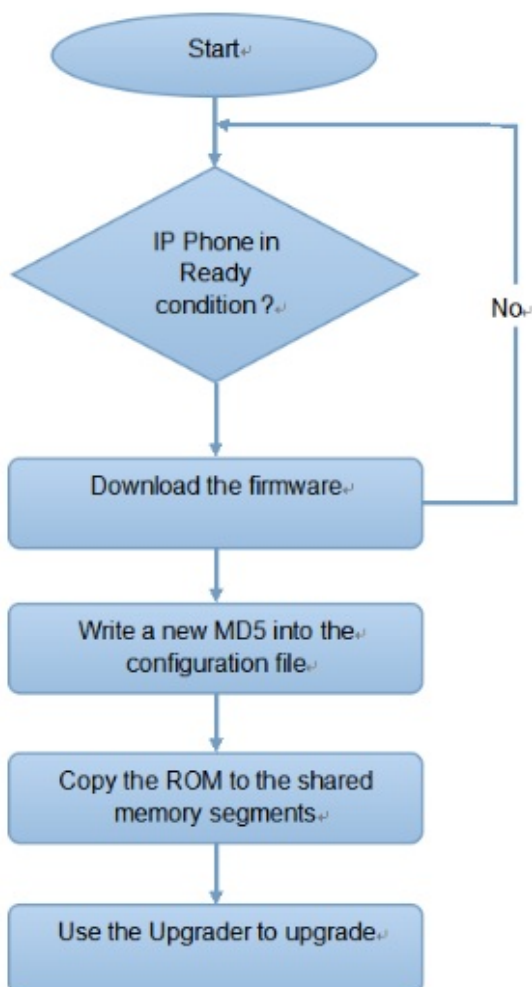
Auto-provisioning via Configuration File

You can configure and upgrade the door phone 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 on the door phone.

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:



Introduction to the Configuration Files for Auto-Provisioning

Configuration files have two formats for auto-provisioning. One is the general configuration files used for the general provisioning and another one is the MAC-based configuration provisioning.

The difference between the two types of configuration files:

- **General configuration provisioning:** a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example, cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files are used for auto-provisioning on a specific device as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

You may click [here](#) to see the detailed format and steps.

Autop Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself according to the schedule.

To set up the schedule on device web **Upgrade > Advanced > Automatic Autop** interface.

Automatic Autop

Mode

Power On ▼

Schedule

Sunday ▼

22

(0~23Hour)

0

(0~59Min)

Parameter Set-up:

- **Mode:**

- **Power On:** select Power on, if you want the device to perform Autop every time it boots up.
- **Repeatedly:** select Repeatedly, if you want the device to perform autop according to the schedule you set up.
- **Power On + Repeatedly:** select Power On + Repeatedly if you want to combine Power On mode and Repeatedly mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
- **Hourly Repeat:** select Hourly Repeat if you want the device to perform Autop every hour.

Static Provisioning Configuration

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

Navigate to **Upgrade > Advanced** 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 Templ...	<input type="button" value="Export"/>

Manual Autop

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

Parameter Set-up:

- **URL:** set up TFTP, HTTP, HTTPS, FTP server address for the provisioning.
- **User Name:** set up the user name if the server needs a user name to be accessed to.
- **Password:** set up the password if the server needs a password to be accessed to.
- **Common AES Key:** set up AES code for the intercom to decipher general auto provisioning configuration file.
- **AES Key (MAC):** set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Tip

- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.

Note

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

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.

To enable it on the web **Upgrade > Advanced** interface.

PNP Option

PNP Config Enabled

Enabled



Call Log

If you want to check on the calls inclusive of the dial-out calls, received calls, missed calls, and forwarded calls in a certain period, you can check and search the call log on the device web interface and export the call log from the device if needed.

Navigate to **Contacts > Call Log** interface.

Call History All ▼ Export

<input type="checkbox"/> Index	Type	Date	Time	Local Identity	Name	Number
<input type="checkbox"/> 1	Dialed	1970-01-01	00:01:47	192.168.36.1 06@192.168.3 6.106	192.168.88.99	192.168.88.9 9@192.168.88 .99

Debug

System Log for Debugging

System logs can be used for debugging purposes.

