- **Parity Check(Odd)**: When enabled, the sum of selected bits must be odd to pass verification. For example, when the second and third bits are selected and their sum is odd, the parity check passes.

Tip

- Parity check is a simple error detection mechanism used to ensure that data has not been corrupted during transmission or storage.
- When it is enabled, the device will first perform the check. Only if the check passes will it read the card number.
- Card Reading Example:
  Suppose total number of bits is 32 and the card data is 0011 1000 0101 1100 0010 0100 0011 1110.

Display Mode	Card Number Length	Site Code	Parity Check
HEX: 385C243E	13-32 Bits: C243E	1-12 Bits: 385	• 2-15 bits(Even): The su is 7, fail to pass the check. • 16-31 bits(Odd): The s is 7, successfully pass the check.

- **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 Clear Time**: When the interval of entering passwords via Wiegand exceeds the time, all entered passwords will be cleared.
- **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 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 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 CRC**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **Wiegand Open Relay**: Select the relay triggered by Wiegand.

When the door phone is in Wiegand output mode, you can configure the Wiegand PIN code output format that determines how data is transmitted. The format should be the same as that of the third-party device.

- **PIN**:
  - **8 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 8 bits, "11100001".
  - **4 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 4 bit,s "0001".
  - **All at once**: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode.

Integration via HTTP API

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

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

- **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**: See the description for each option in the chart below.
- **Username**: Enter the user name 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.

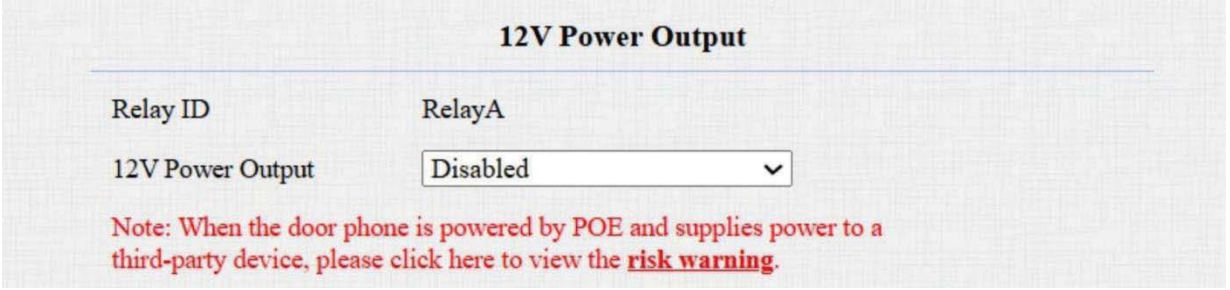
Please refer to the following description for the authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	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 whitelist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required 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 of username and password.
5	Digest	The password encryption method only supports MD5(Message-Digest Algorithm). In the Authorization field of the Http request header:WWW-Authenticate: Digest realm="HTTP API", qop="auth,auth-int", nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

Power Output Control

The device can serve as a power supply for the external relays.

To set it up, go to the **Access Control > Relay > 12V Power Output** interface.



- **12V Power Output**: To supply power for third-party devices, the door phone should be powered by a PoE or DC power connector with input not less than 12V/1.2A.
  - **Disabled**: Turn off the function.
  - **Always**: Provide continuous power.
  - **Triggered by Open Relay**: Provide power to the third-party device when Relay A is triggered via its NO and GND ports. Stop providing the power when Relay A is reset.

- **Timeout(Sec)**: Set the time(3, 5, or 10 seconds) to provide power when **Triggered by Open Relay** is selected.

Note

When the door phone is powered by PoE, its **volume adjustment** affects power supply.

- If the third-party device operates at 12V and ≤0.2A, the door phone supports both Level 1 and 2 volume.
- If the device operates at 12V and 0.2A–0.4A, only Level 1 is supported; Level 2 may cause a shutdown.
- If the device exceeds 0.4A at 12V, it will shut down due to insufficient power.

Integration via RS485

You can connect the device to an external device such as SR01 or an OSDP-based card reader via RS485. To make the connection effective, you need to select the right RS485 mode.

Click here to view the detailed configuration of the OSDP feature.

To set it up, go to the **Device > RS485** interface.

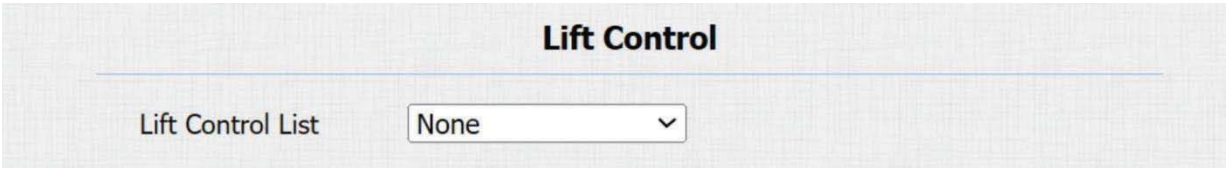
- **Disabled**: The RS485 function is disabled.
- **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **SCBK Value**: Secure Communication Key Value.
    - When it is filled, OSDP will use this value for encryption, employing a customized protocol for communication.
    - When it is left empty, OSDP will use the default encrypted protocol for communication.
- **Others**: Select this option when the device works with the SR01 or other non-OSDP-based devices.

Lift Control

The device can be connected to the Akuvox lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through various types of access methods on the device.

Click here to watch a demonstration video of configuring the lift control feature.

