



Now you can see!



■ Z4/Z5/Z6 Series

USER MANUAL

This user manual covers the following cameras:

- Z4-25IPE-2(IR)
- Z4-25IPE-4(IR)
- Z5-25IPE-2(IR)
- Z5-25IPE-4(IR)
- Z6-32IPE-4(IR)

V5.x User Manual

Notes

- Before operating the camera, we strongly advise users to read this manual and keep it for later use.
- Please use the specified power supply to connect.
- Avoid incorrect operation, shock vibration, heavy pressing which can cause damage to the product.
- Do not use corrosive detergent to clean the body of the camera. If necessary, please use a soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high-grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as the sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not operate the camera in extreme temperatures or extreme humidity conditions.
- Use the power supply supplied authorized by a PROVISION-ISR technician.
- Keep away from heat sources such as radiators, heat registers, stove, etc.
- The instructions in this manual could be outdated; if you need any clarifications you can contact an authorized PROVISION-ISR technician. PROVISION-ISR reserves the right to add changes to this manual and publish it online on our website (www.provision-isr.com): there may be inconsistencies with the latest version. This applies to any and all software upgrades and product improvements, interpretation and modification added. These changes will be published in the latest version without prior notification.
- When this product is in use, the relevant contents of Microsoft, Apple and Google will be involved in. The pictures and screenshots in this manual are only used to explain the usage of our product. The ownership of trademarks, logos and other intellectual properties related to Microsoft, Apple and Google belong to the above-mentioned companies.
- All pictures and examples used in the manual are for reference only.

Table of Contents

1	Introduction	1
1.1	Main differences between Z# models.....	1
2	IE Remote Access	2
2.1	LAN	2
2.1.1	Access through IP-Manager.....	2
2.1.2	Direct Access through IE	4
2.2	WAN	5
3	Live Preview	6
3.1	The Live Preview Interface.....	6
3.2	PTZ Controls.....	7
4	IPC Configuration	8
4.1	System Configuration	8
4.1.1	Basic Information	9
4.1.2	Date & Time Configuration.....	10
4.1.3	Local Config.....	10
4.1.4	Storage	11
4.2	Video Configuration	14
4.2.1	Camera Configuration	14
4.2.2	Video/Audio	16
4.2.3	OSD Configuration	17
4.2.4	Video Mask.....	18
4.3	PTZ	18
4.3.1	PTZ Settings.....	19
4.3.1.1	PTZ Settings:	19
4.3.1.2	RS-485 (Applicable for Z6 only):	19
4.3.1.3	Others (OSD Password):.....	19
4.3.2	Restore	19
4.3.3	Smart Tracking	19
4.4	Alarm Configuration	20
4.4.1	Motion Detection	20
4.4.2	General Fault	22
4.4.3	Alarm In (Not applicable for Z4 Models)	24
4.4.4	Alarm Out (Not applicable for Z4 models).....	26
4.5	Advanced Analytics	27
4.5.1	Camera Tampering.....	27
4.5.2	Line Crossing.....	28
4.5.3	Sterile Area.....	30
4.5.4	Area Entrance / Exit	32
4.5.5	Object Counting.	32
4.5.6	Face Recognition	34
4.5.7	Analytics and Live Display.....	37
4.6	Network Configuration	37

4.6.1	TCP/IP	37
4.6.2	Port.....	39
4.6.3	Auto Report Server Configuration	39
4.6.4	DDNS Configuration	40
4.6.5	SNMP	40
4.6.6	802.1X	40
4.6.7	RTSP	40
4.6.8	UPnP	41
4.6.9	Email Setting.....	42
4.6.10	FTP.....	43
4.6.11	HTTPS.....	44
4.6.12	P2P	46
4.6.13	QoS.....	46
4.1	Security.....	46
4.1.1	User	46
4.1.2	Online Users	47
4.1.3	Block and Allow Lists	48
4.1.4	Security Management	49
4.2	Maintenance.....	50
4.2.1	Configure Backup & Restore.....	50
4.2.2	Reboot Device.....	51
4.2.3	Upgrade.....	51
4.3	Playback	52
5	Mobile Surveillance.....	55
5.1	Network Configuration	55
6	Appendix I : Analytics Configuration Requirements	56
6.1	General	56
6.2	Camera Tampering (Camera shifting / Lens tampering / Camera masking)	57
6.3	Line Crossing.....	58
6.4	Sterile Area	59
6.5	Q & A.....	60

1 Introduction

This IPC (short for IP Camera) is designed for high-performance CCTV solutions. It adopts the state-of-the-art video processing chips and utilizes most advanced technologies, such as video encoding and decoding technology, complies with the TCP/IP protocol, SoC, etc to ensure that this system will be extremely stable and reliable. The IPC device should be used together with Provision-ISR's IP manager or recording devices to enable the quick setting and full utilization of the camera.

1.1 Main differences between Z# models

	<u>Z4-25IPE-4(IR)</u>	<u>Z5-25IPE-4(IR)</u>	<u>Z6-32IPE-4(IR)</u>
Video Output	Network Only	Network Only	Network + CVBS
POE Support	Yes (PoE+~ 30W)	Yes (PoE+~ 30W)	Yes (PoE++~ 60W)
IR Distance	100m	100m	150m
Sensor Family	1/3" CMOS	1/3" CMOS	1/2" CMOS
Sensor Size	1/2.5" CMOS	1/2.5" CMOS	1/1.8" CMOS
Zoom Factor	x25	x25	x32
Lens	4.8mm-120mm	4.8mm-120mm	5.6mm-179.2mm
Preset Speed	80°/Sec	120°/Sec	240°/Sec
Tilt Range	180° with Auto Flip	180° with Auto Flip	180° with digital Flip
Audio-In	No	Yes	Yes
Audio-Out	No	Yes	Yes
Alarm-In	No	Yes (Wet-Contact)	Yes (2 Wet-Contacts)
Alarm-Out	No	Yes	Yes (2)
Power Supply	PoE / DC12V	PoE / DC12V / AC24V	PoE / AC24V
Operation Temperature	-30°C~50°C (Cold start at -20°C)	-30°C~50°C (Cold start at -20°C)	-50°C~65°C (Cold start at -40°C)
Remarks	Bracket not Included	Bracket not Included	

2 IE Remote Access

You may connect IPC via LAN or WAN. In this manual, we will use IE v11 for example. The details are as follows:

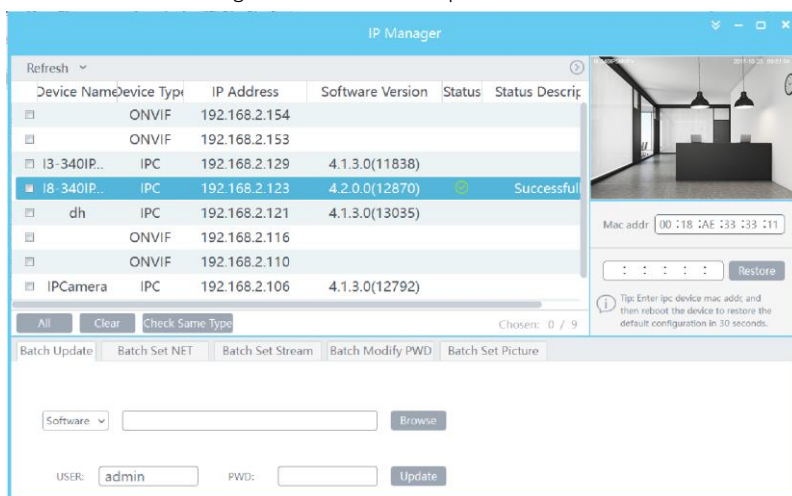
2.1 LAN

In LAN, there are two ways to access IPC:

1. Access through IP Manager Software.
2. Direct access through IE browser.

2.1.1 Access through IP-Manager

- ① Make sure the PC and IPC are connected to the LAN and that the IP-Manager is installed on the PC. You can install the IP manager from the disc provided with the camera or download it by clicking [here](#).
- ② Double-click the IP-Manager icon on the desktop to run this software as shown below:



- ③ Modify the IP address. The default IP address of this camera is 192.168.226.201. Tick all the cameras you wish to set and then click on the “Batch Set NET” tab.

☐ Automatically gets IP address

☒ Uses the following IP address

IP address range: Start

Subnet Mask

End

Gateway

USER:

PWD:

If you wish to use DHCP (IP Address automatic assignment), choose “Automatically gets IP address”, set the password 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:

- 1) In order for the DHCP mode to work, you must have a DHCP server on the LAN.
- 2) Using DHCP for permanent installations is not advisable as the IP Address might change after a while and cause the camera to be unreachable.

If you wish to set static IP addresses, choose “Uses 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.

Please note:

- 1) The IP range must fit the number of chosen cameras.
- 2) 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).



The default password of the administrator is “**123456**”.

④ Double click on the IP address of the system will pop up IE browser and connect to the IPC. IE browser will auto download the Active X control. You must install it in order for the camera to work. After successful installation, a login window will appear as shown below.

PROVISION ISR[®]

IPC

Name:

Password:

Stream Type:

Language:

☐ Remember me

Login

Input the username and password to log in.



The default username is “**admin**”; the default password is “**123456**”.

2.1.2 Direct Access through IE

The default network settings are as shown below:

IP address: **DHCP (According to your LAN configuration)**. If your network doesn't have an active DHCP server, the camera will fall back to IP address **192.168.226.201**

Subnet Mask: **255.255.255.0**

Gateway: **Based on the DHCP Configuration.**

HTTP: **80**

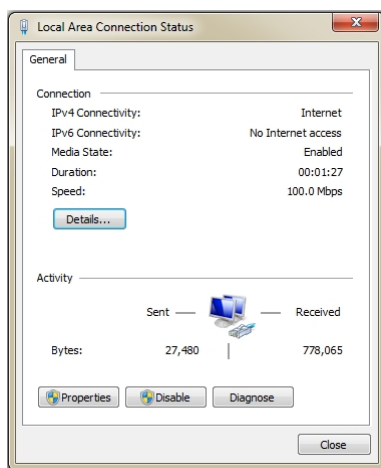
Data port: **9008**

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

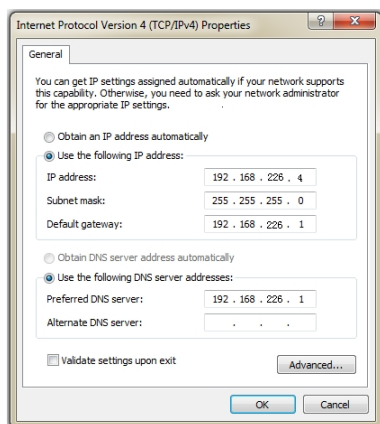
① You can use the IP manager to access the camera even if the camera is still using the default IP address. Double click on the IP address within the IP manager for the system to pop up IE browser and connect to the IPC. IE browser will auto download the Active X control. You must install it in order for the camera to work. After successful installation, a login window will appear.

