



LPRN IP Cameras

User manual

Models:

- 220LPRN-MVF Cameras
- 240LPRN-MVF Cameras

Index

Index.....	2
1) Terms & Conditions	5
2) Camera Activation	7
2.1) IP Manager Tool:	7
2.2) Camera Web Page	7
2.3) NVR:	8
3) Remote Access.....	8
3.1) LAN	8
3.1.1) Access through the IP Manager Tool	8
3.1.2) Direct Access through Web-Browser	10
3.2) WAN.....	10
3.2.1) Direct Access through IP/DDNS	10
3.2.2) Access through NAT/P2P	11
4) Live Preview	12
4.1) Live View Interface	12
4.2) MVF (Motorized Vari-Focal) Controls	13
5) IPC Configuration.....	13
5.1) System Configuration	13
5.1.1) Basic Information	13
5.1.2) Date & Time Configuration	14
5.2) Local Config	15
5.3) Storage.....	15
5.3.1) Management:	15
5.3.2) Record	16
5.3.3) Snapshot	17
5.3.4) FTP Snapshot	17
5.3.5) Serial Port:	18
5.4) Image Configuration	18
5.4.1) Camera Configuration	18
5.4.2) Video/Audio	19
5.4.3) OSD Configuration	21
5.4.4) Video Mask	21
5.4.5) ROI Configuration	21
5.4.6) Zoom/Focus	22

5.5)	Alarm Configuration	22
5.5.1)	Motion Detection.....	22
5.5.2)	General Fault	23
5.5.3)	Alarm In	24
5.5.4)	Alarm Out.....	24
5.5.5)	Alarm Server	24
5.5.6)	Camera Tampering	24
5.5.7)	Audio Exception	25
5.6)	License Plate Detection	26
5.6.1)	Detection Config	26
5.6.2)	Schedule.....	27
5.6.3)	Linkage.....	27
5.6.4)	Comparison and linkage:	28
5.6.5)	Vehicle Database:	29
5.6.6)	OSD	31
5.7)	Network.....	31
5.7.1)	TCP/IP	31
5.7.2)	Port	33
5.7.3)	Auto Report	33
5.7.4)	ONVIF.....	33
5.7.5)	DDNS.....	33
5.7.6)	SNMP	34
5.7.7)	802.1X.....	34
5.7.8)	RTSP	34
5.7.9)	RTMP.....	35
5.7.10)	UPnP.....	35
5.7.11)	Email.....	36
5.7.12)	FTP.....	37
5.7.13)	HTTP POST.....	37
5.7.14)	HTTPS	38
5.7.15)	P2P	40
5.7.16)	QoS.....	40
5.7.17)	Cloud Upgrade	40
5.8)	Security	40
5.8.1)	User.....	40
5.8.2)	Online Users.....	42
5.8.3)	Block and Allow Lists.....	42
5.8.4)	Security Management.....	43
5.8.5)	Check Point Protection	44
5.9)	Maintenance.....	45
5.9.1)	Configure Backup & Restore.....	45
5.9.2)	Reboot Device.....	46
5.9.3)	Upgrade	46

5.9.4)	Debug Mode	47
5.9.5)	Device Information	47
6)	Playback (Search)	48
7)	Data Record	50
8)	Appendix I : Analytics Configuration Requirements	51
8.1)	General	51
8.2)	LPR (License Plate Recognition) Installation and Settings:	51
8.2.1)	General Pre-installation requirements:	51
8.2.2)	General Road Monitoring Installation:	51
8.2.3)	Parking Monitoring Installation:	52
8.2.4)	Default Image Settings	52
9)	Appendix II : Weigand	53
9.1)	General	53
9.2)	Connection:	53

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) 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 as described below.

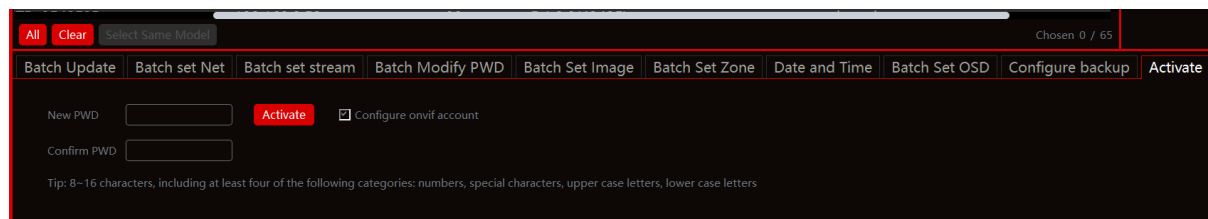
Please note:

- ❖ The activation password must contain at least 8 characters and include 1 letter, 1 number, and 1 special character
 - ❖ After the activation, the camera will reboot to apply the settings.
-

2.1) 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.

2.2) Camera Web Page

When browsing to the camera for the first time, it will take you through a configuration wizard which will include activation.

1. Approve the Privacy and terms of use.
2. Set your region.
3. Set the basic configuration: Frequency, Time zone, Date and time formats.
4. Set your recovery questions.

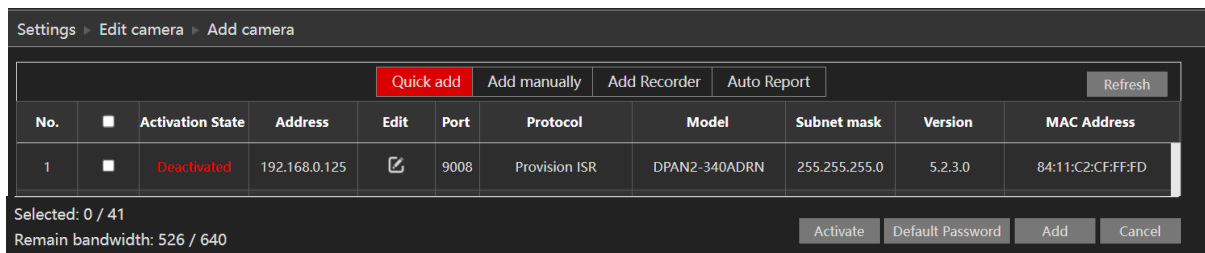
Please note:

- ❖ Skipping this step is possible, but if you lose your password and you don't have recovery questions set, you will have to fully reset the camera using the IP manager tool or the physical reset button on the camera.
-

- Set the new password for the camera. You can choose at this stage if to activate ONVIF user or not. If you are not planning to use ONVIF, it is advisable to disable it.

2.3) NVR:

- Cameras pending activation will show as “Disactivated” in the Activation state column.
- Choose the cameras you wish to activate, and click on “Activate”.
- You can choose a unique activation password, or use a preset activation password that will be used for all activations. Refer to the NVR user manual for more information.



3) 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.

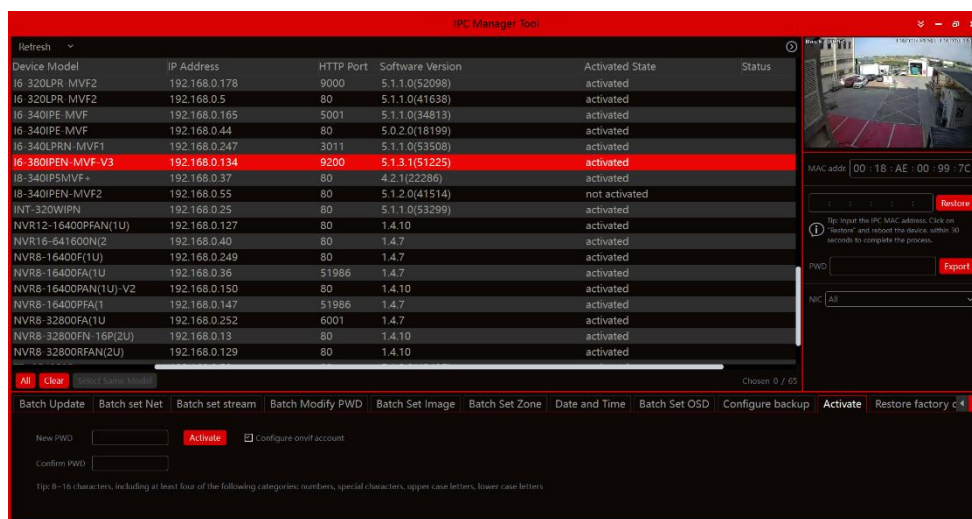
3.1) LAN

In LAN, there are two ways to access IPC:

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

3.1.1) 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.



5. 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.

The screenshot shows a web interface for IP configuration. At the top, there are four tabs: 'Batch Update', 'Batch set Net' (which is highlighted), 'Batch set stream', and 'Batch Modify PV'. Below the tabs, there are two radio buttons: 'IPv4' (selected) and 'IPv6'. Underneath, there are two options: 'Obtain automatically' (unselected) and 'Use the following:' (selected). Below these options are four input fields: 'Start IP', 'End IP', 'Subnet Mask', and 'Gateway'. Each field contains a placeholder IP address (e.g., . . .). At the bottom right, there is a red button labeled 'Batch Set'.

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.

Input the username and password to log in.

The screenshot shows a login window for 'PROVISION ISR'. The window has a grey header with the company logo. Below the logo, there is a large graphic of a camera and a globe. To the right of the graphic, there is a login form with the following fields: 'Name:' (text input), 'Password:' (password input), 'Stream Type:' (dropdown menu showing '3840x2160 25fps'), and 'Language:' (dropdown menu showing 'English'). Below the 'Language' field, there is a link that says 'Forgot Password?'. At the bottom of the form, there is a grey button labeled 'Login'.

3.1.2) 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.
 - a. Open the network and sharing center. Click “Local Area Connection”.
 - b. 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.
 - c. Open your preferred web browser, input the IP address of IPC and confirm. Input the default username and password and click “Login”.

3.2) WAN

3.2.1) 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.