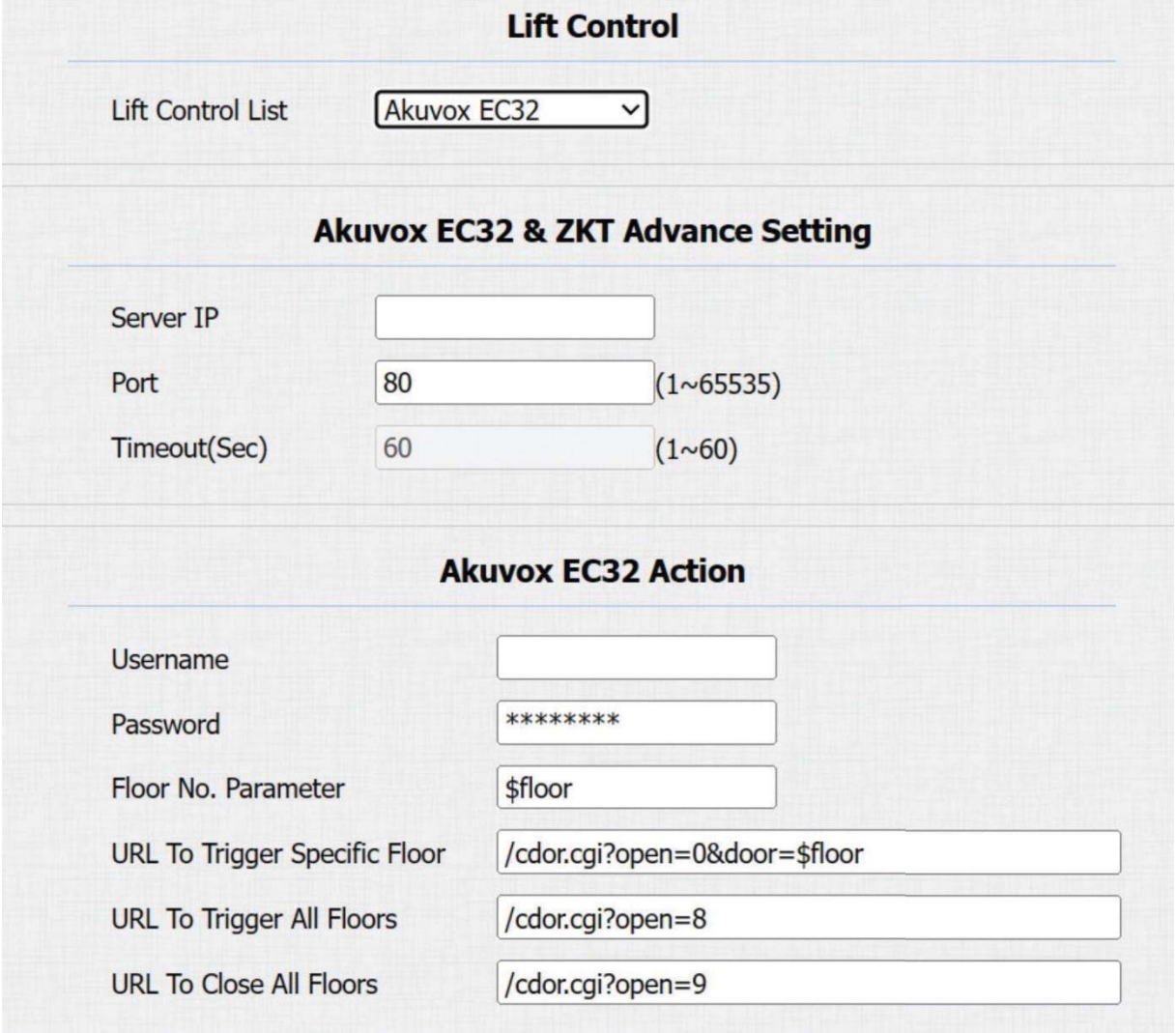
To set it up, go to the **Device > Lift Control** interface.



- **Lift Control List:** Select the lift controller brand.
  - None: The integration will be disabled.
  - Chiyu: Integrate with Chiyu lift controller.
  - KeyKing: Integrate with KeyKing lift controller.
  - Akuvox EC32: Connect the device with the Akuvox EC33 lift controller.
  - ZKT: Integrate with ZKTeco lift controller.

Akuvox Lift Controller

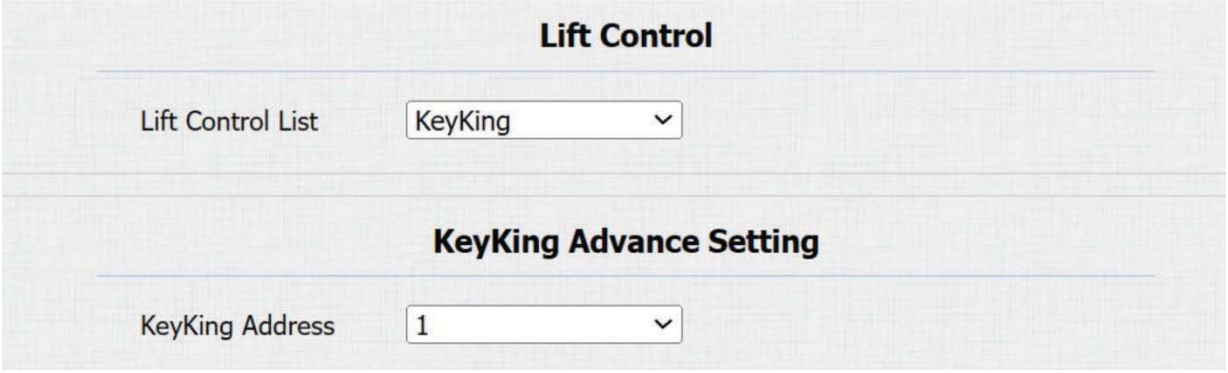
After selecting Akuvox EC32 in the Lift Control List, you need to set up relevant parameters.



- **Server IP:** Enter the IP address of the Akuvox lift controller.
- **Port:** Enter the port of the Akuvox lift controller.
- **Timeout(Sec):** Decide the time limit within which users should press the lift button of their desired floors.
- **Username:** Enter the user name set in the lift controller.
- **Password:** Enter the password set in the lift controller.
- **Floor NO. Parameter:** The floor number parameter is provided by Akuvox. The default is **$floor**. You can define your parameter string.
- **URL To Trigger Specific Floor:** The Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string $floor at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors:** The Akuvox URL for triggering all floors.
- **URL To Close All Floors:** The Akuvox URL for closing all floors.

KeyKing Lift Controller

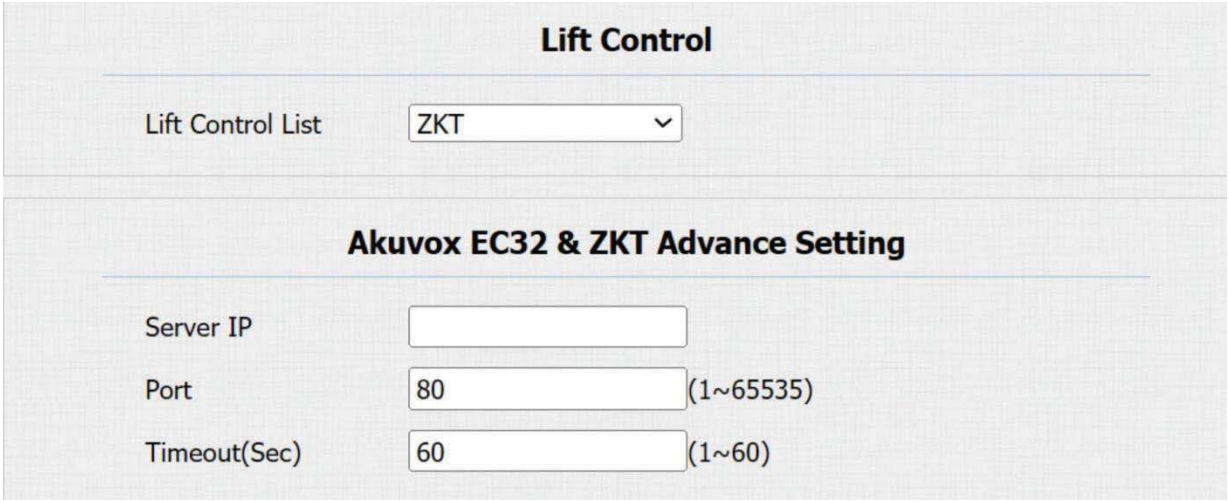
After selecting KeyKing, you need to set the KeyKing address.



