

TRENDNET[®]

User's Guide



**Indoor/Outdoor 5MP H.265 WDR PoE IR
Bullet Network Camera**

**Indoor/Outdoor 5MP H.265 WDR PoE IR Fixed
Turret Network Camera**

TV-IP1514PI / TV-IP1515PI

Table of Contents

Summary.....	4
Key Features.....	4
Disclaimer	4
Caution	4
Chapter 1 System Overview	5
Chapter 1-1 System Requirements	5
Chapter 2 Before Accessing IP Cameras.....	5
Chapter 2-1 Configure IP Addresses using the Camera Search Tool	5
Chapter 2-2 Configure IP Addresses through HTML Connection	6
Chapter 2-3 Web Browser Settings & Software Components Required	6
Chapter 2-4 Login	7
Chapter 3 Camera Operations	8
Chapter 3-1 Live View 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	12
Chapter 4-2-1 General.....	12
Chapter 4-2-2 Quality Basic	13
Chapter 4-2-3 Quality Advance.....	13
Chapter 4-2-3-1 Sense Up+.....	15
Chapter 4-2-3-2 White Balance Control (AWB)	15
Chapter 4-2-5 Privacy Mask.....	16
Chapter 4-3 Controls	16
Chapter 4-3-1 Global Counter.....	16
Chapter 4-3-2 Virtual Input.....	17
Chapter 4-3-3 Metadata	17
Chapter 4-4 Network.....	19
Chapter 4-4-1 General.....	19
Chapter 4-4-2 HTTP Service	19
Chapter 4-4-3 RTSP.....	20
Chapter 4-5-1 SmartEvent	22
Chapter 4-5-2 Motion Detection	24
Chapter 4-6 Notification	24
Chapter 4-6-1 FTP Service	24
Chapter 4-6-2 SMTP (Email) Service	25
Chapter 4-6-3 HTTP POST Service	25
Chapter 4-6-4 SD Card Service	26
Chapter 4-6-5 SD Card Backup File	26
Chapter 4-6-6 Samba Service.....	26
Chapter 4-7 Maintenance.....	27
Appendix.....	28
DDNS Network Settings	28
Advanced Port Forwarding Technology.....	28
Restore to Factory Default	28
Federal Communication Commission Interference Statement	29

RoHS.....	29
Europe – EU Declaration of Conformity	29
Limited Warranty	32

Summary

TRENDnet's Indoor/Outdoor 5MP network camera provides day and night surveillance with a night vision range of up to 30 meters (98 ft.). This bullet network camera delivers year-round surveillance with an IP66 weather rated housing to withstand outdoor environments. Record up to 5MP HD video at 20fps in a space saving H.265 compression format. Easily view live video from the 5MP PoE camera on your mobile device using our free Sentinel mobile app, or on your PC with our free View Manager desktop camera video management software.

Key Features

- Easy Cloud P2P QR code installation
- 5MP HD video (2592 x 1920) at 20 fps
- Night vision IR LEDs for night vision up to 30m (98 ft.)
- Built-in microphone for one-way audio
- Outdoor IP66 weather rating
- Wide Dynamic Range image balancing
- Save installation costs with Power over Ethernet (PoE)
- Programmable motion detection recording and email alerts
- Micro SD card slot (up to 256GB)
- Free Sentinel iOS® and Android™ mobile apps
- Complimentary View Manager PC software
- NDAA / TAA Compliant

Disclaimer

Please be aware that this user manual may cover a range of product specifications for various models. Characteristics and features discussed and/or illustrated in this manual may not be applicable or available to all models. We reserve the right to change product specifications, designs and equipment without notice and without incurring obligation.

Caution

- Do not drop or damage the equipment
- Do not install the equipment near fire or heat sources
- Keep the equipment from rain, moisture, smoke, or dust
- Do not cover the opening of the cabinet with cloth and/or plastic or install the unit in poorly ventilated places. Allow 10cm between this unit and its surroundings
- Do not continue to operate the unit under abnormal conditions such as smoke, odor, or loss of signal whilst power is turned on
- Do not touch the power cord with wet hands
- Do not damage the power cord or leave it under pressure
- To avoid unnecessary magnetic interference, do not operate this unit near magnets, speaker systems, etc.
- All connection cables should be grounded properly

Chapter 1 System Overview

Chapter 1-1 System Requirements

TRENDnet's IP camera uses compression technology that provides high compression rate and superior video quality. However, video performance depends highly on CPU power and network bandwidth for video streaming. The following sections specify the system requirements for using TRENDNET IP cameras.

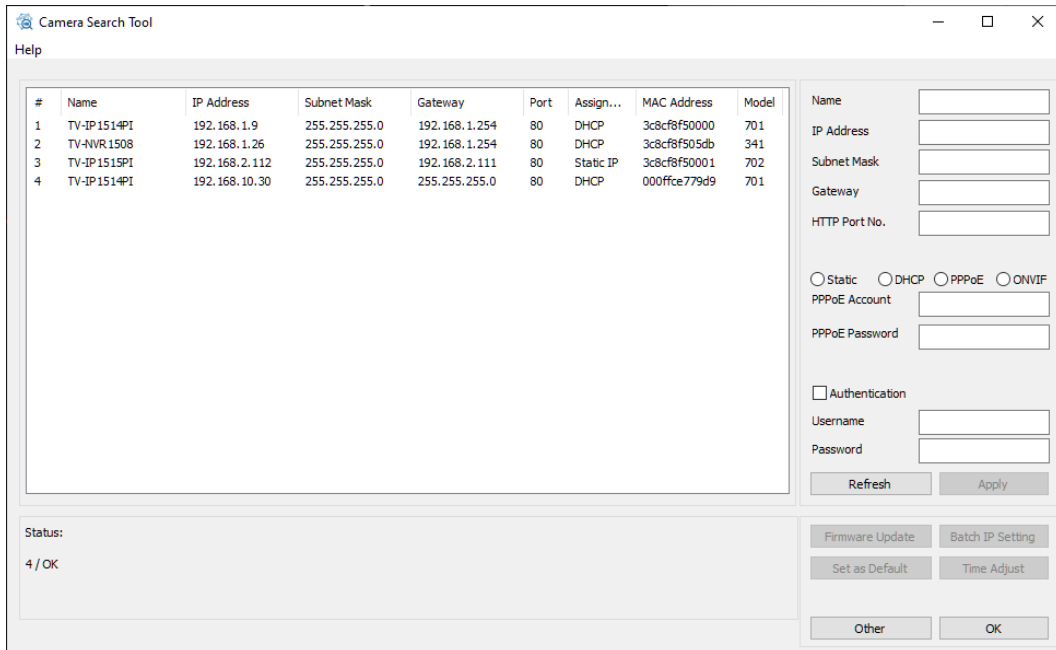
Chapter 2 Before Accessing IP Cameras

Before accessing the IP cameras, make sure that the camera's RJ-45 network connector, audio cable, and power cable are properly connected. To set the IP address, consult your network administrator. Users can use the default IP address to verify the camera's network connection.

