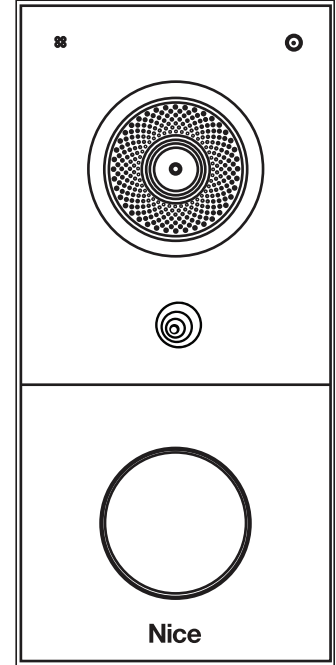


EL-DB-WP

EL-DB-2W



Video Doorbell

Administrator Manual

Nice

Contents

Model Specification and Differences	4
Introduction to Configuration Menu	5
Access the Device	5
Obtain the Device's IP Address	5
Access the Device	6
Access the Device Setting	6
Language and Time Setting	7
Language Setting	7
Time Setting	7
LED Setting	9
LED Light Setting	9
LED Light Status	9
LED Setting on Card Reader Area	10
Volume and Tone Configuration	11
Volume and Tone Configuration	11
Volumes	11
Open Door Tones	11
Upload Tone Files	12
Network Setting	13
Network Status	13
Device Network Configuration	13
Device Deployment in Network	14
NAT Setting	14
Device Web HTTP Setting	15
Intercom Call Configuration	16
IP Call Configuration	16
SIP Call Configuration	16
SIP Account Registration	17
SIP Server Configuration	18
Outbound Proxy Server	18
Data Transmission Type	19
SIP Hacking Protection	19
Audio & Video Codec Configuration	20
Audio Codec	20
Video Codec	20
Video Codec for IP Direct Calls	21
Configure DTMF Data Transmission	22
Access Allowlist Configuration	23
Relay Setting	24
Relay Switch Setting	24
Door Access Schedule Management	25
Configure Door Access Schedule	25
Create Door Access Schedule	25
Import and Export Door Access Schedule	26
Relay Schedule	26
Door Unlock Configuration	27
Unlock by RF Cards	27
Access Settings	28
RF Card Code Format	28
Events Triggered by Using RF Cards	29
Mifare Card Encryption	29
NFC Card	29
Unlock by DTMF Code	30
DTMF White List	30
Unlock by HTTP Command	31
Unlock by Exit Button	31
Relay by Bluetooth	32
Monitor and Image	33

Contents

MJPEG Image Capturing	33
RTSP Stream Monitoring	34
RTSP Basic Setting	34
RTSP Stream Setting	35
RTSP OSD Setting	36
NACK	37
ONVIF	37
SD Card for Storing Videos	37
Security	38
Tamper Alarm Setting	38
Client Certificate Setting	38
Client Certificate	39
Upload TLS Certificate for SIP Account Registration	40
Motion Detection	40
Security Notification	41
Email Notification	41
FTP Notification	42
SIP Call Notification	42
HTTP Notification	42
Action URL	43
Voice Encryption	44
User Agent	44
Web Interface Automatic Log-out	44
High Security Mode	45
Logs	46
Call Logs	46
Door Logs	47
Firmware Upgrade	48
Static Provisioning	49
PNP Configuration	51
Integration with Wiegand & Milestone	52
Integration via Wiegand	52
Integration with Milestone	53
Integration via HTTP API	53
Password Configuration	54
System Reboot and Reset	55
Reboot	55
Reset	55

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

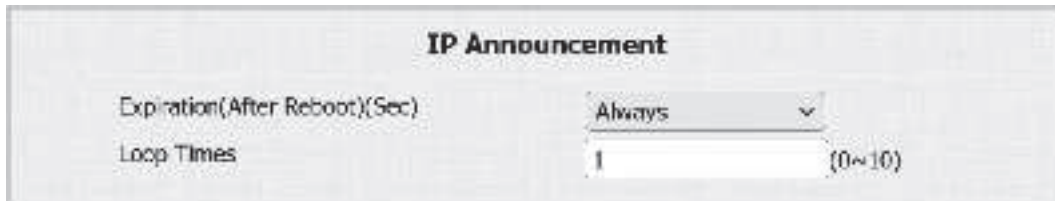
Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, etc.
- **Network:** This section mainly deals with DHCP & static IP settings, RTP port settings, device deployment, etc.
- **Intercom:** This section covers intercom settings, call logs, etc.
- **Surveillance:** This section covers motion detection, RTSP, MJPEG, ONVIF and live streaming.
- **Access Control:** This section covers input control, relay, card settings, private PIN code, Wiegand connection, etc.
- **Device:** This section includes LED, audio, and SD card settings.
- **Setting:** This section includes time & language, action settings, door settings and schedule for access control.
- **Upgrade:** This section covers firmware upgrade, device reset and reboot, configuration file auto-provisioning and fault diagnosis.
- **Security:** This section covers 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.



The screenshot shows a configuration window titled "IP Announcement". It contains two settings: "Expiration(After Reboot)(Sec)" with a dropdown menu set to "Always", and "Loop Times" with a numeric input field set to "1". A range indicator "(0~10)" is shown to the right of the input field.

- **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 Setting

You can 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.

A screenshot of a web-based login interface. At the top, there is a dark gray header bar with the word "Login" in white. Below the header, the form has a light gray background. It contains two labels, "User Name" and "Password", each followed by a white text input field. Below the password field is a checkbox labeled "Remember Username/Password". At the bottom right of the form is a gray button with the text "Login" in white.

NOTE: The Chrome browser is recommended.

Language Setting

You can 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.



The screenshot shows a web interface titled "Web Language". Below the title, there is a label "Mode" followed by a dropdown menu. The dropdown menu is currently set to "English" and has a downward arrow icon.

- **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.



The screenshot shows a web interface titled "NTP". Below the title, there are several settings:

NTP	
Time Zone	GMT+0:00 GMT
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600Sec)
System Time	06:18:04

- **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.

Type

☒ Manual

Date

2024

Year

5

Mon

29

Day

Time

9

Hour

31

Min

41

Sec

☐ Auto

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.

The screenshot shows the 'LED Fill Light' configuration window. It contains three settings: 'Mode' set to 'Auto', 'Min Photoresistor' set to '1500' with a range of '(0~1800)', and 'Max Photoresistor' set to '1600' with a range of '(0~1800)'.

LED Fill Light		
Mode	Auto	
Min Photoresistor	1500	(0~1800)
Max Photoresistor	1600	(0~1800)

- **Mode:**
 - ◇ Auto turns on the LED light automatically.
 - ◇ Always 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.

The screenshot shows the 'Light Of The Button' configuration window. It contains a table with three columns: 'Device Status', 'Color', and 'Display Mode'. Each row represents a different device status and its corresponding LED settings.

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

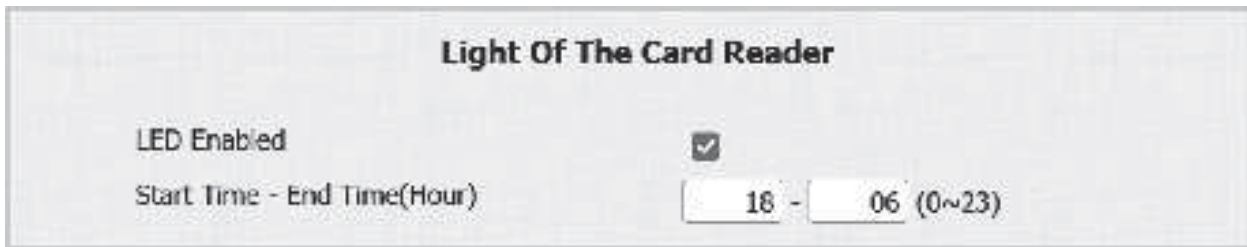
LED Setting

- **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

You can 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.



Light Of The Card Reader

LED Enabled ☒

Start Time - End Time(Hour) - (0~23)

- **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).

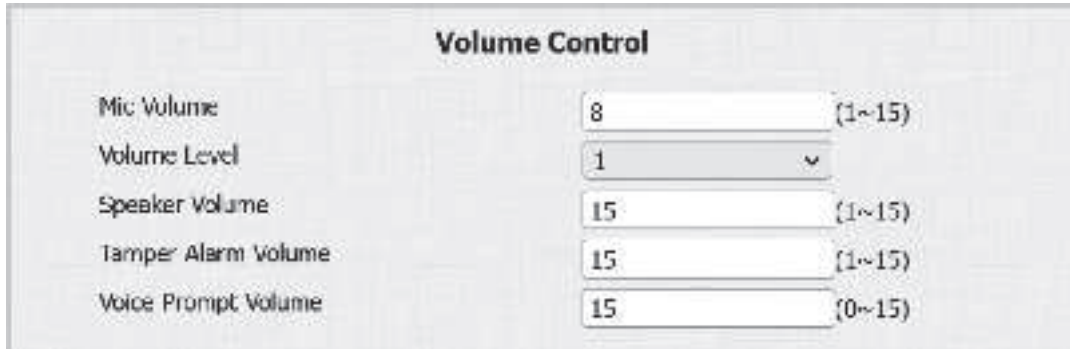
Volume and Tone Configuration

Volume and Tone Configuration

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.