- **KeyKing Advance Setting**: Select the number from 0 to 126. The binary number converted from the address number corresponds to the dip switch on the lift board. For example, if you select 5, set the dip switch to 101000.

ZKT Lift Controller

After selecting ZKT, you need to set up relevant parameters.

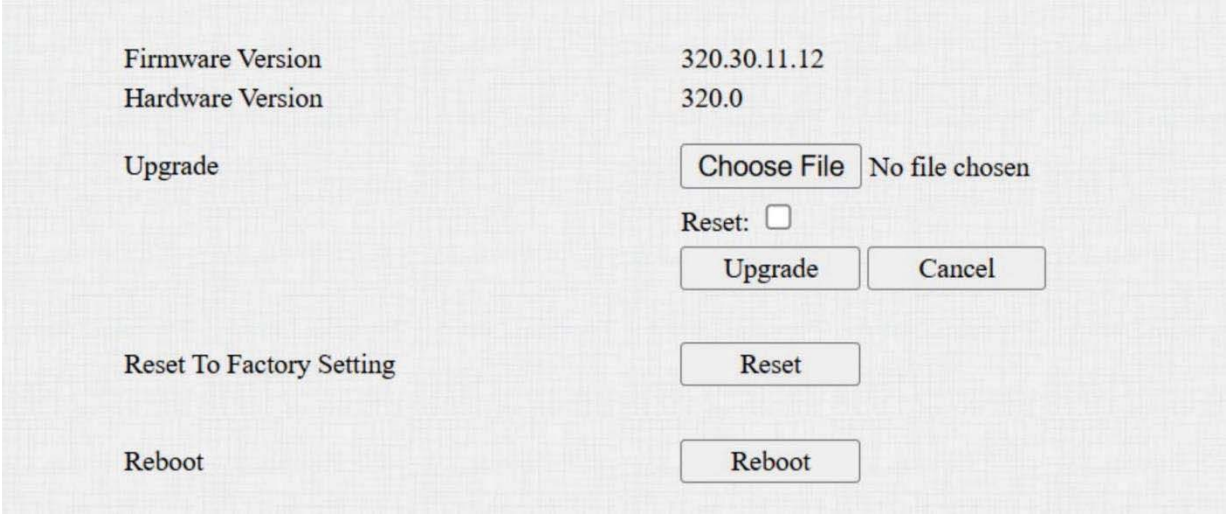


- **Server IP:** Enter the IP address of the controller server.
- **Port:** Enter the port of the controller server.
- **Timeout(Sec):** Decide the time limit within which users should press the lift button of their desired floors.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Note

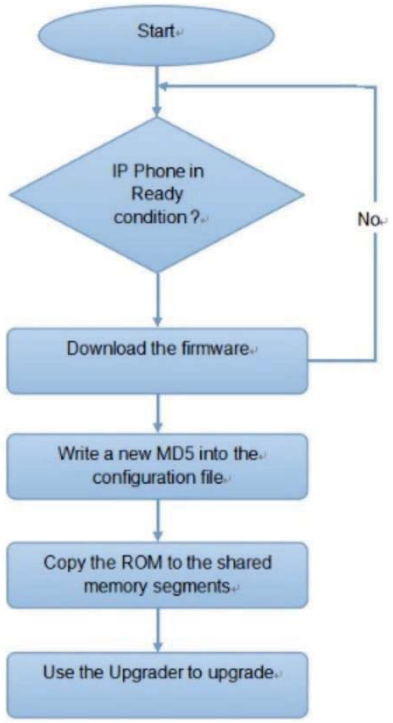
- The upgrade file should be in .rom format.
- Click **here** to download the latest firmware and check new features.

Auto-provisioning

Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade devices in batch via third-party servers. **DHCP, PNP, TFTP, FTP, and HTTPS** are the protocols used by the Akuvox devices to access the URL of the address of the third-party server which stores configuration files and firmware, which will then be used to update the firmware and the corresponding parameters on the device.

Please see the flow chart below:



Configuration Files for Auto-provisioning

Configuration files for auto-provisioning come in two formats: general configuration files and MAC-based configuration files.

Differences:

- **General Configuration Provisioning**:

A general configuration file is stored on a server, allowing all related devices to download the same file to update parameters.

- **MAC-Based Configuration Provisioning**:

MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

Note

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

You may click **here** to see the detailed format and steps.

AutoP Schedule

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

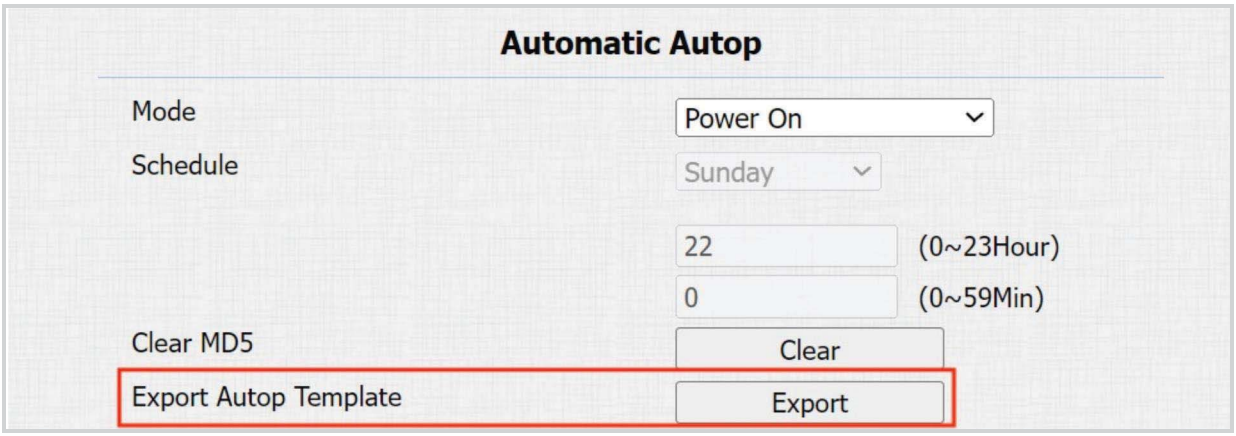
To set it up, go to **System > Auto Provisioning** interface.