Chapter 2-1 Configure IP Addresses using the Camera Search Tool

To configure the IP address of your cameras, download the tool from our website. To change the IP address, subnet mask, gateway, or HTTP port of your cameras, follow the steps below:

- Run the Camera Search Tool
- Click **Refresh**. All available devices will be listed on the screen
- Select the device item from the device list
- To edit or modify IP address, subnet mask, gateway, or HTTP port, use the box
- Click **Apply** for the changes to take effect
- Click **Refresh** again to verify the changed settings



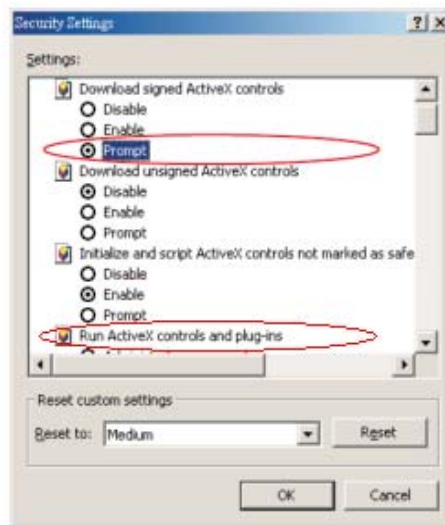
Chapter 2-2 Configure IP Addresses through HTML Connection

To change an IP address on a webpage, type the default IP address (192.168.10.30) into the browser address bar and follow the steps below:

- Due to security reason, create the username and password for the first login. To login to the IP camera, please create the username and password on the login page. Press **Confirm** to complete the setting and login simultaneously.
- 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

Make sure your Internet Explorer allows signed ActiveX plug-in to run on your PC (Active X is not supported in other browsers). Set Download Signed ActiveX plug-in controls to Prompt and enable Run ActiveX control and plug-in. You can set this in Internet Explorer→Tools→Internet Options→Security→Custom Settings.

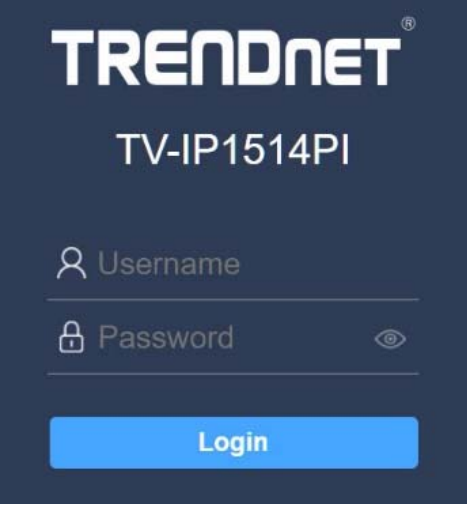


Once completed, you can access the IP camera's live video by entering the default IP address via a web browser. A security warning dialog box will appear. Click OK to download the ActiveX directly from the IP camera.

Please download the latest plugin (IPVide_Plus_TRENDnet.cab) from TRENDnet's website.

Chapter 2-4 Login

Due to security reason, create the username and password for the first login. To login to the IP camera, please create the username and password on the login page. Press **Confirm** to complete the setting and login simultaneously.



The image shows a login interface for a Trendnet TV-IP1514PI camera. The background is dark blue. At the top, the 'TRENDNET' logo is displayed in white, with a registered trademark symbol. Below the logo, the model number 'TV-IP1514PI' is shown in white. There are two input fields: the first is labeled 'Username' with a person icon to its left, and the second is labeled 'Password' with a lock icon to its left and an eye icon to its right. Below these fields is a blue button with the word 'Login' in white text.

Minimum Password Strength Requirements:

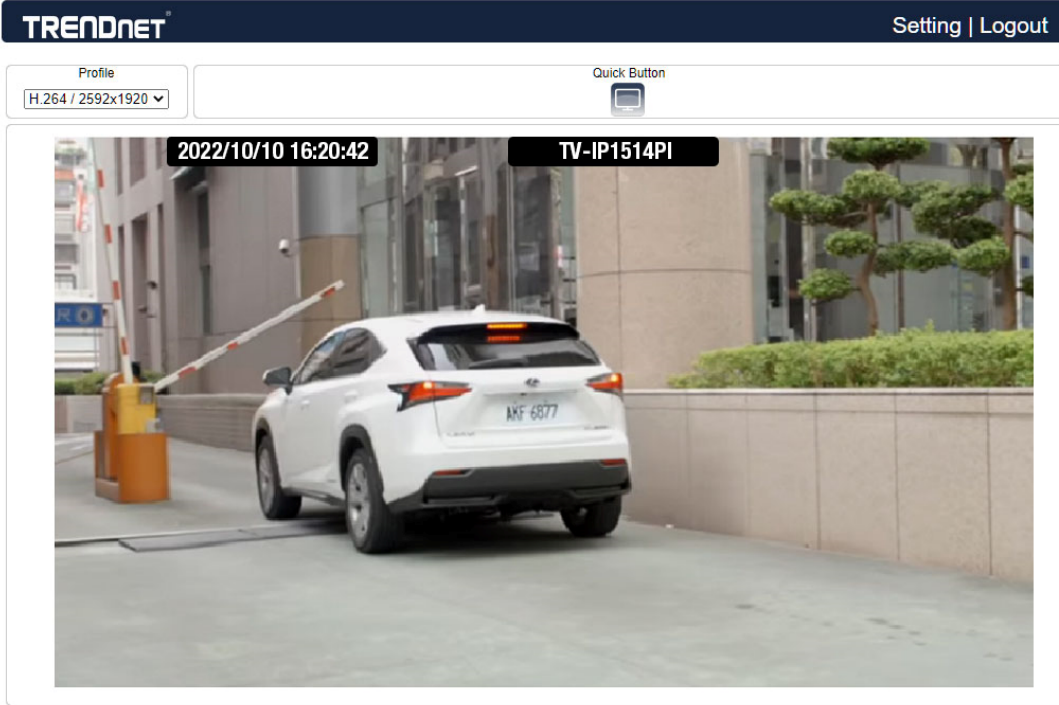
1. The password length must be 8 or more characters.
2. The password must include at least 1 number (0 ~ 9), 1 uppercase letter, 1 lowercase letter and 1 symbol (~ ? / + = , ; . ' @ # ¥ % ^ & * () _ -).

Note: Please preserve the credential for accessing the camera properly. Forgetting the credential for accessing the camera, please perform hardware factory default.

Chapter 3 Camera Operations

When logged in as an administrator, two main features are available: 1) camera operations and 2) configurations.






