PROVISION ISR®

Now you can see!

Outdoor Intercom

User manual

Models:

- INT-320WIPN

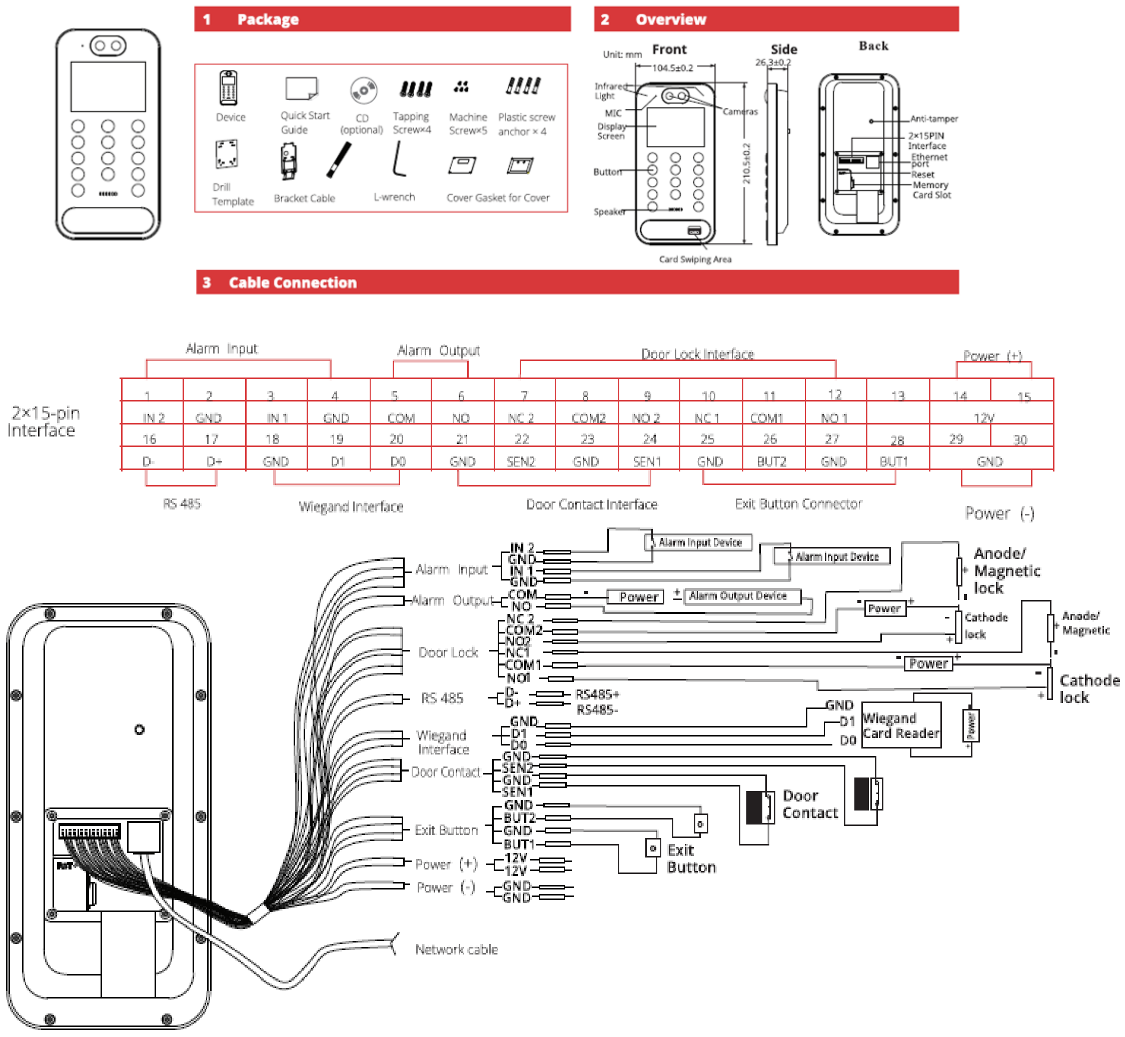
1) Terms & Conditions

- We strongly advise users to read this manual and keep it for later use for proper and safe device usage.
- Please use the provided & authorized by Provision-ISR technician power supply and power source indicated on the marking label. The power voltage must be verified before use.
- Avoid improper operation, shock vibration, and heavy pressing that can cause product damage.
- Do not use corrosive detergents when cleaning. When necessary, please use a soft dry cloth to wipe the dirt off; use neutral detergents for problematic pollution & decay. Any cleanser for high-grade furniture is applicable.
- Keep away from heat sources such as radiators, heat registers, stoves, etc.
- Do not try to repair the device without technical aid or approval.
- For camera installations:
- Avoid aiming the camera directly towards extremely bright objects, such as the sun, which may damage the image sensor.
- Please abstain from reversing the camera. This will result in an inverted image. Please follow the instructions for proper camera installation.
- Do not operate the camera in extreme temperatures or extreme humidity conditions.
- For Recorder & server installations:
- Do not block any ventilation openings and ensure proper airing around the device.
- Perform a safe shutdown before disconnecting from power. Otherwise, HDD damage and configuration loss might occur.
- This device is for indoor use only.
- Do not install this device near water, nor expose it to rainy or moist environments. If any solids or liquids get inside the device's case, turn the device off immediately and have it checked by a qualified technician.
- The instructions in this manual are suitable for all models running Ossia OS. Models which do not support any of the features will have explicit markings.
- For devices with internal power supply, please ensure that the AC 220/110V input selector is set correctly.

- There may be incorrect info or printing errors in this manual. PROVISION-ISR reserves the right to change this manual and publish the revision online on our website (www.provision-isr.com); there may be inconsistencies with the latest version, which apply to any software upgrades and product improvements, interpretation and modification added. Updates and corrections are subject to change without notice.
- All pictures and examples used in the manual are for reference purposes only.

- When this device is in use, the relevant contents of Microsoft, Apple and Google are involved. The ownership of trademarks, logos, and other intellectual properties related to Microsoft, Apple, and Google, belong to the companies mentioned above.

2) Wiring



	Alarm Input				Alarm Output		Door Lock Interface							Power (+)	
2×15-pin Interface	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	IN 2	GND	IN 1	GND	COM	NO	NC 2	COM2	NO 2	NC 1	COM1	NO 1		12V	
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	D-	D+	GND	D1	D0	GND	SEN2	GND	SEN1	GND	BUT2	GND	BUT1	GND	
	RS 485		Wiegand Interface			Door Contact Interface				Exit Button Connector				Power (-)	

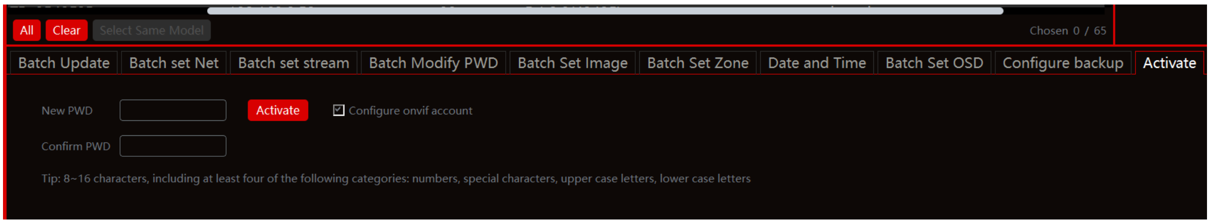
Note:
*The wiegand terminal here is a wiegand input terminal. If you want to connect to an access controller, you shall set the wiegand direction to "Output".

3) Camera Activation

The camera's default state is “Inactive”. This means that the camera must be activated before it can be used. The camera can be activated by 3 methods:

- IP Manager Tool: Select the camera(s) you wish to activate, set the new admin password and click activate (Note: the activation password must contain at least 8 characters and include 1 letter, 1 number, and 1 special character).

  After setting the password, you will have to set the answer to 3 recovery questions of your choice. These recovery questions can be used in case you have lost the admin password you have set.



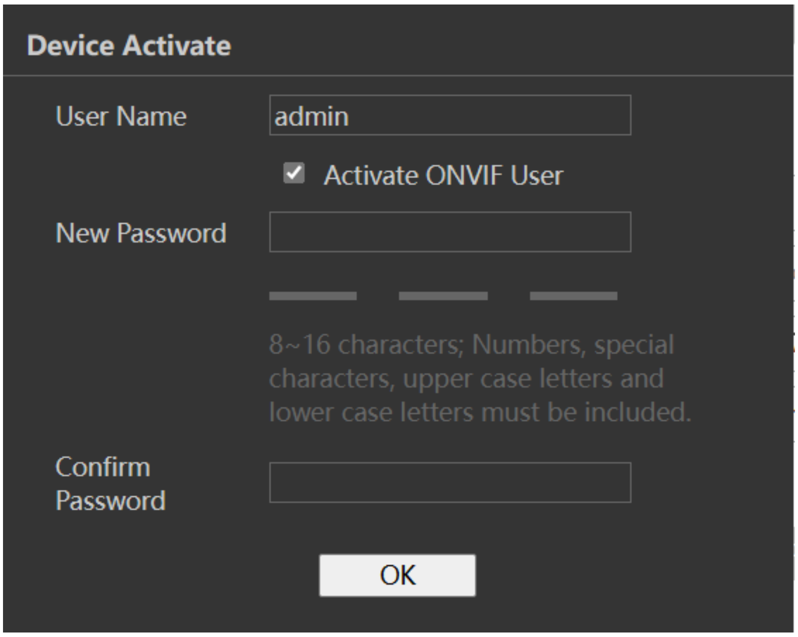
New PWD

Confirm PWD

☑ Configure onvif account

Tip: 8~16 characters, including at least four of the following categories: numbers, special characters, upper case letters, lower case letters

- Logging into the camera web page: When browsing to the camera for the first time, you will be prompted to activate it. Use credentials admin/123456 for the first login, then you will be prompted to set the new admin password and click activate (Note: the activation password must contain at least 8 characters and include 1 letter, 1 number, and 1 special character).
- After setting the password, you will have to set the answer to 3 recovery questions of your choice. These recovery questions can be used in case you have lost the admin password you have set.



User Name: admin

☑ Activate ONVIF User

New Password

8~16 characters; Numbers, special characters, upper case letters and lower case letters must be included.

Confirm Password

- Setting the camera on an NVR: Once set on an NVR, the IPC will be activated automatically.

4) Remote Access

Cameras running FW version >5.1.1 support all modern browsers (Chrome, Firefox, Safari, Opera, Edge), and can also work on Edge in IE mode.

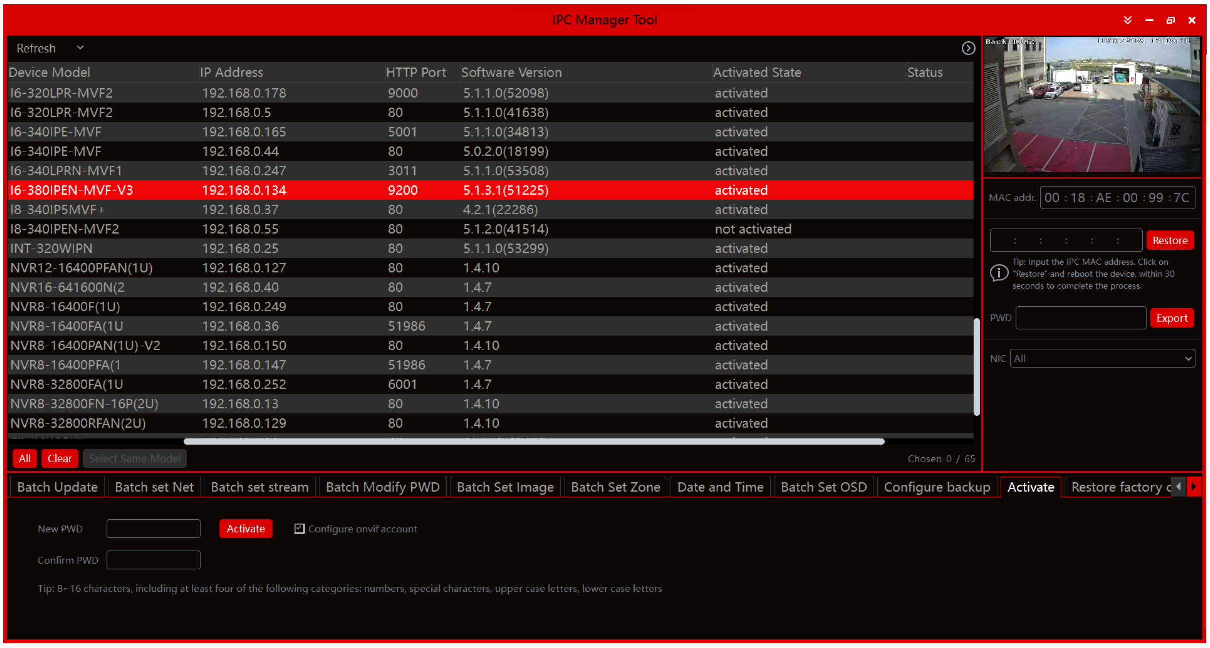
4.1) LAN

In LAN, there are two ways to access IPC:

- Access through IP Manager Software.
- Direct access through IE browser.

4.1.1) Access through the IP Manager Tool

- Make sure the PC and IPC are connected to the LAN and that the IP Manager is installed on the PC. You can download the IP manager from here.
- Double-click the IP-Manager icon on the desktop to run this software.



Device Model	IP Address	HTTP Port	Software Version	Activated State	Status
I6-320LPR-MVF2	192.168.0.178	9000	5.1.1.0(52098)	activated	
I6-320LPR-MVF2	192.168.0.5	80	5.1.1.0(41638)	activated	
I6-340IPE-MVF	192.168.0.165	5001	5.1.1.0(34813)	activated	
I6-340IPE-MVF	192.168.0.44	80	5.0.2.0(18199)	activated	
I6-340LPRN-MVF1	192.168.0.247	3011	5.1.1.0(53508)	activated	
I6-380IPEN-MVF-V3	192.168.0.134	9200	5.1.3.1(51225)	activated	
I8-340IP5MVF+	192.168.0.37	80	4.2.1(22286)	activated	
I8-340IPEN-MVF2	192.168.0.55	80	5.1.2.0(41514)	not activated	
INT-320WIPN	192.168.0.25	80	5.1.1.0(53299)	activated	
NVR12-16400PFAN(1U)	192.168.0.127	80	1.4.10	activated	
NVR16-641600N(2	192.168.0.40	80	1.4.7	activated	
NVR8-16400F(1U)	192.168.0.249	80	1.4.7	activated	
NVR8-16400FA(1U	192.168.0.36	51986	1.4.7	activated	
NVR8-16400PAN(1U)-V2	192.168.0.150	80	1.4.10	activated	
NVR8-16400PFA(1	192.168.0.147	51986	1.4.7	activated	
NVR8-32800FA(1U	192.168.0.252	6001	1.4.7	activated	
NVR8-32800FN-16P(2U)	192.168.0.13	80	1.4.10	activated	
NVR8-32800RFAN(2U)	192.168.0.129	80	1.4.10	activated	

Chosen 0 / 65

MAC addr. 00 : 18 : AE : 00 : 99 : 7C

Tip: Input the IPC MAC address. Click on "Restore" and reboot the device. within 30 seconds to complete the process.

PWD

NIC All

New PWD

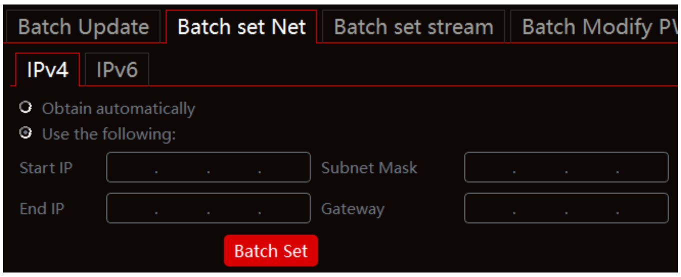
Confirm PWD

☑ Configure onvif account

Tip: 8~16 characters, including at least four of the following categories: numbers, special characters, upper case letters, lower case letters

- Modify the IP address. The default TCP/IP setting of this camera is set to DHCP so the address is not fixed. If no DHCP server is available on your network, the camera setting will change to “fixed IP” with the address 192.168.226.201. Tick all the cameras you wish to set and then click on the “Batch Set NET” tab.

If you wish to set static IP addresses, choose “Use the following IP Addresses”, set the range of IP addresses you wish to assign (First and last address), set the gateway and subnet mask, and click on batch set. Wait for a few moments until the IP manager will configure the cameras. After configuration, the IP addresses of the cameras will refresh automatically.



○ Obtain automatically
○ Use the following:

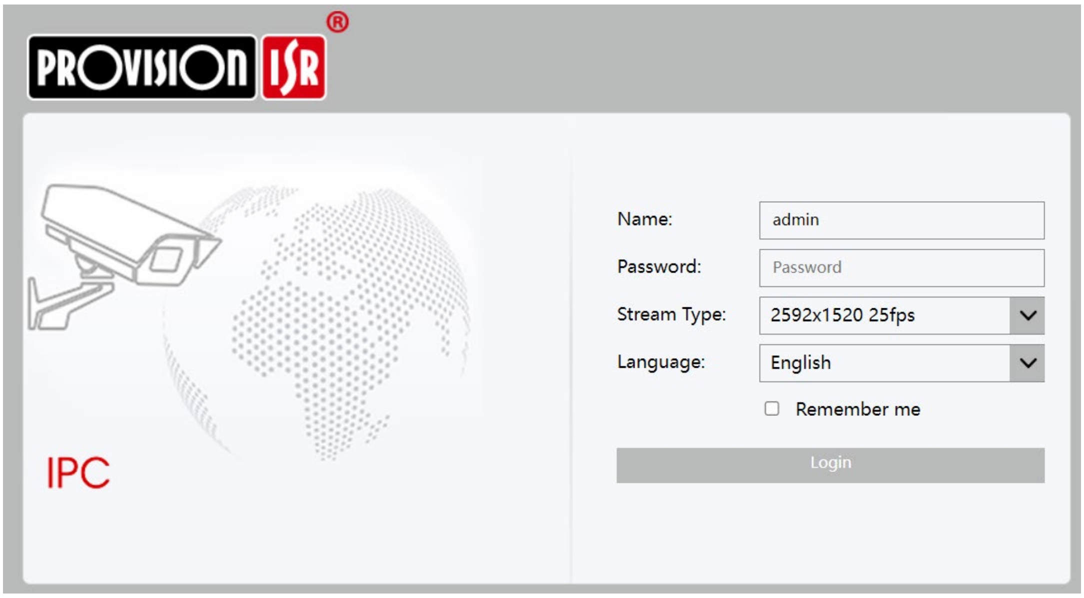
Start IP . . .
Subnet Mask . . .
End IP . . .
Gateway . . .

Please note:

- ❖ The IP range must fit the number of chosen cameras.
- ❖ The selected IP addresses in the specified range must be available.

For example, if the IP address of your computer is 192.168.1.4, then the IP address of the cameras should be changed to 192.168.1.x. (x stands for any number between 1 and 255).

- Double-click on the IP address of the device you want to connect to. The system will automatically open a browser and connect to the IPC. A login window will appear as shown below.



Name: admin

Password: Password

Stream Type: 2592x1520 25fps

Language: English

□ Remember me

Input the username and password to log in.