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

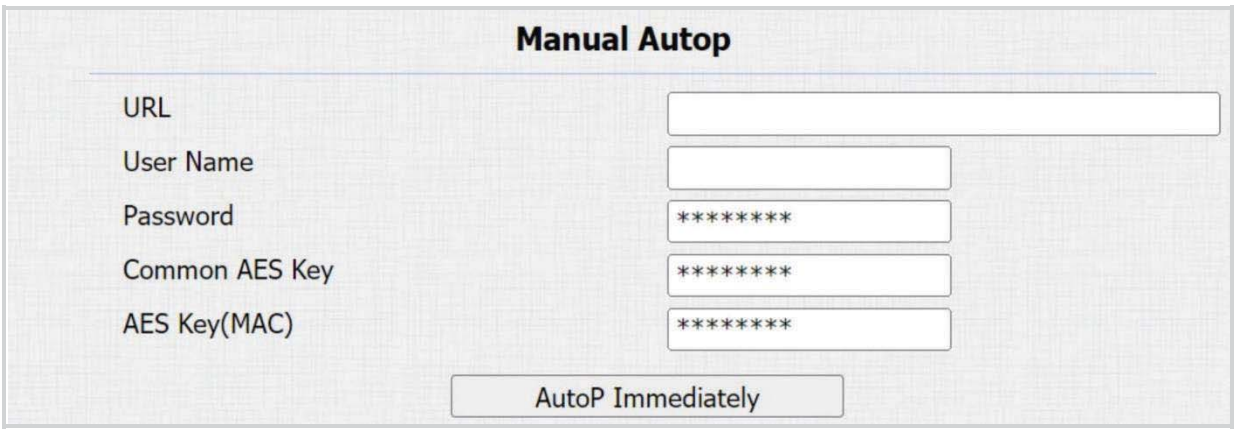
Static Provisioning

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

To set it up, download the template on **System > Auto Provisioning** interface first.



Set up the Autop server in the **Manual Autop** section.



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **User Name**: Enter the username if the server needs a username to be accessed.
- **Password**: Enter the password if the server needs a password to be accessed.
- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop configuration file.

Note

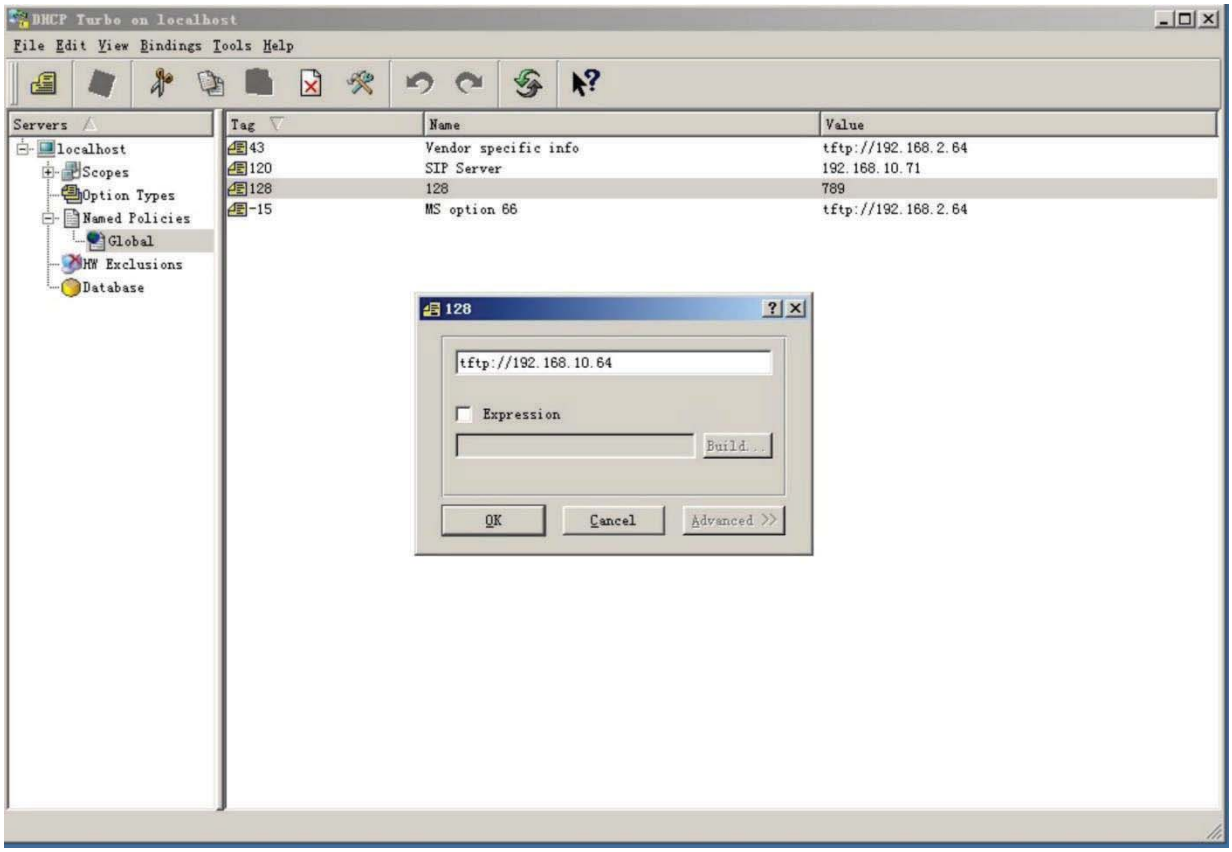
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use the default port 80)
    http://192.168.0.19:8080/(use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/(use the default port 443)

Tip

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

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.