Chapter 3-1 Live View Operations



1. **Quick buttons:** IP camera shortcuts
2. **ActiveX display screen:** Display RTSP H.264 or MJPEG streaming video
3. **Profile switching menu:** Switching from one profile to another
4. **Setup buttons:** IP camera setup menu

Chapter 3-2 Quick Buttons

The quick control panel buttons (Compatible with IE only) are described below:
Files are saved locally under IPVideo folder. (eg. C:\IPVideo)

	Take a snapshot of the video
	Start recording
	Pause recording
	Alarm out
	Enlarge the live view

Chapter 4 Settings

As an administrator, you can configure the IP camera via a standard HTML webpage. Click Setup at the top-right corner of the screen after you log in to the camera.



Chapter 4-1 System



Chapter 4-1-1 General

Under System Settings→General, you will see server system information, such as MAC address, firmware version, os version, system reboot time, and device name settings. To modify these options, follow the instructions below:

Setup > System > General

MAC Address	3c:8c:f8:f5:00:00
Firmware Version	9.0.001.3675
OS Version	Linux 4.9.84
System Reboot Time	2022/10/10 14:36:58 Mon PDT
Device Name	<input type="text" value="TV-IP1514PI"/>
<input type="button" value="OK"/>	

- **MAC Address:** The MAC address of the IP camera
- **Firmware Version:** Firmware version of the IP camera
- **OS Version:** The version number of the IP camera
- **System Reboot Time:** The last time your system was rebooted.
- **Device Name:** The device name can be found using the Camera Search Tool, which allows you to identify the IP cameras. To change the device name, enter a new name for the IP camera and click OK.

Chapter 4-1-2 User

The IP camera supports up to 10 user accounts. Each account can be individually configured for its access rights. To add/edit a user, click Add/Edit User. To access an IP camera without authentication, switch the Bypass Logon option to On. Enable IPScan Bypass Logon to log in the IP camera through IPScan without authentication. To add a user, press Add User, and you will see the following screen:

Setup > System > User

Bypass Logon OFF
IPScan Bypass Logon ON
Password Strength OFF
Authentication Security OFF Within: Min. Failed Login Attempts: IP Block Length: Min.

Account
New Password
Confirm Password
User Group Administrator, Operator, Viewer

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.

Enter the account name, password and confirm password to add new account, and then check to assign the access rights for this account. Click OK to update the settings.

To edit account information, select user for edit and click Edit User. To delete a user, select user for delete and click Remove User. Click Submit to update the settings.

Chapter 4-1-3 Timer Settings

You can change the time of your camera through a HTML web page. Simply select the date and time in the drop-down menus, and click OK to apply. You may also set the holiday list in this page.

Setup > System > Timer

Server Time 2022/10/10 16:58:55 GMT-0800
Synchronize with NTP Every Hour Off
Time Server
Time Zone
Time / / : :
Enable Holiday List

Synchronize with an NTP server

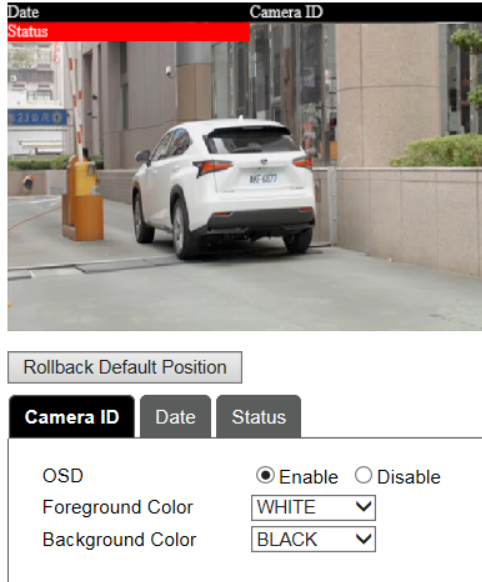
To synchronize with an NTP server, change the Synchronize with NTP to Every Hour. The camera will synchronize its system time with a time server every hour.

Note: This function requires Internet connection.

Chapter 4-1-4 OSD Settings

OSD (on screen display) is for the use of displaying system information on the video. There are features of date and status available.

Setup > System > OSD



Camera ID, Date and Status 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

You can view the system-generated log in this page. Click Save  icon to export the log to a text file. You can also search for log file by selecting the type keyword.

Setup > System > System Log

IP Address	User	Date & Time	Log Description
192.168.1.38	admin	2022/10/11 14:55:18	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:50:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:44:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:38:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:32:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:27:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:21:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:16:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:10:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 14:04:17	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 13:59:07	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 13:54:06	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 13:49:06	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 13:44:06	HTTP User Reject(SYSTEM WRONG)
192.168.1.38	admin	2022/10/11 07:24:39	HTTP User Reject(SYSTEM WRONG)

Chapter 4-2-1 General

To transmit video over a low bandwidth network such as the Internet, set the bit rate close to the actual upload bandwidth. The camera encodes frames based on the bit rate setting.

Setup > Video > General

Video Standard : 60Hz 50Hz

Encoder1

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

Encoder3

Profile Name

Resolution

Output Frame Rate

GOP (Group of Pictures)

Stream Mode

Bit Rate

RTSP URL

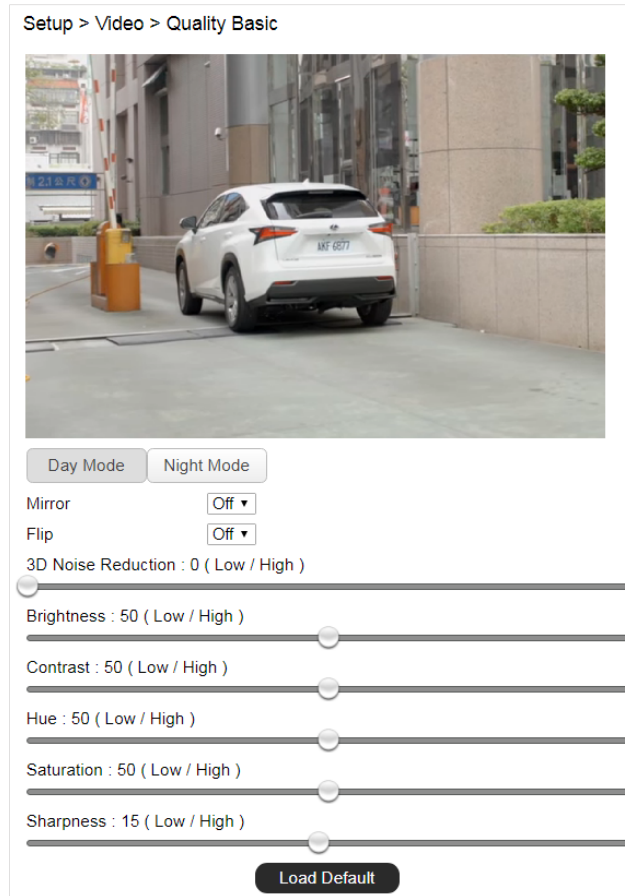
OK

Load Default

- **Profiles:** 3 customizable profiles
- **Video Standard:** NTSC/PAL setting
- **Profile Name:** The selection of H.264/H.265 video compression
- **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:** Variable bit rate, an encoding mode that reduces the use of bandwidth;
- **CBR:** constant bit rate, an encoding mode that consumes more bandwidth
- **Bit rate:** The maximum bit rate available for your network connection
- **RTSP URL:** Allow you to access the video stream via the Real Time Streaming Protocol
- **Image Quality:** The compression rate of the H.264/H.265 stream

Chapter 4-2-2 Quality Basic

This menu allows you to adjust brightness, contrast, contrast, hue, saturation, and sharpness both for the Day Mode and Night Mode. Individual day/night settings ensure the camera to provide optimal video quality.