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 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.



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

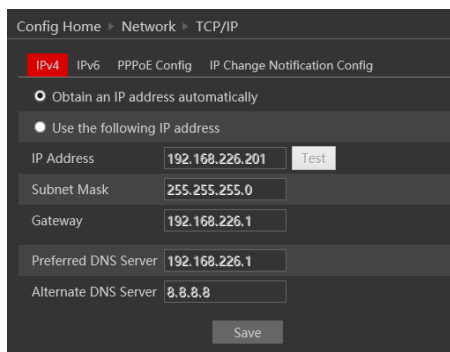


- ② Open the IE browser and input the default address of IPC and confirm. The IE browser will download Active X control automatically.
- ③ After downloading and installing the Active X control, the login dialog box will appear.
- ④ Input the default username and password and click “Login”.

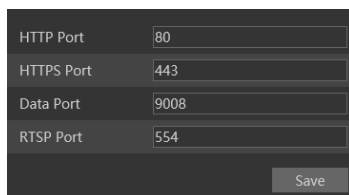
2.2 WAN

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 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.



IP Setup



Port Setup

- ④ Go to the router's management interface through IE 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)

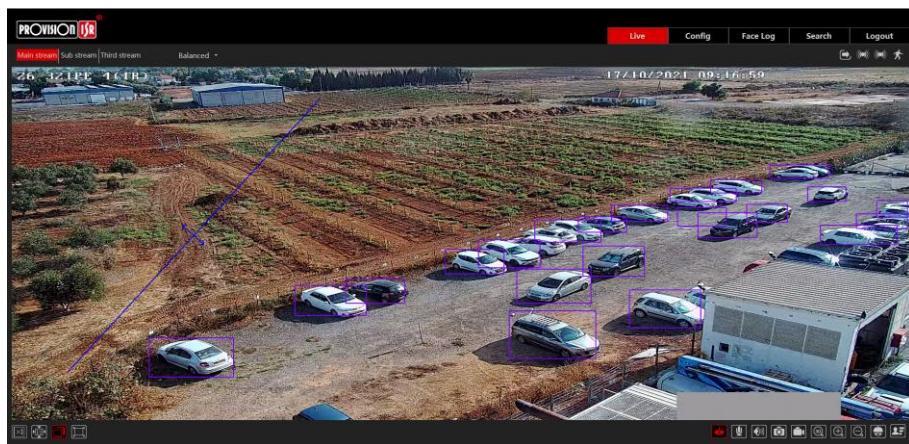
Port Range						
Application	Start	End	Protocol	IP Address		Enable
1	9008	to 9008	Both	192.168.6.	6	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.6.	6	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.6.	166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.6.	156	<input type="checkbox"/>
5	7777	to 7778	Both	192.168.6.	206	<input type="checkbox"/>
6	1029	to 1030	Both	192.168.6.	207	<input type="checkbox"/>

Router Setup

- ④ Open the IE browser and input your WAN IP and HTTP port to access the camera.

3 Live Preview


3.1 The Live Preview Interface





































Icons and operation buttons:

Icon	Description	Icon	Description
	Actual Size		Digital Zoom-Out
	Fit to screen – True Proportions		
	Fit to screen - Stretch		Face Detection Bar
	Full screen		Motion Detection indicator
	Enable/Disable live view		SD Card recording indicator
	Talk (If applicable)		Alarm In Indicator
	Listen (If applicable)		Use mainstream for live-view
	Take Snapshot		Use sub-stream for live-view
	Enable/Disable Local Recording		Use third stream for live-view
	3D control over the PTZ		Choose the buffering plan
	Digital Zoom-in		

3.2 PTZ Controls

Clicking on the PTZ control icon  will open the PTZ control interface. From this interface you can control the movement of the PTZ as well as setting and calling presets, cruises, and other PTZ features.

The descriptions of the control panel are as follows:

Button	Description
	 to rotate the dome upwards;  to rotate the dome downwards;  to rotate the dome towards left;  to rotate the dome towards right;  to rotate the dome diagonally up-left;  to rotate the dome diagonally up-right;  to rotate the dome diagonally down-left;  to rotate the dome diagonally down-right;  to stop rotating the dome.
	Control the movement speed by adjusting the motion speed bar
	Zoom button. Click  to zoom in to the image (Tele); click  to zoom out of the image (Wide).
	Focus button. Click  for far focus; Click  for near focus.
	Iris button. Click  reduce the iris size; click  to increase the iris size.
	Activate scan according to the left/right boundaries. If no boundary was set, the PTZ will scan in 360°
	Switch IR LED on/off (Bypassing the image configuration)
	Random Scan according to the left/right boundaries
	Group Scan
	 - Save the PTZ location to the selected preset number
	 - Call the selected preset and send the PTZ to its location (Not available if the preset is empty)
	 - Delete the selected preset (Not available if the preset is empty)
	 - Activate the cruise according to its setting
	 - Stop the cruise (Moving the camera also stops the cruise)
	 - Activate the pattern according to its setting
	 - Stop the pattern (Moving the camera also stops the cruise)

4 IPC Configuration

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

4.1 System Configuration

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

4.1.1 Basic Information

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

Device Name	Z6-32IPE-4(IR)
Product Model	Z6-32IPE-4(IR)
Brand	Provision ISR
Software Version	5.0.1.0(23389)
Software Build Date	2021-09-10
Kernel Version	20210224
Hardware Version	1.0
Onvif Version	20.12
Video Structured Version	(1.1.8)1.1.0
Face Detection Version	1.65
Face Match Version	1.0.28
OCX Version	2.1.9.1
MAC	00:18:ae:ad:64:6f
PTZ Version	V1.4.10(2020/12/29)
Camera Type	M432IM
Device ID	I646F0018D4P



The following table will explain the available detail field.

<i>Parameter</i>	<i>Meaning</i>
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
Kernel version	The kernel version of the device

Hardware version	The hardware version of the device
ONVIF Version	The current ONVIF version
OCX Version	The current OCX version
Mac Address	The MAC address of device
QR Code	QR Code used for P2P connection

4.1.2 Date & Time Configuration

Setting steps:

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

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 (Internet connection required), synchronize the camera time with the time of the computer you are using or set the time manually.

4.1.3 Local Config

1. Got to “System Configuration” → “Local config” as shown below:

Config Home ▸ System ▸ Local Config

Picture Path	<input type="text" value="C:\Users\Tal Hanoch\Favorites"/>	<input type="button" value="Browse"/>
Record Path	<input type="text" value="C:\Users\Tal Hanoch\Favorites"/>	<input type="button" value="Browse"/>
Video Audio Settings	<input checked="" type="radio"/> Open	<input type="radio"/> Close
Show Bitrate	<input checked="" type="radio"/> Open	<input type="radio"/> 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).

4.1.4 Storage

The SD card feature allows you to insert an SD card into the camera and enable the camera to operate with a 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.

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

Config Home ▸ System ▸ Storage

Management	Record	Snapshot
Capacity	<input type="text" value="7541 MB"/>	
Used Capacity	<input type="text" value="7237 MB"/>	
Remaining Capacity	<input type="text" value="304 MB"/>	
State	<input type="text" value="Normal"/>	
Snapshot Quota	<input type="text" value="10"/>	%
Video Quota	<input type="text" value="90"/>	%
<input type="button" value="Eject"/>		<input type="button" value="Format"/>

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 SD card and allow you to remove it safely. Inserting an SD card to the camera must be done while the camera is powered off.



Note: Using of SD card function should be coordinated with motion or sensor alarms.

The following table will explain the available detail field.

Parameter	Meaning
Capacity	The total capacity of the SD card
Used capacity	The capacity currently being used
Remaining Capacity	The available capacity
State	The state of the SD card.
Snapshot Quota	The percentage of the SD card dedicated for 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 Record

Recycle Recording: Yes

Schedule

☒ Enable Schedule Recording

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 for record
Pre-recording time	The duration of video prior to the recording trigger
Cycle recording	Whether to recycle 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 required dates to it.

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

Config Home ▶ System ▶ Storage

Management Record **Snapshot**

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 on 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 required dates to it.

4.2 Video Configuration

Camera Configuration includes five submenus: Display Configuration, Video Stream, OSD Config, Video Mask and ROI Config.


4.2.1 Camera Configuration

Setting steps:

1. Go to “Video Configuration” → “Display” interface as shown below.

Config Home ▶ Image ▶ Display Settings

Camera Parameters Schedule



Focus Limit: 1M

Zoom Display: ☐

Zoom Speed: 3

Scan Speed: 10

Lens Initialization:

Set North:

Config File: Common

Brightness: 49

Saturation: 50

WDR: ☒ 50

Sharpness: ☐ 100

Noise Reduction: ☐ 100

Defog: Off

BLC: BLC

Location: Auto

Antiflicker: Off

White Balance: Auto

Frequency: 50HZ

Day/Night Mode: Auto

Sensitivity: Mid

Infra-red Mode: Off

Smart IR: Auto

Exposure Mode: Auto

Gain Limit: 75

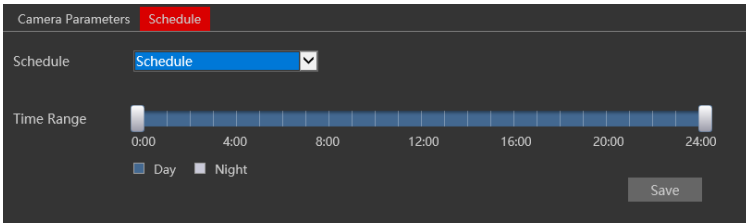
Image Mirror: ☒ Open ☐ Close

Image Flip: ☒ Open ☐ Close

The display parameters are as follows:

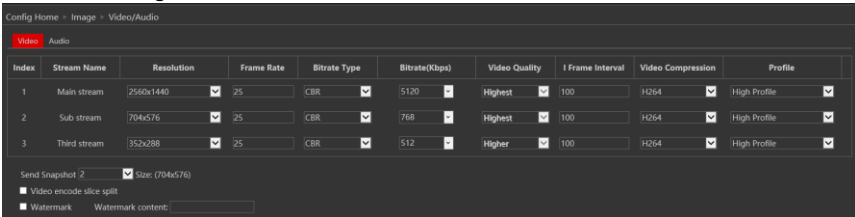
<i>Parameter</i>	<i>Meaning</i>
Config file*	You can set an individual configuration for Day and night. Common is used for both
Brightness	Set the image brightness
WDR	Set the Digital WDR value
Saturation	Set the image saturation
Sharpness	Enable/Disable the sharpness and set its level
Noise reduction	Enable/Disable the 3D-DNR and set its level
Defog	Enable/Disable the defog and set its level
BLC	Set HLC/BLC to deal with advanced light conditions. When set to BLC, you can adjust the BLC location When set to HLC, you can set the HLC schedule
Antiflicker	Set the antiflicker
White Balance	Set the white balance of the camera
Frequency	Set the frequency to 50/60Hz
Day/Night Mode*	Set the day/night mode (Auto/Day/Night/Schedule)
Sensitivity	The light sensor sensitivity
Infra-Red Mode	Set the IR status
Smart IR	Set the smart IR. Smart IR makes sure that the image will not be overexposed due to the IR light.
Exposure Mode	Set the exposure to auto or set it manually
Image Mirror	Mirror the image horizontally
Image Flip	Flip the image vertically
Focus Limit	Set the minimum distance for focusing. The shorter the range, the longer it might take the camera to focus. (Since it needs to search for the focus point in a longer range)
Zoom Display	Choose if the show the zoom ratio as part of the OSD
Zoom Speed	Set the zoom speed
Scan Speed	Set the scan speed (For auto scan tasks)
Lens Initialization	Initialize the lens
Set North	Set the north (Useful for installations where the North direction is important)

*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 schedule accordingly. Click on the “Schedule” tab and set the schedule as you wish.



4.2.2 Video/Audio

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



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

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 and VBR are available. CBR (Constant Bit-Rate) means that no matter how what the video resources are, the 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 in 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 support 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. 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:

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”.

*Z4 models do not support Audio

4.2.3 OSD Configuration

Go to “Video Config” → “OSD” menu to display the interface as shown below.

You may set the device name, time stamp 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.

4.2.4 Video Mask

You can set 4 mask areas at most.

Config Home > Image > Video Mask

26-32 IPE-4 (IR) 17/10/2021 12:52:19

Enable ☒ Draw Area Clear

Mask Area List

ID	Name	Enable
1	Mask Area 1	Yes

Add Delete

To set up video mask

1. Enable video mask.
2. Move the PTZ to the required location using the PTZ controls
3. Click "Draw" button and then drag the mouse to draw the video mask area.
4. Click "Save" button to save the settings.
5. Return to the live to see the following picture.

To clear the video mask:

1. Choose the video mask line you wish to delete
2. Click on "Delete" and confirm.

4.3 PTZ

PTZ section includes all the parameters and settings for the PTZ control and preconfigured actions such as presets, cruises, scans and schedules.

4.3.1 PTZ Settings

Go to “PTZ” → “PTZ settings”

4.3.1.1 PTZ Settings:

Auto PTZ Flip: set whether the camera will perform auto flip when reaching 90° tilt angle.

OSD Language: The preferred language of the Preset 95 OSD menu

OSD Auto Logout: Enable it if you wish the preset 95 OSD menu to automatically close after the set period of time.

4.3.1.2 RS-485 (Applicable for Z6 only):

Set the RS-485 values for analog controllers

PTZ ID: The analog ID of the camera

Protocol: The controlling Protocol you wish to use

Baud-Rate: the desired controlling baud-rate

***Please Note:** All parameters must match exactly the setting of the analog controlling device. Otherwise, the camera will not respond.

4.3.1.3 Others (OSD Password):

This allows you to set a password for accessing the preset 95 OSD Menu. Keep both fields empty if you don't require password.

4.3.2 Restore

Go to “PTZ” → “Restore” allows you to restore some or all of the PTZ parameters.

"Reset" resets all the setting of the camera to factory default.

"Clear" clears all the presets, cruise and patterns saved on the camera.

4.3.3 Smart Tracking

Go to “PTZ” → “Smart Tracking” allows you to modify the PTZ smart tracking feature.

Control Priority: Set the priority for controlling the camera (Tracking/Manual Priority). Note that if “Tracking Priority” is set the user **cannot** control the camera under any circumstances.

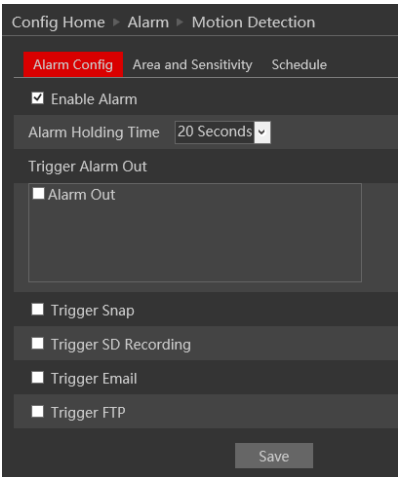
Still time (Seconds): If a tracked target is motionless for the time specified above, the camera will return to the home position.

4.4 Alarm Configuration

Alarm configuration includes four submenus: Motion Detection, General Fault, Alarm in and Alarm Out.

4.4.1 Motion Detection

Go to “Alarm configuration”→ “Motion Detection” to see an interface as below.

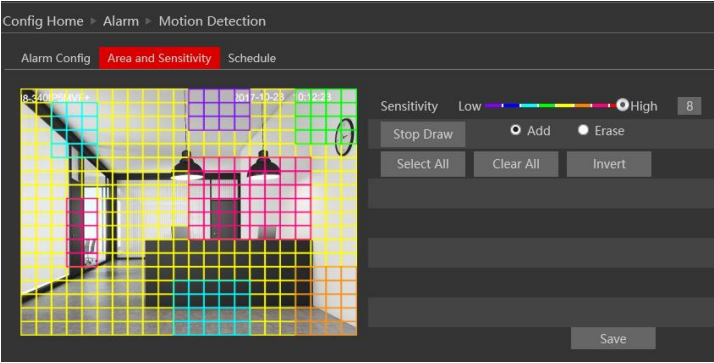


The first tab is the “Alarm Config”. Enable or disable the alarm and set the alarm holding time. The holding time means that the alarm signal will stay active and no additional alarms will be generated during that time.

Choose the camera’s response to the alarm:

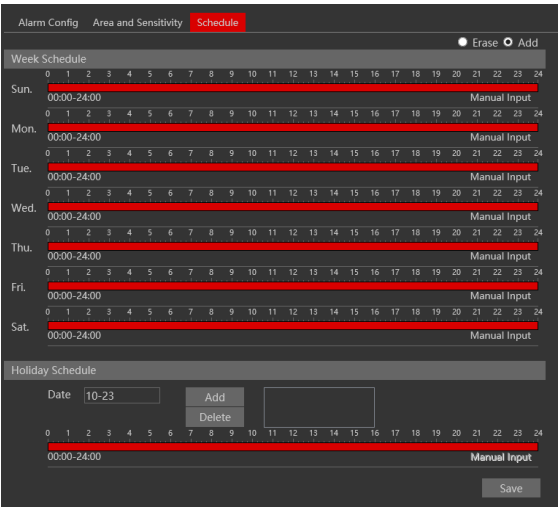
Alarm Triggers:	
Alarm Out	triggers the alarm out relay
Trigger Snap	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

Next is the “Area and Sensitivity” Tab. Move the “Sensitivity” scroll bar to set up the motion sensitivity and click on “draw” to enable the marking on the image. Note that you can set different sensitivities to a different area of the picture as shown below. Once finished, click on “Stop Draw”.



4. Click “Save” to save the settings.

Last is the “Schedule” tab:



Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add required dates to it.

4.4.2 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” to see a screen as shown below. The default tab is “SD Card Full”:

Enable the alarm if required. This alarm will only be relevant if “Recycle Record” is not marked. If “recycle record” is active, the SD card will never get full.

Config Home > Alarm > General Fault

SD Card Full SD Card Error IP Address Collision Cable Disconnected

☒ Enable Alarm

Alarm Holding Time 20 Seconds ▾

Trigger Alarm Out

☐ Alarm Out

☐ Trigger Email

☐ Trigger FTP

Save

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.

Config Home > Alarm > General Fault

SD Card Full SD Card Error IP Address Collision Cable Disconnected

☒ Enable Alarm

Alarm Holding Time 20 Seconds ▼

Trigger Alarm Out

☒ Alarm Out

☐ Trigger Email

☐ Trigger FTP

Save

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 “IP Address Collision”. This alarm will be triggered when another device in the network will be assigned with the same IP address of the IPC (or vice versa).

To activate it, enable the alarm.

SD Card Full SD Card Error IP Address Collision Cable Disconnected

☒ Enable Alarm

Alarm Holding Time 20 Seconds ▼

Trigger Alarm Out

☒ Alarm Out

☐ Trigger Email

☐ Trigger FTP

Save

After enabling the alarm, choose the responses required from the camera in case the alarm will be active. Note that any response related to the network such as email or FTP is not available since in most cases the network will become unavailable for the camera. After the setting is complete, click “Save”.

Last is the “Cable Disconnected” tab. This alarm will be generated if the network cable will be disconnected from the camera. Please note that this alarm is not usable if you are using PoE to power the camera since the disconnection of the cable will cause the camera to turn off due to power loss.

To activate it, enable the alarm.

Config Home ▶ Alarm ▶ General Fault

SD Card Full SD Card Error IP Address Collision Cable Disconnected

☒ Enable Alarm

Alarm Holding Time 20 Seconds

Trigger Alarm Out

☐ Alarm Out

Save

After enabling the alarm, choose the responses required from the camera in case the alarm will be active. Note that any response related to the network such as email or FTP is not available since the disconnection of the network cable prevents any external network communication by the camera. After the setting is complete, click “Save”.

4.4.3 Alarm In (Not applicable for Z4 Models)

Enter “Alarm”→ “Alarm In” to see a screen as shown below:

Config Home ▶ Alarm ▶ Alarm In

Alarm Config Schedule

☒ Enable Alarm

Alarm Type NO

Alarm Holding Time 20 Seconds

Sensor Name Test

Trigger Alarm Out

☐ Alarm Out

☐ Trigger Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

Save

2. Enable the alarm to activate it and see the configuration parameters:

Parameter	Meaning
Sensor ID (Applicable for Z6 model only)	Choose the Sensor you wish to set
Alarm Type	You can set it to “NO” (Normally open) which means that the once the line is closed the alarm will be active, or “NC” (Normally Closed”) which means that once the line is open the alarm will be active.
Alarm Holding Time	The holding time means that the alarm signal will stay active and no additional alarms will be generated during that time.
Sensor Name	You can set a unique name for easy identification.
Alarm Triggers:	
Alarm Out	triggers the alarm out relay
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

3. After the setting is complete, click “Save”.
4. Next, you will need to set the alarm schedule. Click on the “Schedule” tab to get the following interface:

Config Home > Alarm > Alarm In

Alarm Config **Schedule**

☐ Erase ☒ Add

Week Schedule

Sun.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Mon.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Tue.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Wed.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Thu.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Fri.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Sat.