You can set up the function on the web **Upgrade > Advanced > System Log** interface.

System Log

LogLevel	<input type="text" value="3"/>	
Export Log	<input type="button" value="Export"/>	
Remote System Log ...	<input type="text" value="Disabled"/>	Remote System Serv... <input type="text"/>

Parameter Set-up:

- **Log Level:** select log levels from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** click the **Export** tab to export temporary debug log file to a local PC.
- **Remote System Log Enabled:** enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the system log and the remote server address will be provided by Akuvox technical support.

PCAP for Debugging

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

You can set up the function on the web **Upgrade > Advanced > PCAP** interface.

PCAP

PCAP Specific Port

PCAP

Start

Stop

Export

PCAP Auto Refresh

Disabled



Parameter Set-up:

- **PCAP Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank.
- **PCAP:** click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** If you set it as **Enabled**, then the PCAP will continue to capture data packets even after the data packets reach their 50M maximum in capacity. If you set it as **Disabled**, the PCAP will stop data packet capturing when the data packets captured reach the maximum capturing capacity of 1MB.

User Agent

User agent is used for identification purpose when you are analyzing the SIP data packet.

To do this configuration on web **Account > Advanced** interface.

User Agent

User Agent

Password Modification

Modify Device Web Interface Password

To modify web interface password, you can do it on device web interface. Select **admin** for the administrator account and **user** for the user Account. Click the **Change Password** tab to change the password.

Go to **Security > Basic** interface.

Web Password Modify

User Name ▼

Change Password

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

User Name	admin
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

You can also enable the **User** account on the same interface.

Account Status

Admin

Enabled



User

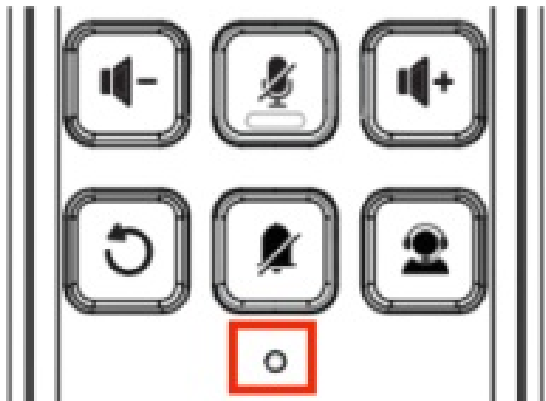
Disabled



System Reboot & Reset

Reboot

You can reboot the device by inserting a pin into the reset hole and holding it for three seconds.



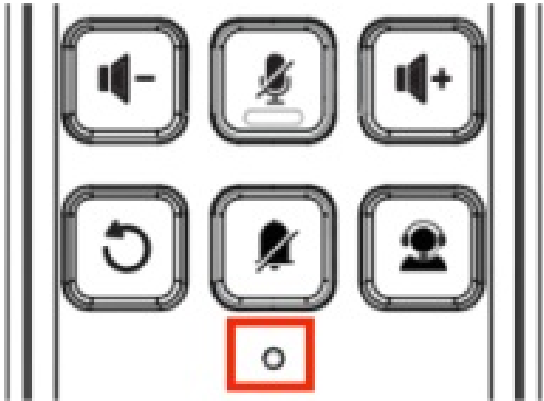
You can also operate it on the device web interface.

Navigate to **Upgrade > Basic** interface.

Firmware Version	560.30.10.10	Hardware Version	560.0.0.0.0.0.0
Upgrade	<input type="text" value="Not selected any files"/> <input type="button" value="Select File"/>	<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Submit"/>		
Reboot	<input type="button" value="Submit"/>		

Reset

You can reset the device by by inserting a pin into the reset hole and holding it for no more than three seconds.



The device system can also be reset on device web interface without approaching the device. Go to **Upgrade > Basic** interface.

Firmware Version	560.30.10.10	Hardware Version	560.0.0.0.0.0.0.0
Upgrade	<input type="text" value="Not selected any files"/> Select File	Submit	Cancel
Reset To Factory Setting	Submit		
Reboot	Submit		