IP Setup

Port Setup

- 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

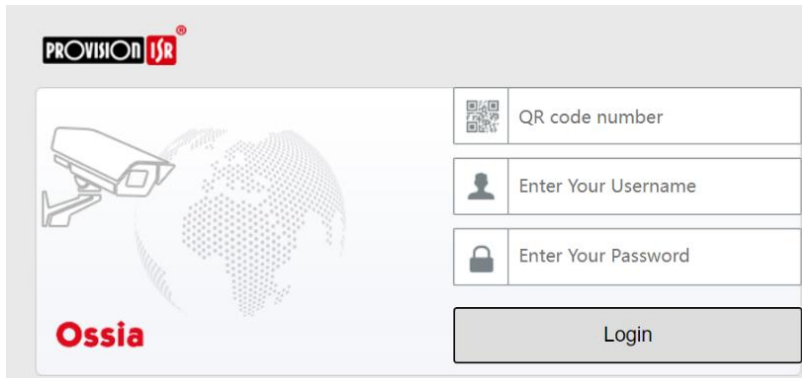
Data Port (Default is 9008) is for IE video data and SDK

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

3.2.2) Access through NAT/P2P

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

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



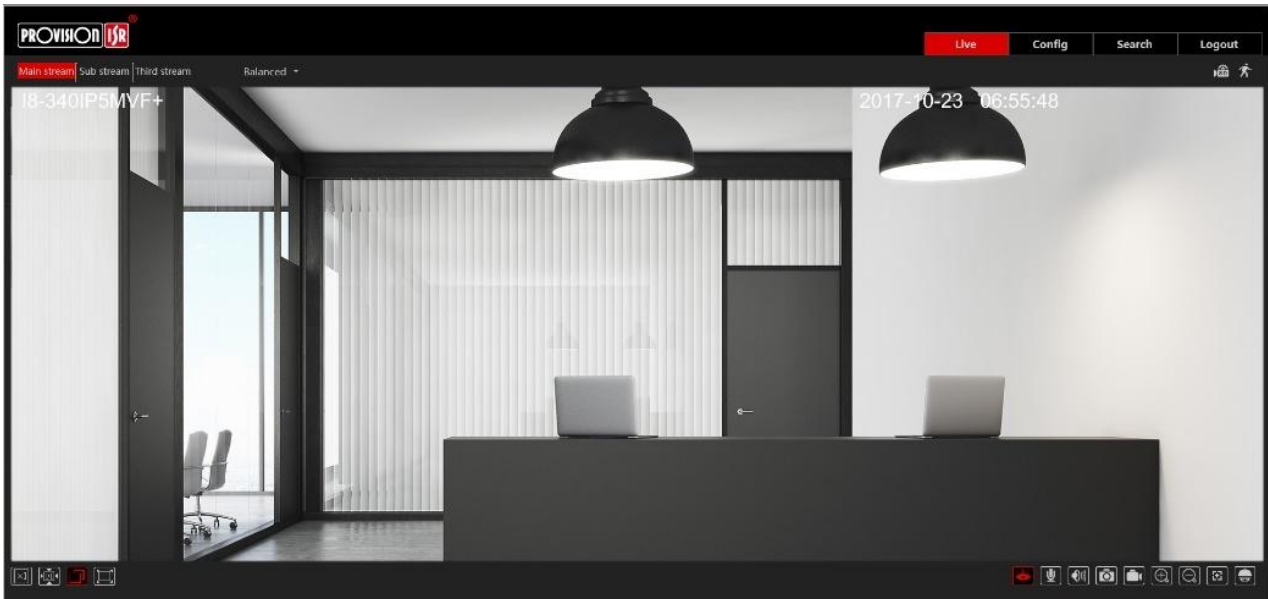
Input the QR code number, user name, and password, then click on "Login"

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
-

4) Live Preview

4.1) Live View Interface








Icons and operation buttons:

Icon	Description	Icon	Description
	Actual Video Size		MVF Controls*
	Fit to screen – True Proportions		Show/Hide Analytics Results
	Fit to screen - Stretch		Show/Hide analytics rules
	Full-screen		Check Point IoT protection Enabled/Disabled
	Measure Tool		Motion Detection indicator
	Enable/Disable live view		LPR Event Indicator
	Talk		SD Card recording indicator
	Listen		Alarm In Indicator
	Take Snapshot		Use mainstream for live-view
	Enable/Disable Local Recording		Use sub-stream for live-view
	Digital Zoom-in		Use third stream for live-view
	Digital Zoom-Out		Choose the buffering plan

4.2) MVF (Motorized Vari-Focal) Controls

Clicking on the MVF lens controls will unfold the MVF control panel. Using this interface, you can control the zoom and focus of the MVF lens.

The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Zoom Out		Focus In
	Zoom In		One Key Focus
	Focus Out		

5) IPC Configuration

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

5.1) System Configuration

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

5.1.1) Basic Information

In the “Basic Information” interface, you can view all the necessary information related to the IPC. 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
Firmware version	The current software version
Software build date	The software build-date
ONVIF Version	The current ONVIF version
OCX Version	The plug-in identifier
MAC	The MAC address of the device
Device ID and QR	QR Code used for P2P connection
S/N	Device serial number

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

Parameter	Explanation
Hardware version	The hardware version
Hardware ID	Hardware identifier
Build ID	The release identifier of the Firmware
Image Version	The image calibration version
Driver Version	The driver version.
Kernel version	The kernel version of the device
Web Version	The web UI version
Video Structured version	The AI engines version on the current firmware

You can also find the privacy statement as well as the open source code statement and usage.

5.1.2) Date & Time Configuration

Setting steps:

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

2. Set the time zone.
3. 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.
4. Refer to the “Summer Time” tab to 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.

5.2) Local Config

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

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 record audio, show the current bit-rate on the live-view image (Local interface only), and save the AI smart snapshots.

5.3) 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:

5.3.1) Management:

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

5.3.2) Record

Click on it to set the video recording parameters and schedule.

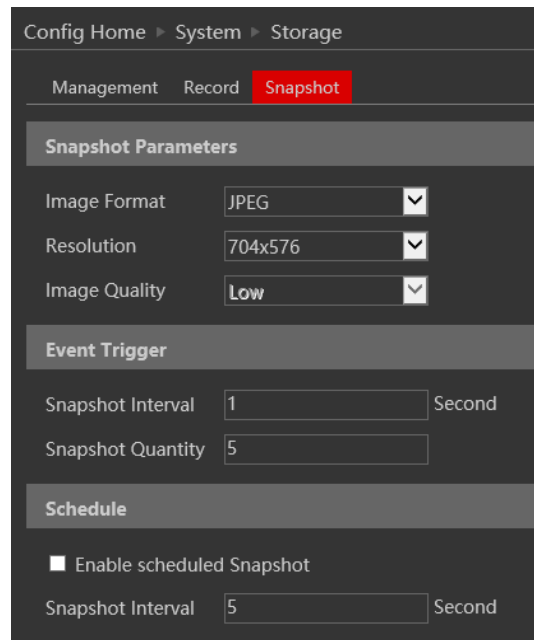
The video parameters are as follows:

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.

5.3.3) 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

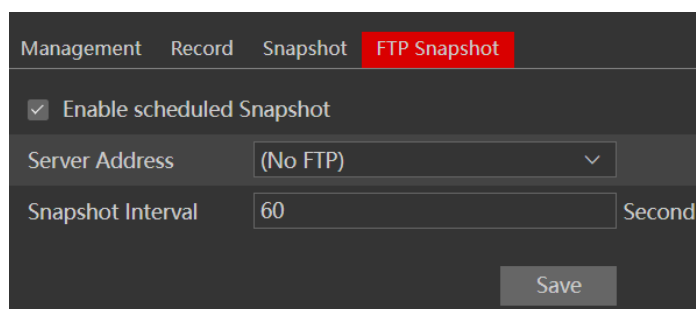
The snapshot parameters are as follows:

Parameter	Meaning
Image Format	The image format is JPEG
Resolution	Set the snapshot resolution
Image quality	The quality of the image reflects 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.

5.3.4) FTP Snapshot

You can set FTP Snapshots if you want to save time snapshots on remote FTP. Configure the FTP through the Network→FTP settings. Choose the FTP server you wish to send the images to and set the intervals between snapshots



Management Record Snapshot **FTP Snapshot**

☒ Enable scheduled Snapshot

Server Address: (No FTP)

Snapshot Interval: 60 Second

Save

5.3.5) Serial Port:

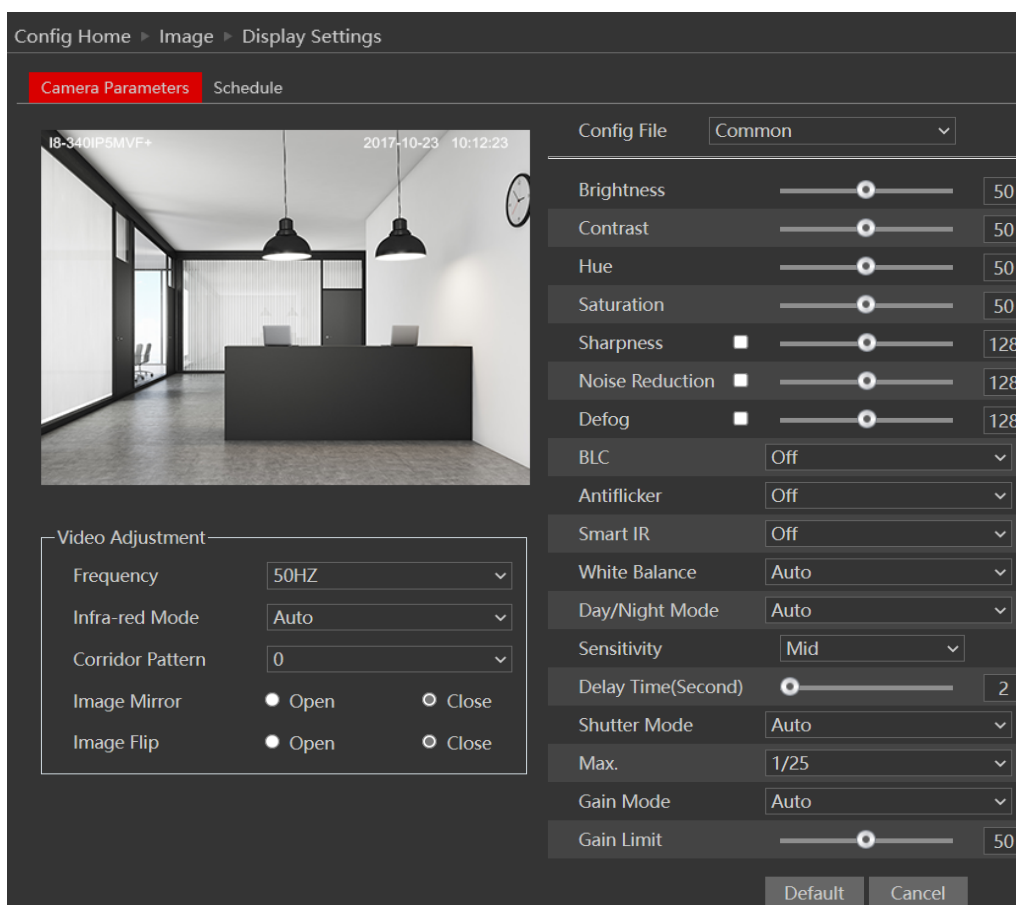
Control auxiliary devices using RS-485 protocol.

5.4) Image Configuration

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

5.4.1) Camera Configuration

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



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
Auto Iris	Enable/Disable the Iris motor (MVF Lenses only)

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
Smart-IR	Enable Smart IR function that prevents burnt pixels due to strong IR illumination.
White Balance	Set the white balance of the camera
Day/Night Mode*	Set the day/night mode (Auto/Day/Night/Schedule)
Sensitivity	The light sensor sensitivity
Delay Time	The delay time before switching day/night modes
Shutter Mode	Set the exposure to auto or set it manually
Max.	Maximum allowed shutter speed
Gain Mode	Set gain to Auto/Manual
Gain Limit	Set the Gain limit
HFR	Enable High Frame Rate (50/60FPS). Will reduce the resolution to 2MP and cancel HWDR if enabled.
Frequency	Set the frequency to 50/60Hz
Infra-Red Mode	Set the IR status
Corridor Pattern	Rotate the image to fit corridors
Image Mirror	Mirror the image horizontally
Image Flip	Flip the image vertically

*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.

5.4.2) 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	3840x2160	20	VBR	5120	Higher	40	H265	High Profile
2	Sub stream	704x576	6	VBR	128	Higher	12	H265	High Profile
3	Third stream	704x576	25	CBR	512	Medium	50	H265	High Profile

Send Snapshot: Sub stream Size: (704x576)

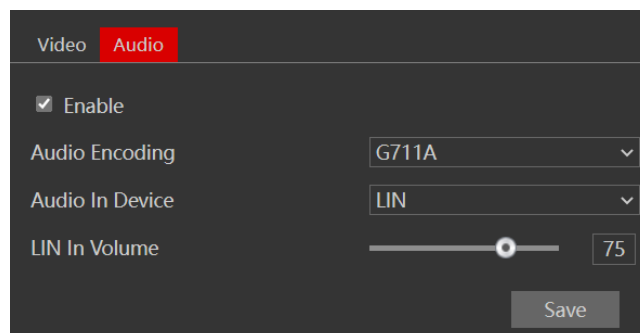
☐ Video encode slice split

☐ 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:



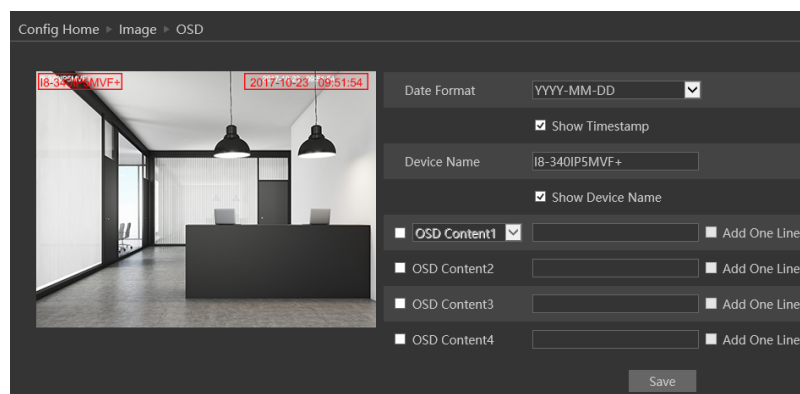
The audio input / built-in microphone is disabled by default. Enable it if you need audio input from the camera.

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”.

5.4.3) 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.



5.4.4) Video Mask

A video mask is used to cover areas that should be censored from the video images.

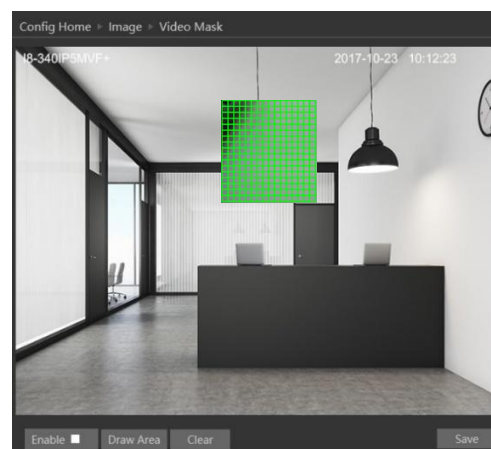
You can set 4 mask areas at most.

To set up a video mask

1. Enable video mask.
2. Click the “Draw” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live view to see the following picture.

To clear the video mask:

Go to the video mask menu and then click the “Clear” button to delete the current video mask area.



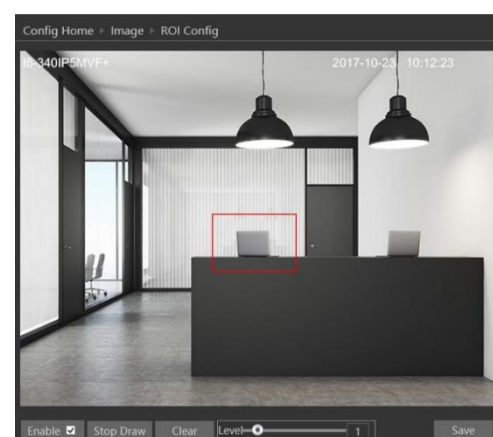
5.4.5) ROI Configuration

ROI is used to allocate a higher bit-rate on a certain area of the image than other areas

To set up ROI

1. Go to Config→ROI menu.
2. Check “Enable” and then click the “Draw” button.
3. Set the level.
4. Click the “Save” button to save the settings.

Now, you will see that the selected ROI area is clearer than other areas, especially in low bit-rate settings.



5.4.6) Zoom/Focus

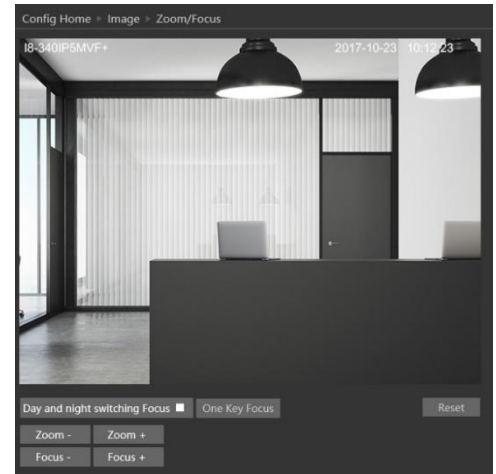
The zoom/focus interface is used for setting the lens of the camera (In MVF Models only).

You can also enable “Day/Night Switching focus” which will refocus the lens every time the camera switched from day to night and vice-versa.

“One Key Focus” will automatically focus the lens in one click.

Zoom +/- will manually control the zoom ratio.

Focus +/- will manually set the focus of the lens.

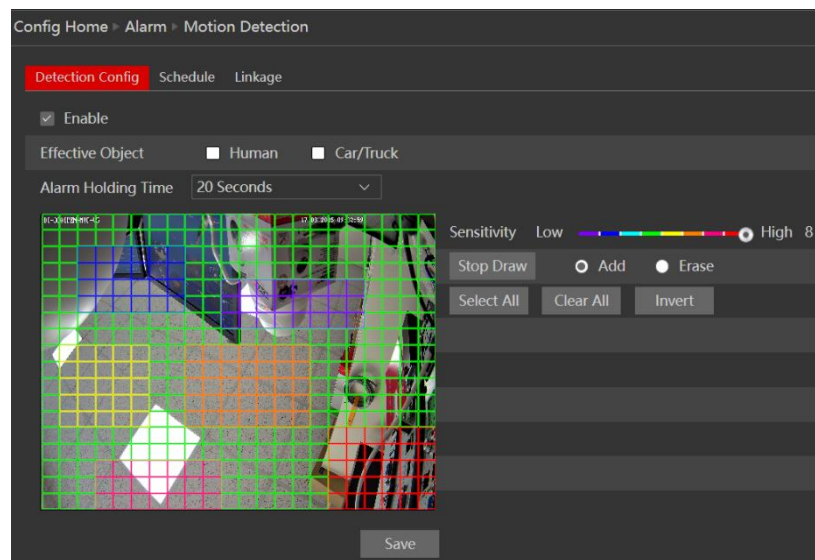


5.5) Alarm Configuration

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

5.5.1) Motion Detection

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



The first tab is the “Detection Config”.