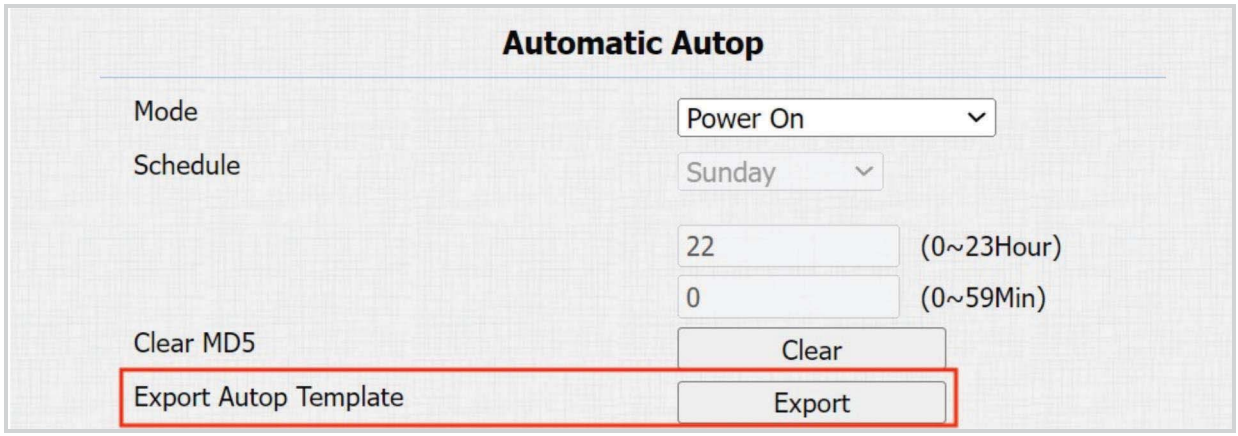


Note

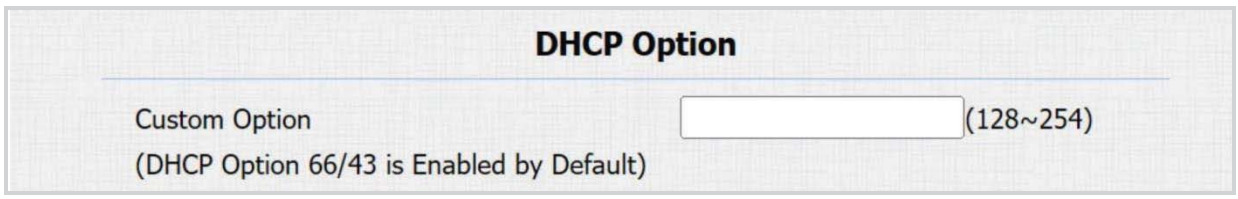
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

Go to **System > Auto Provisioning** interface.



To set up the DHCP Option, scroll to the **DHCP Option** section.



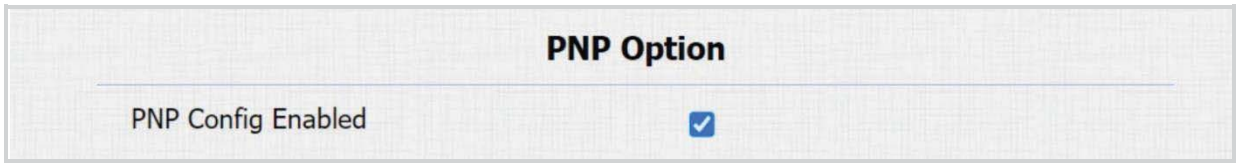
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done 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 upgrade server URL in it.
- **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 upgrade server URL in it.

PNP Configuration

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

Click here to watch the configuration video.

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

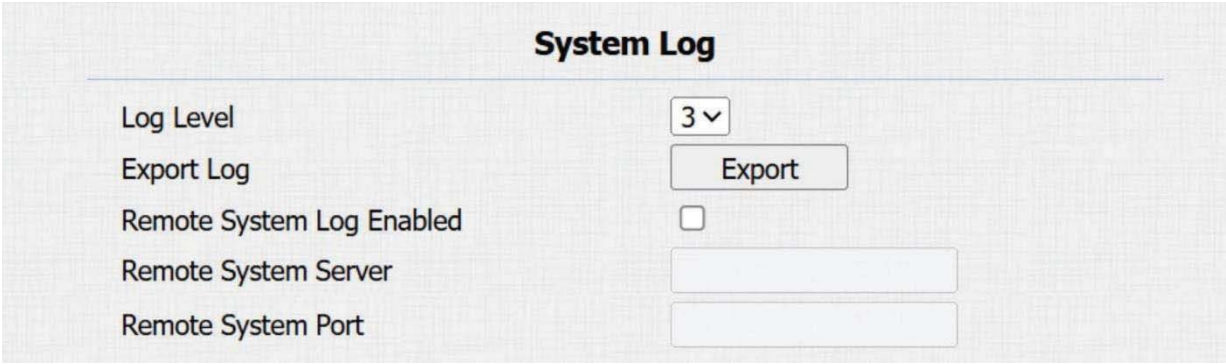


Debug

System Log

System logs can be used for debugging purposes.

Set the system log on the **System > Maintenance > System Log** interface.

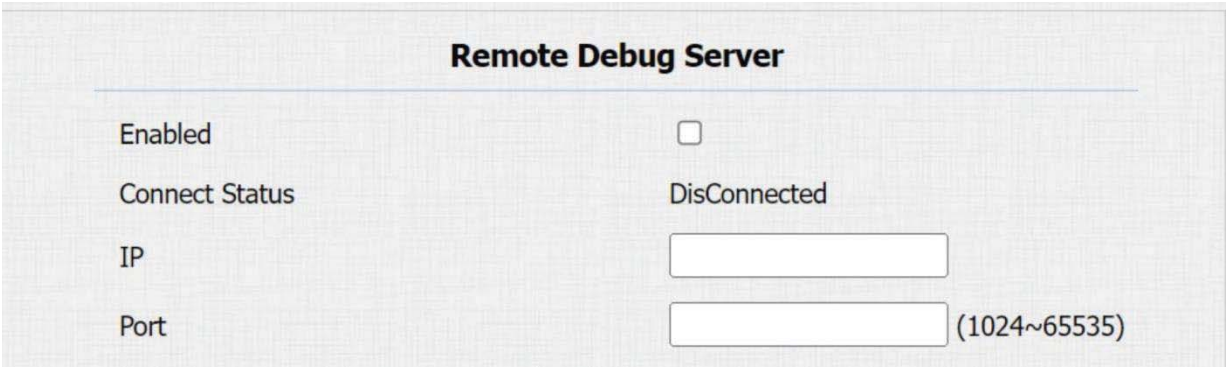


- **Log Level:** Select log levels from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export a temporary debug log file to a local PC.
- **Remote System Server:** Set the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.
- **Remote System Port**: Set the remote system server's port.

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.

To set it up, go to the **System > Maintenance > Remote Debug Server** interface.

