

Innos Technologies ISC Series IP Camera User Manual

Table of Contents

Contents

Summary.....	3
Key Features.....	3
Trademarks & Acknowledgments.....	3
Other References.....	4
Universal ActiveX Control.....	4
HTTP API	4
Disclaimer	4
Caution.....	4
Chapter 1 System Overview.....	5
Chapter 1-1 System Requirements.....	5
Chapter 1-2-2 PC Windows OS.....	5
Chapter 2 Before Accessing IP Cameras.....	6
Chapter 2-1 Configure IP Addresses using the IPScan Utility	6
Chapter 2-2 Configure IP Addresses through HTML Connection	6
Chapter 2-3 Web Browser Settings & Software Components Required.....	7
Chapter 2-4 Login	7
Chapter 3 IP Camera Operations.....	8
Chapter 3-1 HTML Operations.....	8
Chapter 3-2 Quick Buttons	8
Chapter 4 Settings	9
Chapter 4-1 System.....	9
Chapter 4-1-1 General.....	9
Chapter 4-1-2 User	10
Chapter 4-1-3 Timer Settings.....	10
Chapter 4-1-4 OSD Settings.....	11
Chapter 4-1-5 System Log.....	11
Chapter 4-2 Video.....	11
Chapter 4-2-1 General.....	12
Chapter 4-2-2 Quality Basic.....	13
Chapter 4-2-3 Quality Advance.....	14
Chapter 4-2-3-1 Sense Up+.....	16
Chapter 4-2-3-2 White Balance Control (AWB)	16
Chapter 4-2-4 Auto Focus.....	16
Chapter 4-2-5 Day Night Mode Switch	16
Chapter 4-2-6 Privacy Mask	18
Chapter 4-2-7 Audio Adjust.....	18
Chapter 4-2-8 ROI	19
Chapter 4-3 Controls.....	20
Chapter 4-3-1 Digital I/O	20
Chapter 4-3-2 Global Counter.....	20
Chapter 4-3-3 Virtual Input	21
Chapter 4-3-4 Metadata.....	21
Special characters	22
Chapter 4-4 Network.....	22
Chapter 4-4-1 General.....	23
Chapter 4-4-2 HTTP Service	23
Chapter 4-4-3 RTSP	24
Chapter 4-4-4 HTTPs Service	24
Chapter 4-4-5 IP/MAC Address Filtering.....	26

Chapter 4-4-6 DDNS.....	26
Chapter 4-4-7 Push Service	26
Chapter 4-5-1 Event Management	27
Chapter 4-5-2 Motion Detection.....	29
Chapter 4-5-3 Tampering Detection	29
Chapter 4-5-4 Audio Detection.....	30
Chapter 4-6 Notification	30
Chapter 4-6-1 FTP Service	30
Chapter 4-6-2 SMTP (Email) Service	31
Chapter 4-6-3 HTTP POST Service.....	31
Chapter 4-6-4 SD Card Service	32
Chapter 4-6-5 SD Card Backup File	32
Chapter 4-6-6 Samba Service	32
Chapter 4-7 Maintenance	33
Chapter 4-7-1 Firmware Update	33
Chapter 4-8 AI Analytics Module (Optional)	34
Appendix	36
DDNS Network Settings.....	36
Advanced Port Forwarding Technology.....	36
Restore to Factory Default.....	36

Summary

The Innos Technologies ISC Series is designed for professional IP video surveillance applications. The Innos Technologies ISC Series comprises the ISCD turret camera, the ISCB bullet camera and the ISCP PTZ camera. The series provides high-quality network video, efficient video compression, day/night monitoring and image-enhancement functions for reliable operation across a wide range of environments.

ISC Series cameras support intelligent video analytics for detecting and analyzing objects and activities within monitored areas. The series also provides motion detection, privacy masking, user authentication, centralized management, client software, ONVIF-compatible integration and configurable network video streaming.

Available functions may vary depending on the camera configuration and firmware version.

Key Features

- Supports Smart H.264 and H.265 encoding formats.
- Built-in GPU engine for Aida plug-in
- AI detection can send Email or FTP snapshot alarms
- SmartEvent for digital output
- Ultra low light & HDR at 120dB
- Day/night video quality independent scheduling
- Bit rate and frame rate on-the-fly adjustment
- Support dynamic DNS (DDNS) and network time protocol (NTP)
- Support HTTP API integration
- Support ONVIF protocol

Trademarks & Acknowledgments

Windows 7, ActiveX, and Internet Explorer are registered trademarks of Microsoft Corporation in the U.S. and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Flash, Macromedia, and Macromedia Flash Player are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. Linux and DynDNS are registered trademarks of the respective holders. Intel, Pentium, and Intel® Core™ 2 Duo are registered trademarks of Intel Corporation. FFmpeg is a trademark of [Fabrice Bellard](#), originator of the FFmpeg project. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license there from. Other names of companies and their products mentioned in this manual may be trademarks or registered trademarks of their respective owners.

This product contains H.265 (High Efficiency Video Coding, HEVC) codec technologies and is manufactured under the license from Access Advance LLC, and the HEVCAdvance symbol are trademarks of Access Advance LLC.



Covered by one or more claims of the HEVC patents listed at patentlist.accessadvance.com.

Other References

Universal ActiveX Control

Where required by the selected Windows and browser environment, the approved Universal ActiveX Control can be used to display MJPEG, H.264 or H.265 video. Contact Innos Technologies for the approved software package and supporting documentation.

HTTP API

For integration methods not covered by ONVIF, refer to the HTTP API integration documentation provided for the ISC Series.

Disclaimer

This manual covers the Innos Technologies ISC Series including the ISCD turret camera, the ISCB bullet camera and the ISCP PTZ camera. Available functions may vary according to the model, hardware configuration and firmware version. Illustrations and interface images are provided for reference and may differ from the released product. Innos Technologies Inc. reserves the right to update this manual and the product specifications without prior notice.

Caution

- Protect the camera from impact, vibration and physical damage during installation and operation
- Do not install the camera near open flames or excessive heat sources
- The cameras are rated IP67 for resistance to dust and moisture. Correctly fit all cable-entry seals and protective covers to maintain the rated ingress protection
- Use only approved mounting hardware and install the camera on a stable supporting surface
- Disconnect power and contact qualified service personnel if the camera emits smoke or an unusual odor, becomes excessively hot, or shows signs of damage
- Do not handle power or network connections with wet hands
- Do not use damaged cables, connectors or power supplies
- Protect the camera and its cabling from strong electromagnetic interference
- Follow applicable electrical and grounding requirements. Use suitable surge protection for outdoor installations where required



Chapter 1 System Overview

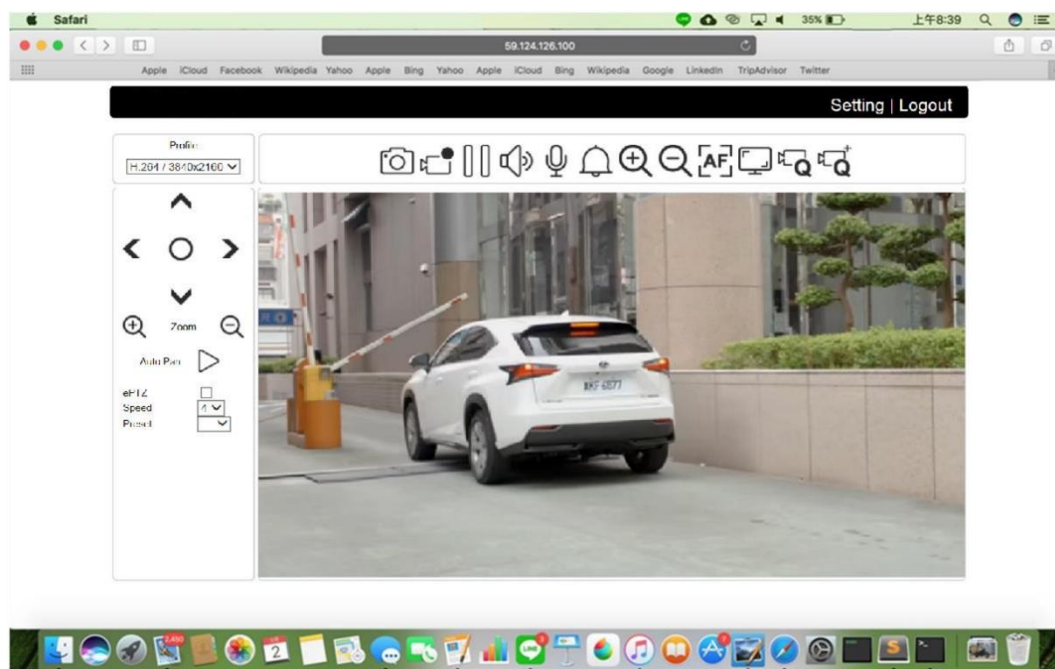
Chapter 1-1 System Requirements

ISC Series cameras use H.264, H.265 and MJPEG video compression to reduce the bandwidth and storage required for video transmission and recording. Viewing performance depends on the selected resolution, frame rate and bit rate, as well as the available network bandwidth and client-device performance.