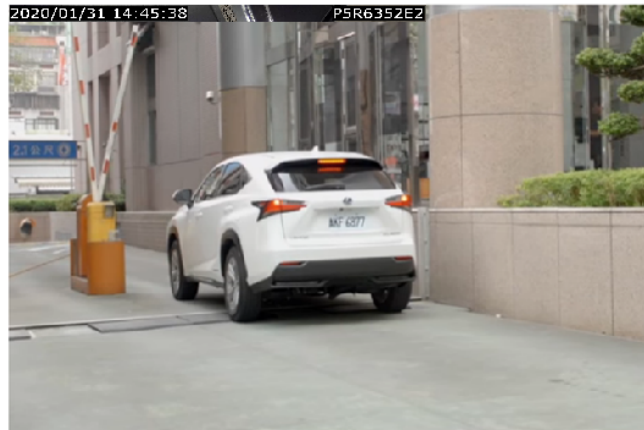
- **Mirror:** Mirror the video
- **Flip:** Flip the video
- **3D Noise Reduction:** If the noise of the video is high at night, set the setting to high if needed.

Chapter 4-2-3 Quality Advance

In this page, you have access to Exposure, Automatic Gain Control, White Balance Control, Sense Up, Shutter Speed, and IR-Cut settings allowing you to adjust camera video quality for day and night.

The camera provides two sets of video quality database for day or night mode. This is very useful settings for video quality especially for ANPR/LPR application where the shutter speed can be customized at night. The video quality settings can be applied by Day and Night Switch explained later in this chapter.

Setup > Video > Quality Advance



Day Mode Night Mode

White Balance Control	Auto
Exposure Value	8
WDR	Auto
Shutter Value Range	Min: 1/20000 Max: 1/25
Auto Gain Control(SENSE UP+)	24
Sense Up	Off
Color Mode	Color
IR LED	0
IR Cut Filter	On

Load Default

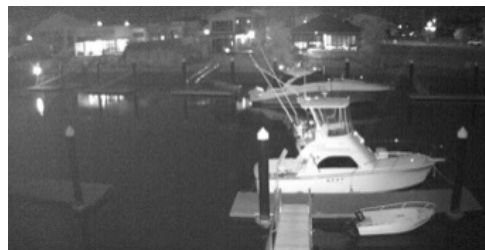
Video setting options are described as follows:

- **White Balance Control:** adjusts the white balance manually or automatically
- **Exposure Value:** adjusts the value of exposure; the higher the value is set, the brighter the video is
- **WDR:** enables or disables Wide Dynamic Range to capture greater details
- **Shutter Value Range:** set the min and max shutter values
- **Auto Gain Control (Sense Up+):** see the below description
- **Sense Up:** select the level of Sense Up to enhance the video
- **Color Mode:** switch between color/black-and-white mode
- **IR LED:** IR LED control
- **IR Cut Filter:** enable/disable the IR cut filter

Without Sense Up

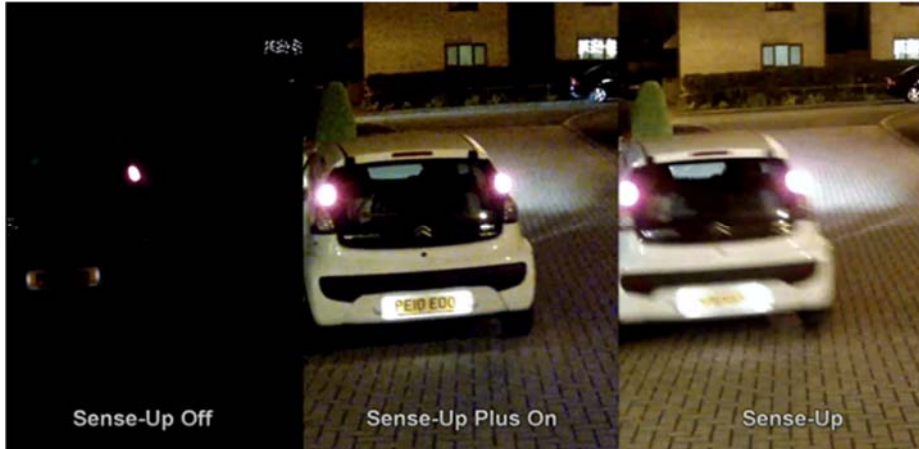


Sense Up by 3 Frames



Chapter 4-2-3-1 Sense Up+

Sense Up+ (AGC) is a low-light and high-sensitivity DSP control that enables outstanding video quality even in low-light environments. Sense Up+ technology can be used for both black-and-white and/or color video modes. To enable Sense Up+, first enable Auto Gain Control (AGC). Use Sense Up+ with 3D noise reduction (3D DNR) can reduce noise that occurs in low light environments. AGC and 3D DNR do not cause motion blur. If the picture is still too dark under the environment, turn on Sense Up (slow shutter) instead, however, it may cause motion blur in low-light conditions.



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

There are day time and night time auto white balance controls (ATW) for the camera.

White Balance Control	Manual ▼
R-Gain	1 ▼ (1~255)
B-Gain	1 ▼ (1~255)

- **White Balance Control:** Auto white balance and manual white balance
- **R-Gain:** Red gain specific auto white control
- **B-Gain:** Blue gain specific auto white control

Chapter 4-2-4 Day Night Mode Switch

The Day/Night Mode Switch allows you to schedule IR activities by (1) auto, (2) day, (3) night, (4) schedule, or (5) external control. When the setting is set to Auto, the IR module is turned on/off automatically according to the signal from the light sensor. The Night setting removes the IR cut filter, and the Day setting keeps the filter on. If you choose Schedule, the filter turns on/off according to the set time period.

Setup > Video > Day Night Mode Switch

Auto , Switch Delay Time 1 ▼ Sec.