1. Enable or disable the alarm.
2. Set the SMD if required. SMD (Smart motion detection) will search for shapes similar to the marked objects. It is not as accurate as AI, but will reduce false motion alarms and will appear as motion events.
3. 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.

4. 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”.
5. Browse to the schedule tab and set the required schedule.
6. Browse to the Linkage tab and choose the camera’s response to the alarm as explained below:

Alarm Triggers:	Explanation:
Trigger Audio Alarm	Triggers an audible alarm through the audio out interface
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card 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
Trigger Alarm Out	Activates the alarm output

7. Click “Save” to save the settings.

5.5.2) 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 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”.

5.5.3) Alarm In

Alarm input is a physical 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.

5.5.4) 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

5.5.5) 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.

5.5.6) 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:
2. Enable the required detection analytics out of Camera Shifting/Lens Tampering/Masking detection.
3. Set the sensitivity. (0 – lowest, 100 – Highest)
4. Set the Alarm linkage as follows:

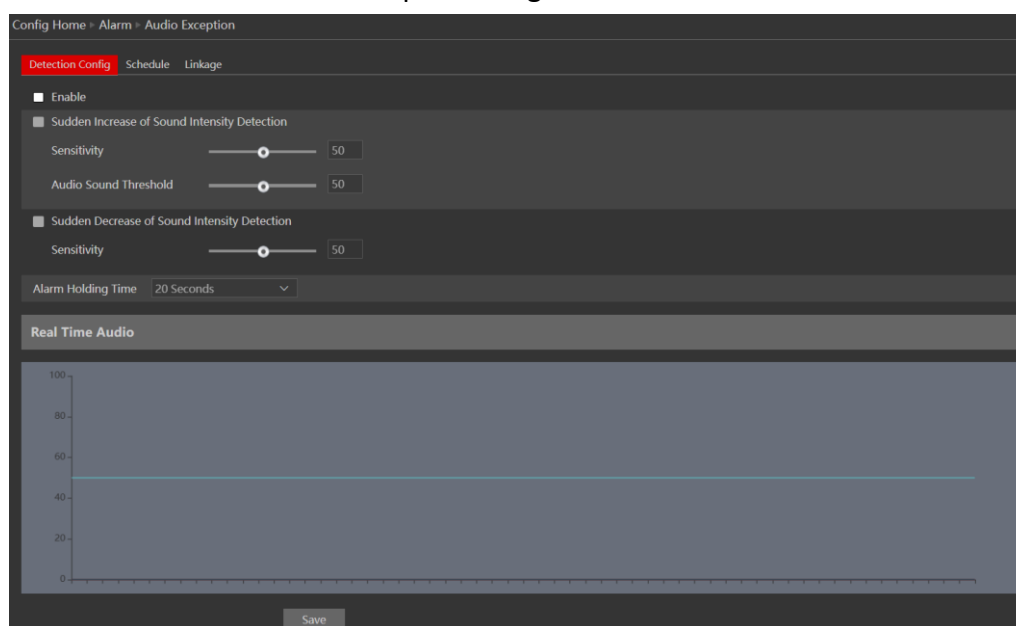
Alarm Triggers:	Explanation:
Trigger Audio Alarm	Triggers an audible alarm through the audio out interface
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email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

5. Click “Save” to confirm.

5.5.7) Audio Exception

Audio Exception is used to detect unusual audial behaviour.

- Go to “Alarm” → “Audio Exception” to get to the interface as shown below:



- Enable the required detection: Sudden increase of sound or Sudden decrease of sound. Use the realtime audio bar to set the audio threshold.

Please note:

- ❖ Audio must be enabled for this feature to work.
-

- Set the schedule as required.
- Set the Alarm Linkage as follows:

Alarm Triggers:	Explanation:
Trigger Audio Alarm	Triggers an audible alarm through the audio out interface
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card 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
Trigger Alarm Out	Activates the alarm output

- Click “Save” to confirm.

5.6) License Plate Detection

The LPR cameras are dedicated for License plate recognition. As part of the LPR AI engine, there is also a Metadata engine to recognize and classify the vehicle. It is an integral part of the LPR.

5.6.1) Detection Config

1. Go to “Analytics” → “License Plate Detection” to get to the interface as shown below:

Config Home » Analytics » License Plate Detection

Detection Config | Schedule | Linkage | Comparison and Linkage | Vehicle Database | OSD

☒ Enable

☒ Save Original Picture To SD Card

☒ Save Object Picture To SD Card

License Plate Detection Area: Asia / ישראל

☐ Capture Plate Absence Vehicle

Alarm Holding Time: 1 Seconds

Recognition Mode: Always

☒ Deduplication Period: 1 Seconds

License Plate Exposure: ☒ [Slider: 8]

16:20:10 PM 18-11-2024

Alarm Area

Detection Area: 1 ☒

Blocked Area: 1 ☐

Object Size

Min Width: 3 % Height: 3 %

Max Width: 50 % Height: 50 %

Draw Area | Clear | Draw Object Size

Save

2. Enable the Alarm if required.
3. Set whether to save the scene image or the object image to the SD Card.
4. Set the license plate region. It is important to choose the correct region since different regions have different sizes and letter shapes.
5. Choose if you want to detect Vehicle without valid license plates.
6. Set the recognition mode:
 - a. Always: The camera will respond to any license plate detected in the detection area
 - b. Only approaching vehicles: The camera will respond only to license plates approaching to it.

- c. Only leaving vehicles: The camera will respond only to license plates moving away from it.

Please note:

- ❖ The detection of approaching/leaving vehicles is done based on the location of the license plate on the image “Y” axis, and will work better on straight roads. If the vehicle is turning while moving towards/away from the camera, this detection method might not work as expected.
-

7. Set the deduplication if required. Disabling deduplication means that a license plate will only be detected and processed **once** as long as it is visible to the camera. If the deduplication is enabled, the license plate will be detected and processed repeatedly based on the set intervals as long as it is visible to the camera.
8. License plate exposure: Gives more weight to the license plate area when setting the auto exposure.
9. Now you will have to set the detection area.
10. Click on “Draw Area”.
11. Draw the polygon. The polygon supports up to 6 junctions.
12. Click “Save” to confirm the settings.
13. You can also set a “Blocked Area”. This area will not recognize objects. If a detection area and a blocked area overlaps, the blocked area will have higher priority.
14. You can set up to 4 block areas. If needed, select the next blocked area number and draw it again.
15. Set the minimum and maximum object size
16. Click “Save” to confirm the settings.

5.6.2) Schedule

1. Click on the “Schedule” tab.
2. Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add the required dates to it. The holiday schedule overtakes the normal schedule.

5.6.3) Linkage

1. Click on the “Linkage” tab.
2. Set the Alarm Linkage as follows:

Alarm Triggers:	Explanation:
Trigger Audio Alarm	Triggers an audible alarm through the audio out interface
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card 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
Trigger Alarm Out	Activates the alarm output

5.6.4) Comparison and linkage:

1. Click on the “Comparison and Linkage”

Config Home > Analytics > License Plate Detection

Detection Config Schedule Linkage **Comparison and Linkage** Vehicle Database OSD

Allow misread digit(s) 0

Set Similar Digits

Alarm Trigger Mode License Plate

Wiegand Size WIEGAND_26_BYTE_10

Allow List Block List Temporary vehicle Unrecognized No Plate

☒ Alarm Out

☐ Wiegand Output Access Card Number

Save

2. Allow misread digit(s): This setting allows to consider a license plate to match the database even if 1 or 2 digits are missing or wrong.
3. Set similar digits: In some countries there are similar digits (l/1, 0/O, Etc.). It is also possible that the LPR engine is not updated. In this interface you can set these corrections manually.

For example: The License plate in the database is 12345678

- a. The camera tolerance is 0 – meaning that only a reading of 12345678 will set a recognition trigger.
- b. The camera tolerance is 1 – meaning that 1 digit/character can be missing or read wrong, and the reading will still be considered as successful. For example: 2345678 / 1345678 / 1245678 / 12345673 Etc.

- c. The camera tolerance is 2 – meaning that 2 digit/character can be missing, and the reading will still be considered as successful. For example: 345678 / 145678 / 125678 / 123456733 Etc.

If you need to set it up, input 1 and 1 in the required fields and click on “Add”

4. Alarm Trigger Mode:

- a. License plate: License plates detected and found in the allow list will trigger an event
- b. License plate and parking card: Once a license plates from allow list is detected, a secondary authentication will be required in the form of parking card. This requires an RFID reader being available and connected to the camera Weigand port. Once both are valid, the camera will trigger an event.

5. Wiegand Config: Set the Wiegand to 26bit or 34bit.

6. Database match trigger. Set the trigger for each one of the database groups:

- a. Alarm out: Will trigger the alarm output of the camera
- b. Weigand Output: will send the vehicle information through the wiegand port to an external controller
 - i. Access Card Number: The access card number from the database will be sent via the Weigand port
 - ii. License plate number (SHA1): A representation of the license plate number will be sent based on the SHA1 protocol.