Chapter 1-2 Software Requirements

Chapter 1-2-1 Apple Mac OS

ISC Series cameras support HTML5 browser-based viewing. On a supported macOS system, live video can be accessed using Safari without installing an additional browser plug-in.



Chapter 1-2-2 PC Windows OS

On a supported Windows system, a compatible web browser can be used to access the camera. Where required, the approved Universal ActiveX Control displays MJPEG, H.264 or H.265 video. When connecting for the first time, follow the on-screen instructions to install the component.

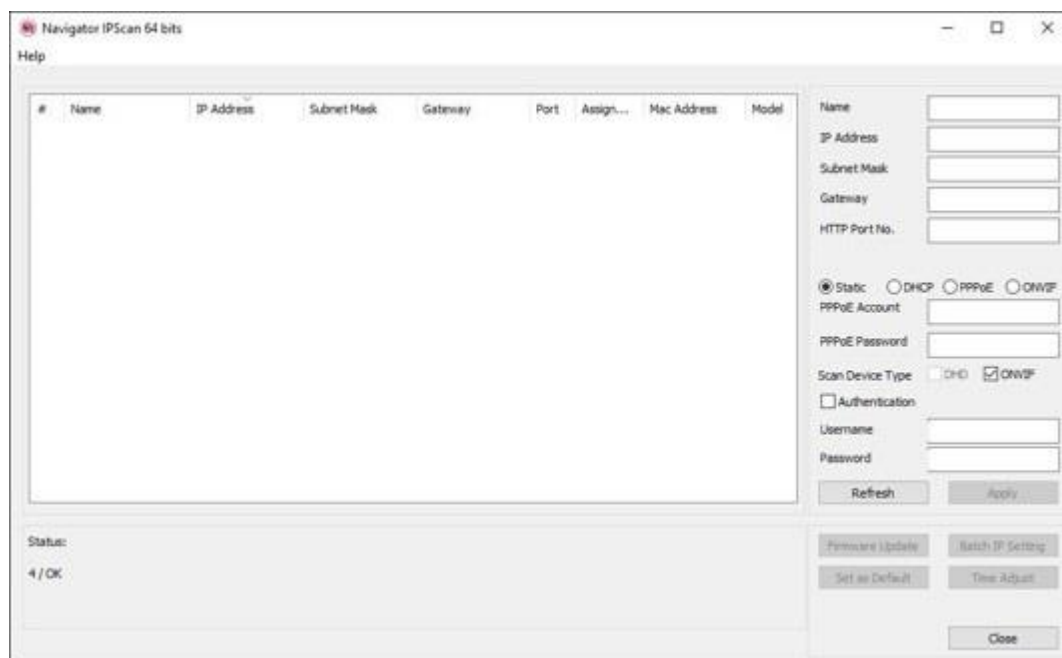
Chapter 2 Before Accessing IP Cameras

Before accessing an ISC Series camera, ensure that the RJ-45 network cable and either the 12 V DC supply or PoE connection are correctly connected. Connect audio cables only when the installed model and configuration support audio. Consult the network administrator before assigning an IP address. The default IP address is 192.168.0.200.

Chapter 2-1 Configure IP Addresses using the IPScan Utility

Obtain the approved IPScan utility from Innos Technologies. Use IPScan to change the camera's IP address, subnet mask, gateway or HTTP port as follows:

- Run the IPScan utility
- Click Refresh. All available devices will be listed on the screen
- Select the device item from the device list
- Enter the required IP address, subnet mask, gateway or HTTP port
- Click Apply for the changes to take effect
- Click Refresh again to verify the changed settings



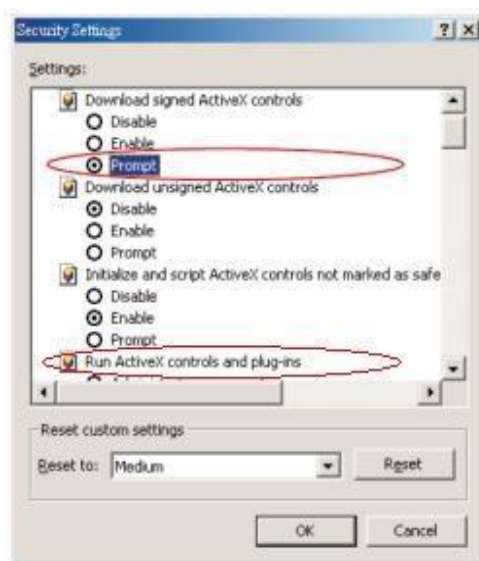
Chapter 2-2 Configure IP Addresses through HTML Connection

To change the IP address through the web interface, enter the default address 192.168.0.200 in the browser address bar and follow these steps:

- For security, create an administrator username and password during the first login. Select Confirm to save the credentials and sign in.
- Click **Setup**→**Network** to edit or modify IP address, subnet mask, gateway, or HTTP port
- Click **Submit** for the changes to take effect.

Chapter 2-3 Web Browser Settings & Software Components Required

If the approved ActiveX component is required, configure Internet Explorer to prompt before downloading signed ActiveX controls and to allow approved ActiveX controls to run. Go to Tools > Internet Options > Security > Custom level.



After completing the browser settings, enter the camera's IP address to open the live-view page. If a security prompt appears, verify the publisher and select the appropriate option to install the approved component.

Chapter 2-4 Login

For security, create an administrator username and password during the first login. Select Confirm to save the credentials and sign in.

Minimum password requirements:

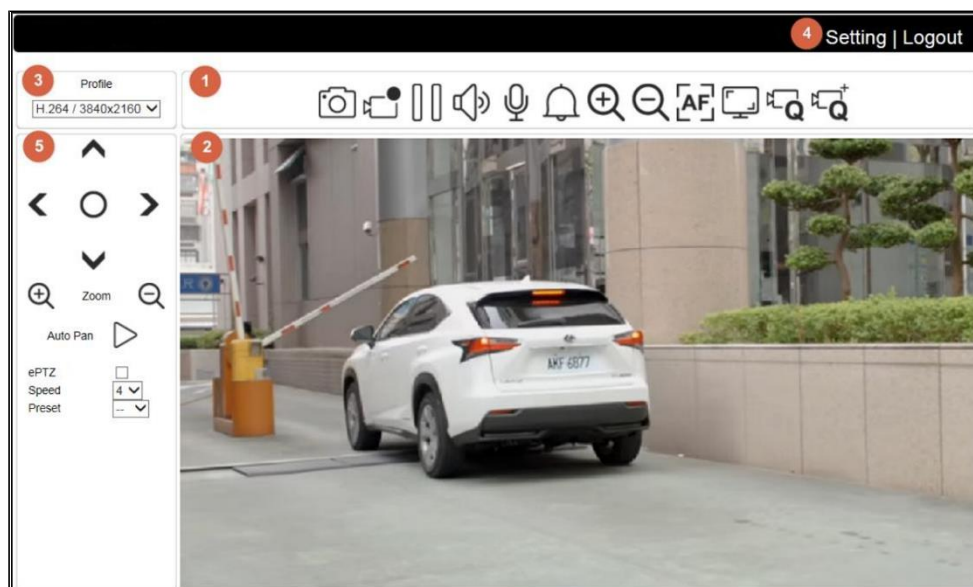
1. Use at least 8 characters.
2. Include at least one number (0-9), one uppercase letter, one lowercase letter and one supported special character.