Day Mode

Night Mode

Schedule

Day to Night Time 0 ▼ : 0 ▼

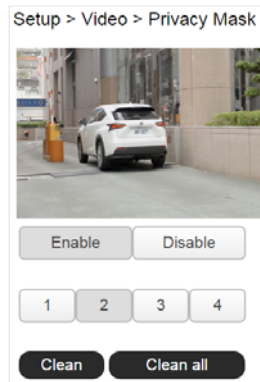
Night to Day Time 0 ▼ : 0 ▼

OK

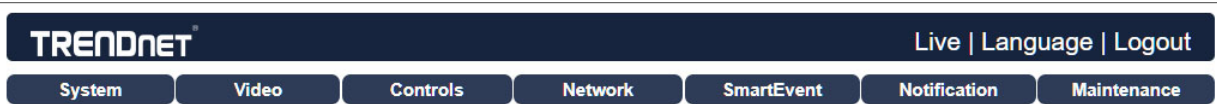
Note: IR-cut camera model only

Chapter 4-2-5 Privacy Mask

TRENDNET camera provides up to 4 sets of privacy masking. Select any of the masking numbers and drag to mask specific areas.



Chapter 4-3 Controls



Chapter 4-3-1 Global Counter

The global counters are for counting a trigger of a remote device. The global counter can be triggered by a metadata, or a virtual input. The global counters can be used for output purposes, such as LED display.

Setup > Controls > Global Counter

Global Counter #1	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #2	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #3	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #4	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #5	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #6	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #7	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #8	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #9	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #10	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #11	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #12	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #13	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #14	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #15	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>
Global Counter #16	State:	<input type="text" value="0"/>	<input type="button" value="Set"/>

Chapter 4-3-2 Virtual Input

The IP camera provides up to 16 virtual inputs. The virtual inputs are CGI commands that these can be used for other remote device to trigger.

Setup > Controls > Virtual Input

Virtual Input #1	State:	<input checked="" type="checkbox"/> 1
Virtual Input #2	State:	<input type="checkbox"/> 0
Virtual Input #3	State:	<input type="checkbox"/> 0
Virtual Input #4	State:	<input type="checkbox"/> 0
Virtual Input #5	State:	<input type="checkbox"/> 0
Virtual Input #6	State:	<input type="checkbox"/> 0
Virtual Input #7	State:	<input type="checkbox"/> 0
Virtual Input #8	State:	<input type="checkbox"/> 0
Virtual Input #9	State:	<input type="checkbox"/> 0
Virtual Input #10	State:	<input type="checkbox"/> 0
Virtual Input #11	State:	<input type="checkbox"/> 0
Virtual Input #12	State:	<input type="checkbox"/> 0
Virtual Input #13	State:	<input type="checkbox"/> 0
Virtual Input #14	State:	<input type="checkbox"/> 0
Virtual Input #15	State:	<input type="checkbox"/> 0
Virtual Input #16	State:	<input type="checkbox"/> 0

Chapter 4-3-3 Metadata

Metadata is the HTTP response of a CGI command. TRENDNET IP camera is able to receive the metadata from an IP device. The metadata is the URL response of an IP device.

Setup > Controls > Metadata

Number	1
Metadata Enable	<input type="checkbox"/>
Metadata Server Name	<input type="text" value="metaservername0"/>
Metadata Type	<input type="text" value="HTTP Multipart Response"/>
Metadata Server IP/DNS	<input type="text" value="metaserver.com"/>
Metadata Server Port	<input type="text" value="80"/>
Account	<input type="text" value="Account"/>
Password	<input type="password" value="*****"/>
Metadata URL	<input type="text" value="/url"/>
Metadata Parser	<input type="text" value="parser"/>

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 example below, TRENDNET IP camera is able to receive the metadata of motion events, MotionDetect token of /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.

To setup metadata, finish the settings below:

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: The IP address of an integrated device.
Metadata Server Port: The port number of the integrated device.
Account: Account name of an integrated device.
Password: password of an integrated device.
Metadata URL: The URL of the an integrated device. "/" is required.
Metadata Parser: The parsing tokens for the valuables of Triggers.

Special characters

If there are special characters such as "/", "\r", "\n", and "\r\n" in the metadata, enter special characters for parsing the metadata.

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

Setup > Controls > Metadata

Number	1
Metadata Enable	<input type="checkbox"/>
Metadata Server Name	<input type="text" value="metaservername0"/>
Metadata Type	HTTP Multipart Response ▾
Metadata Server IP/DNS	<input type="text" value="metaserver.com"/>
Metadata Server Port	<input type="text" value="80"/>
Account	<input type="text" value="Account"/>
Password	<input type="password" value="*****"/>
Metadata URL	<input type="text" value="/url"/>
Metadata Parser	<input type="text" value="parser"/>

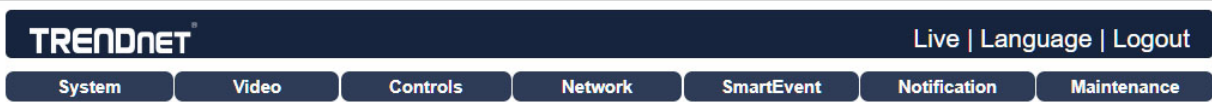
Enter the parsing tokens in the meta parser field for triggering an event from metadata URL of a third party device. The max length is 127 characters including spaces.