00:00-24:00

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Manual Input

Holiday Schedule

Date

10-25

Add

Delete

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

00:00-24:00

Manual Input

Save

5. Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add required dates to it. The holiday schedule overtakes the normal schedule.

4.4.4 Alarm Out (Not applicable for Z4 models)

The Alarm output is actually a relay that can operate many types of devices such as gates, doors, strobe light, and sirens. The alarm out always works in a “NO” mode (Normally open) which means that the relay is open in a normal state and closed in an armed state.

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

Alarm Out ID

Alarm Out0

Alarm Out Mode

Alarm Linkage

Alarm Out Name

alarmOut1

Alarm Holding Time

30 Seconds

Alarm Type

NC

2. Alarm out has 4 modes as described below:

A. Alarm Linkage (Shown Above): This mode will set the alarm out to be triggered as a response to any of the available alarms (Motion, Alarm in, Analytics). If this mode is chosen you will need to set it properly.

Parameter	Meaning
Alarm Out ID (Applicable for Z6 Model)	Choose the alarm out ID you wish to set
Alarm Out Name	You can set a unique name for easy identification.
Alarm Holding Time	The holding time means that the alarm signal will stay active and no additional alarms will be generated during that time.
Alarm Type	Set the required alarm type (NO/NC)

B. Manual Mode: This mode will enable you to manually operate the relay.

Config Home > Alarm > Alarm Out

Alarm Out Mode

Manual Operation

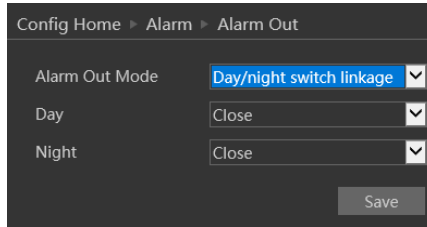
Manual Operation

Open

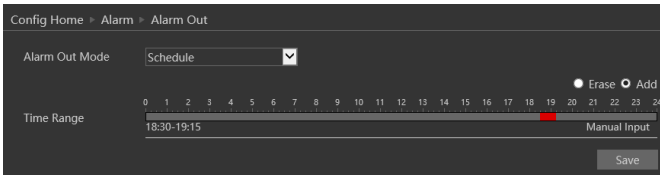
Close

Save

- C. Day/night switch linkage: This mode allows you to set the relay condition according to the day/night mode of the camera.



- D. Schedule mode: This mode allows you to set the relay condition according to a pre-defined schedule. Once chosen you will have to set the schedule. The set schedule will be relevant for all weekdays and cannot be set for each day independently.



3. Press the “Save” button to save the settings.

4.5 Advanced Analytics

This version offers advanced video analytics that was designed to detect special scenarios and events. In Eye-Sight v2, the Video analytics detection is based on true object detection of 3 classes: Humans, 4 wheel vehicle and 2 wheel vehicle. v5.1 offers a variety of Analytics based on Object detection (Line Crossing, Sterile Area, Object Counting) together with advanced face detection and other general analytics such as Camera Tampering

Note that some features might not be available in specific models. For confirmation please refer to the camera’s technical specs.

4.5.1 Camera Tampering

Camera tapering uses special analytics algorithm to detect if the camera was tampered with. This includes: Camera tampering – detects if the camera was shifted from its original location, covered or that the lens was tampered with. Color cast detection – detects if the camera image suffers from unusual color (For example faulty ICR results in pinkish) image.

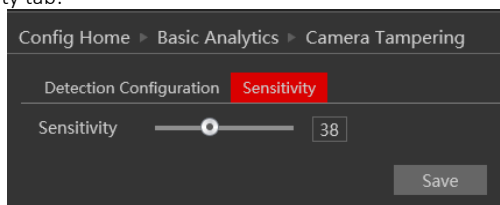
1. Go to “Advanced Analytics” → “Camera Tampering” to get to the interface as shown below:
2. Enable the required detection analytics out of Camera Shifting/Lens Tampering/Masking detection.

3. Set the Alarm response as follows:

<i>Alarm Triggers:</i>	
Alarm Out	triggers the alarm out relay
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

4. Click “Save” to confirm.

5. Go to the sensitivity tab:



6. Set the sensitivity (0 – lowest, 100 – Highest)

7. Click “Save” to confirm.

4.5.2 Line Crossing

Line Crossing Analytics will detect if a defined object crossed a defined line. The crossing direction can be adjusted.

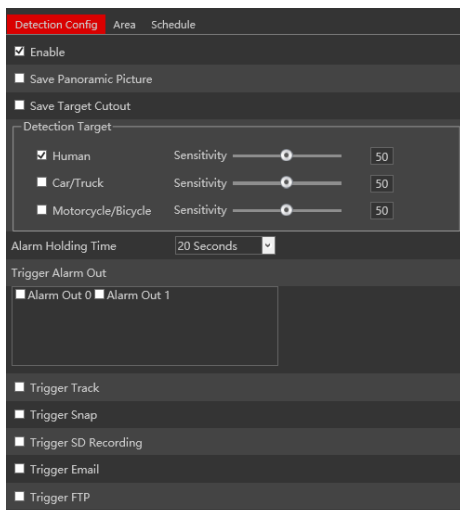
1. Go to “Advanced Analytics”→ “Line Crossing” to get to the interface as shown to the right.

2. Enable Alarm if required.

3. Set weather to save the scene image (Panoramic Picture) or the object image (Target Cutout)

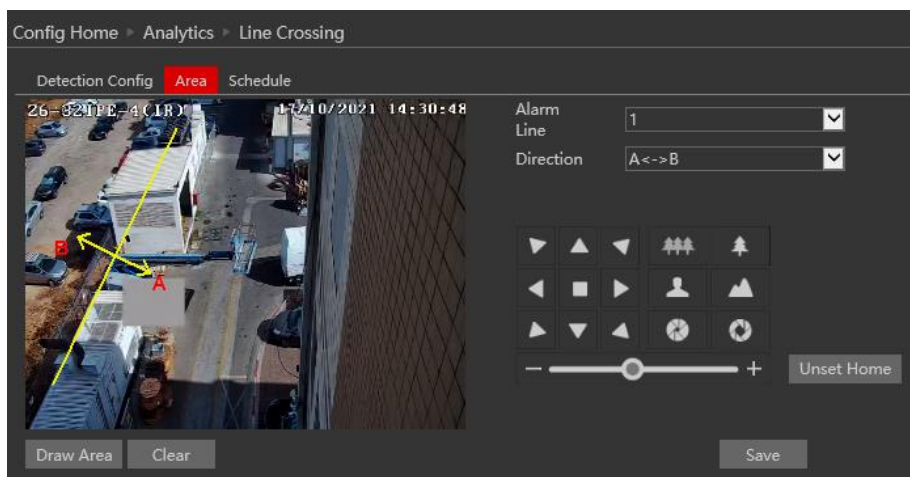
4. Set the alerting objects and detection sensitivity (Objects not marked will be ignored)

5. Set the Alarm response as follows and click “Save” to confirm:



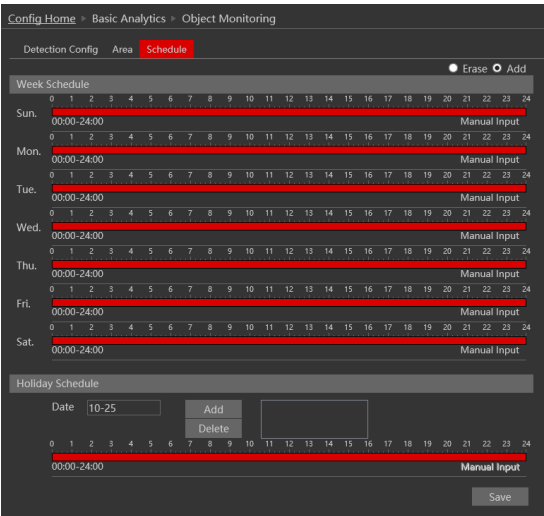
Alarm Triggers:	
Trigger Track	Track the detected object
Alarm Out	triggers the alarm out relay
Trigger Snap	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

6. Now you will have to set the detection area (lines). Click on the “Area” tab to get to the interface shown below.



7. Move the PTZ to the desired location using the PTZ controls
 8. Click on “Draw Area”.
 9. Draw the line. The length of the line should be as long as possible to increase the detection efficiency.
 10. Set the crossing direction. The “A” and “B” sides will reflect on the image on the left. The available options are. $A \rightarrow B$ – Crossing from A side to B side, $B \rightarrow A$ - Crossing from B side to A side, $A < \rightarrow B$ – Crossing from any side to any side.
 11. Click on “Save”
 12. (Applicable if “Trigger Tracking” was set) – Set the home position. The camera will return to the home position after the target was lost for 5 seconds or after the target became static for the set period of time (Can be configured in PTZ→Smart Tracking setting).
- Please note:** if tracking priority was set to “PTZ”, once the home position was set, the control over the PTZ will be lost.
13. Click “Save” to confirm the settings.
 14. You can set up to 4 lines. If you wish to set additional lines, change the Alarm line number and repeat steps 8-11.

15. Next, you will need to set the schedule. Click on the “Schedule” tab to get the following interface:

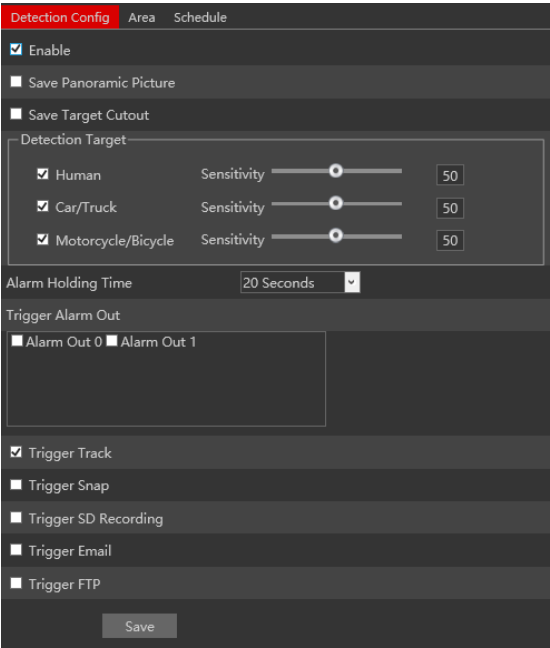


12. Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add required dates to it. The holiday schedule overtakes the normal schedule.