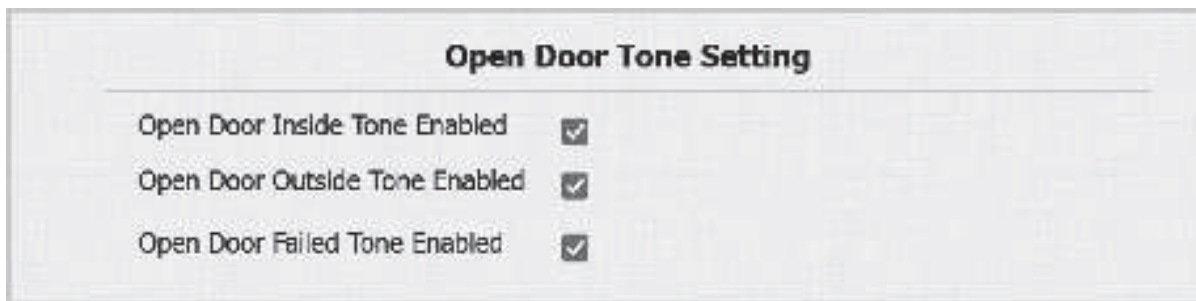


Volume Control		
Mic Volume	8	(1~15)
Volume Level	1	▼
Speaker Volume	15	(1~15)
Tamper Alarm Volume	15	(1~15)
Voice Prompt Volume	15	(0~15)

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

Open Door Tones

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



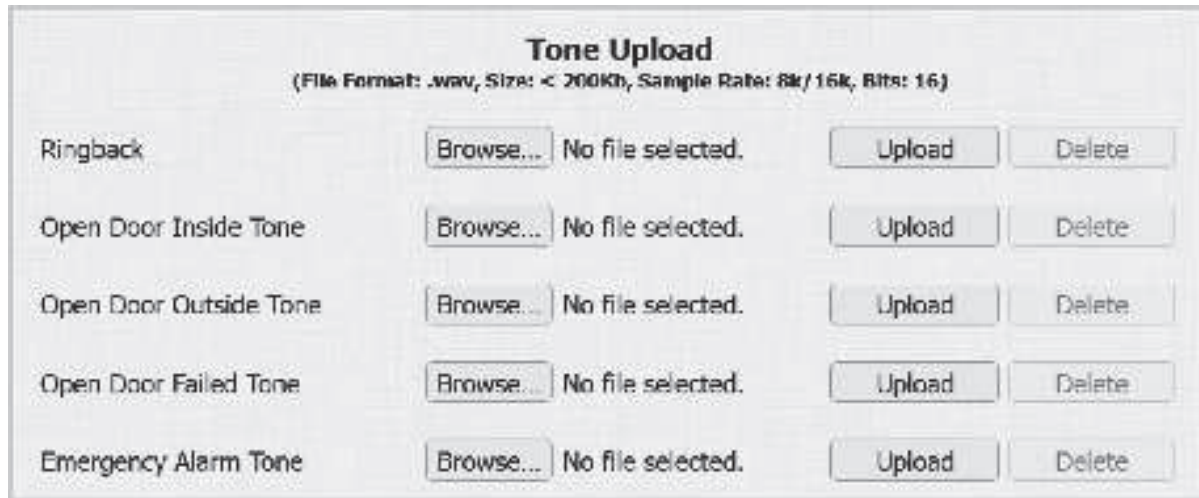
Open Door Tone Setting	
Open Door Inside Tone Enabled	<input checked="" type="checkbox"/>
Open Door Outside Tone Enabled	<input checked="" type="checkbox"/>
Open Door Failed Tone Enabled	<input checked="" type="checkbox"/>

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

Volume and Tone Configuration

Upload Tone Files

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



Tone Upload
(File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16)

Ringback	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Upload"/>	<input type="button" value="Delete"/>
Open Door Inside Tone	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Upload"/>	<input type="button" value="Delete"/>
Open Door Outside Tone	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Upload"/>	<input type="button" value="Delete"/>
Open Door Failed Tone	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Upload"/>	<input type="button" value="Delete"/>
Emergency Alarm Tone	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Upload"/>	<input type="button" value="Delete"/>

- **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.

Network Information	
Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.114
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8

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.

LAN Port	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static IP	
IP Address	<input type="text" value="192.168.1.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Alternate DNS Server	<input type="text"/>

- **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.



The screenshot shows the 'Connect Setting' interface. It includes a title bar 'Connect Setting' and several configuration fields: 'Server Mode' is a dropdown menu set to 'None'; 'Discovery Mode Enabled' is a checkbox that is checked; 'Device Address' consists of five numeric input boxes, each containing the digit '1', separated by dots; 'Device Extension' is a numeric input box containing the digit '1'; and 'Device Location' is a text input box containing the text 'Door Phone'.

- **Server Mode:** It 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.

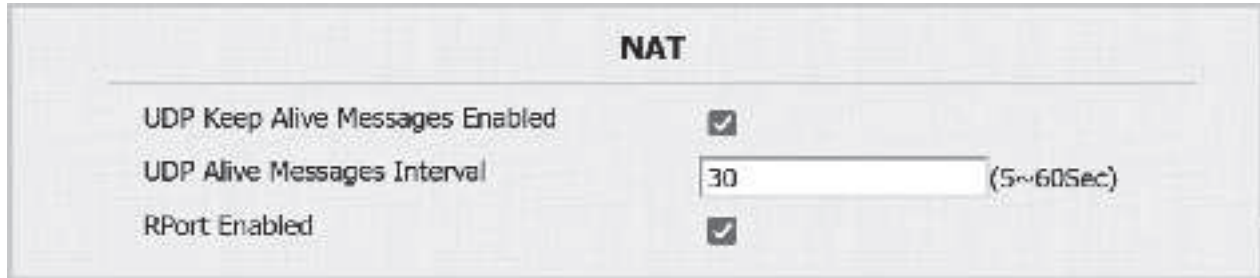


The screenshot shows the 'NAT' interface. It has a title bar 'NAT'. Below it, there is a 'NAT' label and a dropdown menu set to 'Disabled'. Below that, there is a 'Stun Server Address' label and an empty text input box. To the right of the input box is a 'Port' label and a text input box containing the value '3478'.

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

Network Setting

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



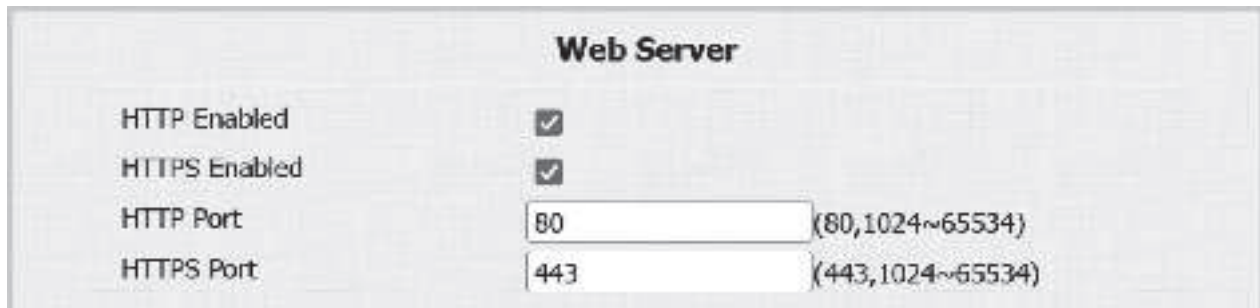
NAT	
UDP Keep Alive Messages Enabled	<input checked="" type="checkbox"/>
UDP Alive Messages Interval	<input type="text" value="30"/> (5~60Sec)
RPort Enabled	<input checked="" type="checkbox"/>

- **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.



Web Server	
HTTP Enabled	<input checked="" type="checkbox"/>
HTTPS Enabled	<input checked="" type="checkbox"/>
HTTP Port	<input type="text" value="80"/> (80,1024~65534)
HTTPS Port	<input type="text" value="443"/> (443,1024~65534)

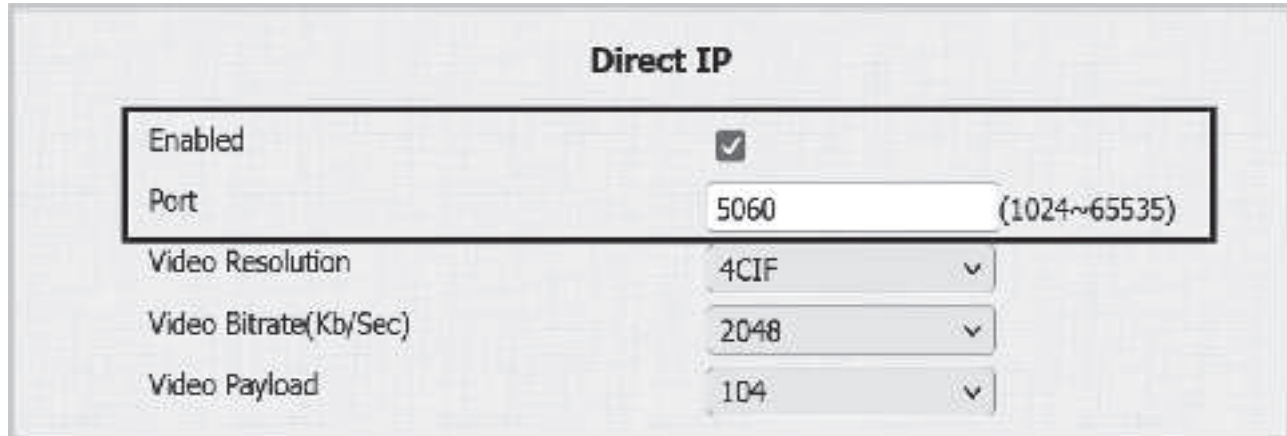
- **HTTP/HTTPS Enabled:** HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port:** Specify the web server port for accessing the device web interface via HTTP/HTTPS.

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.



The screenshot shows the 'Direct IP' configuration window. It contains several settings: 'Enabled' is checked with a checkbox; 'Port' is set to 5060 with a range of (1024~65535) indicated; 'Video Resolution' is set to 4CIF; 'Video Bitrate(Kb/Sec)' is set to 2048; and 'Video Payload' is set to 104. Each of the last three settings has a dropdown arrow next to it.

Direct IP	
Enabled	<input checked="" type="checkbox"/>
Port	5060 (1024~65535)
Video Resolution	4CIF ▼
Video Bitrate(Kb/Sec)	2048 ▼
Video Payload	104 ▼

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.

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

SIP Account Registration

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

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



The screenshot shows the 'SIP Account' configuration page. It has a title 'SIP Account' at the top. Below the title, there are several fields for configuration:

Field	Value
Status	UnRegistered
Account	Account 1 (dropdown menu)
Account Enabled	<input type="checkbox"/>
Display Label	(empty text box)
Display Name	(empty text box)
Register Name	(empty text box)
User Name	(empty text box)
Password	***** (password masked)

- **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.
- **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.
- **User Name:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

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 it up, go to the web **Account > Basic** interface.

The screenshot displays the 'SIP Server Configuration' interface. It is divided into two main sections: 'Preferred SIP Server' and 'Alternate SIP Server'. Each section contains three input fields: 'Server IP' (a text box), 'Port' (a dropdown menu currently set to '5060'), and 'Registration Period' (a text box with '1800' and a range '(30~65535Sec)' to its right).

- **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.

