

# IP-DB

IP VIDEO DOORBELL

OWNERS MANUAL





# IP-DB

## IP VIDEO DOORBELL

### USER MANUAL



## OVERVIEW

The AtlasIED IP-DB is a rugged, high-performance video door phone designed for secure and convenient access control. Built with an IP66 and IK07-rated housing, it offers reliable operation in both outdoor and demanding environments.

The device features a built-in HD camera with infrared night vision, echo cancellation for clear two-way audio, and multiple access methods including RFID cards, PIN codes, and remote unlocking.

With support for SIP protocol, the AtlasIED IP-DB integrates seamlessly with IP phone systems and third-party platforms, making it ideal for commercial and industrial applications.

## SAFETY INSTRUCTIONS

Please read the following safety notices before installing or using this unit. They are crucial for the safe and reliable operation of the device.

- Please use the product-specified power adapter. If you need to use a power adapter provided by another manufacturer due to special circumstances, please confirm that the voltage and current of the provided adapter meet the specifications of this product, and it is recommended to use a product that has passed safety certification, otherwise it may cause fire or electric shock accidents. When using this product, do not damage the power cord, do not twist, stretch and strap it, and do not press it under heavy objects or sandwich between items, otherwise it may cause fire or electric shock caused by broken power cord.
- Before using the product, please confirm that the temperature and humidity of the environment in which it is located meet the working needs of the product. (Moving this product from the air-conditioner to the natural temperature, the surface or internal components of this product may produce condensate vapor, and the product needs to be dried naturally before turning on the power supply.)
- Non-technical service personnel should not disassemble or repair the product by themselves, improper repair may cause accidents such as electric shock, fire, etc., and the warranty service of your product will also be invalid.
- Do not put metal foreign objects such as pins and wires into vents or gaps. Otherwise, it may cause electric shock and other injuries caused by the passage of electricity through metal foreign objects, and if foreign objects or similar metal objects fall into the product, the use should be stopped in time.
- Do not discard or store the plastic bag used for packaging in a place where the child can get it, so as not to cover the head of the young child, causing the nose and mouth to block, resulting in suffocation.
- Please use this product correctly in accordance with the instructions in this product manual, long-term abnormal operation may lead to product damage and safety hazards.



## TABLE OF CONTENTS

<b>Safety Instruction</b> .....	2	Network >> service port .....	33
<b>Overview</b> .....	2	Network >> VPN.....	34
<b>Install Guide</b> .....	4	Network >> Advanced.....	35
Use POE or external Power Adapter .....	4	Line >> SIP .....	37-41
Appendix.....	4	Line >> SIP Hotspot.....	41
Common command modes .....	4	Line >> Dial Plan.....	42
LED status.....	5	Line >> Action Plan.....	43
<b>User Guide</b> .....	6	Line >> Basic Settings .....	44
Panel description.....	7	Line >> PTCR-XR.....	46
Interface description.....	7	Intercom settings >> Features.....	47-48
Installation instructions.....	8	Intercom settings >> Media.....	50
Installation .....	9	Intercom settings >> Camera Settings.....	51-55
Device IP address.....	9	Intercom Setting >> MCAST.....	55
WEB configuration.....	10	Intercom Setting >> Action URL .....	55
SIP Configurations .....	11	Intercom Setting >> Time/Date .....	56
Door opening operation.....	12	Intercom settings >> Time plan.....	58
<b>Basic Function</b> .....	12	Intercom settings >> Tone.....	59
Swipe to open the door .....	12	Intercom settings >> Led .....	59
Remote Door Opening.....	13	Call list >> Call List .....	60
Password to Open Door.....	14	Call list >> Web Dial.....	60
Making Calls.....	15	Function key .....	61-65
Answering Calls .....	16	Security >> Web filter .....	65
End of the Call .....	16	Security >> Trust Certificates.....	66
Auto Answer .....	16	Security >> Device Certificates .....	67
Call Waiting.....	17	Security >> Firewall .....	67
<b>Advance Function</b> .....	19	Device log.....	69
Intercom.....	19	Security settings.....	69
MCAST.....	19-21	EGS Setting >> Features .....	72
Hotspot.....	21-22	EGS Setting >> Relay.....	73
<b>Web Configurations</b> .....	23	EGS Setting >> Card.....	74
Web Page Authentication .....	23	EGS Setting >> Password .....	76
System >> Information.....	23	EGS Setting >> Time Profile.....	77
System >> Account .....	24	EGS Setting >> Logs.....	78
System >> Configurations .....	24	<b>Trouble Shooting</b> .....	79
System >> Upgrade.....	25-28	Get device system information.....	79
System >> Auto Provision.....	28	Reboot device.....	79
System >> FDMS .....	30	Device factory reset .....	79
System >> Tools .....	31	Network Packets Capture.....	79
System >> Reboot.....	31	Get device log.....	79
Network >> Basic.....	32	Common Trouble Cases .....	79





## INSTALL GUIDE

### Use POE or external Power Adapter

IP-DB called as 'the device' hereafter, supports two power supply modes, power supply from external power adapter or over Ethernet (POE) complied switch.


POE power supply saves the space and cost of providing the device additional power outlet. With a POE switch, the device can be powered through a single Ethernet cable which is also used for data transmission. By attaching UPS system to POE switch, the device can keep working at power outage just like traditional PSTN telephone which is powered by the telephone line.

For users who do not have POE equipment, the traditional power adaptor should be used. If the device is connected to a POE switch and power adapter at the same time, the power adapter will be used in priority and will switch to POE power supply once it fails.

Please use the power adapter and the POE switch met the specifications to ensure the device work properly.

### Appendix

#### Common Command Modes

ACTION BEHAVIOR	DESCRIPTION
Standby report IP	In standby mode, long press the speed dial button for 3 seconds, there will be a toot sound will 5 seconds, please press the speed dial button once within 5 seconds, the toot sound will stop automatically reporting IP. IP-DB press the button in the upper right corner. 
Switch network mode	In the standby mode, long-press the speed dial button for 3 seconds and the beep will last for 5 seconds. Within 5 seconds, press the speed dial button three times quickly to switch to the network mode. If there is no IP at present, switch to the default static IP (192.168.1.128). Then switch to DHCP mode when it is the default static IP (192.168.1.128) When DHCP gets to IP, then do not switch and report the IP directly. Report the IP after the successful switch.
Voice loop mode	In the standby mode, long-press the speed dial button for 3 seconds and the beep will last for 5 seconds. Within 5 seconds, after you press the speed dial button twice, the device enters the voice loopback mode. After you press the MIC speaker, you can check the voice related problems. After you press the speed dial button again, you can exit the voice loopback mode



(CONTINUED ON NEXT PAGE)



## INSTALL GUIDE

### LED status

IP-DB has a status indicator. The color of keyboard backlight does not change according to device status.

### IP-DB LED status

TYPE	INDICATOR STATUS	INDICATOR STATUS
LED light	Steady green	Standby (No registration, normal network)
	Steady cyan	Registration success
	Cyan light flash	Talking/Calling/Going
	Red slow flash	Registration failed
	Red slow flash	Network anomaly
	Orange light flash	Upgrade and restore factory
Card reader indicator light	Steady	Standby
	Flashing 1s	A credit card
Power Saving	Light off	Enter the power saving mode
	Indicator light indicates the device status	Exit the power saving mode
Keypad	Steady	Standby
	Light off	Enter the power saving mode





## USER GUIDE

### IP-DB Panel description



### IP-DB Panel introduction

NUMBER	NAME	DESCRIPTION
1	IP Camera infrared lamp	Video signal acquisition and transmission
2	MIC	Audio acquisition
3	DSS key	For speed dial, multicast, intercom, IP broadcast and other functions
4	RFID area	Identification card
5	Speaker	Play sound
6	Photosensitive	Difficulty of sensing light
7	Distance sensor	The distance between the sensing device and the object

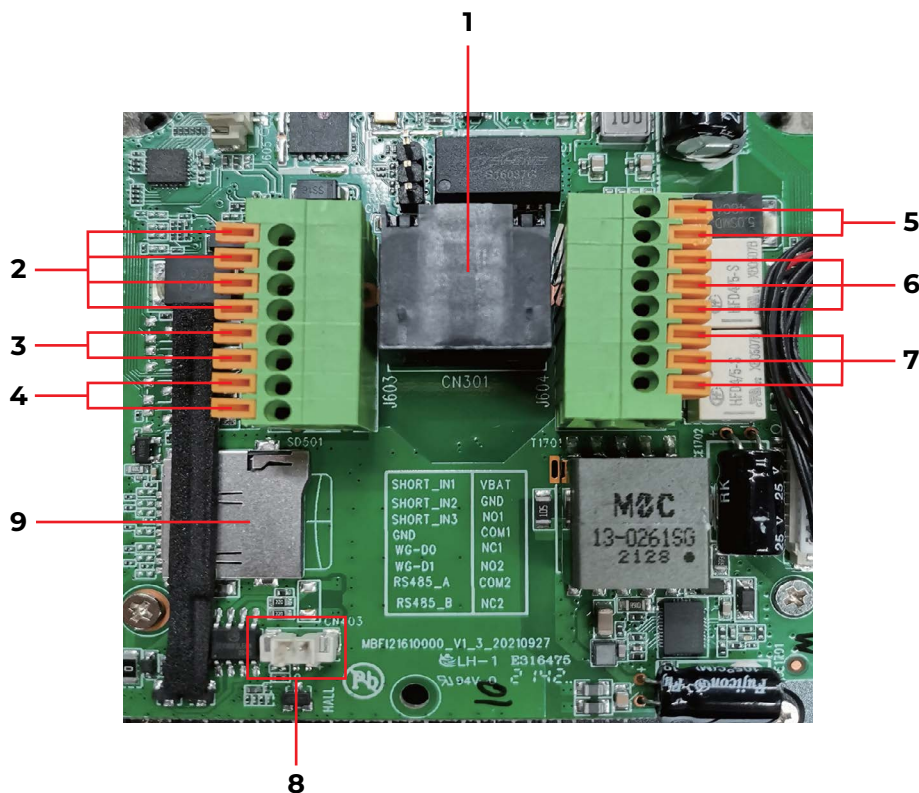


## USER GUIDE

### IP-DB Interface description

Open the rear case of the device, there is a row of terminal blocks for connecting the power supply, electric lock control, etc. The connection is as follows:

#### Interface



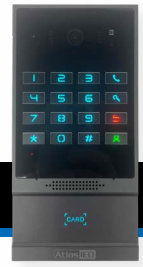
#### Interface

SN	DESCRIPTION
1	Ethernet interface: standard RJ45 interface, 10/100M adaptive, it is recommended to use five or five types of network cable
2	Three groups of short-circuit input detection interfaces: for connecting switches, infrared probes, door magnets, vibration sensors and other input devices
3	Wiegand interface, wiegand in is used to connect wiegand card reader, wiegand out access control controller and other devices
4	RS485 interface
5	Power interface: 12V/1A input, UP-positive electrode, DOWN-negative electrode
6, 7	Two groups of short-circuit output control interface: used to control electric locks, alarms, etc.
8	Line out interface, accessibility aids for the deaf
9	TF interface, support 128G, store snapshot pictures and audio files

# IP-DB

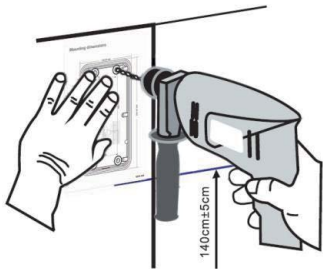
## IP VIDEO DOORBELL

### USER MANUAL

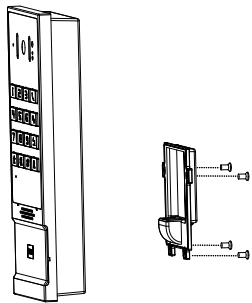


## USER GUIDE

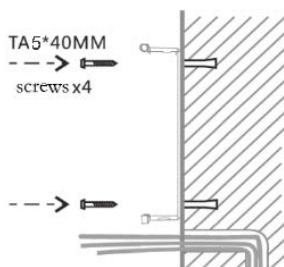
### Installation



1. Draw the installation holes on the wall according to the installation dimension drawing provided by the equipment, use an electric drill to make the vacant place, after drilling the hole, remove the installation dimension drawing, and use a hammer to drive the plastic plug into the drilled hole.



2. Use a screwdriver to loosen the 4 screws on the back, separate the back shell from the wall bracket, and lock the screws on the back of the device at the same time.



3. Align the screw holes of the wall bracket with the holes made on the wall, and fix it to the wall with the supplied screws.

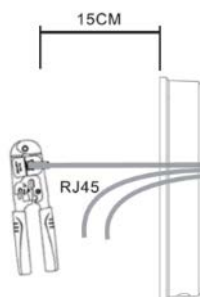
(CONTINUED ON NEXT PAGE)



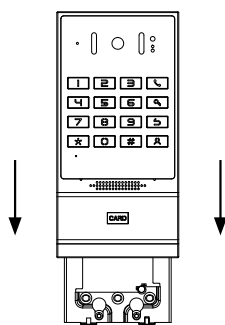


## USER GUIDE

### Installation (continued)



4. Pass all the wires through the silicone plug in the middle of the bottom shell. All wires need to reserve a length of 6"-8".



5. Hang the device and the wall bracket tightly from top to bottom, and tighten the screws at the bottom.

### Installation: Device IP Address

**Method 1:** Connect the speaker, touch and hold the speed-dial button for 3 seconds (30 seconds after power on), wait for the speaker to beep. Press the speed-dial button within 5 seconds, and the system will automatically announce the IP address by voice.

**Method 2:** Touch and hold the speed-dial button for 3 seconds, wait for the speaker to beep, press the speed-dial button three times within 5 seconds, and the system will automatically announce the IP address by voice after successfully switching to the network mode.

### Configuration instructions

DEFAULT CONFIGURATION			
DHCP mode	Default enable	Static IP	192.168.1.128
Voice read IP address	Touch and hold the speed-dial button for 3 seconds, press the speed dial button one times within 5 seconds	Server port	80

# IP-DB

## IP VIDEO DOORBELL

### USER MANUAL



## USER GUIDE

### WEB configuration

When the device and your computer are successfully connected to the network, enter the IP address of the device on the browser as `http://xxx.xxx.xxx.xxx/` and you can see the login interface of the web page management.

### WEB Login

The screenshot shows the AtlasIED web login page. At the top is the AtlasIED logo. Below it is a login form with the following fields: 'User:' with a text input box, 'Password:' with a text input box, and 'Language:' with a dropdown menu set to 'English' and a checkbox. A 'Login' button is at the bottom of the form.

The username and password should be correct to log in to the web page. The default username and password are "admin".





## USER GUIDE

### SIP Configurations

At least one SIP line should be configured properly to enable the telephony service. The line configuration is like a virtualized SIM card. Just like a SIM card on a mobile phone, it stores the service provider and the account information used for registration and authentication. When the device is applied with the configuration, it will register the device to the service provider with the server's address and user's authentication as stored in the configurations.

The SIP line configuration should be set via the WEB configuration page by entering the correct information such as phone number, authentication name/password, SIP server address, server port, etc. which are provided by the SIP server administrator.

WEB interface: After login into the phone page, enter [Line] >> [SIP] and select SIP1/SIP2 for configuration, click apply to complete registration after configuration, as shown below:

### SIP Line Configuration

The screenshot shows the 'SIP' configuration page in the AtlasIED web interface. The left sidebar contains a navigation menu with options: System, Network, Line (selected), Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area has tabs for SIP, SIP Hotspot, Dial Plan, Action Plan, Basic Settings, and Paging Server. The 'SIP' tab is active, showing the 'Line' dropdown set to 'InformaCast@SIP2'. Below this, the 'Register Settings >>' section includes fields for Line Status (Inactive), Username (3019), Display name (InformaCast), Realm, Activate checkbox, Authentication User (3019), Authentication Password (\*\*\*\*), and Server Name. The 'SIP Server 1' section includes Server Address (192.168.1.120), Server Port (5060), Transport Protocol (UDP), and Registration Expiration (3600 seconds). The 'SIP Server 2' section includes similar fields. The 'Proxy Server' section includes Proxy Server Address (192.168.1.120), Proxy Server Port (5060), Proxy User, and Proxy Password. Below these are sections for 'Basic Settings >>', 'Codecs Settings >>', 'Advanced Settings >>', and 'SIP Global Settings >>'. An 'Apply' button is at the bottom.





## USER GUIDE

### Door opening operation

Unlock the door in the following five ways:

1. Open the door by swiping the RFID card, which supports IC card and ID card.
2. Open the door by NFC.
3. The access control helps to call owner, and the owner enters the remote opening password to open the door.
4. The other device helps to call the door phone, enters the corresponding remote authentication code, and opens the door after timeout or the password check length is reached (the authentication code shall be configured in the access list).
5. The door can be opened through the indoor door button when the door phone is in any state.
6. Timed door opening: automatically opens the door in a predetermined time period by setting a timed task.