4.5.3 Sterile Area

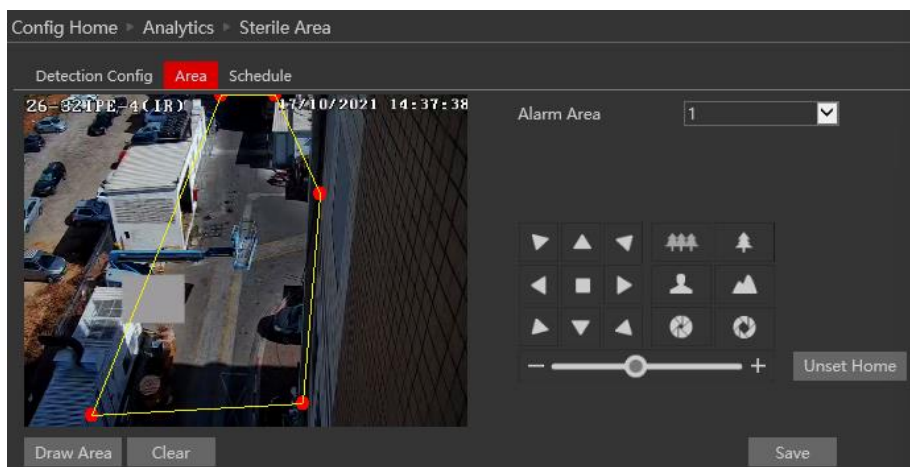
Sterile Area Analytics will detect if any defined object entered the defined area.

- 1. Go to “Advanced Analytics”→ “Sterile Area” to get to the interface as shown to the right:
- 2. Enable Alarm if required.
- 3. Set weather to save the scene image (Panoramic Picture) or the object image (Target Cutout)
- 4. Set the alerting objects and detection sensitivity (Objects not marked will be ignored)
- 5. Set the Alarm response as follows and click “Save” to confirm:

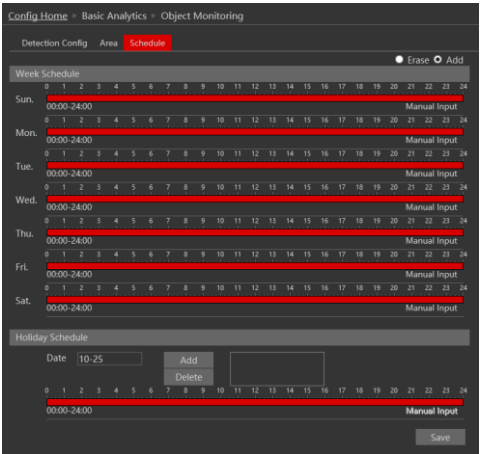


<i>Alarm Triggers:</i>	
Trigger Track	Track the detected object
Alarm Out	triggers the alarm out relay
Trigger Snap	takes a snapshot (SD card must be available)
Trigger SD Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

6. Now you will have to set the detection area (lines). Click on the “Area” tab to get to the interface shown below.



7. Move the PTZ to the desired location using the PTZ controls
 8. Click on “Draw Area”.
 9. Draw the sterile area polygon. It supports up to 6 corners.
 10. Click on “Save”
 11. (Applicable if “Trigger Tracking” was set) – Set the home position. The camera will return to the home position after the target was lost for 5 seconds or after the target became static for the set period of time (Can be configured in PTZ→Smart Tracking setting).
- Please note:** if tracking priority was set to “PTZ”, once the home position was set, the control over the PTZ will be lost.
12. Click “Save” to confirm the settings.
 13. You can set up to 4 detection area. If you wish to set additional areas, change the Alarm area number and repeat stages 8-10.
 14. Next, you will need to set the schedule. Click on the “Schedule” tab to get the following interface:



12. Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add required dates to it. The holiday schedule overtakes the normal schedule.

4.5.4 Area Entrance / Exit

Area Entrance / Exit is an extension of the Sterile Area Analytics. Sterile area will detection any movement within it while **Area Entrance** will only detect defined objects that **enter** the defined area, and **Area Exit** will only detect defined objects that **exiting** the defined area.

4.5.5 Object Counting.

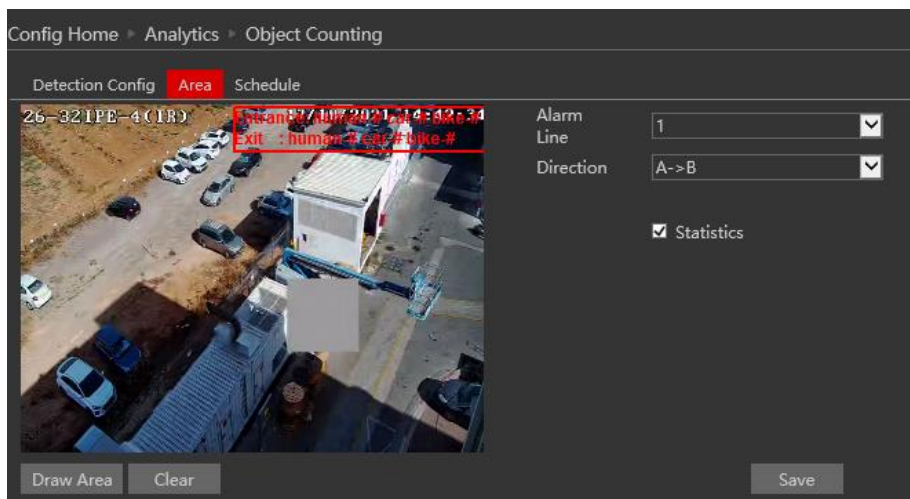
Object counting analytics will detect defined objects crossing a defined line and count is. The counter has “Enter” and “Exit” Separated split into 3 object detection categories (Human, 4 Wheel Vehicle, 2 Wheel Vehicle).

1. Go to “Advanced Analytics”→ “Object Counting” to get to the interface as shown below:

2. Enable Alarm if required.
3. Set weather to save the scene image (Panoramic Picture) or the object image (Target Cutout)
4. Set the alerting objects and detection sensitivity (Objects not marked will be ignored)
5. Set the Alarm response as follows and click “Save” to confirm:

<i>Alarm Triggers:</i>	
Alarm Out	triggers the alarm out relay
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

6. Set the “Reset Count” if needed – The counter will be reset automatically at the end of the defined period.
7. You can manually reset the counter by clicking on the “Reset” button.
8. Now you will have to set entrance mark line. Click on the “Area” tab to get to the interface shown below.



11. Click on “Draw Area”.
12. Define the line. This definition consists out of 2 settings:
 - A. The entrance area: Indicated by a yellow line. Cover the pathway from side to side.
 - B. Entrance Direction: Indicated by an “A”/”B” arrow where the arrow direction is the entrance direction. The direction of exit will be the opposite direction.
13. Set the counter OSD location by dragging it to the desired position on the live preview window.
14. Click “Save” to confirm the settings.

Once enabled, the live interface of the camera will show the marked area together with the counter’s current state.

4.5.6 Face Recognition

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.

1. Go to “Analytics” → “Face Recognition” to get to the interface as shown below:

Config Home > Basic Analytics > Face Comparison

Detection Config Area Advanced Schedule

State Working

☒ Enable

☒ Save Source Information

☒ Save Face Information

Alarm Holding Time 20 Seconds

☐ Trigger SD Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

Save

- 1. Enable the detection and set the detectio requirement.
- 2. Set triggers for face **detection**

Alarm Triggers:	
Alarm Out	triggers the alarm out relay
Save source information	takes a snapshot (SD card must be available)
Save face information	Takes an image of the detected license plate.
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

Next you will need to set the recognition triggers and resonses. Click on “Recognition and Linkage” to open the following interface:

Deduplication Removal Period: Set the time between triggering alert for the same face in the frame.

Similarity threshold: Set the threshold for successful recognition.

Alarm List: Set triggers for each of the preseted groups (Allow List/Block List/Stranger). Available trigger is alarm out only.

Detection Config **Recognition and Linkage** Area Advanced

☒ Duplication Removal Period 4 Seconds

Similarity threshold 75 %

Alarm List Allow list

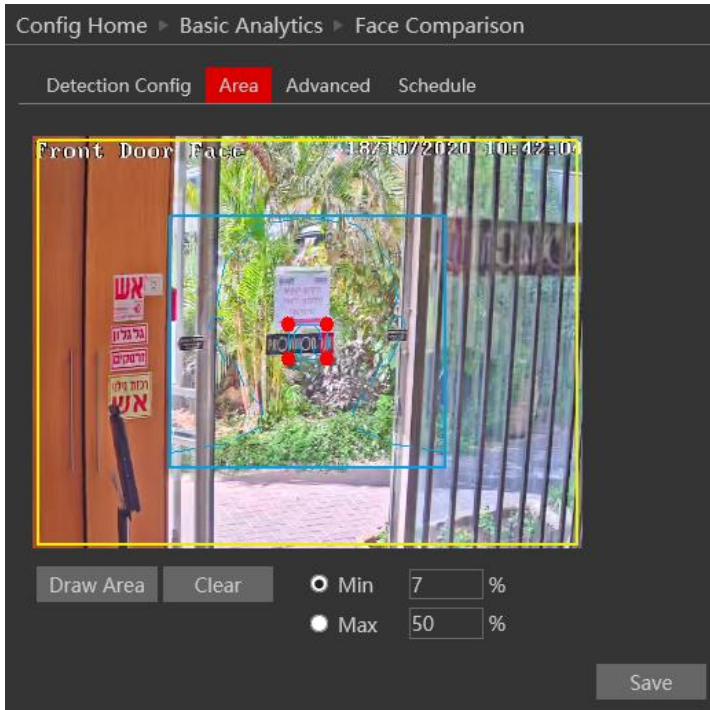
Alarm Trigger Mode Face Only

☐ Alarm Out 0 ☐ Alarm Out 1

Save

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

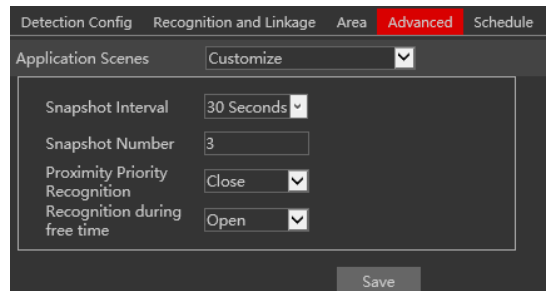
1. Click on “Area” to navigae to the following window.