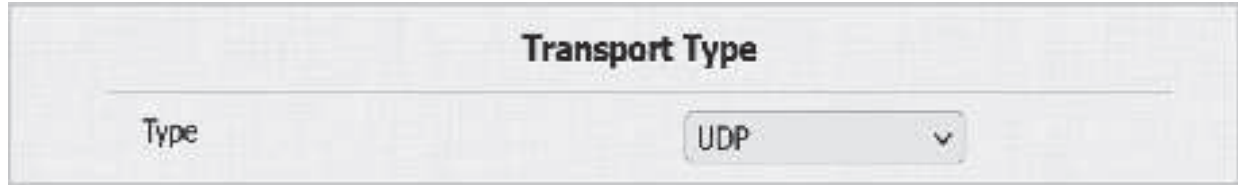
The screenshot shows the 'Outbound Proxy Server' configuration interface. It features a checkbox labeled 'Outbound Enabled'. Below this, there are two rows of input fields: 'Preferred Server IP' and 'Alternate Server IP'. Each row includes a text box for the IP address and a 'Port' dropdown menu, both currently set to '5060'.

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.



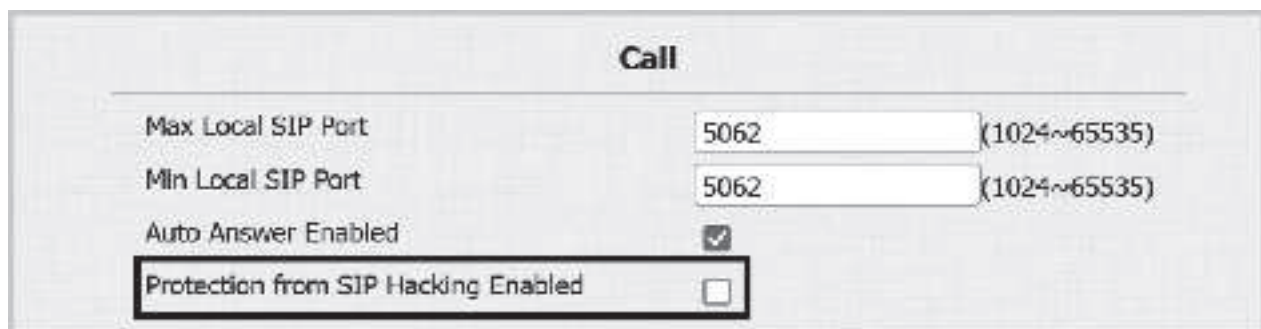
The screenshot shows a web interface titled "Transport Type". Below the title is a horizontal line. Underneath the line, on the left, is the label "Type". To the right of the label is a dropdown menu currently displaying "UDP" with a downward-pointing arrow.

- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** 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. To use it, you need to upload certificates for authentication.
- **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 it, go to **Account > Advanced > Call** interface.



The screenshot shows a web interface titled "Call". Below the title is a horizontal line. Underneath the line, there are four configuration items:

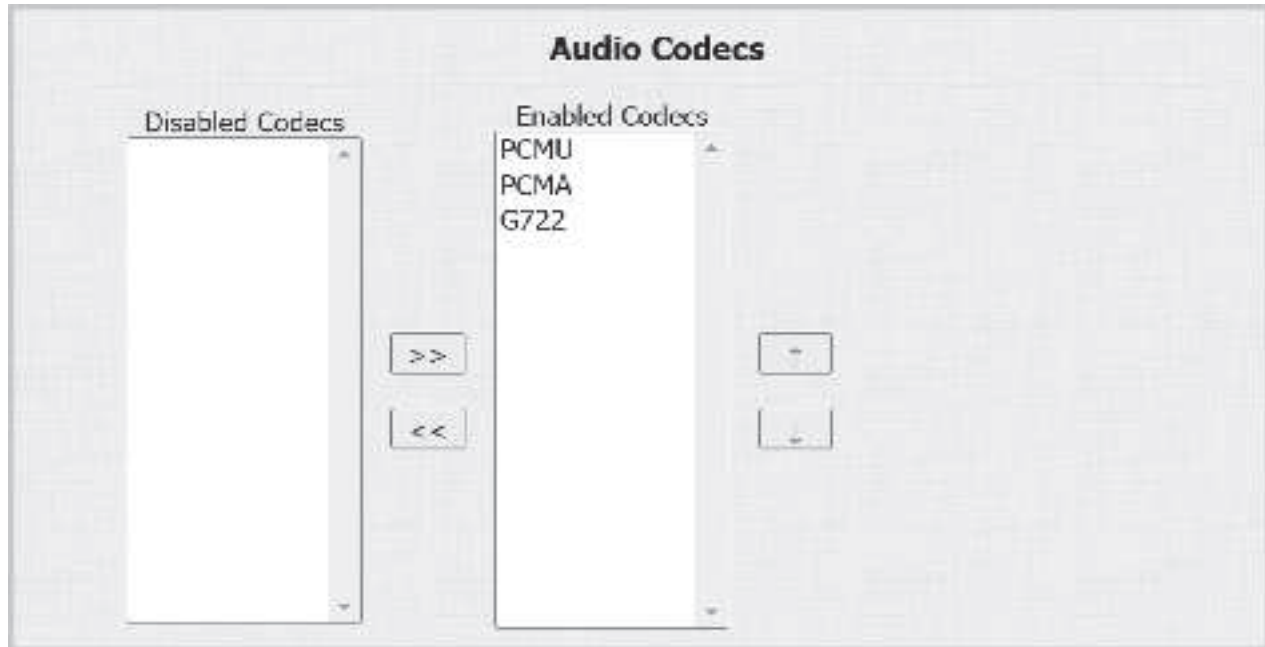
- "Max Local SIP Port" with a text input field containing "5062" and a range "(1024~65535)" to its right.
- "Min Local SIP Port" with a text input field containing "5062" and a range "(1024~65535)" to its right.
- "Auto Answer Enabled" with a checked checkbox.
- "Protection from SIP Hacking Enabled" with an unchecked checkbox. This entire row is highlighted with a black rectangular border.

Audio & Video Codec Configuration

Audio Codec

The doorbell supports three types of codec (*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

To set it up, go to the web **Account > Advanced > Video Codec** interface.



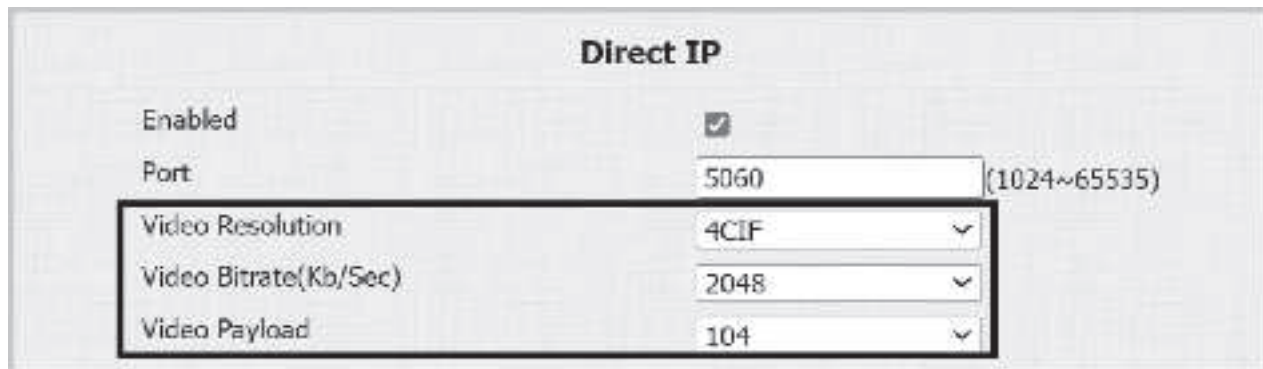
The screenshot shows the 'Video Codec' configuration page. It has a title 'Video Codec' at the top. Below the title, there are four settings: 'Name' with a checked checkbox for 'H.264', 'Resolution' with a dropdown menu set to '4CIF', 'Bitrate(Kb/Sec)' with a dropdown menu set to '2048', and 'Payload' with a dropdown menu set to '104'.

- **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

You can select the IP call video quality by selecting the proper codec resolution according to the network condition.

To set it up, navigate to the **Intercom > Basic > Direct IP** interface.



The screenshot shows the 'Direct IP' configuration page. It has a title 'Direct IP' at the top. Below the title, there are five settings: 'Enabled' with a checked checkbox, 'Port' with a text input field containing '5060' and a range '(1024~65535)' to its right, 'Video Resolution' with a dropdown menu set to '4CIF', 'Video Bitrate(Kb/Sec)' with a dropdown menu set to '2048', and 'Video Payload' with a dropdown menu set to '104'. A black rectangular box highlights the 'Video Resolution', 'Video Bitrate(Kb/Sec)', and 'Video Payload' settings.

- **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.

To set it up, navigate to the **Account > Advanced > DTMF** interface.



DTMF	
Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)

- **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.

You can search, create, edit, and delete the contacts in the allowlist. Set it up on the **Access Control > Access Allowlist** interface.

Search

Index	Name	Phone Number	Account	Floor	
1					<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Page 1

Contact Setting

Name Phone Number

Account

Floor

- **Name:** Name the contact.
- **Phone Number:** The phone number of the contact. It supports IP addresses and SIP numbers.
- **Account:** Select the account to make the call.
- **Floor:** Specify the accessible floor(s) to the contact via the elevator.

Relay Switch Setting

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

The screenshot shows a web interface titled "Relay" with the following configuration fields:

Field	Value
Type	Default state ▾
Mode	Monostable ▾
Trigger Delay(Sec)	0 ▾
Hold Delay(Sec)	3 ▾
DTMF Mode	1 Digit DTMF ▾
1 Digit DTMF	0 ▾
2~4 Digits DTMF	
Relay Status	Low
Relay Name	RelayA

- **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:** Define the 1-digit DTMF code within the range (0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **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.

To set it up, navigate to the web **Setting > Schedule** interface.

Schedule Setting

Mode: Normal ▾

Name:

Start Date - End Date: 20231211 - 20231211

Day: ☐ Mon ☐ Tue ☐ Wed ☐ Thur
☐ Fri ☐ Sat ☐ Sun ☐ Check All

Start Time - End Time: HH ▾ : MM ▾ - HH ▾ : MM ▾

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.