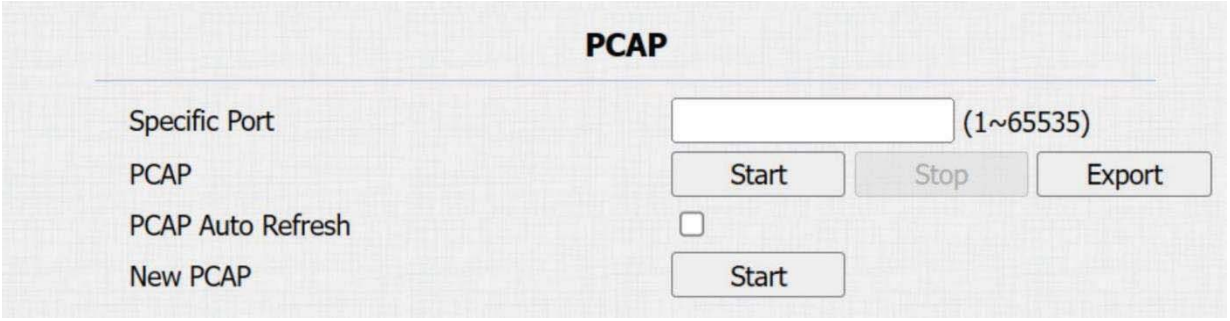


- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.
- **Port**: Enter the port of the server.

PCAP

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

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



- **Specific Port:** Select the specific port from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.
- **New PCAP:** Click Start to capture a bigger data package.

Web Call

The web call feature allows for making calls via the device's web interface, commonly used for remote call testing purposes.

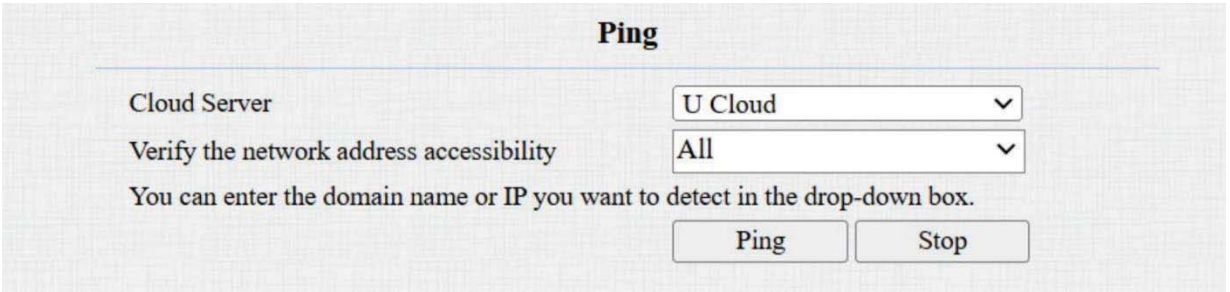
Make a web call on **Intercom > Basic > Web Call** interface.

- **Web Call (Ready):** Enter the target IP/SIP number and select the account to dial out.

Ping

The device allows you to verify the accessibility of the target server.

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



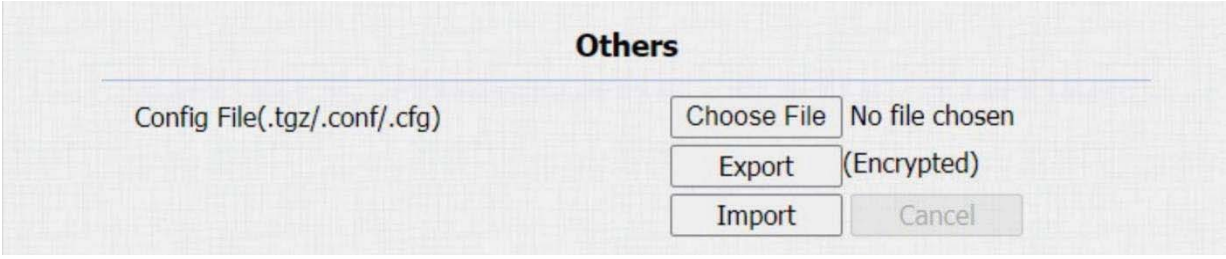
- **Cloud Server**: The server to be verified.

- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Backup

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

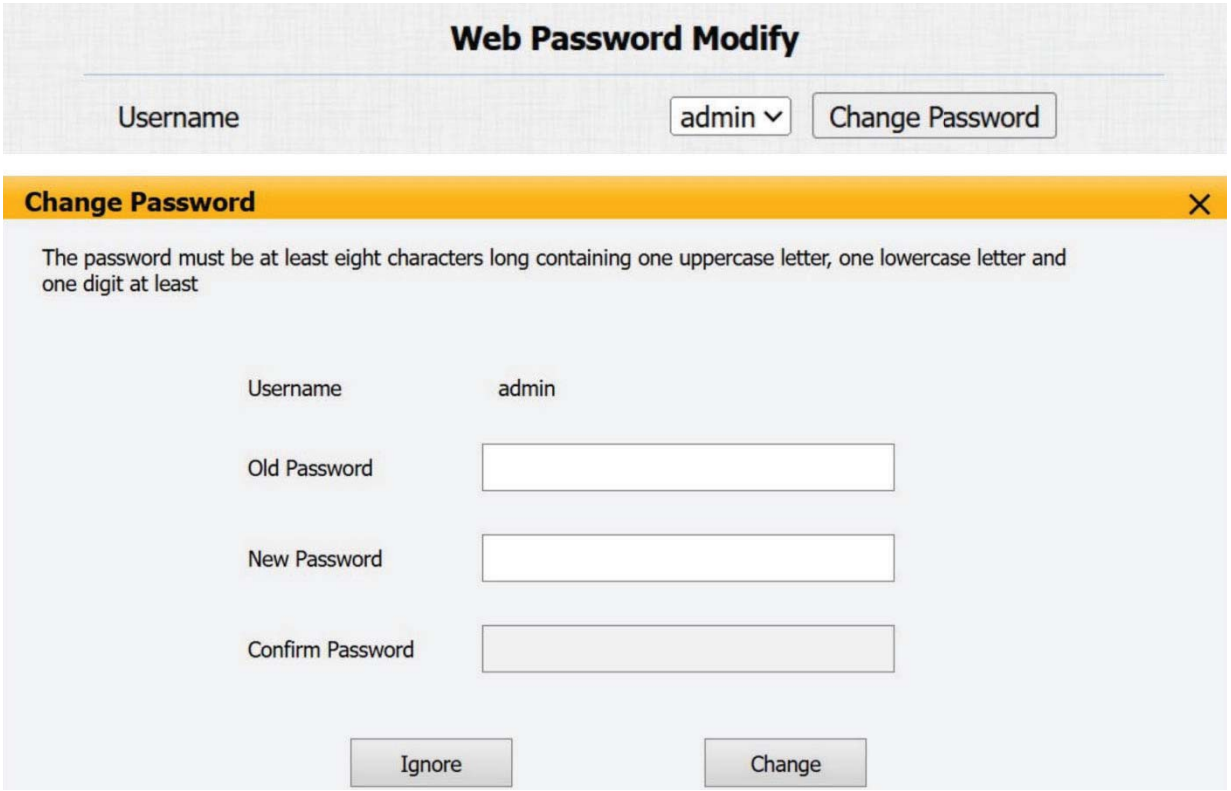
Export the file on the **System > Maintenance > Others** interface. The import file should be in .tgz/.conf/.cfg format.