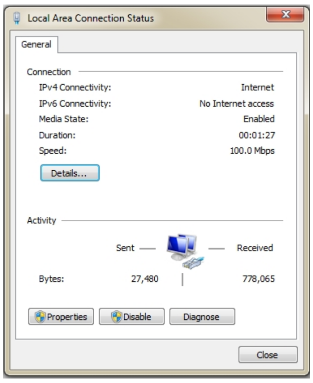
4.1.2) Direct Access through Web-Browser

In case there is no DHCP server available in the network, the default network settings will be as shown below:

IP address: 192.168.226.201
Subnet Mask: 255.255.255.0
Gateway: 192.168.226.1
HTTP: 80
Data port: 9008

You may use the above default settings when you log in to the camera for the first time.

1. You can use the IP manager to access the camera even if the camera is still using the default IP address. Double-click on the IP address within the IP manager for the system to open your default web browser and browse to the camera. You can then set the IP address from the camera configuration menu.
2. If you wish to access the camera using its default IP address (192.168.226.201) you will have to manually set the IP address of the PC to be in the same IP segment as the default settings of the IP camera. Open the network and sharing center. Click “Local Area Connection” to pop up the following window.



Local Area Connection Status

General

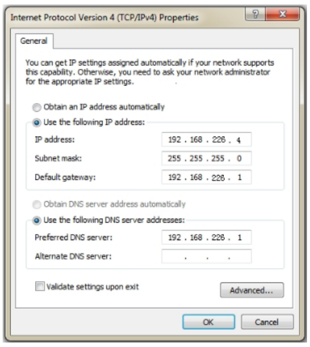
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	00:01:27
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	27,480	778,065

Select “Properties” and then select internet protocol according to the actual situation (most probably you are using IPv4). Next, click on the “Properties” button and set the network of the PC as shown on the right.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 226 . 4

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 226 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 226 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

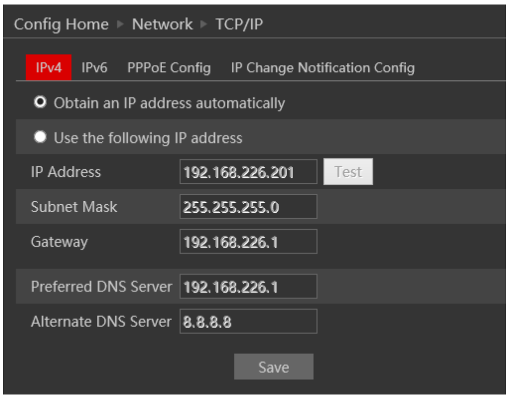
Open your preferred web browser, input the IP address of IPC and confirm. Input the default username and password and click “Login”.

4.2) WAN

4.2.1) Direct Access through IP/DDNS

Allows you to access the camera using a router or virtual server.

1. Make sure the camera is well connected and configured via LAN. Log in to the camera via LAN and go to the Config→Network Config→Port menu to set up the port number.
2. Go to Config→Network Config→TCP/IP menu to modify the IP address.
3. After modifying the IP Address, click on "Port" and modify the port according to your needs.

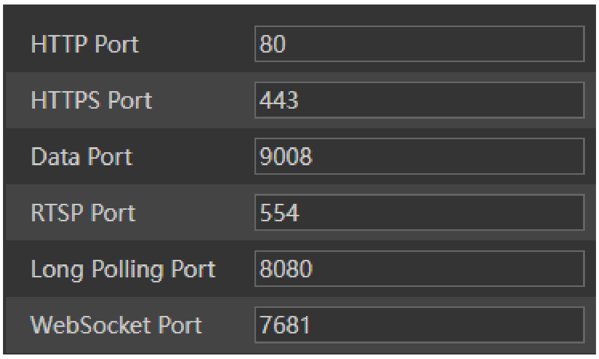


Config Home ▸ Network ▸ TCP/IP

○ Obtain an IP address automatically

● Use the following IP address

IP Address	192.168.226.201 Test
Subnet Mask	255.255.255.0
Gateway	192.168.226.1
Preferred DNS Server	192.168.226.1
Alternate DNS Server	8.8.8.8



HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554
Long Polling Port	8080
WebSocket Port	7681

IP Setup

Port Setup

4. Go to the router's management interface through your browser to forward the IP address and port of the camera to the "Virtual Server". In the picture example below, you will see an example of the setting as if the IPC IP address is "192.168.6.6" and the ports are default (9008 & 80)

   Default Ports:

   HTTP Port (Default is 80) is for HTTP and API

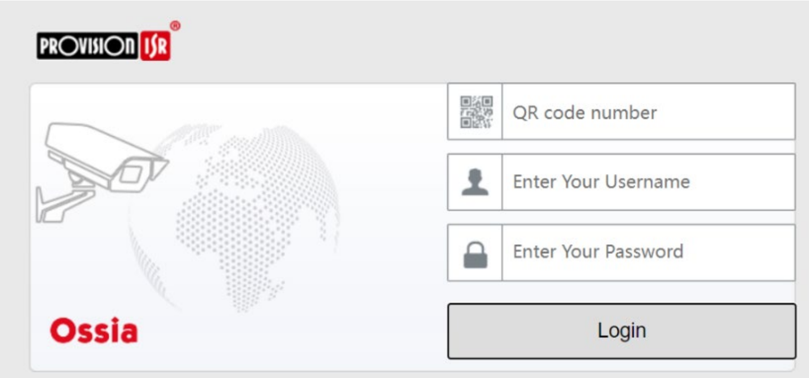
   Data Port (Default is 9008) is for IE video data and SDK

   WebSocket Port (Default is 9681) is for modern browser video streaming

4.2.2) Access through NAT/P2P

P2P allows indirect connection to the camera without the need for port forwarding and virtual server triggers on the router.

1. Enable P2P (Please refer to chapter Network→P2P for more information)
2. Browse to http://www.provisionisr-cloud.com to the following interface



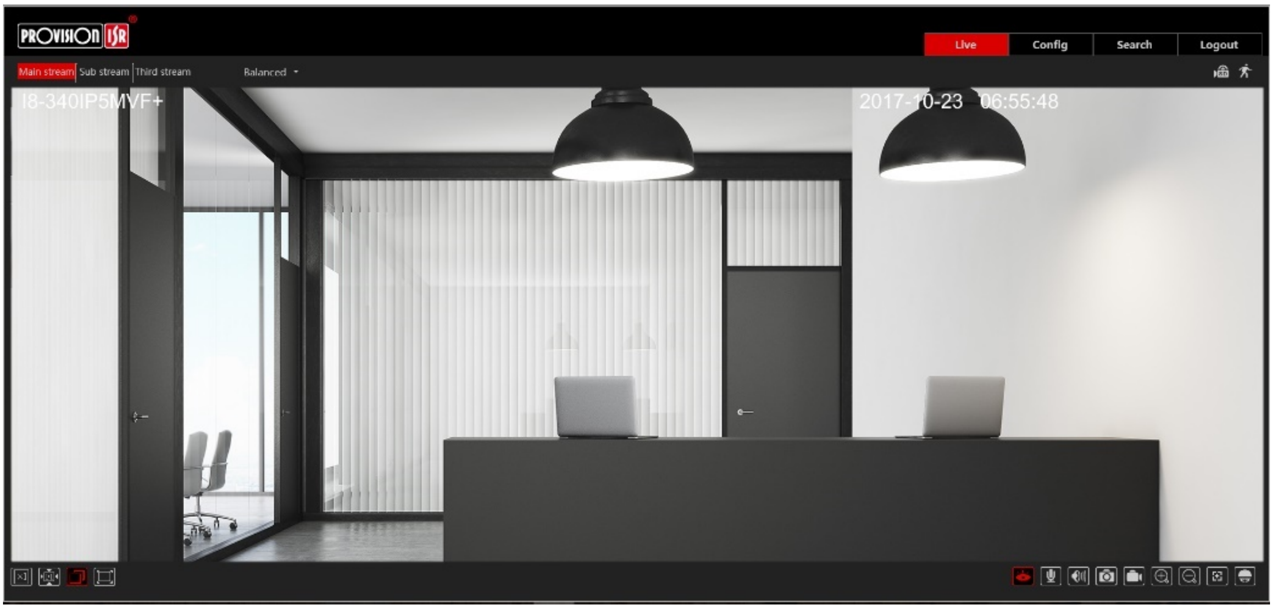
Input the QR code number, user name, and password, then click on "Login"

Please note:

- The QR code number can be found under settings→System→Basic Information.
- P2P Connection is only supported via IE Web browser (Or Edge on IE mode)
- P2P Connection offers limited features/configuration than direct IP/DDNS connection

5) Live Preview

5.1) Live View Interface



Icons and operation buttons:

Icon	Description	Icon	Description
×1	Actual Video Size	👤	Face Detection/Recognition
1:1	Fit to screen – True Proportions	⊕	Digital Zoom-in
⧉	Fit to screen - Stretch	⊖	Digital Zoom-Out
⛶	Full-screen	🏃 / 🏃	Motion Detection indicator
🚪	Open the door	SD	SD Card recording indicator
👁 / 👁	Enable/Disable live view	((•)) / ((•))	Alarm In Indicator
🎤	Talk	Main stream	Use mainstream for live-view

🔊	Listen	Sub stream	Use sub-stream for live-view
📷	Take Snapshot	Third stream	Use third stream for live-view
🎥	Enable/Disable Local Recording	Balanced ▾	Choose the buffering plan

6) IPC Configuration

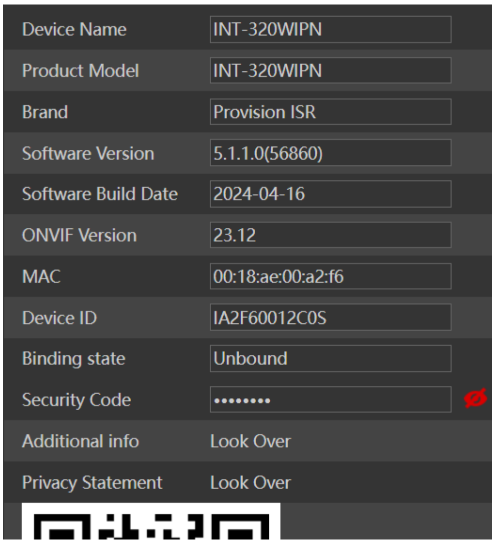
In this chapter, we will go through all the possible configurations of the IPC.

6.1) System Configuration

The “System Configuration” includes four submenus: Basic Information, Date & Time, Local Config, and Storage.

6.1.1) Basic Information

In the “Basic Information” interface, you can view all the necessary information related to the IPC, as seen on the right:



Device Name	INT-320WIPN
Product Model	INT-320WIPN
Brand	Provision ISR
Software Version	5.1.1.0(56860)
Software Build Date	2024-04-16
ONVIF Version	23.12
MAC	00:18:ae:00:a2:f6
Device ID	IA2F60012C0S
Binding state	Unbound
Security Code	••••••••
Additional info	Look Over
Privacy Statement	Look Over

The following table will explain the available detail field.

Parameter	Explanation
Device name	Name of the device – can be modified from the OSD settings
Product Model	The model of the device
Brand	The brand of the camera
Software version	The current software version
Software build date	The software build-date
ONVIF Version	The current ONVIF version
S/N	Device serial number
MAC	The MAC address of the device

Device ID and QR	QR Code used for P2P connection
Binding State	Shows the binding state between the device and mobile app account
Security Code	Required for binding the intercom to the mobile app account. To view the security code, click on the icon and authenticate.

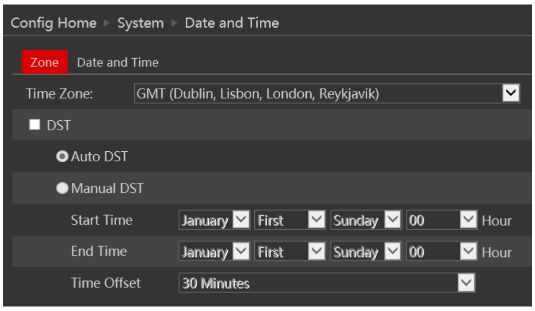
Additional information can be found when clicking on “About this machine”. The relevant details are below

Parameter	**Explanation**
Hardware version	The hardware identifier of the device
Kernel version	The kernel version of the device
Video Structured version	The AI engines version on the current firmware

6.1.2) Date & Time Configuration

Setting steps:

1. Go to Config→Date & Time menu as shown below.



Config Home ▸ System ▸ Date and Time

Zone | Date and Time

Time Zone: GMT (Dublin, Lisbon, London, Reykjavik)

□ DST

◉ Auto DST

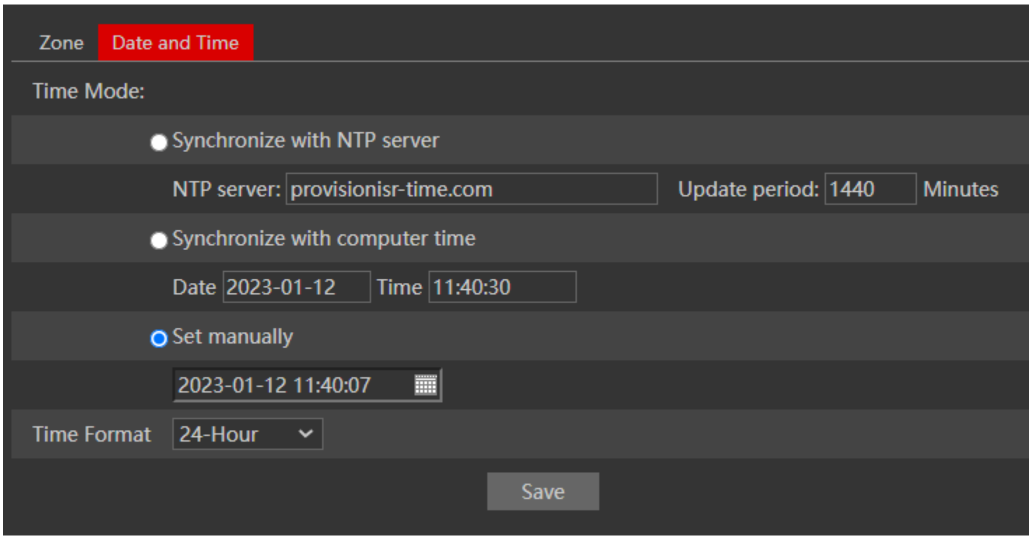
○ Manual DST

Start Time: January, First, Sunday, 00 Hour

End Time: January, First, Sunday, 00 Hour

Time Offset: 30 Minutes

2. Set the time zone.
3. Enable DST mode if required. DST settings are already configured according to your time zone. If you wish to set the DST manually, switch to “Manual DST” and set it accordingly.
4. To set the date and time, click on the “Date and Time” tab. You may synchronize the camera time with an NTP server and set the NTP time correction intervals (Internet connection required), synchronize the camera time with the time of the computer you are using, or set the time manually.



Zone | Date and Time

Time Mode:

○ Synchronize with NTP server

NTP server: provisionisr-time.com Update period: 1440 Minutes

○ Synchronize with computer time

Date 2023-01-12 Time 11:40:30

● Set manually

2023-01-12 11:40:07

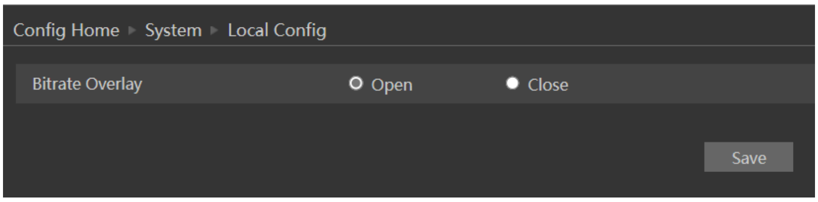
Time Format 24-Hour

Save

5. Set the camera time format (12/24H)

6.2) Local Config

Go to “System Configuration” →“Local config” as shown below:

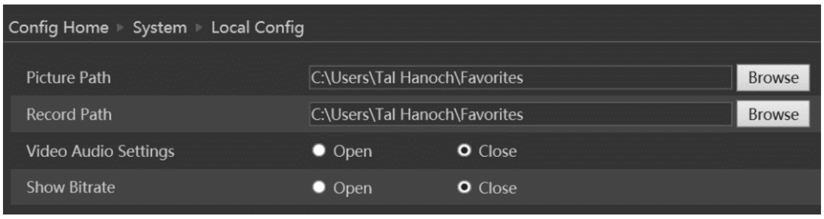


Config Home ▸ System ▸ Local Config

Bitrate Overlay ● Open ○ Close

Save

Using an older IE web browser will open the following interface



Config Home ▸ System ▸ Local Config

Picture Path C:\Users\Tal Hanoch\Favorites Browse

Record Path C:\Users\Tal Hanoch\Favorites Browse

Video Audio Settings ○ Open ● Close

Show Bitrate ○ Open ● Close

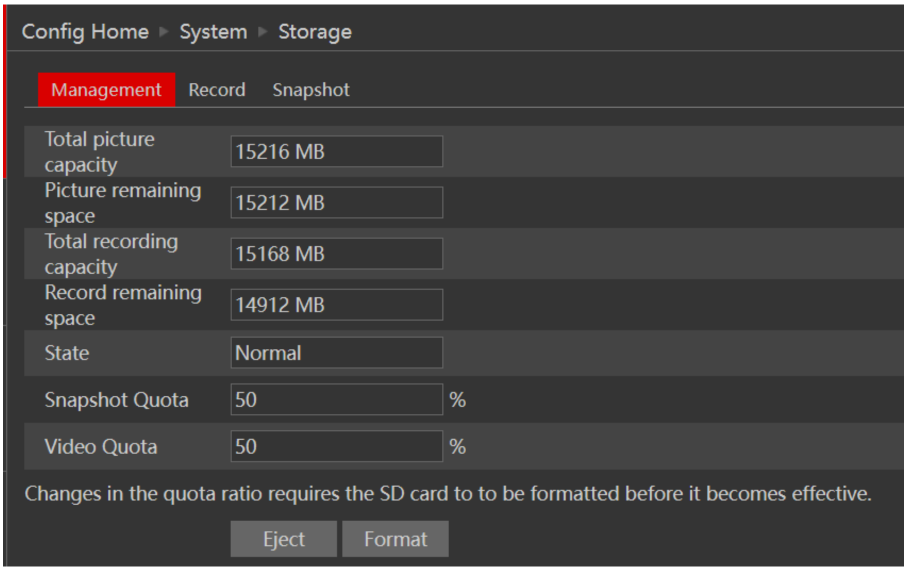
From here you can set the path on your computer where local snapshots and videos will be saved.

You can also choose if the camera will show the current bit-rate on the live-view image (Local interface only).

6.3) Storage

The SD card feature allows you to insert an SD card into the camera and enable the camera to operate with local storage. The SD card will be used for both snapshot and video files. You can allocate a certain percentage for each from the settings menu.

Go to “System Configuration” →“Storage” as shown below:



Total picture capacity: 15216 MB

Picture remaining space: 15212 MB

Total recording capacity: 15168 MB

Record remaining space: 14912 MB

State: Normal

Snapshot Quota: 50 %

Video Quota: 50 %

Changes in the quota ratio requires the SD card to to be formatted before it becomes effective.

If it is the first time you are using the SD card with the camera or if the state is showing any value different than “Normal”, you should click on “Format” before the SD card will be available for recording.

Click “Eject card” to stop writing data to the SD card and allow you to remove it safely.

Inserting an SD card into the camera must be done while the camera is powered off.