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
  
```



Chapter 4-4-1 General

Network settings are the basic settings that connect TRENDNET IP cameras to the network. The default IP address of IP cameras is 192.168.10.30. Enter this IP address into your web browser to verify the network connection between a local PC and your IP camera.

To set up a local area network, enter the IP address, subnet mask, gateway, and DNS. Click OK to update the settings.

Setup > Network > General

Network	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
IP Address	<input type="text" value="192.168.10.30"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.0.1"/>
Primary DNS	<input type="text" value="168.95.1.1"/>
Secondary DNS	<input type="text" value="168.95.1.1"/>
QoS(DSCP)	<input type="text" value="0"/> (0~63)

To acquire Internet access, contact your local Internet Service Provider (ISP) for a global IP address. Enter the IP address (global), subnet mask, and gateway IP provided by your ISP.

- **Primary DNS** —The IP address of the default and first DNS server
- **Secondary DNS IP Address**—The IP address of the backup and second DNS server to the default DNS
- **QoS(DSCP)** —Based on DSCP standard, set the TCP/IP packet header for packet priority.

A router, gateway, or other DHCP software server can remotely assign an IP address to your IP camera. There is no need to manually configure the IP address, subnet mask, and gateway. However, every time the DHCP service is rebooted, the IP address of the IP camera may vary. You may need to use IPscan to search for the IP camera. To enable DHCP, click the DHCP option and click Submit.

Note: Once the DHCP option is enabled, the IP camera is assigned an IP address by the DHCP server. This feature is only permitted in LAN environments.

Chapter 4-4-2 HTTP Service

HTTP is a reliable protocol for video streaming. With correct port forwarding, videos can be sent over the Internet. Details are described in the appendix. To change the HTTP port number, consult your network administrator. Choose the streaming type you want to use (HTTP & HTTPS or HTTPS). Click OK for the changes to take effect.

Setup > Network > HTTP Service

HTTP Port	<input type="text" value="80"/>
HTTP Connection Policy	<input checked="" type="radio"/> HTTP & HTTPS <input type="radio"/> HTTPS Service

Chapter 4-4-3 RTSP

RTSP is another reliable protocol for video streaming. With correct port forwarding, videos can be sent over the Internet. Details are described in the appendix.

Setup > Network > RTSP

RTSP Port	<input type="text" value="554"/>
RTSP Authentication	<input checked="" type="radio"/> On <input type="radio"/> Off
Encoder1	<input type="text" value="stream0"/>
Encoder2	<input type="text" value="stream1"/>
Encoder3	<input type="text" value="stream2"/>

Settings on this page are described below:

- **RTSP Authentication:** Enabling this option will require username and password when connecting to the RTSP stream
- **Encoder:** Change encoder name.

Chapter 4-4-4 HTTPs Service

TRENDNET IP camera support HTTPs (Hypertext Secure Transmission Protocol) service. HTTPs is an Internet protocol that ensures the integrity and confidentiality of data as it travels between users' computers and websites. When users visit any website, they want a secure and private online experience.

HTTPs can be regarded as the advanced security version of HTTP. The SSL protocol is added as a security certificate. Therefore, the website can prevent data thief from directly seeing the transmitted data even if they intercept the transmitted information by using the encryption on the agreement.

HTTPs Service Enable Disable

There are two options to set HTTPs service:

1. The first option is to create a free self-signed certificate by filling-in the blank field below, then click **Create a certificate.**

HTTPs Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTPs Status	Disable
Certificate Status	Not installed
Method	<input type="text" value="Create self-signed certificate"/>
Country	<input type="text" value="US"/>
State or province	<input type="text" value="Taiwan123"/>
Locality	<input type="text" value="Taipei123"/>
Organization	<input type="text" value="IPCAM12"/>
Organization Unit	<input type="text" value="IPCAM123"/>
Common Name	<input type="text" value="nw.example.com@@123"/>
Validity	<input type="text" value="365"/>

A pop up message will display:



Then, you will notice that **Certificate Status** has changed from **Not Installed** to **Active**

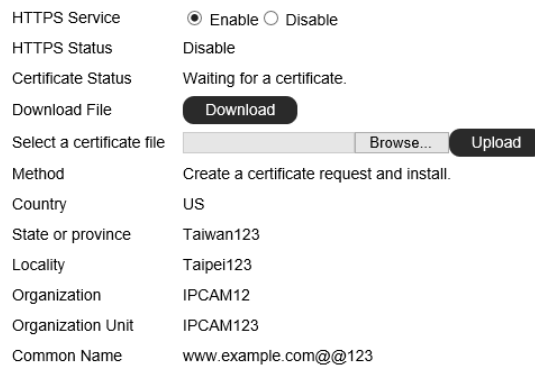


Click **OK** to activate HTTPS function. And the **HTTPS Status** will have changed from **Disable** to **Enable**.



This IP Camera may now be connected via HTTPS protocol with your browser

2. The second option is to purchase an SSL certificate by selecting **Create a certificate request and install**. After purchasing the SSL certificate from a third party company, browse your computer to upload the SSL certificate. If it is successful, the **Certificate Status** will have changed from **Not Installed** to **Active**. And **HTTPS Status** will have changed from **Disable** to **Enable**.



Chapter 4-4-5 DDNS

The DDNS service allows you to automatically update the DNS server. TRENDNET provides three DDNS servers to choose from (we recommend you use the first one from the drop-down menu). Click OK for the changes to take effect.

Setup > Network > DDNS

Server Name

DDNS ON

Account

Password

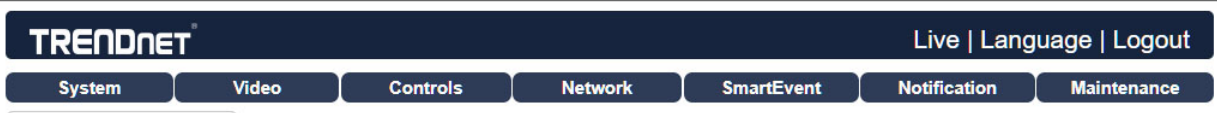
Host Name

WAN IP

To activate DDNS, go to www.ddnsipcam.com. If the IP camera is on Internet with a global IP address, use the last 6 digits of the MAC address as the host name with default account and the default password,. The IP camera will automatically register to www.ddnsipcam.com.

Note: The DDNS feature requires Internet connection.

Chapter 4-5-1 SmartEvent



Here you can configure the detection settings for alarm, global counter, virtual input, meta data and network failure. Choose an event type for entering the event name and event condition for triggering an alarm. Click **Save the event** button for saving 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 0/3)

Trigger

Enable	Trigger	Operator	Value	Duration
<input type="checkbox"/>	Network Detection	=	<input type="text" value="1 or 0"/>	<input type="text" value="0"/> Sec.