Note: Store the credentials securely. If the administrator credentials are lost, restore the camera to its factory-default settings as described in the Appendix.

Chapter 3 IP Camera Operations

After signing in as an administrator, you can access live camera operations and configuration settings.

Chapter 3-1 HTML Operations



1. **Quick buttons:** IP camera shortcuts
2. **Live-view area:** Displays the selected MJPEG, H.264 or H.265 video stream
3. **Profile menu:** Switches between configured video profiles
4. **Setup button:** Opens the camera configuration menu
5. **ROI control panel:** Controls digital pan, tilt and zoom within the image

Chapter 3-2 Quick Buttons

The quick-control buttons are described below. Audio, alarm-output and other hardware-dependent buttons appear only when supported by the model and configuration.

	Take a snapshot of the video
	Start recording
	Pause recording
	Speaker output control
	Microphone input control
	Alarm out
	Camera zoom in
	Camera zoom out
	Camera auto focus
	Enlarge the live view
	Video quality basic
	Video quality advance

Chapter 4 Settings

Administrators can configure the camera through its web interface. After signing in, select Setup in the upper-right corner of the page.



Chapter 4-1 System



Chapter 4-1-1 General

System Settings > General displays the MAC address, firmware version, operating-system version, last restart time and device name.

Setup > System > General

MAC Address	8c:1f:64:bf:df:84
Firmware Version	14.0.001.6590
OS Version	Linux 4.9.84
System Reboot Time	1970/01/01 08:00:14 Thu CST
Device Name	ISCD16X3

OK

- **MAC Address:** The MAC address of the IP camera
- **Firmware Version:** Firmware version of the IP camera
- **OS Version:** The camera operating-system version
- **System Reboot Time:** The most recent camera restart time
- **Device Name:** The name used to identify the camera in IPScan. Enter a new name and select OK to apply the change.

Chapter 4-1-2 User

The camera supports up to 10 user accounts. Each account can be assigned individual access rights. To add or edit an account, select Add/Edit User. Bypass Logon and IPScan Bypass Logon allow access without normal authentication and should be enabled only on a trusted network.

Setup > System > User

Bypass Logon ☐ OFF
 IPScan Bypass Logon ☒ ON
 Password Strength ☐ OFF
 Authentication Security ☐ OFF Within: 30 Min. Failed Login Attempts: 5 IP Block Length: 5 Min.
 Operation Timeout ☒ ON 10 Min.

Account
 New Password
 Password has to meet the following criteria:
 (1) More than or equal to 8 characters,
 (2) Allow uppercase letter, lowercase letter, number digit, and special character,
 (3) Must have at least three types of character sets.
 Confirm Password
 User Group ☒ Administrator, ☐ Operator, ☐ Viewer

Enter the account name and password, confirm the password, assign the required access rights and select OK.

To modify an account, select the user and choose Edit User. To remove an account, select the user and choose Remove User. Select Submit to apply the changes.

Chapter 4-1-3 Timer Settings

Set the camera date and time using the web interface, then select OK. A holiday schedule can also be configured on this page.

Setup > System > Timer

Server Time 2022/01/11 14:42:59
 Synchronize with NTP ☐ Every Hour ☒ Off
 Time Server time.stdtime.gov.tw
 Time Zone
 Time 2022/1/11 14:42:51
 Enable Holiday List ☒

Select	Name	Start Date(Month-Date Hour:Min)	End Date(Month-Date Hour:Min)
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59
☐		1 - 1 0:00	12 - 31 23:59

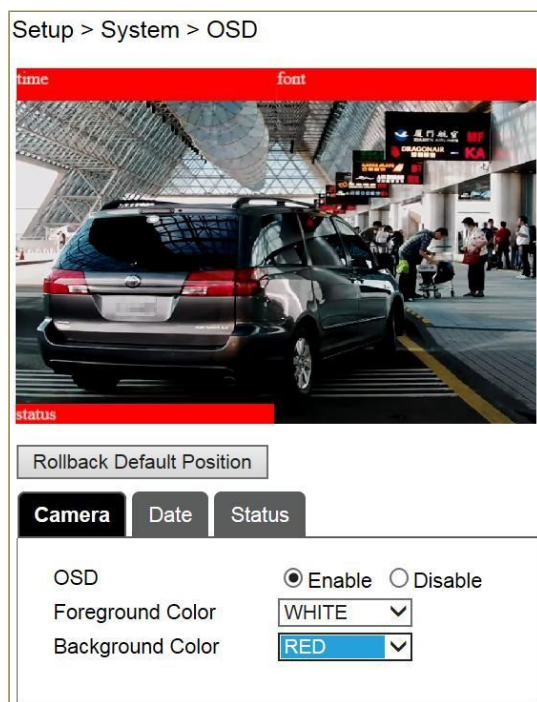
Synchronize with an NTP server

Set Synchronize with NTP to Every Hour to synchronize the camera clock with the configured NTP server once per hour.

Note: NTP synchronization requires network access to the configured NTP server.

Chapter 4-1-4 OSD Settings

OSD (on-screen display) places the configured camera ID, date and status information on the video image.



The available Camera ID, Date and Status options are described below:

- OSD: Click to enable or disable the OSD
- Foreground Color: The color of the text
- Background Color: The background color of the text

Chapter 4-1-5 System Log

This page displays camera-generated system logs. Select the Save icon to export the log as a text file, or filter the displayed records by log type.

Setup > System > System Log

Page 1 of 4 Type: ALL Displaying 1 to 5 of 19 items			
IP Address	User	Date & Time	Log Description
192.168.3.153	admin	2022/01/11 14:40:06	User Login(SYSTEM MESSAGE)
192.168.3.153	admin	2022/01/11 14:39:45	HTTP User Reject(SYSTEM WRONG)
192.168.3.153	admin	2022/01/11 14:39:36	User Logout(SYSTEM MESSAGE)
192.168.3.153	admin	2022/01/11 14:04:53	Restore Default Settings(SYSTEM MESSAGE)
192.168.3.153	admin	2022/01/11 13:57:08	Updated Video Settings(SYSTEM MESSAGE)

Chapter 4-2 Video



Chapter 4-2-1 General

Configure the stream resolution, frame rate and bit rate according to the available network bandwidth. Every models support a maximum frame rate of 30 fps, depending on the selected stream settings.

Setup > Video > General

Encoder2 : ☒ Enable ☐ Disable

Encoder3/TV Out : ☐ Disable/(TV Out Enable) ☒ Enable/(TV Out Disable)

Video Standard : ☐ 60Hz ☒ 50Hz

Fixed Bitrate Mode : ☒ Enable ☐ Disable

Image Enhance Mode :

Encoder1

Profile Name :

Resolution :

Output Frame Rate :

GOP (Group of Pictures) :

Stream Mode :

Bit Rate :

RTSP URL :

Encoder3

Profile Name :

Resolution :

Output Frame Rate :

GOP (Group of Pictures) :

Stream Mode :

Bit Rate :

RTSP URL :

Encoder2

Profile Name :

Resolution :

Output Frame Rate :

GOP (Group of Pictures) :

Stream Mode :

Bit Rate :

RTSP URL :

Encoder4

Profile Name :

Resolution :

Output Frame Rate :

Image Quality :

RTSP URL :