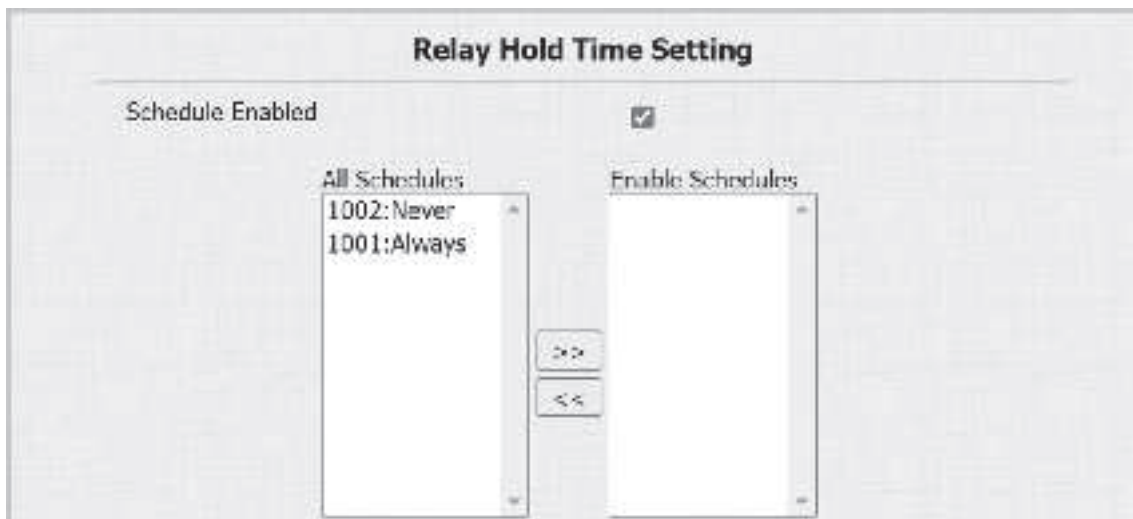
To set it up, go to the **Setting > Schedule** interface. The file exports in TGZ format. The import file should be in XML format



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**.

The screenshot shows a web interface for adding a user. It is divided into two main sections: 'User Basic' and 'RF Card'. In the 'User Basic' section, there are three fields: 'User ID' with the value '1', 'Name' which is empty, and 'Role' with a dropdown menu showing 'General User'. The 'RF Card' section has a 'Code' field which is empty, an 'Obtain' button, and a '+Add' button at the bottom.

- **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.

The screenshot shows the 'Card Type Support' interface. It has a title bar 'Card Type Support'. Below the title bar, there is a section 'IC Support Enabled' with a checked checkbox and an 'Apply' button.

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.

The screenshot shows the 'Import/Export User' interface. It has a title bar 'Import/Export User'. Below the title bar, there are two rows of controls. The first row has 'User Data (.tgz)' with a 'Choose File' button and 'No file chosen' text, followed by 'Import' and 'Export' buttons. The second row has 'AES Key For Import' with a text field containing '*****'.

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.

The screenshot shows the 'Access Setting' window. It has a 'Relay' checkbox which is checked. Below it is a 'Web Relay' dropdown menu set to '0'. Next to it is a 'Floor No.' dropdown menu set to 'None'. There are two list boxes: 'All Schedules' on the left and 'Enable Schedules' on the right. 'All Schedules' contains '1001:Always' and '1002:Never'. 'Enable Schedules' contains '1001:Always'. Between the two list boxes are two arrows, one pointing right and one pointing left. At the bottom of the window are two buttons: 'Submit' and 'Back to list'.

- **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.

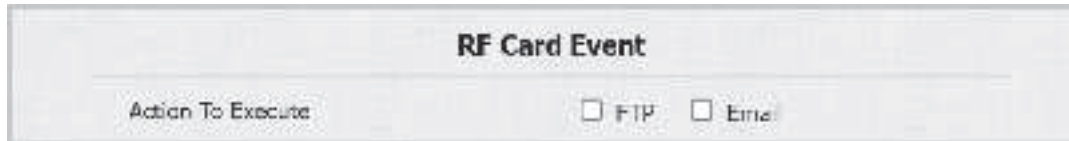
The screenshot shows the 'RFID' interface. It has a label 'IC Card Display Mode' next to a dropdown menu. The dropdown menu is open and shows the selected value '8HN'.

- **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.



The screenshot shows the 'RF Card Event' configuration window. It has a title bar 'RF Card Event'. Below the title bar, there is a section 'Action To Execute' with two checkboxes: 'FTP' and 'Email'.

- **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.



The screenshot shows the 'Mifare Card Encryption' configuration window. It has a title bar 'Mifare Card Encryption'. Below the title bar, there are three fields: 'Enabled' with a checkbox, 'Sector / Block' with two input boxes containing '0' and '0', and 'Block Key' with a password field containing asterisks.

- **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



The screenshot shows the 'Contactless Smart Card' configuration window. It has a title bar 'Contactless Smart Card'. Below the title bar, there is a section 'NFC Enabled' with a checked checkbox.

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.

The screenshot shows the 'Relay' configuration page. It includes fields for 'Type' (set to 'Default state'), 'Mode' (set to 'Monostable'), 'Trigger Delay(Sec)' (set to '0'), and 'Hold Delay(Sec)' (set to '3'). A section titled 'DTMF Mode' is highlighted with a red box, containing '1 Digit DTMF' (set to '0') and '2~4 Digits DTMF' (empty). Below this, 'Relay Status' is set to 'Low' and 'Relay Name' is 'RelayA'.

- **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.

Door Access Schedule Management

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.

Set it up on the web **Access Control > Relay > Open Relay Via HTTP** interface.

The screenshot shows a web interface titled "Open Relay Via HTTP". It contains three fields: "Enabled" with a checkbox, "User Name" with a text input field, and "Password" with a password input field (displayed as asterisks).

- **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 set it up, navigate to the **Access Control > Input** interface.

The screenshot shows a web interface titled "Input A". It contains several fields: "Enabled" with a checkbox, "Trigger Electrical Level" with a dropdown menu (set to "Low"), "Action To Execute" with radio buttons for FTP, Email, SIP Call, and HTTP, "HTTP URL" with a text input field, "Action Delay" with a text input field (set to "0") and a range "(0~300Sec)", "Action Delay Mode" with a dropdown menu (set to "Unconditional Execution"), "Execute Relay" with a dropdown menu (set to "None"), and "Door Status" with a text input field (set to "DoorA: High").

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

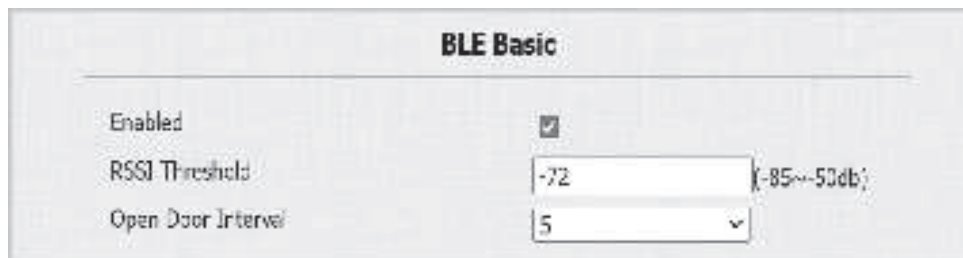
Door Access Schedule Management

- **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:** Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode:**
 - ◇ **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.

Relay by Bluetooth

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.



BLE Basic	
Enabled	<input checked="" type="checkbox"/>
RSSI Threshold	<input type="text" value="-72"/> (-85~-50db)
Open Door Interval	<input type="text" value="5"/>

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.

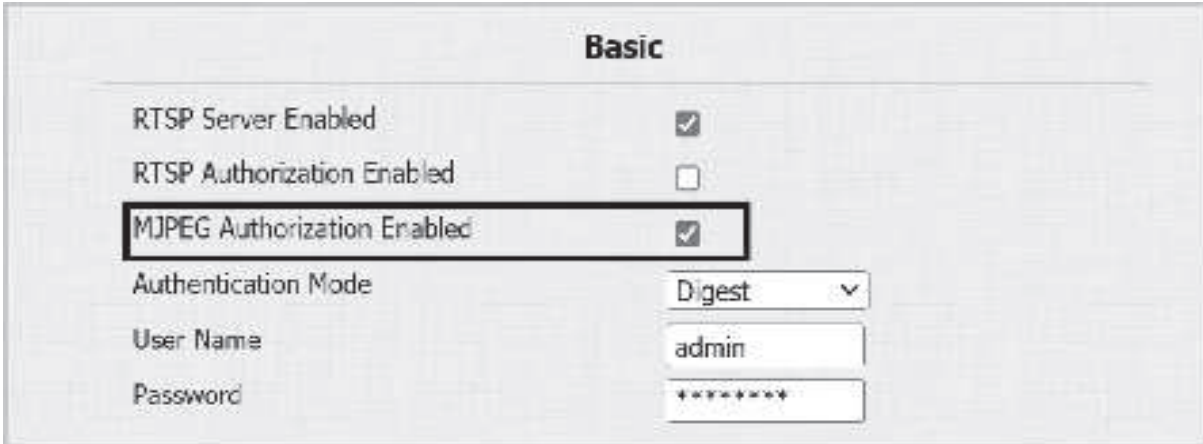
RTSP (Real Time Streaming Protocol) can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format is **rtsp://**

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.



The screenshot shows the 'Basic' configuration page. It contains several settings: 'RTSP Server Enabled' with a checked checkbox, 'RTSP Authorization Enabled' with an unchecked checkbox, 'MJPEG Authorization Enabled' with a checked checkbox (highlighted by a black rectangle), 'Authentication Mode' set to 'Digest' via a dropdown menu, 'User Name' set to 'admin' in a text field, and 'Password' shown as a masked field with asterisks.

- **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.

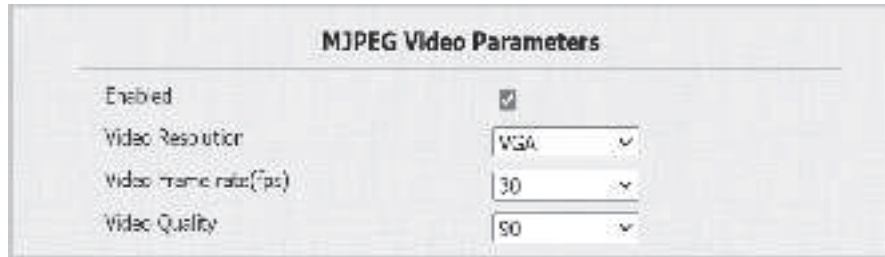
TIP:

- 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**

Door Access Schedule Management

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.