5.6.5) Vehicle Database:

Click on the “Database” tab:

Config Home > Analytics > License Plate Detection

Detection Config Schedule Linkage Comparison and Linkage **Vehicle Database** OSD

Add Bulk Entry

License plate number List Type All Types Search Export

	Index	License plate number	Owner	Phone Number	Access Card Number	List Type	Start Time	End Time	Operate
<input type="checkbox"/>	1	664****3	98***	*	*	Allow List	01/01/2025 00:00:00	31/12/2036 00:00:00	
<input type="checkbox"/>	2	177****4	28*****	*	*	Allow List	01/01/2025 00:00:00	31/12/2036 00:00:00	
<input type="checkbox"/>	3	451****7	98***	*	*	Allow List	01/01/2025 00:00:00	31/12/2036 00:00:00	
<input type="checkbox"/>	4	587****1	1*****	*	*	Allow List	01/01/2025 00:00:00	31/12/2036 00:00:00	

Adding a single new vehicle:

Click on “Add” to add a single entry:

Add

License plate number List Type Allow List

Start Time End Time ☐ Valid Forever

Owner Phone Number

Access Card Number License plate type Save

1. License plate number (Mandatory): The vehicle license plate
2. List Type (Mandatory): Choose from "Allow", "Temporary" and "Block" lists
3. Validity (Mandatory): The valid duration of the vehicle. The vehicle will not be considered as valid outside this time frame. Set the start time and end time or set "Valid Forever"
4. Owner (Optional): Set the vehicle owner.
5. Phone number (Optional): Set the vehicle owner's phone number.
6. Access card (Optional): If you want to use Wiegand input/output based on Parking Access card, you need to input this value.
7. License plate type (Optional): Set the license plate type.
8. Click "Save"

Adding a multiple vehicles:

1. Click on "Bulk Entry"
2. Click on "Download" to download the CSV template.
3. Fill the template file based on the following explanation:
 - a. License plate number (Mandatory): A maximum of 12 characters supported.
 - b. Phone Number (Mandatory): A maximum of 14 characters supported.
 - c. Owner name (Mandatory): A maximum of 12 characters supported.
 - d. The effective start time (Mandatory): format: YYYY/MM/dd hh:mm:ss; time range is from 1970 to 2037.
 - e. The effective end time (Mandatory): format: YYYY/MM/dd hh:mm:ss; time range is from 1970 to 2037.
 - f. Vehicle type (Optional): A maximum of 12 characters supported.
 - g. List Type (Mandatory): 1 stands for block list; 2 stands for allow list; 3 stands for temporary vehicle.
 - h. Card Number (Optional): A maximum of 9 numbers supported.

Please note:

- ❖ Editing this file with Microsoft Excel tends to change the date/time format unexpectedly which will result in an error when uploading the file to the camera.
-

4. Click on "Choose File" and select the full template file.
5. Click on "Upload" to upload and save it.

Editing a vehicle:

1. Click on "Edit" on the bottom of the interface.
2. Click on "Modify" on the entry you wish to edit.
3. Edit the required fields and click on "Save"

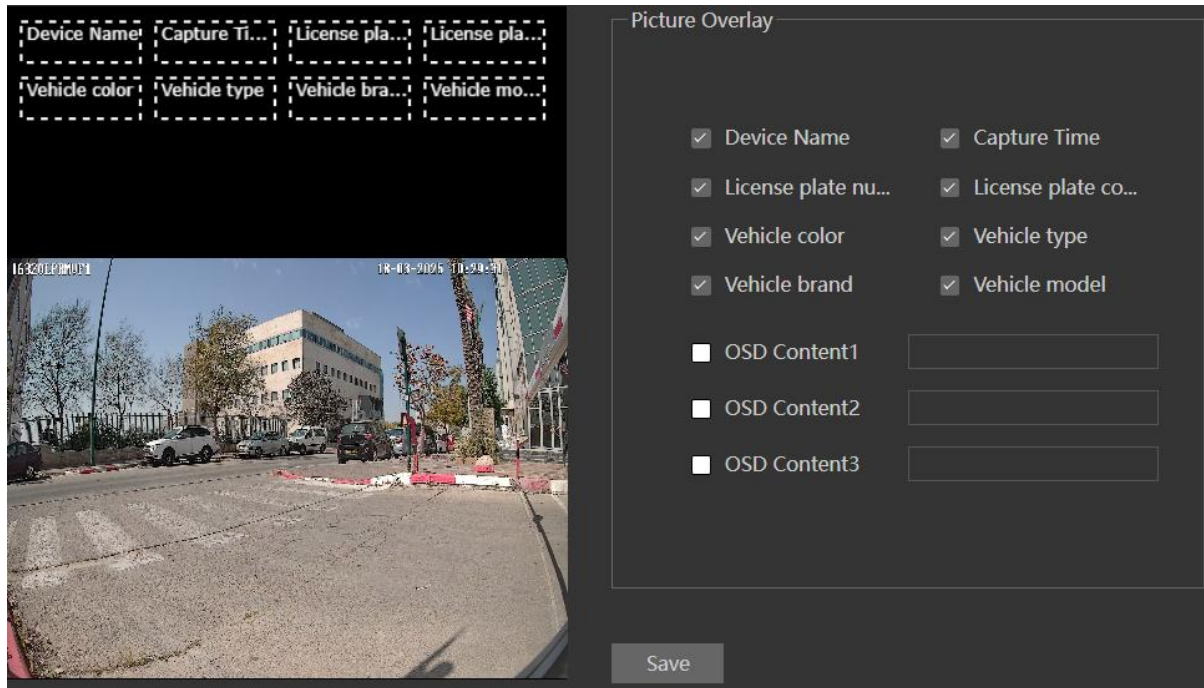
Deleting a vehicle(s)

1. Click on "Edit" on the bottom of the interface.
2. Choose the cameras you wish to update or input the number in the search field

3. Click on “Delete” and confirm.
4. “Batch delete” will delete all entries.

5.6.6) OSD

1. Click on the OSD Tab:

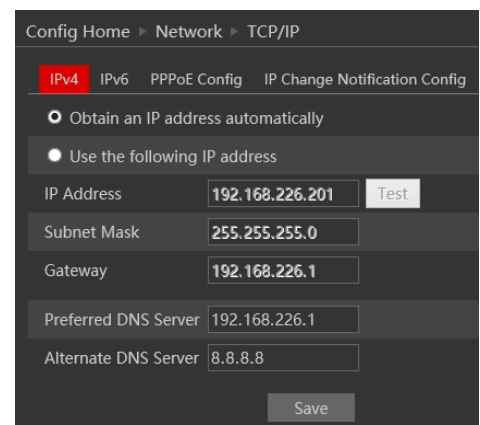


2. Choose the Metadata values you wish to be visible on the image when detected.
3. Click on “Save” to confirm.

5.7) Network

5.7.1) 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.



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.

The next tab is PPPoE:

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.

5.7.2) 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 9009) is for advanced integrations using long polling API.
5. WebSocket Port (Default is 7681) is for modern browser video streaming

Port	Auto Report	ONVIF	DDNS	SNMP	802.1X	RTSP
HTTP Port	80					
HTTPS Port	443					
Data Port	9008					
RTSP Port	554					
Long Polling Port	8080	<input checked="" type="checkbox"/>				
WebSocket Port	7681					

5.7.3) 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.

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.

The Camera will report back to the defined server its current IP using port 2009.

Config Home > Network > Advanced

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

☐ Enable

Server Port: 2009

Server Address:

Device ID: 1

Save

5.7.4) 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:

Port Auto Report **ONVIF** DDNS SNMP 802.1X RTSP RTMP UPnP Email FTP HTTP POST HTTPS

Add Modify Delete

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”. The following interface will pop up:

Set the username, password, and user type for the required user and click OK.

5.7.5) 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.

5.7.6) 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. 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 V1/2/3, we will not explain how to configure it in this manual. Please refer to SNMP common manuals for advances configuration.

5.7.7) 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.

5.7.8) 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.

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 has a unique RTSP address. Input the desired address into your RTSP player.
4. Notice that the camera also supports multicast addresses that can be used as well for supporting players.
5. Enabling “Allow anonymous login” will authorize RTSP connection without the need for a username/password.
6. Click “Save” to confirm and save settings.

5.7.9) RTMP

Real-Time Messaging Protocol (RTMP) is a communication protocol for streaming audio, video, and data over the Internet.

Unlike RTSP, once RTMP is configured, the camera will commence video streaming to the configured server as long as it is online.

4. Go to “Network” → “RTMP” interface as shown below

5. Enable if necessary
6. Set the video stream type (Main/Sub/Third-Stream)
7. Set reconnection time
8. Set the server address. Confirm that the server is listening at the specified address, otherwise, the status will remain “Not Connected”

Please note:

- ❖ RTMP only works with H.264 Encoding. Please make sure to configure it on both the IPC and NVR (If available).
-

5.7.10) UPnP

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

Select “Enable UPnP” and then input a friendly name.

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.

5.7.11) Email

Go to “Network” → “Email” interface.

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.

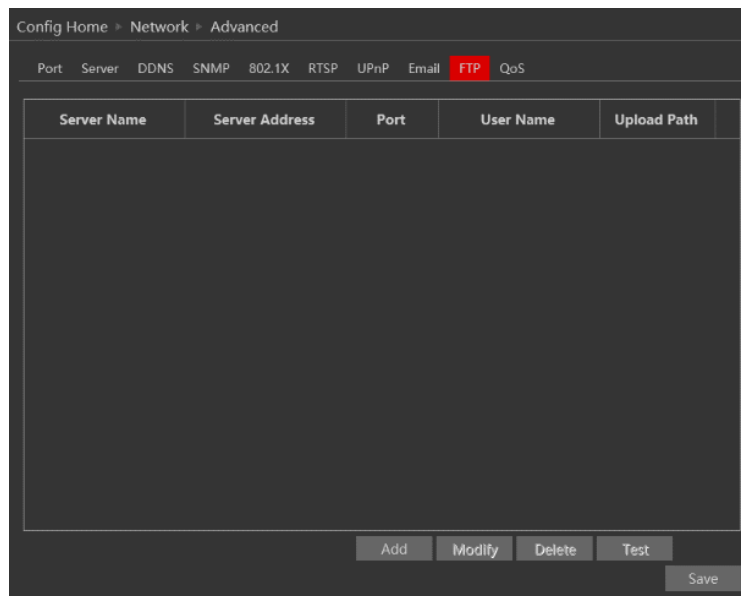
To input a new mail recipient, input the recipient address and click on “Add”. The new address will be added to the recipient list box.