## BASIC FUNCTION

### Swipe to open the door

- Access control settings on web page → EGS Setting → Add Card Rule → Select "Type" (Normal card provides open door function, Add card and Del card provides add and delete card function. Default Normal card)
- Enter your name and card number (just enter the first 10 digits of the card number), and clicking "Add" to add the card to the list.
- Access the card reading area of the device through the configured ID card (figure 1) to open the door.

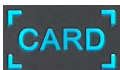


Figure 1

### Card

AtlasIED

Feature Relay Personnel Management Time Profile Logs

Personnel Management > Edit

**Personnel information**

Name

Card Number Type

Card Number

Password Type

Password

Number

Location

CallForward

**Privilege**

Relay ☒ Relay1 ☒ Relay2

Mode

Times



## BASIC FUNCTION

### Remote Door Opening

- Set access control on the web page -> EGS Setting -> Password -> Add password rule -> Select "Remote"
- Enter your name, password and number, add to the password list.
- The owner answers the access control call and presses " \* "(default password) or "123456" (new password) to open the door for visitors.

### Remote Door Opening

AtlasIED

Feature Relay Personnel Management Time Profile Logs

Personnel Management > Edit

Personnel information

Name John Smith

Card Number Type Normal

Card Number 2202729051

Password Type Local & Remote

Password 1361

Number

Location

CallForward

Privilege

Relay ☒ Relay1 ☒ Relay2

Mode Enable

Times 0

Cancel Apply





## BASIC FUNCTION

### Password to Open Door

- Configure access on Web → EGS Setting → Password → Add password rule → Select "Local " (only the i64 supports local password access)
- Enter your your name and password password to the password list.
- Owners and visitors can open the door by entering "6789" (default password) or "123456" (new password) and press # by using the keypad.

The screenshot shows the AtlasIED web interface. On the left is a blue sidebar with a menu: System, Network, Line, Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting (highlighted), and Platform Access. At the top of the main area are tabs: Feature, Relay, Personnel Management (selected), Time Profile, and Logs. The main content area is titled 'Personnel Management > Add'. It contains two sections: 'Personnel Information' and 'Privilege'. The 'Personnel Information' section has fields for Name, Card Number Type (Normal), Card Number, Password Type (Local), Password, Number, Location, and CallForward. The 'Privilege' section has checkboxes for Relay1 and Relay2 (both checked), a Mode dropdown (Enable), and a Times field. At the bottom are 'Cancel' and 'Apply' buttons.



## BASIC FUNCTION

### Making Calls

After setting the function key to Hot key and setting the number, press the function key to immediately call out the set number, as shown below:

### Function Setting

Key	Type	Name	Value	Subtype	Line	Media
DSS Key 1	Key Event			Handfree	AUTO	DEFAULT
DSS Key 2	Key Event			Lock	AUTO	DEFAULT
DSS Key 3	Key Event			Release	AUTO	DEFAULT
DSS Key 4	Memory Key	IP-CONSOLE-GH	192.168.1.51	Speed Dial	IP-CONSOLE-C	DEFAULT
DSS Key 5	Memory Key	IC Trigger	2315	Speed Dial	InformaCast@S	DEFAULT
DSS Key 6	None			None	AUTO	DEFAULT
DSS Key 7	None			None	AUTO	DEFAULT

Apply

Programmable Key Settings >>

Advanced Settings >>

After setting the speed dial according to the above settings, IP-DB can directly dial the set number by pressing the management center button (figure 1).



Figure 1

You can also press the dial button (figure 2) first, then enter the number you want to call, and automatically call after timeout.



Figure 2



## BASIC FUNCTION

### Answering Calls

After setting up the automatic answer and setting up the automatic answer time, it will hear the ringing bell within the set time and automatically answer the call after timeout. Cancel automatic answering. When a call comes in, you will hear the ringing bell and will not answer the phone over time.

### End of the Call

You can hang up the call through the Release key (you can set the function key as the Release key) or turn on the speed dial button to hang up the call.

IP-DB can also use the back button (Figure 1) to hang up the call.



Figure 1

### Auto Answer

The user can turn off the auto-answer function (enabled by default) on the device webpage, and the ring tone will be heard after the shutdown, and the auto-answer will not time out.

**Web interface:** Enter [Line] >> [SIP], Enable auto answer and set auto answer time and click submit.

### WEB line enable auto answer

SIP P2P auto answering:

Enter [Line]>>[Basic settings], Enable auto answer and set auto answer time and click submit.

(CONTINUED ON NEXT PAGE)





## BASIC FUNCTION

### Enable auto answer for IP calls

The screenshot shows the AtlasIED web interface. On the left is a navigation menu with categories: System, Network, Line (selected), Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area has tabs for SIP, SIP Hotspot, Dial Plan, Action Plan, Basic Settings (selected), and Paging Server. Under the Basic Settings tab, there are two sections: STUN Settings and SIP P2P Settings. The STUN Settings section includes fields for STUN NAT Traversal (set to FALSE), Server Address, Server Port (3478), Binding Period (50 seconds), and SIP Waiting Time (800 milliseconds), with an Apply button. The SIP P2P Settings section includes fields for Enable Auto Answering (checked), Auto Answering Delay (0 seconds), DTMF Type (RFC2833), DTMF SIP INFO Mode (Send 10/11), Use VPN (checked), Call-ID Format (Sid@Sip), Display name, User Name, Block RTP When Alerting (unchecked), and Request-Line Format (Normal), with an Apply button.

- Auto Answer Timeout (0~120)  
The range can be set to 0~120s, and the call will be answered automatically when the timeout is set.

### Call Waiting

- Enable call waiting: new calls can be accepted during a call.
- Disable call waiting: new calls will be automatically rejected and a busy signal will be prompted.
- Enable call waiting tone: when you receive a new call on the line, the device will beep.

Users can enable/disable call waiting in the device interface and the web interface.

- Web interface: enter [Intercom Settings] >> [Features], enable/disable call waiting, enable/disable call waiting tone.

(CONTINUED ON NEXT PAGE)



## BASIC FUNCTION

### Call Waiting

Atlas IED

Features Media Settings Camera Settings MCAST Action Time/Date Time Plan

System Network Line Intercom Settings Call List Function Key Security Device Log Security Settings

Basic Settings >>

Enable Call Waiting: ☒ Auto HangUp Delay: 3 (0~30)second(s)

Enable Auto On Hook: ☒ Auto HangUp Tone: ☒ Disable Mute for Ring: ☐

Enable Silent Mode: ☐

Ban Outgoing: ☐ Default Ans Mode: Video Default Dial Mode: Video

Enable Restricted Incoming List: ☒ Enable Restricted Outgoing List: ☒ Enable Country Code: ☐

Country Code: Area Code:

Allow IP Call: ☒ P2P IP Prefix:

Restrict Active URI Source IP: Push XML Server:

Line Display Format: XXX@SIPn Auto Resume Current: ☒

Call Number Filter:

### Call Waiting tone

Atlas IED

Features Media Settings Camera Settings MCAST Action Time/Date Time Plan

System Network Line Intercom Settings Call List Function Key Security Device Log Security Settings EGS Setting Platform Access

Basic Settings >>

Tone Settings >>

Enable Holding Tone: ☒ Enable Call Waiting Tone: ☒

Play Dialing DTMF Tone: ☒ Play Talking DTMF Tone: ☒

Auto Answer Tone: ☒ Boot Up Tone: Default

Network Connected Tone: Default Network Disconnect Tone: Default

Ring Back Tone: Mandatory Local Tone Custom Ringback Sound: Default

Busy Tone: Default Open Failed Prompting: Default

Open Success Prompting: Default Issuing Success Prompting: Default

Close Door Prompting: Default Revoke Prompting: Default

Issuing Failed Prompting: Default Door Sensor Prompting: Default

Revoke Failed Prompting: Default

DND Settings >>

Intercom Settings >>

Response Code Settings >>

Apply



## ADVANCE FUNCTION

### Intercom

The equipment can answer intercom calls automatically.

#### WEB Intercom

The screenshot shows the Atlas IED web interface. On the left is a navigation menu with options: System, Network, Line, Intercom Settings (selected), Call List, and Function Key. The main content area has tabs for Features, Media Settings, Camera Settings, MCAST, Action, Time/Date, and Time Plan. Under the Media Settings tab, there are sections for Basic Settings >>, Tone Settings >>, DND Settings >>, and Intercom Settings >>. The Intercom Settings section contains four checkboxes: Enable Intercom (checked), Enable Intercom Tone (checked), Enable Intercom Mute (unchecked), and Enable Intercom Barge (checked). Below these is a Response Code Settings >> section and an Apply button.

### Intercom

PARAMETERS	DESCRIPTION
Enable Intercom	When the intercom system is enabled, the device will accept the SIP header call-info of the Call request Command automatic call
Enable Intercom Barge	If the option is enabled, device will answer the intercom call automatically while it is in a normal call, and it will reject new intercom call if there is already one intercome call
Enable Intercom Mute	Enable mute during intercom mode
Enable Intercom Ringing	If the incoming call is intercom call, the device plays the intercom tone.

### MCAST

This feature allows user to make some kind of broadcast call to people who are in multicast group. User can configure a multicast DSS Key on the phone, which allows user to send a Real Time Transport Protocol (RTP) stream to the pre-configured multicast address without involving SIP signaling. You can also configure the phone to receive an RTP stream from pre-configured multicast listening address without involving SIP signaling. You can specify up to 10 multicast listening addresses.

(CONTINUED ON NEXT PAGE)



## ADVANCE FUNCTION

### MCAST (continued)

#### MCAST

The screenshot shows the 'MCAST' configuration page in the AtlasIED web portal. The left sidebar contains a navigation menu with options: System, Network, Line, Intercom Settings (selected), Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area is titled 'MCAST Listening' and includes the following settings:

- Sip Priority:** 1 (dropdown)
- Enable Page Priority:** ☐
- Enable Prio Chan:** ☐
- Enable Emer Chan:** ☐
- Intercom Priority:** 1 (dropdown)
- Mcast Listening Renew Time:** 0 (text input)
- Multicast Tone:** ☒

Below these settings is a table for configuring 10 multicast channels:

Index/Priority	Name	Host:port	Channel
1	<input type="text"/>	<input type="text"/>	0 (dropdown)
2	<input type="text"/>	<input type="text"/>	0 (dropdown)
3	<input type="text"/>	<input type="text"/>	0 (dropdown)
4	<input type="text"/>	<input type="text"/>	0 (dropdown)
5	<input type="text"/>	<input type="text"/>	0 (dropdown)
6	<input type="text"/>	<input type="text"/>	0 (dropdown)
7	<input type="text"/>	<input type="text"/>	0 (dropdown)
8	<input type="text"/>	<input type="text"/>	0 (dropdown)
9	<input type="text"/>	<input type="text"/>	0 (dropdown)
10	<input type="text"/>	<input type="text"/>	0 (dropdown)

An 'Apply' button is located below the table. Below the table is the 'MCAST Dynamic' section with the following setting:

- Auto Exit Expires:** 60 (text input)

An 'Apply' button is also present for this section.

#### MCAST

PARAMETERS	DESCRIPTION
Enable Auto MCAST	Send the multicast configuration information by Sip Notify signaling, and the device will configure the information to the system for multicast listening or cancel the multicast listening in the system after receiving the information
Auto MCAST Timeout Delete Time	When a multicast call does not end normally, but for some reason the device can no longer receive a multicast RTP packet, this configuration cancels the listening after a specified time
SIP Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.
Intercom Priority	Compared with multicast and SIP priority, high priority is pluggable and low priority is rejected
Enable Page Priority	Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first.
Enable Mcast Tone	When enabled, play the prompt sound when receiving multicast
Name	Listened multicast server name
Host:port	Listened multicast server's multicast IP address and port.

(CONTINUED ON NEXT PAGE)



## ADVANCE FUNCTION

### MCAST (continued)

#### Multicast:

- Go to web page of [Function Key] >> [Function Key], select the type to multicast, set the multicast address, and select the codec.
- Click Apply.
- Set up the name, host and port of the receiving multicast on the web page of [Intercom Settings] >> [MCAST].
- Press the DSSKey of Multicast Key which you set.
- Receive end will receive multicast call and play multicast automatically.

#### MCAST Dynamic:

Description: send multicast configuration information through SIP notify signaling. After receiving the message, the device configures it to the system for multicast monitoring or cancels multicast monitoring in the system.

### Hotspot

SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand the quantity of sip account. Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, and if any of them answer, the other devices will stop ringing and not be able to answer at the same time. When A B or C device is called out, it is called out with A SIP number registered with device A.

PARAMETERS	DESCRIPTION
Enable Hotspot	Enable or disable hotspot
Mode	This device can only be used as a client
Monitor Type	The monitoring type can be broadcast or multicast. If you want to restrict broadcast packets in the network, you can choose multicast. The type of monitoring on the server side and the client side must be the same, for example, when the device on the client side is selected for multicast, the device on the SIP hotspot server side must also be set for multicast
Monitor Address	The multicast address used by the client and server when the monitoring type is multicast. If broadcasting is used, this address does not need to be configured, and the system will communicate by default using the broadcast address of the device's wan port IP
Remote Port	Fill in a custom hotspot communication port. The server and client ports need to be consistent
Name	Fill in the name of the SIP hotspot. This configuration is used to identify different hotspots on the network to avoid connection conflicts
Line Settings	Sets whether to enable the SIP hotspot function on the corresponding SIP line



(CONTINUED ON NEXT PAGE)



## ADVANCE FUNCTION

### Hotspot (continued)

#### Client Settings:

As a SIP hotspot client, there is no need to set up a SIP account, which is automatically acquired and configured when the device is enabled. Just change the mode to "client" and the other options are set in the same way as the hotspot.

#### SIP hotspot

The screenshot shows the 'SIP Hotspot' settings page in the AtlasIED web interface. The left sidebar contains a navigation menu with options: System, Network, Line (selected), Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area has tabs for SIP, SIP Hotspot, Dial Plan, Action Plan, Basic Settings, and Paging Server. The 'SIP Hotspot' tab is active, showing 'No Registration' status. Below this, the 'SIP Hotspot Settings' section includes: 'Enable Hotspot' (Disabled), 'Mode' (Client), 'Monitor Type' (Broadcast), 'Monitor Address' (224.0.2.0), 'Local Port' (16360), and 'Name' (SIP Hotspot). The 'Line Settings' section shows 'Line 1' and 'Line 2' both set to 'Enabled'. An 'Apply' button is at the bottom.

The device is the hotspot server, and the default extension is 0. The device ACTS as a client, and the extension number is increased from 1 (the extension number can be viewed through the [SIP hotspot] page of the webpage).

Calling internal extension:

- The hotspot server and client can dial each other through the extension number before
- Extension 1 dials extension 0



## WEB CONFIGURATIONS

### Web Page Authentication)

Users can log into the device's web page to manage user device information and operate the device. Users must provide the correct user name and password to log in. If the password is entered incorrectly three times, it will be locked and can be entered again after 5 minutes.

The details are as follows:

- If an IP is logged in more than the specified number of times with a different user name, it will be locked. If a user name logs in more than a specified number of times on a different IP, it is also locked.

### System >> Information

User can get the system information of the device in this page including,

- Model
- Hardware
- Software
- Uptime
- Last uptime
- MEMInfo
- System time

And summarization of network status,

- Network Mode
- MAC
- IP
- Subnet mask
- Default gateway

Besides, summarization of SIP account status,

- SIP User
- SIP account status (Registered / Unapplied / Trying / Timeout )





## WEB CONFIGURATIONS

### System >> Account

#### WEB Account

The screenshot shows the 'WEB Account' configuration page. The top navigation bar includes 'Information', 'Account', 'Configurations', 'Upgrade', 'Auto Provision', 'Tools', and 'Reboot'. The left sidebar lists 'System', 'Network', 'Line', 'Intercom Settings', 'Call List', 'Function Key', and 'Security'. The main content area is titled 'Add New User' and contains fields for 'Username', 'Web Authentication Password', 'Confirm Password', and 'Privilege' (a dropdown menu set to 'Administrators'). Below these fields is an 'Add' button. Under the 'User Accounts' section, there is a table with two columns: 'User' and 'Privilege'. The table contains one entry: 'admin' with 'Administrators' as the privilege. Below the table is a 'User Management' section with a dropdown menu showing 'admin' and 'Delete' and 'Modify' buttons.

On this page the user can change the password for the login page.

Users with administrator rights can also add or delete users, manage users, and set permissions and passwords for new users.

### System >> Configurations

On this page, users with administrator privileges can view, export, or import the phone configuration, or restore the phone to factory Settings.

#### System Setting

The screenshot shows the 'System Setting' configuration page. The top navigation bar includes 'Information', 'Account', 'Configurations', 'Upgrade', 'Auto Provision', 'Tools', and 'Reboot'. The left sidebar lists 'System', 'Network', 'Line', 'Intercom Settings', 'Call List', 'Function Key', 'Security', 'Device Log', 'Security Settings', 'EGS Setting', and 'Platform Access'. The main content area is titled 'Export Configurations' and contains three instructions: 'Right click here to SAVE configurations in \'.txt\' format.', 'Right click here to SAVE nc configurations in \'.txt\' format.', and 'Right click here to SAVE configurations in \'.xml\' format.'. Below these instructions is an 'Import Configurations' section with a 'Configuration file:' label, a text input field, and 'Select' and 'Import' buttons. Under the 'Clear Configuration >>' section, there is a message: 'Click \'.Clear\' button to reset the configuration files!'. Below this message are two lists: 'Content to Keep' (MMI, BASIC NETWORK, SIP, AUTOPROVISION) and 'Content to Reset' (DSS KEY, TR069). Between these lists are two arrows (one pointing right, one pointing left). At the bottom of the page is a 'Clear' button.





