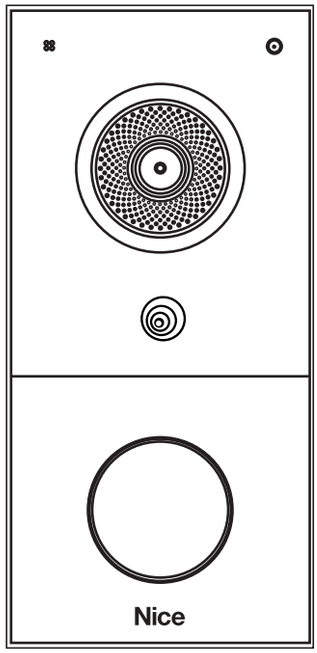
PRINTER'S INSTRUCTIONS:
LITERATURE, Quick Start Guide, Nice EL-DB-WP, -SX: 10034943 Rev-B X1; INK: BLACK; MATERIAL: 20 MEAD BOND WHT PAPER; SIZE: 8.5.000" x 11.000"; SCALE: 1-1; FOLD: SADDLE STITCH

EL-DB-WP
EL-DB-2W



Video Doorbell

Administrator Manual

Nice

Contents

Contents

Model Specification and Differences

Model	EL-DB-WP	EL-DB-2W
Camera	2M pixels, automatic lighting	2M pixels, automatic lighting
Relay In	2	2
Relay Out	1	1
WiFi	√	X
Card Reader	√	√
Microphone	1	1
Speaker	1	1
Bluetooth	√	√
TF Card Slot	1	1
Wiegand Port	√	√
Tamper Alarm	√	√
Power Supply	12V DC Connector (If not using PoE)	802.3af Power-over- Ethernet

Introduction to Configuration Menu

Status	Basic information such as product information, network information, account information, etc.
Account	Concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, etc.
Network	DHCP & static IP settings, RTP port settings, device deployment, etc.
Intercom	Intercom settings, call logs, etc.
Surveillance	Motion detection, RTSP, MJPEG, ONVIF and live streaming
Access Control	Input control, relay, card settings, private PIN code, Wiegand connection, etc.
Device	LED, audio, and SD card settings
Setting	Time & language, action settings, door settings and schedule for access control
Upgrade	Firmware upgrade, device reset and reboot, configuration file auto-provisioning and fault diagnosis
Security	High-security mode configuration, password modification, tamper alarm, HTTP API settings, etc.

Access the Device

Obtain the Device's IP Address

Check the Device IP address by holding the push button. You can set up the IP announcement loop times on the Device > Audio interface.

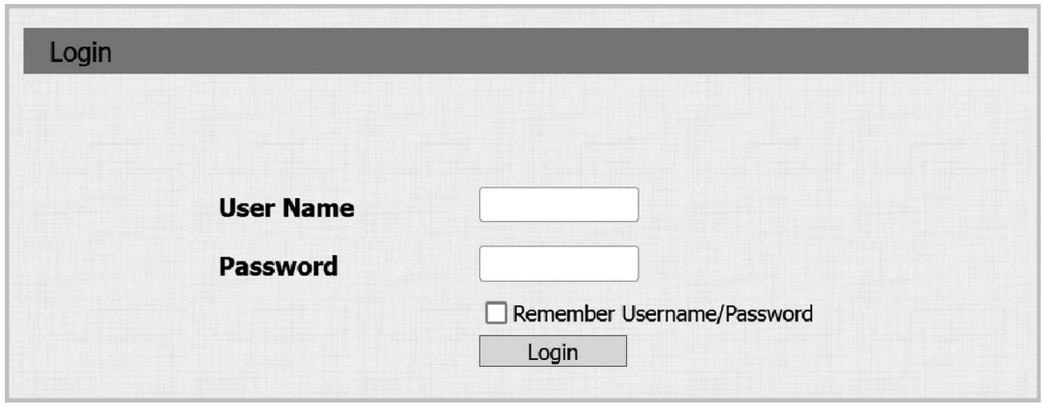
Expiration(After Reboot)(Sec)	Set the time limit within which users should hold the call button to sound the IP announcement after the device reboot. If you select *Always*, users can hold the call button anytime for IP announcement after the device reboot.
Loop Times	Set the IP announcement loop times.

Access the Device

Access the Device Setting

Enter the device IP address in a browser, and log into the device web interface to configure and adjust parameters.

The default user name is *admin*, but password is set upon first connection either by web or configurator.



NOTE: The Chrome browser is recommended.

Language and Time Setting

Language Setting

Set up the device web language using the device web **Setting > Time/Lang > Web Language** interface.

The device supports the following web languages:

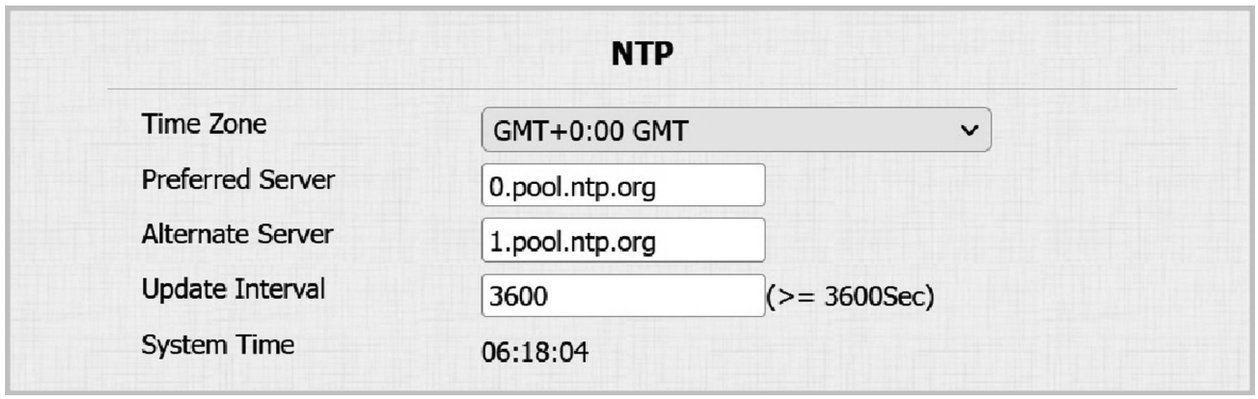
English, *Russian*, *Portuguese*, *Spanish*, *Italian*, *Dutch*, *French*, *German* and *Turkish*.

- **Mode:** *English* is the default web language.

Time Setting

The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on your device.

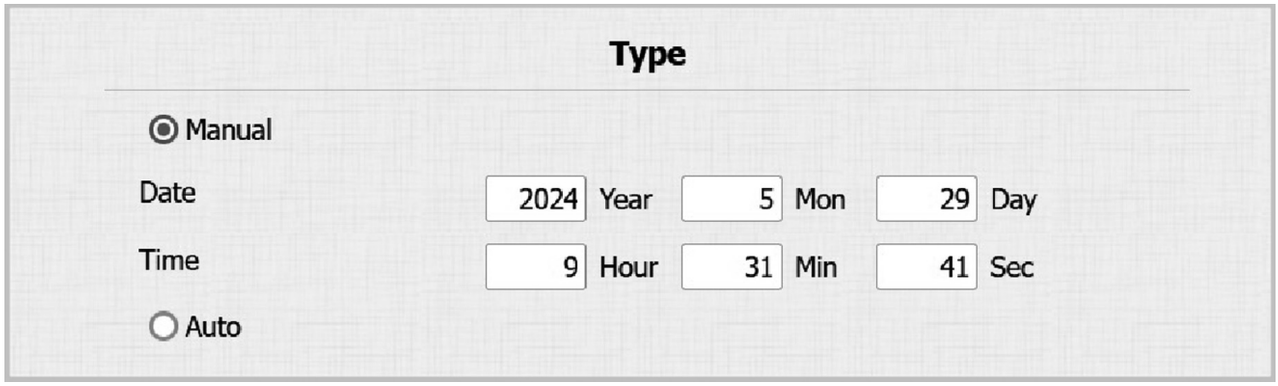
Set it up on the **Setting > Time/Lang > NTP** interface. The time will automatically be set when connected to Nice Home Management.



Time Zone	Select the specific time zone based on where the device is used. The default time zone is GMT+0:00.
Preferred Server	Enter the primary NTP server address for updating the time. The default NTP server address is 0.pool.ntp.org.
Alternate Server	Enter the backup NPT server address when the primary one fails.
Update Interval	Set the time update interval. For example, if you set it as 3600, the device will send a request to the NPT server for the time update every 3600 seconds.
System Time	Display the current device time.

Language and Time Setting

You can also set up the time manually. Select *Manual*, and enter the date and time.

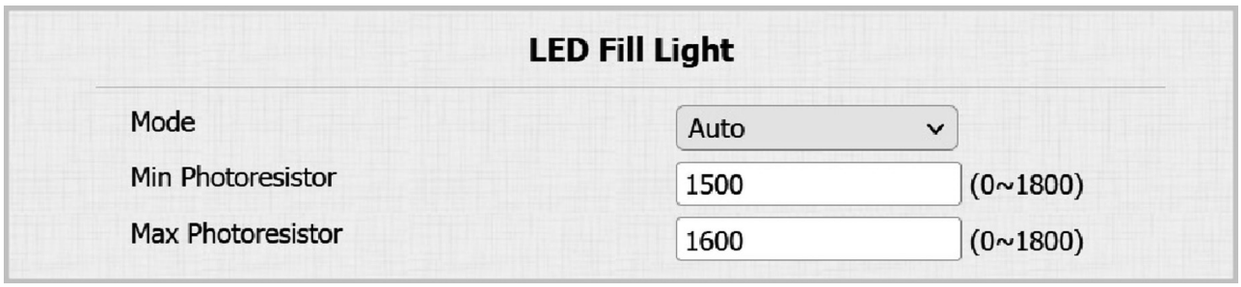


LED Setting

LED Light Setting

LED fill light is mainly designed to reinforce the light at night or in a dark environment.

Set it up on the **Device > LED Setting > LED** Fill Light interface.

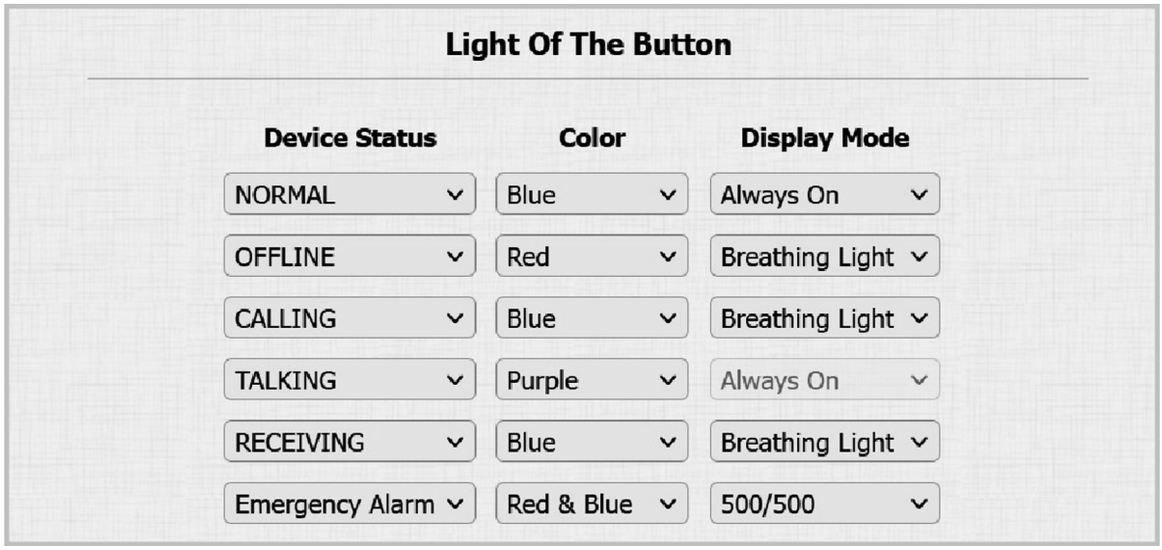


Mode	◊ Auto turns on the LED light automatically. ◊ Aways OFF turns off the LED light. ◊ Specific Time turns on the LED according to the schedule.
Min/Max Photoresistor	Set the minimum and maximum Photoresistor value, based on the current actual photo-resistor value detected to control the ON-OFF of the LED light. You can set the maximum Photoresistor value for the LED to be activated and the minimum value for it to be shut off.

LED Light Status

LED display adjustment is used to indicate the light changes of the call button in different states. The LED status allows users to verify the current mode of the device.

Set it up on the web **Device > LED Setting > Light of The Button** interface.



LED Setting

Device Status	There are six statuses: *Normal*, *Offline*, *Calling*, *Talking*, *Receiving* and *Emergency Alarm*. The status cannot be changed.
Color	Select from *Blue*, *Red* or *Purple*. You can select *Red & Blue* (flashing red and blue alternately) for **Emergency Alarm** status.
Display Mode	Set the different flashing frequencies.

LED Setting on Card Reader Area

Enable or disable the LED lighting on the card reader area. You can also set a specific time during which the LED will be disabled to reduce power consumption.

Set it up on the **Device > LED Setting > Light of The Card Reader** interface.

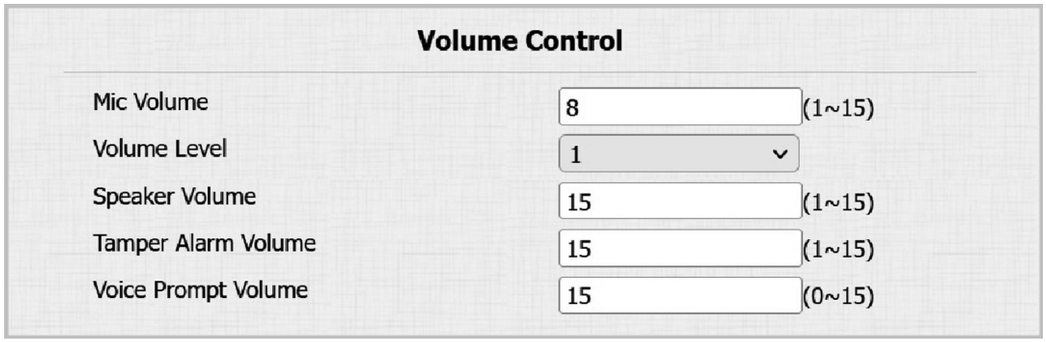
LED Enabled	Click to Enable or Disable.
Start Time - End Time(Hour)	Set the LED light valid time. If the time is set from 8-0 (Start time - End time), the LED light will stay on from 8:00 a.m. to 12:00 p.m. for one day (24 hours).

Volume and Tone Configuration

Volume and tone configuration include various volume controls. Tones can be uploaded to enrich the user experience.

Volumes

To set up volumes, go to the web **Device > Audio** interface.



Tamper Alarm Volume	Set the volume when the tamper alarm is triggered.
Voice Prompt Volume	Set the voice prompt volume level.

Open Door Tones

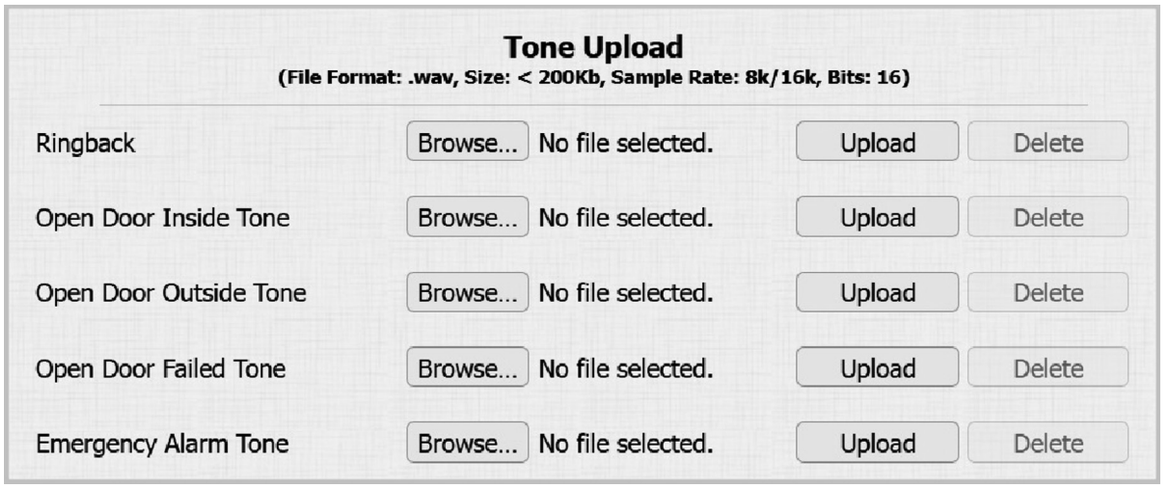
Enable or disable the door-opening tones on the web **Device > Audio > Open Door Tone Setting** interface.

Open Door Inside Tone Enabled	The tone sounds when users open the door by pressing the **Exit** Button.
Color	The tone sounds when users open doors via various device-supported access methods.
Display Mode	The tone sounds when opening the door fails.

Volume and Tone Configuration

Upload Tone Files

Customize ringback, door-opening and emergency alarm tones. Upload files on the **Device > Audio > Tone Upload** interface.