The screenshot shows a web interface titled "MJPEG Video Parameters". It contains four settings:

Parameter	Value
Enabled	<input checked="" type="checkbox"/>
Video Resolution	VGA
Video frame rate(fps)	30
Video Quality	90

- **Video Resolution:** Specify the image resolution, varying from the lowest CIF (352×288 pixels) to the highest 1080P (1920×1080 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.



The screenshot shows a web interface titled "Basic" for RTSP settings. It contains six settings:

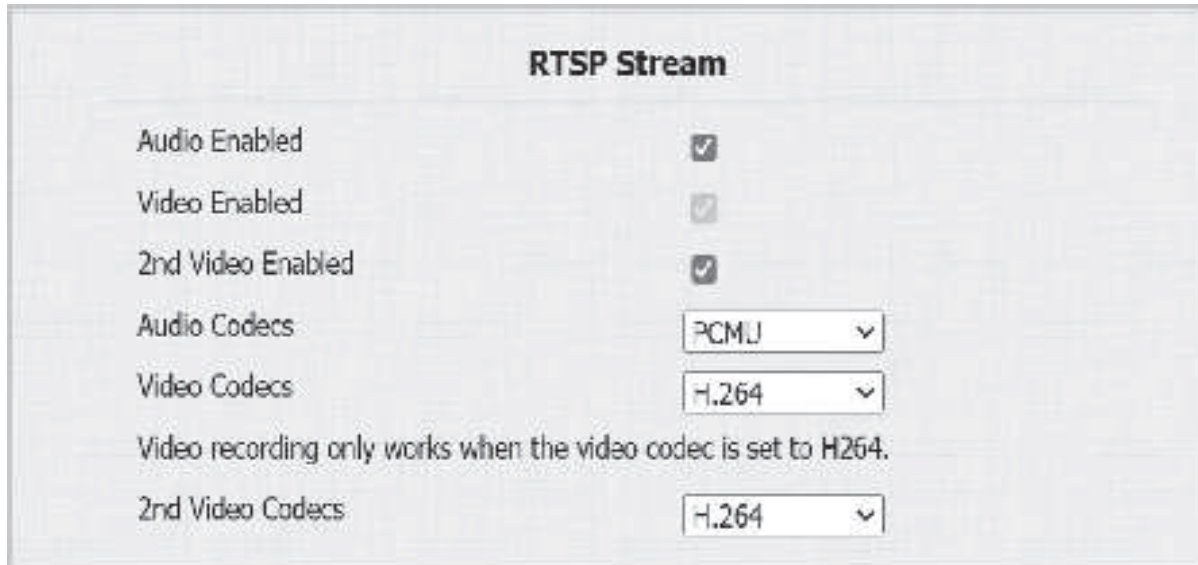
Parameter	Value
RTSP Server Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input checked="" type="checkbox"/>
Authentication Mode	Digest
User Name	admin
Password	*****

- **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.



The screenshot shows the 'RTSP Stream' configuration window. It contains several settings:

- Audio Enabled:** A checkbox that is checked.
- Video Enabled:** A checkbox that is checked.
- 2nd Video Enabled:** A checkbox that is checked.
- Audio Codecs:** A dropdown menu with 'PCMU' selected.
- Video Codecs:** A dropdown menu with 'H.264' selected.
- A text note: 'Video recording only works when the video codec is set to H264.'
- 2nd Video Codecs:** A dropdown menu with 'H.264' selected.

- **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.
 - ◇ **MJPEG:** 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.

The screenshot shows a configuration window titled "H.264 And H.265 Video Parameters". It contains six settings, each with a label and a dropdown menu:

Parameter	Value
Video Resolution	720P
Video Frame rate(fps)	30
Video Bitrate(Kb/Sec)	2048
2nd Video Resolution	VGA
2nd Video Frame rate(fps)	30
2nd Video Bitrate(Kb/Sec)	512

- **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.

The screenshot shows a configuration window titled "RTSP OSD Setting". It contains two settings:

Parameter	Value
RTSP OSD Color	White
RTSP OSD Text	


- **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.

Door Access Schedule Management

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.



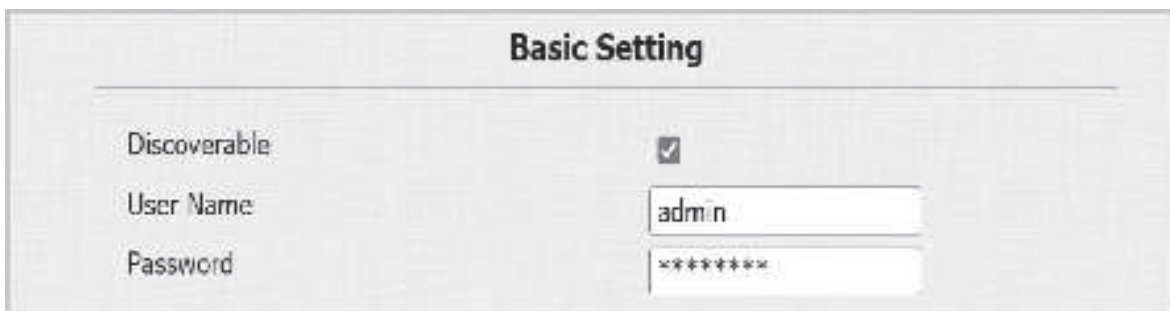
The screenshot shows a web interface titled "Others". It contains a label "Return Code When Refuse" next to a dropdown menu showing "486(Busy Here)". Below this is a checkbox labeled "NACK Enabled" which is checked.

- **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 set it up, go to the **Surveillance > ONVIF** interface.



The screenshot shows a web interface titled "Basic Setting". It has three fields: "Discoverable" with a checked checkbox, "User Name" with a text input field containing "admin", and "Password" with a text input field containing "*****".

- **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.

Set it up on the **Security > Basic > Tamper Alarm** interface. Click *Disarm* to clear the alarm.



The screenshot shows the 'Tamper Alarm' configuration interface. It has a title bar 'Tamper Alarm' and a horizontal separator line. Below the line, there are three settings on the left and two on the right. The left settings are 'Enabled', 'Key Status', and 'Trigger Options'. The right settings are a 'Disarm' button and a 'High' label above a dropdown menu showing 'Only Alarm'.

Tamper Alarm	
Enabled	<input type="checkbox"/> Disarm
Key Status	High
Trigger Options	Only 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.

Client Certificate

Index	Issue To	Issuer	Expire Time	
1				<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

Client Certificate Upload(.PEM/.DER/.CER/.CRT)

Index

Choose File

No file chosen

Auto ▾

Only Accept Trusted Certificates

Disabled ▾

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.

To set it up, go to **Security > Advanced** interface.

SIP Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	akpbx		Sun Sep 10 03:21:52 2049	Delete

SIP Server Certificate Upload(.PEM/.DER/.CER)

Choose File No file chosen Submit Cancel

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.

Motion Detection Options

Suspicious Object Movement Detection: Disabled

Time Interval: 10 (0~120Sec)

Action To Execute: ☐ FTP ☐ Email ☐ SIP Call ☐ HTTP

HTTP URL:

Motion Detect Time Setting

Day: ☒ Mon ☒ Tue ☒ Wed ☒ Thur ☒ Fri ☒ Sat ☒ Sun ☐ Check All

Start Time - End Time: 00 : 00 - 23 : 59

- **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.

Security

- **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.

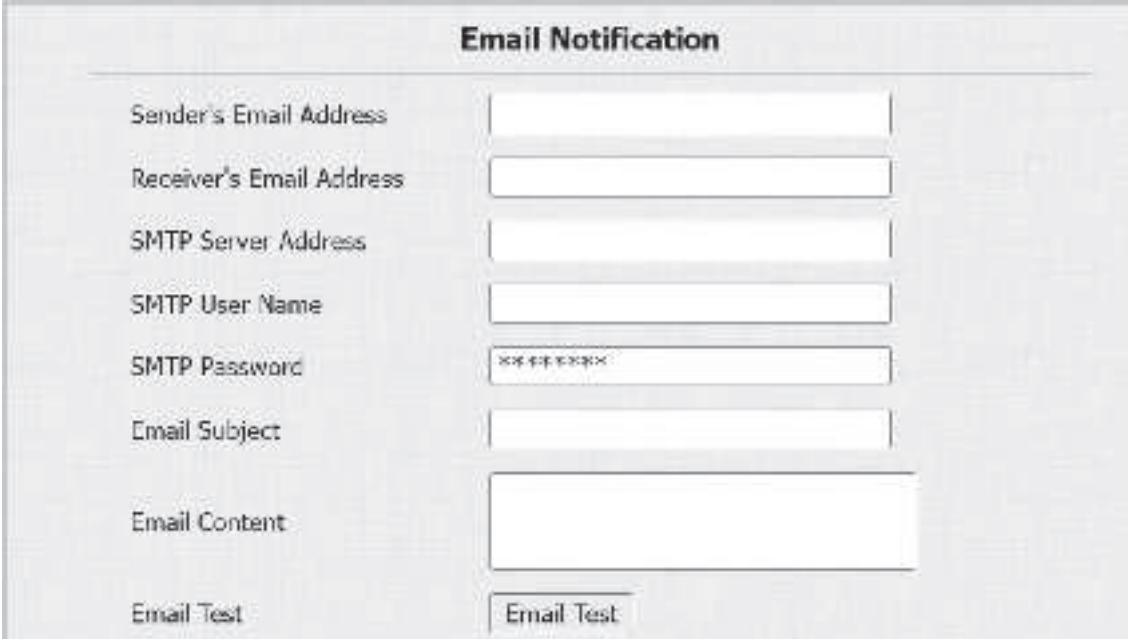
Security Notification

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.