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.

1. Click on “Advanced” to navigate to the following window.



2. Set the application scene. First lets understand the vlues:
 - a. Snapshot intervals: The time between each snapshot capturing of the same face.
 - b. Snapshot Number: Limit the number of snapshot taken of the same face.
 - c. Proximity Priority Comparison: Give priority to detect faces closer to the camera (Bigger faces are closer to the camera)
 - d. Comparison during free time (Future Development).

We have prepared 2 presets for you:

- a. Access Control: Very fast face sampling intervals (0.5 Seconds) without a limit. (65535) and priority to closer faces.
- b. Security Monitoring: Slower sampling intervals (30 Seconds) with a snapshot limit. (3) and no priority to closer faces.

Use “Customize” to configure your own setting.

Eventually, set the analytic schedule in the schedule tab.

4.5.7 Analytics and Live Display.

Once enabled, the Analytics will appear on the camera’s live interface. It will only appear on Ossia devices running v1.4.3 if configured so.

4.6 Network Configuration

Network configuration includes eight submenus: Port, IP Address, Server Configuration, IP Notify, DDNS Config, RTSP, UPnP, Mail Setting, and FTP.

4.6.1 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

Subnet Mask

Gateway

Preferred DNS Server

Alternate DNS Server

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:

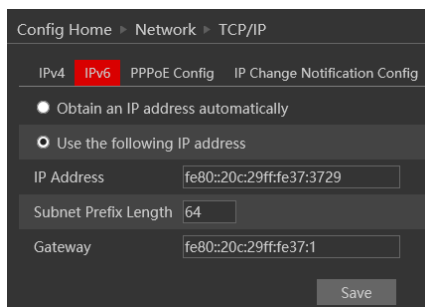
- 1) In order for the DHCP mode to work, you must have a DHCP server on the LAN.
- 2) Using DHCP for permanent installations is not advisable as the IP Address might change after a while and cause the camera to be unreachable.

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:

- 1) The selected IP address must be available.

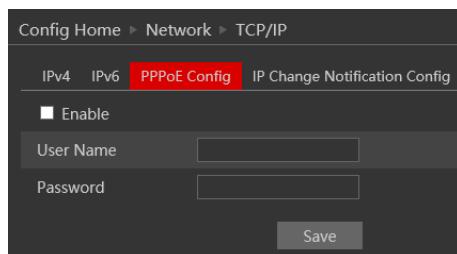
The next tab is IPv6:



The screenshot shows the 'Config Home > Network > TCP/IP' interface. The 'IPv6' tab is selected. Under the 'IPv6' tab, there are two radio buttons: 'Obtain an IP address automatically' (which is selected) and 'Use the following IP address'. Below these, there are input fields for 'IP Address' (containing 'fe80::20c:29ff:fe37:3729'), 'Subnet Prefix Length' (containing '64'), and 'Gateway' (containing 'fe80::20c:29ff:fe37:1'). A 'Save' button is located at the bottom right.

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

The next tab is PPPoE:



The screenshot shows the 'Config Home > Network > TCP/IP' interface. The 'PPPoE Config' tab is selected. Under the 'PPPoE Config' tab, there is a checkbox labeled 'Enable' which is currently unchecked. Below this, there are input fields for 'User Name' and 'Password'. A 'Save' button is located at the bottom right.

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 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.

4.6.2 Port

1. Go to “Network”→ “Port” to see the interface as shown below.

Port	Value
HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554

2. Input port number for IE access in the “HTTP Port” textbox.
3. Input the port number for audio & video transmission in the “Data Port” textbox.
4. Set the RTSP port for video/audio transmission over RTSP
5. Set the HTTPS port in case that you wish to use Secured HTTP connection.

4.6.3 Auto Report Server Configuration

Go to “Network”→ “Auto Report Server”.

Field	Value
Enable	<input type="checkbox"/>
Server Port	2009
Server Address	
Device ID	1

This section refers to “Auto Report Server”. Enable it if required.

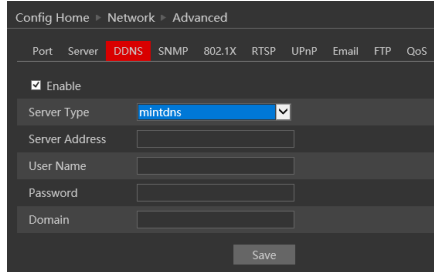
Auto report server will make the camera to report back to the defined Ossia VMS authentication server using the port 2009.

Set the port (default port is 2009. It is advisable not to change it.) Set the server address

(usually it is the Ossia VMS address which needs to be a static address or DDNS). Set a unique device ID. Each of the devices using auto server report should have its own ID. The Camera will report back to the defined server its current IP using port 2009.

4.6.4 DDNS Configuration

1. Enter into "Network"→"DDNS" tab as below:



Config Home > Network > Advanced

Port Server **DDNS** SNMP 802.1X RTSP UPnP Email FTP QoS

☒ Enable

Server Type: **mintdns** ▼

Server Address:

User Name:

Password:

Domain:

Save

4.6.5 SNMP

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. In order to Enable and work with SNMP, you need that the switch or another server on the network will support this protocol as well. Though our IPC fully supports SNMP will not explain how to configure it in this manual.

4.6.6 802.1X

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.

4.6.7 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
------	--------	------	------	--------	------	------	-------	-----	-----

☒ Enable

Port

RTSP Address

Multicast address

Main stream	<input type="text" value="239.0.0.0"/>	<input type="text" value="50554"/>
Sub stream	<input type="text" value="239.0.0.1"/>	<input type="text" value="51554"/>
Third stream	<input type="text" value="239.0.0.2"/>	<input type="text" value="52554"/>
Audio	<input type="text" value="239.0.0.3"/>	<input type="text" value="53554"/>

☐ Allow anonymous login (No username or password required)

Save

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

4.6.8 UPnP

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

Config Home > Network > Advanced

Port	Server	DDNS	SNMP	802.1X	RTSP	UPnP	Email	FTP	QoS
------	--------	------	------	--------	------	------	-------	-----	-----

☐ Enable

UPnP Name

Save

Then double-click “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.

4.6.9 Email Setting

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 Email that will be sent by the system,
Recipient Address	The email addresses that Emails generated by the system will be sent to.

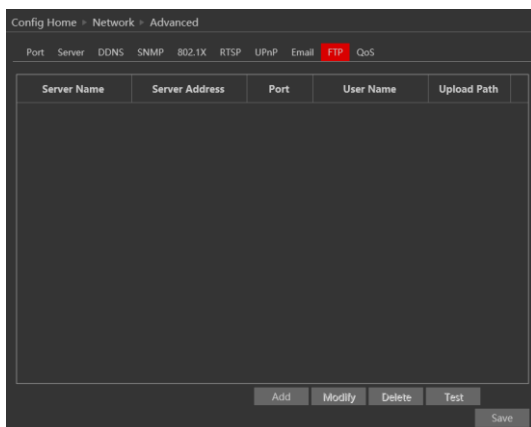
After all parameters are properly set up, you can click “Test” to confirm that the system can connect to the email server with the provided details. If an email sent successful, a “Test Successful” window will pop up, if not, you should try other email addresses or check and correct the settings.

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

Notice: 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.

4.6.10 FTP

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



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.

The 'Add FTP' dialog box contains the following fields and controls:

- Server Name: [Text Input Field]
- Server Address: [Text Input Field]
- Upload Path: [Text Input Field] (with 'Example/Dir/folder' as a placeholder)
- Port: [Text Input Field] (with '21' as a placeholder)
- User Name: [Text Input Field]
- Password: [Text Input Field]
- ☐ Anonymous
- OK button
- Cancel button

Click on “Modify” to edit the information of the FTP server

Click on “Delete” to delete the FTP server

Click on “Test” to confirm the setting and availability of the FTP server.

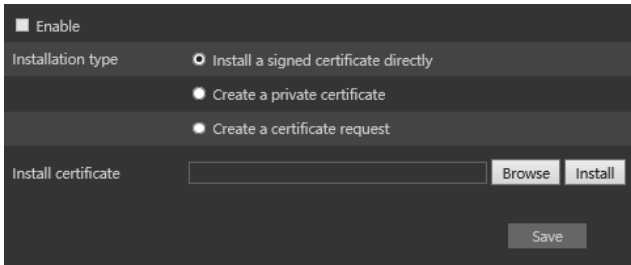
4.6.11 HTTPS

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 from 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 in order 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 about the SSL certificate and HTTPS connection.

Go to “Network” → “HTTPS”. interface as shown below. Enable the HTTPS if required. (Enabling HTTPS completely disables HTTP connection).



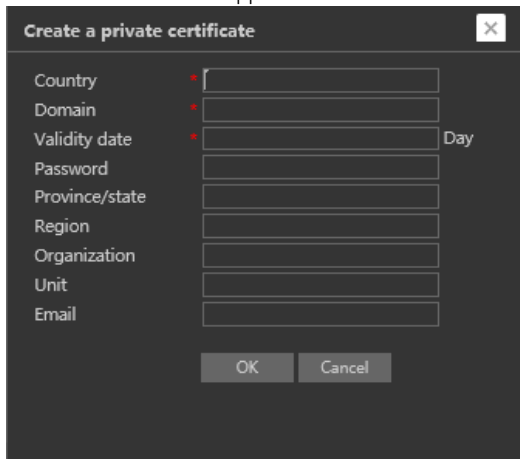
1.If you already have an SSL certificate in hand, choose “Install a signed certificate directly”. Click on “Browse” and choose your certificate. Click on “Install”, wait for the procedure to complete and click on “Save”

2. If you wish to use basic HTTPS connection, click on “Create a private certificate”. The

interface will update to:

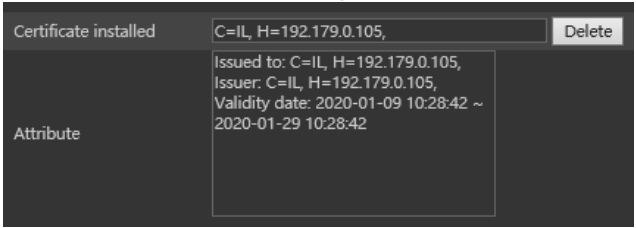
Create a private certificate Create

Click on “Create”. The interface below will appear.