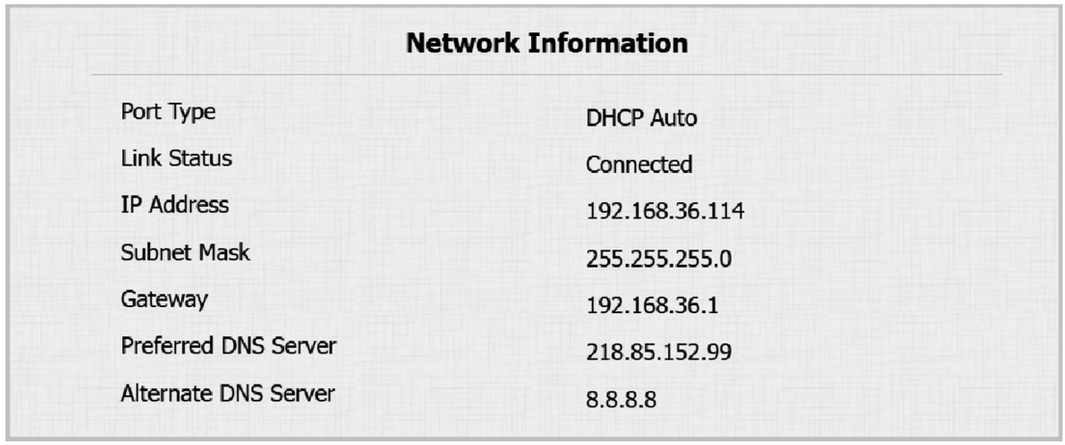
Ringback	The tone is heard by the users who call the device.
Open Door Inside Tone	The tone sounds when users open the door by pressing the **Exit** button.
Open Door Outside Tone	The tone sounds when users open doors via various device-supported access methods.
Open Door Failed Tone	The tone sounds when the door opening fails.
Emergency Alarm Tone	The tone sounds when the emergency alarm is triggered.

NOTE: File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16.

Network Setting

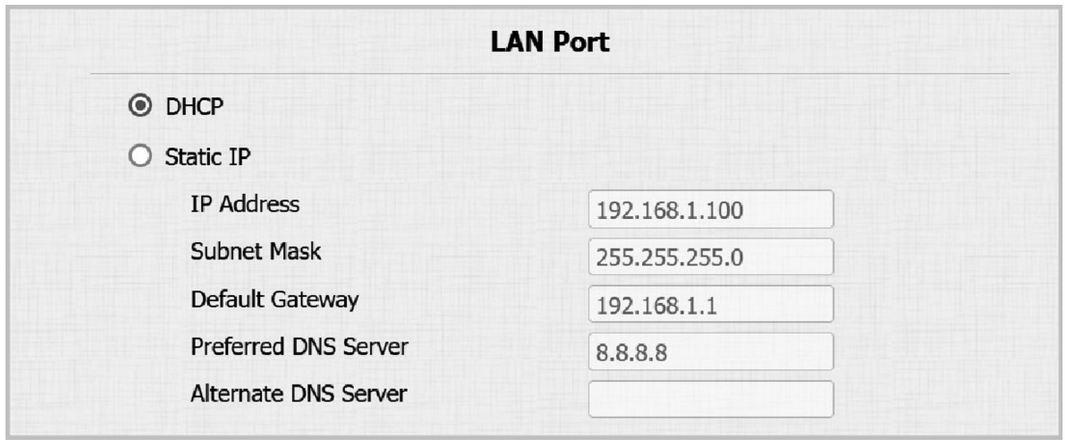
Network Status

Check the network status on the web **Status > Network Information** interface.



Device Network Configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the DHCP server. To set it up, go to **Network > Basic** interface.



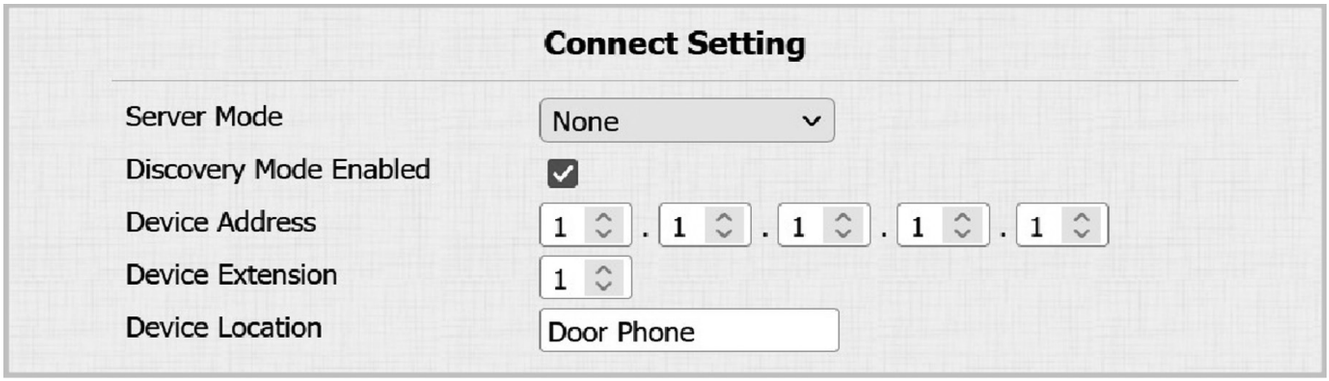
DHCP	DHCP mode is the default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server automatically with IP address, subnet mask, default gateway and DNS server address.
Static IP	When static IP mode is selected, the IP address, subnet mask, default gateway and DNS server address should be configured according to the network environment.
IP Address	Set up the IP address when 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 preferred or alternate Domain Name Server (DNS) server according to the actual network environment. The preferred DNS server is the primary server while the alternate DNS server is the secondary one. The secondary server is for backup.

Network Setting

Device Deployment in Network

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

To set it up, navigate to the web **Network > Advanced > Connect Setting** interface.



Server Mode	This mode is automatically set up according to the device connection with a specific server in the network such as *SDMC*, *Cloud* or *None*. *None* is the default factory setting, indicating the device is not in any server type.
Discovery Mode Enabled	When enabled, the device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
Device Address	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	The device extension number.
Device Location	The location in which the device is installed and used.

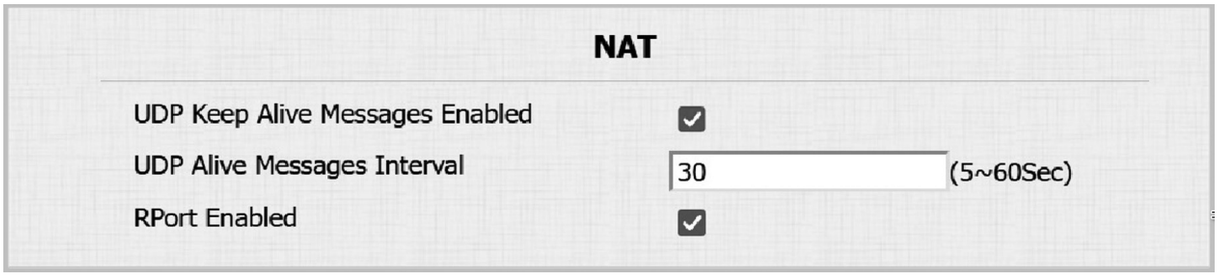
NAT Setting

Network Address Translation (NAT) allows devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

To enable NAT, go to **Account > Basic > NAT** interface.

Stun Server Address	Enter the server address when the device is in a Wide Area Network (WAN).
Port	The server port.

To set up NAT, navigate to the web **Account > Advanced > NAT** interface.

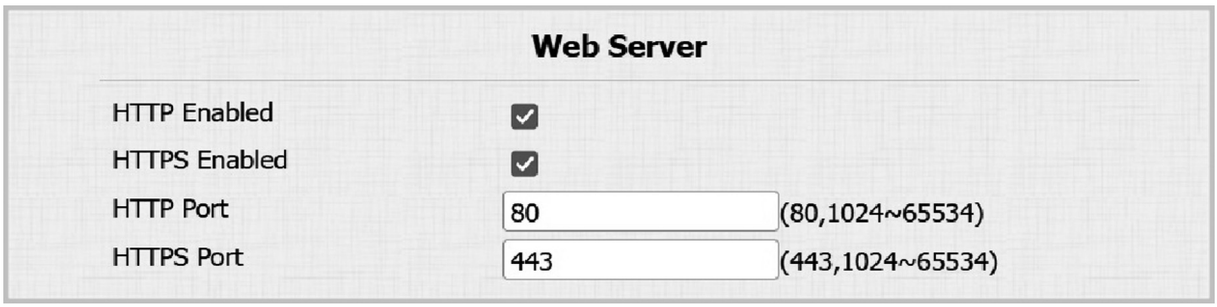


UDP Keep Alive Messages Enabled	If enabled, the device will send the message to the SIP server which will recognize whether the device is online.
UDP Alive Messages Interval	Set the message-sending interval from 5-60 seconds. The default is 30 seconds.
RPort	Enable the RPort when the SIP server is in a WAN.

Device Web HTTP Setting

This function manages device website access. The device supports two remote access methods: *HTTP* and *HTTPS* (encryption).

Set it up on the **Network > Advanced > Web Server** interface.



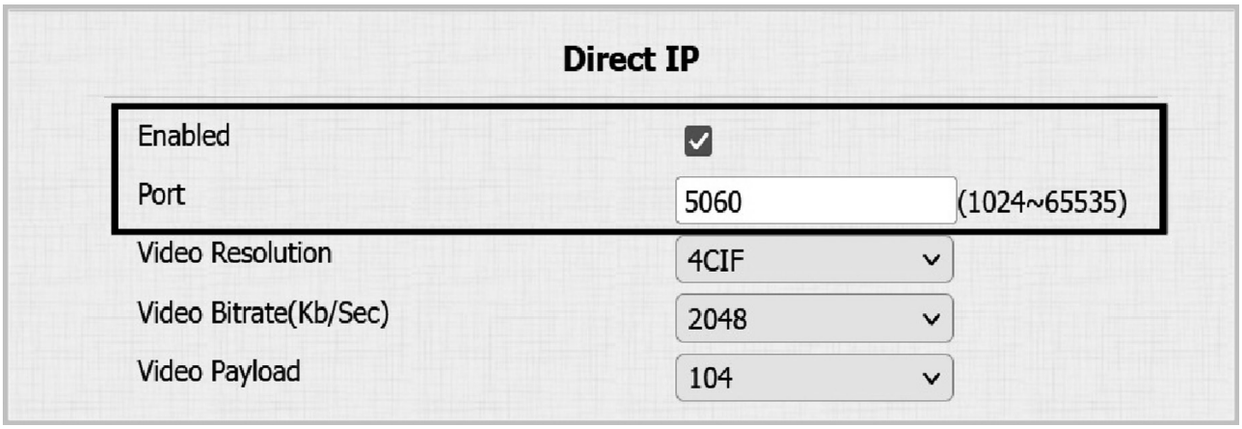
HTTP/HTTPS Enabled	HTTP and HTTPS are enabled by default.
HTTP/HTTPS Port	Specify the web server port for accessing the device web interface via HTTP/HTTPS.

Intercom Call Configuration

IP Call Configuration

An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Enable Direct IP on the **Intercom > Basic > Direct IP** interface.



Port: Set the port for direct IP calls. The default is 5060, with a range from 1-65535. If you enter a value other than 5060, ensure consistency with the corresponding device for data transmission.

SIP Call Configuration

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

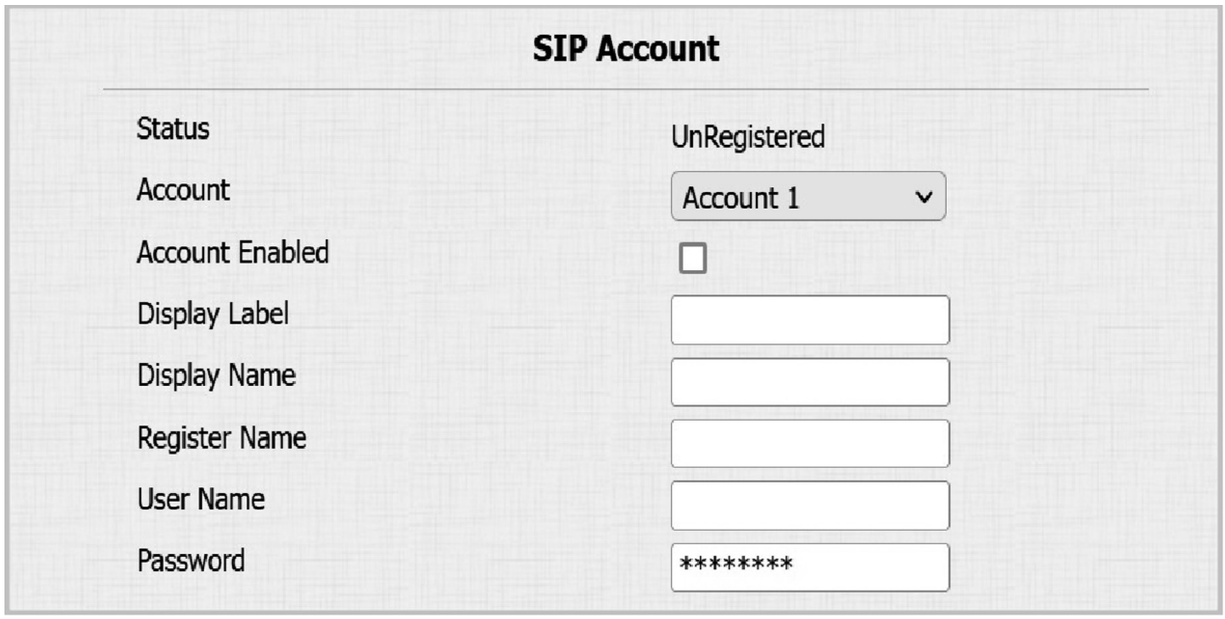
An SIP call uses SIP to send and receive data between SIP devices and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires an SIP account, a SIP address for each device, and configuring SIP settings on the devices.

Intercom Call Configuration

SIP Account Registration

Each device needs a SIP account to make and receive SIP calls. Video Doorbell devices support the configuration of two SIP accounts, which can be registered under two independent servers.

To set up an SIP account, navigate to the web **Account > Basic > SIP Account** Interface.



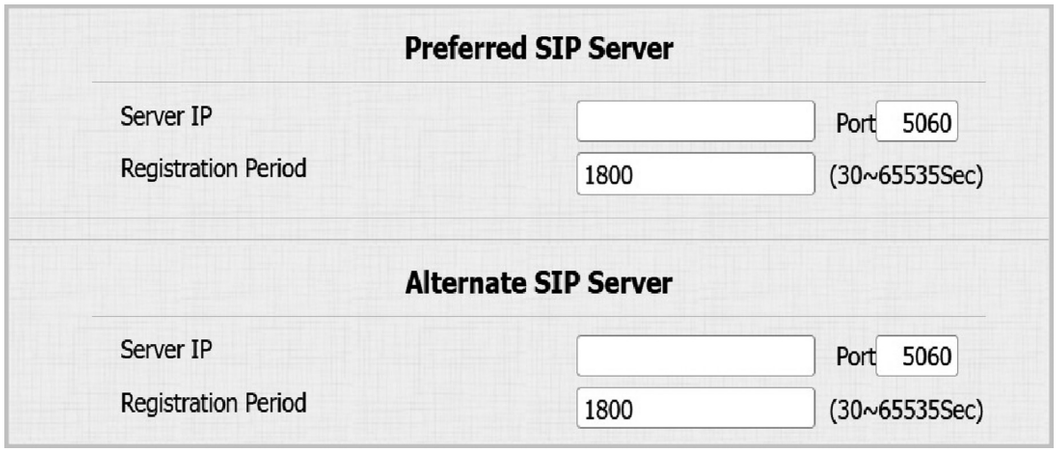
Status	Indicate whether the SIP account is registered or not.
Account 1/ Account 2	The doorbell supports 2 SIP accounts. ◊ Account 1 is the default account for call processing. ◊ The system switches to Account 2 if Account 1 is not registered. ◊ To designate the account to be used for outgoing calls, select the account number.
Display Label	The label of the device will be displayed.
Display Name	The designation for Account 1 or 2 is to be shown on the device itself on the calling screen.
Register Name	Same as the username from the PBX server.
Access Control	Input control, relay, card settings, private PIN code, Wiegand connection, etc.
User Name	Same as the username from the PBX server for authentication.
Password	Same as the password from the PBX server for authentication.

Intercom Call Configuration

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 using the Built-in from Nice Home Management. By default, this is enabled and should point to the Nice Home management controller.

To set up an SIP server, go to the web **Account > Basic** interface.



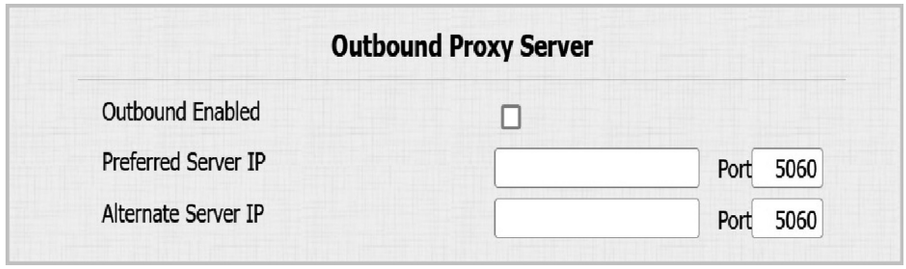
Server IP	Enter the server's IP address or its domain name.
Port	Specify the SIP server port for data transmission.
Registration Period	Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified period.

Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission.

To set it up, go to the web **Account > Basic > Outbound Proxy Server** Interface.

Preferred Server IP	Enter the SIP proxy server's IP address.
Port	Set the port for establishing a call session via the outbound proxy server.
Alternate Server IP	Enter the SIP proxy IP address to be used when the main proxy server malfunctions.
Port	Set the proxy port to establish a call session via the backup outbound proxy server. By default, this is enabled and should be the IP address of the Nice Home Management controller.



Intercom Call Configuration

Data Transmission Type

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

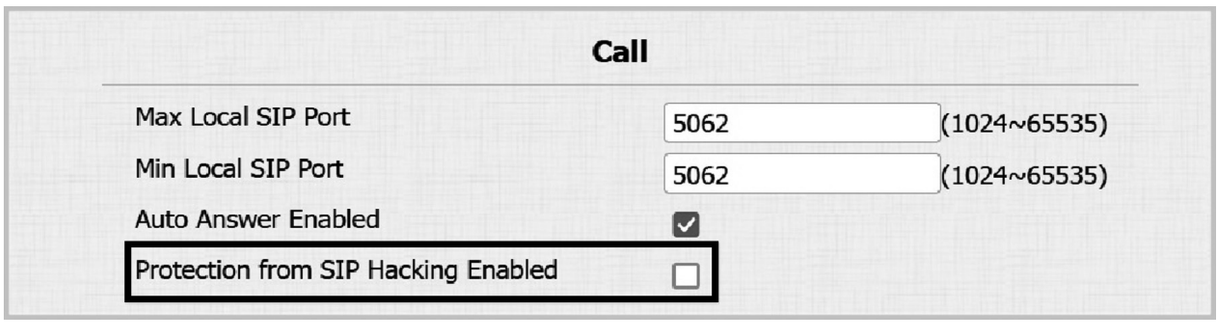
To set it up, go to the web **Account > Basic > Transport Type** interface.

UDP	This is an unreliable (but very efficient) transport layer protocol. It is the default transport protocol.
TCP	This is a less efficient (but reliable) transport layer protocol.
TLS	This is an encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. Certificates for authentication will need to be uploaded in order to use TLS.
DNS-SRV	A DNS service record defines the location of servers. This record includes the hostname and port number of the server, as well as the priority and weight values that determine the order and frequency of using the server.

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.

To enable, go to **Account > Advanced > Call** interface.

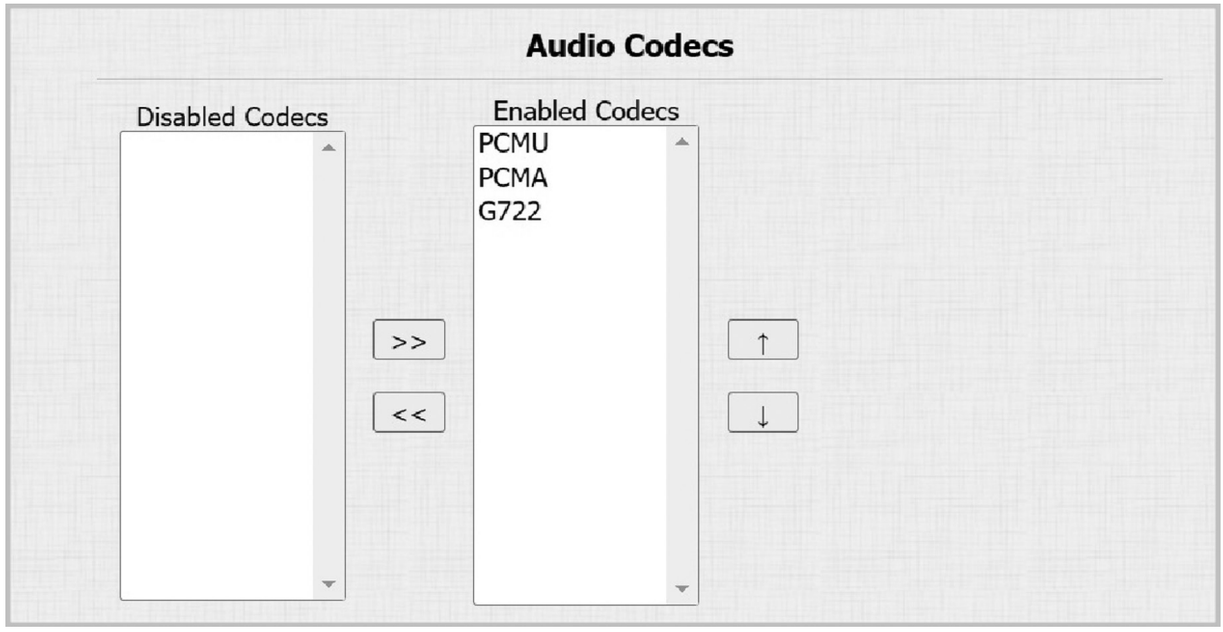


Audio & Video Codec Configuration

Audio Codec

The doorbell supports three types of codecs (*PCMU*, *PCMA* and *G722*) for encoding and decoding the audio data during the call session. Each 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.

Set it up on the **Account > Advanced > Audio Codecs** interface:



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

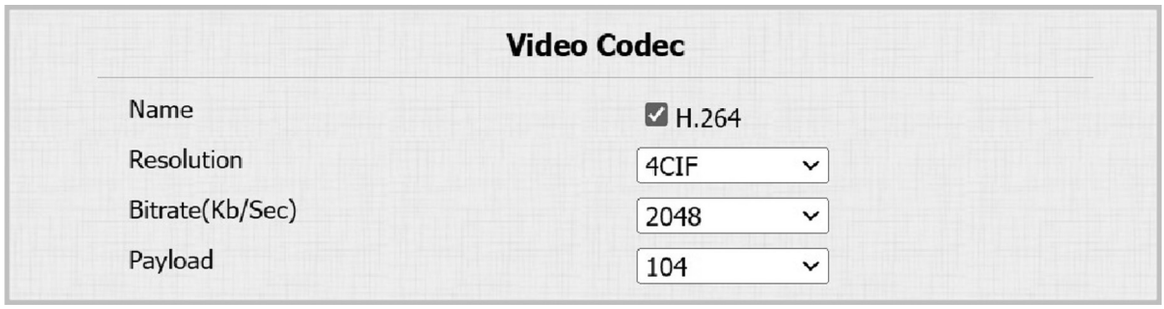
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec

The doorbell supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

Audio & Video Codec Configuration

Go to the web **Account > Advanced > Video Codec** interface to set it up.

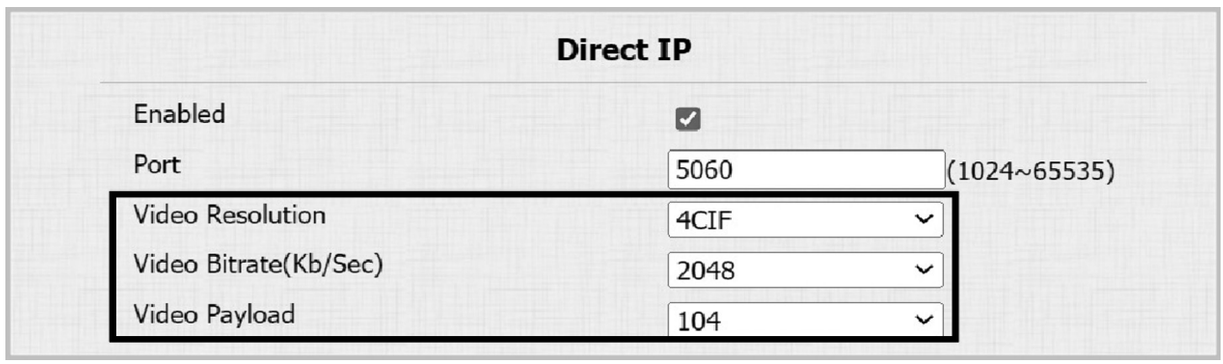


Name	Check to enable the H264 video codec format for the doorbell video stream.
Resolution	Select the resolution from the provided options. The default code resolution is *4CIF*.
Bitrate	The video stream bitrate ranges from *128* to *2048* kbps. The greater the bitrate, the more data transmitted every second and the clearer the video will be. The default code bitrate is *2048*.
Payload	The payload ranges from *90* to *119* for configuring audio/video configuration files. The default is *104*.

Video Codec for IP Direct Calls

Select the IP call video quality by selecting the proper codec resolution according to the network condition.

Navigate to the **Intercom > Basic > Direct IP** interface to set it up.

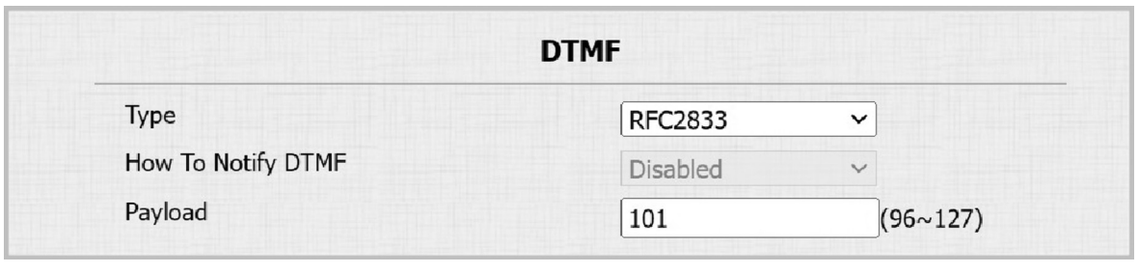


Video Resolution	Select the resolution from the provided options.
Video Bitrate	The video stream bitrate ranges from *128* to *2048* kbps. The default bitrate is *2048*.
Video Payload	The payload ranges from *90* to *119* for configuring audio/video configuration files. The default is *104*.

Configure DTMF Data Transmission

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 doorbell and other intercom devices for third-party integration.

Navigate to the **Account > Advanced > DTMF** interface to set it up.

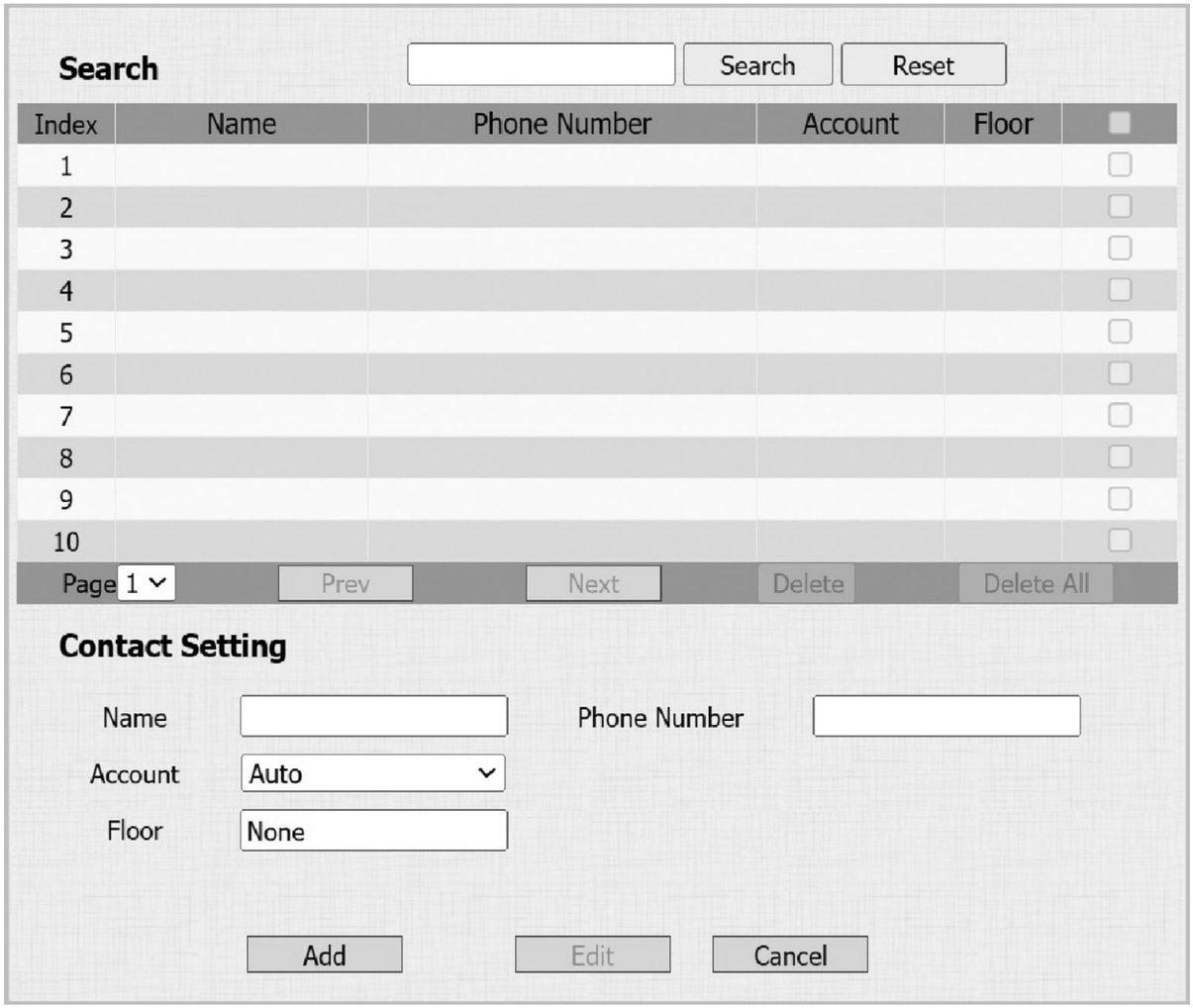


Type	Select from the following options: *Inband*, *RFC2833*, *Info*, *Info+Inband*, *Info+RFC2833* based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
How to Notify DTMF	Select *Disabled*, *DTMF*, *DTMF-Relay* or *Telephone-Event* according to the specific type adopted by the third-party device. You are required to set it up only when the third-party device to be matched with adopts Info mode.
Payload	Set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

Access Allowlist Configuration

The doorbell can store up to 1000 contacts, giving access permission to indoor monitors or other devices.

Search, create, edit, and delete the contacts in the allowlist. The **Access Control > Access Allowlist** interface is used to set it up.

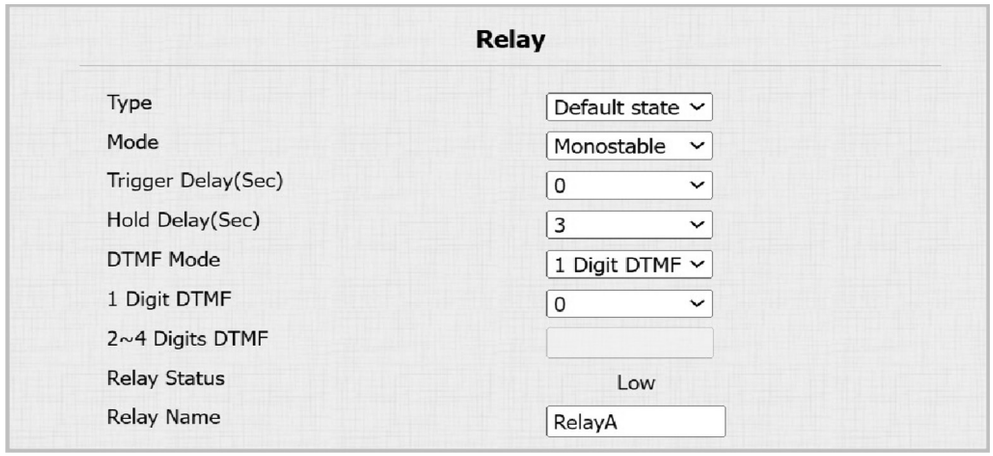


Name	Name the contact.
Resolution	The phone number of the contact. It supports IP addresses and SIP numbers.
Bitrate	Select the account to make the call.
Payload	Specify the accessible floor(s) to the contact via the elevator.

Relay Setting

Relay Switch Setting

You can configure the relay switch(es) and DTMF for the door access on the web **Access Control > Relay** interface.



Type	Determine the interpretation of the Relay Status regarding the state of the door: ◊ **Default Status (Normally Open):** A *Low* status in the Relay Status field indicates that the door is closed, while *High* indicates that it is opened. ◊ **Invert Status (Normally Closed):** A *Low* status in the Relay Status field indicates an opened door, while *High* indicates a closed one.
Mode	Specify the conditions for automatically resetting the relay status. ◊ **Monostable:** The relay status resets automatically within the relay delay time after activation. ◊ **Bistable:** Latching the relay status resets upon triggering the relay again.
Trigger Delay(Sec)	Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the **Unlock** button.
Hold Delay(Sec)	Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
DTMF Mode	Set the digits of the DTMF code.
1 Digit DTMF	Input control, relay, card settings, private PIN code, Wiegand connection, etc.
2~4 Digits DTMF	Set the DTMF code based on the number of digits selected in the DTMF Mode.
Relay Status	Indicate the states of the relay, which are normally opened and closed. By default, it shows low for *Normally Closed(NC)* and high for *Normally Open(NO)*.
Relay Name	Assign a distinct name for identification purposes.

NOTE: External devices connected to the relay require separate power adapters.