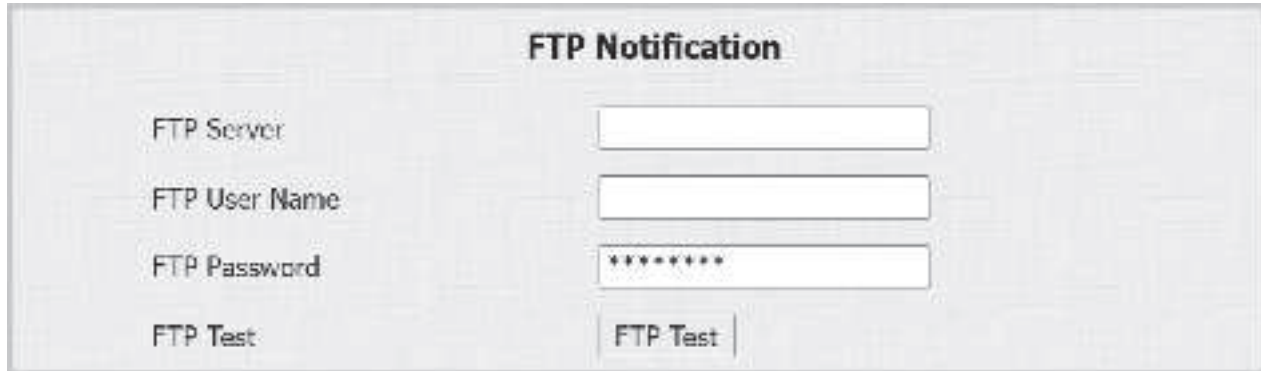
The screenshot shows a web interface titled "Email Notification". It contains several input fields for configuring email settings: "Sender's Email Address", "Receiver's Email Address", "SMTP Server Address", "SMTP User Name", "SMTP Password" (with a masked input), "Email Subject", and "Email Content" (a larger text area). At the bottom, there is an "Email Test" button.

- **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.

Set it up in the **FTP Notification** section.



The screenshot shows a configuration window titled "FTP Notification". It contains four input fields: "FTP Server", "FTP User Name", and "FTP Password" (masked with asterisks), and a "FTP Test" button.

- **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.

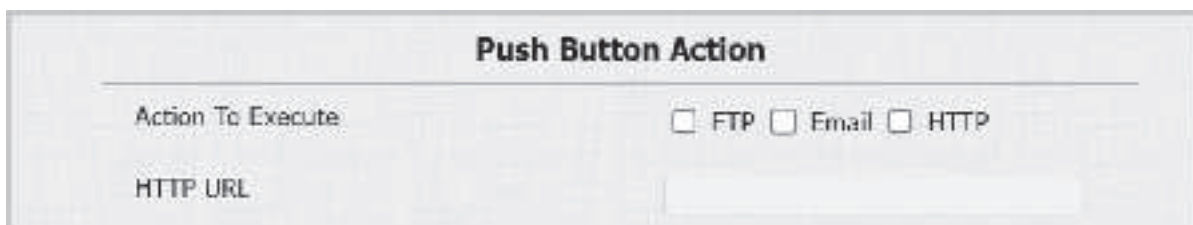


The screenshot shows a configuration window titled "SIP Call Notification". It contains two input fields: "SIP Call Number" and "SIP Caller Name".

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.



The screenshot shows a configuration window titled "Push Button Action". It has a section "Action To Execute" with three checkboxes: "FTP", "Email", and "HTTP". Below this is an "HTTP URL" input field.

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 Entered	\$card_sn	Http://server ip/invalidcard=\$card_sn

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

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

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

Action URL

Enabled

☐

Make Call

Hang Up

Relay Triggered

Relay Closed

InputA Triggered

InputB Triggered

InputA Closed

InputB Closed

Suspicious Object Movement Detection

Valid Card Entered

Invalid Card Entered

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.



The screenshot shows a configuration box titled "Encryption". Inside, there is a label "Voice Encryption(SRTP)" followed by a dropdown menu currently set to "Disabled".

Set it up on the web **Account > Advanced > Encryption** interface.

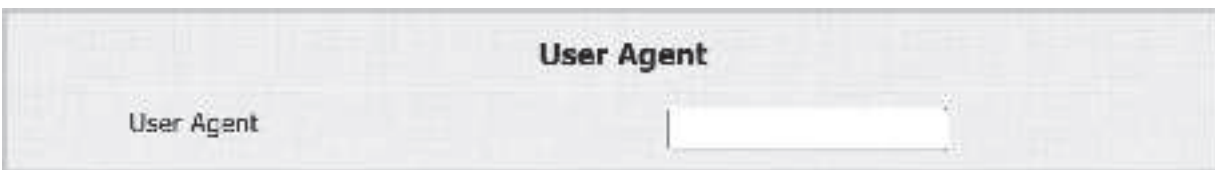
- **Voice Encryption(SRTP):** Choose *Disabled*, *Optional* or *Compulsory*. If *Optional* or *Compulsory* is selected, the voice during the call is encrypted and you can grab the RTP packet to view it.

User Agent

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

To set it up, navigate to the **Account > Advanced > User Agent** interface.

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

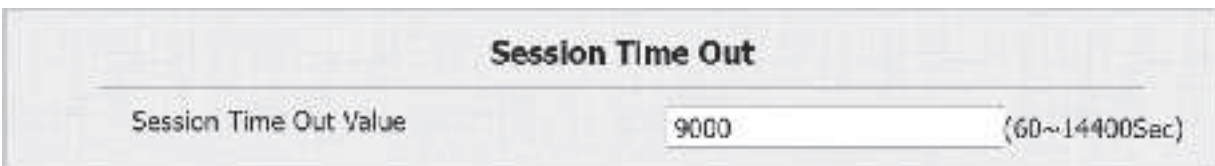


The screenshot shows a configuration box titled "User Agent". Inside, there is a label "User Agent" followed by an empty text input field.

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 set it up, go to **Security > Basic > Session Time Out** interface.



The screenshot shows a configuration box titled "Session Time Out". Inside, there is a label "Session Time Out Value" followed by a text input field containing the value "9000". To the right of the input field, there is a range indicator "(60~14400Sec)".

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.

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.

Save Call Log Enabled ☒

Call History

All ▾ Hang Up

Time

mm/dd/yyyy ☐ - mm/dd/yyyy ☐

Name/Number

Search

Export

Index	Type	Date	Time	Local Identity	Name	Number	<input type="checkbox"/>
1							<input type="checkbox"/>
2							<input type="checkbox"/>
3							<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>
11							<input type="checkbox"/>
12							<input type="checkbox"/>
13							<input type="checkbox"/>
14							<input type="checkbox"/>
15							<input type="checkbox"/>

Page 1 ▾

Prev

Next

Delete

Delete All

- **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.

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.

Save Door Log Enabled ☒

Status All

Time mm/dd/yyyy - mm/dd/yyyy

Name/Code Search Export

Index	Name	Code	Type	Date	Time	Status	
1	1	FFB59828	Card	2024-04-03	02:05:00	Success	<input type="checkbox"/>
2	1	FFB59828	Card	2024-04-03	02:04:58	Success	<input type="checkbox"/>
3	1	FFB59828	Card	2024-04-03	02:04:52	Success	<input type="checkbox"/>
4	1	FFB59828	Card	2024-04-03	02:04:40	Success	<input type="checkbox"/>
5	1	FFB59828	Card	2024-04-03	02:04:37	Success	<input type="checkbox"/>
6	1	FFB59828	Card	2024-04-03	02:04:11	Success	<input type="checkbox"/>
7	1	FFB59828	Card	2024-04-03	02:04:09	Success	<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>
11							<input type="checkbox"/>
12							<input type="checkbox"/>
13							<input type="checkbox"/>
14							<input type="checkbox"/>
15							<input type="checkbox"/>

Page 1
Prev
Next
Delete
Delete All

- **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.

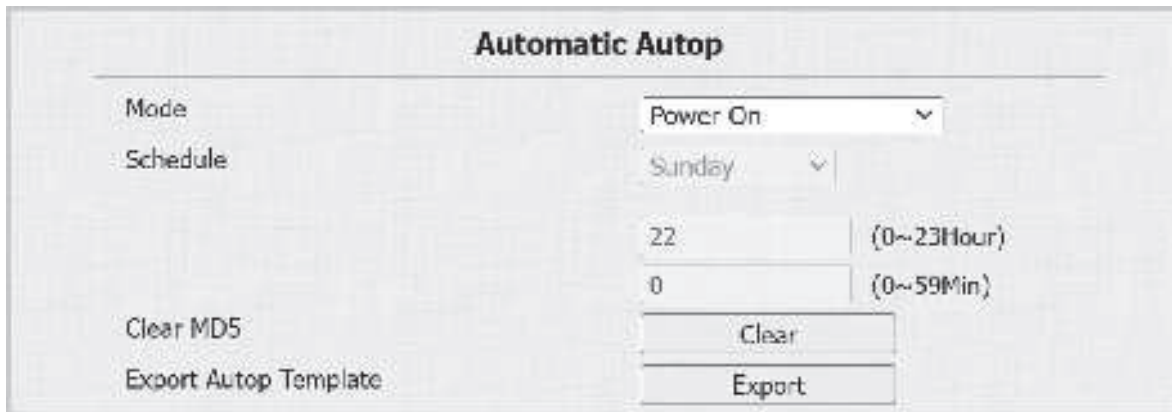
Firmware Upgrade

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

Firmware Version	312.30.10.18
Hardware Version	312.13
Upgrade	<input type="button" value="Browse..."/> No file selected.
	Reset: <input type="checkbox"/>
	<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Reset"/>
Reboot	<input type="button" value="Reboot"/>

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

Auto-provisioning via Configuration File



The image shows a web-based configuration interface titled "Automatic Autop". It contains several fields and buttons. The "Mode" field is a dropdown menu set to "Power On". The "Schedule" field is a dropdown menu set to "Sunday". Below the schedule, there are two input fields: "22" with a range "(0~23Hour)" and "0" with a range "(0~59Min)". At the bottom, there are two buttons: "Clear MD5" and "Export Autop Template".