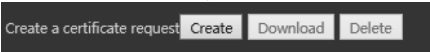


Input the details (The country field is set by 2 capital letters. For example for Israel the user should input "IL"). The fields marked with * are mandatory. All the rest are optional. Click on "OK". Once the procedure is finished, the SSL certificate will be automatically installed as follows.

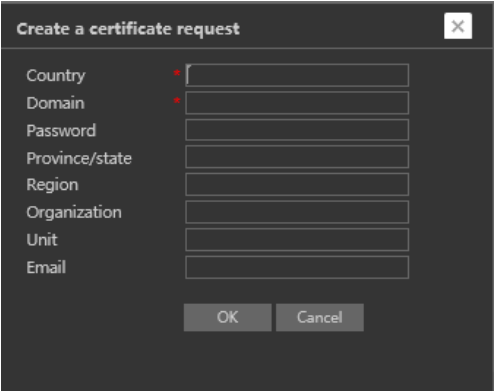
Please note: Using this method will display an error message by the browser everytime you connect to the camera, as the camera is not recognized as a certified SSL certificate issuer.



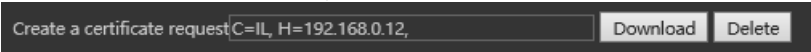
3. If you wish to create an SSL certificate with an issuer of your choice, choose "Create a certificate request". The interface will update to:



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



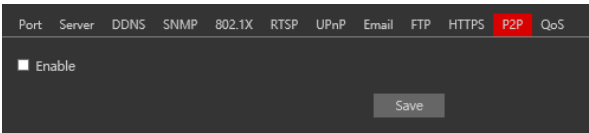
Input the details (The country field is set by 2 capital letters. For example for Israel the user should input "IL"). The fields marked with * are mandatory. All the rest are optional. Click on "OK". The interface will update.



Click on "Download". A file called "svrCert.pem" will be downloaded. Submit this file to the certificate issuer when required. When you receive the final certificate from the issuer, install it by choosing "Install a signed certificate directly".

4.6.12 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”



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

4.6.13 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.

4.1 Security

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

4.1.1 User

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

Config Home - Security - User			
Add Modify Delete			
Index	User Name	User Type	Bind MAC
1	admin	Administrator	

Adding a user:

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

Input the username, password and confirm the password.

Set the user type. 3 user types are available:

- A. Administrator – Can perform all action and settings on the camera.
- B. Advanced user – Can view and configure the camera excluding the “User Access” section.
- C. 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”

Modify user:

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

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.

You can also bind a MAC address for the user as explained in the “Add user” section.

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.

Note: The default user “admin” cannot be deleted.

4.1.2 Online Users

“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.

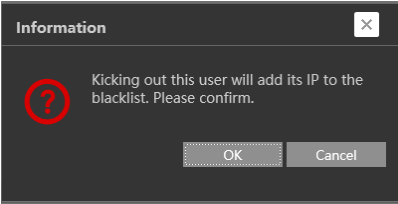
Go to “Network” → “Online Users” to access the following interface.

Config Home - Security - Online User

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

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.



Important Note: once the user is kicked out, the IP address used for connection will be blacklisted. 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.

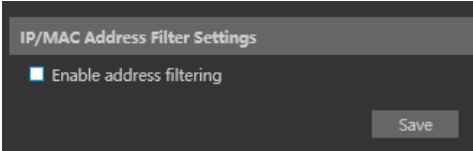
4.1.3 Block and Allow Lists

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

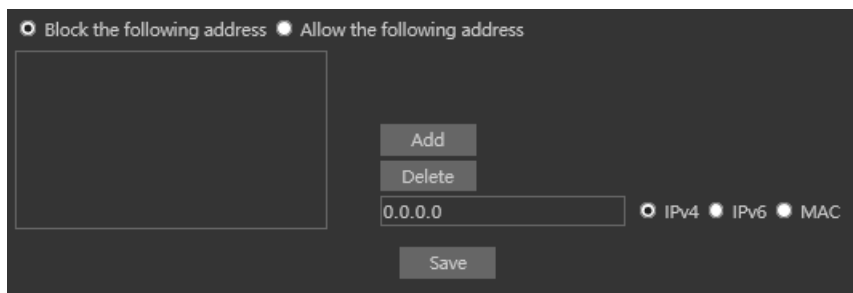
Once a “Block” list is created, all devices except the blocked devices will be allowed to connect to the camera.

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.



The lists can be based on IP Only / MAC only / Both IP and MAC together.



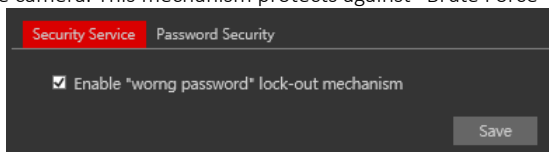
Enable the filtering you wish to activate. For the demonstration, we will enable both IP and MAC filtering, so the instructions below are true for both.

- 1) Choose the type of list you wish to create (block or allow)
- 2) Input the IP/MAC address you wish to add to the list
- 3) Set whether the input is IPv4/IPv6/MAC address
- 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.

4.1.4 Security Management

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

“Security Service” enables a mechanism that locks the IPC to incoming connection after 3 wiring attempts. Releasing the camera from a locked state is by waiting the lock duration or hard rebooting the camera. This mechanism protects against “Brute Force” attack.



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

Password level divides to 3 levels:

- 1) Low: No Requirements.
- 2) Mid: Minimum of 8 characters. Contains at least one number and one character.
- 3) 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 for a password change. The current password cannot be reused. Older passwords are not kept and can be used again.

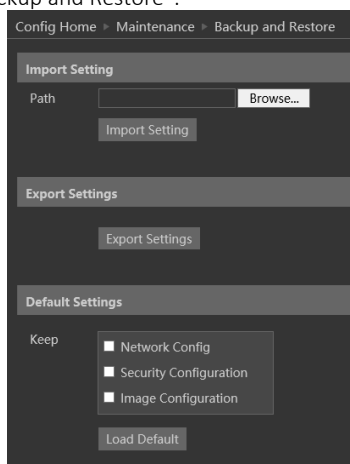
4.2 Maintenance

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

4.2.1 Configure 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 uniformed. This section also allows you to restore the camera's setting to factory default with some exceptions.

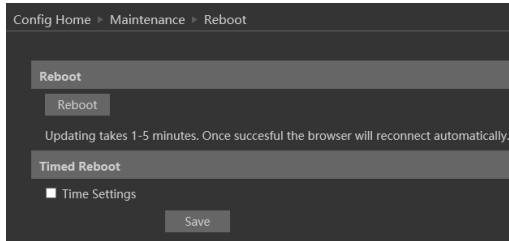
Go to "Maintenance" → "Backup and Restore".



- **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 on 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 configuration that will be saved:
 - **Network Config:** Will save all the network section configuration
 - **Security Configuration:** Will save all the security section configuration.
 - **Image configuration:** Will save the image section configuration.

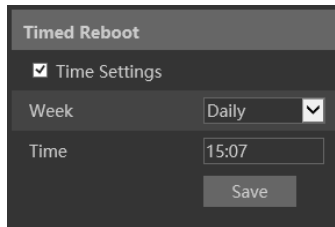
4.2.2 Reboot Device

Go to “Maintenance”→”Reboot” to see the interface as shown below.



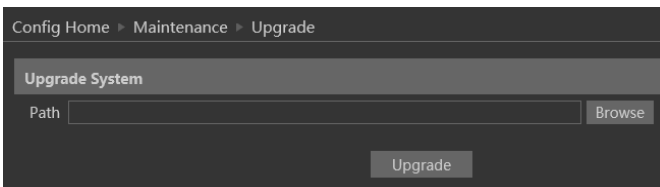
In order to reboot the IPC click on the reboot “Reboot” button and confirm the pop up prompt message, then wait for the reboot process to finish.

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 on a daily basis. The reboot will occur on the specified day and time.



4.2.3 Upgrade

Go to “Maintenance”→”Update” to open the interface as shown below.



1. Click “Browse” button to select the upgrade file.
2. Click “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.

Notice:

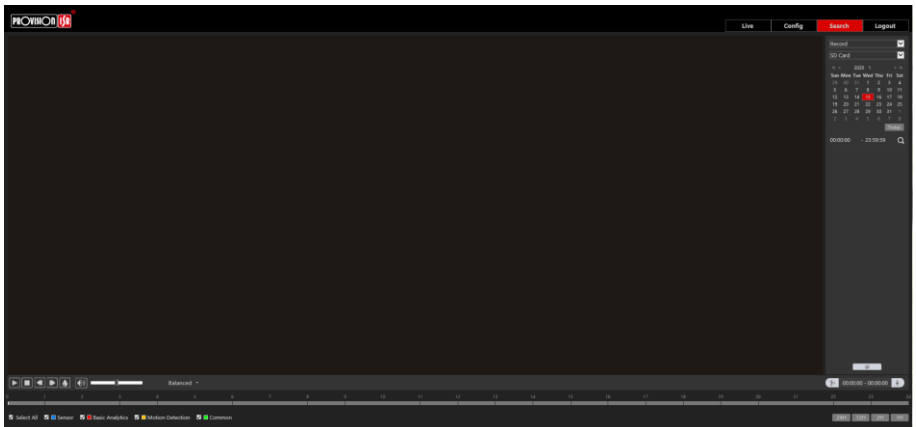
- 1) You must not disconnect to PC or close the IPC during the upgrade process to prevent permanent damage to the camera.
- 2) The camera update file is **.TAR. the “TAR” file should not be extracted.

4.3 Playback

Playing back videos taken by the camera have 2 options:

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

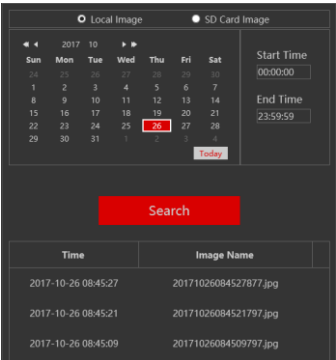
To access the playback interface, click on the “Search” Main tab. The interface below will appear.



- 1) First, you will have to choose which type of media you wish to search. On the left top corner choose from Photo and 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 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 ☒ Basic 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.