Door Access Schedule Management

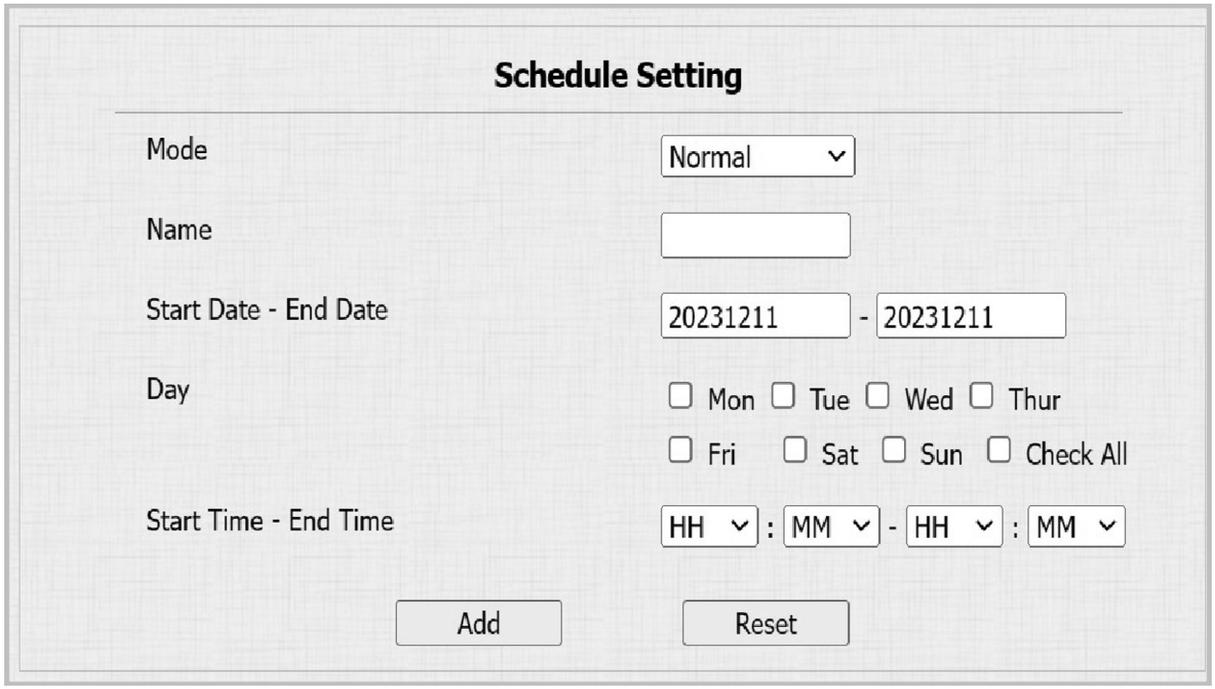
Configure Door Access Schedule

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.

Create Door Access Schedule

You can create door access schedules for daily, weekly or custom time periods.

Navigate to the web **Setting > Schedule** interface to set it up.



Mode	◊ **Normal:** Set the schedule based on the month, week and day. It is used for a long period schedule. ◊ **Weekly:** Set the schedule based on the week. ◊ **Daily:** Set the schedule based on 24 hours a day.
Name	Name the schedule.

Door Access Schedule Management

Import and Export Door Access Schedule

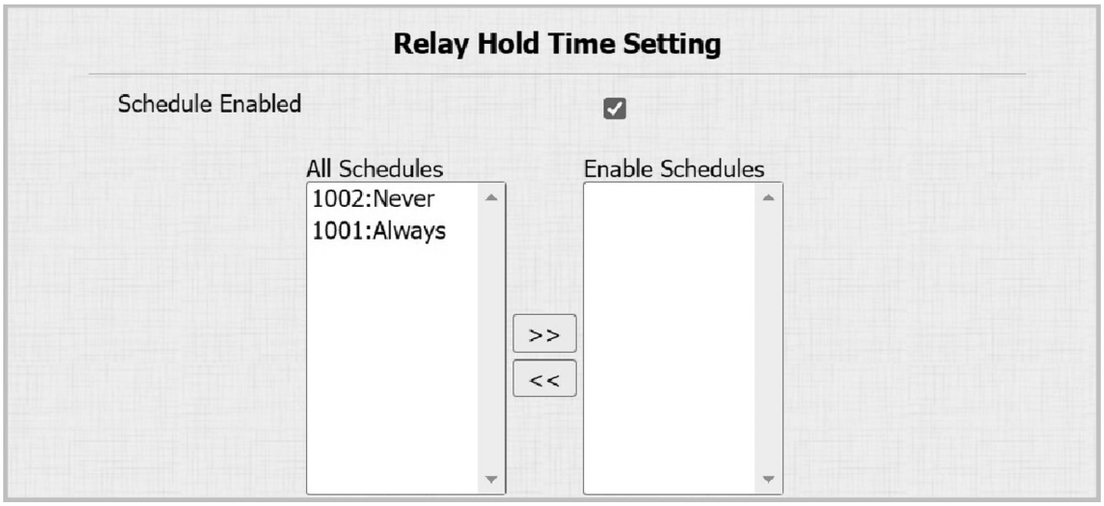
You can create door access schedules one by one or in bulk. You can export the current schedule file, edit the file or add more schedules following the format, as well as import the new file to the desired devices. This helps you manage your door access schedules easily.

Go to the **Setting > Schedule** interface to setup schedules. The file exports in TGZ format. The import file should be in XML format.

Relay Schedule

The relay schedule allows you to set a specific relay to always open at a certain time. This is helpful for situations like keeping the gate open after school or keeping the door open during work hours.

To set up a relay schedule, navigate to the **Access Control > Relay > Relay Hold Time Setting** interface.



Schedule Enabled: Assign particular door access schedules to the chosen relay. Simply move them to the **Selected Schedules** box.

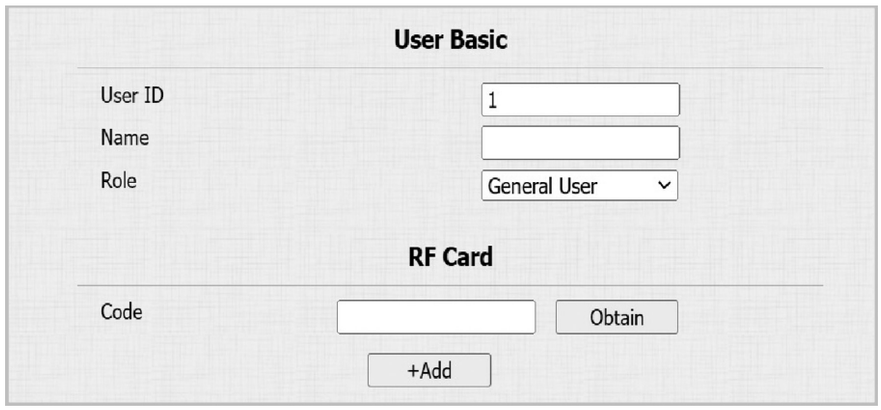
For instructions on creating schedules, consult the **Create Door Access Schedule section** on the previous page.

Door Unlock Configuration

Unlock by RF Cards

The RF card should be assigned to a particular user for door opening. When adding a user, you can also customize settings such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

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

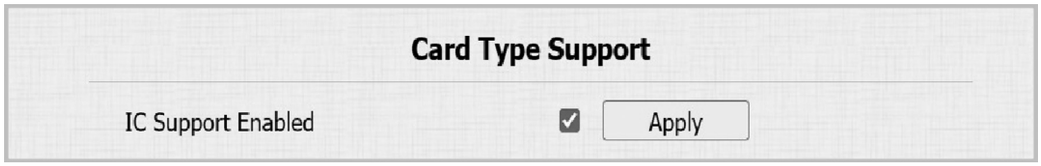


User ID	The unique identification number assigned to the user.
Name	The name of this user.
Role	Define the user as a *General User* or an *Administrator*. The Admin card can be used to add a user card. Please refer to **Configure Admin Cards** and **User Cards** for detailed configuration.
Code	The card number that the card reader reads.

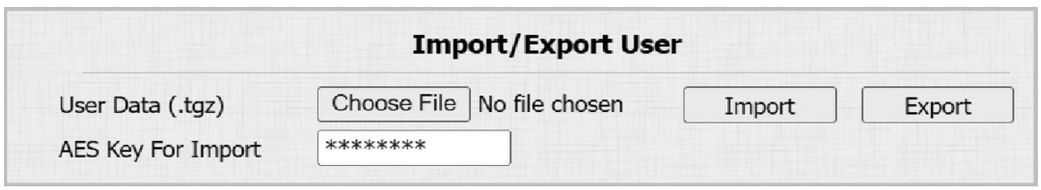
NOTE:

- Each user can have a maximum of 5 cards added.
- The device allows to add 5,000 users.
- RF cards operating at 13.56 MHz frequencies are compatible with the doorbell for access.

To enable the IC card function, navigate to the **Access Control > Card Setting > Card Type Support** interface.



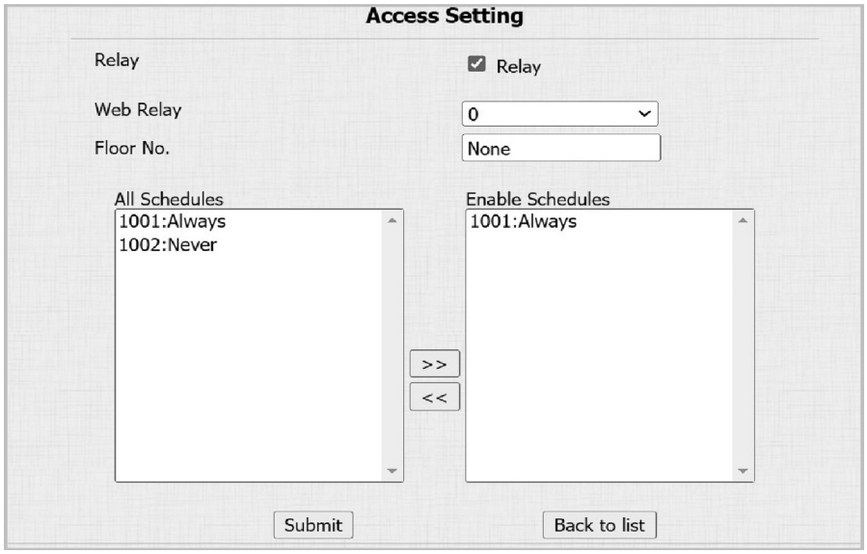
After adding users, you can export the user data and import it to another intercom device for quick management. On the **Access Control > User** interface, scroll to the **Import/Export User** section.



Door Access Schedule Management

Access Settings

After user information and RF card code are entered, you can scroll down to the **Access Setting** and configure RF card access control.



Relay	The relay to be unlocked using the door-opening methods should be assigned to the user.
Web Relay	Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
Floor No.	Specify the accessible floor(s) to the user via the elevator.
Schedule	Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options: ◊ **Always:** Allows door opening without limitations on door open counts during the valid period. ◊ **Never:** Prohibits door opening.

RF Card Code Format

To integrate the RF card door access with the third-party intercom system, you need to match the RF card code format with the one used by the third-party system.

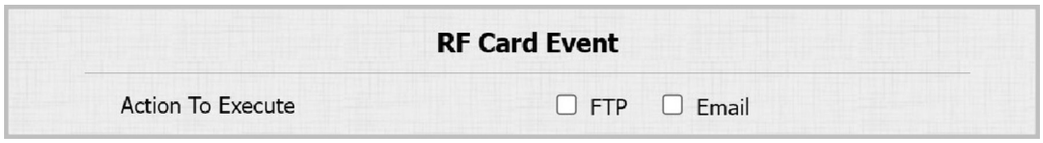
To set it up, go to **Access Control > Card Setting > RFID** interface.

- **IC Card Display Mode:** Set the card number format from the provided options. The default format in the device is *8HN*.

Door Unlock Configuration

Events Triggered by Using RF Cards

You can set up the events triggered by swiping the RF cards on the **Access Control > Card Setting > RF Card Event** interface.

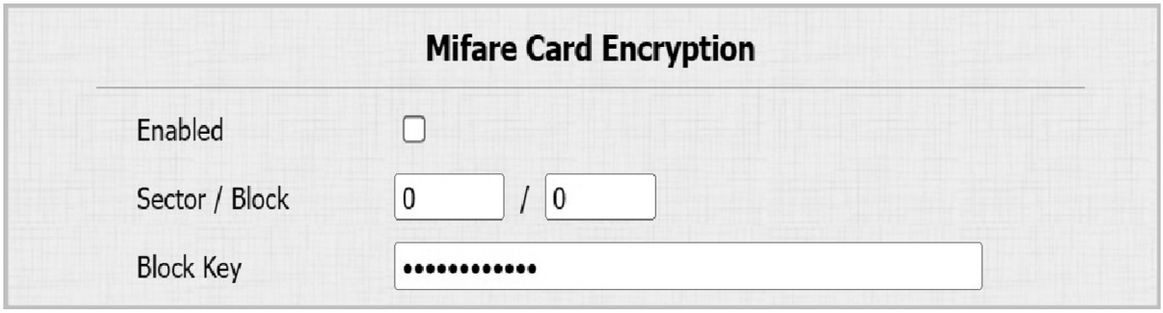


- **Action to Execute:** Set the actions that occur when the door is opened by swiping the RF card.
  - ◊ **Email:** Send a message to the preconfigured Email address.
  - ◊ **FTP:** Send a message to the preconfigured FTP address.

Mifare Card Encryption

The video doorbell can encrypt Mifare cards for greater security. When this feature is enabled, it reads the data in the cards' designated sectors and blocks, not the UID.

To encrypt the card, navigate to the **Access Control > Card Setting > Mifare Card Encryption** interface.



Sector/Block	Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
Block Key	Set a password to access the data stored in the predefined sector/block.

NFC Card

NFC (Near Field Communication) is a popular way for door access. It uses radio waves for data transmission interaction. The device can be unlocked by NFC. You can keep the mobile phone closer to the device for door access.

To use the specific card, go to **Access Control > Card Setting > Contactless Smart Card** interface.

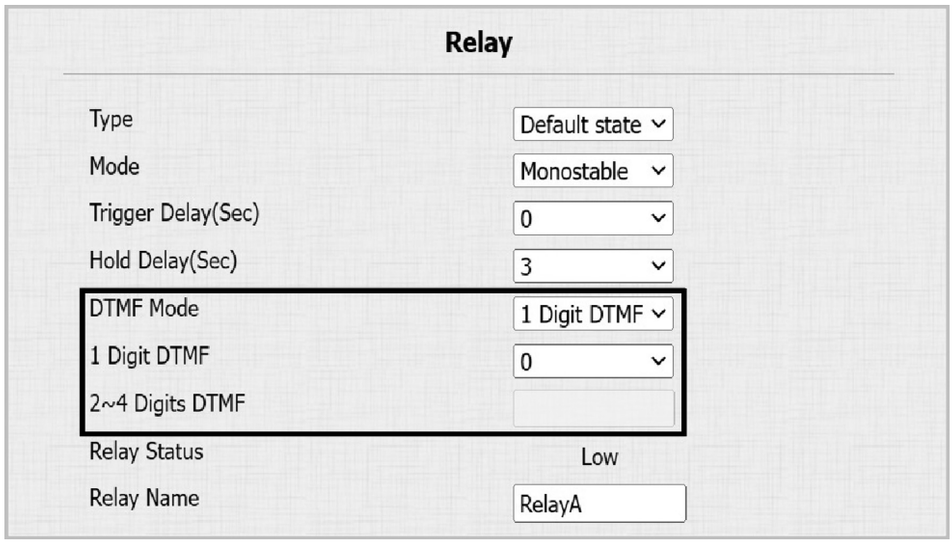
NOTE:

- The NFC feature is not available on iPhones.
- Please refer to Open the Door via NFC for detailed configuration.

Unlock by DTMF Code

Dual-tone multi-frequency signaling (DTMF) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad or by tapping the unlock tab with the DTMF code on the screen.

To configure DTMF codes, go to **Access Control > Relay** interface.



DTMF Mode	Set the number of digits for the DTMF code.
1 Digit DTMF	Define the 1-digit DTMF code within the range (0-9 and *,#) when the DTMF Mode is set to 1-digit.
2-4 Digit DTMF	Set the DTMF code based on the number of digits selected in the DTMF Mode.

NOTE: To open the door with DTMF, the intercom devices that send and receive the unlock command must use the same mode and code. Otherwise, the DTMF unlock may fail.

DTMF White List

To secure door access via DTMF codes, you can set up the DTMF whitelist on the device web **Access Control > Relay > Open Relay Via DTMF** interface so that only the caller numbers you designated in the doorbell can use the DTMF code to gain door access.

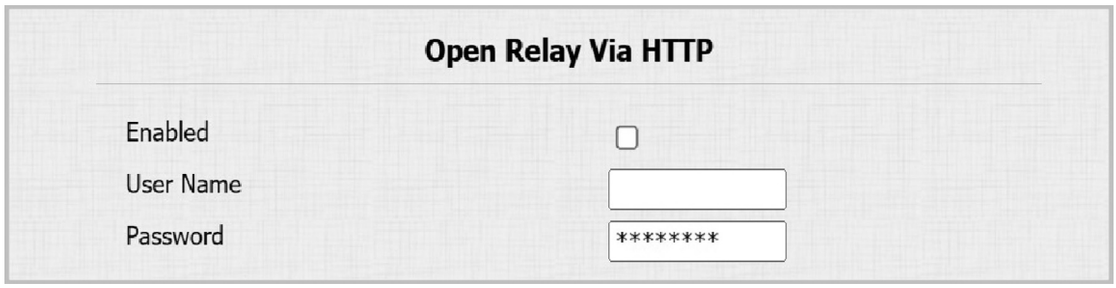
- **Assigned The Authority For:** Specify the contacts authorized to open doors via DTMF:
  - ◊ **Disabled:** No numbers can unlock doors using DTMF.
  - ◊ **Allowlist And Push Button:** Doors can be opened by numbers added to the doorbell's contact list and pressing the push button.
  - ◊ **All Numbers:** Any numbers can unlock using DTMF.