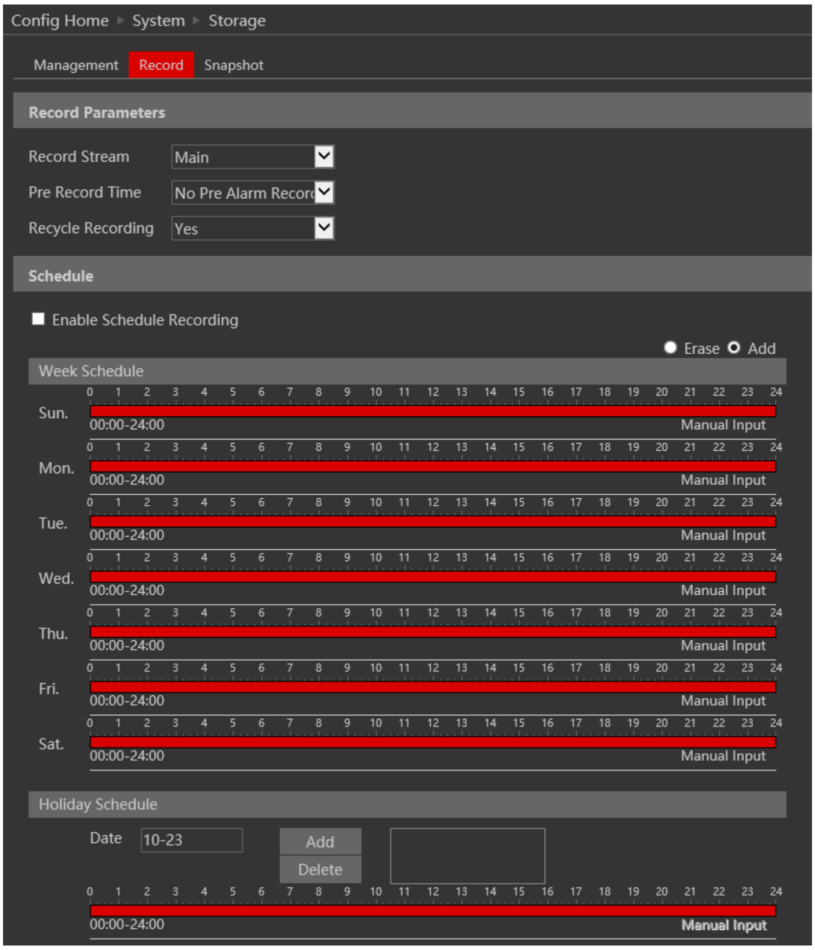
Please note:

- Removing the SD card while the camera is working without using the “Eject” button, will corrupt all the record data and make it unusable.

The following table will explain the available detail fields.

Parameter	**Meaning**
Total picture capacity	The total capacity dedicated to pictures (Snapshots)
Picture remaining space	Available capacity for pictures (Snapshots)
Total recording capacity	The total capacity dedicated to video records
Recording remaining space	Available capacity for video records
State	The state of the SD card.
Snapshot Quota	The percentage of the SD card dedicated to Snapshots
Video Quota	The percentage of the SD card dedicated to Videos

The next tab is “Record”. Click on it to set the video recording parameters and schedule.



Config Home ▸ System ▸ Storage

Management | Record | Snapshot

Record Parameters

Record Stream: Main

Pre Record Time: No Pre Alarm Recor

Recycle Recording: Yes

Schedule

□ Enable Schedule Recording

● Erase ○ Add

Week Schedule

Sun.	00:00-24:00	Manual Input
Mon.	00:00-24:00	Manual Input
Tue.	00:00-24:00	Manual Input
Wed.	00:00-24:00	Manual Input
Thu.	00:00-24:00	Manual Input
Fri.	00:00-24:00	Manual Input
Sat.	00:00-24:00	Manual Input

Holiday Schedule

Date: 10-23 | Add | Delete

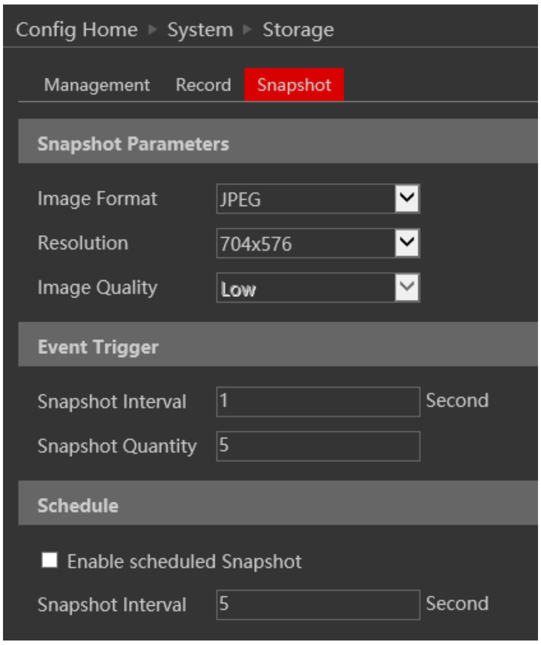
00:00-24:00 | Manual Input

The video parameters are as follows:

Parameter	Meaning
Record stream	Which video stream will be used to record
Pre-recording time	The duration of the video before the recording trigger
Cycle recording	Whether to recycle the record or stop when the SD card is full

Below are the schedule settings. Enable the schedule if required and set the recording time for each of the weekdays. You can also set a holiday schedule and add the required dates to it.

The next tab is “Snapshot” Click on it to set the snapshot parameters and schedule.



Snapshot Parameters

Image Format: JPEG

Resolution: 704x576

Image Quality: Low

Event Trigger

Snapshot Interval: 1 Second

Snapshot Quantity: 5

Schedule

□ Enable scheduled Snapshot

Snapshot Interval: 5 Second

The snapshot parameters are as follows:

Parameter	Meaning
Image Format	The image format is JPEG
Resolution	Set the snapshot resolution
Image quality	The quality of the image reflects its size.
Snapshot Interval	The duration between two snapshots
Snapshot Quantity	The total number of snapshots to be taken after a trigger
Scheduled snapshots	Taking a snapshot according to a specified schedule

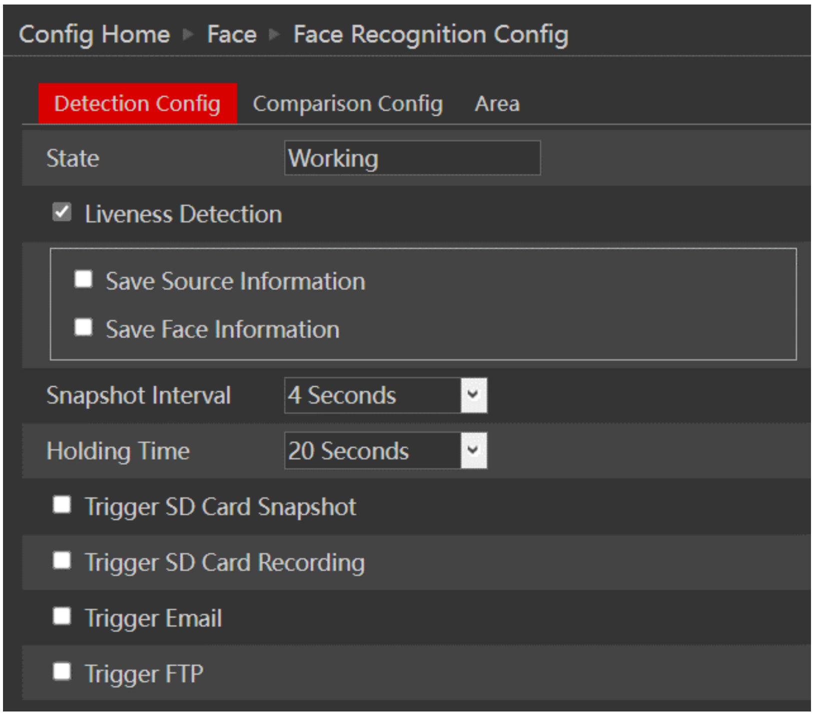
Below are the schedule settings. Enable the schedule if required and set the recording time for each of the weekdays. You can also set a holiday schedule and add the required dates to it.

6.4) Face

This camera offers advanced face detection/recognition alrorythm to identify people and respond accordingly.

6.4.1) Face Recognition Config

Face Recognition analytics will detect human faces in the defined area run the recognition algorithm and compare it to the camera internal database. If there is a match, the camera will trigger the required alerts. The face recognition is enabled by default to allow the normal operation of the device.


Config Home ▸ Face ▸ Face Recognition Config

Detection Config | Comparison Config | Area

State: Working

☑ Liveness Detection

□ Save Source Information

□ Save Face Information

Snapshot Interval: 4 Seconds

Holding Time: 20 Seconds

□ Trigger SD Card Snapshot

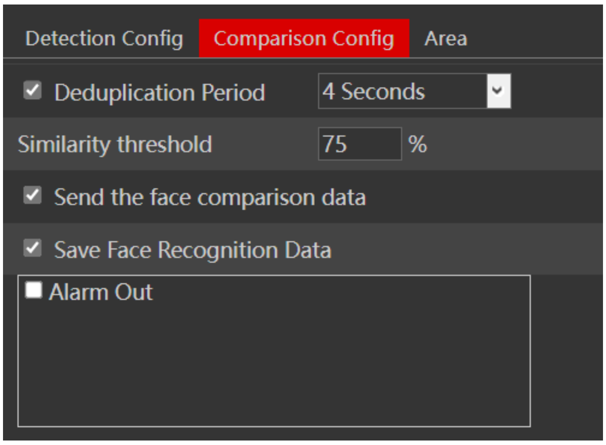
□ Trigger SD Card Recording

□ Trigger Email

□ Trigger FTP

Options:	Explanation:
Liveness Detection	Use dual lens and IR technology to confirm that the face is a real human face with 3D feauteres.
Save source information	Wether to keep the full scene image in case of face detection event
Save Face information	Wether to keep the cropped face image in case of face detection event
Snapshot interval	The time between taking snapshots of the same face
Holding time	The time between face detection event triggers
Trigger Snap	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

The next step is to set the recognition settings. Click on the “Comparison Config” Tab:


Detection Config | Comparison Config | Area

☑ Deduplication Period: 4 Seconds

Similarity threshold: 75 %

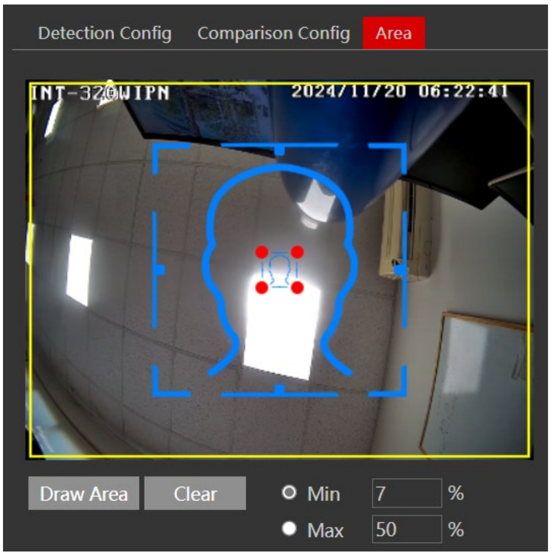
☑ Send the face comparison data

☑ Save Face Recognition Data

□ Alarm Out

Options:	**Explanation:**
Deduplication Period	During the specified period, delete duplicate comparison results.
Similarity Threshold	When the similarity between the captured face image and the face image in the database exceeds the defined threshold, alarms will be triggered.
Send Face Comparison Data	If disabled, the face comparison results will not be displayed on the terminal screen or the live interface of the web client.
Save Face Comparison Data	If enabled, the comparison data will be saved, allowing you to search for face recognition results in the data record interface. If disabled, any face comparison data generated after disabling this function will not be available for search in the data record interface.
Alarm Out	Select if alarm output will be triggered as response

Next you will need to set the detection area and fice size



○ Min 7 %

● Max 50 %

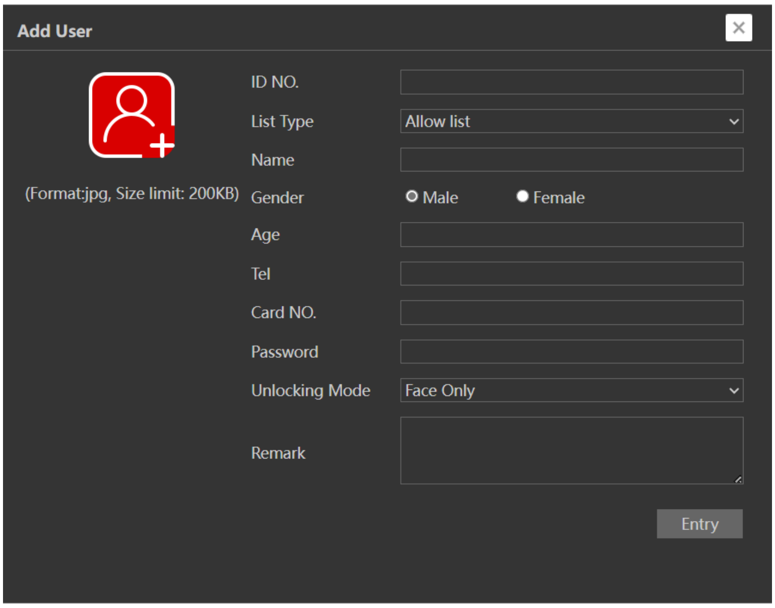
1. Click on “Area” to navigae to the following window.
2. Set the detection area (marked in yellow).
3. Set the minimum and maximum face size in the frame. (Marked in blue). Notice that the blue face sketch is reference only. Its position is not changing any setting.

Next we will set the installation application. Different application requires different behavior from the face detection algorithm.

6.4.2) Face Database Management

Here you will manage your face database. You can add, edit and delete faces from this interface. There are four ways to add face pictures:

Adding face pictures one by one: Click to open the "Add User" icon to open the following interface:



Add User

(Format:jpg, Size limit: 200KB)

ID NO.	
List Type	Allow list
Name	
Gender	● Male ○ Female
Age	
Tel	
Card NO.	
Password	
Unlocking Mode	Face Only
Remark	

Click on the “Add image icon” (🔒) to select a face picture saved on the local PC. Ensure the selected picture meets the specified format and size requirements.

Fill in the relevant information for the face picture and click "Entry" to add it.

See the explanation below.
(O) means that the field is **Optional** and can remain blank
(M) means that the field is **Mandatory** and must be filled

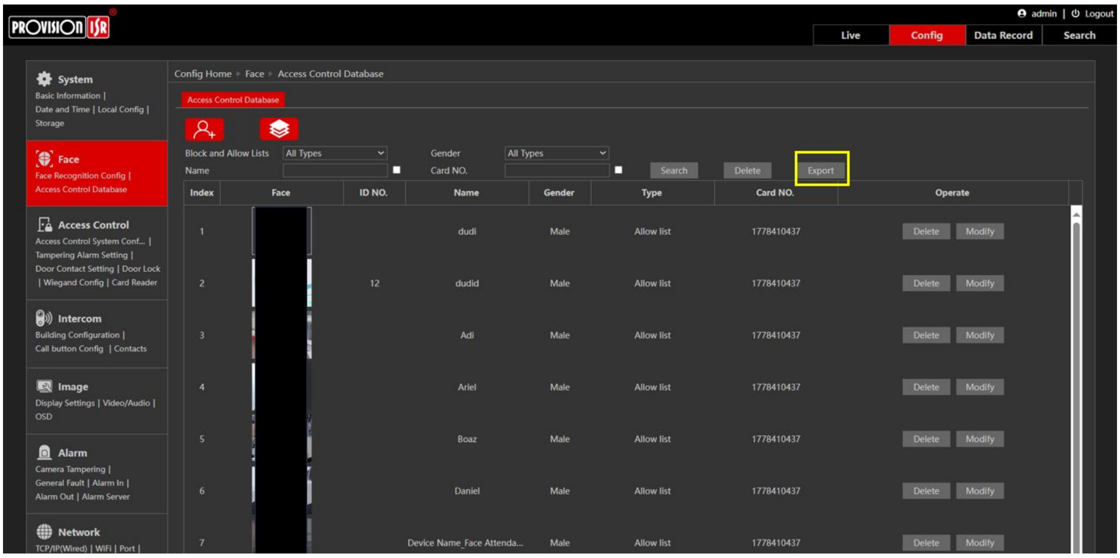
Options:	**Explanation:**
ID No. (O)	Preferred ID Number
List Type (M)	The list type where the face will be added. The options are: Visitor, Allow list, Block list.
Name (M)	The name of the person
Gender (O)	The gender of the person
Age (O)	The age of the person
Tel (O)	The telephone number of the person
Card No. (O/M)	The RFID card number. Optional, unless chosen as part of the unlocking mode
Password (O/M)	A numeric PIN. Optional, unless chosen as part of the unlocking mode
Unlocking Mode (M)	Choose between face only, swiping card only, or a combination of unlocking modes.
Remark (O)	Any remark you wish to add

Adding multiple face pictures at once: Click the bulk add icon (≋) button, then click "Rule" to view the file requirements. Follow the provided instructions to add multiple face pictures simultaneously.
For example, use a people information file (.csv) as shown.
Place the information file and images in the same directory as demonstrated.
Click "Choose Face" to select the pictures you want to import, then click "All Entry" to upload them.
Adding face pictures using the face album management tool:
Use the face album management tool for efficient batch processing and importing of face pictures.

Adding captured pictures in live mode: Once a face is detected, click on the Face to open the "Add Face" dialog then follow the instructions as stated in "Adding face pictures one by one".
Use the "Modify" option to update the person's information or click "Delete" to remove the face picture.

6.5) Import / Export face DB using intercom

1. Go to Access control database > press Search > press Export


PROVISION ISR
admin | Logout
Live
Config
Data Record
Search
System
Basic Information | Date and Time | Local Config | Storage
Face
Face Recognition Config | Access Control Database
Access Control
Access Control System Conf... | Tampering Alarm Setting | Door Contact Setting | Door Lock | Wiegand Config | Card Reader
Intercom
Building Configuration | Call button Config | Contacts
Image
Display Settings | Video/Audio | OSD
Alarm
Camera Tampering | General Fault | Alarm In | Alarm Out | Alarm Server
Network
TCP/IP(Wired) | WiFi | Port |
Config Home ▸ Face ▸ Access Control Database
Access Control Database
Search
Delete
Export

Block and Allow Lists: All Types
Gender: All Types
Name:
Card NO.:

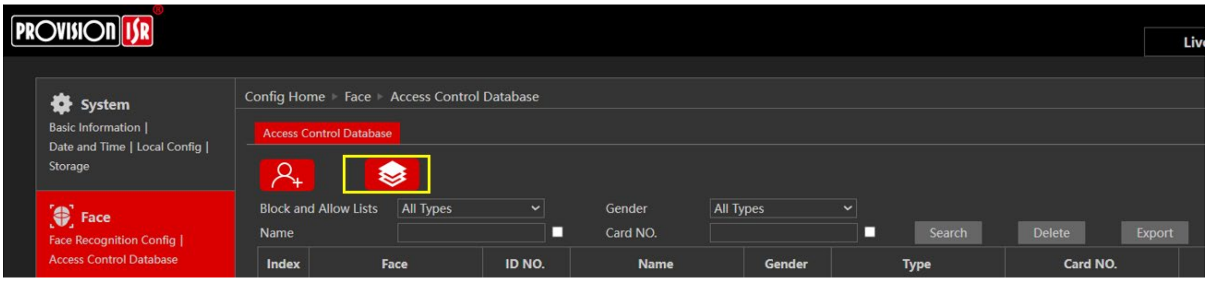
Index	Face	ID NO.	Name	Gender	Type	Card NO.	Operate
1	[redacted]		dudi	Male	Allow list	1778410437	Delete Modify
2	[redacted]	12	dudid	Male	Allow list	1778410437	Delete Modify
3	[redacted]		Adi	Male	Allow list	1778410437	Delete Modify
4	[redacted]		Ariel	Male	Allow list	1778410437	Delete Modify
5	[redacted]		Boaz	Male	Allow list	1778410437	Delete Modify
6	[redacted]		Daniel	Male	Allow list	1778410437	Delete Modify
7	[redacted]		Device Name_Face Attenda...	Male	Allow list	1778410437	Delete Modify

A CSV and face images area exported into .RAR file.