Then the page you see allows you to choose the action to take when the chosen events are detected, such as sending JPEG images to an FTP server or an email account. To schedule event monitoring, choose **Schedule** when you edit an event and highlight the time periods you want the camera to detect events. Click **Save the event** button to update the settings.

Setup > SmartEvent > SmartEvent

Enable Event 1

Event Name

Condition 1 Condition 2 Condition 3 Condition 4 Condition 5

Condition Name

Trigger Schedule Action

Enable Holiday List

Select	Schedule	Start Time	End Time
<input checked="" type="checkbox"/>	All	0:00	23:59
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00
<input type="checkbox"/>	Sun	0:00	0:00

Click **Action** to select the outputs for event triggering.

Setup > SmartEvent > SmartEvent

Enable Event 1

Event Name

Condition 1 Condition 2 Condition 3 Condition 4 Condition 5

Condition Name

Trigger Schedule Action

(Current number/Maximum number of Action Rule is 0/10)

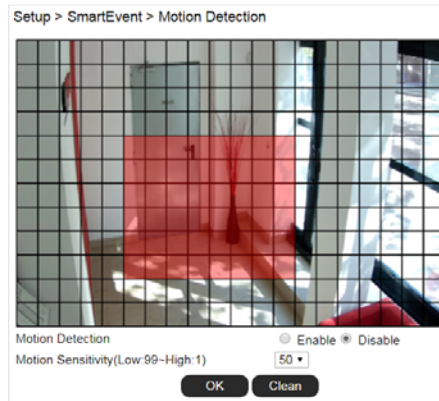
- FTP Service, Rule Number:0 [Edit](#)
- SMTP Service, Rule Number:0 [Edit](#)
- Push Service Setting, Rule Number:0 [Edit](#)
- HTTP POST Service, Rule Number:0 [Edit](#)
- Global Counter, Rule Number:0 [Edit](#)
- Virtual Input, Rule Number:0 [Edit](#)
- SD Card Service, Rule Number:0 [Edit](#)
- SAMBA Service, Rule Number:0 [Edit](#)

- **FTP Service:** Mail event logs to an FTP server.
- **SMTP Service:** Mail event logs to an SMTP server.
- **Push Service Setting:** When the alarm is triggered, can send push notification to specified iOS and Android.
- **Alarm Out:** Trigger the digital output of the IP camera.
- **HTTP POST Service:** Send notification snapshots to a specified website when alarm is triggered.
- **Global Counter:** To set a value between 0 and 65,535 or add value range from -99 to 99.
- **Virtual Input:** Enable or disable a specific virtual input among the 16 sets.
- **SD Card Service:** When the alarm is triggered, the screenshot is saved to the SD card.
- **Samba Service:** Set to send data of the selected encoder profile to the predefined samba server.

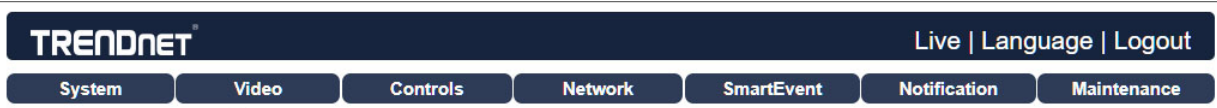
Note: To activate SmartEvent / Action setting, please also configure corresponding action in **Controls** setup page or **Notification** setup page.

Chapter 4-5-2 Motion Detection

The IP camera provides motion detection feature. Click on Motion Detection to determine the areas to monitor. Simply double-click or drag across the areas you want to monitor, and cancel your selection by double-click again or drag across the areas you don't want to monitor with the right mouse button. Click OK button to update the settings.



Chapter 4-6 Notification



Chapter 4-6-1 FTP Service

Enter the required FTP information to send 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

- **FTP Channel:** There are three FTP servers that can be configured.
- **Number:** The number of FTP service.
- **FTP Server Name:** The name of the FTP server.
- **FTP/DNS Server:** The FTP server's address.
- **FTP/DNS Server Port:** The FTP server's port number.
- **Account:** The account name to log in to the FTP server.
- **Password:** The password of the account.
- **Directory:** The file path for storing the JPEG snapshots.
- **Prefix:** The prefix of the JPEG filename.
- **Postfix:** The postfix of the JPEG filename.
- **File Format:** The JPEG file format based on different JPEG encoder.

Chapter 4-6-2 SMTP (Email) Service

For alarm notification with JPEG snapshots, enter the required information to enable this Email notification service.

Setup > Notification > SMTP Service

E-mail Receiver Setting

E-mail Address1: receiver@mail.com

E-mail Address2: []

E-mail Address3: []

E-mail Address4: []

E-mail Address5: []

E-mail Sender Setting

E-mail Address: sender@mail.com

SMTP Server: mail.com

SMTP Authentication

Auth Login

Auth SSL

Auth TLS

SMTP Port: 25

Authentication: OFF

Auth Account: sender

Auth Password: []

OK Send Mail & Status

- **Receiver E-mail Address:** Address of receiving mailbox.
- **Sender E-mail Address:** Address of sending mailbox.
- **SMTP Server:** Enter the address of mail server.
- **SMTP Authentication:** Select authentication type
- **SMTP Port:** The default port number is 25 (mail server port).
- **Authentication:** Enable or disable mail service
- **Auth Account:** User name of the mail server
- **Auth Password:** Password of sending mailbox.

Chapter 4-6-3 HTTP POST Service

Through the POST protocol, the camera can automatically send notification snapshots to a website if an alarm is triggered.

Setup > Notification > HTTP POST Service

Number: 1

HTTP POST Server Name: httpservername

HTTP POST Server IP/DNS: httpserver.com

HTTP POST Server Port: 80

Account: admin

Password: []

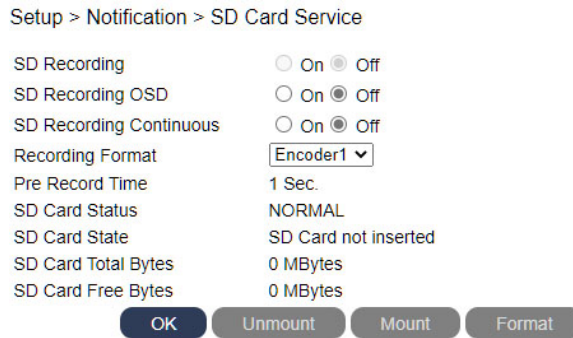
HTTP POST URL: /url

HTTP POST JSON: /json

- **HTTP POST Server Name:** The HTTP POST server
- **HTTP POST Server IP/DNS:** The IP/DNS address of the HTTP Post server
- **HTTP POST Server Port:** The port number of the HTTP Post server
- **Account:** The account
- **Password:** The password
- **HTTP POST URL :** The CGI command to send HTTP POST
- **HTTP POST JSON :** The JSON text editor

Chapter 4-6-4 SD Card Service

Ensure a SD card is properly installed to the camera before you enable the SD recording option. The camera will start recording videos when an alarm occurs.



Warning: Ensure to click **Unmount** before removing the SD card, or the system may crash.

Note: SD card model only

Chapter 4-6-5 SD Card Backup File

To download a specific clip, right-click the file you want to download and save the AVI file to a local PC.

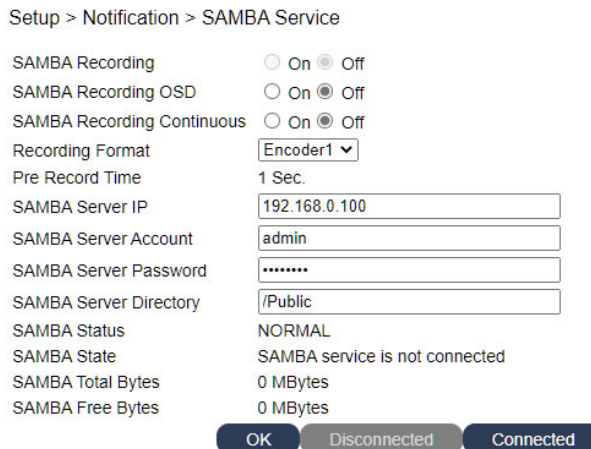
Setup > Notification > SD Card Backup File

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



Chapter 4-6-6 Samba Service

The streaming of the camera can be recorded as AVI files to a Samba server. Continuous and pre-alarm recordings are available. To do so, provide required information for Samba service. Circular recording is available for overwriting the oldest recording files if the Samba server gets full.



- **Samba Recording:** Enable Samba recording service.
- **Samba Recording OSD:** Timestamp OSD on the AVI files
- **Samba Recording Continuous:** Enable/disable Samba continuous recording.
- **Recording Format:** The resolution of the AVI files
- **Pre-record Time:** Pre-alarm recording based on the alarm settings