## WEB CONFIGURATIONS

### System >> Configurations (continued)

- **Export Configurations**  
Right click to select target save as, that is, to download the device's configuration file, suffix ".txt". (note: profile export requires administrator privileges)
- **Import Configurations**  
Import the configuration file of Settings. The device will restart automatically after successful import, and the configuration will take effect after restart
- **Clear Configurations**  
Select the module in the configuration file to clear.  
- **SIP:** account configuration.  
- **AUTOPROVISION:** automatically upgrades the configuration TR069:TR069 related configuration  
- **MMI:** MMI module, including authentication user information, web access protocol, etc. DSS Key: DSS Key configuration
- **Clear Tables**  
Select the local data table to be cleared, all selected by default.
- **Reset IP-DB**  
The phone data will be cleared, including configuration and database tables.

### System >> Upgrade

#### Upgrade

The screenshot shows the 'Upgrade' section of the IP-DB web interface. The interface has a blue header with the 'Atlas IED' logo and a navigation bar with tabs: Information, Account, Configurations, Upgrade, Auto Provision, Tools, and Reboot. A left sidebar shows a tree view with 'System' selected. The main content area is divided into several sections:

- Software Upgrade:** Shows 'Current Software Version: 1.2.5.3' and a 'System Image File' field with a 'Select' button and an 'Upgrade' button.
- Upgrade Server:** Shows 'Upgrade Server Address1' and 'Upgrade Server Address2' fields with an 'Apply' button.
- Firmware Information:** Shows 'Current Software Version: 1.2.5.3', 'Server Firmware Version: Checking', and an 'Upgrade' button. Below it is a 'New Firmware Information' field.
- Ring Upgrade:** Shows a 'Load Server File' field with a 'Select' button and an 'Upload' button. A note indicates supported formats: '(\*.wav, \*.mp3)'.
- Ring List:** A table with columns 'Index', 'File Name', and 'File Size'. There is a 'Delete' button at the bottom right of the table.

Upgrade the software version of the device, and upgrade to the new version through the webpage. After the upgrade, the device will automatically restart and update to the new version.

Click select, select the version and then click upgrade.

Upgrade the ringtone, support wav and MP3 format.



## WEB CONFIGURATIONS

**System >> Upgrade** (continued)

### Firmware Upgrade:

- Web page: Login phone web page, go to [System] >> [Upgrade].

### Web page firmware upgrade

The screenshot shows the 'Upgrade' tab in the web interface. The left sidebar contains a menu with 'System' selected. The main content area is titled 'Software Upgrade' and includes the following sections:

- Current Software Version:** 1.2.5.3
- System Image File:** A text input field with a 'Select' button and an 'Upgrade' button.
- Upgrade Server:**
  - Upgrade Server Address1:** A text input field.
  - Upgrade Server Address2:** A text input field.
  - Apply:** A button.
- Firmware Information:**
  - Current Software Version:** 1.2.5.3
  - Server Firmware Version:** Checking
  - Upgrade:** A button.
  - New Firmware Information:** A text input field.
- Ring Upgrade:**
  - Load Server File:** A text input field with a 'Select' button and an 'Upload' button.
  - File Type:** (\*.wav, \*.mp3)
- Ring List:** A table with columns: Index, File Name, File Size, and a 'Delete' button.

### Firmware upgrade

PARAMETER	DESCRIPTION
<b>UPGRADE SERVER</b>	
Enable Auto Upgrade	Enable automatic upgrade, If there is a new version txt and new software firmware on the server, phone will show a prompt upgrade message after Update Interval.
Upgrade Server Address1	Set available upgrade server address.
Upgrade Server Address2	Set available upgrade server address.
Update Interval	Set Update Interval.
<b>FIRMWARE INFORMATION</b>	
Current Software Version	It will show Current Software Version.
Server Firmware Version	It will show Server Firmware Version.
[Upgrade] button	If there is a new version txt and new software firmware on the server, the page will display version information and upgrade button will become available; Click [Upgrade] button to upgrade the new firmware.
New version description information	When there is a corresponding TXT file and version on the server side, the TXT and version information will be displayed under the new version description information.



## WEB CONFIGURATIONS

### System >> Upgrade (continued)

#### Firmware Upgrade: (continued)

- The file requested from the server is a TXT file called vendor\_model\_hw10.txt. Hw followed by the hardware version number, it will be written as hw10 if no difference on hardware. All Spaces in the filename are replaced by underline.
- The URL requested by the phone is HTTP:// server address/vendor\_Model\_hw10.tx : The new version and the requested file should be placed in the download directory of the HTTP server, as shown in the figure:
- TXT file format must be UTF-8
- vendor\_model\_hw10.TXT The file format is as follows:  
Version=1.6.3 #Firmware  
Firmware=xxx/xxx.z #URL, Relative paths are supported and absolute paths are possible, distinguished by the presence of protocol headers.  
BuildTime=2018.09.11 20:00  
Info=TEXT|XML  
  
Xxxxx  
Xxxxx  
Xxxxx  
Xxxxx
- After the interval of update cycle arrives, if the server has available files and versions, the phone will prompt as shown below. Click [view] to check the version information and upgrade.





## WEB CONFIGURATIONS

### System >> Auto Provision

Webpage: Login and go to [System] >> [Auto provision].

#### Auto provision settings

The screenshot shows the 'Auto Provision' settings page. The left sidebar contains a menu with options: System, Network, Line, Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area is titled 'Basic Settings' and includes the following fields:

- CPE Serial Number: 00100400FV02001000000d84a0d4558
- Authentication Name: [Text Input]
- Authentication Password: [Text Input]
- Configuration File Encryption Key: [Text Input]
- General Configuration File Encryption Key: [Text Input]
- Download Fail Check Times: 1
- Save Auto Provision Information: ☐
- Download CommonConfig Enabled: ☒
- Enable Server Digest: ☐
- List Update Mode: Add

Below the basic settings, there are links to expand other sections: DHCP Option >>, DHCPv6 Option >>, SIP Plug And Play (PnP) >>, Plug and Play >>, Static Provisioning Server >>, Autoprovision Now >>, TR069 >>, and MDNS >>. An 'Apply' button is located at the bottom right of the form.

Devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods are enabled, the priority from high to low as below:

**PNP>DHCP>TR069> Static Provisioning**

Transferring protocol: FTP, TFTP, HTTP, HTTPS

#### Auto provision

Auto Provision	
PARAMETERS	DESCRIPTION
<b>BASIC SETTINGS</b>	
CPE Serial Number	Display the device SN
Authentication Name	The user name of provision server
Authentication Password	The password of provision server
Configuration File Encryption Key	If the device configuration file is encrypted , user should add the encryption key here
General Configuration File Encryption Key	If the common configuration file is encrypted, user should add the encryption key here

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

### System >> Auto Provision (continued)

Save Auto Provision Information	Save the HTTP/HTTPS/FTP user name and password. If the provision URL is kept, the information will be kept.
Download	Whether phone will download the common configuration file.
Common Config enabled	
Enable Get Digest From Server	When the feature is enable, if the configuration of server is changed, phone will download and update.
<b>DHCP OPTION</b>	
Option Value	Configure DHCP option, DHCP option supports DHCP custom option   DHCP option 66   DHCP option 43, 3 methods to get the provision URL. The default is Option 66.
Custom Option Value must be same as server define.	Custom Option value is allowed from 128 to 254. The option value
Enable DHCP Option 120	Use Option120 to get the SIP server address from DHCP server.
<b>DHCPv6 OPTION</b>	
Option Value	Configure DHCPv6 option, DHCPv6 option supports custom option   option 66   option 43, 3 methods to get the provision URL. The default is Disable.
Custom Option Value	Custom option number. Must be from 128 to 254.
Enable DHCP Option 120	Set the SIP server address through DHCP option 120.
<b>SIP PLUG AND PLAY (PnP)</b>	
Enable SIP PnP	Whether enable PnP or not. If PnP is enabled, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature will respond and send a Notify with URL to phone. Phone could get the configuration file with the URL.
Server Address	Broadcast address. As default, it is 224.0.0.0.
Server Port	PnP port
Transport Protocol	PnP protocol, TCP or UDP.
Update Interval	PnP message interval.
<b>STATIC PROVISIONING SERVER</b>	
Server Address	Provisioning server address. Support both IP address and domain address.
Configuration File Name	The configuration file name. If it is empty, phone will request the common file and device file which is named as its MAC address. The file name could be a common name, \$mac.cfg, \$input.cfg. The file format supports CFG/TXT/XML.
Protocol Type	Transferring protocol type, supports FTP, TFTP, HTTP and HTTPS
Update Interval	Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour.
Update Mode	Provision Mode. 1. Disabled. 2. Update after reboot. 3. Update after interval.

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

System >> Auto Provision (continued)

STATIC PROVISIONING SERVER	
<b>TR069</b>	
Enable TR069	Enable TR069 after selection
ACS Server Type	There are 2 options Serve type, common and CTC.
ACS Server URL	ACS server address
ACS User	ACS server username (up to is 59 character)
ACS Password	ACS server password (up to is 59 character)
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
TLS Version	TLS Version
STUN server address	Enter the STUN address
Enable the STUN	Enable the STUN

System >> FDMS

FDMS

FDMS

FDMS INFORMATION SETTINGS	
Community Designations	Name of equipment installation community
Building a movie theater	Name of equipment installation building
Room Number	Equipment installation room name



## WEB CONFIGURATIONS

### System >> Tools

This page gives the user the tools to solve the problem.

#### Tools

The screenshot shows the web configuration interface for the IP-DB device. The top navigation bar includes tabs for Information, Account, Configurations, Upgrade, Auto Provision, Tools, and Reboot. The left sidebar lists various system settings categories. The main content area is titled 'Tools' and contains several sections: Syslog, Web Capture, Oneclick Export Debug Info, Watch Dog, and Diagnostics. Each section has specific configuration options and buttons.

Section	Configuration Options
Syslog	<ul style="list-style-type: none"><li>Enable Syslog: <input type="checkbox"/></li><li>Server Address: <input type="text" value="0.0.0.0"/></li><li>Server Port: <input type="text" value="514"/></li><li>APP Log Level: <input type="text" value="Warning"/></li><li>Export Log: <input type="checkbox"/></li><li>Apply button</li></ul>
Web Capture	<ul style="list-style-type: none"><li>Start button</li><li>stop button</li></ul>
Oneclick Export Debug Info	<ul style="list-style-type: none"><li>Oneclick Export De button</li></ul>
Watch Dog	<ul style="list-style-type: none"><li>Enable Watch Dog: <input checked="" type="checkbox"/></li><li>Apply button</li></ul>
Diagnostics	<ul style="list-style-type: none"><li>Command Option: <input type="text" value="PING"/></li><li>IP Address: <input type="text"/></li><li>Diagnostics Result: <input type="text"/></li><li>Start button</li><li>stop button</li></ul>

**Syslog:** When enabled, set the syslog software address, and log information of the device will be recorded in the syslog software during operation. If there is any problem, log information can be analyzed by technical support.

### System >> Reboot

This page can restart the device.

The screenshot shows the 'Reboot' section of the web configuration interface. It contains a single button labeled 'Reboot' and a text instruction: 'Click [Reboot] button to restart!'.

Reboot

Click [Reboot] button to restart!

Reboot



## WEB CONFIGURATIONS

### Network >> Basic

This page allows users to configure network connection types and parameters.

#### Network Basic Setting

The screenshot shows the 'Network Basic Setting' page. On the left is a sidebar with a tree view containing: System, Network (selected), Line, Intercom Settings, Call List, Function Key, Security, Device Log, and Security Settings. The main content area has tabs for 'Basic', 'Service Port', 'VPN', and 'Advanced'. Under the 'Basic' tab, there are sections for 'Network Mode' (set to 'IPv4 Only'), 'IPv4 Network Status' (showing IP: 192.168.1.69, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, and MAC: 00:d8:4a:0d:45:58), and 'IPv4 Settings'. The 'IPv4 Settings' section has three radio buttons: 'Static IP' (selected), 'DHCP', and 'PPPoE'. Below these are input fields for IP, Subnet Mask, Default Gateway, Primary DNS Server, Secondary DNS Server, and DNS Domain.

#### Network Basic Setting

FIELD NAME	EXPLANATION
<b>IPv4 NETWORK STATUS</b>	
IP	The current IP address of the equipment
Subnet mask	The current Subnet Mask
Default gateway	The current Gateway IP address
MAC	The MAC address of the equipment
<b>IPv4 SETTINGS</b>	
<b>SETTINGS</b>	
Select the appropriate network mode. The equipment supports three network modes:	
Static IP	Network parameters must be entered manually and will not be changed. All parameters are provided by the ISP.
DHCP	Network parameters are provided automatically by a DHCP server.
If Static IP is chosen, the screen below will appear. Enter values provided by the ISP.	
DNS Server Configured by	Select the Configured mode of the DNS Server.
Primary DNS Server	Enter the server address of the Primary DNS.
Secondary DNS Server	Enter the server address of the Secondary DNS.
DNS Domain	Enter the domain of the DNS.





## WEB CONFIGURATIONS

### Network >> Basic (continued)

#### Attention:

- 1) After setting the parameters, click [Apply] to take effect.
- 2) If you change the IP address, the webpage will no longer responds, please enter the new IP address in web browser to access the device.
- 3) If the system USES DHCP to obtain IP when device boots up, and the network address of the DHCP Server is the same as the network address of the system LAN, then after the system obtains the DHCP IP, it will add 1 to the last bit of the network address of LAN and modify the IP address segment of the DHCP Server of LAN. If the DHCP access is reconnected to the WAN after the system is started, and the network address assigned by the DHCP server is the same as that of the LAN, then the WAN will not be able to obtain IP access to the network

### Network >> service port

This page provides the settings of webpage login protocol, protocol port and RTP port.

#### Service port setting interface

The screenshot shows the 'Service Port Settings' page in the Atlas IED web configuration tool. The page has a blue header with the Atlas IED logo and four tabs: Basic, Service Port, VPN, and Advanced. The 'Service Port' tab is selected. On the left, there is a sidebar with a tree view containing: System, Network (selected), Line, Intercom Settings, Call List, Function Key, and Security. The main content area is titled 'Service Port Settings' with a help icon. It contains the following settings:

- Web Server Type: HTTP (dropdown menu)
- Web Logon Timeout: 15 (text input) (10~60)Minute
- Web Auto Login: ☐
- HTTP Port: 80 (text input)
- HTTPS Port: 443 (text input)
- RTP Port Range Start: 10000 (text input) (1025~65530)
- RTP Port Quantity: 1000 (text input) (10~1000)

An 'Apply' button is located at the bottom right of the settings area.

#### Server Port

PARAMETER	DESCRIPTION
Web server type	Restart after setting takes effect. Optional web login as HTTP/HTTPS
Web login timeout	The default is 15 minutes, the timeout will automatically log out of the login page, and you need to log in again
Web page automatic login	No need to enter the user name and password after the timeout, it will automatically log in to the web page.
HTTP port	The default is 80, if you want system security, you can set other por Such as: 8080, web page login: HTTP://ip:8080 t
HTTPS port	The default is 443, same as HTTP port usage
RTP port start range	The value range is 1025-65535. The value of rtp port starts from the initial value set. Each time a call is made, the value of the voice and video ports is increased by 2
RTP port quantity	Number of calls



## WEB CONFIGURATIONS

### Network >> VPN

#### Network VPN Settings

Virtual Private Network (VPN) Status

VPN IP Address: 0.0.0.0

**VPN Mode**

Enable VPN: ☐

Enable NAT: ☐

L2TP: ☐ OpenVPN: ☐

Open VPN mode: tun

**Layer 2 Tunneling Protocol (L2TP)**

L2TP Server Address: 0.0.0.0

Authentication Name:

Authentication Password:

Apply

**OpenVPN Files**

Load OpenVPN File:  Select Upload

**Certificates List**

Index	File Name	File Size
-------	-----------	-----------

Virtual Private Network (VPN) is a technology to allow device to create a tunneling connection to a server and becomes part of the server's network. The network transmission of the device may be routed through the VPN server.

For some users, especially enterprise users, a VPN connection might be required to be established before activate a line registration. The device supports two VPN modes, Layer 2 Transportation Protocol (L2TP) and OpenVPN.

The VPN connection must be configured and started (or stopped) from the device web portal.

#### • L2TP

**NOTICE! The device only supports non-encrypted basic authentication and non-encrypted data tunneling. For users who need data encryption, please use OpenVPN instead.**

To establish a L2TP connection, users should log in to the device web portal, open page [Network] -> [VPN]. In VPN Mode, check the "Enable VPN" option and select "L2TP", then fill in the L2TP server address, Authentication Username, and Authentication Password in the L2TP section. Press "Apply" then the device will try to connect to the L2TP server.