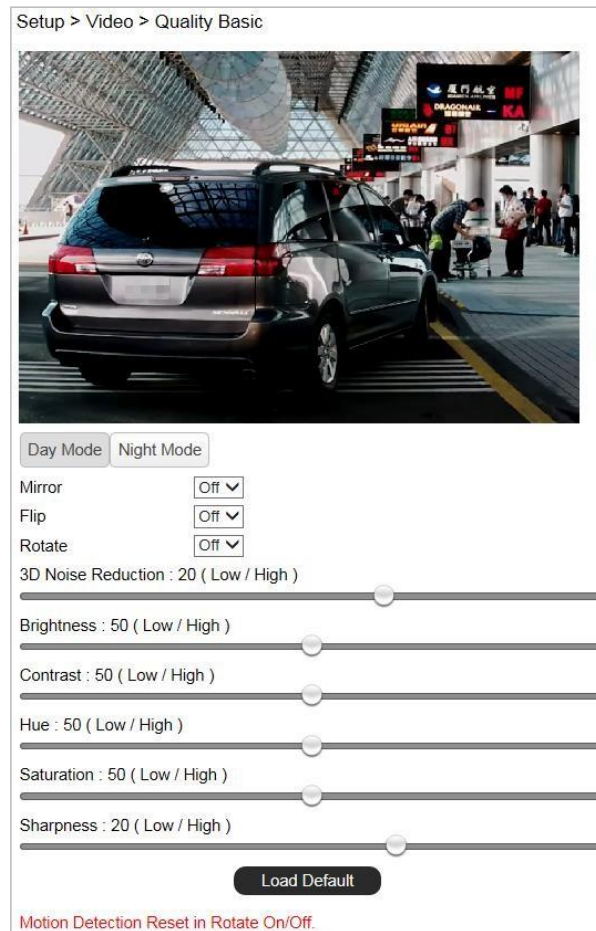
OK Load Default

- **Profiles:** 4 customizable profiles
- **Video Standard:** NTSC/PAL setting
- **Image Enhance Mode:** Enables or disables D-WDR; both models support D-WDR up to 120 dB
- **Profile Name:** Selects the H.264, H.265 or MJPEG video stream profile
- **Resolution:** The resolution of the video stream
- **Output Frame Rate:** The frame rate of the video
- **GOP:** The number of I-frames to be displayed in one second
- **Stream Mode:** VBR varies the bit rate according to scene complexity; CBR targets a constant bit rate
- **Bit Rate:** Sets the target or maximum stream bit rate
- **RTSP URL:** Displays the address used to access the stream through RTSP
- **Image Quality:** Sets the compression quality of the selected video stream

Chapter 4-2-2 Quality Basic

Use this page to adjust brightness, contrast, hue, saturation and sharpness independently for day and night operation.

Setup > Video > Quality Basic



Day Mode Night Mode

Mirror Off ▾

Flip Off ▾

Rotate Off ▾

3D Noise Reduction : 20 (Low / High)

Brightness : 50 (Low / High)

Contrast : 50 (Low / High)

Hue : 50 (Low / High)

Saturation : 50 (Low / High)

Sharpness : 20 (Low / High)

Load Default

Motion Detection Reset in Rotate On/Off.

- **Mirror:** Mirrors the image horizontally
- **Flip:** Flips the image vertically
- **Rotate:** Rotates the image by 90 degrees for corridor viewing, when available
- **3D Noise Reduction:** Reduces image noise; excessive settings may reduce moving-image detail

Chapter 4-2-3 Quality Advance

This page provides exposure, automatic gain control, white balance, shutter, IR illumination and IR-cut-filter settings for day and night operation.

Separate day and night image settings can be configured to maintain suitable image quality under changing lighting conditions.

Setup > Video > Quality Advance



Day Mode Night Mode

DeFog	Off ▼
White Balance Control	Auto ▼
Exposure Value	8 ▼
WDR	Auto ▼
Shutter Value Range	Min: 1/20000 ▼ Max: 1/30 ▼
Auto Gain Control(SENSE UP+)	30 ▼
Sense Up	Off ▼
Color Mode	Color ▼
Light Setting	Smart Dual Light ▼
	Light Duration 10 ▼ (10~100)
	Sensitivity 5 ▼ (1~10)
IR LED	0 ▼
White LED	0 ▼
IR Cut Filter	On ▼

Load Default

Video setting options are described as follows:

- **Defog:** Improves local contrast when the scene appears hazy or has low contrast
- **White Balance Control:** Selects automatic or manual white-balance adjustment
- **Exposure Value:** Increases or decreases overall image exposure
- **D-WDR:** Enables or disables digital wide dynamic range, up to 120 dB
- **Shutter Value Range:** Sets the minimum and maximum shutter values
- **Automatic Gain Control (Sense Up+):** Adjusts gain for low-light operation
- **Sense Up:** Selects slow-shutter enhancement for low-light scenes
- **Color Mode:** Selects color or black-and-white imaging
- **IR Light Setting:** Both ISC Series models use infrared illumination and a mechanical IR-cut filter for day/night operation. Warm-light and smart-dual-light functions are not specified for these models.
 - IR illumination modes:
 - Auto: The camera switches between color and IR-assisted black-and-white operation according to ambient light
 - Day: Forces color operation with the IR-cut filter enabled
 - Night: Enables IR-assisted black-and-white operation with the IR-cut filter removed
- **IR LED:** Enables or disables IR illumination
- **IR Cut Filter:** Enables or disables the mechanical IR-cut filter

Without Sense Up



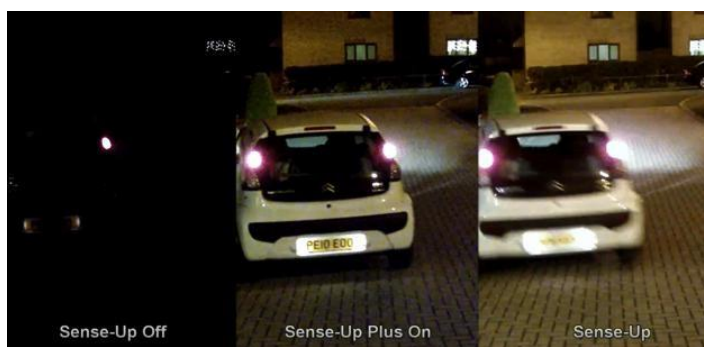
Sense Up by 3 Frames



Note: Available options depend on the model and firmware version.

Chapter 4-2-3-1 Sense Up+

Sense Up+ uses automatic gain control to improve low-light visibility. Combining gain control with 3D noise reduction can reduce visible noise. If additional sensitivity is required, Sense Up uses a slower shutter, which may introduce motion blur.



Chapter 4-2-3-2 White Balance Control (AWB)

The camera provides automatic white-balance controls for day and night operation.

White Balance Control	Manual ▼
One Push AWC	R-Gain 128 ▼ (1~255)
	B-Gain 128 ▼ (1~255)

- **White Balance Control:** Selects automatic or manual white balance
- **R-Gain:** Adjusts the red channel in manual white-balance mode
- **B-Gain:** Adjusts the blue channel in manual white-balance mode
- **One Push AWC:** Performs a one-time automatic white-balance adjustment

Chapter 4-2-4 Auto Focus

The ISC Series support automatic focus for the installed 2.8-12 mm lens.

Zoom Speed	1 ▼	Zoom in	Zoom out
Focus Speed	2 ▼	Focus Near	Focus Far
		Step Near	Step Far
Quick Zoom	Wide	Tele	
Quick Focus	Auto Focus		
Lens Initialize	Start		

- **Zoom Speed:** Sets the zoom-in and zoom-out speed
- **Focus Speed:** Sets the near-focus and far-focus adjustment speed
- **Quick Zoom:** Moves directly to the specified zoom ratio
- **Quick Focus:** Starts an automatic focus operation
- **Lens Initialize:** Reinitializes the zoom and focus mechanism

Note: Available lens controls depend on the installed lens and firmware version.

Chapter 4-2-5 Day Night Mode Switch

The Day/Night Mode Switch provides Auto, Day, Night and Schedule modes. Auto mode controls the IR illumination and IR-cut filter according to ambient light. Night mode removes the IR-cut filter for improved IR sensitivity; Day mode enables the filter for color imaging.

Schedule mode changes day/night operation according to the configured time periods.

Setup > Video > Day Night Mode Switch

☒ Auto , Switch Delay Time Sec.