NOTE: When selecting this option, the calling indoor monitor(s) should be added into the doorbell's contact list.

Unlock by HTTP Command

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

Setup the HTTP command on the web **Access Control > Relay > Open Relay Via HTTP** interface.



User Name	Set a username for authentication in HTTP command URLs.
Password	Set a password for authentication in HTTP command URLs.

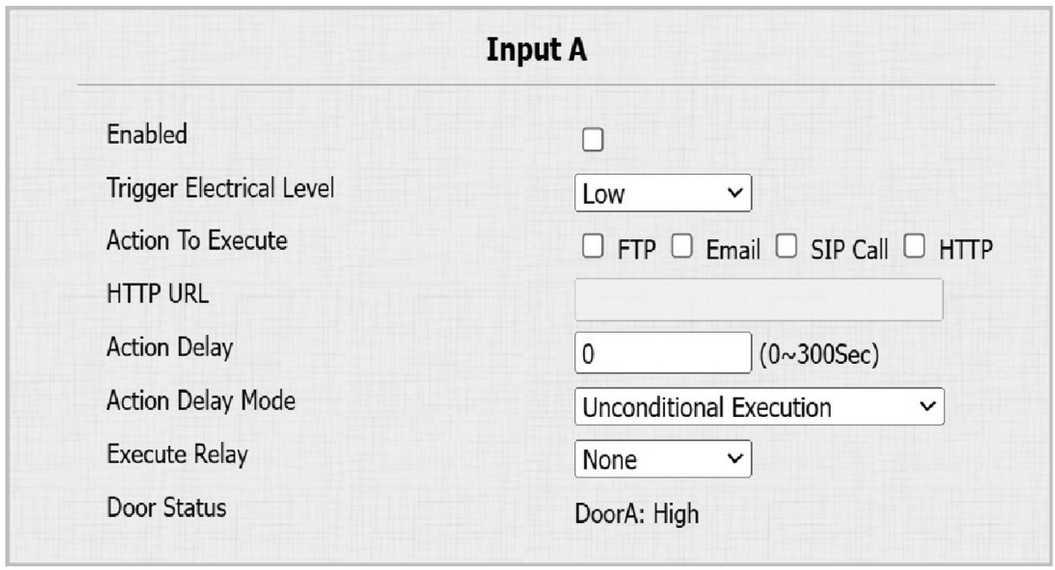
TIP: Here is an HTTP command URL example for relay triggering.

NOTE: The HTTP format for relay triggering varies depending on whether the doorbell's high secure mode is enabled.

Unlock by Exit Button

When users need to open the door from inside by pressing the **Exit** button, you need to set up the *Input* terminal that matches the **Exit** button to activate the relay for the door access.

To setup an Input, navigate to the **Access Control > Input** interface.



Enabled	To use a specific input interface.
Trigger Electrical Level	Set the input interface to trigger at a low or high electrical level.

Door Access Schedule Management

This table continued from previous page...

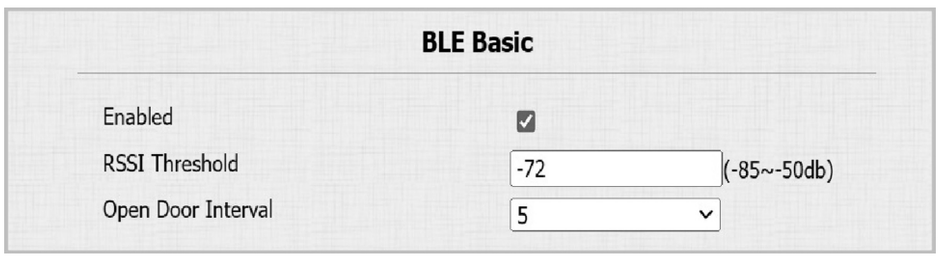
Action To Execute	Set the desired actions that occur when the specific Input interface is triggered. ◊ **FTP:** Send a screenshot to the preconfigured FTP server. ◊ **Email:** Send a screenshot to the preconfigured Email address. ◊ **SIP Call:** Call the preset number upon the trigger. ◊ **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
HTTP URL	Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
Action Delay	◊ **Unconditional Execution:** The action will be carried out when the input is triggered. ◊ **Execute If Input Still Triggered:** The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
Execute Relay	Specify the relay to be triggered along with the input triggering.
Door Status	Display the status of the input signal.

BLE

Only compatible with *Nice Home Management*, see **Integration Note** for details.

The Bluetooth-enabled doorbell app enables users to enter the door hands-free. They can either open the door with the app in their pockets or wave their phones towards the doorbell as they get closer to the door.

To configure Bluetooth, go to **Access Control > BLE** interface.



RSSI Threshold	Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
Open Door Interval	Set the interval (sec) between consecutive Bluetooth door access attempts.

Monitor and Image

MJPEG and RTSP are the primary monitoring stream types discussed in this chapter.

MJPEG (Motion JPEG) is a video compression format that uses JPEG images for each video frame. Video doorbell devices display live streams on the web interface and capture monitoring screenshots in MJPEG format.

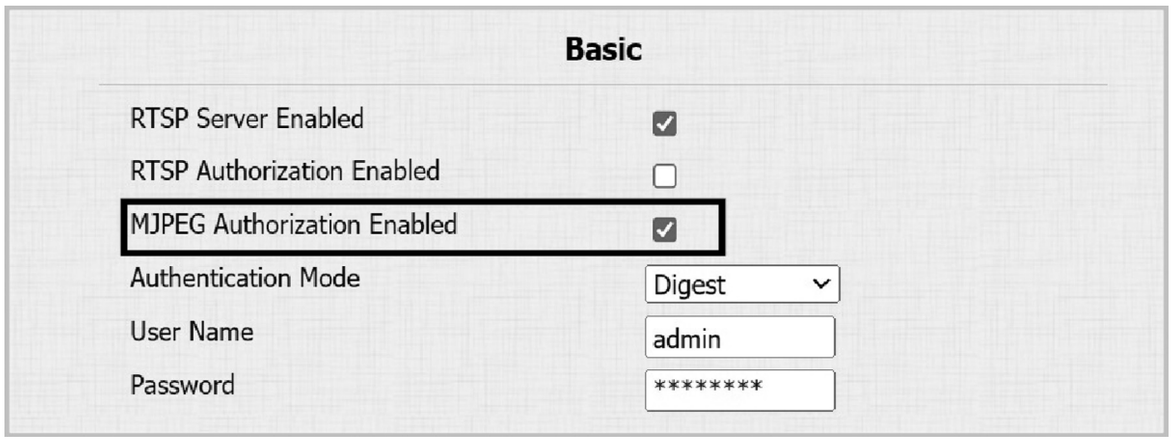
Settings related to MJPEG determine video quality and the on/off status of the live stream function.

RTSP (Real Time Streaming Protocol) can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format is **rtsp:// Device's IP/live/ch00_0**

ONVIF (Open Network Video Interface Forum) enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

MJPEG Image Capturing

You can take a monitoring image in MJPEG format with the device. To do this, you need to turn on the MJPEG function and choose the image quality. To set it up, navigate to **Surveillance > RTSP > Basic** interface.



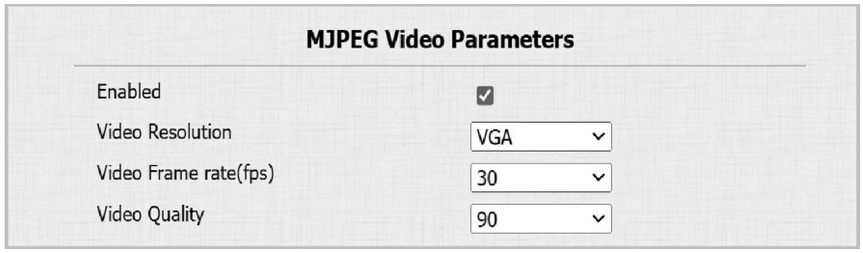
- **MJPEG Authorization Enabled:** Once enabled, accessing the doorbell's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username and RTSP Password.

TIP:

- To view a dynamic stream, use the URL: **http://device_IP:8080/video.cgi**.
- For capturing a screenshot, use the following URLs with the image formats varying accordingly:
  - ◊ **http://device_IP:8080/picture.cgi**
  - ◊ **http://device_IP:8080/picture.jpg**
  - ◊ **http://device_IP:8080/jpeg.cgi**

For example, if you want to capture the JPG format image of the doorbell with the IP address 192.168.1.104, you can enter **http://192.168.1.104:8080/picture.jpg** on the web browser.

You can set up the MJPEG video parameters in the MJPEG Video Parameters section.



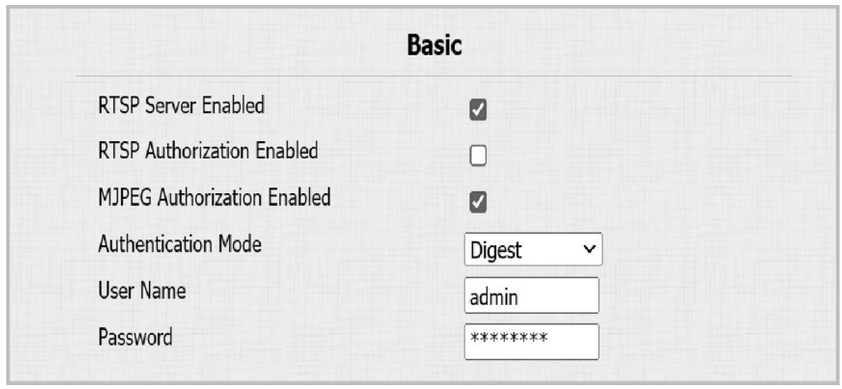
Video Resolution	Specify the image resolution, varying from the lowest CIF (352×288 pixels) to the highest 1080P (1920x1080 pixels).
Video Frame rate(fps)	Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
Video Quality	The video bitrate ranges from 50 to 90.

RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

You are required to set up the RTSP function on the device web **Surveillance > RTSP > Basic** interface in terms of RTSP Authorization, authentication, password, etc before you can use the function.

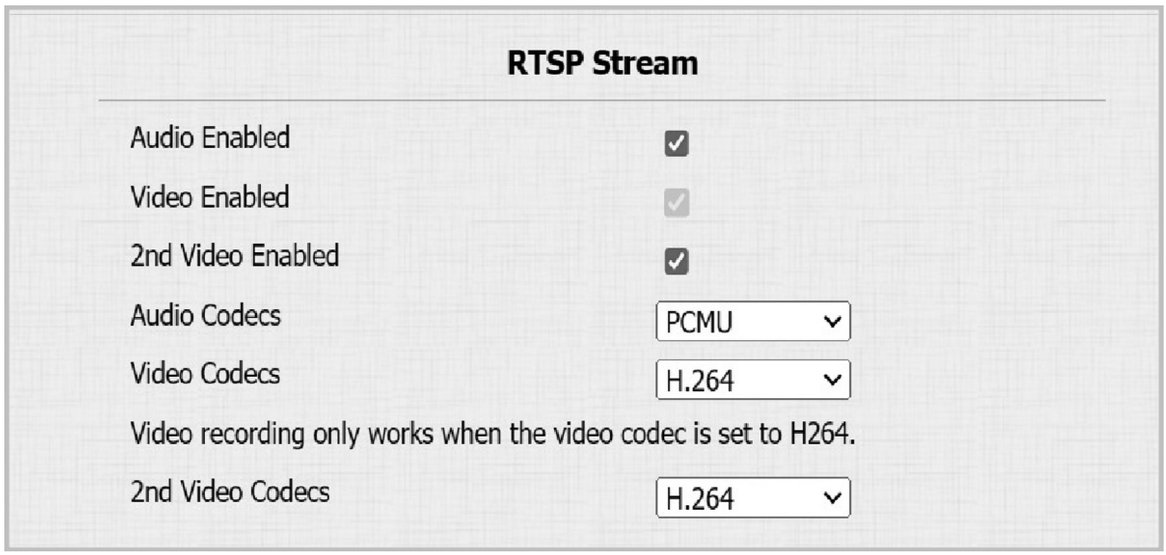


RTSP Authorization Enabled	Once enabled, configure RTSP Authentication Mode, RTSP Username and RTSP Password. These credentials are required for accessing the doorbell's RTSP stream from other intercom devices like indoor monitors.
Authentication Mode	Select between *Basic* and *Digest*. Basic is the default authentication type. ◊ **Basic:** The username and password are joined in the form "username: password", followed by the Base64 encoding before being sent to the server. The server then decrypts the string to retrieve the username and password for verification. ◊ **Digest:** Use hashing instead of the easily reversible Base64 encoding. A token is used for verification.
User Name	Set the username for authorization.
Password	Set the password for authorization.

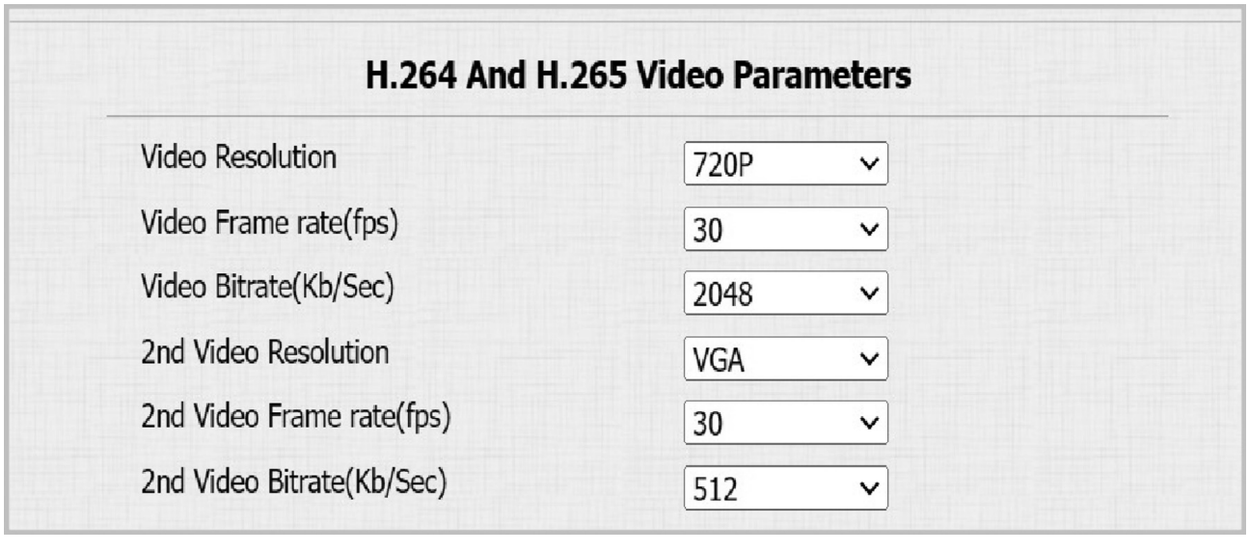
RTSP Stream Setting

The RTSP stream can use either H.264 or MJPEG as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate and other settings.

Go to **Surveillance > RTSP > RTSP Stream** interface.



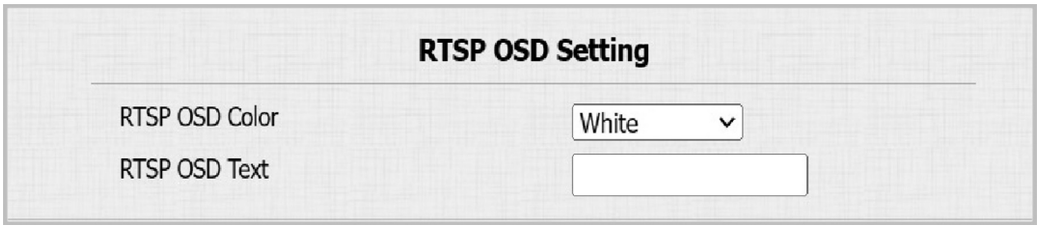
Audio Enabled	Decide whether the RTSP stream has sound.
Video Enabled	Decide whether the RTSP stream has video. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
2nd Video Enabled	Video doorbell supports two RTSP streams.
Audio Codecs	Choose a suitable audio codec for RTSP audio.
Video Codecs	Specify the video compression formats. ◊ **H.264:** Offer highly efficient compression, but this setting has a higher latency and computational load. ◊ **H.265:** Offer superior compression efficiency and support for higher resolutions, but this setting has higher computational requirements and potential compatibility issues. ◊ **MJEPG:** Offer improved quality, but it has inefficient compression. You can set up the video parameters for H.264 and H.265 in the **H.264 and H.265 Video Parameters** section.