When the VPN connection established, the VPN IP Address should be displayed in the VPN status. There may be some delay of the connection establishment. User may need to refresh the page to update the status.

Once the VPN is configured, the device will try to connect to the VPN automatically when the device boots up every time until user disable it. Sometimes, if the VPN connection does not established immediately, user may try to reboot the device and check if VPN connection established after reboot.



## WEB CONFIGURATIONS

### Network >> VPN (continued)

#### • OpenVPN

To establish an OpenVPN connection, user should get the following authentication and configuration files from the OpenVPN hosting provider and name them as the following,

OpenVPN Configuration file:	client.ovpn
CA Root Certification:	ca.crt
Client Certification:	client.crt
Client Key:	client.key

User then upload these files to the device in the web page [Network] -> [VPN], Section OpenVPN Files. Then user should check "Enable VPN" and select "OpenVPN" in VPN Mode and click "Apply" to enable OpenVPN connection.

Same as L2TP connection, the connection will be established every time when system rebooted until user disable it manually.

### Network >> Advanced

#### Network Setting

The screenshot displays the 'Network Setting' page in the AtlasIED web interface. The left sidebar shows a navigation menu with options: System, Network (selected), Line, Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area has tabs for Basic, Service Port, VPN, and Advanced. The 'Advanced' tab is active, showing various network configuration sections:

- Link Layer Discovery Protocol (LLDP) Settings:** Includes checkboxes for 'Enable LLDP' and 'Enable Learning Function', and a 'Packet Interval' field set to 60 seconds.
- Cisco Discovery Protocol (CDP) Settings:** Includes a checkbox for 'Enable CDP' and a 'Packet Interval' field set to 60 seconds.
- DHCP VLAN Settings:** Includes dropdowns for 'Option Value' (set to Disabled) and 'Option Value Data Type' (set to Auto), and a text field for 'DHCP Option Vlan' set to 0.
- Quality Of Service (QoS) Settings:** Includes checkboxes for 'Enable DSCP', and fields for 'Audio DSCP' (46), 'Signal DSCP' (46), and 'Video DSCP' (46).
- ARP Cache Life:** Includes a text field for 'ARP Cache Life' set to 2 minutes.
- WAN VLAN Settings:** Includes checkboxes for 'Enable VLAN', and fields for 'WAN VLAN ID' (256), '802.1p Signal Priority' (0), and '802.1p Media Priority' (0).

An 'Apply' button is located at the bottom right of the settings area.

Network advanced Settings are typically configured by IT administrators to improve the quality of device service.



## WEB CONFIGURATIONS

**Network >> Advanced** (continued)

### Network Setting

FIELD NAME	EXPLANATION
<b>LLDP SETTINGS</b>	
Enable LLDP	Enable or disable LLDP
Packet Interval	LLDP Send detection cycle
Enable Learning Function	Learn the discovered device information on the device
<b>QoS SETTINGS</b>	
Pattern	Voice quality assurance (off by default)
<b>DHCP VLAN SETTINGS</b>	
Parameters values	128-254, Obtain the VLAN value through DHCP
<b>WAN PORT VIRTUAL WAN</b>	
WAN port virtual Wan	WAN port Settings
<b>LAN PORT VIRTUAL LAN</b>	
LAN port virtual LAN	LAN port Settings
<b>802.1X</b>	
Enable 802.1X	Enable or disable 802.1X
Username	Confirm Username
Password	Confirm Password





## WEB CONFIGURATIONS

Line >> SIP

SIP

Atlas IED

SIP SIP Hotspot Dial Plan Action Plan Basic Settings Paging Server

Line: InformaCast@SIP2

**Register Settings >>**

Line Status: Inactive	Activate: <input type="checkbox"/>
Username: 3019	Authentication User: 3019
Display name: InformaCast	Authentication Password: ****
Realm:	Server Name:

**SIP Server 1:**

Server Address: 192.168.1.120

Server Port: 5060

Transport Protocol: UDP

Registration Expiration: 3600 second(s)

Proxy Server Address: 192.168.1.120

Proxy Server Port: 5060

Proxy User:

Proxy Password:

**SIP Server 2:**

Server Address:

Server Port: 5060

Transport Protocol: UDP

Registration Expiration: 3600 second(s)

Backup Proxy Server Address:

Backup Proxy Server Port: 5060

**Basic Settings >>**

**Basic Settings >>**

Enable Auto Answering: <input checked="" type="checkbox"/>	Auto Answering Delay: 0 (0~120)second(s)
Enable Hotline: <input type="checkbox"/>	Hotline Delay: 0 (0~30)second(s)
Dial Without Registered: <input checked="" type="checkbox"/>	Hotline Number:
DTMF Type: AUTO	DTMF SIP INFO Mode: Send 10/11
Request With Port: <input checked="" type="checkbox"/>	Enable DND: <input type="checkbox"/>
Use STUN: <input type="checkbox"/>	Use VPN: <input checked="" type="checkbox"/>
Enable Failback: <input checked="" type="checkbox"/>	Signal Failback: <input type="checkbox"/>
Failback Interval: 1800 second(s)	Signal Retry Counts: 3 (1~10)

**Basic Settings >>**

**Codecs Settings >>**

Disabled Codecs:	Enabled Codecs:
G.726-16 G.726-24 G.726-32 G.726-40 G.723.1 MPA	G.722 G.711U G.711A G.729AB opus iLBC





## WEB CONFIGURATIONS

Line >> SIP (continued)

### SIP

PARAMETERS	DESCRIPTION
<b>REGISTER SETTINGS</b>	
Line Status	Display the current line status at page loading. To get the up to date line status, user has to refresh the page manually.
Activate	Whether the service of the line should be activated
Username	Enter the username of the service account.
Authentication User	Enter the authentication user of the service account
Display Name	Enter the display name to be sent in a call request.
Authentication Password	Enter the authentication password of the service account
Realm	Enter the SIP domain if requested by the service provider
Server Name	Input server name.
<b>SIP SERVER 1</b>	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
<b>SIP SERVER 2</b>	
Server Address	Enter the IP or FQDN address of the SIP server
Server Port	Enter the SIP server port, default is 5060
Transport Protocol	Set up the SIP transport line using TCP or UDP or TLS.
Registration Expiration	Set SIP expiration date.
SIP Proxy Server Address	Enter the IP or FQDN address of the SIP proxy server.
Proxy Server Port	Enter the SIP proxy server port, default is 5060.
Proxy User	Enter the SIP proxy user.
Proxy Password	Enter the SIP proxy password.
Backup Proxy Server Address	Enter the IP or FQDN address of the backup proxy server.
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060.
<b>BASIC SETTINGS</b>	
Enable Auto Answering	Enable auto-answering, the incoming calls will be answered automatically after the delay time
Auto Answering Delay	Set the delay for incoming call before the system automatically answered it
Enable Hotline	Enable hotline configuration, the device will dial to the specific number immediately at audio channel opened by off-hook handset or turn on hands-free speaker or headphone

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

Line >> SIP (continued)

Hotline Delay	Set the delay for hotline before the system automatically dialed it
Hotline Number	Set the hotline dialing number
Dial Without Registered	Set call out by proxy without registration
Enable Missed Call Log	If enabled, the phone will save missed calls into the call history record.
DTMF Type	Set the DTMF type to be used for the line
Use VPN	Set the line to use VPN restrict route
Use STUN	Set the line to use STUN for NAT traversal
Enable Failback	Whether to switch to the primary server when it is available.
Failback Interval	A Register message is used to periodically detect the time interval for the availability of the main Proxy.
Signal Failback	Multiple proxy cases, whether to allow the invite/register request to also execute failback.
Signal Retry Counts	The number of attempts that the SIP Request considers proxy unavailable under multiple proxy scenarios.
Codecs Settings	Set the priority and availability of the codecs by adding or remove them from the list.
<b>ADVANCED SETTINGS</b>	
Use Feature Code	When this setting is enabled, the features in this section will not be handled by the device itself but by the server instead. In order to control the enabling of the features, the device will send feature code to the server by dialing the number specified in each feature code field.
Enable Blocking Anonymous Call	Set the feature code to dial to the server
Disable Blocking Anonymous Call	Set the feature code to dial to the server
Call Waiting On Code	Set the feature code to dial to the server
Call Waiting Off Code	Set the feature code to dial to the server
Send Anonymous On Code	Set the feature code to dial to the server
Send Anonymous Off Code	Set the feature code to dial to the server
Enable Session Timer	Set the line to enable call ending by session timer refreshment. The call session will be ended if there is not new session timer event update received after the timeout period
Session Timeout	Set the session timer timeout period
BLF Server	The registered server will receive the subscription package from ordinary application of BLF phone. Please enter the BLF server, if the sever does not support subscription package, the registered server and subscription server will be separated.
Keep Alive Type	Set the line to use dummy UDP or SIP OPTION packet to keep NAT pinhole opened
Keep Alive Interval	Set the keep alive packet transmitting interval
Keep Authentication	Keep the authentication parameters from previous authentication
Blocking Anonymous Call	Reject any incoming call without presenting caller ID
User Agent	Set the user agent, the default is Model with Software Version.

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

Line >> SIP (continued)

Specific Server Type	Set the line to collaborate with specific server type
SIP Version	Set the SIP version
Anonymous Call Standard	Set the standard to be used for anonymous
Local Port	Set the local port
Ring Type	Set the ring tone type for the line
Enable user=phone	Sets user=phone in SIP messages.
Use Tel Call	Set use tel call
Auto TCP	Using TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes
Enable Rport	Set the line to add rport in SIP headers
Enable PRACK	Set the line to support PRACK SIP message
DNS Mode	Select DNS mode, A, SRV, NAPTR
Enable Long Contact	Allow more parameters in contact field per RFC 3840
Enable Strict Proxy	Enables the use of strict routing. When the phone receives packets from the server, it will use the source IP address, not the address in via field.
Convert URI	Convert not digit and alphabet characters to %hh hex code
Use Quote In Display Name	Whether to add quote in display name, i.e. "VoIP" vs VoIP
Enable GRUU	Support Globally Routable User-Agent URI (GRUU)
Sync Clock Time	Time Sync with server
Enable Inactive Hold	With the post-call hold capture package enabled, you can see that in the INVITE package, SDP is inactive.
Caller ID Header	Set the Caller ID Header
Use 182 Response for Call waiting	Set the device to use 182 response code at call waiting response
Enable Feature Sync	Feature Sync with server
Enable SCA	Enable/Disable SCA (Shared Call Appearance )
CallPark Number	Set the CallPark number.
Server Expire	Set the timeout to use the server.
TLS Version	Choose TLS Version.
uaCSTA Number	Set uaCSTA Number.
Enable Click to Talk	With the use of special server, click to call out directly after enabling.
Enable Chgport	Whether port updates are enabled.
Intercom Number	Set Intercom Number.
Unregister On Boot	Whether to enable logout function.

(CONTINUED ON NEXT PAGE)





## WEB CONFIGURATIONS

### Line >> SIP (continued)

Enable MAC Header	Whether to open the registration of SIP package with user agent with MAC or not.
Enable Register MAC Header	Whether to open the registration is user agent with MAC or not.
PTime(ms)	Set whether to bring ptime field, default no.
<b>SIP GLOBAL SETTINGS</b>	
Strict Branch	Set up to strictly match the Branch field.
Enable Group	Set open group.
Enable RFC4475	Set to enable RFC4475.
Enable Strict UA Match	Enable strict UA matching
Registration Failure Retry Time	Set the registration failure retry time.
Local SIP Port	Modify the phone SIP port.
Enable uaCSTA	Set to enable the uaCSTA function.

### Line >> SIP Hotspot

SIP hotspot is a simple and practical function. It is simple to configure, can realize the function of group vibration, and can expand the number of SIP accounts.

### Line >> Dial Plan

#### Dial Plan

**Basic Settings**

☐ Press # to invoke dialing
 ☐ Dial Fixed Length  to Send
 ☒ Send after  second(s)(3~30)
 ☐ Press # to Do Blind Transfer
 ☐ Blind Transfer on Onhook
 ☐ Attended Transfer on Onhook
 ☐ Attended Transfer on Conference Onhook
 ☐ Enable E.164

#### Phone 7 Dialing Methods

PARAMETERS	DESCRIPTION
Press # to invoke dialing	The user dials the other party's number and then adds the # number to dial out;
Dial Fixed Length	The number entered by the user is automatically dialed out when it reaches a fixed length
Timeout dial	The system dials automatically after timeout



## WEB CONFIGURATIONS

### Line >> Dial Plan (continued)

Dial Plan Add:

#### Custom Setting of Dial-Up Rules

#### Dial Plan Add

Digit Map:

Apply to Call: Outgoing Call

Match to Send: No

Media: Default

Line: SIP DIALPEER

Destination:

Port:

Alias(Optional): No Alias

Phone Number:

Length:

Suffix:

Add

#### Dial Plan Option

Delete Modify

#### User-defined Dial Plan Table

Index	Digit Map	Call	Match to Send	Line	Alias Type: Number(length)	Suffix	Media
-------	-----------	------	---------------	------	----------------------------	--------	-------

#### Dial-Up Rule Configuration Table

PARAMETERS	DESCRIPTION
<b>Dial rule</b>	There are two types of matching: Full Matching or Prefix Matching. In Full matching, the entire phone number is entered and then mapped per the Dial Peer rules. In prefix matching, only part of the number is entered followed by T. The mapping with then take place whenever these digits are dialed. Prefix mode supports a maximum of 30 digits.
<b>Note: Two different special characters are used.</b> <ul style="list-style-type: none"> <li>• x – Matches any single digit that is dialed.</li> <li>• [ ] – Specifies a range of numbers to be matched. It may be a range, a list of ranges separated by commas, or a list of digits.</li> </ul>	
<b>Destination</b>	Set Destination address. This is for IP direct
<b>Port</b>	Set the Signal port, and the default is 5060 for SIP.
<b>Alias</b>	Set the Alias. This is the text to be added, replaced or deleted. It is an optional item.
<b>Note: There are four types of aliases.</b> <ul style="list-style-type: none"> <li>• all: xxx – xxx will replace the phone number.</li> <li>• add: xxx – xxx will be dialed before any phone number.</li> <li>• del – The characters will be deleted from the phone number.</li> <li>• rep: xxx – xxx will be substituted for the specified characters.</li> </ul>	
<b>Suffix</b>	Characters to be added at the end of the phone number. It is an optional item.
<b>Length</b>	Set the number of characters to be deleted. For example, if this is set to 3, the phone will delete the first 3 digits of the phone number. It is an optional item.



## WEB CONFIGURATIONS

### Line >> Dial Plan (continued)

This feature allows the user to create rules to make dialing easier. There are several different options for dialing rules. The examples below will show how this can be used.

**Example 1: All Substitution** – Assume that it is desired to place a direct IP call to IP address 172.168.2.208. Using this feature, 123 can be substituted for 172.168.2.208.

#### Dial rules table (1)

User-defined Dial Plan Table ?							
Index	Digit Map	Call	Match to Send	Line	Alias Type: Number(length)	Suffix	Media
1	"123"	Out	No	SIP DIALPEER(172.16.1.15:5560)			Default

**Example 2: Partial Substitution** – To dial a long-distance call to Beijing requires dialing area code 010 before the local phone number. Using this feature 1 can be substituted for 010. For example, to call 62213123 would only require dialing 162213123 instead of 01062213123.

#### Dial rules table (2)

User-defined Dial Plan Table ?							
Index	Digit Map	Call	Match to Send	Line	Alias Type: Number(length)	Suffix	Media
1	"1T"	Out	No	Fanvil@SIP1	rep:010(1)		Default

**Example 3: Addition** – Two examples are shown. In the first case, it is assumed that 0 must be dialed before any 11-digit number beginning with 13. In the second case, it is assumed that 0 must be dialed before any 11-digit number beginning with 135, 136, 137, 138, or 139. Two different special characters are used.

x – Matches any single digit that is dialed.

[ ] – Specifies a range of numbers to be matched. It may be a range, a list of ranges separated by commas, or a list of digits.