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

5.7.12) 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, upload path, and connection protocol. 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.

5.7.13) HTTP POST

HTTP POST is used mainly for system integrations. Once enabled, the camera will send **selected 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.

5.7.14) 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).

If you want to install a certificate you already have, it should be in “crt” format. The certificate allows the IPC to encrypt data, but it will also need the private key in order to decrypt data. Please follow the steps below to avoid errors with the certificate.

1. Open your certificate (*.crt) file using a text editor such as Notepad or Notepad++
2. Open your private key (*.key) file using a text editor such as Notepad or Notepad++
3. Copy the content of the private key file and paste it above the content of the certificate file.
4. Save the edited certificate file as a copy and close both files.
5. Choose “Signed certificate already available. Install directly”, click on “Browse” and select the edited certificate file.
6. Click on “Import” to import the file.
7. If the certificate is protected by a password select “Encryption”, input the password and click on “OK”. Otherwise keep the selection on “Decrypted” and click on Ok.
8. Once you see the installed certificate with its details, click on “Apply”
9. 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:

Create a private certificate

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 every time you connect to the camera, as the camera is not recognized as a certified SSL certificate issuer.

5.7.15) 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 (<https://www.provisionisr-cloud.com>).

5.7.16) 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.

5.7.17) Cloud Upgrade

Cloud Upgrade allows you to update the IPC firmware directly from the cloud. Change the Upgrade Option to Notify Only to get notifications from the camera concerning.

You can manually check for available updates by clicking on the “Manual Check”.

If there is an available update, click on “Upgrade” to apply it.

5.8) Security

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

5.8.1) User

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

Config Home » Security » User		
<div> Add Modify Delete Security Question </div>		
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”

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

5.8.2) 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 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.

5.8.3) 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

Add
Delete

☐ IPv4 ☐ IPv6

Save

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.

5.8.4) 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.

The screenshot shows the 'Security Management' configuration page with the 'Security Service' tab selected. It features a dark theme. At the top, there are three tabs: 'Security Service' (highlighted in red), 'Password Security', and 'Authentication'. Below the tabs, there are three settings: 'Enable "Wrong password" lock-out mechanism' with a checked checkbox, 'Trigger Email' with an unchecked checkbox, and 'Logout Time' set to '3600' with a unit dropdown set to 'Second'. A 'Save' button is located at the bottom right.

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.

The screenshot shows the 'Security Management' configuration page with the 'Password Security' tab selected. It features a dark theme. At the top, there are three tabs: 'Security Service', 'Password Security' (highlighted in red), and 'Authentication'. Below the tabs, there are two settings: 'Password Level' with a dropdown menu set to 'strong', and 'Expiration Time' with a dropdown menu set to 'Never'.

Password level divides into 3 levels:

10. Low: No Requirements.
11. Mid: Minimum of 8 characters. Contains at least one number and one character.
12. 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.

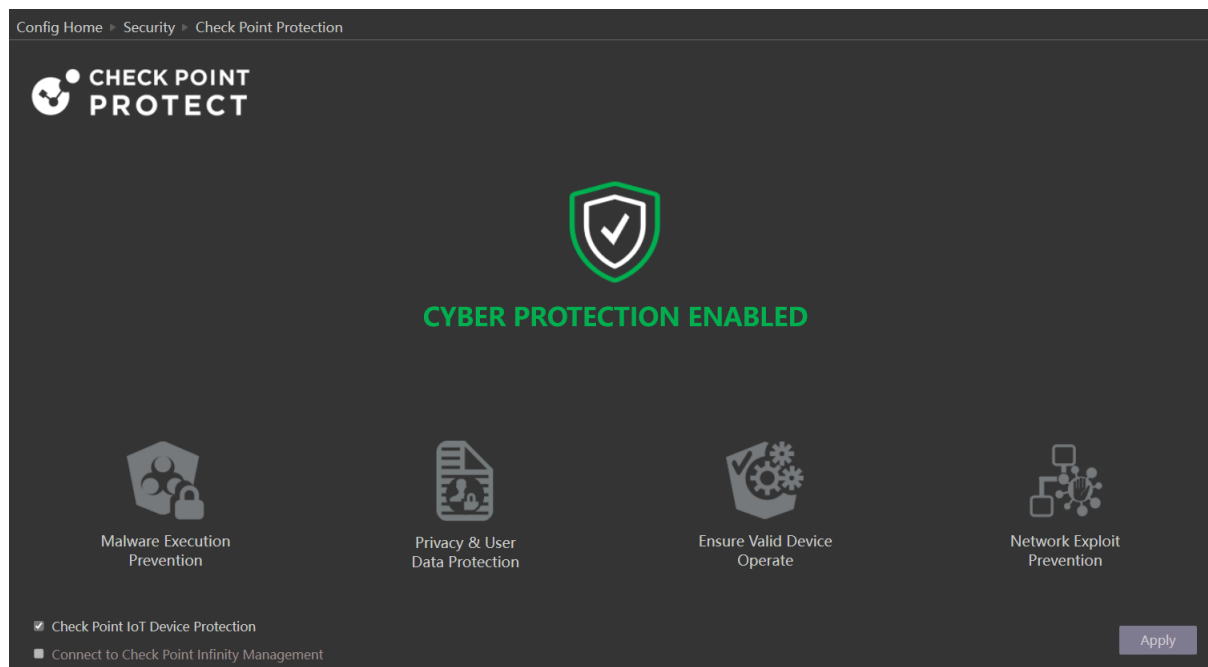
“Authentication” is used for API HTTP login.

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

5.8.5) Check Point Protection

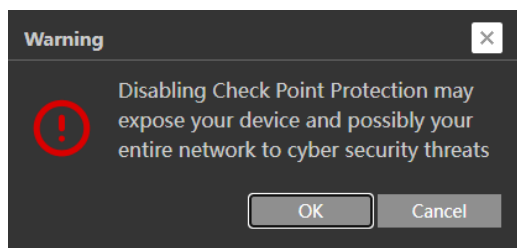
Check Point IoT Protect Nano agent is a dedicated real-time runtime cyber protection layer provided by Check Point®.

Click on Settings→Security→Check Point Protection to open the following interface:



Disabling the protection:

1. Untick “Check Point IoT Device Protection”
2. The following message will pop up



3. Confirm that you wish to proceed.
4. Click “Apply”
5. Input the admin password and confirm again.

Please note:

1. It is highly advised to keep the IoT Protect enabled at all times.
2. Disabling Check Point protection may expose your device and possibly your entire network to cyber security threats

5.9) Maintenance

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

5.9.1) 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 uniform. This section also allows you to restore the camera's setting to factory default with some exceptions.

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

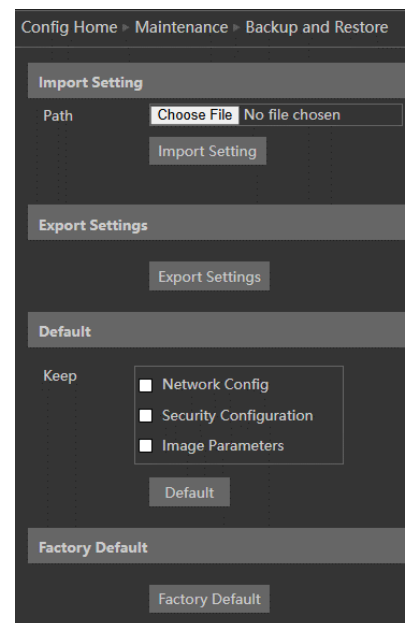
Importing Settings: If you have a configuration file and you wish to import it to the camera, click on "browse" and choose the relevant config file.

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.

Default: Load default settings of the camera while keeping the basic settings configured. Notice that you can mark some configurations that will be saved:

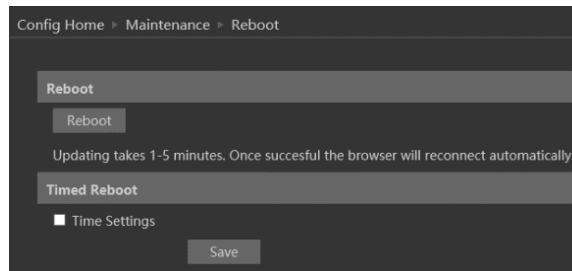
1. Network Config: Will save all the network section configuration
2. Security Configuration: This will save all the security section configurations.
3. Image configuration: Will save the image section configuration.



Factory default: If for any reason you wish to restore your camera settings to factory default, you can use the "Factory Default" button. It will revert all settings and configurations back, and completely reset the camera.

5.9.2) Reboot Device

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

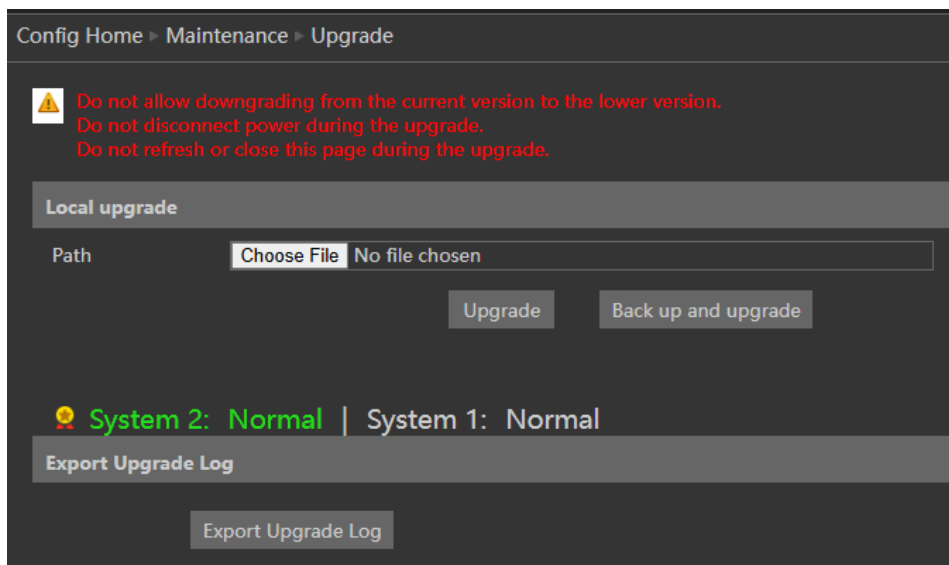


To reboot the IPC, click on the reboot “Reboot” button and confirm the pop-up prompt message, then wait for the reboot process to finish.