Video Resolution	Specify the image resolution, varying from the lowest CIF (352×288 pixels) to the highest 1080P (1920x1080 pixels).
Video Frame rate(fps)	Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
Video Bitrate(Kb/Sec)	The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but it results in higher file sizes and more bandwidth. The default is *2048 kbps*.
2nd Video Resolution	Specify the image resolution for the second video stream channel.
2nd Frame rate(fps)	Set the frame rate for the second video stream channel.
2nd Video Bitrate(Kb/Sec)	Set the bit rate for the second video stream channel. The default is *512 kbps*.

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture. Set it up on the web **Surveillance > RTSP > RTSP OSD Setting** interface.

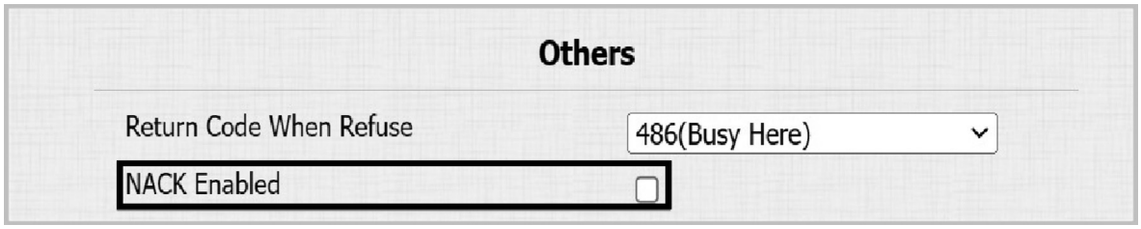


RTSP OSD Color	There are five color options, White, Black, Red, Green, and Blue for RTSP watermark text.
RTSP OSD Text	Customize the watermark text.

NACK

NACK (Negative Acknowledgment) indicates a failure or error in data transmission or processing. It is used to request retransmission or signal the failure to the sender for ensuring data integrity.

To enable NACK, navigate to the **Intercom > Call Feature > Others** interface.



- **NACK Enabled:** It can be used to prevent losing data packets in the weak network environment when discontinued and mosaic video images occur.

ONVIF

You can access the real-time video from the device's camera from Nice Home Management, a web browser or other third-party devices like NVR (Network Video Recorder). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

To setup ONVIF, go to the **Surveillance > ONVIF** interface.

Discoverable	When enabled, the video from the doorbell camera can be searched by other devices.
User Name	Set the username required for accessing the doorbell's video stream on other devices. The default User Name is *admin*.
Password	Set the password required for accessing the doorbell's video stream on other devices. The default Password is *admin*.

TIP: Once the settings are configured, simply enter the ONVIF URL to access the video stream on the third-party device: **http://Device's IP:80/onvif/device_service**.

SD Card for Storing Videos

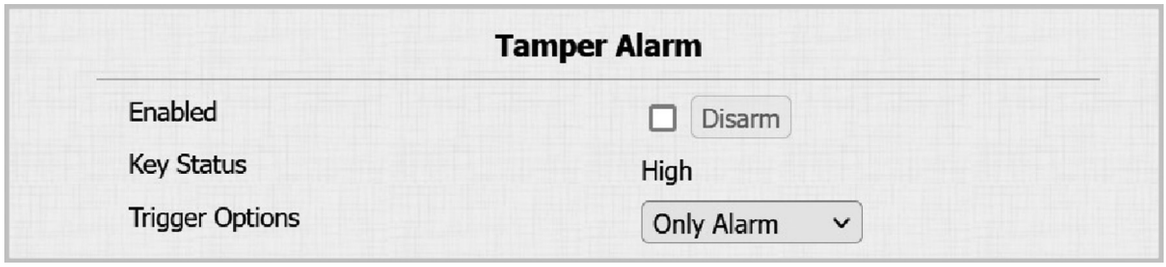
The device can be inserted into an SD card for storing motion and call videos.

To check the videos, go to **Device > SD Card** interface. When there is not enough space in the SD card to record the next video, the system automatically deletes the oldest video.

Tamper Alarm Setting

The tamper alarm function prevents anyone from removing the devices without permission. It does this by setting off the tamper alarm and making calls to a designated location when the device detects a change in its gravity value from the original one.

Seup the *Tamper Alarm* on the **Security > Basic > Tamper Alarm** interface. Click *Disarm* to clear the alarm.



- **Trigger Options:** Select what can be triggered when the gravity sensor is triggered.

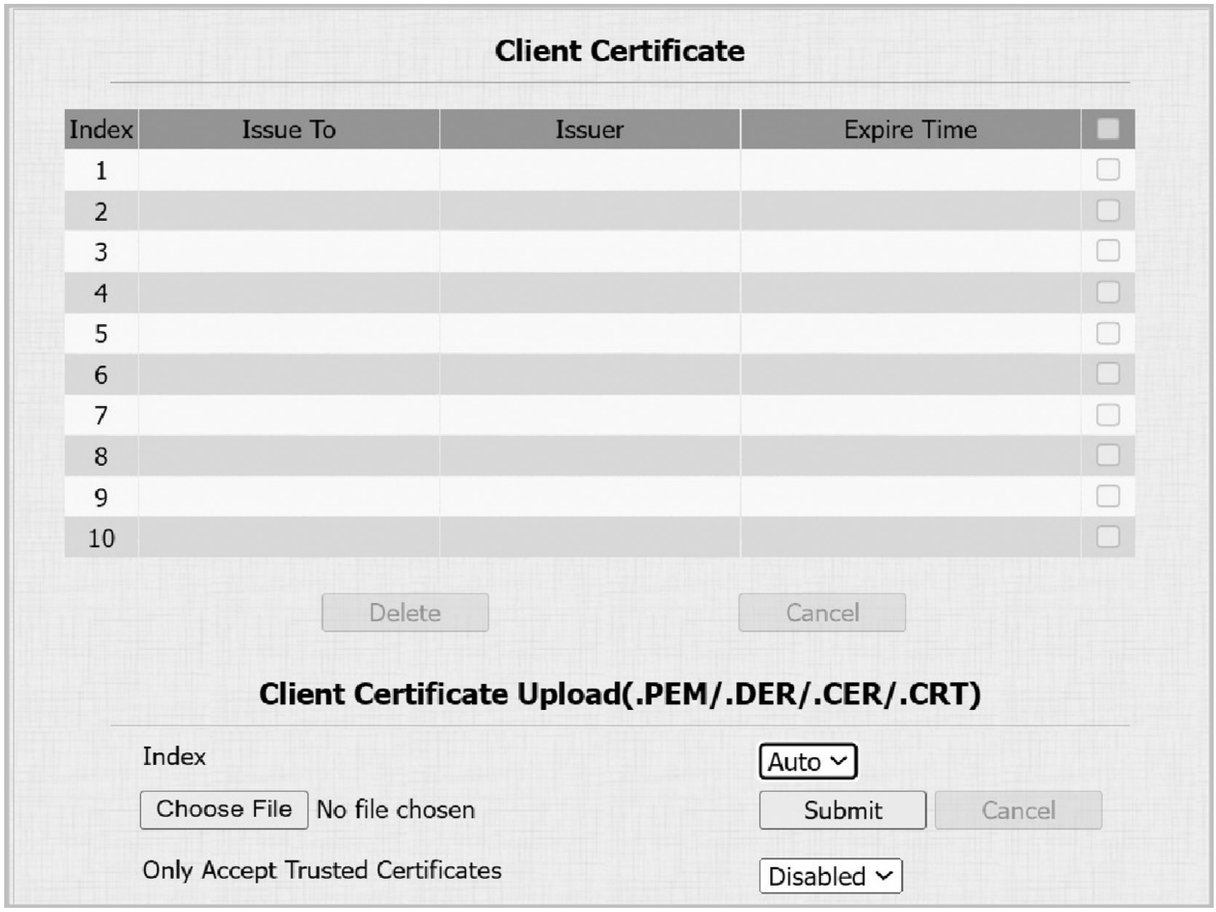
Client Certificate Setting

Certificates ensure communication integrity and privacy. To use the SSL protocol, you need to upload the right certificates for verification.

Client Certificate

This certificate verifies the server to the video doorbell when they want to connect using SSL. The doorbell verifies the server's certificate against its client certificate list.

Upload and configure the Client Certificate on the **Security > Advanced> Web Server Certificate** interface.



Index:

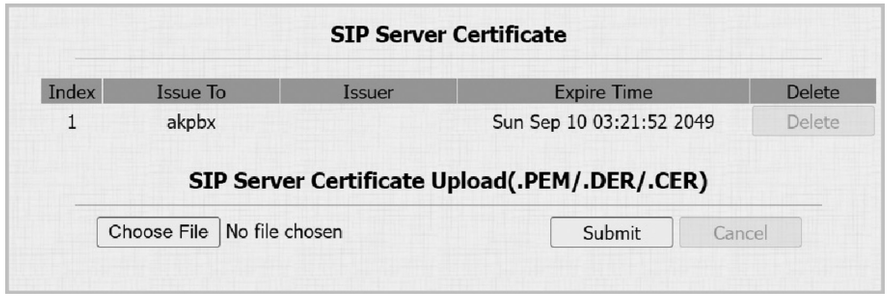
- ◊ **Auto:** The uploaded certificate will be displayed in numeric order.
- ◊ **1 to 10:** The uploaded certificate will be displayed according to the value selected.

- **Choose File:** Click **Choose File** to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, the video doorbell will verify the server certificate based on the client certificate list as long as the authentication succeeds. If set to *Disabled*, the video doorbell will not verify the server certificate whether the certificate is valid or not.

Upload TLS Certificate for SIP Account Registration

Before applying for a SIP account from a SIP or a DNS server using the TLS protocol, you'll need to upload a TLS certificate. This certificate is essential for server authentication.

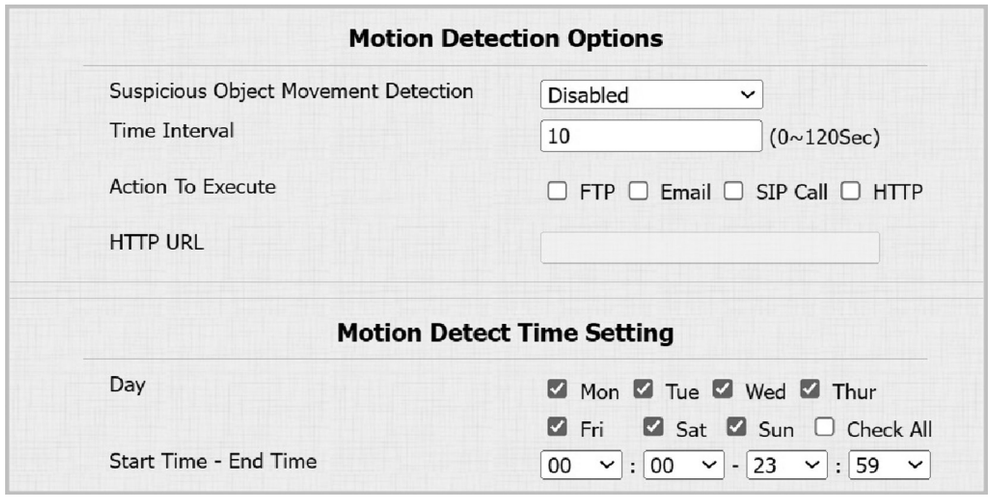
Access the **Security > Advanced** interface to setup the certificate.



Motion Detection

Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved. It activates the system to perform the appropriate action.

Set up motion detection on the **Surveillance > Motion** interface.



Suspicious Object Movement Detection	Select *Video Detection* to enable video-based motion detection during the monitoring of the suspicious moving object.
Time Interval	If you set the default time interval as 10 sec, the motion detection period will be 10 seconds. Assuming that we set the time interval as 10, and the first movement captured can be seen as the start point of the motion detection. If the movement continues through 7 seconds of the 10 second interval, the alarm will be triggered at 7 seconds (the first trigger point). Motion detection action can be triggered (sending out notification) anywhere between 7-10 seconds once the movement is detected. A 10-second interval is a complete cycle of motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the Time interval minus three.

Action To Execute	Set the desired actions that occur when suspicious movement is detected. ◊ **FTP:** Send a screenshot to the preconfigured FTP server. ◊ **Email:** Send a screenshot to the preconfigured Email address. ◊ **SIP Call:** Call the preset number upon trigger. ◊ **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
HTTP URL	Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

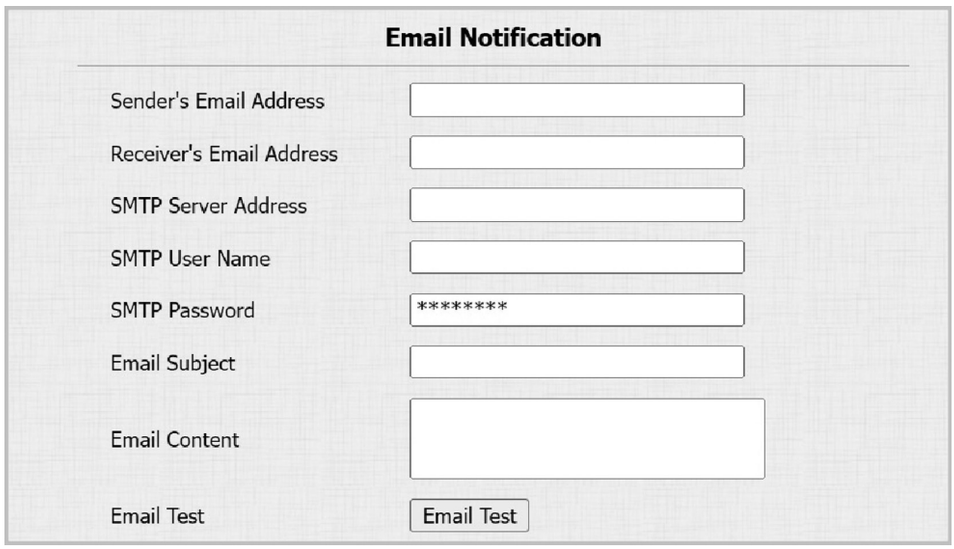
Security Notification

A security notification informs users or security personnel of any breach or threat that the doorbell detects. For example, if the doorbell detects something unusual, the system sends a notification to users or security through email, phone call or other methods.

To set up security notifications, go to **Setting > Action** interface.

Email Notification

Set up email notification to receive screenshots of unusual motion from the device.

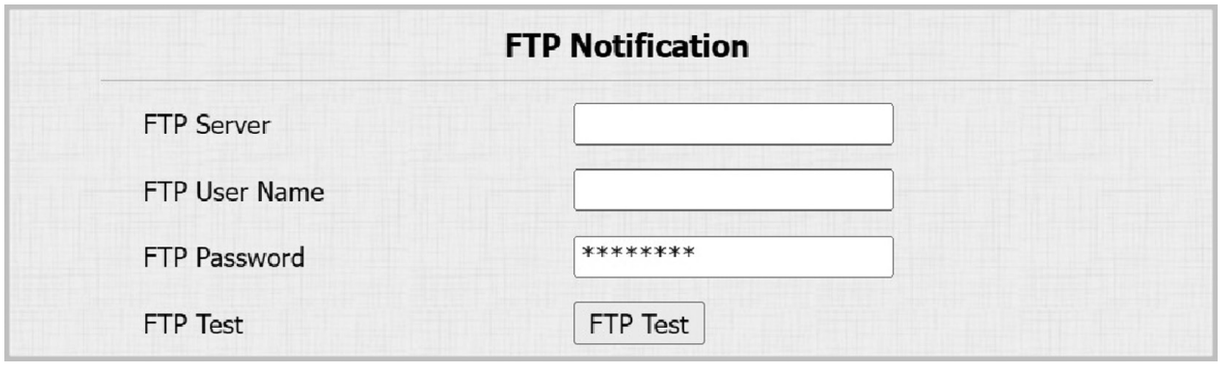


SMTP Server Address	The SMTP server address of the sender.
SMTP User Name	The SMTP username is usually the same as the sender's email address.
SMTP Password	The password of the SMTP service is the same as the sender's email address.
Email Test	Used to test whether the email can be sent and received.

FTP Notification

To get notifications through FTP server, you need to set up the FTP settings. The doorbell will upload a screenshot to the specified FTP folder if it senses any unusual motion.

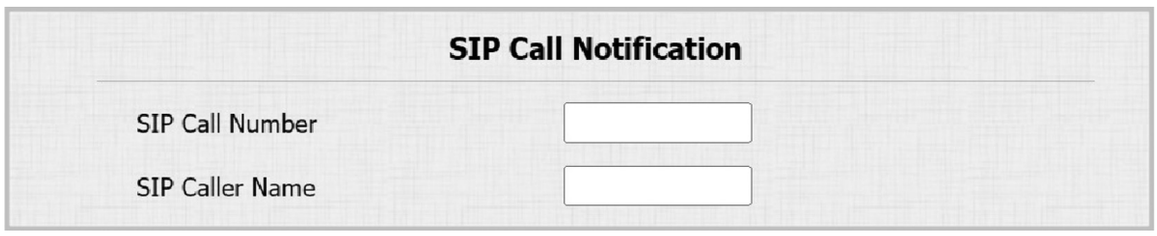
Setup using **FTP Notification**.



FTP Server	Set the address (URL) of the FTP server.
FTP User Name	Enter the user name to access the FTP server.
FTP Password	Enter the password to access the FTP server.
FTP Test	Used for testing whether the FTP notification can be sent and received by the FTP server.

SIP Call Notification

In addition to FTP and Email notification, the doorbell can also make a SIP call when some feature action is triggered.



Set it up in the SIP Call Notification section.