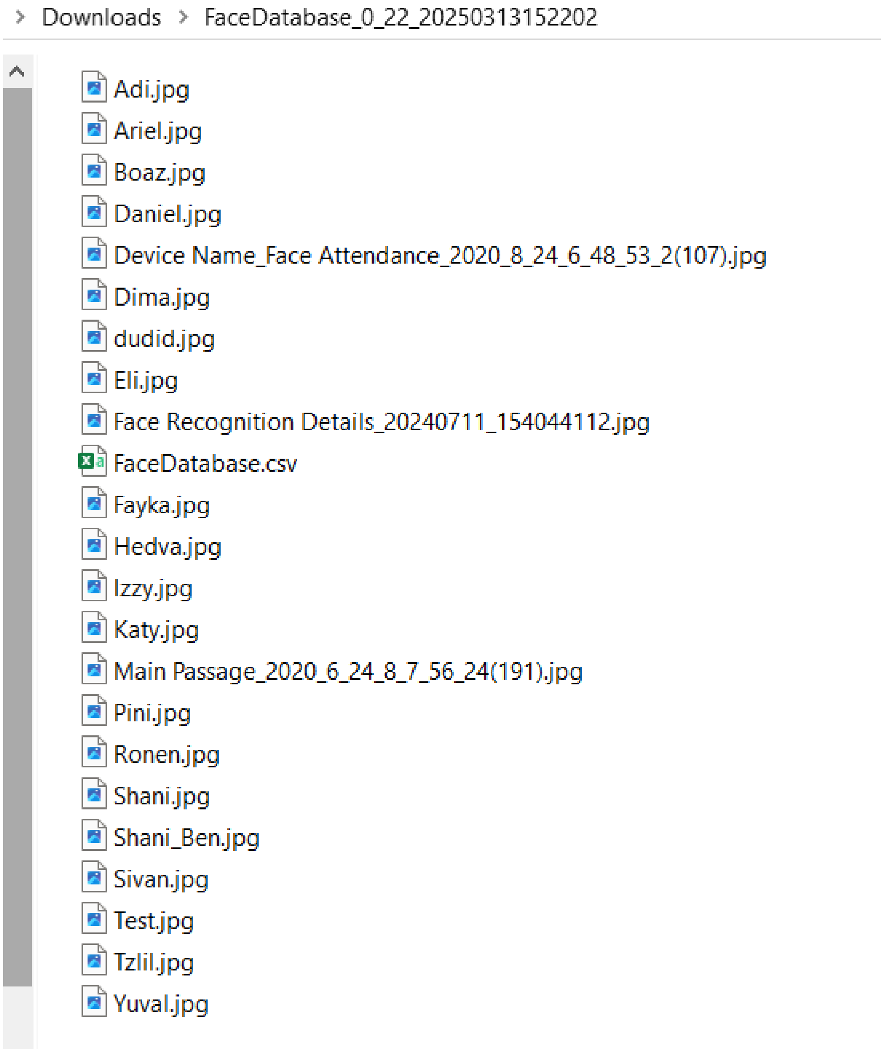
2.Extract the .RAR

3.Importing:

While in access control database > press Bulk Entry:



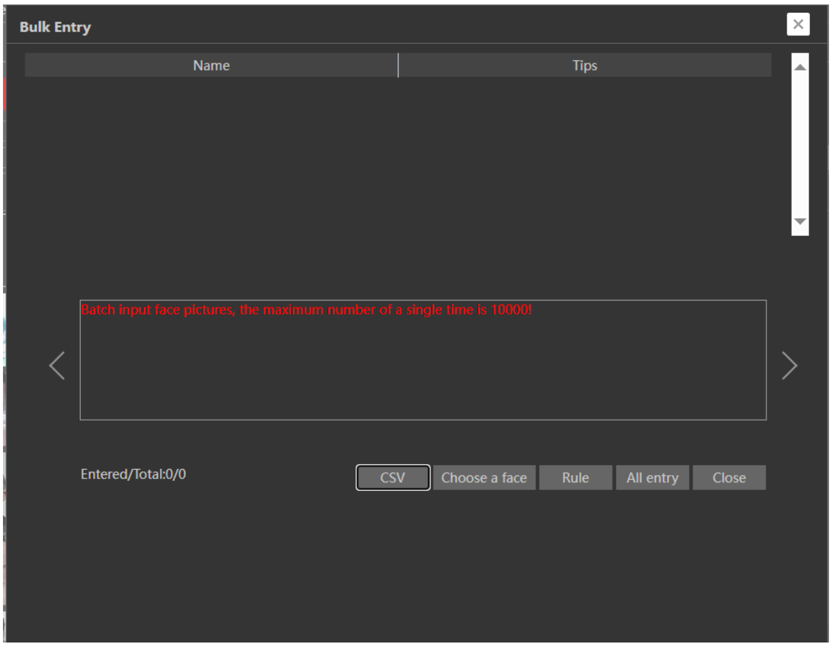
Your extracted folder should look like this


› Downloads › FaceDatabase_0_22_20250313152202

- Adi.jpg
- Ariel.jpg
- Boaz.jpg
- Daniel.jpg
- Device Name_Face Attendance_2020_8_24_6_48_53_2(107).jpg
- Dima.jpg
- dudid.jpg
- Eli.jpg
- Face Recognition Details_20240711_154044112.jpg
- FaceDatabase.csv
- Fayka.jpg
- Hedva.jpg
- Izzy.jpg
- Katy.jpg
- Main Passage_2020_6_24_8_7_56_24(191).jpg
- Pini.jpg
- Ronen.jpg
- Shani.jpg
- Shani_Ben.jpg
- Sivan.jpg
- Test.jpg
- Tzlil.jpg
- Yuval.jpg

Note: that one of the files is the CSV, and the rest are images

4.Then Choose the CSV File:

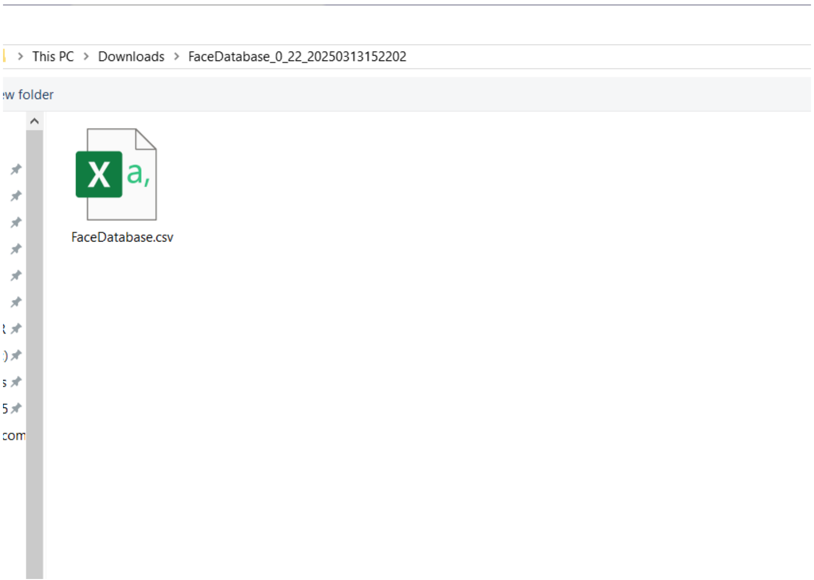


Bulk Entry

Name	Tips

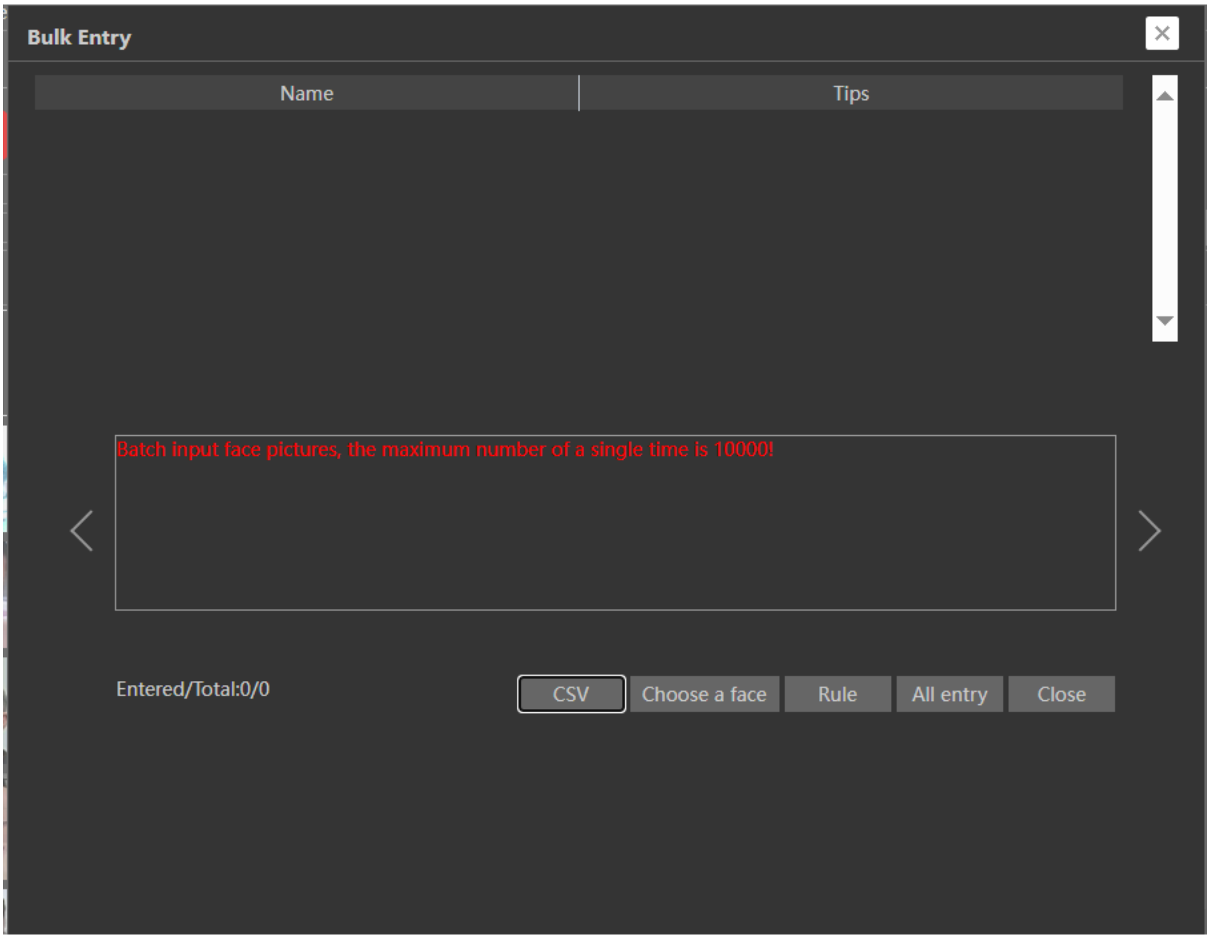
Batch input face pictures, the maximum number of a single time is 10000!

Entered/Total:0/0



This PC > Downloads > FaceDatabase_0_22_20250313152202

Then Press “Choose a face” and select all faces in the exported folder



Batch input face pictures, the maximum number of a single time is 10000!

6.6) RFID Key-Fob registration

The INT-320WIPN supports EM (125kHz) and Mifare (13.56MHz) RFID protocols. If you wish to use it, you can perform one of the 2 actions below.

6.6.1) Use the integral reader Input:

If the RFID card doesn't present the number, or the number is not known to you, use this method:

1. Access the device web page using the configured IP, port, username and password.
2. Browse to Settings→Access Control→User Management
3. Click on the "Add User" Icon
4. Set the List Type to "Allow List" (Default)
5. Input the name
6. Click on the "Card NO." field (Do not input any data)
7. Present the RFID card to the INT-320WIPN RFID reader. You will hear an audio prompt "Badge read correctly" and the Key fob number will be filled automatically.
8. Click on Entry to save.
9. If you need to add additional Key Fobs, repeat steps 3-8

6.6.2) Manual Reading:

If the RFID card has a number on it, or the number is known to you, use this method:

1. Access the device web page using the configured IP, port, username and password.
2. Browse to Settings→Access Control→User Management
3. Click on the "Add User" Icon
4. Set the List Type to "Allow List" (Default)
5. Input the name
6. Click on the "Card NO." field and input the card number manually
7. Click on Entry to save.
8. If you need to add additional Key Fobs, repeat steps 3-7

6.7) Access Control

Settings and management of the integral access control feature of the intercom.

6.7.1) Access Control System Config

In the "Config" tab you can set the basic features of the intercom as described below:

Options:	Explanation:

Select Language	Select the screen display language on the panel
Select Voice	Select the language of the voice prompts
Screen sleep time	Set how long the screen display will turn off after no person appears. The default time is 30s. Please set it as needed. In a sleep state, once a person is detected by the camera, it will be turn on immediately.
Keypad Blacklight	Select “Auto”, “Manual” or “Off” as needed
Volume	Set the volume of the voice prompt
Screen Brightness	Set the brightness of the screen of the terminal. The adjustable range is from 150 to 255.

In the “Custom Voice” you can add your customized audio files to the device.

Select the voice prompt you want to replace, then click “Browse” to choose the desired audio file. Next, click “Upload” to upload the file and rename it if needed.

Once your custom voice prompt is uploaded, you can select it from the audio list and click “Listen” to preview it.

6.7.2) Tampering Alarm Setting

The device is equipped with the physical back tamper switch to detect when the unit is disassembled from the wall. Enable it if required and set the triggers as needed.

Alarm Triggers:	**Explanation:**
Trigger Alarm Out	Trigger the selectedalarm out relay
Trigger Audio Alarm	Trigger audible alarm
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

6.7.3) Door Contact Setting

Each door lock interface also has a door sensor that detects if the door is open or closed. If needed, you can set an alarm for events where the door is kept open longer than the allowed duration. Set it as below.

1. Choose the relevant door contact.
2. Enable the event trigger if needed.
3. Set the variables and triggers as below.

Alarm Triggers:	**Explanation:**

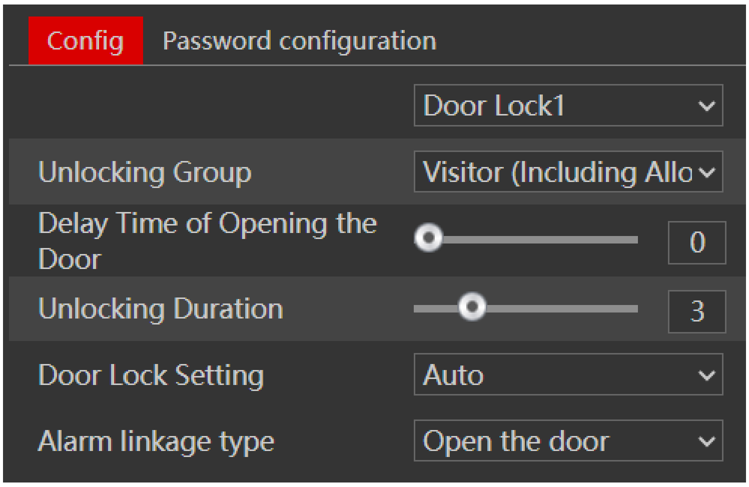
Door Contact Input type	Choose between NO (Normally Opened) and NC (Normally Closed)
Delay Time of Opening the Door	Specifies the allowable time for the door to remain open. For example, if set to 10 seconds, an alarm will be triggered if the door is not closed within 10 seconds.
Alarm Delay Time	Defines the delay before triggering an alarm when door contact faults are detected. For instance, if set to 3 seconds, an alarm will be triggered 3 seconds after detecting a door contact failure. The value can range from 0 to 999 seconds. If set to "0," the alarm will trigger immediately.
Trigger Alarm Out	Trigger the selectedalarm out relay
Trigger Audio Alarm	Trigger audible alarm
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

6.7.4) Door Lock

Here you can set the door lock features and configurations, together with password configurations for opening the door.

6.7.4.1) Config

Here you can set the door lock features and configurations



Door Lock1

Unlocking Group: Visitor (Including Allo

Delay Time of Opening the Door: 0

Unlocking Duration: 3

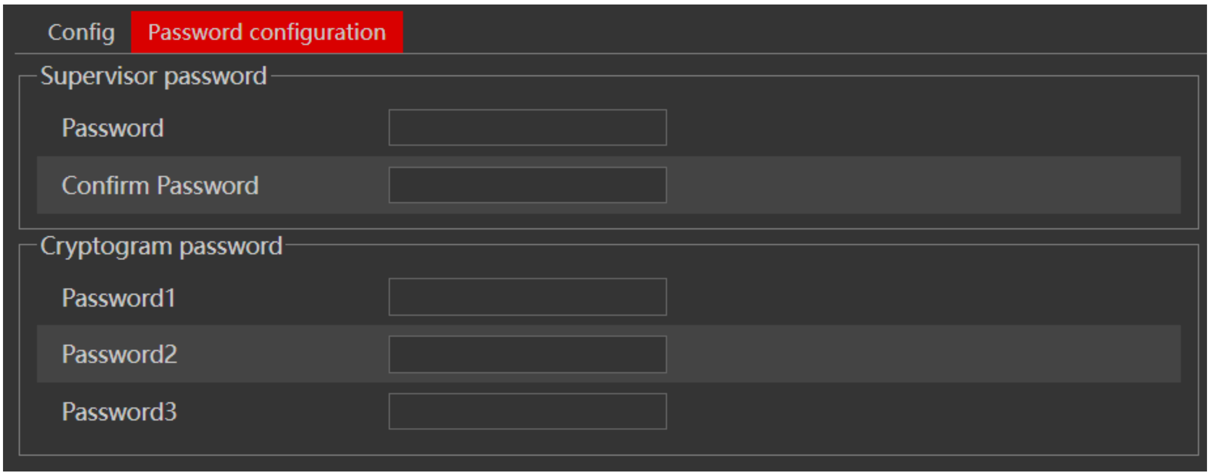
Door Lock Setting: Auto

Alarm linkage type: Open the door

Alarm Triggers:	**Explanation:**
Unlocking Group	Specifies the group that will unlock the door automatically upon successful face detection / recognition. The options are: Allow List, Visitor (including Allow List), and Unrecognized (which includes both Visitors and the Allow List)
Delay Time of Opening the Door	Sets the delay time before the door unlocks. The range is from 0 to 10 seconds. For example, if the unlocking mode is set to “Swiping Card” and the delay time is set to 2 seconds, the door will unlock 2 seconds after successfully reading the card.
Unlocking Duration	Defines the maximum time the door remains unlocked before it automatically locks again. The range is from 1to 10 seconds. For instance, if the duration is set to 3 seconds, the door will automatically lock 3 seconds after unlocking.
Door Lock Setting	Select between **“Auto”**, **“NO”** (Normally Open), or **“NC”** (Normally Closed) as needed. If “Auto” is selected, the system will open the door based on pre-defined unlocking conditions.
Alarm Linkage Type	Specifies whether the door should open or close when an alarm is triggered. Choose the appropriate setting based on your requirements.

6.7.4.2) Password Configuration

Password configurations for opening the door.



Supervisor password

Password

Confirm Password

Cryptogram password

Password1

Password2

Password3

The Supervisor password is a PIN that opens the door in any state or condition. It must be made from 4 digits
You can also set 3 wide range passwords that can be used by any user when the door opening mode contains password. It can contain 6-15 digits.