### Line >> Action Plan

#### Action Plan

Atlas IED

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

SIP

SIP Hotspot

Dial Plan

Action Plan

Basic Settings

Paging Server

Action Plan Add

Action:

Default

Number:

Direction:

Both

MCAST Codec:

PCMU

URL1:

Username:

URL:

Type:

Early

Line:

AUTO

Password:

UserAgent:

Add

Action Plan Option

Delete

Modify

User-defined Action Plan Table

Index	Action	Number	Type	Direction	Line	URL Index	Username	URL	UserAgent
-------	--------	--------	------	-----------	------	-----------	----------	-----	-----------

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

Line >> Action Plan (continued)

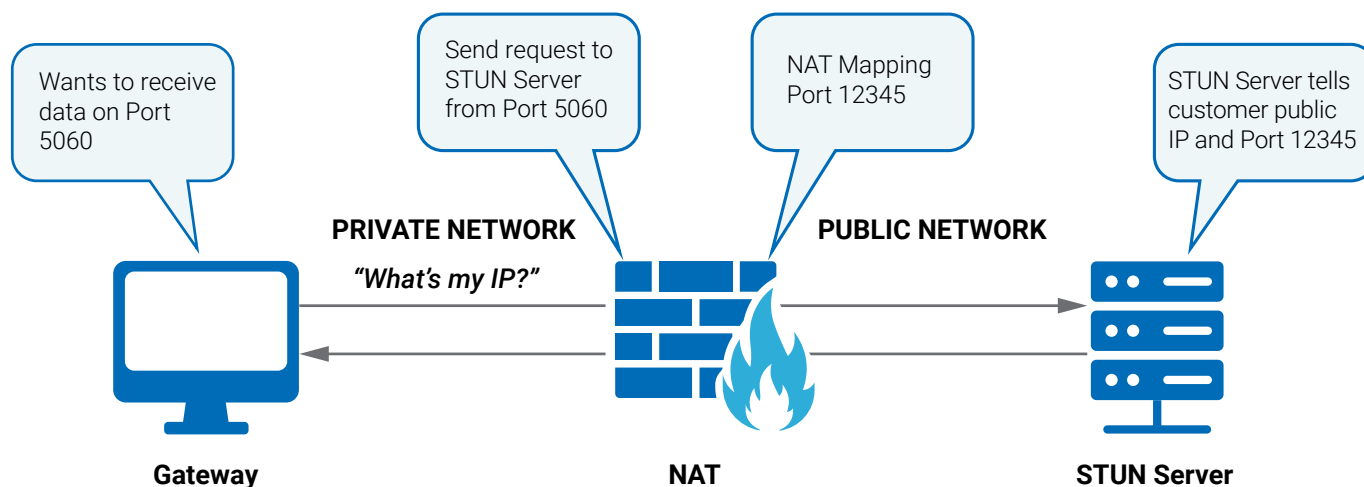
### Action Plan

PARAMETER	DESCRIPTION
Number	Auxiliary phone number (support video)
Type	Support video display on call.
Direction	For call mode, incoming/outgoing call displays video
Line	Set up outgoing lines.
Username	Bind the user name of the IP camera.
Password	Bind IP camera password.
URL	Video streaming information.
User Agent	Set user agent information
MCAST Codec	Set mcast codec
Action	Select action

### Line >> Basic Settings

STUN - Simple Traversal of UDP through NAT - A STUN server allows a phone in a private network to know its public IP and port as well as the type of NAT being used. The equipment can then use this information to register itself to a SIP server so that it can make and receive calls while in a private network.

### Basic Settings





## WEB CONFIGURATIONS

Line >> Basic Settings (continued)

### Line Basic Setting

The screenshot shows the AtlasIED web configuration interface. The left sidebar contains a menu with options: System, Network, Line (selected), Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area is titled 'Basic Settings' and contains two sections: STUN Settings and SIP P2P Settings. The STUN Settings section includes fields for STUN NAT Traversal (set to FALSE), Server Address, Server Port (set to 3478), Binding Period (set to 50 seconds), and SIP Waiting Time (set to 800 milliseconds). The SIP P2P Settings section includes checkboxes for Enable Auto Answering (checked), Auto Answering Delay (set to 0 seconds), DTMF Type (set to RFC2833), DTMF SIP INFO Mode (set to Send 10/11), Use VPN (checked), Call-ID Format (set to Sid@Sip), Display name, User Name, Block RTP When Alerting (unchecked), and Request-Line Format (set to Normal). An 'Apply' button is located at the bottom of each section.

### Line Basic Setting

PARAMETERS	DESCRIPTION
<b>STUN SETTINGS</b>	
Server Address	Set the STUN server address
Server Port	Set the STUN server port, default is 3478
Binding Period	Set the STUN binding period which can be used to keep the NAT pinhole opened.
SIP Waiting Time	Set the timeout of STUN binding before sending SIP messages
<b>SIP P2P SETTINGS</b>	
Enable Auto Answering	Automatically answer incoming IP calls after the timeout period is enabled
Auto Answering Delay	Automatic answer timeout setting
DTMF Type	Set the DTMF type of the line.
DTMF SIP INFO Mode	Set SIP INFO mode to send '*' and '#' or '10' and '11'



## WEB CONFIGURATIONS

### Line >> PTCR-XR

The RTCP-XR mode is based on THE RTP Control Extended Report (RFC3611). It sends RTCP-XR packets to evaluate network packet loss, delay, and voice quality.

### RTCP-XR

The screenshot shows the web configuration interface for the IP Video Doorbell. The left sidebar contains a menu with options: System, Network, Line (selected), Intercom Settings, Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area is titled 'STUN Settings' and 'SIP P2P Settings'. The 'STUN Settings' section includes fields for STUN NAT Traversal (set to FALSE), Server Address, Server Port (3478), Binding Period (50 seconds), and SIP Waiting Time (800 milliseconds). The 'SIP P2P Settings' section includes fields for Enable Auto Answering (checked), Auto Answering Delay (0 seconds), DTMF Type (RFC2833), DTMF SIP INFO Mode (Send 10/11), Use VPN (checked), Call-ID Format (Sid@Sip), Display name, User Name, Block RTP When Alerting (unchecked), and Request-Line Format (Normal). Both sections have an 'Apply' button.

### Set RTCP-XR

PARAMETERS	DESCRIPTION
<b>VQ RTCP-XR SETTINGS</b>	
VQ RTCP-XR Session Report	Whether to enable sending VQ reports in session mode
VQ RTCP-XR Interval Report	Whether to enable sending VQ reports in Interval mode
Period for Interval Report (5~99)	The interval at which VQ reports are periodically sent
Warning threshold for Moslq(15~40)	When the Moslq value x10 is lower than the threshold, a warning message is generated
Critical threshold for Moslq(15~40)	When the CALCULATED Moslq value x10 is lower than the threshold, a critical report is generated
Warning Threshold for Delay (10~2000)	When the One-way delay is greater than the threshold, the IP phone generates a warning report
Critical Threshold for Delay (10~2000)	When the One-way delay is greater than the threshold, the IP phone generates a critical report
Display Report Options on web	Whether to display the VQ report data for the last call through a web page



## WEB CONFIGURATIONS

### Intercom Settings >> Features

#### Features

**Basic Settings >>**

Enable Call Waiting:	<input checked="" type="checkbox"/>	Auto HangUp Delay:	<input type="text" value="3"/> (0~30)second(s)
Enable Auto On Hook:	<input checked="" type="checkbox"/>	Disable Mute for Ring:	<input type="checkbox"/>
Auto HangUp Tone:	<input checked="" type="checkbox"/>		
Enable Silent Mode:	<input type="checkbox"/>		
Ban Outgoing:	<input type="checkbox"/>	Default Dial Mode:	<input type="text" value="Video"/>
Default Ans Mode:	<input type="text" value="Video"/>		
Enable Restricted Incoming List:	<input checked="" type="checkbox"/>	Enable Country Code:	<input type="checkbox"/>
Enable Restricted Outgoing List:	<input checked="" type="checkbox"/>	Area Code:	<input type="text"/>
Country Code:	<input type="text"/>		
Allow IP Call:	<input checked="" type="checkbox"/>	P2P IP Prefix:	<input type="text" value="."/>
Restrict Active URI Source IP:	<input type="text"/>	Push XML Server:	<input type="text"/>
Line Display Format:	<input type="text" value="xxx@SIPn"/>	Auto Resume Current:	<input checked="" type="checkbox"/>
Call Number Filter:	<input type="text"/>	Talking Duration:	<input type="text" value="120"/> (20~86400)second(s)
Limit Talking Duration:	<input checked="" type="checkbox"/>	Enable Http Api Auth:	<input checked="" type="checkbox"/>
Call Timeout:	<input type="text" value="120"/> (1~3600)second(s)	Http Api PassWord:	<input type="text" value="admin"/>
Http Api UserName:	<input type="text" value="admin"/>	Description:	<input type="text" value="IP Video Doorphone"/>
Ring Timeout:	<input type="text" value="120"/> (1~3600)second(s)		

#### Feature Parameters

PARAMETERS	DESCRIPTION
<b>BASIC SETTINGS</b>	
Enable Call Waiting	Enable this setting to allow user to take second incoming call during an established call. Default enabled.
Enable Auto Handdown	The phone will hang up and return to the idle automatically at hands-free mode
Auto Handdown Time	Specify Auto handdown time, the phone will hang up and return to the idle automatically after Auto Hand down time at hands-free mode, and play dial tone Auto handdown time at handset mode
Enable Silent Mode	When enabled, the phone is muted, there is no ringing when calls, you can use the volume keys and mute key to unmute.
Disable Mute for Ring	When it is enabled,you can not mute the phone.
Ban Outgoing	If you select Ban Outgoing to enable it, and you cannot dial out any number.
Default Reply Mode	Select the default mode after an incoming call, including Video and Audio
Default Dial Mode	Select the default mode after an dialling, including Video and Audio
Enable Restricted Incoming List	Whether enable Restricted Incoming List
Enable Restricted Outgoing List	Wether enable Restricted Outgoing List
Enable country Code	Wether enable country Code

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

### Intercom Settings >> Features (continued)

Country Code	Country Code
Area Code	Area Code
Allow IP Call	If enabled, user can dial out with IP address
P2P IP Prefix	You can set IP call prefix, for example, i set it as "172.16.2.", then i input #160 in dialpad and press dial key, it will call 172.16.2.160 automatically
Restrict Active URI Source IP	Set the device to accept Active URI command from specific IP address.
Push XML Server	Configure the Push XML Server, when phone receives request, it will determine whether to display corresponding content on the phone which sent by the specified server or not.
Line Display Format	Line display format including SIPn/SIPn : xxx/xxx@SIPn
Call Number Filter	Configure a special character & ,if the number is 78 & 9. The call will be filtered out&
Auto Resume Current	If the current path changes, the hold will be automatically resume
Limit Talking Duration	Automatically hang up the call after enabling the time set for the call
Talking Duration	Call duration, 20-600s
No Answer Auto Hang Up Timeout	If the call is not answered, the call will be automatically hung up after the timeout
Enable Push XML Auth	To enable push xml auth, user password is required
Ringing timeout	If the call is not answered, automatic hang-up after timeout
Show description information	Show description information on the IP scan tool software. Default is "IP Video Doorphone"
<b>TONE SETTINGS</b>	
Enable Holding Tone	When turned on, a tone plays when the call is held
Enable Call Waiting Tone	When turned on, a tone plays when call waiting
Play Dialing DTMF Tone	Play DTMF tone on the device when user pressed a phone digit at dialing, default enabled.
Play Talking DTMF Tone	Play DTMF tone on the device when user pressed a phone digits during taking, default enabled.
Auto-answer beep	When switched on, a beep will be heard when the auto-answer is activated.
Tone of open door successfully	<p><b>Closed:</b> No prompt tone is played after the door is opened successfully.</p> <p><b>Default:</b> Use the default prompt tone.</p> <p><b>Voice:</b> Built-in voice prompt by default, default is "open the door successfully".</p> <p>Supports custom door opening success prompt tone, which can be customized in system - upgrade - ringtone or after the door is opened and the ringtone file upgrades successfully.</p>
Tone of open door unsuccessfully	<p><b>Closed:</b> There is no prompt tone after the door fails to open.</p> <p><b>Default:</b> Use the default prompt tone.</p> <p><b>Voice:</b> built-in voice prompt by default, default is "failed to open the door".</p> <p>Supports custom door opening failure prompt tone, in the system - upgrade - ringtone, or after failing to open the door and the ringtone file upgrades unsuccessfully.</p>

(CONTINUED ON NEXT PAGE)





## WEB CONFIGURATIONS

### Intercom Settings >> Features (continued)

Door closing beep	<p><b>Close:</b> no beep after closing the door</p> <p><b>Default:</b> Use the default beep</p> <p><b>Voice:</b> default built-in voice prompt, default is "Close"</p> <p>Support custom door closing tone, in the system - upgrade - ringtones, after upgrading the ringtone file under the door closing available settings to use the custom</p>
Successful card addition beep	<p><b>Close:</b> No beep after successful card addition</p> <p><b>Default:</b> Use the default beep.</p> <p><b>Voice:</b> default built-in voice prompt, default is "Card added successfully"</p> <p>Support customizable beep for successful card addition, in the system - upgrade - ringtones, after upgrading the ringtones file available under successful card addition settings to use a custom</p>
Add card failure beep	<p><b>Close:</b> No beep after failed card addition</p> <p><b>Default:</b> Use the default beep</p> <p><b>Voice:</b> default built-in voice prompt, default is "card refill failed"</p> <p>Support customizable sound for card failure, in the system - upgrade - ringtones, after upgrading the ringtones file under the card failure can be set to use a custom</p>
Successful beep for card deletion	<p><b>Close:</b> No beep after successful card deletion</p> <p><b>Default:</b> Use the default beep</p> <p><b>Voice:</b> default built-in voice prompt, default is "card deletion successful"</p> <p>Support for customising the successful card deletion tone, in System - Upgrade - Ringtone, after upgrading the ringtone file under the successful card deletion you can set to use a customised</p>
Card deletion failure beep	<p><b>Close:</b> No beep after failed card deletion</p> <p><b>Default:</b> Use the default beep</p> <p><b>Voice:</b> default built-in voice prompt, default is "card deletion failed"</p> <p>Support for customising the card deletion failure tone, in System - Upgrade - Ringtone, after upgrading the ringtone file under the card deletion failure can be set to use a customised</p>
Magnetic door detection beep	<p><b>Closed:</b> No beep after door magnetic detection anomaly</p> <p><b>Default:</b> Use the default beep</p> <p><b>Voice:</b> default built-in voice prompt, default is "Please close the door"</p> <p>Customised door detection tones are available under System - Upgrade - Ringtones, after upgrading the ringtone file the door detection can be set to use a customised</p>
<b>INTERCOM SETTINGS</b>	
Enable Intercom	When intercom is enabled, the device will accept the incoming call request with a SIP header of Alert-Info instruction to automatically answer the call after specific delay.
Enable Intercom Mute	Enable mute mode during the intercom call
Enable Intercom Tone	If the incoming call is intercom call, the phone plays the intercom
Enable Intercom Barge	Enable Intercom Barge by selecting it, the phone auto answers the intercom call during a call. If the current call is intercom call, the phone will reject the second intercom call
<b>RESPONSE CODE SETTINGS</b>	
Busy Response Code	Set the SIP response code on line busy
Reject Response Code	Set the SIP response code on call rejection





## WEB CONFIGURATIONS

### Intercom Settings >> Media

#### Media Settings

The screenshot shows the 'Media Settings' page in the AtlasIED web interface. The left sidebar contains a navigation menu with options: System, Network, Line, Intercom Settings (selected), Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area has tabs for Features, Media Settings (selected), Camera Settings, MCAST, Action, Time/Date, and Time Plan. Under 'Media Settings >>', there are various configuration fields: Default Ring Type (2.wav), Call Volume (7), Media Volume (3), Speakerphone SignalTone Volume (3), MCAST Handfree Volume (5), DTMF Payload Type (101), Handfree Mic Gain (3), OPUS Payload Type (107), ILBC Payload Type (97), Enable VAD (unchecked), Disable AEC (unchecked), H.264 Payload Type (117), Video Direction (sendonly), Audio Delay (0), Noise Reduction Level (Mid), OPUS Sample Rate (OPUS-NB), and ILBC Payload Length (20millisecor). Below these are sections for RTP Control Protocol(RTCP) Settings, RTP Settings, and Alert Info Ring Settings.

#### Media Settings

PARAMETERS	DESCRIPTION
<b>Codecs Settings</b>	Select the enabled and disabled voice codecs codec: G.711A/U, G.722, G.729, ILBC, opus, G.726, G.723.1
<b>MEDIA SETTING</b>	
<b>Default Ring Type</b>	Set the default ring type. If the caller ID of an incoming call was not configured with specific ring type, the default ring will be used.
<b>Speakerphone Volume</b>	Set the speakerphone volume, the value must be 1~9
<b>Speakerphone Ring Volume</b>	Set the ring volume in the speakerphone, the value must be 1~9
<b>Speakerphone Ring Volume</b>	Set the ring volume in the speakerphone, the value must be 1~9
<b>DTMF Payload Type</b>	Enter the DTMF payload type, the value must be 96~127.
<b>Opus payload type</b>	Enter the opus payload type, the value must be 96~127.
<b>OPUS Sample Rate</b>	Set the opus sample rate, including OPUS-NB (8KHz), OPUS-WB (16KHz)
<b>ILBC Payload Type</b>	Set the ILBC Payload Type
<b>ILBC Payload Length</b>	Set the ILBC Payload Length

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

### Intercom Settings >> Media (continued)

Enable VAD	Enable Voice Activity Detection. When enabled, the device will suppress the audio transmission with artificial comfort noise signal to save the bandwidth.
H.264Payload Type	Set the H264 Payload Type, the value must be 96~127.
<b>RTP CONTROL PROTOCOL(RTCP) SETTINGS</b>	
CNAME user	Set CNAME user
CNAME host	Set CNAME host
<b>RTP SETTINGS</b>	
RTP keep alive	Hold the call and send the packet after 30s
<b>ALERT INFO RING SETTINGS</b>	
Value	Set the value to specify the ring type.
Ring Type	Type1-Type9

### Intercom Settings >> Camera Settings

Customers can configure camera related parameters and adjust video coding related settings.