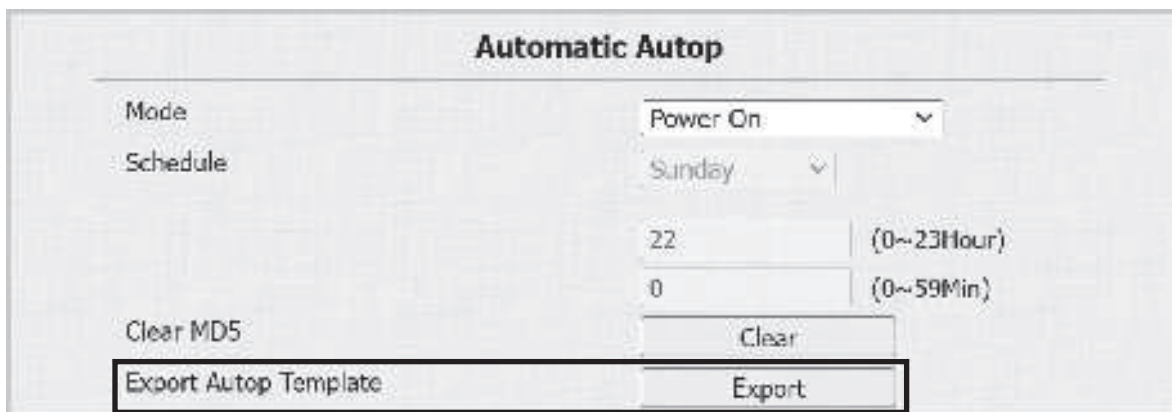
- **Mode:**

- ◇ **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.

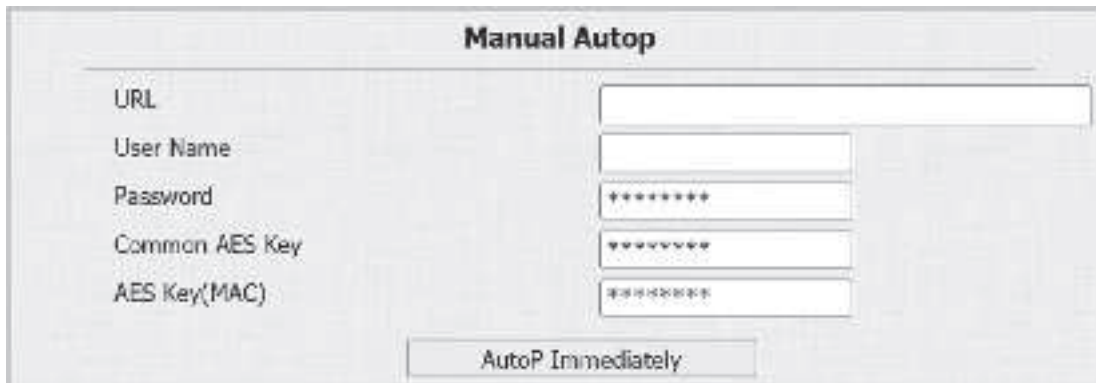
To set it up, download the template on **Upgrade > Advanced > Automatic Autop** interface first.



This image is identical to the one above, showing the "Automatic Autop" configuration interface. However, the "Export Autop Template" button is highlighted with a black rectangular border, indicating it is the button to click to download the template.

Auto-provisioning via Configuration File

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



The screenshot shows a window titled "Manual Autop". It has five input fields on the right side, each corresponding to a label on the left: "URL", "User Name", "Password", "Common AES Key", and "AES Key(MAC)". The "Password" and "Common AES Key" fields are masked with asterisks. Below these fields is a button labeled "AutoP Immediately".

- **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.

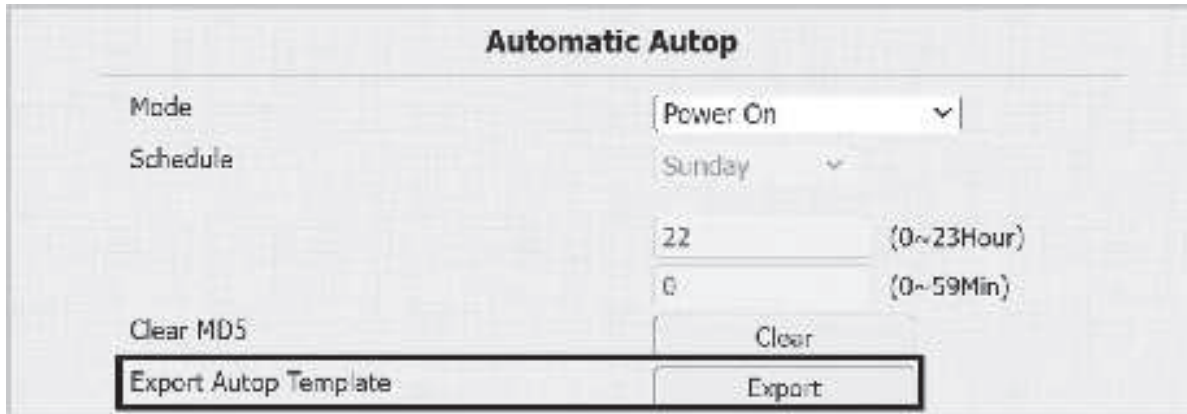
NOTE:

- 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

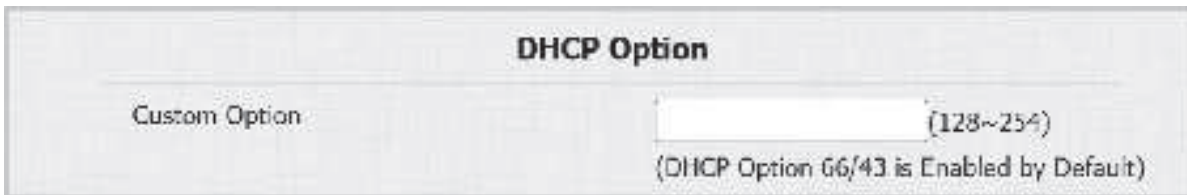
Set up DHCP Autop with Power On mode and export Autop Template to edit the configuration.

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



The screenshot shows the 'Automatic Autop' configuration window. It has a title bar 'Automatic Autop'. Below it, there are two rows of settings. The first row has 'Mode' set to 'Power On' (with a dropdown arrow) and 'Schedule' set to 'Sunday' (with a dropdown arrow). The second row has '22' (with a range '(0~23Hour)') and '0' (with a range '(0~59Min)'). Below these are two buttons: 'Clear MD5' and 'Clear'. At the bottom, there are two buttons: 'Export Autop Template' and 'Export'. The 'Export Autop Template' button is highlighted with a red rectangle.

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



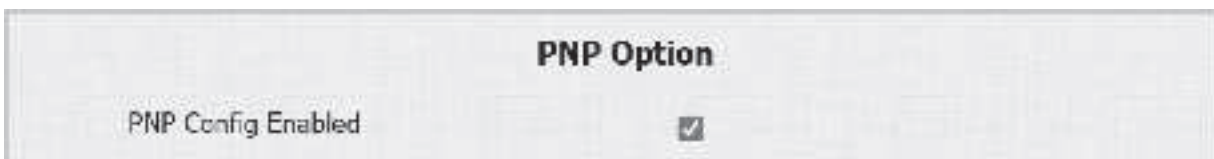
The screenshot shows the 'DHCP Option' configuration window. It has a title bar 'DHCP Option'. Below it, there is a 'Custom Option' field with a value of '(128~254)'. Below the field, there is a note: '(DHCP Option 66/43 is Enabled by Default)'.

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

Set it up on the web **Upgrade > Advanced > PNP Option** interface.



The screenshot shows the 'PNP Option' configuration window. It has a title bar 'PNP Option'. Below it, there is a 'PNP Config Enabled' checkbox, which is checked.

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.

The screenshot shows a configuration window titled "Wiegand". It contains several settings, each with a label and a control element (dropdown menu or checkbox):

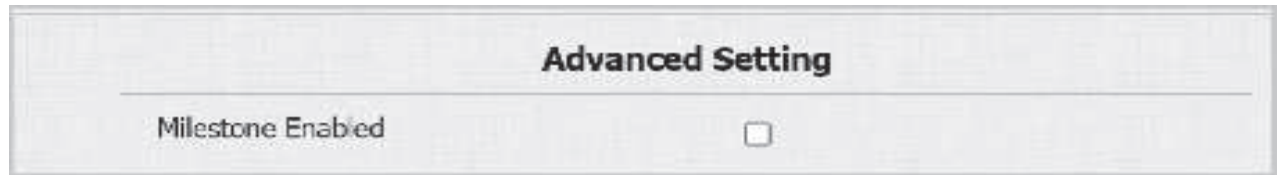
Setting	Value
Wiegand Display Mode	8HN
Wiegand Card Reader Mode	wiegand-26
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output CRC Enabled	<input checked="" type="checkbox"/>

- **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:** Determine the sequence of the card number.
 - ◇ **Normal:** The card number is displayed as received.
 - ◇ **Reversed:** The order of the card number is reversed.
- **Wiegand Output Basic Data Order:** 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 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 on the **Surveillance > ONVIF > Advanced Setting** interface.



The screenshot shows a web interface titled "Advanced Setting". Below the title, there is a label "Milestone Enabled" followed by an unchecked checkbox.

Integration via HTTP API

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

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



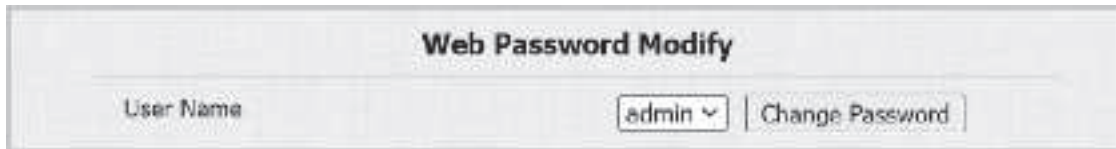
The screenshot shows a web interface titled "HTTP API". It contains four configuration items:

- HTTP API Enabled:** A checkbox that is checked.
- Authorization Mode:** A dropdown menu with "Digest" selected.
- User Name:** A text input field containing "admin".
- Password:** A text input field containing "*****".

- **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*.