6.7.5) Wiegand Config

Wiegand is a communication protocol commonly used in access control systems for transmitting data between devices like card readers and controllers. It is widely recognized for its simplicity and reliability in short-distance data transfer.

Wiegand Config:
You can select Wiegand Input, Wiegand Output, or Off based on the setup:
Select Wiegand Input if a card reader is connected to the Wiegand interface.
Select Wiegand Output if an access controller is connected to the Wiegand interface.

Wiegand Mode:
You can choose from the following bit configurations: 26-bit (8 digits), 26-bit (10 digits), 34-bit, 37-bit, 42-bit, 46-bit, 58-bit, or 66-bit.

6.7.6) Card Reader

The card reader configuration refers to the integral RFID reader of the intercom
You can select which RFID protocol will be used. If both are disabled, RFID will not be available.
If "IC Card" is enabled, you can configure the following encryption options as needed:

IC Card Anti-Cloning: Prevents unauthorized duplication of IC cards.
MI Card Encryption: Encrypts MIFARE cards for enhanced security.
CPU Card Encryption: Provides encryption for cards with a built-in microprocessor.

DESFire Card Encryption: Secures DESFire cards using advanced encryption standards.

Please note:

- ❖ A professional card enroller is required to encrypt the cards. If you wish to use the card encryption feature, you must purchase a card enroller and complete the necessary setup in advance

6.8) Intercom

Configure from here the intercom communication and dialing platforms.

6.8.1) Building + Master/Slave Configuration:

Since the intercom and monitor are communicating in SIP protocol, there can be only 1 main door(Master) unit, and up to 8 sub-door (slave) unit.
If the intercom is the Master, choose "Main Door Station"
If the intercom is a slave, choose "Sub Door Station" and input the IP of the Master unit in the "Main Door Station IP".

The other information is optional, but advised not to be altered to prevent malfunctions.

6.8.2) Call Button Config:

The intercom has a "Quick Call" button. This button can perform 3 actions:

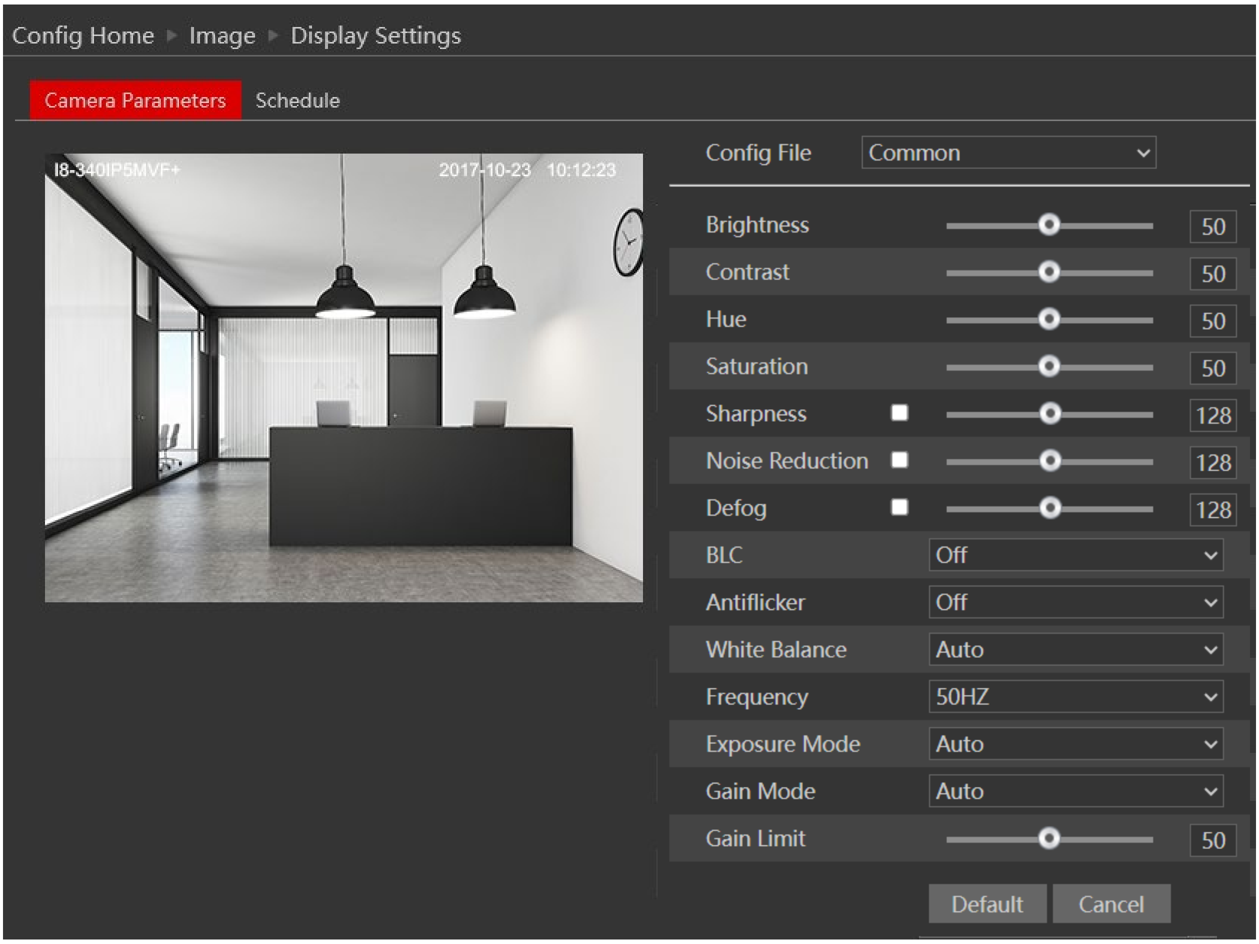
- Call Ossia VMS (The intercom must be added to it directly)
- Call Provision Cam2 Mobile App (Must be bound to it)
- Call an in door monitor. You should set the indoor monitor number you wish to call to when pressing the quick call button. (Must be configured on the monitor as well).

6.9) Image Configuration

Image Configuration includes five submenus: Display Settings, Video/Audio Stream, OSD Config, Video Mask, and ROI Config.

6.9.1) Camera Settings

Setting steps:
Go to "Image" → "Display" interface as shown below.



Config Home ▸ Image ▸ Display Settings

Config File: Common

Brightness: 50

Contrast: 50

Hue: 50

Saturation: 50

Sharpness: □ 128

Noise Reduction: □ 128

Defog: □ 128

BLC: Off

Antiflicker: Off

White Balance: Auto

Frequency: 50HZ

Exposure Mode: Auto

Gain Mode: Auto

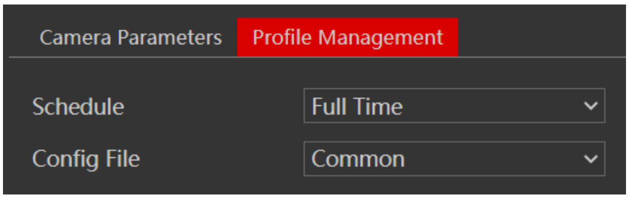
Gain Limit: 50

The display parameters are as follows:

Parameter	**Meaning**
Config file*	You can set an individual configuration for Day and night. Common is used for both
Brightness	Set the image brightness
Contrast	Set the image contrast
Hue	Set the image hue
Saturation	Set the image saturation
Sharpness	Enable/Disable the sharpness and set its level
Noise reduction	Enable/Disable the 3D-DNR and set its level
Defog	Enable/Disable the defog and set its level
BLC	Set HLC/BLC/True-WDR to deal with advanced light conditions.
Level	The Level of the HWDR/BLC/HLC
Antiflicker	Changes the camera refresh rate to reduce flickers
White Balance	Set the white balance of the camera
Gain Mode	Set gain to Auto/Manual
Gain Limit	Set the Gain limit

Frequency	Set the frequency to 50/60Hz

*If you set the day/night mode to schedule or you wish to differentiate between the daytime and night-time image settings, you will need to set the profiles accordingly. Click on the “Profile Management” tab and set the schedule as you wish.

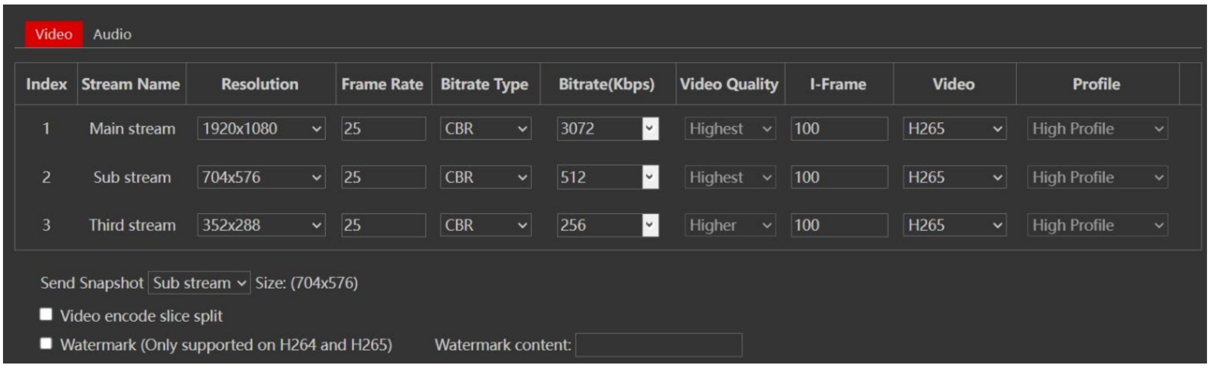


Schedule: Full Time

Config File: Common

6.9.2) Video/Audio

Go to “Video configuration” → “Video/Audio” to see an interface as shown below.



Index	Stream Name	Resolution	Frame Rate	Bitrate Type	Bitrate(Kbps)	Video Quality	I-Frame	Video	Profile
1	Main stream	1920x1080	25	CBR	3072	Highest	100	H265	High Profile
2	Sub stream	704x576	25	CBR	512	Highest	100	H265	High Profile
3	Third stream	352x288	25	CBR	256	Higher	100	H265	High Profile

Send Snapshot Sub stream Size: (704x576)

□ Video encode slice split

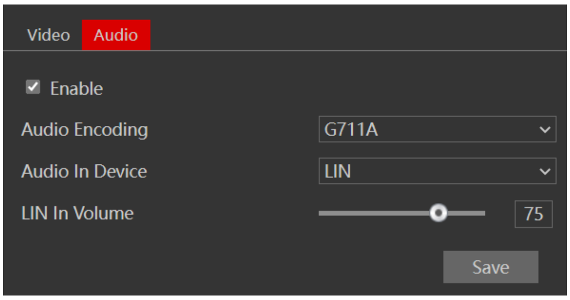
□ Watermark (Only supported on H264 and H265) Watermark content:

Three video streams are available. You can set each one of them differently with the limitations of the camera’s capabilities.

Parameter	Meaning
Resolution	The higher the resolution is, the bigger the image is.
Frame rate	The higher the frame rate is, the more fluent the video is. However, more storage room will be taken up.
Bitrate type	CBR (Constant Bit-Rate) means that the video compression bitrate will be constant as configured. This will not only facilitate the image quality better in a constant bitrate but also help to calculate the capacity of the recording. VBR (Variable Bit-Rate) means that the compression bitrate can be automatically adjusted according to the change of the video resources with the configured bit-rate as the maximum value. This will help to optimize the storage network bandwidth.
Video Quality	When VBR is selected, you need to choose image quality. The higher the image quality you choose, the more bitrate will be required.
Bitrate	Please set it according to your needs while taking into consideration the bandwidth and storage limits.
I Frame interval	It is recommended to use the default value. If the value is too high, the read speed picture group will be slow resulting in video quality loss.

Video Compression	Choose between H.265 and H.264. The IPC also supports MJPEG on sub-stream resolution but you need to make sure that the application connected to the camera also supports it.
Profile	Baseline, main profile, and high profile are optional. A baseline profile is mainly used in interactive applications with low complexity and delay. The main or high profile is mainly used for higher coding requirements.
Send Snapshot	Please select it according to the actual situation.
Video encode slice split	If enabled, you may get a more fluent image even when using a low-performance PC.
Watermark	You can set a watermark that will appear on the image.

In the next tab, we have "Audio" settings as shown below:



☑ Enable

Audio Encoding: G711A

Audio In Device: LIN

LIN In Volume: 75

The audio input / built-in microphone is disabled by default. Enable it if you need audio input from the camera.

Set the encoding profile as desired and the type of audio input. If LIN (Line) is selected, it means that the audio input is already amplified and the input volume will be set to "low". If MIC (Microphone) will be selected, it means that the audio signal is not amplified and the input volume will be set to "high".

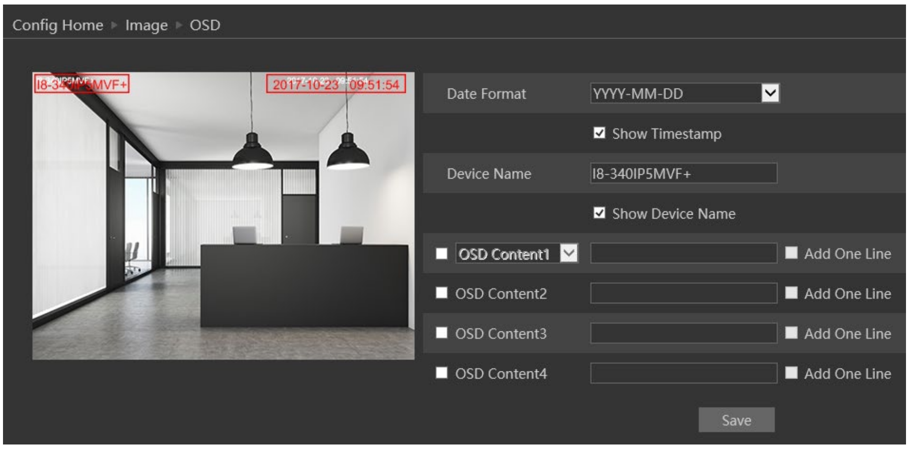
Please note:

- Since audio is required for the intercom to operate normally, it is enabled by default. Disabling the audio will cause the intercom to malfunction.

6.9.3) OSD Configuration

Go to "Image" → "OSD" menu to display the interface as shown below.

You may set the device name, timestamp, and custom OSDs here. Drag the time stamp and custom OSD over the image on the left side to set their position. Then press the “Save” button to save the settings.



Config Home ▸ Image ▸ OSD

Date Format: YYYY-MM-DD

☑ Show Timestamp

Device Name: I8-340IP5MVF+

☑ Show Device Name

□ OSD Content1 □ Add One Line

□ OSD Content2 □ Add One Line

□ OSD Content3 □ Add One Line

□ OSD Content4 □ Add One Line

Save

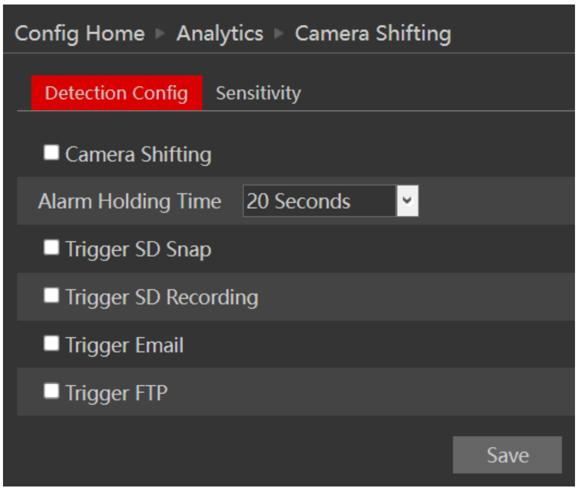
6.10) Alarm Configuration

Alarm configuration includes four submenus: General Fault, and Alarm Server.

6.10.1) Camera Tampering

Camera tapering uses a special analytics algorithm to detect if the camera was tampered with. This analytics detects if the camera was shifted from its original location, covered or that the lens was tampered with.

1. Go to “Alarm”→ “Camera Tampering” to get to the interface as shown below:



Config Home ▸ Analytics ▸ Camera Shifting

Detection Config | Sensitivity

□ Camera Shifting

Alarm Holding Time: 20 Seconds

□ Trigger SD Snap

□ Trigger SD Recording

□ Trigger Email

□ Trigger FTP

Save

2. Enable the required detection analytics out of Camera Shifting/Lens Tampering/Masking detection.
3. Set the Alarm response as follows:

Alarm Triggers:	Explanation:

Trigger Alarm Out	Trigger the selectedalarm out relay
Trigger Audio Alarm	Trigger audible alarm
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

4. Click “Save” to confirm.
5. Go to the sensitivity tab
6. Set the sensitivity (0 – lowest, 100 – Highest)
7. Click “Save” to confirm.

6.10.2) General Fault

A problem with the network cable or with the SD card will produce a general fault. The alarms can be configured as follows: SD Card Full, SD Card Error, IP Address Conflict, Network cable disconnected.
Enter “Alarm Configuration”→ “General Faults”.
The default tab is “SD Card Full”:
Enable the alarm if required. This alarm will only be relevant if the “Recycle Record” is not marked. If the “recycle record” is active, the SD card will not trigger an event once the card is filled.
After enabling the alarm, choose the responses required from the camera in case the alarm will be active. After the setting is complete, click “Save”.
Next is the “SD Card Error” Tab. This alarm will be triggered if any fault will be developed with the SD card. It can be a malfunction or removing the SD card from the camera.

To activate it, enable the alarm.
After enabling the alarm, choose the responses required from the camera in case the alarm will be active. After the setting is complete, click “Save”.

6.10.3) Alarm In

Alarm input is a pysical connection or alarm (sensor) to the camera. Here you can set the sensor properties such as type (NO/NC), Holding time, name and triggers as well as active schedule.

1. Choose the alarm input you wish to set
2. Enable/Disable it
3. Set the Alarm type (NO/NC)
4. Set the holding time (No reoccuring events will happen during the holding time)
5. Set the sensor name (Optional)
6. Set the triggers as follows:

Alarm Triggers:	**Explanation:**
Trigger Alarm Out	Trigger the selectedalarm out relay
Trigger Door Lock	Open the selected door lock in response
Trigger Audio Alarm	Trigger audible alarm
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

7. Apply settings.
8. You can apply the setting to the other sensor by using “Apply settings to” button, or repeat steps 1-7

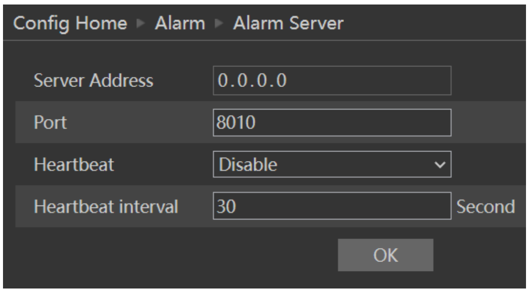
6.10.4) Alarm Out

Alarm output is a relay activation from the camera cable. The alarm output has 4 work methods:

1. Alarm Linkage: Trigger of the alarm output as a trigger to another event
2. Manual: Manual activation/deactivation of the output
3. Switch Day/Night Mode: Different activations for day and night modes
4. Timing: Activating the relay by schedule

6.10.5) Alarm Server

Alarm server is used mainly for system integrations. Once enabled, the camera will send all events to a dedicated listening server. These events will be sent in an XML format that needs to be parsed by the server. If required, a heartbeat can be set to confirm that the server that the camera is working and has network connectivity to it.