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.

5.9.3) Upgrade

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



1. Click the “Browse” button to select the upgrade file.
2. Click the “Upgrade” button to start the upgrading process of the IPC. You can select “Backup and upgrade” in order to back up the camera’s configuration before the update process.
3. The device will restart automatically once completed.

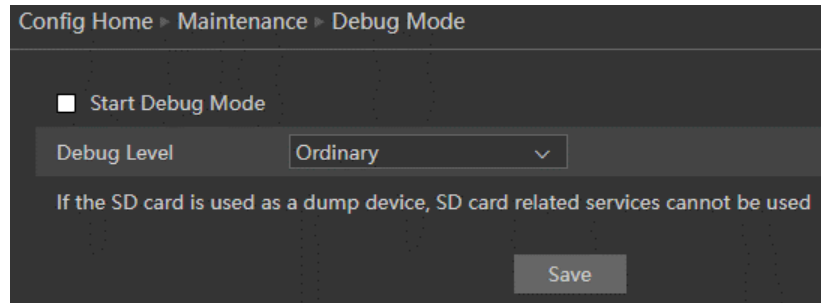
Please note:

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 *.pkg.
-

5.9.4) Debug Mode

The debug mode allows you to extract valuable technical information regarding the camera operation in order for the technical support and R&D to understand better bugs and faults with the camera's operation.

Go to "Maintenance" → "Debug Mode" to open the interface as shown below.



1. Insert an SD Card to the camera and format it.
2. Choose the Debug level advised by the technical team.
3. Select the "Start Debug Mode" and click on Save.
4. Once the issue was reproduced, eject the SD Card and send its content to the technical team

Please note:

1. The SD Card will be formatted and overwritten as part of this operation. If you have record and snapshot data on the SD Card, please replace it before enabling this option.
 2. Removing the SD Card without properly ejecting it from the SD Card interface will corrupt its content, and make it unuseable.
-

5.9.5) Device Information

Use this option to export full device information and current configuration.

1. Click on "Export"
 2. Confirm the privacy statement and click on "Next"
 3. Input the password of the camera and confirm
 4. The process will take some time. Please wait patiently. Once finished, the browser will download the file automatically.
 5. Send the downloaded file to the technical department.
-

Please note:

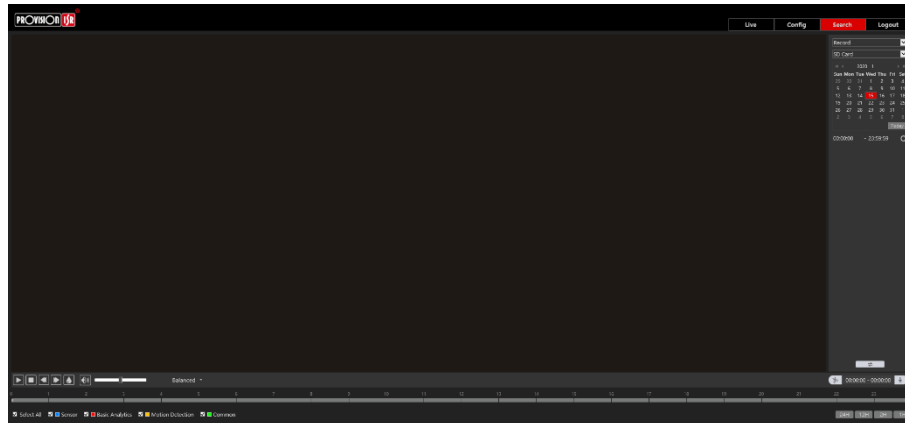
The file contains valueable information, but it is fully encrypted and can only be used by our technical team.

6) Playback (Search)

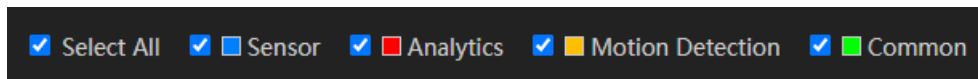
Playing back videos taken by the camera have 2 options:

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
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:



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

End Time

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

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

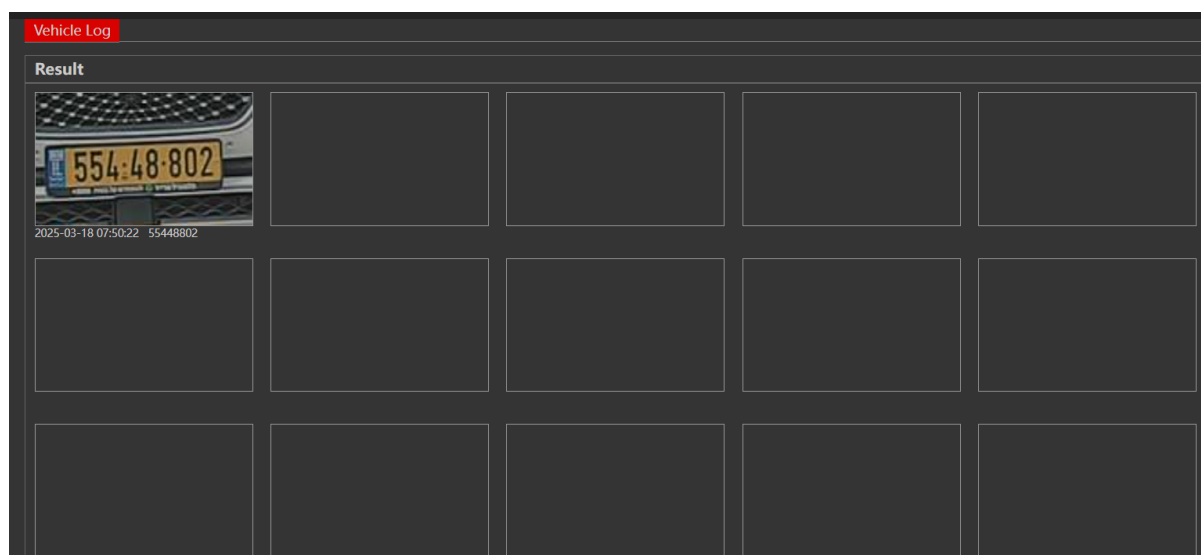
For Videos

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 the previous file		Buffering mode selection

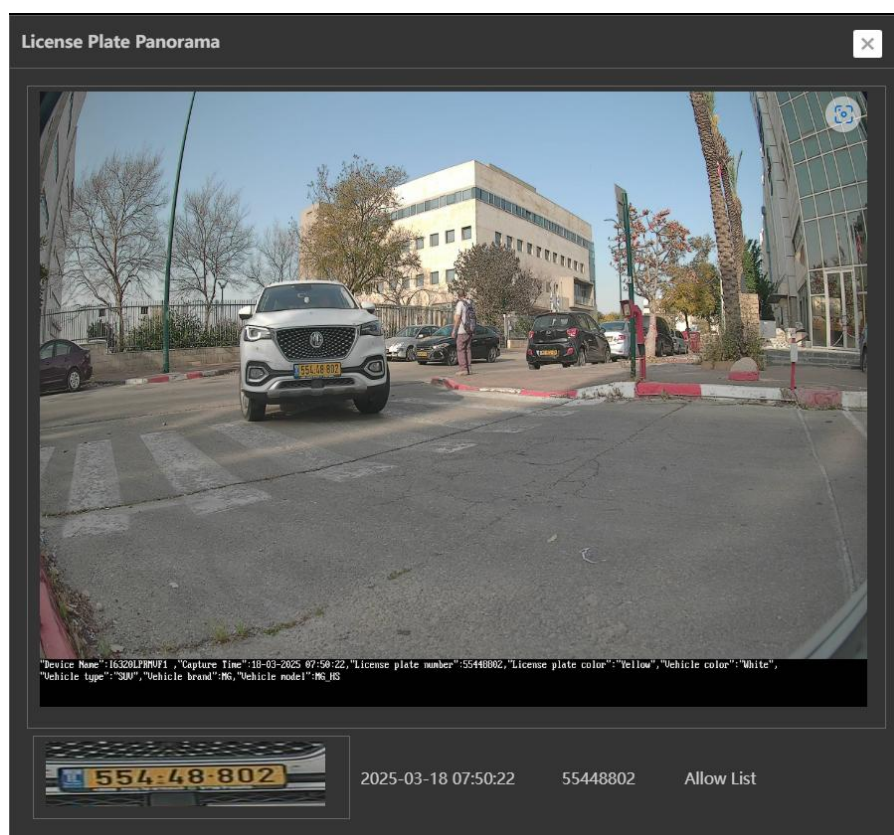
7) Data Record

This section allows you to search for LPR events stored on the SD Card (If applicable)

1. Set all the search fields and filters and click on Search. The following results will appear:



2. Click on a result to view it in detail:



3. If you need to export the results, choose if to export all the data including images, or just the raw data, and click on Export. Note that exporting the full data might take a long while to accomplish.

8) Appendix I : Analytics Configuration Requirements

8.1) General

Provision-ISR's LPR analytics requires a proper installation for optimal license plate reading. Installing the camera without following the installation thumb rules, might have dramatic results on the detection / recognition results.