Light sensor current value 100

Day to Night Threshold

Night to Day Threshold

☐ Day Mode

☐ Night Mode

☐ Schedule

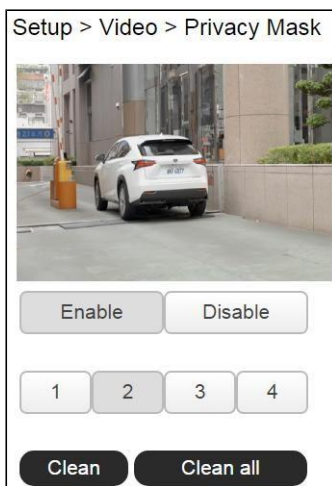
OK

- **Auto:** Enables automatic day/night switching
- **Light Sensor Current Value:** Displays the current ambient-light reading
- **Day-to-Night Threshold:** Sets the threshold for switching to night mode
- **Night-to-Day Threshold:** Sets the threshold for returning to color mode
- **Day Mode:** Forces color imaging
- **Night Mode:** Forces IR-assisted black-and-white imaging
- **Schedule:** Changes day/night operation according to configured times

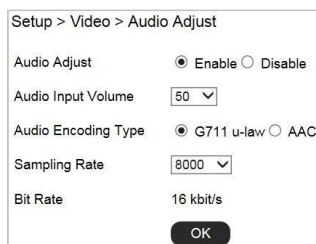
Note: All ISC Series models use a removable mechanical IR-cut filter.

Chapter 4-2-6 Privacy Mask

ISC Series cameras provide up to four privacy-mask areas. Select a mask number and drag over the area to be obscured.



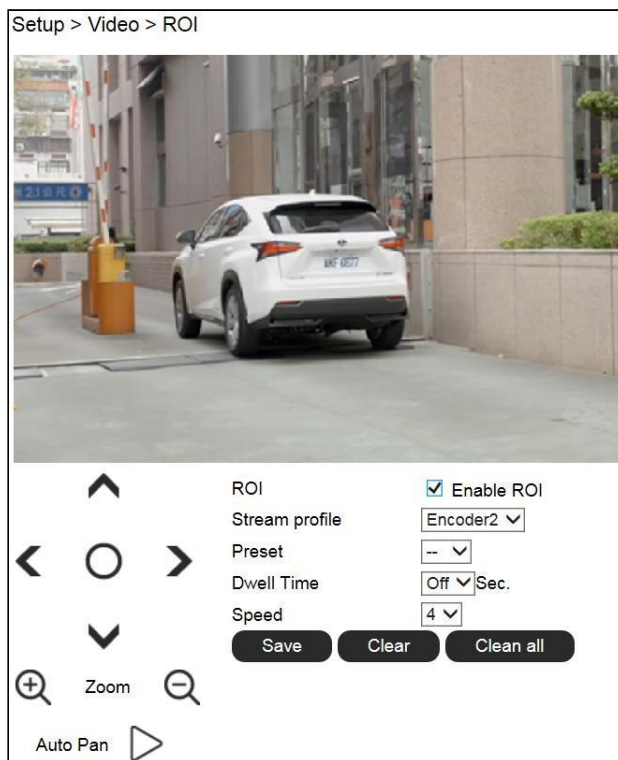
Chapter 4-2-7 Audio Adjust



- **Audio Adjust:** Enables audio functions, depends on the supplied hardware configuration
- **Audio Input Volume:** Adjusts microphone or line-input volume
- **Audio Encoding Type:** Selects the supported audio codec
- **Sampling Rate:** Sets the audio sampling rate
- **Bit Rate:** Displays or sets the audio bit rate, when available

Chapter 4-2-8 ROI

ISC Series cameras support digital Region of Interest (ROI) control when enabled by the firmware. Select Enable ROI and use the controls to position the selected region.



- **Stream Profile:** Selects the stream used for ROI viewing
- **Preset:** Selects one of the available ROI presets
- **Dwell Time:** Sets how long the camera remains at the selected ROI preset
- **Speed:** Sets the movement speed between ROI positions

Select Save to apply the changes, or Clear All to remove the configured settings.

Note: Available options depend on the model and firmware version.

Note: Enabling privacy masking may enable ROI automatically and disable EPTZ.

Note: ROI availability depends on the firmware version.

Chapter 4-3 Controls



Chapter 4-3-1 Digital I/O

Digital input/output functions require a supported hardware interface. Where available, connect the external alarm input and select NO (normally open) or NC (normally closed) as required.



Chapter 4-3-2 Global Counter

Global counters record triggers received from configured metadata or virtual inputs and can be used by supported event actions. Availability depends on the model and firmware configuration.



Chapter 4-3-3 Virtual Input

The firmware can provide up to 16 virtual inputs for integration through CGI commands. Availability depends on the model and firmware configuration.

Setup > Controls > Virtual Input

Virtual Input #1	State: ☒ 1
Virtual Input #2	State: ☐ 0
Virtual Input #3	State: ☐ 0
Virtual Input #4	State: ☐ 0
Virtual Input #5	State: ☐ 0
Virtual Input #6	State: ☐ 0
Virtual Input #7	State: ☐ 0
Virtual Input #8	State: ☐ 0
Virtual Input #9	State: ☐ 0
Virtual Input #10	State: ☐ 0
Virtual Input #11	State: ☐ 0
Virtual Input #12	State: ☐ 0
Virtual Input #13	State: ☐ 0
Virtual Input #14	State: ☐ 0
Virtual Input #15	State: ☐ 0
Virtual Input #16	State: ☐ 0

Chapter 4-3-4 Metadata

Metadata integration processes HTTP responses received from a configured IP device. Availability depends on the model and firmware configuration.

Setup > Controls > Metadata

Number	1
Metadata Enable	☒
Metadata Server Name	metaservername0
Metadata Type	HTTP Multipart Response ▾
Metadata Server IP/DNS	metaserver.com
Metadata Server Port	80
Account	Account
Password	*****
Metadata URL	/url
Metadata Parser	parser

OK Cancel

In the example below, the camera receives the MotionDetect token from the /getalarmmotion CGI command. The resulting %Trigger1% value can be used by Event Management for a configured action. /getalarmmotion CGI command, from an IP device. The events are captured into the valuable %Trigger1% for actions. In the SmartEvent, %Trigger1% can be used for a global counter for event triggering.

Configure metadata integration as follows:

Metadata Enable: Enable metadata service.

Metadata Server Name: Specify the name of the metadata service.

Metadata Type: (1) HTTP multipart response, (2) HTTP response

- (1) HTTP multipart response—Continuous responses
- (2) HTTP response—Client-pull by a schedule

Metadata Server IP/DNS: Address of the integrated device. Metadata

Server Port: Port used by the integrated device.

Account: Account name for the integrated device.

Password: Password for the integrated device

Metadata URL: URL of the integrated device; include the required leading slash

Metadata Parser: Defines the tokens used to populate trigger variables

Special characters

Enter special parsing characters such as /, \r, \n or \r\n where required.

%Split%

%CR% => \r

%LF% => \n

%CRLF% => \r\n

Metadata Enable
☒

Metadata Server Name

Metadata Type

Metadata Server IP/DNS

Metadata Server Port

Account

Password

Metadata URL

Metadata Parser

hit2=%Trigger3%,

Enter the parsing tokens in the meta parser field for triggering an event from metadata URL of a third party device.
The max length is 127 characters including spaces.

The parsing tokens of Metadata response are described below::

```

%Trigger1% => Metadata #1
%Trigger2% => Metadata #2
%Trigger3% => Metadata #3
%Trigger4% => Metadata #4
%Trigger5% => Metadata #5
%Trigger6% => Metadata #6
%Trigger7% => Metadata #7
%Trigger8% => Metadata #8
%Trigger9% => Metadata #9
%Trigger10% => Metadata #10
%Trigger11% => Metadata #11
%Trigger12% => Metadata #12
%Trigger13% => Metadata #13
%Trigger14% => Metadata #14
%Trigger15% => Metadata #15
%Trigger16% => Metadata #16

%Split%
%CR% => \r
%LF% => \n
%CRLF% => \r\n

```

OK

Cancel

Chapter 4-4 Network



Chapter 4-4-1 General

Network settings connect the ISC Series camera to an IP network. The default address is 192.168.0.200. Enter this address in a browser to verify communication between the camera and a computer on the same network.