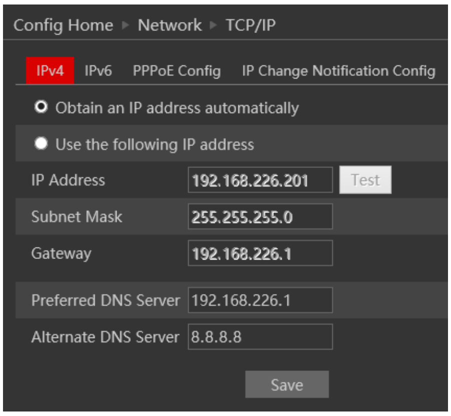

Config Home ▸ Alarm ▸ Alarm Server

Server Address: 0.0.0.0
Port: 8010
Heartbeat: Disable
Heartbeat interval: 30 Second

6.11) Network

6.11.1) TCP/IP

Go to “Network”→ “TCP IP” tab to see the interface shown below. The first and default tab is IPv4 Protocol. There are two options for IP setup: obtain an IP address automatically by DHCP or a defined IP address. You may choose one of the options as required.



Config Home ▸ Network ▸ TCP/IP

IPv4 | IPv6 | PPPoE Config | IP Change Notification Config

◉ Obtain an IP address automatically

● Use the following IP address

IP Address: 192.168.226.201 [Test]

Subnet Mask: 255.255.255.0

Gateway: 192.168.226.1

Preferred DNS Server: 192.168.226.1

Alternate DNS Server: 8.8.8.8

DHCP (Automatic IP Assignment): Use “Obtain an IP address automatically” for the camera to communicate with an available DHCP server that will assign the camera with an IP address automatically.

Please note:

- For the DHCP mode to work, you must have a DHCP server on your network.
- Using DHCP for permanent installations is not advisable as the IP Address might change after a while and cause the camera to be unreachable.

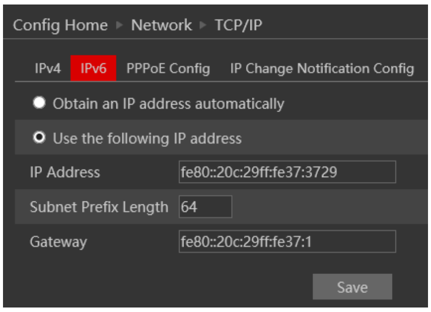
Manual IP Assignment: If you wish to set static IP addresses, choose “Use the following IP Address”, set the range of IP addresses you wish to assign (First and last address), set the gateway and subnet mask, and click on batch set. Wait for a few moments until the IP manager will configure the cameras. After configuration, the IP addresses of the cameras will refresh automatically.

Please note:

- The selected IP address must be available

The next tab is IPv6:

If you need to use IPv6, configure it in the same method as described for IPv4.



Config Home ▸ Network ▸ TCP/IP

IPv4 | IPv6 | PPPoE Config | IP Change Notification Config

● Obtain an IP address automatically

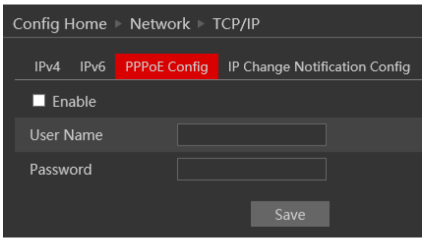
◉ Use the following IP address

IP Address: fe80::20c:29ff:fe37:3729

Subnet Prefix Length: 64

Gateway: fe80::20c:29ff:fe37:1

The next tab is PPPoE:


Config Home ▸ Network ▸ TCP/IP

IPv4 IPv6 PPPoE Config IP Change Notification Config

□ Enable

User Name

Password

For PPPoE, the user is required to manually input the username and password for dial-up internet. After saving the username/password information set up an IP address change notification. Last, connect with Modem and the device will dial-up internet automatically.

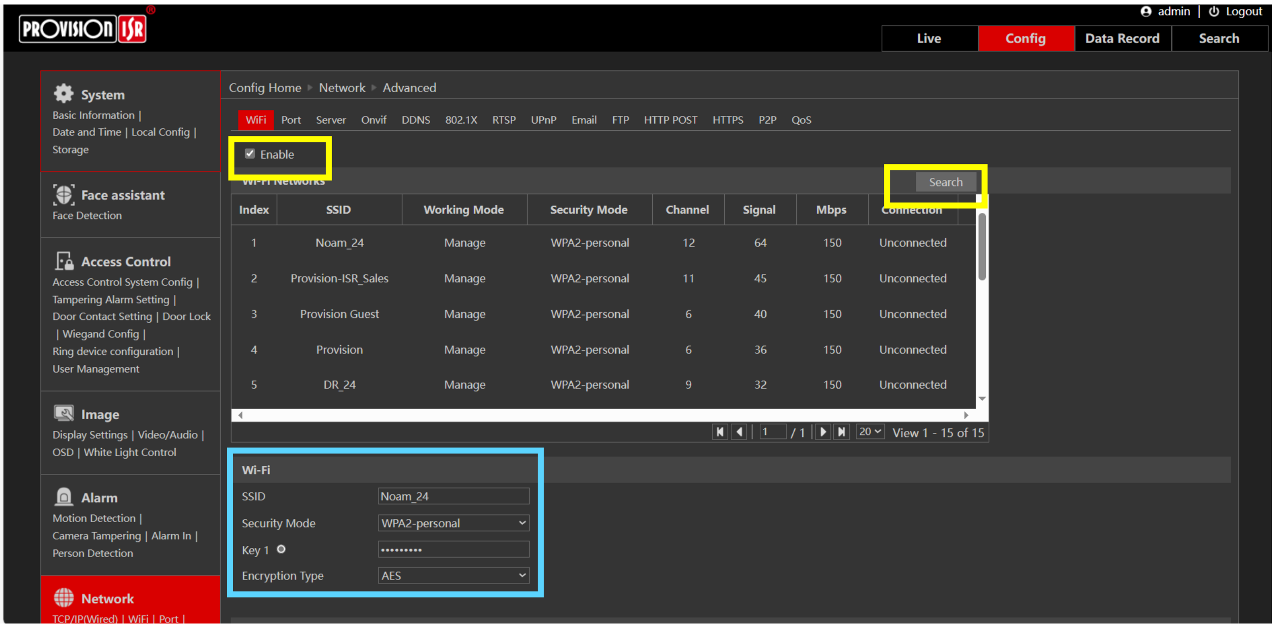
Press the “Save” button to save the settings.

The next tab is “IP Change Notification Config”: If you have used DHCP and you need to be notified that the IP Address assigned to the camera was changed, enable it and set Email or FTP for the notification process.

6.11.2) WiFi Configuration

After the DB is up and running, you can go to the WiFi settings of the DB:

1. Go to Network > WiFi
2. Enable WiFi, and press “search”
3. Choose your WiFi network, and provide the proper password below.



PROVISION ISR
admin | Logout
Live
Config
Data Record
Search
System
Basic Information | Date and Time | Local Config | Storage
Face assistant
Face Detection
Access Control
Access Control System Config | Tampering Alarm Setting | Door Contact Setting | Door Lock | Wiegand Config | Ring device configuration | User Management
Image
Display Settings | Video/Audio | OSD | White Light Control
Alarm
Motion Detection | Camera Tampering | Alarm In | Person Detection
Network
TCP/IP(Wired) | WiFi | Port |
Config Home ▸ Network ▸ Advanced
WiFi Port Server Onvif DDNS 802.1X RTSP UPnP Email FTP HTTP POST HTTPS P2P QoS
Search

☑ Enable

Wi-Fi Networks

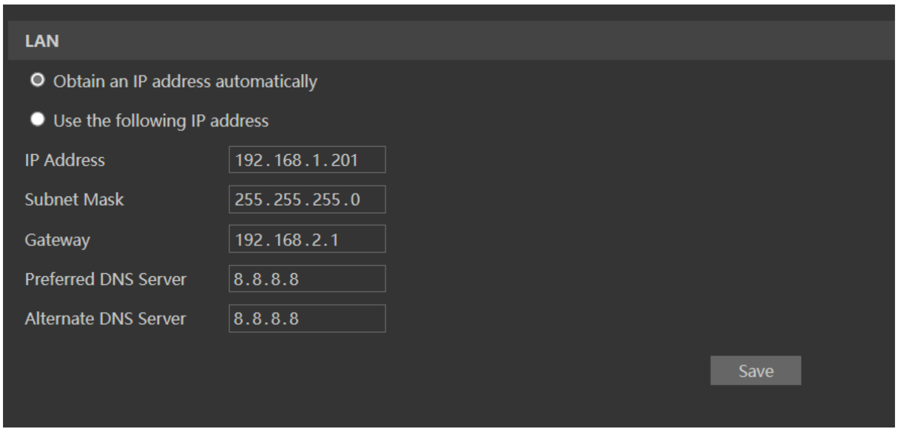
Index	SSID	Working Mode	Security Mode	Channel	Signal	Mbps	Connection
1	Noam_24	Manage	WPA2-personal	12	64	150	Unconnected
2	Provision-ISR_Sales	Manage	WPA2-personal	11	45	150	Unconnected
3	Provision Guest	Manage	WPA2-personal	6	40	150	Unconnected
4	Provision	Manage	WPA2-personal	6	36	150	Unconnected
5	DR_24	Manage	WPA2-personal	9	32	150	Unconnected

1 / 1 20 View 1 - 15 of 15

Wi-Fi

SSID	Noam_24
Security Mode	WPA2-personal
Key 1	•••••••••
Encryption Type	AES

4. Set the WiFi IP configuration below (Default is DHCP)



LAN

● Obtain an IP address automatically

○ Use the following IP address

IP Address	192.168.1.201
Subnet Mask	255.255.255.0
Gateway	192.168.2.1
Preferred DNS Server	8.8.8.8
Alternate DNS Server	8.8.8.8

5. Press “Save”
6. Once complete, the device will connect.

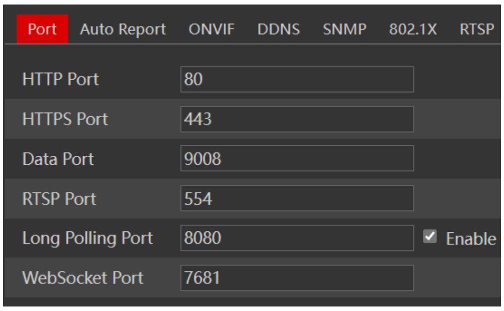
Please note:

❖ WIFI will be used **ONLY** after the Ethernet cable has been disconnected.

6.11.3) Port

Go to “Network”→ “Port” to see the following interface:

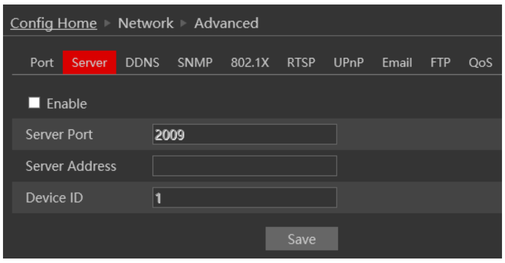
1. HTTP Port (Default is 80) is for HTTP and API
2. Data Port (Default is 9008) is for IE video data and SDK
3. RTSP Port (Default is 554) is for RTSP video streaming
4. Long Polling Port (Default is 8080) is for advanced integrations using long polling API.
5. WebSocket Port (Default is 9681) is for modern browser video streaming



HTTP Port	80	
HTTPS Port	443	
Data Port	9008	
RTSP Port	554	
Long Polling Port	8080	☑ Enable
WebSocket Port	7681	

6.11.4) Auto Report

This section refers to “Auto Report Server”. Enable it if required.
Auto report server will make the camera report back to the defined server using port 2009.



☐ Enable

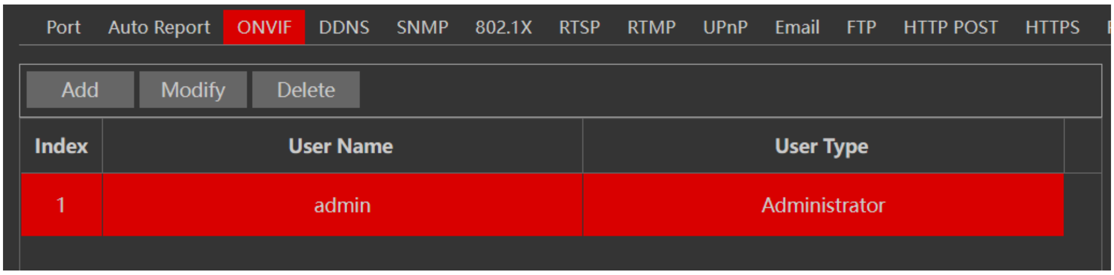
Server Port	2009
Server Address	
Device ID	1

Go to “Network”→ “Auto Report”.
Set the port (default port is 2009. It is advisable not to change it.) Set the server address (usually it is the CMS address which needs to be a static address). Set a unique device ID. Each of the devices using auto server report should have its unique ID.
The Camera will report back to the defined server its current IP using port 2009.

6.11.5) ONVIF

This is the ONVIF management interface. From here you can enable/disable ONVIF and also manage ONVIF users that can be differentiated from the standard IPC users.

Go to “Network”→ “ONVIF” to see the following interface:



Index	User Name	User Type
1	admin	Administrator

If there are no available users, it means that ONVIF is disabled. To enable it, click on “Add”. Set the username, password, and user type for the required user and click OK.

6.11.6) DDNS

DDNS should be used when your ISP (Internet Service Provider) provides you with a dynamic valid IP. The DDNS will update your dynamic address and link it to a fixed domain.
Enter into the "Network"→"DDNS" tab and set the DDNS as required.

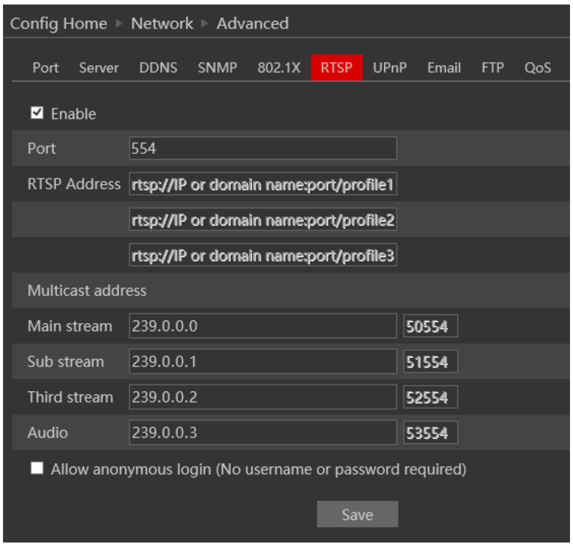
6.11.7) 802.1X

The 802.1X standard is designed to enhance the security of wireless and local area networks (WLANs) that follow the IEEE 802.11 standard. 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority.

6.11.8) RTSP

RTSP is used to stream video/audio using the shared protocol. v4.2 is also supporting RTSP using Multicast protocol.

Go to “Network”→ “RTSP” interface as shown below.


Config Home ▸ Network ▸ Advanced
Port Server DDNS SNMP 802.1X RTSP UPnP Email FTP QoS
Save

☑ Enable

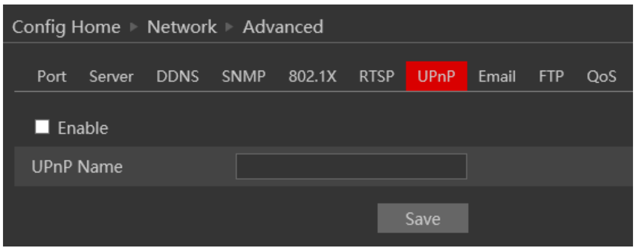
Port	554	
RTSP Address	rtsp://IP or domain name:port/profile1	
	rtsp://IP or domain name:port/profile2	
	rtsp://IP or domain name:port/profile3	
Multicast address		
Main stream	239.0.0.0	50554
Sub stream	239.0.0.1	51554
Third stream	239.0.0.2	52554
Audio	239.0.0.3	53554

□ Allow anonymous login (No username or password required)

- Enable the RTSP if required.
- RTSP Port: Access Port of the streaming media. The default port is 554.
- RTSP Address: each of the streams has a unique RTSP address. Input the desired address into your RTSP player.
- Notice that the camera also supports multicast addresses that can be used as well for supporting players.
- Enabling “Allow anonymous login” will authorize RTSP connection without the need for a username/password.
- Click “Save” to confirm and save settings.

6.11.9) UPnP

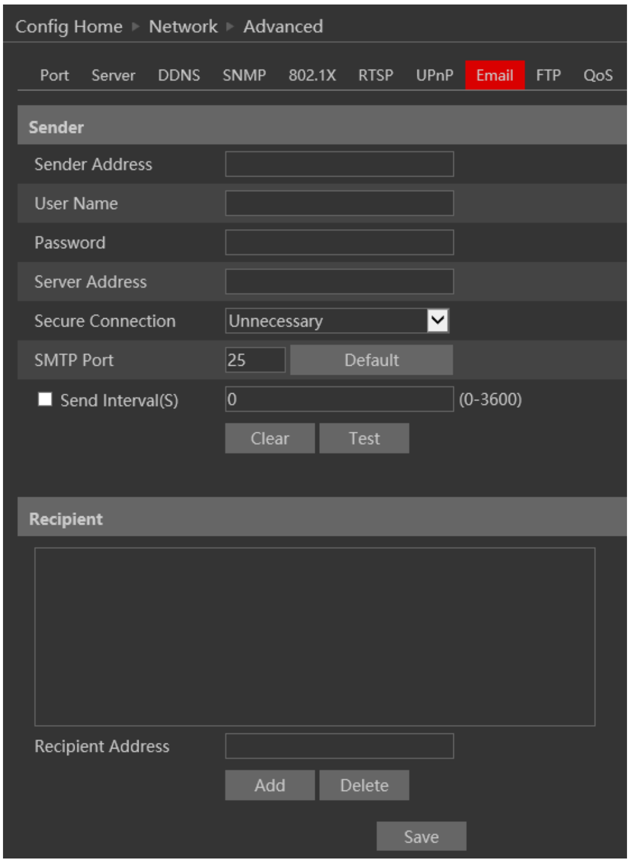
Go to “Network”→ “UPnP” interface as shown below.
Select “Enable UPnP” and then input a friendly name.


Config Home ▸ Network ▸ Advanced
Port Server DDNS SNMP 802.1X RTSP UPnP Email FTP QoS
□ Enable
UPnP Name
Save

Then double-click the “Network” icon on the desktop of the PC to see an icon with the name and IP address of the camera. You may quickly access the device by double-clicking this icon.

6.11.10) Email

Go to “Network” → “Email” interface.


Config Home ▸ Network ▸ Advanced
Port Server DDNS SNMP 802.1X RTSP UPnP Email FTP QoS
Sender
Sender Address
User Name
Password
Server Address
Secure Connection Unnecessary
SMTP Port 25 Default
□ Send Interval(S) 0 (0-3600)
Clear Test
Recipient
Recipient Address
Add Delete
Save

The input fields are as follows:

Field	Meaning
Sender Address	Sender’s e-mail address
User Name	The username of the Email account
Password	The password for the Email account
Server Address	The SMTP/Outgoing Email server address
Secure Connection	Choose between Unnecessary/SSL/TLS

SMTP Port	The SMTP port. The default port will be used according to the secure connection choice but can be edited manually if required.
Send Intervals	The minimum time duration between 2 Emails that will be sent by the system,
Recipient Address	The email addresses that Emails generated by the system will be sent to.

After all the parameters are properly set up, you can click “Test” to confirm that the system can connect to the email server with the provided details. If an email is sent successfully, a “Test Successful” window will pop up, if not, you should try other email addresses or check and correct the settings.

To input a new mail recipient, input the recipient address and click on “Add”. The new address will be added to the recipient list box.