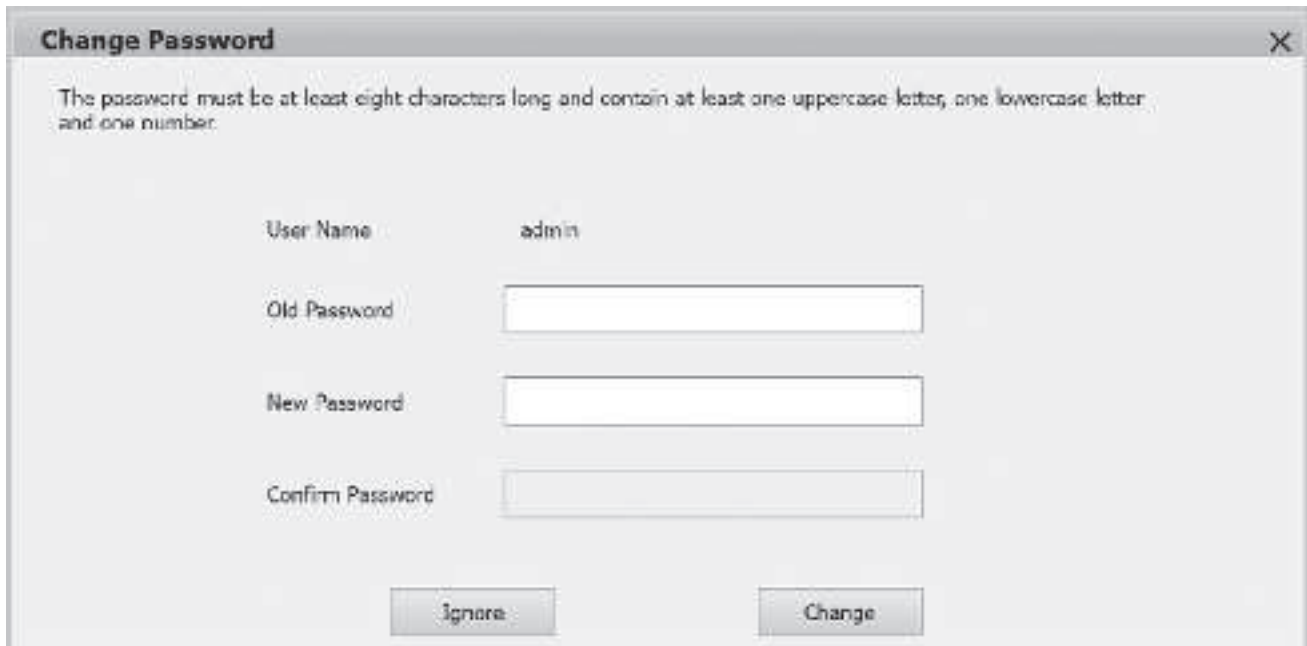
Password Configuration

You can modify the device web password for both the administrator account and the user account. To set it up, go to **Security > Basic > Web Password Modify** interface.



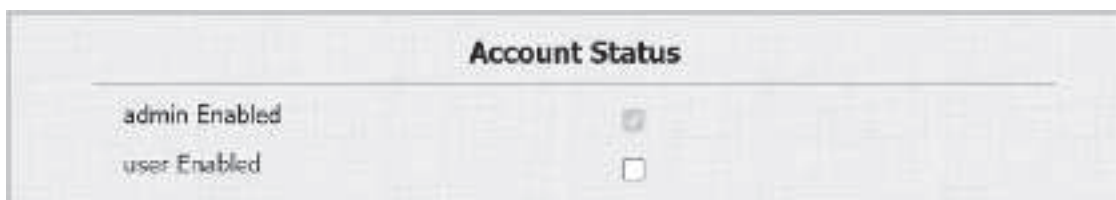
The 'Web Password Modify' interface features a title bar with the text 'Web Password Modify'. Below the title bar, there is a 'User Name' label followed by a dropdown menu showing 'admin' and a 'Change Password' button.

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



The 'Change Password' dialog box has a title bar with 'Change Password' and a close button (X). The main content area contains a password policy note: 'The password must be at least eight characters long and contain at least one uppercase letter, one lowercase letter and one number.' Below this, there are four input fields: 'User Name' (pre-filled with 'admin'), 'Old Password', 'New Password', and 'Confirm Password'. At the bottom, there are two buttons: 'Ignore' and 'Change'.

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

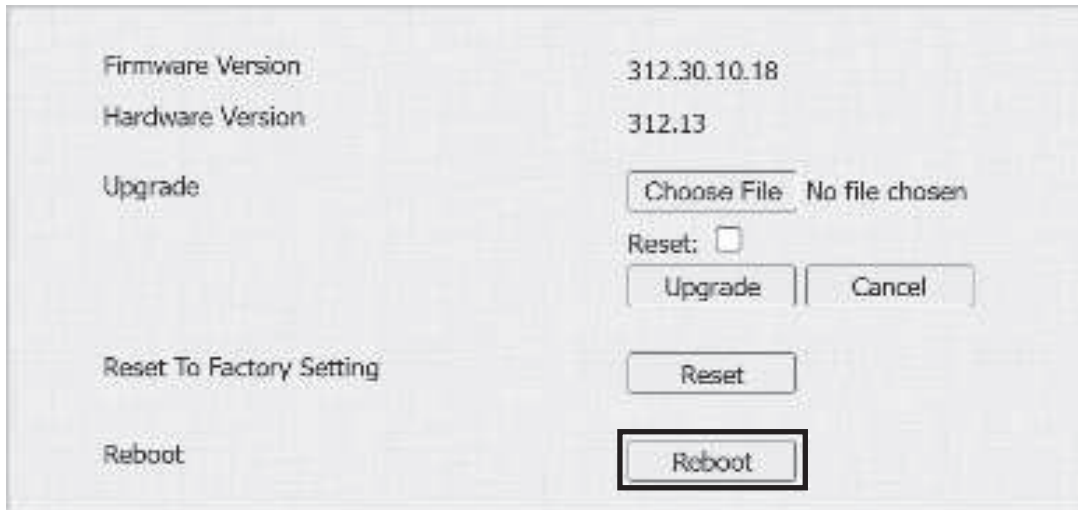


The 'Account Status' interface has a title bar with the text 'Account Status'. Below the title bar, there are two rows of controls. The first row is for the 'admin' account, showing 'admin Enabled' and a checked checkbox. The second row is for the 'user' account, showing 'user Enabled' and an unchecked checkbox.

System Reboot and Reset

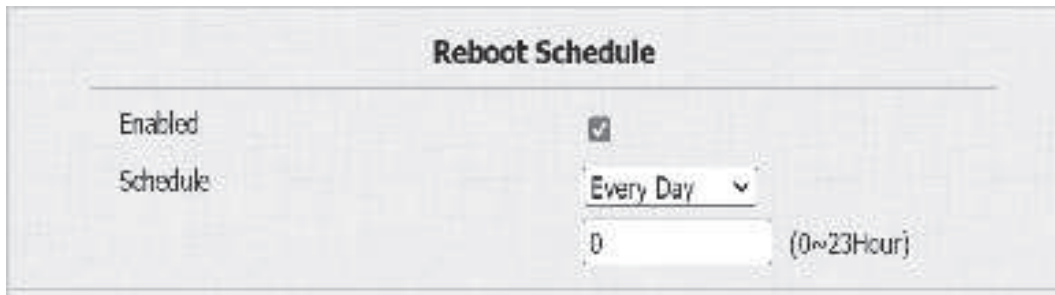
Reboot

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.



This screenshot shows the 'Upgrade > Basic' interface. It displays the 'Firmware Version' as 312.30.10.18 and the 'Hardware Version' as 312.13. Under the 'Upgrade' section, there is a 'Choose File' button and the text 'No file chosen'. Below this is a 'Reset:' checkbox which is unchecked, followed by 'Upgrade' and 'Cancel' buttons. The 'Reset To Factory Setting' section has a 'Reset' button. The 'Reboot' section at the bottom has a 'Reboot' button, which is highlighted with a red rectangle.

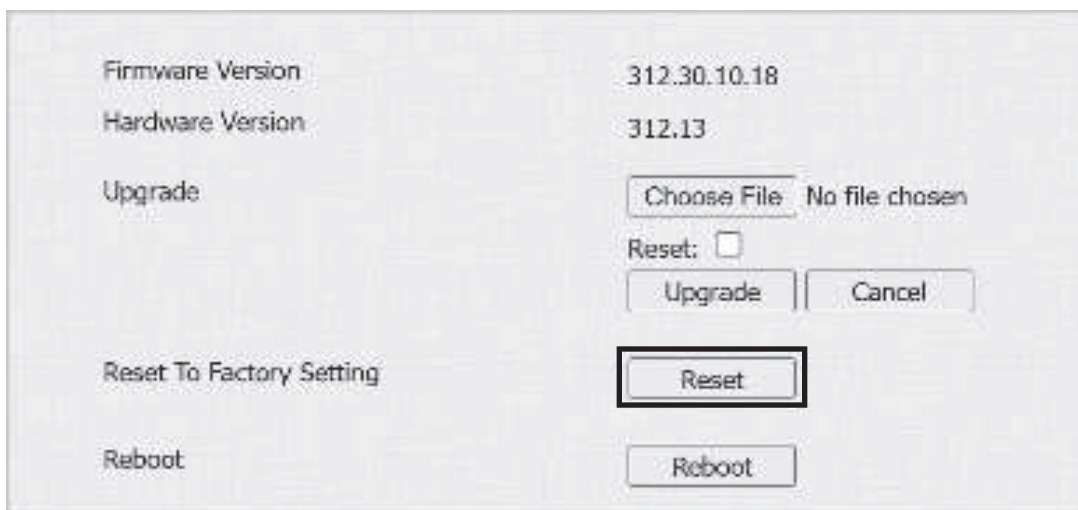
To set up the schedule, go to the **Upgrade > Advanced** interface.



This screenshot shows the 'Reboot Schedule' interface. It has a title 'Reboot Schedule' at the top. Below the title, there is an 'Enabled' checkbox which is checked. Under the 'Schedule' section, there is a dropdown menu set to 'Every Day' and a text input field containing '0', with '(0~23Hour)' to its right.

Reset

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



This screenshot shows the 'Upgrade > Basic' interface, similar to the one above. It displays the 'Firmware Version' as 312.30.10.18 and the 'Hardware Version' as 312.13. Under the 'Upgrade' section, there is a 'Choose File' button and the text 'No file chosen'. Below this is a 'Reset:' checkbox which is unchecked, followed by 'Upgrade' and 'Cancel' buttons. The 'Reset To Factory Setting' section has a 'Reset' button, which is highlighted with a red rectangle. The 'Reboot' section at the bottom has a 'Reboot' button.

Technical Support

760-438-7000

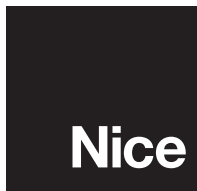
Monday - Friday, 6:00 a.m. – 4:00 p.m. PST

Nice North America

c/o Customer Service

5919 Sea Otter Place, Ste. 100

Carlsbad, CA 92010



Niceforyou.com