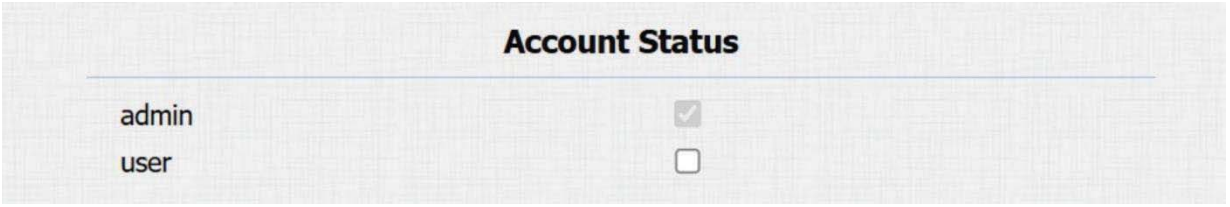
Password Modification

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

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



To enable or disable the user account, scroll to the **Account Status** section.

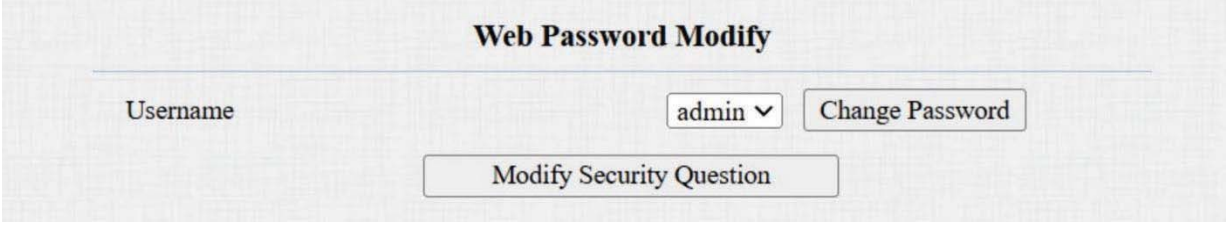


Modify Security Questions

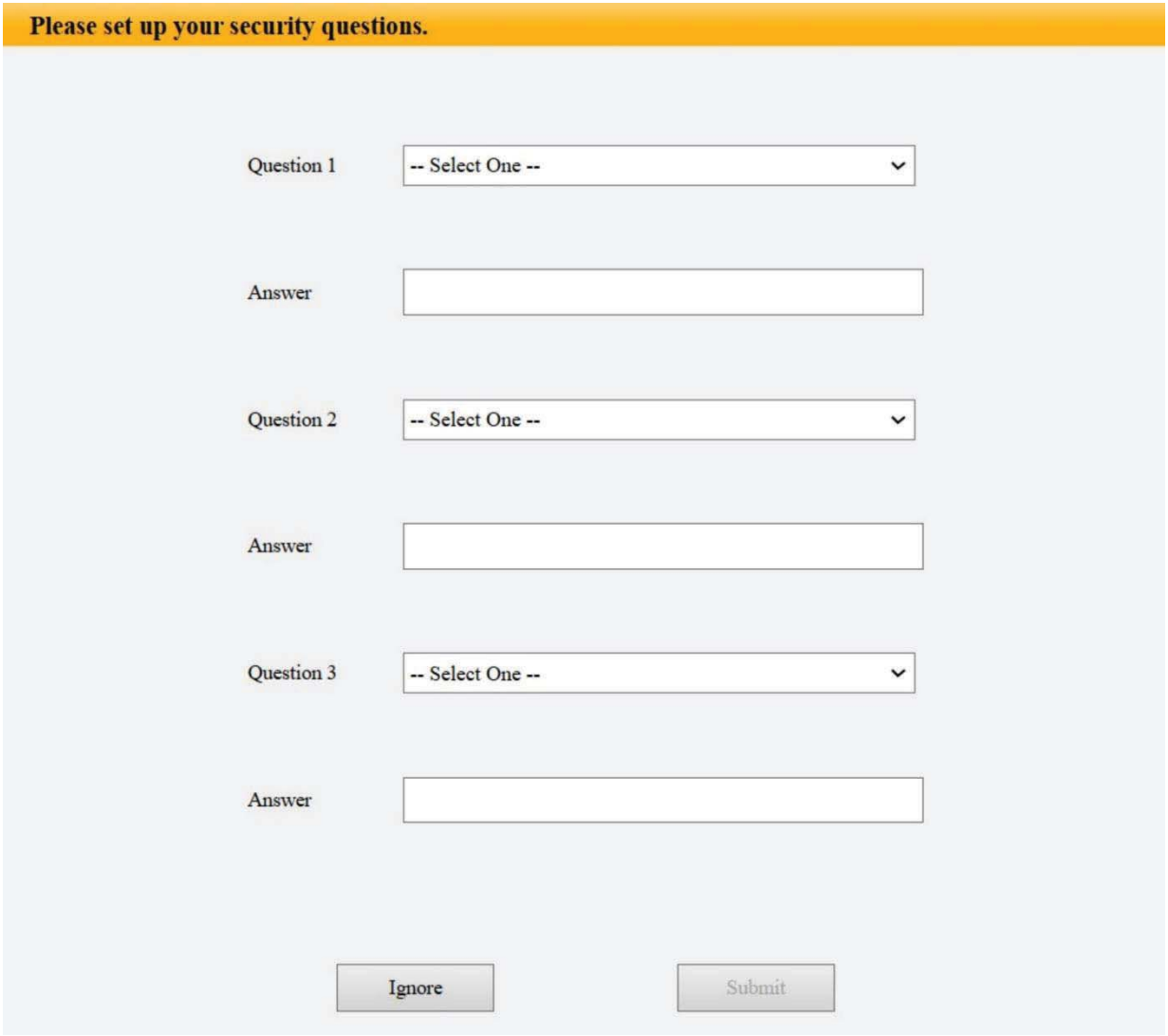
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

To set it up, go to the **System > Security** interface. Click **Modify Security Questions.**



You are required to fill in the correct password before modifying the security questions.