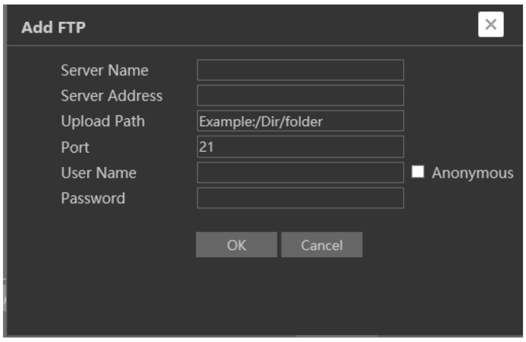
Please note:

- ❖ If you change the static IP into PPPoE and select mailbox, there will be an e-mail sent to your mailbox for notifying a new IP address

6.11.11) FTP

Go to “Network” →”FTP” interface.
To add a new FTP server click on “Add” and input the FTP server’s server name, address, port number, username, password, and upload path, click OK to confirm the setting.

Click on “Modify” to edit the information on the FTP server
Click on “Delete” to delete the FTP server
Click on “Test” to confirm the setting and availability of the FTP server.

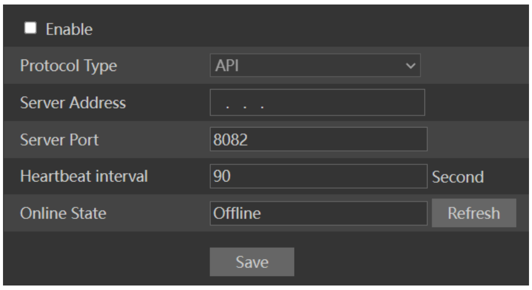


Add FTP

Server Name:
Server Address:
Upload Path: Example:/Dir/folder
Port: 21
User Name: □ Anonymous
Password:

6.11.12) HTTP POST

HTTP POST is used mainly for system integrations. Once enabled, the camera will send **AI events only** to a dedicated listening server. These events will be sent in a detailed XML format that needs to be parsed by the server.
If required, a heartbeat can be set to confirm that the server that the camera is working and has network connectivity to it.

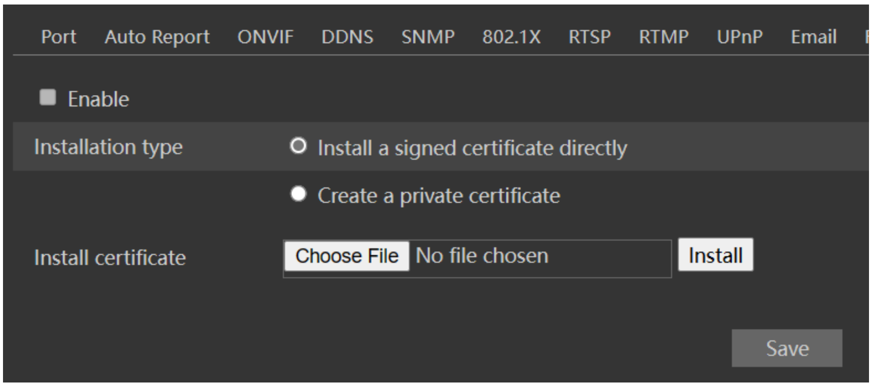


□ Enable
Protocol Type: API
Server Address: . . .
Server Port: 8082
Heartbeat interval: 90 Second
Online State: Offline

6.11.13) HTTPS

HTTPS (Secured HTTP) is used to establish a secured and encrypted connection between the camera and the client (IE in our case). This will prevent anyone on the network to be able to get information packets and other information by sniffing the network.
The HTTPS must have an SSL certificate to work properly. An authentic certificate must be created by an authorized SSL certificate provider. This will confirm its security and validity. (The internet browser will authenticate the certificate when connecting to the camera).

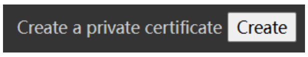
This is a brief explanation of the SSL certificate and HTTPS connection.
Go to "Network" →"HTTPS". interface as shown below. Enable HTTPS if required. (Enabling HTTPS completely disables HTTP connection).



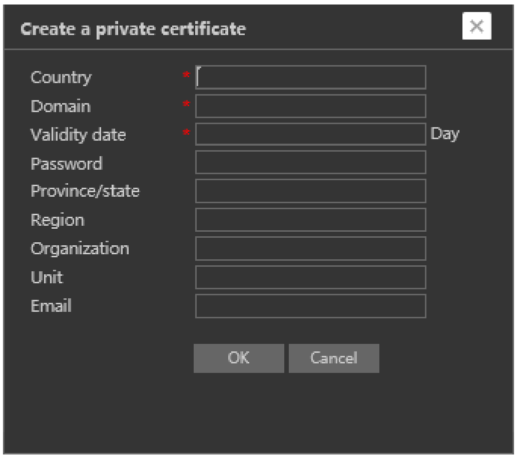
□ Enable

Installation type ○ Install a signed certificate directly
● Create a private certificate

Install certificate: No file chosen

If you already have an SSL certificate in hand, choose "Install a signed certificate directly". Click on "Browse" and choose your certificate. Click on "Install", wait for the procedure to complete, and click on "Save"
If you wish to use a basic HTTPS connection, click on "Create a private certificate". The interface will update to:  .

Click on "Create". The interface below will appear.

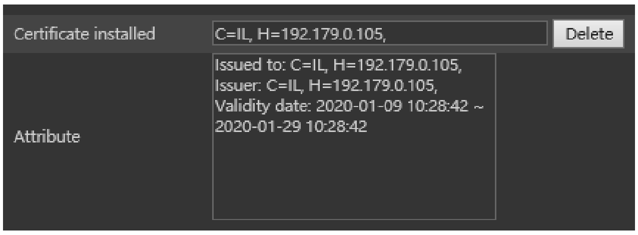


Create a private certificate

Country *
Domain *
Validity date * Day
Password
Province/state
Region
Organization
Unit
Email

Input the details (The country field is set by 2 capital letters. For example for Israel the user should input "IL"). The fields marked with * are mandatory. All the rest are optional.

Click on “OK”. Once the procedure is finished, the SSL certificate will be automatically installed as follows.



Certificate installed: C=IL, H=192.179.0.105,

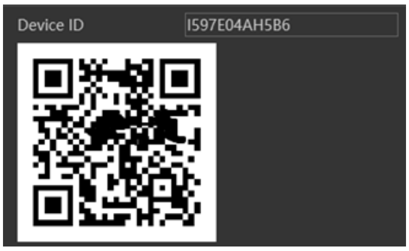
Attribute: Issued to: C=IL, H=192.179.0.105,
Issuer: C=IL, H=192.179.0.105,
Validity date: 2020-01-09 10:28:42 ~ 2020-01-29 10:28:42

Please note:

- ❖ Using this method will display an error message by the browser every time you connect to the camera, as the camera is not recognized as a certified SSL certificate issuer.

6.11.14) P2P

P2P is used to connect directly to the camera through an advanced NAT interface.
Go to “Network” →”P2P”.
Enable P2P if required.
Once enabled you can refer to “Settings”→”System”→”Basic Information”



Device ID: I597E04AH5B6

Scan the QR code using the “Provision Cam2” mobile APP or input the device ID manually in the P2P domain (https://www.provisionisr-cloud.com).

6.11.15) QoS

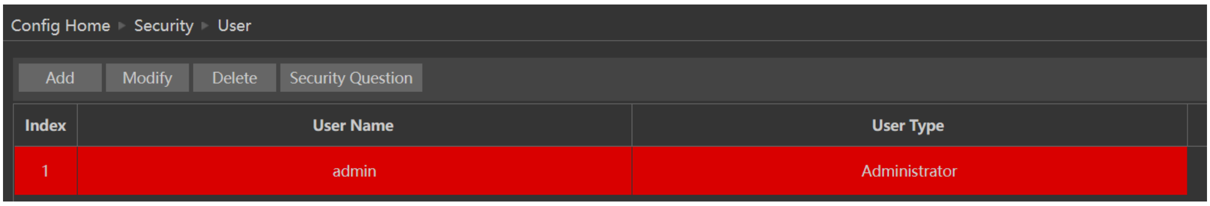
Quality of Service (QoS) is an advanced feature that prioritizes internet traffic for applications to minimize the impact of busy bandwidth. It must be supported by the switch/router being used.

6.12) Security

Security configuration includes three submenus: User Settings, Online Users, and Block & Allow lists.

6.12.1) User

Go to “Network” →“User” to access the following interface.



Index	User Name	User Type
1	admin	Administrator

Adding a user:

Click on the “Add” button to pop up the “Add user” dialog box.

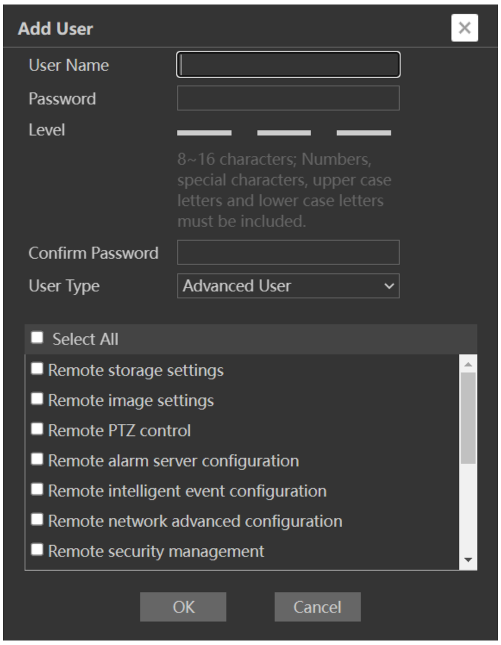
Input the username, and password and confirm the password.

Set the user type. 3 user types are available:

- Administrator – Can perform all actions and settings on the camera.
- Advanced user – Can view and configure the camera excluding the “User Access” section.
- Normal User – Can only view the live image and cannot configure.

At this stage, you can also bind a MAC address for the user. This means that this user will only be able to connect from a single pre-defined device and his access will be denied if he will try to connect from any other device.

Click on “OK” and “Save”



User Name
Password
Level
8~16 characters; Numbers, special characters, upper case letters and lower case letters must be included.
Confirm Password
User Type: Advanced User

□ Select All
□ Remote storage settings
□ Remote image settings
□ Remote PTZ control
□ Remote alarm server configuration
□ Remote intelligent event configuration
□ Remote network advanced configuration
□ Remote security management

Modify user:

Select the user you wish to modify and click on the “Modify” button. A modification window will pop up as shown above.

You can change the username if required. If you wish to edit the password of the user, tick “modify password” and input the old password, new password, and confirmation of the new password.

Click “OK” to save.

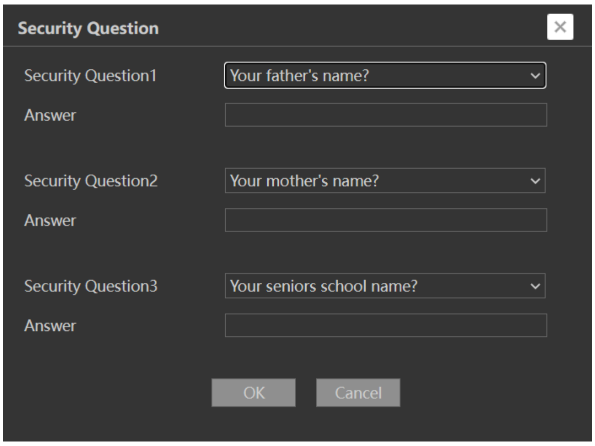
Delete user:

Select the user you wish to delete and click on the “Delete” button. A confirmation prompt will pop up. Click “Ok” to confirm.

Editing the Security Questions:

If you wish to set/edit the security questions used to recover your admin password, you can do so by clicking on “Security Question”. The following window will pop up:

Choose 3 questions from the drop-down list and set the correct answers. Note that when recovering a lost admin password, **all** questions should be answered correctly



Security Question

Security Question1: Your father's name?

Answer:

Security Question2: Your mother's name?

Answer:

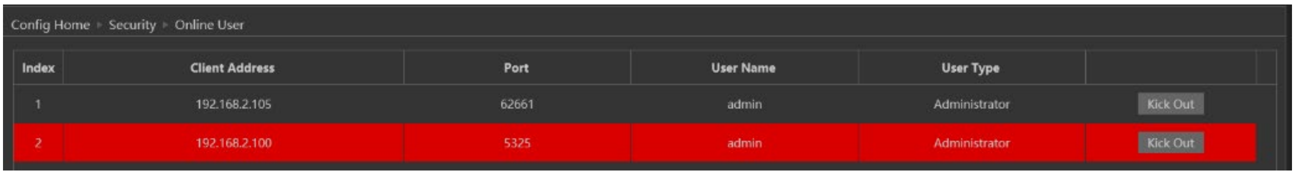
Security Question3: Your seniors school name?

Answer:

6.12.2) Online Users

The “Online users” section will allow you to view users who are currently connected to the camera. Administrator-level users can also kick out other users who are currently connected to the camera.

Go to “Network” →“Online Users” to access the following interface.



Config Home ▸ Security ▸ Online User

Index	Client Address	Port	User Name	User Type	
1	192.168.2.105	62661	admin	Administrator	Kick Out
2	192.168.2.100	5325	admin	Administrator	Kick Out

You can view the IP address, port, username, and user type used for the connection.

The “Kick Out” button will kick out the selected user and input his IP address to the blacklist.

Click on it for the relevant user and confirm the prompt message.

Please note:

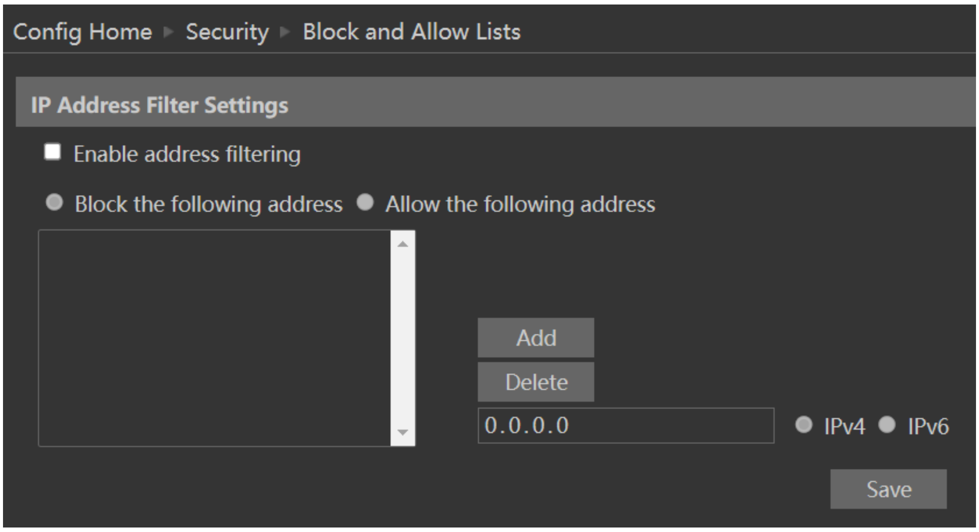
Once the user is kicked out, the IP address used for the connection will be blocklisted. Therefore, the device used for connection will not be able to connect to the camera until the IP address will be manually removed from the blacklist.

6.12.3) Block and Allow Lists

“Block and Allow” lists allow the user to create lists of IP/MAC addresses that will be allowed or denied for connection.

Once a “Block” list is created, all devices except the blocked devices will be allowed to connect to the camera.
Once an “Allow” list is created, all devices except the allowed devices will be blocked from connecting to the camera.

Go to “Network” →“Block and Allow Lists” to access the following interface.



Config Home ▸ Security ▸ Block and Allow Lists

IP Address Filter Settings

□ Enable address filtering

● Block the following address ● Allow the following address

0.0.0.0 ● IPv4 ● IPv6

The lists can be based on IPv4/IPv6.

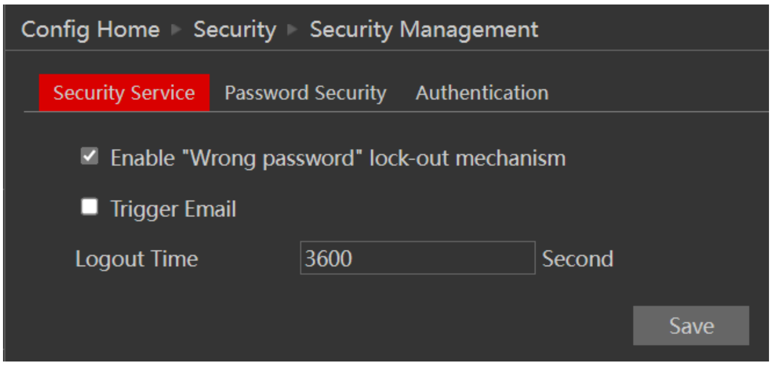
Enable the filtering you wish to activate.

1. Choose the type of list you wish to create (block or allow)
2. Set whether the input is IPv4/IPv6 address
3. Input the IP address you wish to add to the list
4. Click on add.
5. If you wish to add more than one address, repeat stages 1-4
6. Once finished, click “Save” to confirm, save the settings, and enable the lists.

6.12.4) Security Management

“Security Management” Allows the user to enhance the device security by adding protection layers and rules.

“Security Service” enables a mechanism that locks the IPC to an incoming connection after 5 wrong attempts. Releasing the camera from a locked state is done by waiting for the lock duration or hard rebooting the camera. This mechanism protects against a “Brute Force” attack.



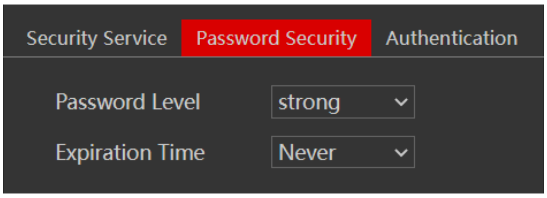
☑ Enable "Wrong password" lock-out mechanism

□ Trigger Email

Logout Time 3600 Second

Ticking the “Trigger Mail” will send a mail to the selected recipients notifying them that the camera entered a “lock” state due to multiple failed login attempts.

“Password security” allows the user to set the password required strength and password change policy.



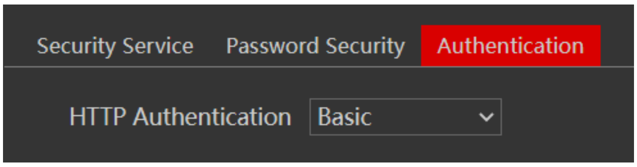
Password Level strong

Expiration Time Never

Password level divides into 3 levels:

- Low: No Requirements.
- Mid: Minimum of 8 characters. Contains at least one number and one character.
- High: Minimum of 8 characters. Contains at least one number, one character, and one special character.

Expiration time: After the set duration (30 Days, 60 Days, Half a Year, Year), the camera will demand a password change. The current password cannot be reused. Older passwords are not kept and can be used again.
“Authentication” is used for API HTTP login.



HTTP Authentication Basic

“Basic” is Base64 authentication, and “Token” is digest MD5 authentication.

6.13) Maintenance

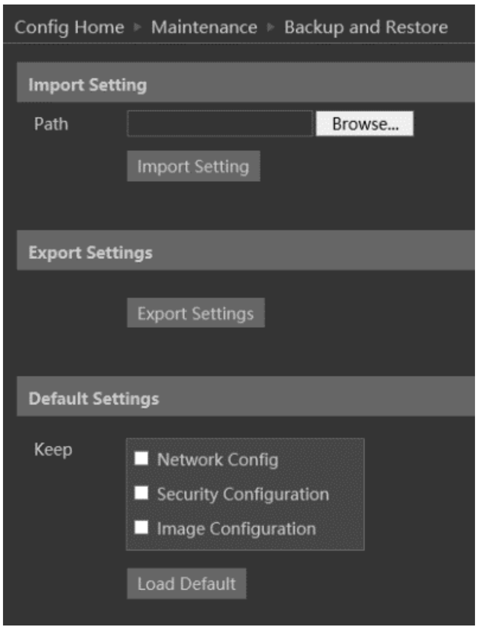
Maintenance includes 4 submenus: Backup & Restore, Reboot, Upgrade, and Operation log.