#### Camera Settings

**AtlasIED**

Features Media Settings **Camera Settings** MCAST Action Time/Date Time Plan

System  
Network  
Line  
**Intercom Settings**  
Call List  
Function Key  
Security  
Device Log  
Security Settings  
EGS Setting  
Platform Access

**Connection Mode Setting**

Native Camera: Local Came Apply

**Camera Settings**

White Balance Mode: Auto Mode Exposure Mode: Auto Mode  
Exposure Time: 0 (0~10000) Exposure Gain: 0 (0~1024)  
Contrast Mode: Auto Mode Contrast: 17 (0~100)  
Saturation Mode: Auto Mode Saturation: 96 (0~200)  
Sharpness Mode: Auto Mode Sharpness: 6 (0~1023)  
Wide Dynamic: Disabled WDR: 0 (0~10)  
Enable IRCUT: Synchronization  
Image Mode: Auto Brightness: 104 (0~100)  
Enable Onvif: Enable Call Stream: Main Stream  
Enable Onvif Auth: Enable Enable Rtsp Auth: Enable  
H.264 Payload Type: 117 (96~127) Enable Http Preview: Enable  
Fill Light: Auto Mode  
Default Apply

**Osd Settings**

Osd Time: Disabled Osd Text: Disabled  
Apply



## WEB CONFIGURATIONS

Intercom Settings >> Camera Settings (continued)

PARAMETERS	DESCRIPTION
<b>CONNECTION MODE SETTING</b>	
<b>Native Camera</b>	Local: Automatically use the local camera to transmit images External: After setting the external camera, it will automatically use the external camera to transmit images
<b>CAMERA SETTINGS</b>	
<b>White Balance Mode</b>	<p><b>Auto mode:</b> The camera automatically makes the most appropriate adjustments according to the color temperature of the shooting scene, and automatically compensates for the color of the light source.</p> <p><b>Lock mode:</b> Fixed white balance parameters will not be automatically adjusted according to the actual color temperature.</p> <p><b>Incandescent lamp mode:</b> To compensate for the hue of incandescent lamps, it is suitable for use under beige light sources (bulbs, tungsten lamps, candles) and other light sources of this type.</p> <p><b>Warm light mode:</b> Compensate the hue of warm light, suitable for light sources with a color temperature of about 2700K. Natural light mode: It can be used for white balance in outdoor shooting and has a wide range of applications.</p> <p><b>Fluorescent lamp light:</b> Compensate the hue of fluorescent lamps, suitable for use under fluorescent light sources (fluorescent lamps, energy-saving lamps) and other types of light sources.</p>
<b>Exposure Mode</b>	<p><b>Auto mode:</b> The camera automatically sets the parameters, no need for the operator to adjust.</p> <p><b>Manual exposure time:</b> Set the exposure time by yourself, the range is 0~10000</p> <p><b>Manual exposure gain:</b> Set the exposure gain by yourself, the range is 0~1024</p> <p><b>All manual:</b> Manually set the exposure time and gain.</p>
<b>Exposure Time</b>	It refers to the time to press the shutter. Increasing the exposure time can increase the signal-to-noise ratio and make the image clear. The longer the time, the more the sum of photons to the CCD\CMOS surface, the brighter the captured image will be, but if it is overexposed, the photo will be too bright and lose the image details; if it is underexposed, the photo will be too dark.
<b>Exposure Gain</b>	It refers to the amplification gain of the analog signal after double sampling, but the noise signal is also amplified in the process of amplifying the image signal. The gain is generally only used when the signal is weak, but you do not want to increase the exposure time.
<b>Contrast Mode</b>	<p><b>Auto mode:</b> The camera automatically sets the contrast according to the environment, no need for the operator to adjust</p> <p><b>Manual mode:</b> Manually set the camera's contrast parameters.</p>
<b>Contrast</b>	Contrast refers to the contrast between light and dark in the picture. Increase the contrast, the brighter areas will be brighter and the darker areas will be darker, and the contrast between light and dark will increase.
<b>Saturation Mode</b>	<p><b>Auto mode:</b> The camera automatically sets the saturation according to the environment, without the need for the operator to adjust</p> <p><b>Manual mode:</b> Manually set the camera's saturation parameters.</p>
<b>Saturation</b>	Saturation refers to the color. Adjusting the saturation will change the color. The greater the adjustment, the more distorted the image color. Adjusting the saturation is only suitable for pictures with insufficient colors. When the saturation is adjusted to the lowest, the image will lose its color and become a black and white image.
<b>Sharpness Mode</b>	<p><b>Auto mode:</b> The camera automatically sets the sharpness according to the environment, no need for the operator to adjust</p> <p><b>Manual mode:</b> Manually set the sharpness parameters of the camera</p>

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

### Intercom Settings >> Camera Settings (continued)

Sharpness	Sharpness is sometimes called "sharpness", which is an indicator that reflects the sharpness of the image plane and the sharpness of the edges of the image. If you increase the sharpness, the contrast of the details on the image plane is also higher and it looks clearer.
Wide dynamic	Enable or disable wide dynamic. Turning on wide dynamic allows the camera to see the image in a very strong contrast
Wide dynamic range	Set image brightness by yourself, range 0~10
Turn on IRCUT	Whether to open IRCUT
Image mode	<b>Daytime (color):</b> The camera transmits color images when there is sufficient light during the day <b>Night (black and white):</b> The camera transmits black and white images when there is insufficient light at night <b>Automatic:</b> The camera transmits color images when the light is sufficient during the day according to the light sensitivity, and transmits black and white images when the light is insufficient at night
Brightness	Set the image brightness by yourself, the range is 0~100
Enable Onvif	Enable or disable the onvif protocol, after enabling it, the device can be discovered through a recorder that supports ONVIF
Call Stream	Main stream or sub stream used in video call
Enable Onvif Auth	Is authentication required when using onvif protocol (with username and password)
Enable Rtsp Auth	When using rtsp protocol, whether authentication is required (with username and password)
H.264 Payload Type	Set the load type of h.264, the range is 96~127
<b>OSD SETTINGS</b>	
Osd Time	Turn on/off the date display of the camera image interface.
Osd Text	Enable/disable the text display of the camera image interface.
<b>VIDEO CODECS</b>	
H264 Video Stream	Support H.264 encoding format
Bitrate Control	<b>VBR:</b> Video call will adapt to the bit rate of the opposite end, so that the video effect is better. <b>CBR:</b> The video call will not change according to the bit rate set by itself.
Resolution	Support 1080P, 720P, 4CIF, VGA, CIF, QVGA
Frame Rate (fps)	The larger the value is, the more fluent the video is, and the higher the requirement for network bandwidth is; adjustment is not recommended
BitRate	It refers to the data flow used by video files in unit time, also known as code rate or code flow rate. Generally speaking, sampling rate is the most important part of picture quality control in video coding. Generally, the unit we use is KB / s or MB / s
I Frame Interval	The larger the value, the worse the video quality, otherwise the better the video quality; adjustment is not recommended.
<b>RTSP INFORMATION</b>	
Main Stream Url	Display the main stream URL address
Sub Stream Url	Display the sub stream URL address

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

Intercom Settings >> Camera Settings (continued)

SNAPSHOT	
Input trigger	Select the input port that triggers the capture
Call trigger	Select the call status that triggers the capture
Movement detection trigger	Whether to enable monitoring capture
Saving Method of Capture	Set how to save the captured image, including: server, Storage Card, Server and Storage Card
Server Address	Enter the server address
Username	Enter a username
Password	Enter a password

### SnapShot

SnapShot Trigger Mode:

Snapshot By Relay: ☐ Relay1 ☐ Relay2

Snapshot By Input: ☐ Input1 ☐ Input2 ☐ Input3

Snapshot By State: ☐ Talking ☐ Ringing ☐ Calling

Snapshot By Motion Detection: ☐

Snapshot Save: Server

Server Url:

Username:  Password:

[Right Click here to Save Camera Photo](#)

- Capture trigger mode:** Input trigger, call status trigger, movement detection trigger
- Input trigger:** Select the input port to trigger the snapshot
- Call status trigger:** The snapshot is triggered when an incoming call, call, or call occurs
- Movement detection trigger:** A capture is triggered when the camera detects abnormal action
- Snapshot save:** Save the screenshot to the server or SD card. Support 128G
- Server url:** Server address (Upload through FTP, TFTP, HTTP, or HTTPS) :ftp://IP:port@user:password/



## WEB CONFIGURATIONS

### Intercom Setting >> MCAST

It is easy and convenient to use multicast function to send notice to each member of the multicast via setting the multicast key on the device and sending multicast RTP stream to pre-configured multicast address. By configuring monitoring multicast address on the device, monitor and play the RTP stream which sent by the multicast address.

### Intercom Setting >> Action URL

#### Action URL

#### ACTION URL EVENT SETTINGS

URL for various actions performed by the phone. These actions are recorded and sent as xml files to the server. Sample format is <http://InternalServer/FileName.xml>

#### Action URL

The screenshot shows the Atlas IED web configuration interface. The top navigation bar includes tabs for Features, Media Settings, Camera Settings, MCAST, Action, Time/Date, and Time Plan. The left sidebar contains a menu with categories like System, Network, Line, Intercom Settings (selected), Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area is titled 'Action URL Event Settings' and contains a list of events with corresponding input fields for their respective Action URLs. The 'Action URL Report Type' is set to 'URL'.

Action URL Report Type:	URL
Setup Completed:	
Registration Succeeded:	
Registration Disabled:	
Registration Failed:	
Incoming Calls:	
Outgoing Calls:	
Call Established:	
Call Terminated:	
Phone Silent:	
Phone Unsilent:	
Call Mute:	
Call Unmute:	
Missed Calls:	
IP Changed:	
Phone State Idle:	
Phone State Talking:	
Phone State Ringing:	
Start Reboot:	
Web API Auth Changed:	
Echo Test:	
Input1:	
Reset Input1:	
Input2:	
Reset Input2:	
Input3:	
Reset Input3:	
Output1:	



## WEB CONFIGURATIONS

### Intercom Setting >> Time/Date

Users can configure the device's time Settings on this page.

#### Time/Date

The screenshot shows the AtlasIED web configuration interface. The left sidebar contains a menu with options: System, Network, Line, Intercom Settings (selected), Call List, Function Key, Security, Device Log, Security Settings, EGS Setting, and Platform Access. The main content area is titled 'Time/Date' and contains three sections: Network Time Server Settings, Time/Date Format, and Daylight Saving Time Settings. The Network Time Server Settings section includes checkboxes for 'Time Synchronized via SNTP' (checked), 'Time Synchronized via DHCP', and 'Time Synchronized via DHCPv6'. It also has input fields for 'Primary Time Server' (0.pool.ntp.org), 'Secondary Time Server' (time.nist.gov), a dropdown for 'Time zone' (UTC+8 Beijing, Singapore, Perth, Irkutsk), and a 'Resync Period' field (60 seconds). The Time/Date Format section includes a checkbox for '12-hour clock' and a 'Time/Date Format' dropdown (DD MMM WW) showing '16 OCT THU'. The Daylight Saving Time Settings section includes dropdowns for 'Location' (None) and 'DST Set Type' (Disabled), with an 'Apply' button. At the bottom, there is a 'Manual Time Settings' section with input fields for date (2025-10-16), hour (2), and minute (39), and an 'Apply' button.

#### Time/Date

Time/Date	
FIELD NAME	EXPLANATION
<b>NETWORK TIME SERVER SETTINGS</b>	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP protocol
Primary Time Server	Set primary time server address
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization.
Time zone	Select the time zone
Resync Period	Time of re-synchronization with time server
<b>DAYLIGHT SAVING TIME SETTINGS</b>	
Location	Select the user's time zone specific area

(CONTINUED ON NEXT PAGE)





## WEB CONFIGURATIONS

### Intercom Setting >> Time/Date (continued)

DST Set Type	Select automatic DST according to the preset rules of DST, or the manually input rules
Offset	The DST offset time
Month Start	The DST start month
Week Start	The DST start week
Weekday Start	The DST start weekday
Hour Start	The DST start hour
Month End	The DST end month
Week End	The DST end week
Weekday End	The DST end weekday
Hour End	The DST end hour
<b>MANUAL TIME SETTINGS</b>	
To set the time manually, you need to disable the SNTP service first, and you need to fill in and submit each item of year, month, day, hour and minute in the figure above to make the manual settings successful.	
System time: Display system time and its source (SIP automatic get >SNTP automatic get >manual manual setting)	





### WEB CONFIGURATIONS

#### Intercom Settings >>Time plan

The user can set the time point and time period for the device to perform a certain action.

#### Time Plan

Atlas IED

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

Platform Access

FeaturesMedia SettingsCamera SettingsMCASTActionTime/DateTime Plan

Time Plan Settings:

Enable Time Plan List:☒

Enable Time Plan Pause:☒

Apply

Time Plan:

Name:

Type:

Timed reboot

Repetition period:

Monthly

☐1

☐2

☐3

☐4

☐5

☐6

☐7

☐8

☐9

☐10

Monthly:

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

Start Date:

End Date:

Effective Time:

0

:

0

:

0

:

0

:

0

:

0

Add

Time Plan List:

☐Index

Name

Type

Special configure

Repetition period

Start Date

End Date

Effective Time

Delete

#### Time Plan

PARAMETERS	DESCRIPTION
Name	Enter a defined action name
Type	Timing restart, timing upgrade, timing sound detection, timing playback audio
Audio path	Support local <b>Local:</b> select the audio file uploaded locally
Audio settings	Select the audio file you want to play, it supports trial listening, and you can play it immediately after clicking the trial listening
Repeat cycle	<b>Do not repeat:</b> execute once within the set time range <b>Daily:</b> Perform this operation in the same time frame every day <b>Weekly:</b> Do this in the time frame of the day of the week <b>Monthly:</b> the time frame of the month to perform this operation
Effective time	Set the time period for execution

58

1601 JACK MCKAY BLVD.  
ENNIS, TEXAS 75119 U.S.A.

TELEPHONE: (800) 876-3333  
SUPPORT@ATLASIED.COM

AtlasIED.com



## WEB CONFIGURATIONS

### Intercom settings >> Tone

The user can configure the prompt tone of the device on this page. You can select the country area or customize the area. The selected area can directly appear the default information, and the customized one can modify the key tone, callback tone and other information.

#### Tone

The screenshot shows the 'Tone Settings' page in the AtlasIED web interface. The left sidebar contains a menu with options: System, Network, Line, Intercom Settings (selected), Call List, Function Key, Security, Device Log, Security Settings, and EGS Setting. The main content area has tabs for Features, Media Settings, Camera Settings, MCAST, Action, Time/Date, Time Plan, and Tone (selected). The 'Tone Settings' section includes a dropdown for 'Select Your Tone' (set to 'United States') and various tone configuration fields: Dial Tone (350+440/0), Ring Back Tone (440+480/2000,0/4000), Busy Tone (480+620/500,0/500), Congestion Tone, Call waiting Tone (440/300,0/10000,440/300,0/10000,0/0), Holding Tone, Error Tone, Stutter Tone, Information Tone, Dial Recall Tone (350+440/100,0/100,350+440/100,0/100,350+440/100,0/100,350+440/0), Message Tone, Howler Tone, Number Unobtainable Tone (400/500,0/6000), Warning Tone (1400/500,0/0), and Auto Answer Tone. An 'Apply' button is at the bottom right.

### Intercom settings >> LED

The user can configure the status and color of the indicator light on this page.

#### LED

The screenshot shows the 'LED' settings page in the AtlasIED web interface. The left sidebar is the same as the previous page. The main content area has tabs for Features, Media Settings, Camera Settings, MCAST, Action, Time/Date, Time Plan, Tone, and Led (selected). The 'LED' section includes a dropdown for 'status light' (set to 'LED1') and configuration options for Default Light (Priority goes from high to low), Network Abnormal, SIP Register Fail, Ring, In Using, SIP Register Success, and Default. Each option has a 'Status' dropdown and a 'Color' dropdown. An 'Apply' button is at the bottom right. Below the LED settings is an 'Advanced Settings' section with 'Save Power' (ON), 'Timeout To Power Saving' (60 seconds), and 'Enable Card LED' (ON). Another 'Apply' button is at the bottom right.



## WEB CONFIGURATIONS

### Intercom settings >> LED (continued)

**Status indicator:** The user can customize how the LED displays when the device is in different status.

**Energy-saving mode:** The device automatically turns off the LED when the device is not in use. The user can turn on or off the energy-saving mode.

**Energy-saving mode timeout:** The user can set the timeout of the energy-saving mode after inactivity. The default timeout is 60 seconds.