8.2) LPR (License Place Recognition) Installation and Settings:

In general, license plate recognition is used for 2 main purposes:

1. General Road Monitoring.
2. Parking Monitoring and Management

Each usage required different type of installation

8.2.1) General Pre-installation requirements:

1. Please follow the requirements below to get the best analytics results:
2. Check the visibility, from the camera point of view.
3. Select the best place which covers the area you wish to monitor.
4. Connect the camera to a stable base. Shaking and vibrations reduces accuracy and might generate false alarms.
5. Vehicle Size should be $\leq 50\%$ of the Scene
6. Vehicle Height should be $\geq 10\%$ of the Scene
7. License plate camera tilt angle not more than $-5^\circ \sim 5^\circ$
8. No obstruction between the camera and license plate

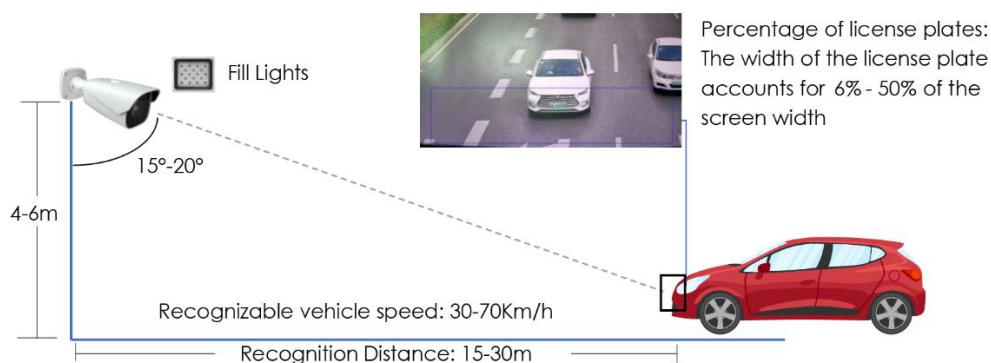
Using Fill Light (Optional):

Fill light must be used where the license plate is fully reflective (Characters + Background) In such case IR cannot be used. The strength of the fill light should not overexpose the license plate. (depends on country)

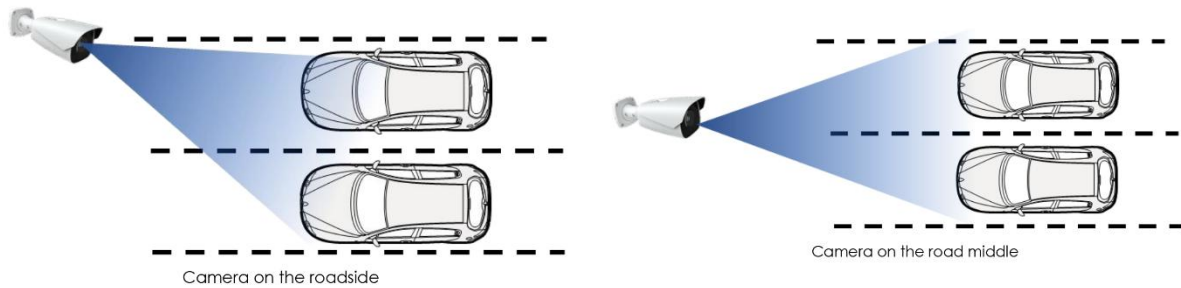
Thumb rules for a successful installation:

1. The license plate can be read by a human eye
2. The license plate size meets the configuration range
3. The detection area should be set to deliver best quality results
4. The license plate should be visible for more than 1 second

8.2.2) General Road Monitoring Installation:



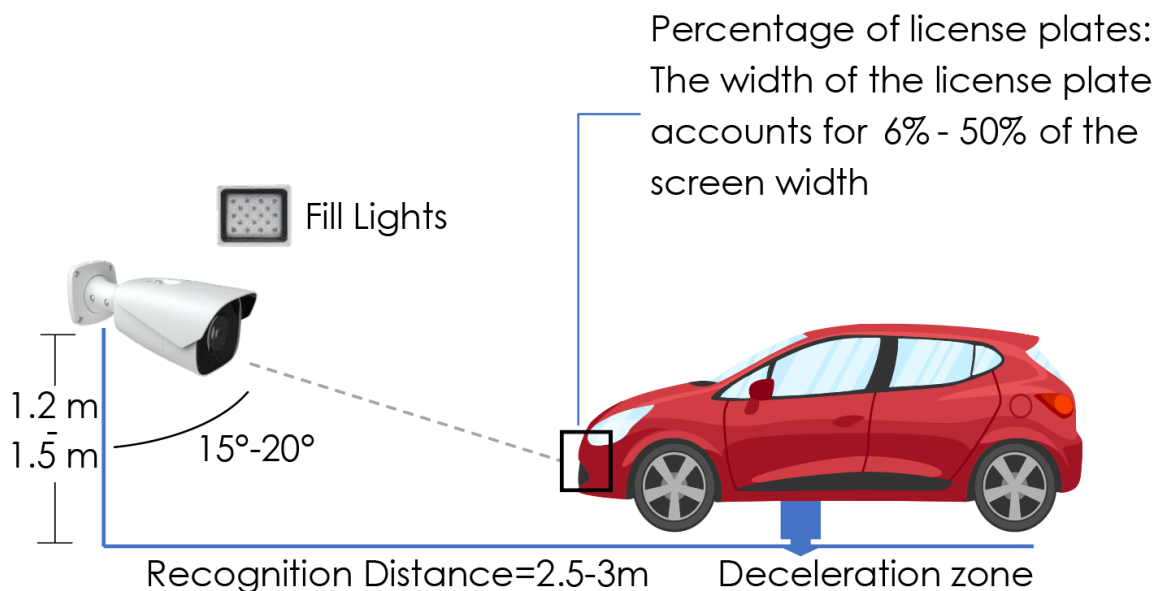
The camera can be installed to cover 1 / 2 lanes as follows:



Detection Area Settings:

Draw the snapshot area only in the closer lane, and at the bottom of the screen, covering about one third of the area

8.2.3) Parking Monitoring Installation:



Detection Area Settings:

Draw the detection area where the car slows down, for example near a speed bump, entrance gate, stop sign etc.

8.2.4) Default Image Settings

Day Mode:

Brightness: Default value

Day/Night Mode: Day

Infra-Red Mode: Auto

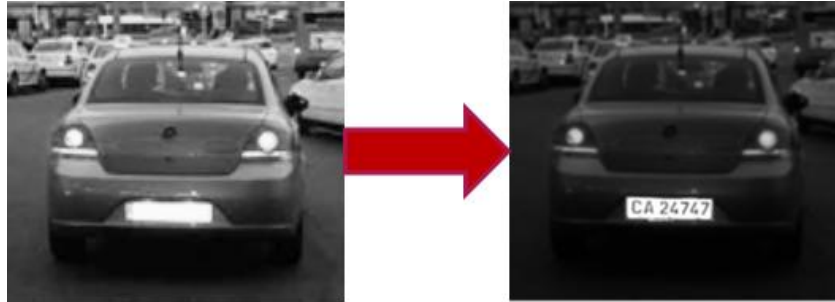
Max. (Shutter): According to the live scene. For static vehicles (gate) use $\sim 1/100$. The faster the vehicle speed, the smaller the value needs to be set ($\sim 1/500$)

Gain Mode: Auto

Gain Value: ~ 10

Night Mode:

Brightness: If the license plate is reflective, the brightness should be set to ~5. (General Image will be darker)



Day/Night Mode: Night

Infra-Red Mode: Auto

Smart IR: On

Max. (Shutter): According to the live scene. For static vehicles (gate) use ~1/100. The faster the vehicle speed, the smaller the value needs to be set (~1/500)

Gain Mode: Auto

Gain Value: ~10

9) Appendix II : Weigand

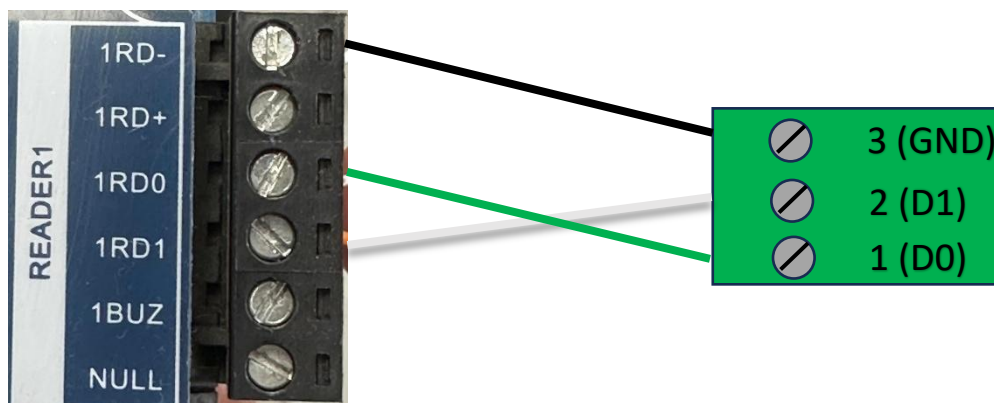
9.1) General

The Wiegand protocol is a unidirectional communication standard used by RFID readers to transmit binary data to access controllers via pulse signals on two data lines, Data0 and Data1.

9.2) Connection:

The Weigand port has 3 terminals:

- 1 → D0 (Data0), Usually Green: Should be connected to the controller D0 terminal.
 - 2 → D1 (Data1), Usually White: Should be connected to the controller D1 terminal.
 - 3 → GND (Ground), Usually Black: Should be connected to the controller D0 terminal.
- Refer to the illustration below. Note that different controllers might have different connection terminals.



Provision-ISR

11 Atir Yeda St, Kfar Saba,
Israel

Postal Code: 4442510

Tel: (972-9) 741 7511

Web: www.provision-isr.com