Enter the required IP address, subnet mask, gateway and DNS values, then select OK.

Setup > Network > General

Network ☒ Static ☐ DHCP ☐ PPPoE

IP Address

Subnet Mask

Gateway

Primary DNS

Secondary DNS

Account

Password

QoS(DSCP) (0~63)

2nd IP Address ☐ Enable ☒ Disable

2nd IP Address

2nd Subnet Mask

3rd IP Address ☐ Enable ☒ Disable

3rd IP Address

3rd Subnet Mask

OK

For access through a routed network, obtain the required addressing information from the network administrator or Internet service provider.

- **Primary DNS:** Address of the preferred DNS server
- **Secondary DNS:** Address of the alternate DNS server
- **QoS (DSCP):** Sets the DSCP value used to prioritize network packets

A DHCP server can assign the camera's IP address, subnet mask and gateway automatically. Because the assigned address may change, use IPScan or the DHCP server's client list to locate the camera. Select DHCP and then Submit to enable automatic addressing.

Note: Use DHCP only when a reachable DHCP server is available on the local network.

Chapter 4-4-2 HTTP Service

HTTP can be used for web access and supported video transport. To change the HTTP port or configure port forwarding, consult the network administrator. Select HTTP & HTTPS or HTTPS as required, then select OK.

Setup > Network > HTTP Service

HTTP Port

HTTP Connection Policy ☒ HTTP & HTTPS ☐ HTTPS Service

OK

Chapter 4-4-3 RTSP

RTSP provides access to supported video streams. Port-forwarding considerations are described in the Appendix.

Setup > Network > RTSP

RTSP Port	554
RTSP Authentication	☒ On ☐ Off
Encoder1	stream0
Encoder2	stream1
Encoder3 (TV Out)	stream2
Encoder4	stream3

Settings on this page are described below:

- **RTSP Authentication:** Requires a username and password for access to an RTSP stream
- **Encoder:** Sets the encoder name used in the stream address

Chapter 4-4-4 HTTPs Service

ISC Series cameras support HTTPS (Hypertext Transfer Protocol Secure), which encrypts communication between the camera and the client browser.

HTTPS uses a digital certificate and TLS encryption. A self-signed certificate can encrypt traffic but will not normally be trusted automatically by client browsers.

Setup > Network > HTTPS Service

HTTPS Service ☐ Enable ☒ Disable

Two certificate-configuration methods are available:

- Option 1: Enter the required information and select Create a certificate to generate a self-signed certificate.

HTTPS Service ☒ Enable ☐ Disable

HTTPS Status: Disable

Certificate Status: Not installed

Method:

Country:

State or province:

Locality:

Organization:

Organization Unit:

Common Name:

Validity:

A confirmation message appears after the certificate is created.



Certificate Status changes from Not Installed to Active when installation succeeds.

HTTPS Service	☒ Enable ☐ Disable
HTTPS Status	Disable
HTTPS Port	443
Certificate Status	Active
Method	Create self-signed certificate
Country	US
State or province	
Locality	
Organization	IPCAM12
Organization Unit	IPCAM123
Common Name	www.example.com@@123
OK Remove a certificate.	

Select OK to enable HTTPS. HTTPS Status changes from Disable to Enable.

HTTPS Service	☒ Enable ☐ Disable	→	HTTPS Service	☒ Enable ☐ Disable
HTTPS Status	Disable		HTTPS Status	Enable

The camera can now be accessed using HTTPS.

2. Option 2: Select Create a certificate request and install. Submit the certificate request to a trusted certificate provider, then upload the issued certificate. After successful installation, Certificate Status changes to Active and HTTPS Status changes to Enable.

HTTPS Service	☒ Enable ☐ Disable
HTTPS Status	Disable
Certificate Status	Waiting for a certificate.
Download File	Download
Select a certificate file	Browse... Upload
Method	Create a certificate request and install.
Country	US
State or province	
Locality	
Organization	IPCAM12
Organization Unit	IPCAM123
Common Name	www.example.com@@123

Chapter 4-4-5 IP/MAC Address Filtering

ISC Series cameras provide IP/MAC address filtering to control access from specified network devices. Enable the service, enter the address and select OK.

- **IP/MAC Address Filtering:** Enables or disables address filtering
- **Allow / Deny:** Permits or blocks the specified address
- **IP Address:** Specifies the IP address to be filtered
- **MAC Address:** Specifies the MAC address to be filtered

Chapter 4-4-6 DDNS

DDNS associates a domain name with a changing public IP address. Select an available DDNS provider from the camera interface, enter the required account information and select OK.

The available DDNS registration method depends on the configured provider and firmware version. Contact Innos Technologies for the approved DDNS service information.

Note: DDNS requires Internet access and valid service-provider credentials.

Chapter 4-4-7 Push Service

Where supported and configured, the camera can send alarm notifications to an approved iOS or Android mobile application through the configured cloud service.

- **Push Service:** Enables or disables push notifications
- **Push Time:** Sets the camera's reporting interval to the configured notification service
- **ID:** Application identifier for a subscribed mobile device
- **Address:** Email account associated with the registered mobile device

Chapter 4-5-1 Event Management



Use Event Management to configure supported alarm, counter, virtual-input, metadata and network-failure conditions. Enter an event name, select the trigger conditions and save the event.

Setup > SmartEvent > SmartEvent

Enable Event 1 ☐

Event Name

Condition 1 Condition 2 Condition 3 Condition 4 Condition 5

Condition Name

Trigger Schedule Action

Detection Time Sec. Sleep Time Sec.

(Current number/Maximum number of Trigger Rule is 1/3)

Trigger

Enable	Trigger	Operator	Value	Duration
☐	Digital Input #1	=	1 or 0	0 Sec.

Save the event. Cancel

Select the action to be performed when the event occurs, such as uploading a JPEG image to an FTP server, sending an email notification or saving a snapshot to the SD card. Use Schedule to define active monitoring periods.

Condition 1 Condition 2 Condition 3 Condition 4 Condition 5

Condition Name: Aida Triggering 1

Trigger Schedule Action

Enable Holiday List ☐

Select	Schedule	Start Time	End Time
☒	All	0:0	23:59
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0
☐	Sun	0:0	0:0

Save the event Cancel

Select Action to configure the outputs used by the event.

Setup > SmartEvent > SmartEvent

Enable Event 1 ☒

Event Name: Aida Event 1

Condition 1 Condition 2 Condition 3 Condition 4 Condition 5

Condition Name: Aida Triggering 1

Trigger Schedule Action

(Current number/Maximum number of Action Rule is 1/10)

FTP Service, Rule Number:0	Edit
SMTP Service, Rule Number:0	Edit
Push Service Setting, Rule Number:0	Edit
Alarm Out, Rule Number:1	Edit
HTTP POST Service, Rule Number:0	Edit
Global Counter, Rule Number:0	Edit
Virtual Input, Rule Number:0	Edit
SD Card Service, Rule Number:0	Edit
SAMBA Service, Rule Number:0	Edit

Save the event Cancel

- **FTP Service:** Uploads configured event information or snapshots to an FTP server
- **SMTP Service:** Sends configured event notifications through an SMTP server
- **Push Service Setting:** Sends a notification to a configured iOS or Android application, where supported
- **Alarm Out:** Activates the digital output, where supported by the hardware
- **HTTP POST Service:** Sends configured event data or snapshots to the specified server
- **Global Counter:** Sets or changes the configured counter value
- **Virtual Input:** Enables or disables one of the configured virtual inputs
- **SD Card Service:** Saves an event snapshot to the installed SD card
- **Samba Service:** Sends the selected stream to a configured Samba server

Note: Configure the corresponding Controls or Notification service before enabling an event action. Available actions depend on the model and firmware configuration.