6.13.1) Backup & Restore

Backup and restore are used to save the camera's configuration on a PC and use it in case the camera's configuration was changed or when you wish to change the configuration of several cameras to be uniform. This section also allows you to restore the camera's setting to factory default with some exceptions.

Go to "Maintenance"→" Backup and Restore".

Importing Settings: If you have a configuration file and you wish to import it to the camera, click on "browse" and choose the relevant config file.
After choosing the file click on "Import settings" and wait for the process to finish.



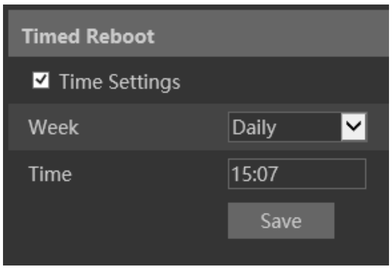
Exporting settings: If you wish to export the configuration settings of the camera click on "Export". Choose the location on your PC and set the file name. Click on "OK" to save the file in the desired location.

Loading factory default: If for any reason you wish to restore your camera settings to factory default, you can use the "Load Default" button. Notice that you can mark some configurations that will be saved:

- Network Config: Will save all the network section configuration
- Security Configuration: This will save all the security section configurations.
- Image configuration: Will save the image section configuration.

6.13.2) Reboot Device

Go to "Maintenance"→"Reboot".
To reboot the IPC, click on the reboot "Reboot" button and confirm the pop-up prompt message, then wait for the reboot process to finish.
You can also set a scheduled reboot. Tick the "Time Settings" and set the time period and time for the reboot. You can choose a day of the week when the reboot will automatically take place or you can set it to happen daily. The reboot will occur on the specified day and time.



☑ Time Settings
Week: Daily
Time: 15:07

6.13.3) Upgrade

Go to "Maintenance"→"Update".

1) Click the "Browse" button to select the upgrade file.
2) Click the "Upgrade" button to start the upgrading process of the IPC.

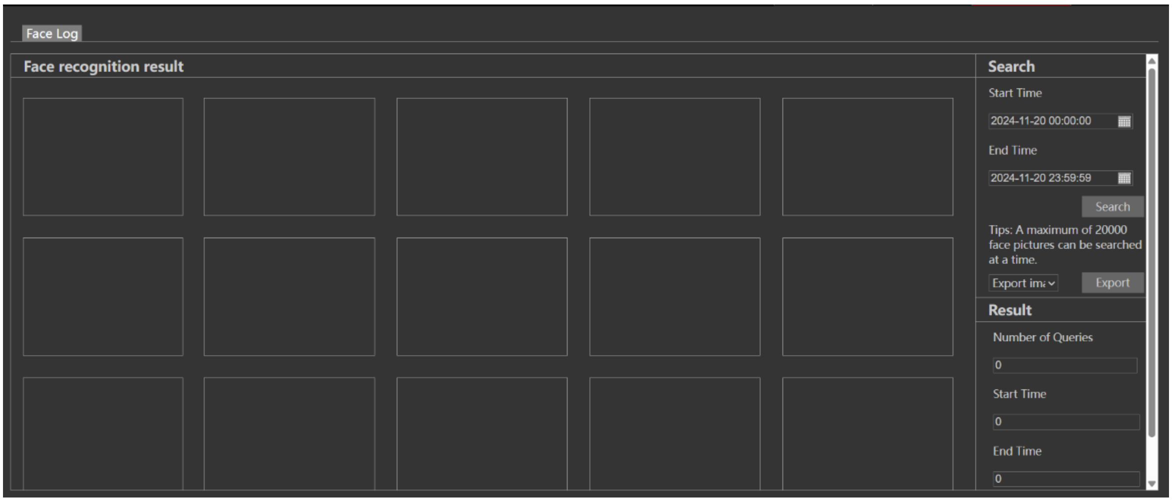
3) The device will restart automatically once completed.
4) Depending on the update release note, the IPC configuration might reset.

Please note:

- You must not disconnect to PC or close the IPC during the upgrade process to prevent permanent damage to the camera.
- The camera update file is ***.TAR. the “TAR” file should not be extracted.

7) Data Record

The data record is used to extract face detection/recognition events from the intercom, assuming that saving the face data is enabled and an SD card is available.



Start Time: 2024-11-20 00:00:00

End Time: 2024-11-20 23:59:59

Tips: A maximum of 20000 face pictures can be searched at a time.

Number of Queries: 0

Start Time: 0

End Time: 0

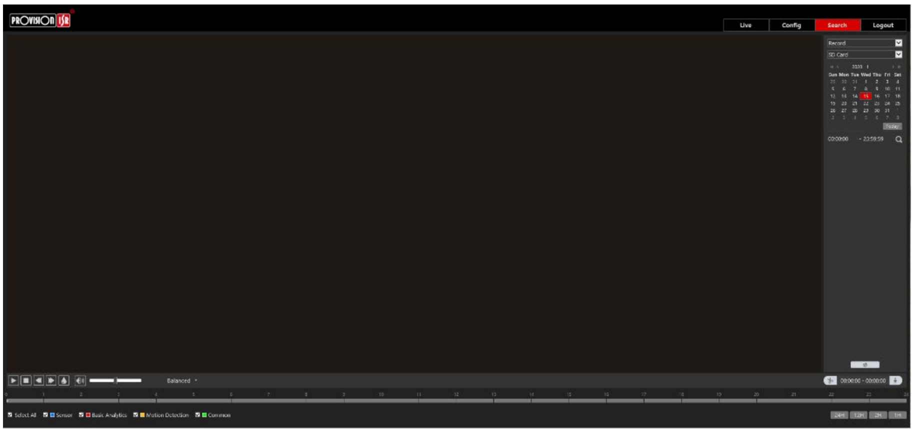
1. Set the time frame within you wish to search
2. Click “Search”
3. You can export the results if required by clicking on “Export”

8) Playback (Search)

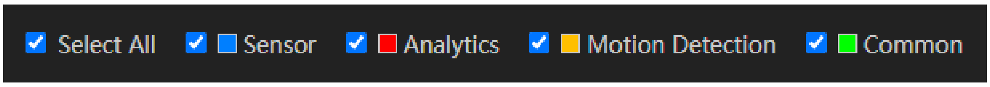
Playing back videos taken by the camera have 2 options:

1. Video files/Images saved locally on the PC (If any were taken)
2. Video files/Images saved on the Camera SD card (If available)

To access the playback interface, click on the "Search" Main tab. The interface below will appear.

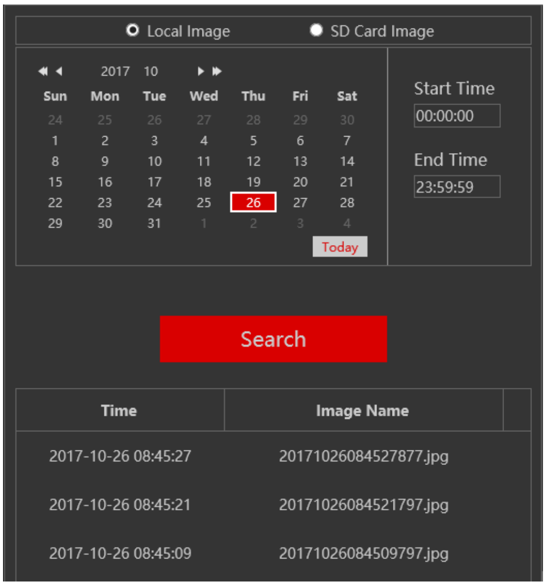


1. First, you will have to choose which type of media you wish to search for. On the left top corner choose from Photo and Video Photo Video
2. Choose the location of the stored media. You can either choose "Local" – which is your PC or you can choose "SD Card" which is the camera's internal SD Card.
3. If you chose the SD card as the search source you can also define the alarm trigger as follows:



☑ Select All ☑ 🟦 Sensor ☑ 🟥 Analytics ☑ 🟨 Motion Detection ☑ 🟩 Common

4. Set the search range. You can choose a single day and set a time range of up to 24 hours. (Full day). Once finished click on "Search" to show the results.



○ Local Image ● SD Card Image

◀◀ ◀ 2017 10 ▶ ▶▶

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Today

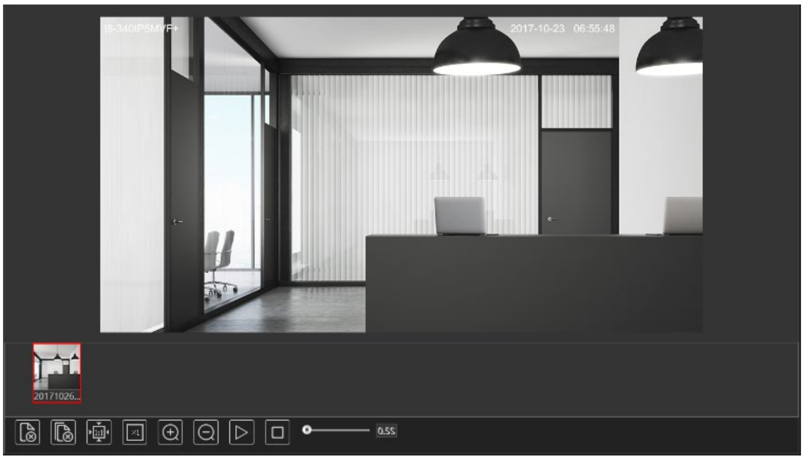
Start Time 00:00:00

End Time 23:59:59

Search

Time	Image Name
2017-10-26 08:45:27	20171026084527877.jpg
2017-10-26 08:45:21	20171026084521797.jpg
2017-10-26 08:45:09	20171026084509797.jpg

5. Double-click on the image/video from the list for it to show on the main playback window and to the playback queue.



6. The playback controls are described below. Notice that it is different for Videos and Photos

For Photos

Icon	Description	Icon	Description
⊗	Close the displayed image	⊕	Digital Zoom In
⊗	Close the displayed image and delete the queue list	⊖	Digital Zoom out
⤓	Download the displayed image to your PC (SD Card search only)	▷	Play a slideshow of the queued images
⤓	Download the displayed image and queue list to your PC (SD Card search only)	□	Stop the slideshow
1:1	Fit the image to the screen	─○── 2.5S	Dwell time between images
×1	Display the image in real-size		

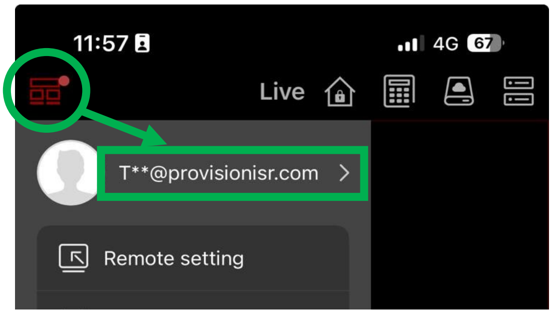
For Videos

Icon	Description	Icon	Description
▶	Play	▶|	Play next file
❚❚	Pause playback	▨	Enable/Disable Watermark
■	Stop Playback	⤓	Download the selected file (SD Card only)
◀◀	Reduce playback speed	🔊 ──■──	Enable/Disable Audio + Volume control
▶▶	Increase playback speed	⛶	Full-screen mode
|◀	Play the previous file	Balanced ▾	Buffering mode selection

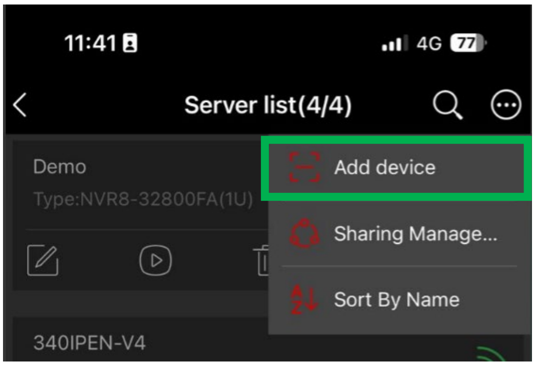
9) Binding with Provision Cam2 Mobile App.

In order to work properly, the Intercom must be bound to a user account using Provision Cam2 mobile app. In order to bind it, follow the next steps:

1. Log into the Intercom interface and navigate to Config→Network→P2P
2. Make sure that it is enabled.
3. Navigate to Config→System→Basic Information.
4. Make sure that the binding state is “Unbound”. If already bound you can see the admin account. If needed, you can unbind it by clicking on “Unbind”
5. Click on the icon next to the “Security Code” field
6. Input the admin password and confirm.
7. Open the Provision Cam2 app.
8. Make sure you are logged into your account (Click on the menu icon and confirm you see your account details on the top as demonstrated below)



9. Click on “Add Device” in the server list



10. Use the phone camera to scan the QR code on the bottom of the Intercom page
11. The app will communicate with the server and recognize the intercom, then it will switch to the authentication page.
12. Set the desired name (Free input field) and input the security code from the Intercom web interface and click on “Add”

Please note:

- Adding the intercom to the app must be done with the security code. Adding the intercom with standard username and password will make it work like a standard IP camera and disable all the intercom features.
- During the binding process, the intercom and mobile app must be on the same timezone.

10)Calling to CAM2 app

Calling the Mobile APP from the Door Station

To initiate a call to the mobile APP from either the main or sub door station, please ensure the feature is enabled in advance:

1. Go to **Config → Intercom Interface**.
2. Enable **"Press button to call APP"**, then save the settings.

Please note:

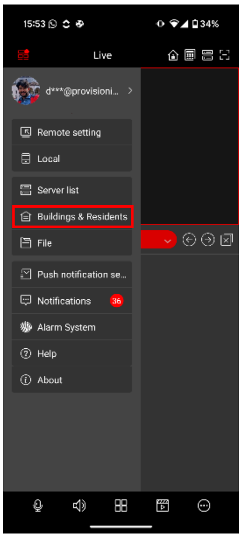
- Make sure the door station has already been added to the mobile APP before attempting to place a call.
- When this feature is enabled, any of the three call methods (button press, app platform, or indoor station) can function simultaneously. Once a call is answered on **any one** of the devices, the others will automatically end the call.

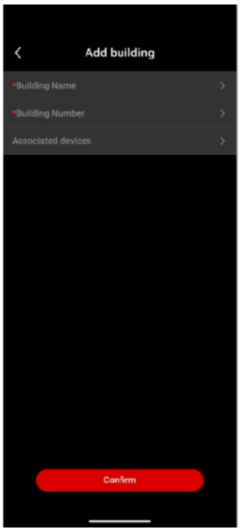
Calling a Resident via Room/Apartment Number

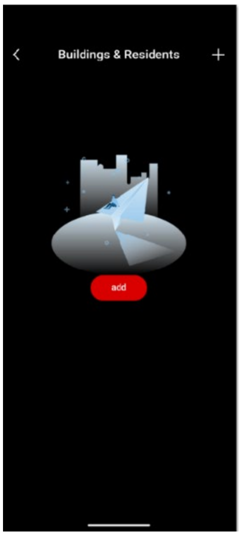
Visitors can call a resident’s mobile APP by pressing the assigned room number on the door station. Prior to this, the administrator must configure the building and resident details within the APP:

Setup Steps:

1. Make sure that your intercom is binded to the CAM2 app.
2. In the APP's live view interface, tap the menu and select **“Buildings & Residents”**.
3. Tap **“Add”** to input the building name and number, then link the door station accordingly.







11)Provision Cam2 Push Notifications

Both the bound user and his shared accounts can choose which push notifications they want to receive.

1. Go to main menu (Top right icon)
2. Click on "Push Notification Settings"
3. Click on the Intercom
4. Choose your preferred notifications.

Please note:

Incoming calls from the intercom will appear as standard phone calls, and doesn't require to open the app in order to receive or reject it.

12)Calling an Indoor Monitor (MON-TCH7)

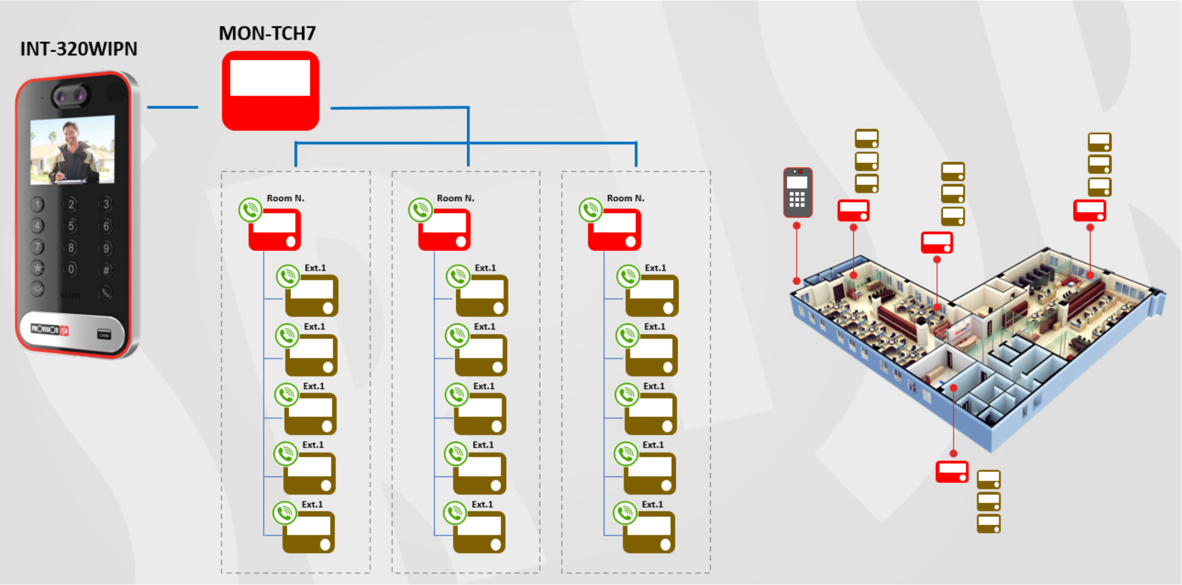
There are 2 ways to call the indoor monitor.

1. Quick Call button: If you have only 1 monitor, the easiest way is to configure the "Quick Call" button. You can configure it by following the instructions in section 5.7.2) Call Button Config
2. Manual Call: Every indoor unit has a room number, Input the indoor unit number and click on the "Call" button.

3. Extensions**: every** indoor unit can have up to 5 extensions **(more indoor units chained to the main indoor unit)** to learn how to set it up refer to [the MON-TCH7 Guide]

    - When calling to an indoor unit with extensions, the unit and all of it's chained extensions will ring, until answering the call.

Illustration of architecture with extensions:



13)Opening a Door

There are 3 ways to open a door from the intercom interface:

1. Admin PIN: If the admin PIN is set, you can use it to open the door
2. Face Recognition: Setting the face database with access control rules.
3. Indoor Monitor (MON-TCH7): If you have monitor communicating with the intercom, you can set password on the Monitor device and then authenticate it to open the door. If order to do so, input the indoor monitor number, followed by the PIN and click on #.

Please note:

The opening methods described above are from the intercom main panel only. There are many other ways to open the door remotely. This includes Ossia NVRs, Provision Cam2 Mobile App, Ossia VMS, MON-TCH7 Monitors.

Provision-ISR
11 Atir Yeda St, Kfar Saba,
Israel
Postal Code: 4442510
Tel: (972-9) 741 7511
Web: www.provision-isr.com