### Call list >> Call List

#### • Restricted Incoming Calls

It same as blacklist. By adding a number into the blacklist, user will no longer receive phone call from that number and it will be rejected automatically by the device until user delete it from the blacklist.

User can add specific number to be blocked, or a prefix where any numbers matched the prefix will all be blocked.

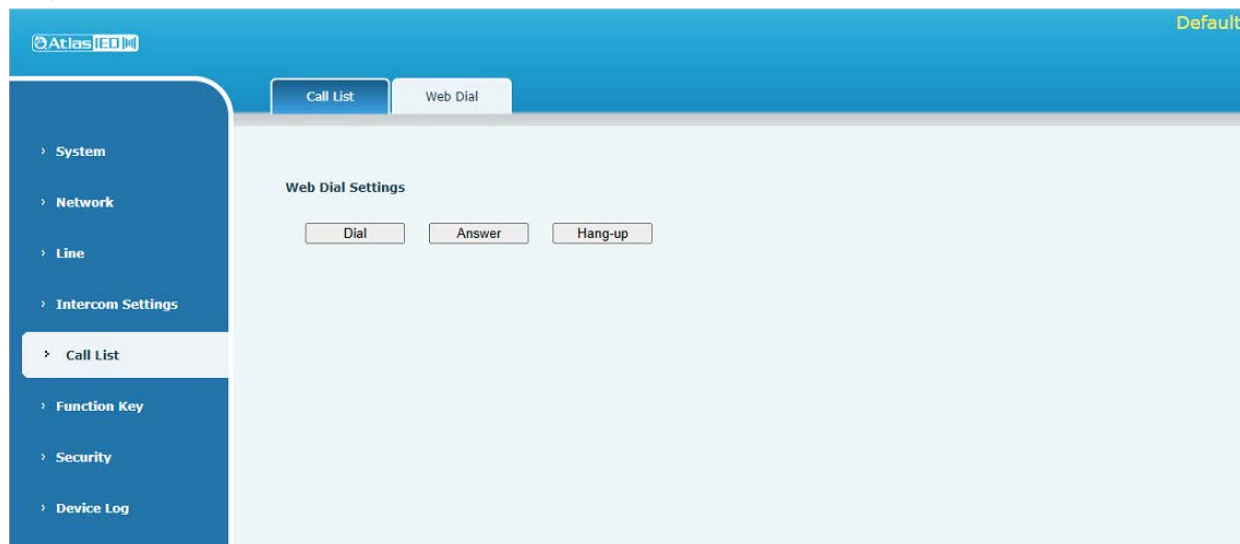
#### • Restrict Outgoing Call

You can set the rule to restrict some numbers from dialing out,until you remove the number from the table.

### Call list >> Web Dial

Use web page to call, answer and hang up.

#### Webpage Dial





## WEB CONFIGURATIONS

### Function key

#### Function Key Settings

Default

> System  
 > Network  
 > Line  
 > Intercom Settings  
 > Call List  
 > **Function Key**  
 > Security  
 > Device Log  
 > Security Settings  
 > EGS Setting

#### Function Key Settings >>

Key	Type	Name	Value			Subtype	Line	Media
DSS Key 1	Key Event			+	-	Handfree	AUTO	DEFAULT
DSS Key 2	Key Event			+	-	Lock	AUTO	DEFAULT
DSS Key 3	Key Event			+	-	Release	AUTO	DEFAULT
DSS Key 4	Memory Key	IP-CONSOLE-GH	192.168.1.51	+	-	Speed Dial	IP-CONSOLE-G	DEFAULT
DSS Key 5	Memory Key	IC Trigger	2315	+	-	Speed Dial	InformaCast@S	DEFAULT
DSS Key 6	None			+	-	None	AUTO	DEFAULT
DSS Key 7	None			+	-	None	AUTO	DEFAULT

#### Programmable Key Settings >>

#### Advanced Settings >>

#### Function Key Settings >>

##### Programmable Key Settings >>

Key	Desktop	Dialer	Ringing	Alerting	Talking	Desktop Long Pressed
Key1	Deskey1	Deskey1	Answer	End	End	Main Menu
Key2	Deskey2	Deskey2	Answer	End	End	
Key3	Deskey3	Deskey3	Answer	End	End	Invalid
Key4	Deskey4(IP-CONSC)	Deskey4(IP-CONSC)	Answer	End	End	Invalid
Key5	Deskey5(IC Trigger)	Deskey5(IC Trigger)	Answer	End	End	Invalid
Key6	Deskey6	Deskey6	Answer	End	End	Invalid
Key7	Deskey7	Deskey7	Answer	End	End	Invalid

Apply

#### Function Key Settings >>

##### Programmable Key Settings >>

##### Advanced Settings >>

Dial Mode Select Group Call  
 Call Switched Time 16 (5~50)second(s)  
 First Number Start Time 06:00 (00:00~23:59)
 First Number End Time 18:00 (00:00~23:59)

Apply



## WEB CONFIGURATIONS

### Function key (continued)

PARAMETERS	DESCRIPTION
<b>FUNCTION KEY SETTINGS</b>	
<b>Memory</b>	<b>Speed Dial:</b> The user can directly dial the set number. This feature is convenient for customers to dial frequent numbers. <b>Intercom:</b> This feature allows the operator or secretary to quickly connect to the phone, widely used in office environments
<b>Key event</b>	The user can select a function key as the shortcut to trigger an event <b>Handfree:</b> One-click to open the hands-free <b>Audio play:</b> play music stored locally <b>OK:</b> Confirm key <b>Volume Up:</b> Increase the volume <b>Volume Down:</b> Decrease the volume <b>Redial:</b> redial out the last number dialed <b>Release:</b> Hang up the call <b>Call Back:</b> dial back the last call Volume Circle
<b>DTMF</b>	Press during a call to send the set DTMF
<b>Mcast Paging</b>	Configure the multicast address and voice encoding. User can initiate multicast by pressing this key
<b>Action URL</b>	The user can use a specific URL to make basic calls to the device, open the door, etc.
<b>Mcast Listening</b>	In standby, press the function key, if the RTP of the multicast is detected, the device will monitor the multicast
<b>PTT</b>	<b>Speed Dial:</b> Make a call when pressed, and end the call when lifted. <b>Intercom:</b> Start the intercom when pressed, and end the intercom when lifted. <b>Multicast:</b> Initiate multicast when pressed, and end multicast when lifted
<b>PROGRAMMABLE KEY SETTINGS</b>	
<b>Desktop</b>	<b>None:</b> Nothing happens when you press the speed dial <b>Dsskey1:</b> When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. <b>Dsskey2:</b> When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2
<b>Dialer</b>	<b>None:</b> Nothing happens when you press the speed dial <b>Dsskey1:</b> When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. <b>Dsskey2:</b> When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2
<b>Ringing</b>	<b>Answer:</b> Set to answer, when there is an incoming call, if auto answer is disabled, press the speed dial key to answer the call <b>End:</b> set to end, when there is an incoming call, press the speed dial button to hang up the call
<b>Talking</b>	<b>End:</b> set to end, when there is a call, press the speed dial key to hang up the call <b>Volume up:</b> set as volume up button, when there is a call, press the speed dial button to increase the volume <b>Volume down:</b> set as volume up button, when there is a call, press the speed dial button to decrease the volume <b>Dsskey1:</b> When it is set to dsskey1, follow the settings of dsskey1 to make call, answer, etc. <b>Dsskey2:</b> When it is set to dsskey2, perform operations such as calling and answering according to the setting of dsskey2
<b>Desktop Long Pressed</b>	<b>None:</b> Long press the speed dial key does not respond <b>Main menu:</b> Long press the speed dial key to enter the command line mode

(CONTINUED ON NEXT PAGE)



## WEB CONFIGURATIONS

### Function key (continued)

ADVANCED SETTINGS	
Hot Key Dial Mode Select	Number 1 call number 2 mode selection. <Main/Secondary>: If the first number is not answered within the set time, the second number will be automatically switched. <Day/Night>: The system time is automatically detected during the call. If it is daytime, the first number is called, otherwise the second number is called.
Call Switched Time	Set number 1 to call number 2 time, default 16 seconds
Day Start Time	The start time of the day when the <Day/Night> mode is defined. Default "06:00"
Day End Time	The end time of the day when the <Day/Night> mode is defined. Default "18:00"

### Memory

Enter the phone number in the input box. When you press the function key, the device will call out the set phone number. This button can also be used to set the IP address, press the function key to make an IP direct call.

### Memory Key

Atlas IED

Default

System
Network
Line
Intercom Settings
Call List
Function Key
Security
Device Log
Security Settings

#### Function Key Settings >>

Key	Type	Name	Value	Subtype	Line	Media
DSS Key 1	Key Event			Handfree	AUTO	DEFAULT
DSS Key 2	Key Event			Lock	AUTO	DEFAULT
DSS Key 3	Key Event			Release	AUTO	DEFAULT
DSS Key 4	Memory Key	IP-CONSOLE-GH	192.168.1.51	Speed Dial	IP-CONSOLE-G	DEFAULT
DSS Key 5	Memory Key	IC Trigger	2315	Speed Dial	InformaCast@S	DEFAULT
DSS Key 6	None			None	AUTO	DEFAULT
DSS Key 7	None			None	AUTO	DEFAULT

Apply

#### Programmable Key Settings >>

#### Advanced Settings >>

### Memory Key

TYPE	NUMBER	LINE	SUBTYPE	USAGE
Memory	Fill in the SIP account or IP address of the called party	The line corresponding to the SIP account	Speed Dial	Using the speed dial mode, press the button to quickly dial the set number.
			Intercom	Using the intercom mode, when the SIP phone at the opposite end supports the intercom function, the call can be automatically answered.



## WEB CONFIGURATIONS

### Multicast

Multicast function is to deliver voice streams to configured multicast address; all equipment monitored the multicast address can receive and play the broadcasting. Using multicast functionality would make deliver voice one to multiple which are in the multicast group simply and conveniently.

The DSS Key multicast web configuration for calling party is as follow:

### Multicast

Atlas IED
Default

- System
- Network
- Line
- Intercom Settings
- Call List
- Function Key
- Security
- Device Log
- Security Settings

#### Function Key Settings >>

Key	Type	Name	Value	Subtype	Line	Media
DSS Key 1	Key Event		+ -	Handfree	AUTO	DEFAULT
DSS Key 2	Key Event		+ -	Lock	AUTO	DEFAULT
DSS Key 3	Key Event		+ -	Release	AUTO	DEFAULT
DSS Key 4	Memory Key	IP-CONSOLE-GH	192.168.1.51	Speed Dial	IP-CONSOLE-G	DEFAULT
DSS Key 5	Memory Key	IC Trigger	2315	Speed Dial	InformaCast@S	DEFAULT
DSS Key 6	None		+ -	None	AUTO	DEFAULT
DSS Key 7	None		+ -	None	AUTO	DEFAULT

Apply

Programmable Key Settings >>

Advanced Settings >>

### Web Multicast

TYPE	NUMBER	SUBTYPE
Multicast	Set the host IP address and port number, they must be separated by a colon (The IP address range is 224.0.0.0 to 239.255.255.255, and the port number is preferably set between 1024 and 65535)	G.711A
		G.711U
		G.729AB
		iLBC
		opus
		G.722





## WEB CONFIGURATIONS

### PTT

Keep pressing the shortcut key set to make a call, release it and hang up

### PITT

**Function Key Settings >>**

Key	Type	Name	Value	Value2	Subtype	Line	Media
DSS Key 1	PTT		632	182	Speed Dial	184@SIP1	DEFAULT
DSS Key 2	None				None	AUTO	DEFAULT
DSS Key 3	None				None	AUTO	DEFAULT
DSS Key 4	None				None	AUTO	DEFAULT
DSS Key 5	None				None	AUTO	DEFAULT
DSS Key 6	None				None	AUTO	DEFAULT
DSS Key 7	None				None	AUTO	DEFAULT
DSS Key 8	None				None	AUTO	DEFAULT

### Security >> Web Filter

Users can set up to allow only a certain network segment IP to access the device

### Web Filter

**Atlas IED**

Web Filter | Trust Certificates | Device Certificates | Firewall

System | Network | Line | Intercom Settings | Call List | Function Key | **Security** | Device Log | Security Settings

**Web Filter Table**

Start IP Address	End IP Address	Option

**Web Filter Table Settings**

Start IP Address  End IP Address

**Web Filter Setting**

Enable Web Filter ☐

**Web Filter Table**

Start IP Address	End IP Address	Option
192.168.1.1	192.168.254.254	<input type="button" value="Modify"/> <input type="button" value="Delete"/>



## WEB CONFIGURATIONS

### Security >> Web Filter (continued)

Add and delete the allowed IP network segments; configure the start IP address in the start IP, configure the end IP address in the end IP, and then click [Add] to add successfully. You can set a large network segment or add it into several network segments. When deleting, select the starting IP of the network segment to be deleted in the list, and then click [Delete] to take effect.

Enable web filtering: configure to enable/disable web access filtering; click the [Submit] button to take effect

**Note:** If the device you access to the device is on the same network segment as the device, do not configure the web filtering network segment to be outside your own network segment, otherwise you will not be able to log in to the web page.

### Security >> Trust Certificates

You can upload and delete uploaded trust certificates.

#### Trust Certificate

Atlas IED

Default

Web Filter

Trust Certificates

Device Certificates

Firewall

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

Platform Access

Permission Certificate

Permission Certificate

Disabled

Common Name Validation

Disabled

Certificate Mode

All Certificates

Apply

Import Certificates

Load Server File

Select

Upload

Certificates List

Index	File Name	Issued To	Issued By	Expiration	File Size
					<div>Delete</div>





## WEB CONFIGURATIONS

### Security >> Device Certificates

Select the default certificate or the custom certificate as the device certificate. You can upload and delete uploaded certificates.

#### Device Certificate

Atlas IED

Default

Web Filter

Trust Certificates

Device Certificates

Firewall

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

Device Certificates

Device Certificates

Default Certificates

(existence)

Apply

Import Certificates

Load Server File

Select

Upload

Certification File

File Name	Issued To	Issued By	Expiration	File Size
				<div>Delete</div>

### Security >> Firewall

#### Firewall

Atlas IED

Default

Web Filter

Trust Certificates

Device Certificates

Firewall

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

Firewall Type

Enable Input Rules:

Enable Output Rules:

Apply

Firewall Input Rule Table

Index/Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range

Firewall Output Rule Table

Index/Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range

Firewall Settings

Input/Output

Input

Src Address

Dst Address

Deny/Permit

Deny

Src Mask

Dst Mask

Protocol

UDP

Src Port Range

Dst Port Range

Add

Rule Delete Option

Input/Output

Input

Index To Be Deleted

Delete



## WEB CONFIGURATIONS

### Security >> Firewall (continued)

Through this page, you can set whether to enable the input and output firewalls, and at the same time, you can set the input and output rules of the firewall. Use these settings to prevent malicious network access, or restrict internal users from accessing some resources of the external network, and improve safety.

The firewall rule setting is a simple firewall module. This function supports two kinds of rules: input rules and output rules. Each rule will be assigned a serial number, and a maximum of 10 each rule can be set.

Taking into account the complexity of firewall settings, the following will illustrate with an example:

#### Web Firewall

PARAMETER	DESCRIPTION
Enable Input Rules	Whether enable Input Rules
Enable Output Rules	Whether enable Output Rules
Input/output	Select the current rule as an input or output rule
Deny/permit	Choose the current rule is deny or allowed;
Protocol	There are four types of protocols:TCP, UDP, ICMP, IP
Port Range	Port range
Src Address	The source address can be the host address, network address, or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0.
Dst Mask	The destination address can be a specific IP address or all addresses 0.0.0.0; it can also be a network address similar to *.*.*.0, such as 192.168.1.0.
Src Port Range	It is the source address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of type 255.255.255.0, it means that the filter is a network segment;
Dst Port Range	It is the destination address mask. When it is configured as 255.255.255.255, it means it is a specific host. When it is set as a subnet mask of 255.255.255.0 type, it means that a network segment is filtered;

After setting, click [Add], a new item will be added to the firewall output rules, as shown in the figure below:

#### Firewall rules list

Firewall Input Rule Table ?

Index	Deny/Permit	Protocol	Src Address	Src Mask	Src Port Range	Dst Address	Dst Mask	Dst Port Range
-------	-------------	----------	-------------	----------	----------------	-------------	----------	----------------

Then select and click the button [Submit].

In this way, when the device runs: ping 192.168.1.118, it will not be able to send data packets to 192.168.1.118 because of the prohibition of the output rule. But ping other IPs in the 192.168.1.0 network segment can still receive the response packets from the destination host normally.

#### Delete firewall rules

**Rule Delete Option ?**

Input/Output
Index To Be Deleted

Select the list you want to delete and click [Delete] to delete the selected list.



## WEB CONFIGURATIONS

### Device log

You can crawl the device log, when you encounter unusual problems, please send the device log to the technical staff for positioning problem.

### Security settings

Enable Tamper: after enable, when the device is removed by force, the alarm information will be sent to the server and the alarm ring will be played.