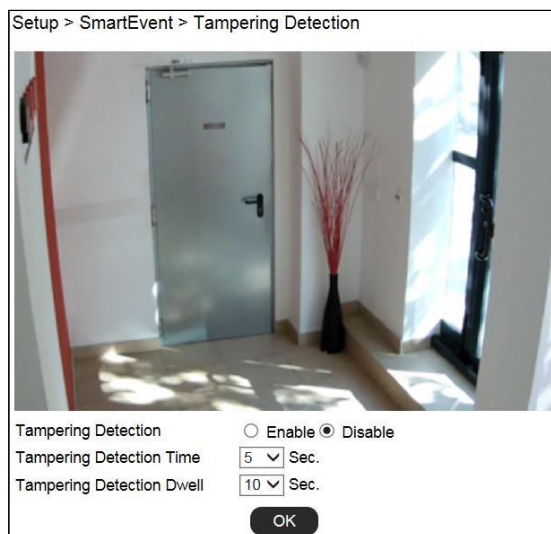
Chapter 4-5-2 Motion Detection

Enable Motion Detection and select the image areas to be monitored. Double-click or drag to select an area; use the right mouse button to remove a selection. Select OK to apply the settings.



Chapter 4-5-3 Tampering Detection

Where supported by the firmware, tampering detection can generate an alarm when the camera view or focus changes significantly or the lens is obstructed. Select Enable and configure the required settings.

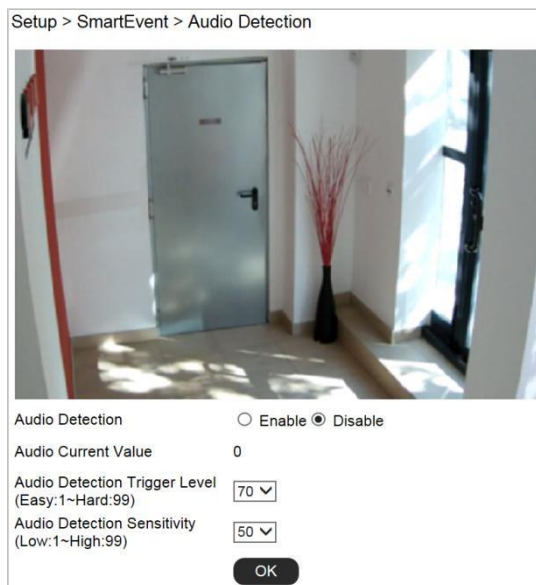


- **Tampering Detection:** Enables or disables tampering detection
- **Tampering Detection Time:** Sets the detection time
- **Tampering Detection Dwell:** Sets the alarm-output duration

Chapter 4-5-4 Audio Detection

When audio detection is available and enabled, sound above the configured threshold can trigger an event.

Setup > SmartEvent > Audio Detection



Audio Detection ☐ Enable ☒ Disable

Audio Current Value 0

Audio Detection Trigger Level (Easy:1~Hard:99) 70 ▼

Audio Detection Sensitivity (Low:1~High:99) 50 ▼

OK

- **Audio Detection:** Enables or disables audio detection
- **Audio Current Value:** Displays the current received audio level
- **Audio Detection Trigger Level:** Sets the audio level that triggers an event
- **Audio Detection Sensitivity:** Sets detection sensitivity

Note: Audio functions depend on the model and supplied hardware configuration.

Chapter 4-6 Notification



Chapter 4-6-1 FTP Service

Enter the required FTP information to upload alarm snapshots to an FTP server.

Setup > Notification > FTP Service

Number	FTP Server Name	FTP/DNS Server	Port
1	FTPServerName	ftp.server.com	21
2	FTP1ServerName	ftp1.server.com	21
3	FTP2ServerName	ftp2.server.com	21

Number 1

FTP Server Name FTPServerName

FTP/DNS Server ftp.server.com

FTP/DNS Server Port 21

Account admin

Password

Directory /alarm_peg/

Prefix

Postfix

OK Cancel

- **FTP Channel:** Selects one of the available FTP server configurations
- **Number:** Identifies the FTP service configuration

- **FTP Server Name:** Name assigned to the FTP server configuration
- **FTP/DNS Server:** Address of the FTP server
- **FTP/DNS Server Port:** Network port used by the FTP server
- **Account:** Username for the FTP server
- **Password:** Password for the FTP account
- **Directory:** Destination directory for JPEG snapshots
- **Prefix:** Prefix added to the JPEG filename
- **Postfix:** Postfix added to the JPEG filename
- **File Format:** Selects the JPEG output format or encoder

Chapter 4-6-2 SMTP (Email) Service

Enter the required mail-server information to send alarm notifications with JPEG snapshots.

- **Receiver Email Address:** Address that receives the notification
- **Sender Email Address:** Address used to send the notification
- **SMTP Server:** Address of the mail server
- **SMTP Authentication:** Selects the authentication type
- **SMTP Port:** Port used by the mail server; the displayed default is 25
- **Authentication:** Enables or disables SMTP authentication
- **Auth Account:** Username for the mail server
- **Auth Password:** Password for the sender account

Chapter 4-6-3 HTTP POST Service

HTTP POST can send configured event data or snapshots to a web server when an alarm is triggered.

- **HTTP POST Server Name:** Name assigned to the server configuration
- **HTTP POST Server IP/DNS:** Address of the HTTP POST server
- **HTTP POST Server Port:** Port used by the HTTP POST server
- **Account:** Username for the server, when required
- **Password:** Password for the server account, when required
- **HTTP POST URL:** CGI path used for the HTTP POST request
- **HTTP POST JSON:** JSON payload editor

Chapter 4-6-4 SD Card Service

Install a compatible SD card before enabling SD recording. The camera can record video when an alarm occurs.

Setup > Notification > SD Card Service

SD Recording	☐ On ☒ Off
SD Recording OSD	☐ On ☒ Off
SD Recording Continuous	☐ On ☒ Off
Recording Format	Encoder1 ▼
Pre Record Time	1 Sec.
SD Card Status	NORMAL
SD Card State	Unmount
SD Card Total Bytes	0 MBytes
SD Card Free Bytes	0 MBytes

OK Unmount Mount Format

Warning: Select Unmount before removing the SD card to avoid file-system corruption or data loss.
Note: Supported capacity depends on the model as specified above.

Chapter 4-6-5 SD Card Backup File

To download a clip, right-click the required file and save the AVI file to the local computer.

Setup > Notification > SD Card Backup File

(Right Button->Play, Right Button->Stop)

Delete Refresh

Chapter 4-6-6 Samba Service

The selected camera stream can be recorded as AVI files to a configured Samba server. Continuous and pre-alarm recording can be enabled. Circular recording overwrites the oldest files when the configured storage becomes full.

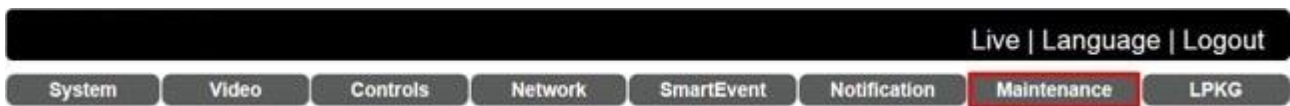
Setup > Notification > SAMBA Service

SAMBA Recording	☐ On ☒ Off
SAMBA Recording OSD	☐ On ☒ Off
SAMBA Recording Continuous	☐ On ☒ Off
Recording Format	Encoder1 ▼
Pre Record Time	1 Sec.
SAMBA Server IP	192.168.0.100
SAMBA Server Account	admin
SAMBA Server Password	••••••••
SAMBA Server Directory	/Public
SAMBA Status	NORMAL
SAMBA State	SAMBA service is not connected
SAMBA Total Bytes	0 MBytes
SAMBA Free Bytes	0 MBytes

OK Disconnected Connected

- **Samba Recording:** Enables or disables Samba recording
- **Samba Recording OSD:** Adds a timestamp to recorded AVI files
- **Samba Recording Continuous:** Enables or disables continuous recording
- **Recording Format:** Selects the recording stream and resolution
- **Pre-record Time:** Sets the pre-alarm recording duration
- **Samba Server IP:** Address of the Samba server
- **Samba Server Account:** Username for the Samba server
- **Samba Server Password:** Password for the Samba account
- **Samba Server Directory:** Destination directory for recordings
- **Samba Status:** Displays the Samba server status
- **Samba State:** Displays the connection state
- **Samba Total Bytes:** Displays total server storage
- **Samba Free Bytes:** Displays available server storage

Chapter 4-7 Maintenance



Chapter 4-7-1 Firmware Update

On the Maintenance page, select Load Default to restore factory settings or Reboot System to restart the camera. The interface indicates whether network settings are retained.