HTTP Notification

You can also set up an HTTP message sent to the HTTP server.

Set up the HTTP URL when configuring desired actions. The URL format is http://HTTP server's IP/ Message content.

Action URL

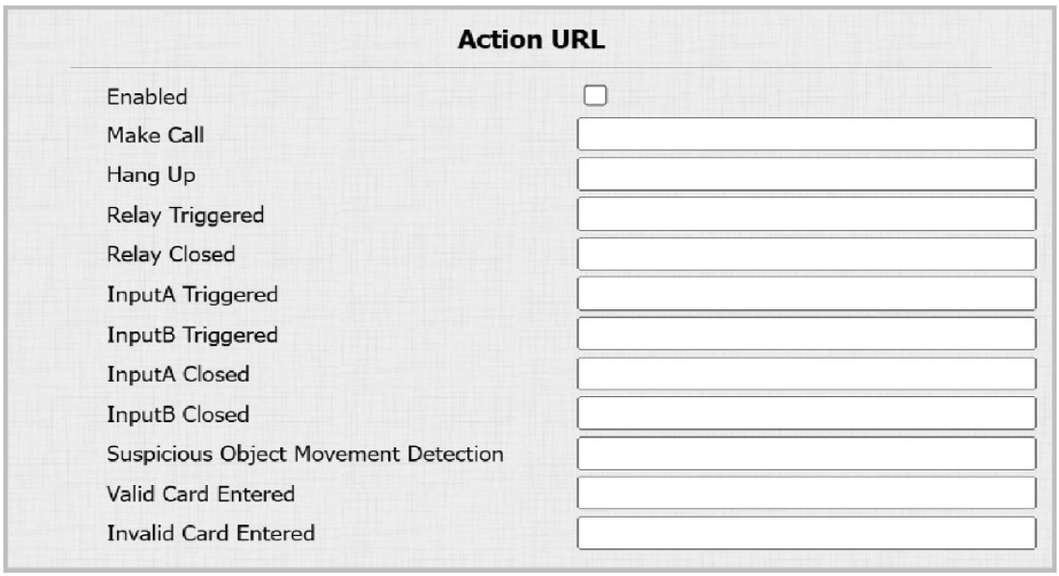
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, or RF card access changes.

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	Suspicious Object Movement Detection	$active_user	Http://server ip/active_user=$active_user
8	Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
9	Invalid Card En-tered	$card_sn	Http://server ip/invalidcard=$card_sn

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

To set it up, go to the Setting > Action URL interface.



Security

Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the *Real-time Transport Protocol* (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance and replay protection.

Setup *Encryption* on the web **Account > Advanced > Encryption** interface.

- **Voice Encryption(SRTP):** Choose *Disabled*, *Optional* or *Compulsory*. If *Optional* or *Compulsory* is selected, the voice during the call is encrypted and you can grab the RTP packet to view it.

User Agent

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

To setup *User Agent*, navigate to the **Account > Advanced > User Agent** interface.

- **User Agent:** Device name by default.

Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, but you'll be required to login again by entering the user name and the passwords for security purposes or for the convenience of operation.

To setup *Session Time Out*, go to **Security > Basic > Session Time Out** interface.

High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods and more.

Enable it on the **Security > Basic > High Security Mode** interface.

Important Notes

1. By default, the *High Security Mode* is disabled when you upgrade the device from a version without the mode to a version with the mode. But if you reset the device to its factory settings, the mode is enabled by default.
2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.
   - ◊ 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 for relay triggering varies depending on whether high secure mode is enabled or disabled.
   - ◊ If the mode is enabled, the device only accepts the new HTTP formats below for door opening.
   - ◊ http://username:password@deviceIP/fcgi/OpenDoor? action=OpenDoor&DoorNum=1
   - ◊ http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is disabled, the device can use both the new formats above and the old format below:

- ◊ http://deviceIP/fcgi/do? action=OpenDoor&UserName=username&Password=password&DoorNum=1

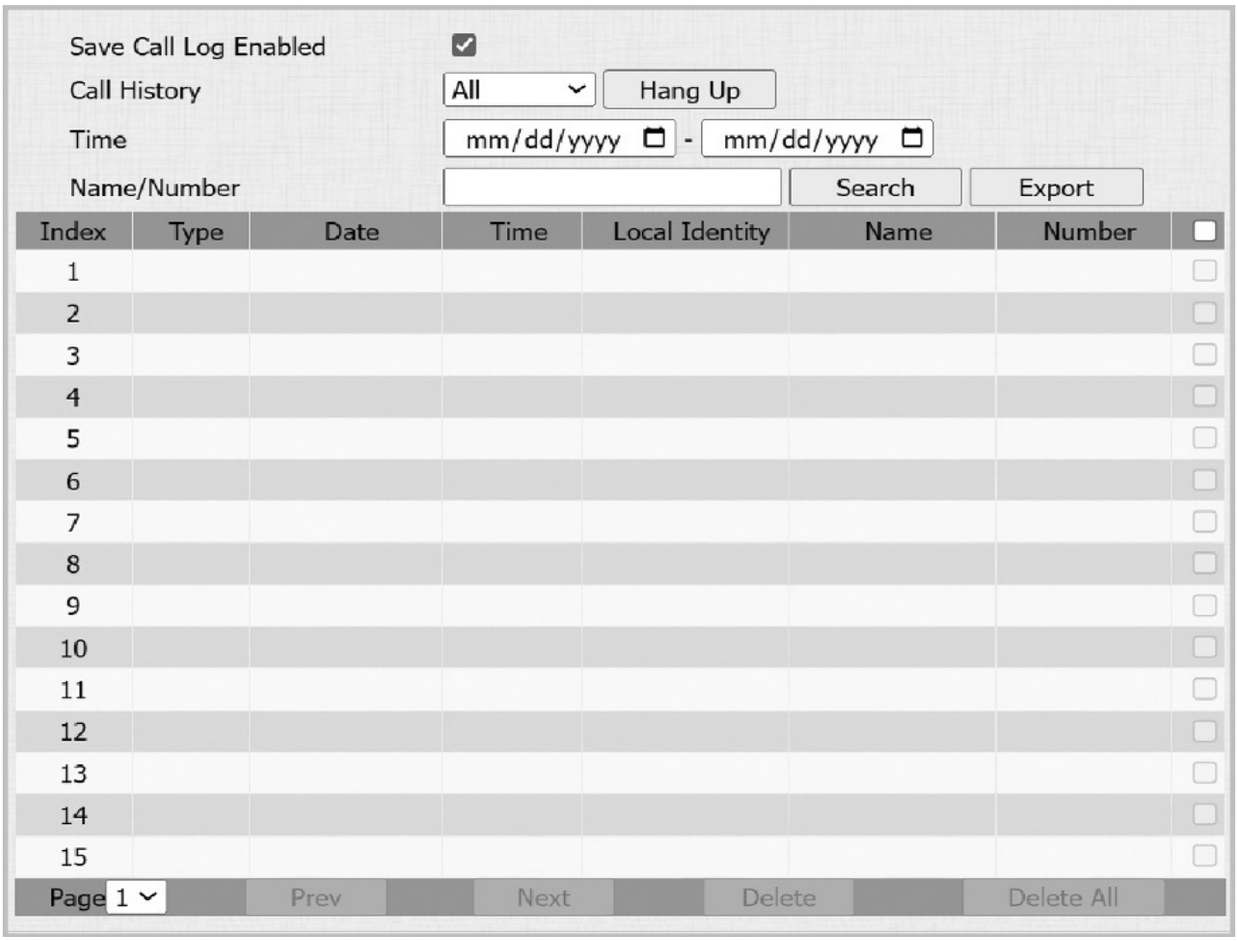
4. It cannot import/export configuration files in tgz. format between a device with high security mode and another device without high security mode.

Logs

Call Logs

To check dial-out, received and missed calls within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

Go to the **Intercom > Call** Log interface.



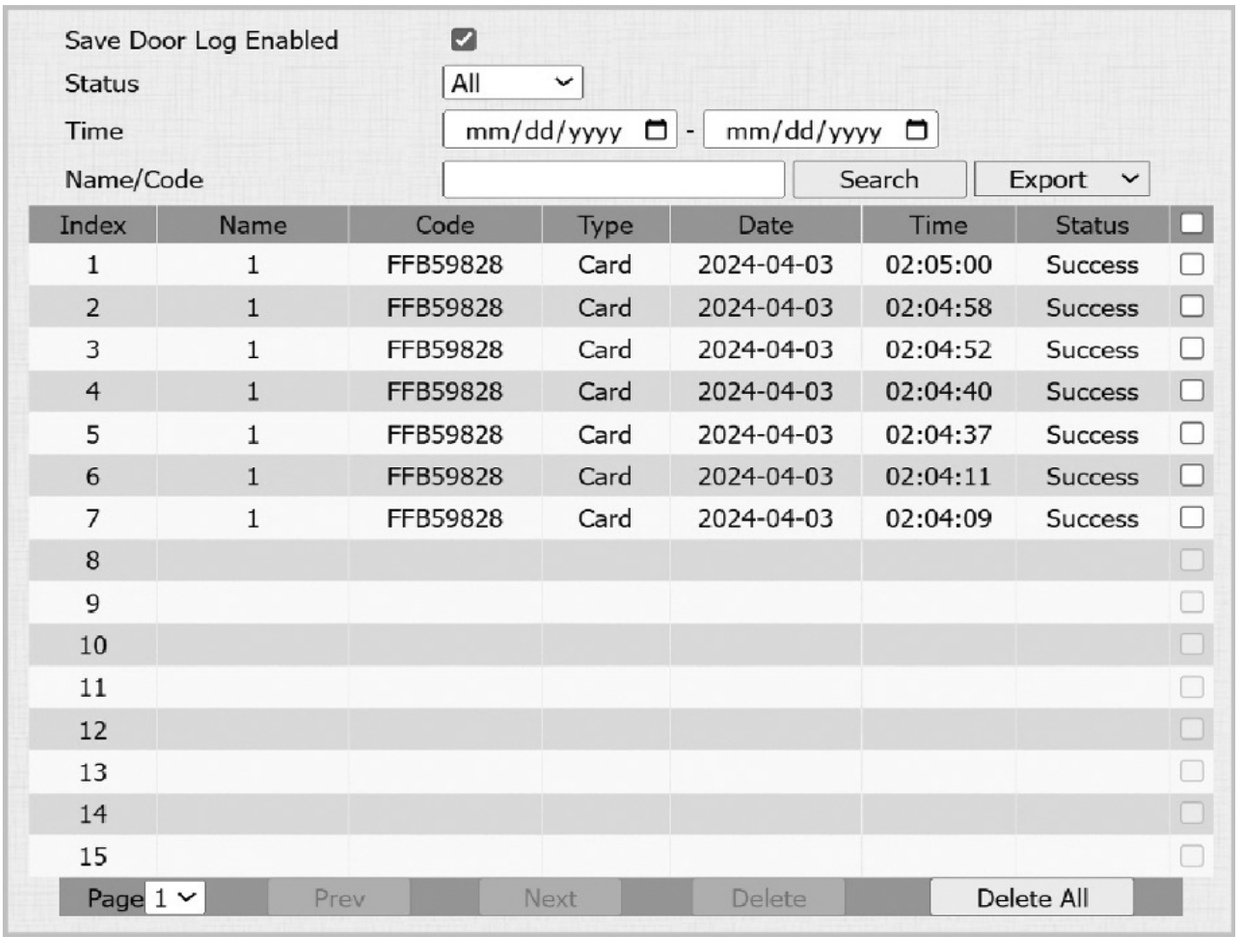
Call History	There are four specific types of call logs: *All*, *Dialed*, *Received* and *Missed*.
Time	Search the desired call log by entering a certain period.
Name/Number	Search the desired call log by entering the name and number.

Logs

Door Logs

To search and review various types of door access history, simply check the door logs on the device's web interface.

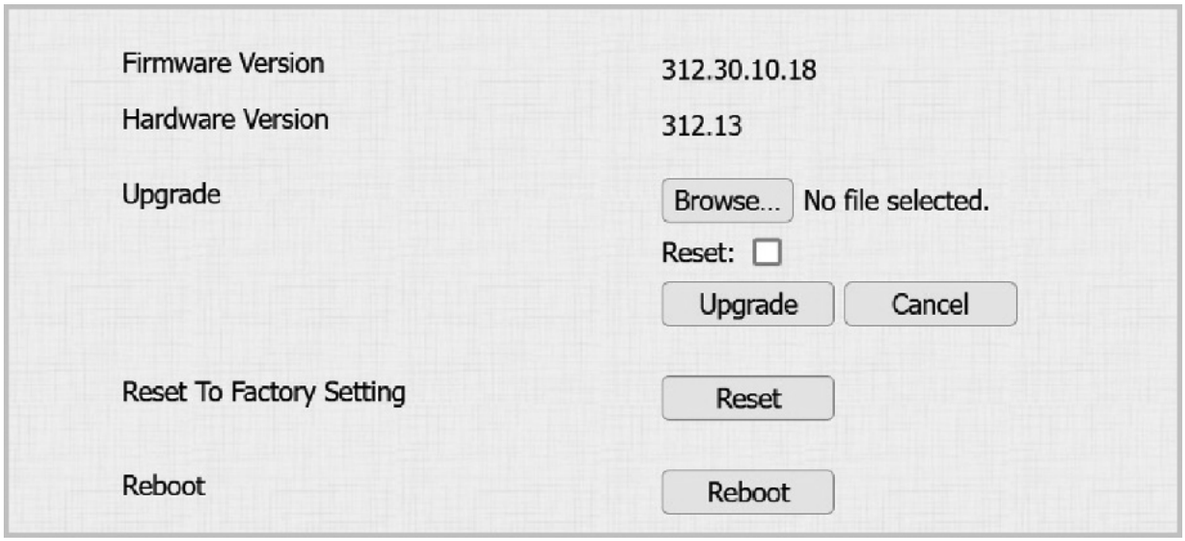
Go to the **Access Control > Door Log** interface.



Status	*Display All*, *Successful* and *Failed* door-opening records.
Time	Search the desired call log by entering a certain period.
Name	Display user name. If it is an unknown key or card, it will display *Unknown*.
Code	If the door is opened by RF cards, the card code will be displayed. If the door is opened by an HTTP command, it will be empty.
Type	Display the access methods.

Firmware Upgrade

Video doorbell devices can be upgraded on the device web interface. Upgrade the device on the **Upgrade > Basic** interface.



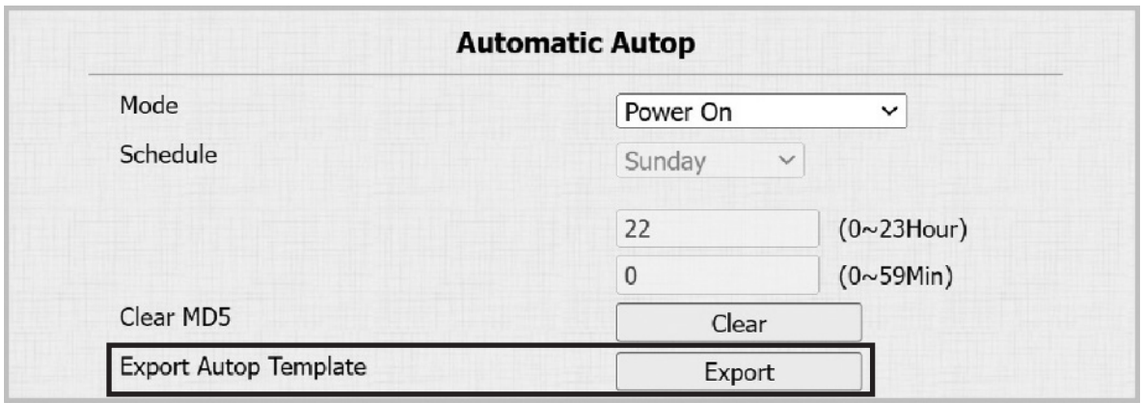
NOTE: The upgrade files should be in .rom format.

- **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

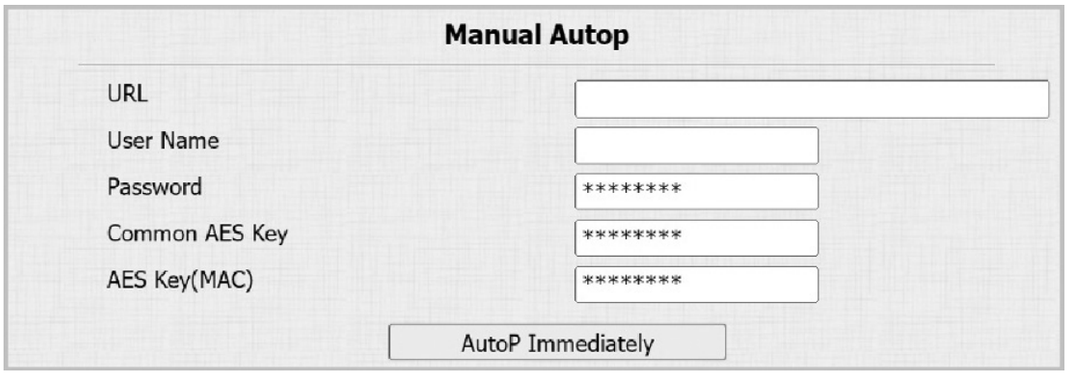
You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device will perform the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP and HTTPS are the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

To setup *Automatic Autop*, download the template on **Upgrade > Advanced > Automatic Autop** interface first.