#### Security Settings

Atlas IED

Default

System
Network
Line
Intercom Settings
Call List
Function Key
Security
Device Log
Security Settings
EGS Setting
Platform Access

Basic Settings

Ringtone Duration:  (1~500)s  
Input & Tamper Server Address:   
Message:   

Apply

Input Settings >>

Output Settings >>

Motion Detection Settings >>

Tamper Alarm Settings >>

Tamper Alarm Reset

Reset Alarm Status 

Reset

Noise Alarm Settings >>

### Security Settings

PARAMETERS	DESCRIPTION
<b>BASIC SETTINGS</b>	
Ringtone Duration	Set the ringtone duration, default value is 2 seconds.
Input & Tamper Server Address	Set remote server address. The device will send message to the server when the alarm is triggered. The message format is: Alarm_Info:Description=i16SV;SIP User=;Mac=0c:38:3e:3a:06:65;IP=; port=Input .
Information	Fill in the information attached to the upload server
<b>INPUT SETTINGS</b>	
Input	Enable or disable Input
Triggered by	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger.



## WEB CONFIGURATIONS

Input Duration	Set the Input change duration time, the default is 5 seconds.
Triggered Action	<p><b>Send SMS:</b> Set the alert message send to server if selected.</p> <p><b>Event:</b> The device will perform corresponding Dss Key configurations if any key is selected, by default the value is none</p> <p><b>Triggered Ringtone:</b> Select triggered ring tone.</p>
Triggered Ringtone	Ringtone selection
<b>OUTPUT SETTINGS</b>	
Enable Logs	Enable or disable LOG
Triggered by DTMF Ringtone	Select the DTMF trigger ring tone.
Triggered by URI Ringtone	Select the URI trigger ring tone.
Triggered By SMS Ringtone	Select the SMS trigger ring tone.
Triggered By Dsskey Ringtone	Select the Dsskey trigger ring tone.
Output Response	Enable or disable Output Response
Standard Status	When choosing the low level trigger (NO: normally open), when meet the trigger condition, trigger the NO port disconnected.
	When choosing the high level trigger (NC: normally close), when meet the trigger condition, trigger the NC port close.
Output Duration	Set the output change duration time, the default is 5 seconds.
Input trigger	When the input port meets the trigger condition, the output port will trigger (the port level time changes, controlled by <output duration>).
Trigger by DTMF	Enable or disable trigger by DTMF. The device will check the received DTMF sent by remote device, if it matches the DTMF trigger code, the device will trigger corresponding output port.
DTMF Trigger Code	Input the DTMF trigger code, default value is 1234.
DTMF Reset Code	Input the DTMF reset code, default value is 4321.
Reset By	<p>Reset the output port mode by duration or state.</p> <p>By duration: Reset the output port status when output duration occurs.</p> <p>By state: Reset the output port status when device's call state changes.</p>
Trigger by URI	<p>Enable or disable trigger by URI.</p> <p>User can send commands from remote device or server to i16SV series device, if the command is correct, then device will trigger corresponding output port.</p>
Trigger Message	Input trigger message for trigger by URI mode.
Rest Message	Input reset message for trigger by URI mode.
Trigger by SMS	Enable or disable trigger by SMS. User can send ALERT command to i16SV series device, if the command is correct, then device will trigger corresponding output port.
Trigger SMS	Input trigger message for trigger by SMS mode.
Reset SMS	Input reset message for trigger by SMS mode.
Trigger by Input	Select the input port, when the input port meets the trigger condition, the output port will be triggered (The Port level time change, By < Output Duration > control)

(CONTINUED ON NEXT PAGE) 70



## WEB CONFIGURATIONS

Trigger By Call state	Select call state to trigger the output port, options are: Talking: When the device's talking status changes, trigger the output port. Ringing: When the device's ringing status changes, trigger the output port. Calling: When the device's calling status changes, trigger the output port.
Trigger By DssKey	Enable or disable trigger by dsskey. If any of the dsskey is selected, when the dsskey application performs, the output port will be triggered.
Triggered Hangup	Trigger the output port after hanging up
Hangup Delay	Hang up trigger delay, default 5 seconds
<b>MOTION DETECTION SETTINGS</b>	
Motion Detection Alarm	Enable or disable motion detection
Trigger Duration	Set the trigger delay time, the default is 3 seconds, the range: 0~3600 seconds
Trigger ringtone	Support ringtone selection
Trigger behavior: Send SMS	Enable or disable the input port to send messages to the server
Function key	When set to dsskey1 or dsskey2, trigger dsskey to make a call, the default is none
<b>TAMPER ALARM SETTINGS</b>	
Enable Tamper Alarm	Whether to enable tamper detection, if the terminal is violently dismantled, the tamper is triggered and always play the set alarm ringtone
Alarm command	When detected someone tampering the equipment, the alarm signal will be sent to the corresponding server
Reset command	When the equipment receives the command of reset from server, the equipment will stop alarm
Alarm Ringtone	Alarm ringtone setting
<b>DETACHABLE ALARM RESET</b>	
Reset alarm state	Reset the play of stop ringtone





## WEB CONFIGURATIONS

### EGS Setting >> Features

#### ESG Feature Settings

Atlas IED

Default

Feature Relay Personnel Management Time Profile Logs

System Network Line Intercom Settings Call List Function Key Security Security Settings EGS Setting Platform Access

**Basic Settings**

Relay1 Mode: Monostable

Relay2 Mode: Monostable

Relay2 Follow Mode: Independence

RFID Format: 8H10D

Wiegand Mode: Input

Wiegand Parity Check: Enable

Relay Open Mode: ☒ Card Reader ☒ Password

Keypad Input Mode: Password & Dial

Relay Log Export Enable: ☐

Relay Log Server Addr: 0.0.0.0

Relay Log Server Port: 514

☐ Authentication Method

Relay1 Open Duration: 5

Relay2 Open Duration: 5

Asynchronization Delay Time: 1

Wiegand Format: 8H10D

Wiegand Type: 34

Wiegand Password Output Type: Disable

Card Reader Working Mode: Normal

Keypad \* To Switch Input Mode: Disable

Relay Log Server Type: UDP

Relay Log Info: <8>doorIndex:

Include Snapshot: ☐

Disabled State: Card Reader Local Password

Enabled State:

Apply

You can set basic access control Settings on this screen

#### ESG Feature Parameters

FIELD NAME	EXPLANATION
<b>BASIC SETTINGS</b>	
<b>Relay1 Mode</b>	Monostable: there is only one fixed action status for door unlocking. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. Initial Value is Monostable
<b>Relay1 Duration</b>	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
<b>Relay2 Mode</b>	Monostable: there is only one fixed action status for door unlocking. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. Initial Value is Monostable
<b>Relay2 Duration</b>	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
<b>Relay2 Mode</b>	Monostable: there is only one fixed action status for door unlocking. Bistable: there are two actions and statuses, door unlocking and door locking. Each action might be triggered and changed to the other status. After changed, the status would be kept. Initial Value is Monostable





## WEB CONFIGURATIONS

### EGS Setting >> Features (continued)

Relay2 Duration	Door unlocking time for Monostable mode only. If the time is up, the door would be locked automatically. Initial Value is 5 seconds.
Relay2Follow mode	Independent: Open the door independently with Relay1 Synchronous: open the door at the same time as Relay1 Asynchronous: Relay1 opens after a period of time Relay2 opens
Asynchronous delay	The user can set the asynchronous door opening delay time of Relay1 and Relay2, the default is 1 second
RFID card format	Supported access control card format
Wiegand format	Supported Wiegand access card format
Wiegand mode	Optional input port or output port, default in
Wiegand Type	Support 26 and 34
Enable Card Reader	Enable or disable card reader for RFID cards.
Card Reader Working Mode	Set ID card stats: Normal: This is the work mode, after the slot card can to open the door. Card Issuing: This is the issuing mode, after the slot card can to add ID cards. Card Revoking: This is the revoking mode, after the slot card can to delete ID cards.

### EGS Setting >> Relay

#### Relay

Atlas IED

Default

Feature

Relay

Personnel Management

Time Profile

Logs

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

Platform Access

Relay Status

Door Sensor1

Door Sensor Check Delay1

5

Door Sensor2

Door Sensor Check Delay2

5

Relay Status1:

Close

Door Sensor Status1:

N/A

Relay Status2:

Close

Door Sensor Status2:

N/A

Apply

Relay Control

Relay

1

Action

Open

Mode

Once

Exec



## WEB CONFIGURATIONS

### EGS Setting >> Relay (continued)

#### Relay

FIELD NAME	EXPLANATION
<b>RELAY STATUS</b>	
Door Sensor1	Enable or disable door sensor 1
Door Sensor Check Delay 1	Door Sensor1 detection delay time setting,5 seconds by default
Door Sensor2	Enable or disable door status sensor 2
Door Sensor Check Delay 2	Door Sensor2 detection delay time setting,5 seconds by default
Lock Status 1	Door Close/Open
Door Sensor Status1	Door Close/Open
Lock Status 2	Door Close/Open
Door Sensor Status2	Door Close/Open
<b>DOOR LOCK CONTROL</b>	
Door Lock	Execute a door lock to open or close the door
Action	Door Open/Close
Open mode	Once: perform door opening action, and will be closed automatically when timeout. Continue: perform the door opening action, the door will not be closed automatically and need to closed manually when timeout.

### EGS Setting >> Card

#### Card

Atlas IED

Default

Feature

Relay

Personnel Management

Time Profile

Logs

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

Personnel Management > Add

Personnel information

Name

Card Number Type

Card Number

Password Type

Password

Number

Location

CallForward

Privilege

Relay

Mode

Times



## WEB CONFIGURATIONS

### EGS Setting >> Card (continued)

#### Card Rule

FIELD NAME	EXPLANATION
<b>IMPORT CARD LIST</b>	
Click the <Select> to choose to import remote card list file (cardlist.csv) and then clicking <Update> can batch import remote card rule.	
<b>ADD CARD RULE</b>	
<b>Type</b>	Standard, namely to open the door card. Add, swipe the added card administrator card in the standby mode, the device will enter the card add mode, and then swipe the card, the card that has not been added to the card list will be added. Delete, swipe the added card delete administrator card in standby, the device will enter the card delete mode, and then swipe the card, the added card will be deleted
<b>Relay</b>	Swipe to open the door lock
<b>Mode</b>	Closed, swiping is unsuccessful after disabling Enable, swipe the card to take effect after enabling Time zone, swiping the card in the set time zone takes effect
<b>Times</b>	The number of times the card can be swiped in a time period
<b>Name</b>	User name
<b>Card Number</b>	RFID card number. You can manually fill in the first 10 digits of the card number or select the existing card number
<b>Period</b>	The time to add the card, automatically generated
<b>CARD LIST</b>	
<b>Operation</b>	Delete, delete all Export, support to export to csv. file





## WEB CONFIGURATIONS

### EGS Setting >> Password

#### Password Rule

AtlasIED

Default

Feature Relay Personnel Management Time Profile Logs

Personnel Management > Add

Personnel information

Name

Card Number Type

Card Number

Password Type

Password

Number

Location

CallForward

Privilege

Relay ☒ Relay1 ☒ Relay2

Mode

Times

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

#### Time to add the card, automatically generated Rule

FIELD NAME	EXPLANATION
<b>IMPORT PASSWORD LIST</b>	
Click the <Select> to choose to import remote password list file (passwordlist.csv) and then clicking <Update> can batch import remote password rule.	
<b>ADD PASSWORD RULE</b>	
<b>Type</b>	Local, that is, the local door opening password, enter the password dial interface in standby and enter the set opening password to open the door immediately
	Remote, remote opening password, when the indoor unit calls the door or when the door calls the indoor unit to open the door, enter the DTMF password to open the door
	Remote and local, one password supports two door opening methods at the same time
<b>Relay</b>	A door lock with a code
<b>Mode</b>	Closed, unsuccessful password opening after disabling Enable, after enabling the password to open the door to take effect Time zone, the password to open the door takes effect during the set time zone
<b>Times</b>	The number of times the door can be opened with a password in a time period
<b>Name</b>	User name
<b>Password</b>	Password to open the door



## WEB CONFIGURATIONS

### EGS Setting >> Password (continued)

Number	When the indoor unit calls the access control or the access control calls the indoor unit to open the door, enter the DTMF password to open the door
Period	Time to add the card, automatically generated
<b>PASSWORD LIST</b>	
Operation	Delete, delete all. Export, support to export to csv. file

### EGS Setting >> Time Profile

#### Time Profile

#### Time Profile

FIELD NAME	EXPLANATION
<b>IMPORT TIME LIST</b>	
Click the <Select> to choose to import remote Profile list file (timeProfileList.csv) and then clicking <Update> can batch import remote Period.	
<b>PERIOD ADD</b>	
Name	Set the name of the time period
Repetition period	<b>No repetition:</b> Opening the door in the set time period is valid, and it is invalid at other times <b>Daily:</b> It is valid to open the door in the time period set daily, and it is invalid at other times <b>Weekly:</b> It is valid to open the door in the time period set every week, and it is invalid at other times <b>Monthly:</b> Open the door in the time period set every month is valid, and it is invalid at other times
Effective time	Set the effective time



## WEB CONFIGURATIONS

### EGS Setting >> Logs

#### Logs

Atlas IED

Default

Feature

Relay

Personnel Management

Time Profile

Logs

System

Network

Line

Intercom Settings

Call List

Function Key

Security

Device Log

Security Settings

EGS Setting

Relay Logs

Total: 47

Page : 1

Previous

Next

Delete All

Right Click here to Save Logs

Relay	Result	Name	Source	Type	Reason	Time
1	Success	Mitek Lab IP-CONSOLE-GH	S:192.168.1.51	Remote Password		2025/04/08 22:20:25
1	Success	Mitek Lab IP-CONSOLE-GH	S:192.168.1.51	Remote Password		2025/03/25 21:06:04
1	Success	Manny Kitagawa	P:1361	Local Password		2025/03/22 00:18:23
2	Success	Manny Kitagawa	P:1361	Local Password		2025/03/22 00:18:23
1	Success	Manny Kitagawa	C:2202729051	Card Reader		2025/03/22 00:18:07
2	Success	Manny Kitagawa	C:2202729051	Card Reader		2025/03/22 00:18:07
1	Success	Mitek Lab IP-CONSOLE-GH	S:192.168.1.130	Remote Password		2025/03/22 00:17:41
1	Success	Mitek Lab IP-CONSOLE-GH	S:192.168.1.130	Remote Password		2025/03/21 23:54:55
1	Success	Manny Kitagawa	C:2202729051	Card Reader		2025/03/21 22:14:52
2	Success	Manny Kitagawa	C:2202729051	Card Reader		2025/03/21 22:14:52

#### Logs

FIELD NAME	EXPLANATION
Relay	Relay
Result	Display the result of a single door opening (success or failure)
Name	The name of the person who opened the door
Source	Card number or password to open the door
Type	Door opening type, including password, credit card
Reason	Reasons for failed door opening
Time	Opening time



## TROUBLE SHOOTING

When the device is not working properly, users can try the following methods to restore the device to normal operation or collect relevant information to send a problem report to the technical support mailbox.

### Get device system information

Users can obtain information through the [System] >> [Information] option on the device webpage. The following information will be provided: Device information (model, software and hardware version) and Internet Information etc.

### Reboot device

User can restart the device through the webpage, click [System] >> [Reboot Phone] and click [Reboot] button, or directly unplug the power to restart the device.

### Device factory reset

Restoring the factory settings will delete all configurations, database and configuration files on the device and the device will be restored to factory default state. To restore the factory settings, please go to [System] >> [Configuration] >> [Reset Phone] page, and click [Reset] button, the device will return to the factory default state.

### Network Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the webpage of the device, open the webpage [System] >> [Tools], and click the [Start] option in the "Network Packets Capture". A message will pop up asking the user to save the captured file. At this time, the user can perform related operations, such as starting/deactivating the line or making a call, and clicking the [Stop] button on the webpage after completion. Network packets during the device are saved in a file. Users can analyze the packet or send it to the Technical Support mailbox.

### Get device log

Log information is helpful when encountering abnormal problems. In order to obtain the log information of the device, the user can log on to the device web page, open the web page [device log], click the "start" button, follow the steps of the problem until the problem appears, and then click the "end" button, "save" to the local for analysis or send the log to the technician to locate the problem.

## Common Trouble Cases

### Trouble Cases

TROUBLE CASE	SOLUTION
Device could not boot up	<ol style="list-style-type: none"> <li>1. The device is powered by external power supply via power adapter or POE switch. Please use standard power adapter provided or POE switch met with the specification requirements and check if device is well connected to power source.</li> <li>2. If the device enters "POST mode" (the SIP/NET and function button indicators are always on), the device system is damaged. Please contact your location technical support to help you restore your equipment system.</li> </ol>
Device could not register to a service provider	<ol style="list-style-type: none"> <li>1. Please check if the device is connected to the network.</li> <li>2. If the network connection is good, please check your line configuration again. If all configurations are correct, contact your service provider for support, or follow the instructions in "10.4 Network Data Capture" to obtain a registered network packet and send it to the Support Email to help analyze the issue.</li> </ol>