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












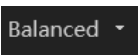


The playback controls are described below. Notice that it is different for Videos and Photos

• 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
	Fit the image to the screen		Dwell time between images
	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 previous file		Buffering mode selection

5 Mobile Surveillance

This IPC supports mobile surveillance from internet browsers and iOS/Android mobile phones using Provision-ISR's application "Provision Cam2"

5.1 Network Configuration

- **Access the device via LAN**

Step 1: Connect device via a wireless router. Then checkmark DHCP both in router and device to automatically acquire IP address or enter the IP address manually.

Step 2: Use WIFI function on your mobile phone to connect the wireless router.

Note: Make sure your phone network and device network are on the same network segment on LAN.

Step 3: Add the IP address and port in the mobile phone surveillance client.

- **Access the device via 3G network**

Step 1: Set the device network. Please enter Main Menu→Setup→Network tab.

▶ If you use PPPoE to connect the device, please enable PPPoE and input username and password received from your ISP in network tab. Then click "Apply". You can enter Main Menu→Information→Network tab to see the IP address. If you want to utilize dynamic domain name, please apply for a domain name in a DNS server supported by the device.

▶ If you have a static WAN IP address, please enter Main Menu→Setup→Network tab to input your IP address, gateway, and port.

▶ If you use LAN IP address, please enter Main Menu→Setup→Network tab to input your IP address, gateway and port and then forward IP address and port number in virtual server setup of the router or virtual server(If you have enabled the UPnP function in both the device and router, you can skip this step). Port forwarding setting may be different in different routers and servers. Please refer to the router's manual for details. After you forward your LAN IP address and port, please check the WAN IP address of the router or server.

Step 2: Add the WAN IP address or domain name in mobile phone surveillance client.

6 Appendix I : Analytics Configuration Requirements

6.1 General

Provision-ISR's IPC analytics supports a variety of analytics capabilities as follow:

New Generation (DDA Analytics):

Starting from v5.0

- 1) Object Counting (Based on DDA Object Detection)
- 2) Line Crossing (Based on DDA Object Detection)
- 3) Sterile Area (Based on DDA Object Detection)
- 4) Face Detection.
- 5) Face Recognition
- 6) Camera Tampering

S-Sight v2: Basic camera Tampering / Pixel-Based Line Crossing & Sterile Area

Eye-Sight v2: Basic camera Tampering / DDA AI Line Crossing, Sterile Area, People Counting and Face detection

Pre-installation requirements:

Please follow the requirements below to get the best analytics results:

- 1) Check the visibility, from the camera point of view.
- 2) Select the best place which covers the area you wish to protect.
- 3) Connect the camera to a stable base. Shaking and vibrations reduces accuracy and might generate false alarms.
- 4) Avoid reflective surface areas, such as shiny floor or mirrors.
- 5) Select bright area with different background colors than the objects colors.
- 6) The camera height depends on the actual focal length of the lens.

Lens	Mounting Height
2.8mm	2.6 ~ 3.2m
3.6mm	3.3 ~ 5.0m

Now we will go to specific installation requirements for each of the analytics capabilities:

6.2 Camera Tampering (Camera shifting / Lens tampering / Camera masking)

This Analytics is designed to detect physical damage to the camera that might prevent it from protecting its designated area. It will alert against any changes that occurred in the camera after its initial installation and include:

1. Camera shifting: In case the camera was forcibly moved out of place so it wouldn't cover the required area.
2. Camera Masking: Detects if the camera was covered or tampered in a way that blocks its view.
3. Lens Tampering: Detects lens tampering causing blurred image.

Configuration requirements:

There are no special requirements for the camera tampering analytics

6.3 Line Crossing

Detects if an object crossed a defined line. The crossing direction can be adjusted from each side of the line or from both sides.

Configuration requirements:

1. Select a bright area. Avoid constantly moving objects such as trees and scenes with many lighting changes.
2. The detection area should be well lighted and bright.
3. Install the camera at a height of 2.8 meters and more from the ground.
4. Install the camera at an angle of about 45 degrees from the ground.
5. The smallest detected object size shall not be smaller than 1 percent of the total scene.
6. The largest detected object size shall not be larger than 1/8 of the total scene.
7. **Make sure** that the object is displayed for at least two seconds for precise identification.

General Remarks:

1. Up to 4 lines can be set. Each line can be set with different configuration.

Inapplicable Scenes

1. Low Light Scenes.
2. Area with a lot of movements.
3. Area with frequently changing or uneven lights.
4. Low installation angle.



Low Light Scene – Inapplicable

– Low Light

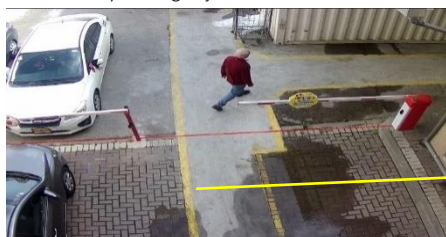


Area with many movements – Inapplicable

Inapplicable – Many moving object



Low Angle Installation – Inapplicable



Correct Installation

6.4 Sterile Area

This function is designed to use indoors. It is mainly used to detect motion in a protected area.

The alarm will be triggered within 3 up to 5 sec if someone enters into the detected area.

Configuration requirements:

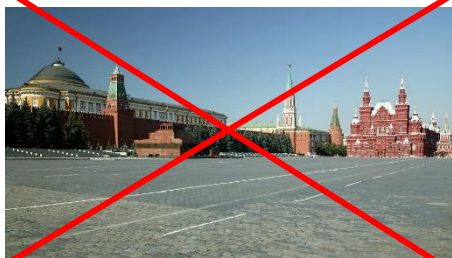
1. The defined area should be located under stable and uniformed lighting.
2. The camera must be installed at a height of 1 meter to 3 meters.
3. It is advised that the camera should be installed in the corner of the room.
4. The size of people/objects should be from 1/5 to 1/2 of the entire scene.
5. The defined area should preferably be less crowded and motionless.

General Remarks:

1. It is possible to define 4 different areas. The rules and requirements are the same.

Inapplicable Scenes

1. Outdoor Scenes.
2. Area with a lot of movements.
3. Area with frequently changing or uneven lights



Outdoor Scene – Inapplicable



High Traffic Scene – Inapplicable



Correct installation

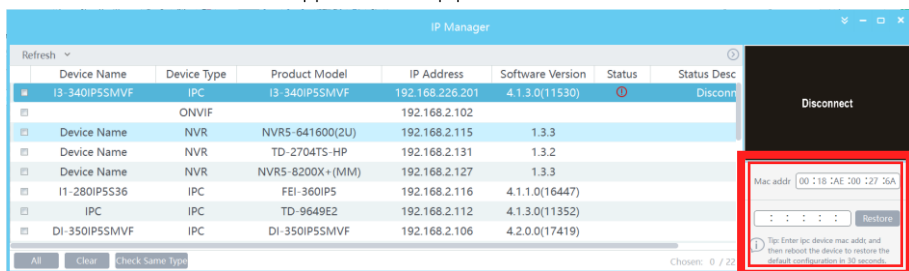
6.5 Q & A

1. Q: How to find my password if I forget it?

A: The default username is “admin” and the default password is “123456”.

If you have changed the password and you can't remember it, press and hold the physical reset button on the camera (If available) or use the IP Manager to reset the camera to factory default as follows:

- A. Open the IP Manager and locate the required camera.
- B. Click on the camera line in the IP manager.
- C. Input the MAC address of the camera into the restore window (The MAC address of the camera will appear in the op part of it:



- D. Click on “Restore”, and wait for the message “Device restored successfully”
- E. Disconnect the camera from power and reconnect it **within 30 seconds**.
- F. The camera will boot up in factory default.

Default IP: 192.168.226.201

User name: admin

Password: 123456

2. Q: The IPC fails to connect devices through IE browser, why?

A: Network cable is not connected well. Please check the connection and make sure it is connected securely to the camera.

B: IP was not assigned to an IP.

C: Web port number has been revised: contact an administrator or use the IP manager to get the correct port number.

D: If none of the above worked, recover the IPC's default setting by using the physical reset button on the camera (Press and hold if available) or using the IP Manager to reset the camera to factory default.

Note: Default IP: 192.168.226.201, mask number: 255.255.255.0

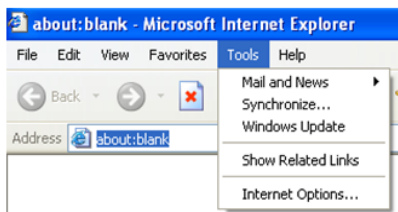
3. Q: IP tool cannot search for devices, why?

A: It may be caused by the anti-virus/firewall software on your computer. Please disable it and try to search device again.

4. Q: IE cannot download ActiveX control. How can I do?

a. Your IE browser probably set to block ActiveX controls. Please perform the following steps:

- ① Open IE browser. Click Tools-----Internet Options....



- ② Select Security-----Custom Level....Refer to Fig 4-1

- ③ Enable all the sub-options under “ActiveX controls and plug-ins”. Refer to Fig 4-2

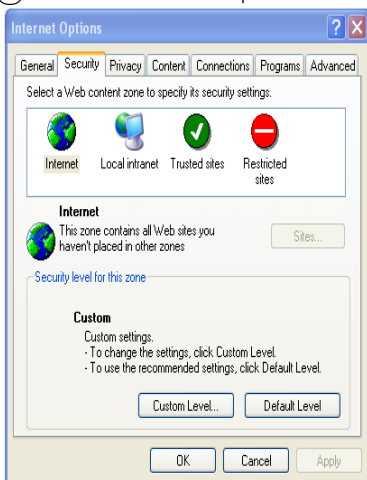


Fig 4-1

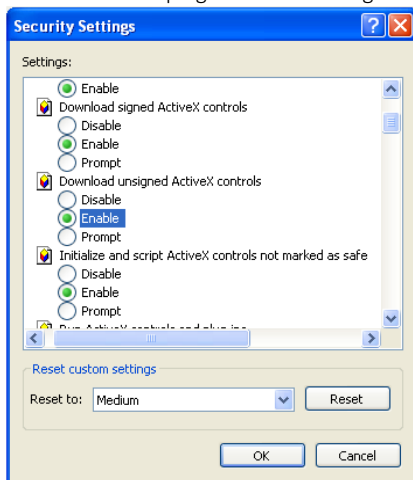


Fig 4-2

- ④ Click ok to finish setup.

b. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.

5. Q: No sound can be heard, why?

A: Audio input device was not connected. Please connect and try again.

B: Audio was not enabled in the live view interface. Please check the AUDIO item to enable this function.



Now you can see!



www.provision-isr.com

Technical Support: support@provisionisr.com