Auto-provisioning via Configuration File

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



URL	Specify the TFTP, HTTP, HTTPS or FTP server address for the provisioning.
Username	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.

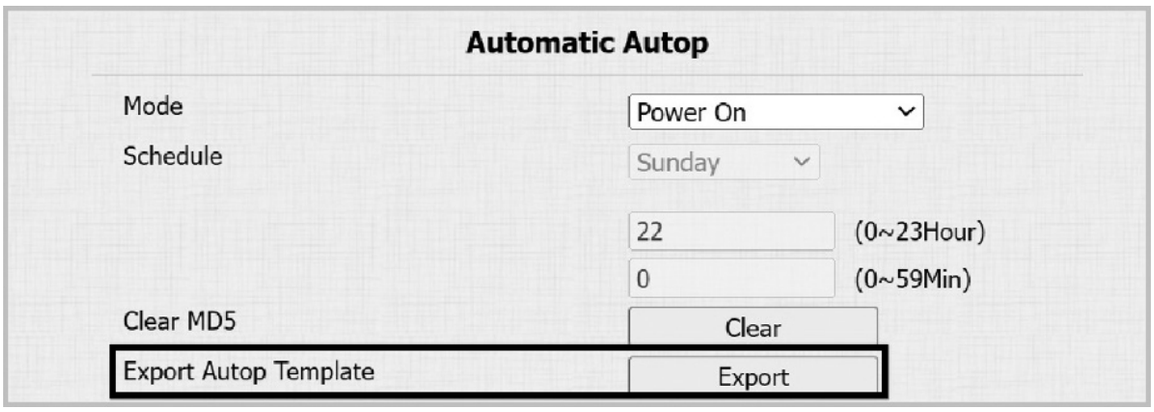
NOTE:

- 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)

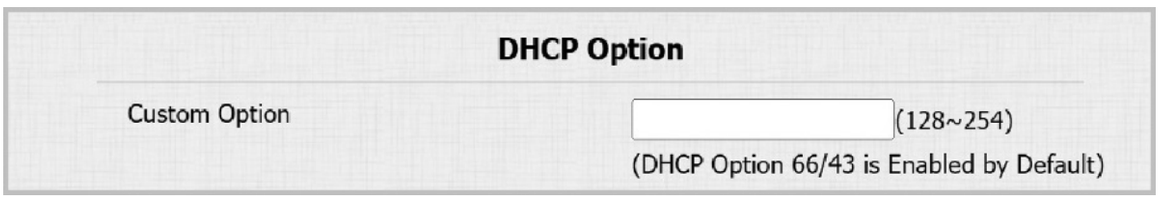
Auto-provisioning via Configuration File

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

Go to the **Upgrade > Advanced > Automatic Autop** interface.



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

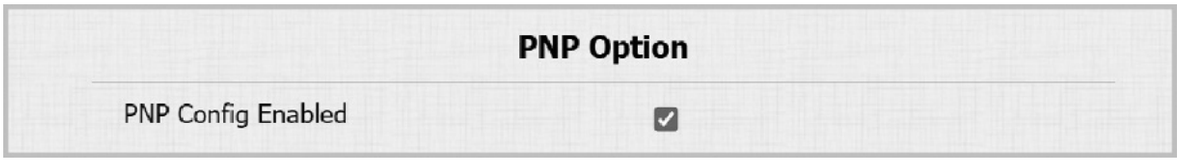


Custom Option	Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
DHCP Option 43	If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is automtically set within the software. Configure the DHCP server with option 43 along with upgrade server URL.
DHCP Option 66	If none of the above is set, the device software will automatically use DHCP Option 66 to get the upgrade server URL. Configure the DHCP server with option 66 along with the upgrade server URL.

PNP Configuration

PNP (Plug and Play) 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.

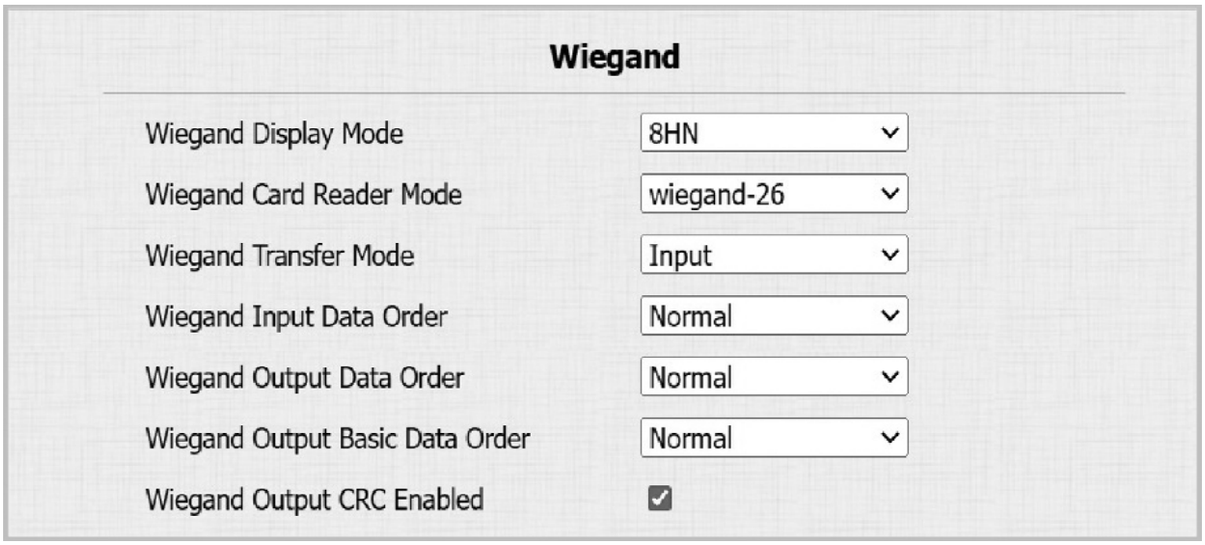
Setup PNP on the web **Upgrade > Advanced > PNP Option** interface.



Integration with Wiegang & Milestone

Integration via Wiegand

The device can be integrated with third-party devices via Wiegand. Set it up on the **Access Control > Card Setting > Wiegand** interface.



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 access control terminal and the third- party device. It's automatically configured.
Wiegand Transfer Mode	◊ **Input:** The device serves as a receiver. ◊ **Output:** The device serves as a sender. If users can only open the door by swiping an RF card, select the Wiegand transfer mode as *Output*. ◊ **Convert To Card No. Output:** The device serves as a sender. If users are assigned multiple door-opening methods, select the Wiegand transfer mode as *Convert To Card No. Output*.
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	◊ **Normal:** The card number is displayed as received. ◊ **Reversed:** The order of the card number is reversed.
Wiegand Output CRC Enabled	Set the sequence of the Wiegand output data. ◊ **Normal:** The data is displayed as received. ◊ **Reversed:** The order of the data bits is reversed.
Wiegand Output CRC Enabled	It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.

Integration with Third Party Device

Integration with Milestone

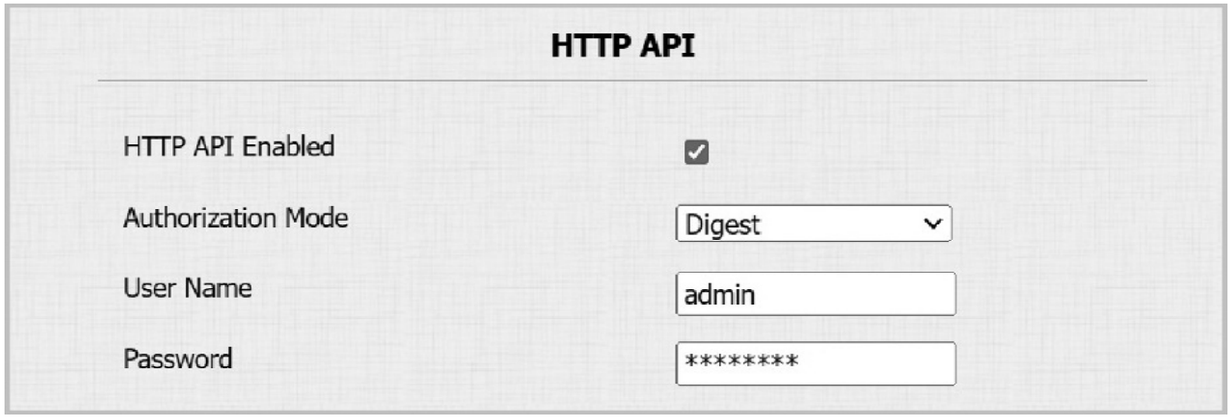
If you want the doorbell to be monitored by Milestone or any third- party devices that have been integrated with Milestone, you need to enable the feature.

Enable it using the **Surveillance > ONVIF > Advanced Setting** interface.

Integration via HTTP API

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

Setup the API on the web **Security > HTTP API** interface.



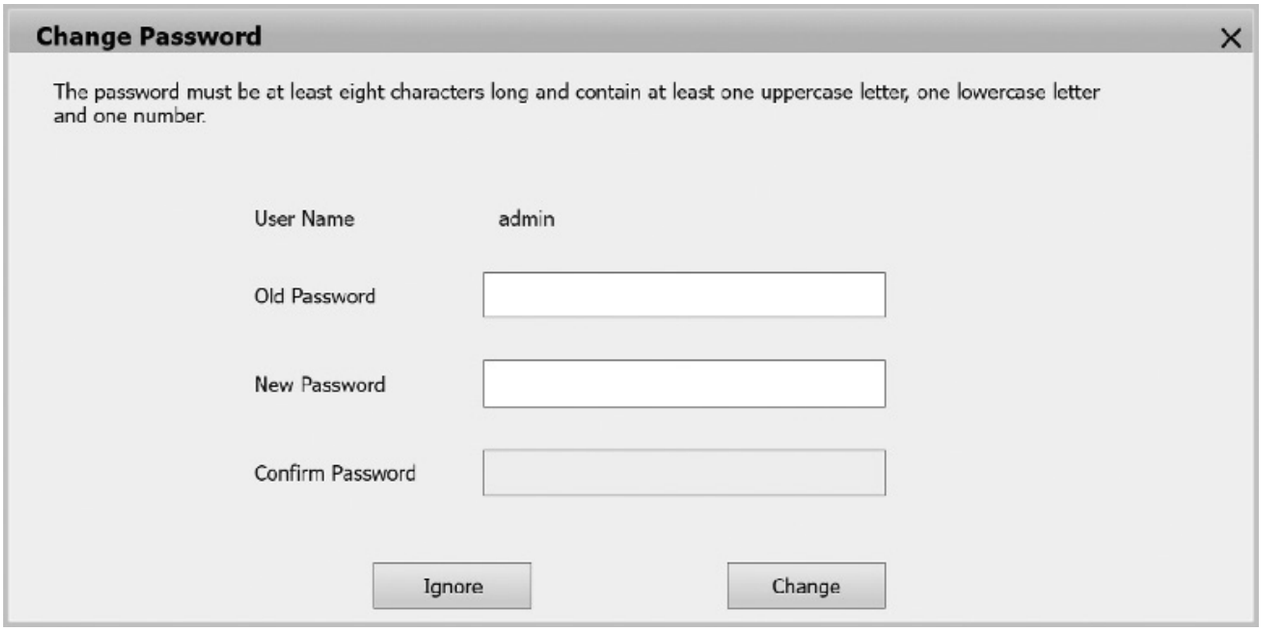
Enabled	Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
Authorization Mode	The default setting is *Digest*. You are required to fill in the username and password 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 user name for authentication. The default is *admin*.
Password	Enter the password for authentication. The default is *admin*.

Password Configuration

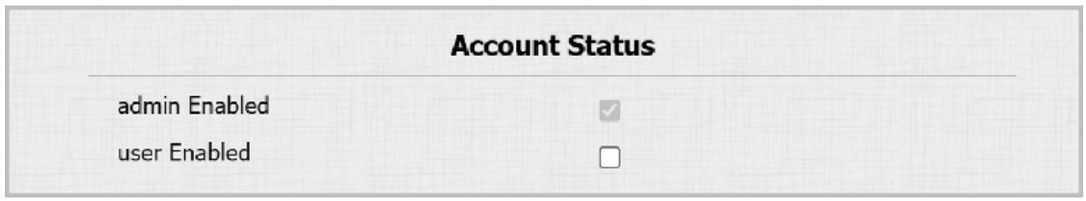
You can modify the device web password for both the administrator account and the user account.

To setup, go to **Security > Basic > Web Password Modify** interface.

Click **Change Password** to modify the password.



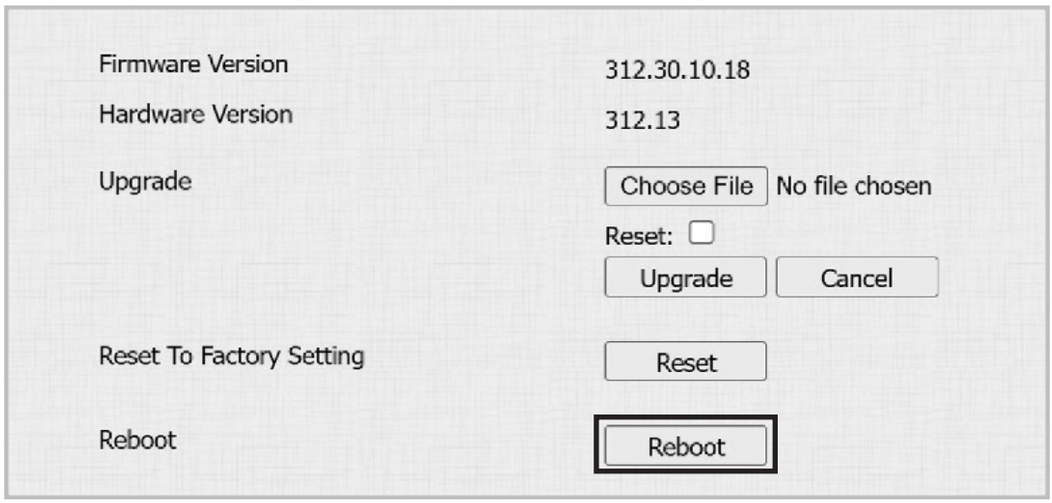
To enable or disable the user account, scroll to the **Account Status** section.



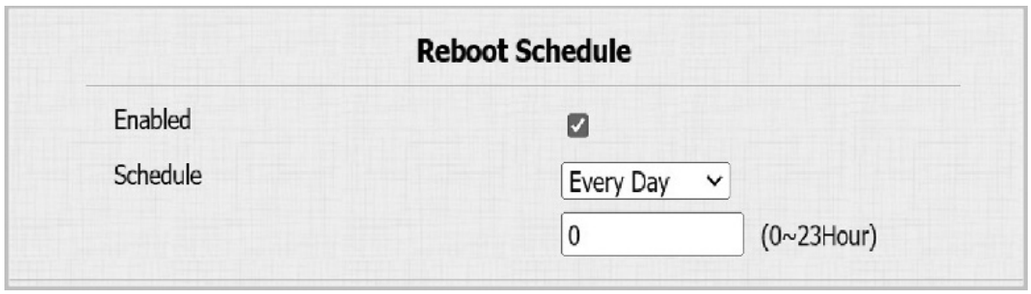
System Reboot and Reset

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 **Upgrade > Basic** interface.

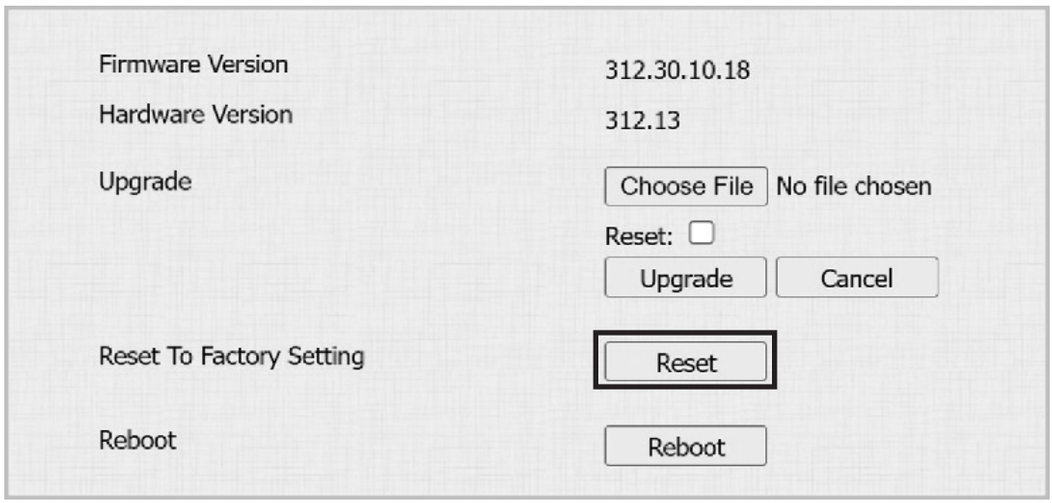


To set up the schedule, go to the **Upgrade > Advanced** interface.



Reset

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



Technical Support
760-438-7000
Monday - Friday, 6:00 a.m. – 4:00 p.m. PST

Nice North America
c/o Customer Service
5919 Sea Otter Place, Ste. 100
Carlsbad, CA 92010

Nice **Niceforyou.com**

10034943 Rev-B X1