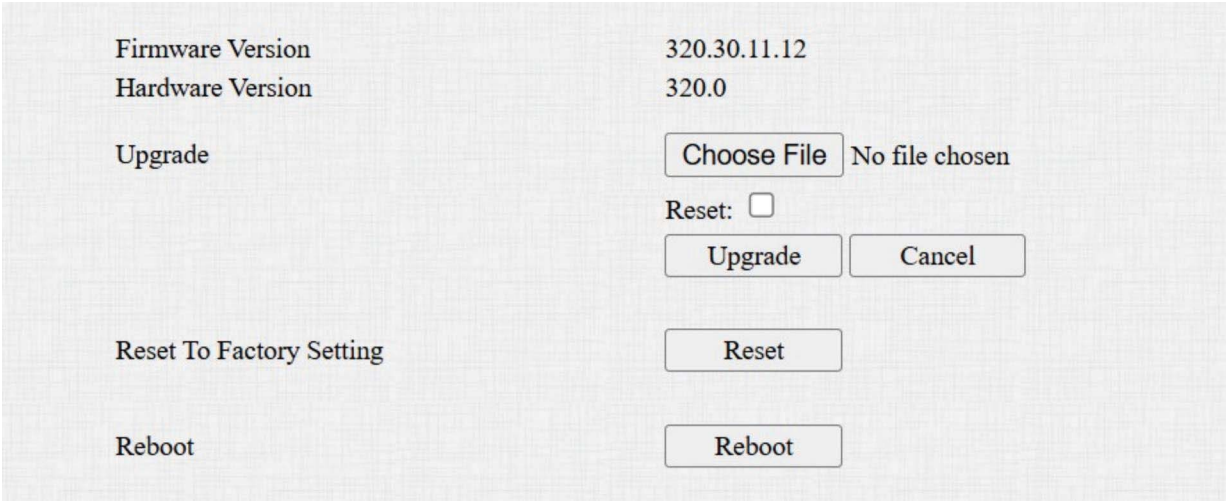


System Reboot&Reset

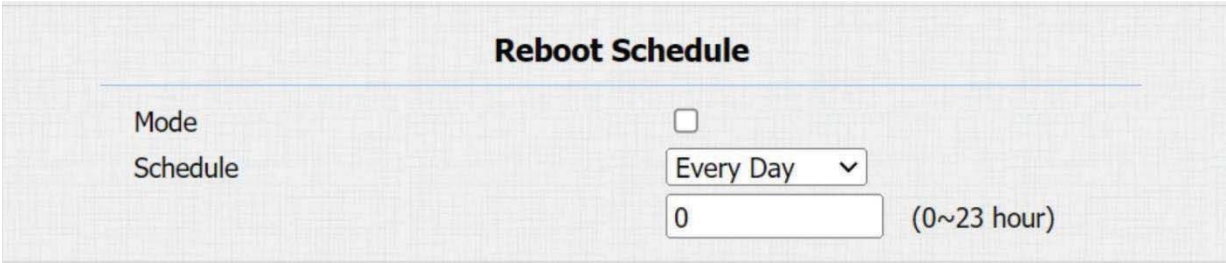
Reboot

If you want to restart the device system, you can operate it on the device web. Moreover, you can set up a schedule for the device to be restarted.

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

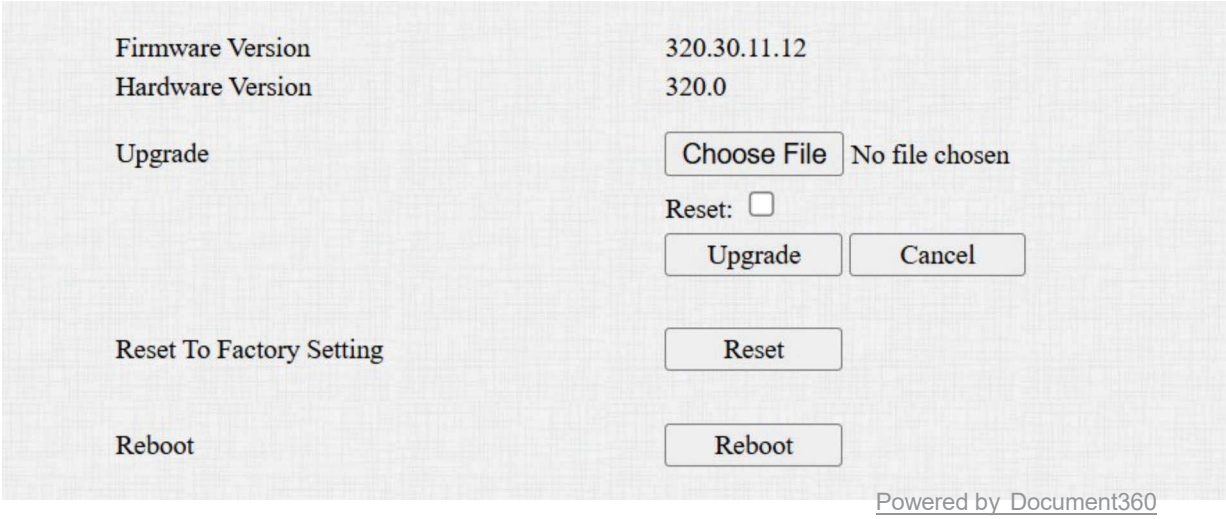


To set up the schedule, go to the **System > Auto Provisioning** interface.



Reset

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



FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.

CE
Frequency (TX):
BLE: 2402-2480MHz
NFC: 13.56MHz
4G:
Band 1: 1920-1980MHz
Band 3: 1710-1785MHz
Band 5: 824-849MHz
Band 7:2500-2570MHz
Band 8: 880-915MHz
Band 20: 832-862MHz
Band 28: 703-748MHz
Band 38: 2570-2620MHz
Band 40: 2300-2400MHz
Band 41: 2496-2690MHz

Frequency (RX):
BLE: 2402-2480MHz
NFC: 13.56MHz
4G:
Band 1: 2110-2170MHz
Band 3: 1805-1880MHz
Band 5: 869-894MHz
Band 7: 2620-2690MHz
Band 8: 925-960MHz
Band 20: 791-821MHz
Band 28: 758-803MHz
Band 38: 2570-2620MHz
Band 40: 2300-2400MHz
Band 41: 2496-2690MHz

Power:
BLE: 4.93dBm
NFC: -2.5 dBμA/m@3m
4G: 25dBm