Select Export Config File to save the configuration, or Import Config File to load a saved configuration.

To update firmware, select Browse, choose the approved firmware file and select Submit.

Setup > Maintenance > Firmware Update

Please do not turn off power and wait until this web page shows up automatically. Fail to update firmware correctly due to network communication issue may damage this machine and may be required to ship back to your vendor for repair.

flashtnt9852x.bin:Application Firmware
 flashtnt9852x-s.bin:Encrypted Application Firmware
 pluginnt9852x.bin:plug-in package
 pluginnt9852x-s.bin:plug-in package

Browse... Submit

Upload 0%

Export Config File Export

Network Setting ☐
 System Setting ☒
 Controls Setting ☒
 Event Setting ☒
 Services Setting ☒
 Video Setting ☒

Import Config File Browse... Upgrade

Reboot System Reboot System

Default Settings

☒ Initialize without Network Settings & System Setting
☐ Initialize All Settings Load Default

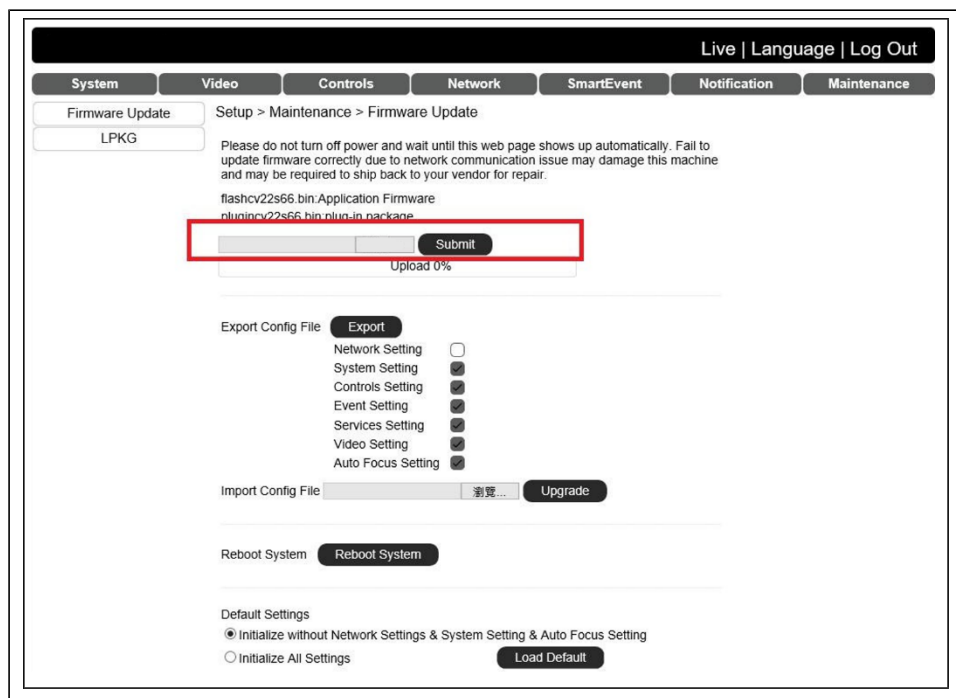
Warning: Do not disconnect power during a firmware update. Interruption may make the camera inoperable.

Note: If the password is lost and factory reset is not suitable, contact Innos Technologies for assistance.

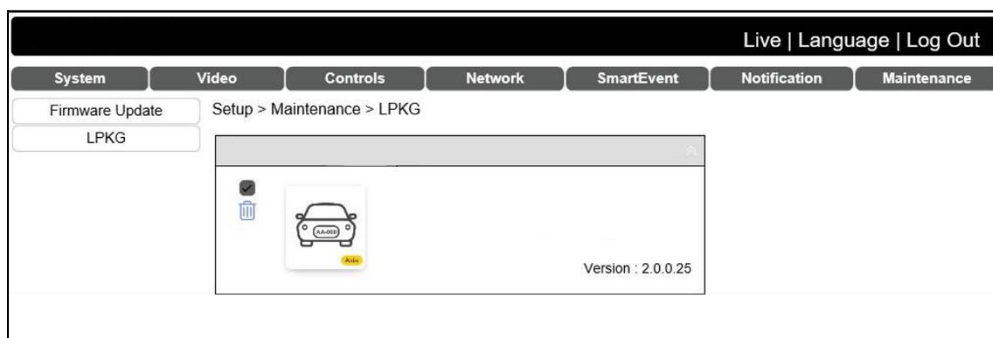
Chapter 4-8 AI Analytics Module (Optional)



Open Maintenance > Firmware Update, select Browse and choose the approved AI analytics plug-in file. The supplied package may use the filename plugincv22s66.bin. Select Submit to install it.



After installation, open the AI Plug-in Package page to view the installed module information.



Select the plug-in icon to open the AI analytics page. The service uses port 8592. Use the available controls to enable or remove the plug-in.  

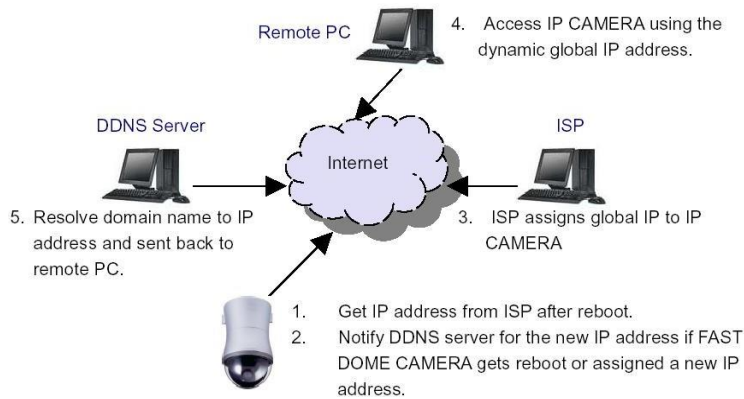


Appendix

DDNS Network Settings

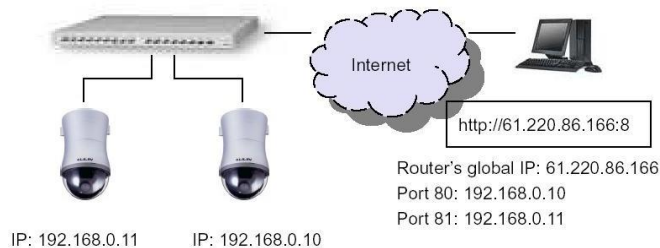
DDNS can provide remote access using a stable domain name when the camera's public IP address changes. The required configuration depends on the network and selected DDNS provider.

When the public IP address changes, the camera updates the configured DDNS provider. A remote user can then use the registered domain name, which the DDNS service resolves to the current public IP address.



Advanced Port Forwarding Technology

Port forwarding allows multiple devices on a private network to be reached through one public IP address. In the example below, router port 80 forwards to 192.168.0.10 and port 81 forwards to 192.168.0.11. A remote connection to public port 81 is forwarded to 192.168.0.11.



Restore to Factory Default

To restore the camera to its factory-default settings, follow these steps:

1. Press and hold the Reset button for 15 seconds, then release it.
2. Wait for the camera to restart.
3. Run IPScan to locate the camera on the network.
4. Open the camera's IP address in a supported web browser.
5. For security, create a new administrator username and password during the first login. Select Confirm to save the credentials and sign in.