- **Samba Server IP:** The IP address of the Samba server
- **Samba Server Account:** The account of the Samba server
- **Samba Server Password:** The password of the Samba server
- **Samba Server Directory:** The target path of the recordings on the Samba server
- **Samba Status:** The system status of the Samba server
- **Samba State:** The connection status of the Samba server
- **Samba Total Bytes:** The storage size of the Samba server
- **Samba Free Bytes:** The free storage size of the Samba server

Chapter 4-7 Maintenance



In the Maintenance page, you can click Load Default to restore the camera to factory settings, or click Reboot System to restart the camera. Restoring to factory settings does not affect IP addresses.

To export camera settings, click on Export Config File for other cameras. Click on Import Config File for importing camera settings.

To update the firmware of your IP camera, click Browse and locate the update file. Click Submit to start the firmware update.

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.

flashssc327a.bin:Application Firmware

Choose File No file chosen

Upload 0%

Export Config File

Network Setting

System Setting

Controls Setting

SmartEvent Setting

Notification Setting

Video Setting

Import Config File No file chosen

Reboot System

Default Settings

Initialize without Network Settings & System Setting

Initialize All Settings

Warning: Never disconnect the power during the update. This could cause irreversible damage to your device.

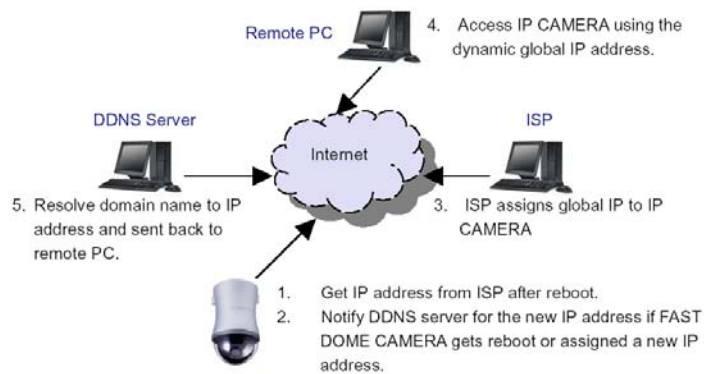
Note: If you forget your password, please contact your vendor or send the device to us.

Appendix

DDNS Network Settings

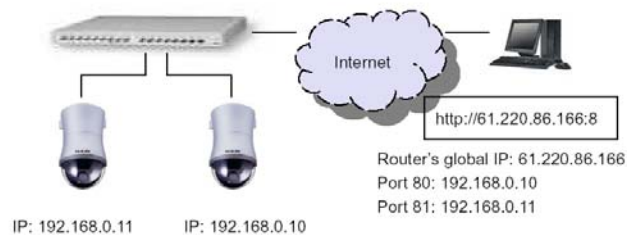
One of the advantages of adopting DDNS and PPPoE services is to save the cost of renting a global IP address. When you power on a camera with a video server and connect to the Internet with the PPPoE service, the camera asks your ISP for a dynamic global IP address. This Internet-accessible IP address will be renewed by the ISP every time you log on the Internet.

Whenever the IP is changed, the camera with the video server will notify the DDNS server of your new IP address. A remote user who intends to connect to the camera with the video server can enter the domain name in the web browser. The domain name will be translated to a new IP address to be used by the camera.



Advanced Port Forwarding Technology

Communication port forwarding technology has been widely used to share a global Internet IP to other devices on the network. The infrastructure of this technology is shown in the below figure, in which the port 80 of the IP router is forwarded to the device with an IP of 192.168.0.10, and the port 81 of the router is forwarded to the device with an IP of 192.168.0.11. When a remote PC on the Internet tries to access the port 81, the user is actually accessing 192.168.0.11, private IP given by the router.



Restore to Factory Default

To restore the IP camera to the factory default, follow the below procedures:

1. Press and hold "Reset Key" for 15 seconds and release.
2. The camera will restart.
3. Launch to Camera Search Tool to search for the IP camera.
4. Access the IP camera via an Internet browser.
5. Due to security reason, create the username and password for the first login. To login to the IP camera, please create the username and password on the login page. Press **Confirm** to complete the setting and login simultaneously.

Regulations

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

RoHS



This product is RoHS compliant.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the Directive 2004/108/EC and 2006/95/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the

Directive 2004/108/EC and 2006/95/EC:

Safety: EN60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

EMC: EN 55022:2010 CLASS B

EN50130-4:2011

EN 61000-3-2:2014

EN 61000-3-3:2013

Directive: EMC Directive 2004/108/EC, RoHS Directive 2011/65/EU

WEEE Directive 2012/19/EU, REACH Regulation No.1907/2006

Česky [Czech]	TRENDnet tímto prohlašuje, že tento CAMERA je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2004/108/ES a 2006/95/ES.
Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr CAMERA overholder de væsentlige krav og øvrige relevante krav i direktiv 2004/108/EF og 2006/95/EF.
Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät CAMERA in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2004/108/EG und 2006/95/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme CAMERA vastavust direktiivi 2004/108/EÜ ja 2006/95/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, TRENDnet, declares that this CAMERA is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC and 2006/95/EC.
Español [Spanish]	Por medio de la presente TRENDnet declara que el CAMERA cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2004/108/CE y 2006/95/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑΤRENDnet ΔΗΛΩΝΕΙ ΟΤΙ CAMERA ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2004/108/EK, 2006/95/EK και.
Français [French]	Par la présente TRENDnet déclare que l'appareil CAMERA est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2004/108/CE, 2006/95/CE et.
Italiano [Italian]	Con la presente TRENDnet dichiara che questo CAMERA è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2004/108/CE e 2006/95/CE.
Latviski [Latvian]	Aršo TRENDnet deklarē, ka CAMERA atbilst Direktīvas 2004/108/EK un 2006/95/EK būtiskajām prasībām un citiemar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis CAMERA atitinka esminius reikalavimus ir kitas 2004/108/EB ir 2006/95/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel CAMERA in overeenstemming is met de

	essentiële eisen en de andere relevante bepalingen van richtlijn 2004/108/EG en 2006/95/EG.
Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan CAMERA jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2004/108/KE u 2006/95/KE.
Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a CAMERA megfelel a vonatkozó alapvető követelményeknek és az 2004/108/EK és a 2006/95/EK irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym TRENDnet oświadcza, że CAMERA jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2004/108/WE i 2006/95/WE.
Português [Portuguese]	TRENDnet declara que este CAMERA está conforme com os requisitos essenciais e outras disposições da Directiva 2004/108/CE e 2006/95/CE.
Slovensko [Slovenian]	TRENDnet izjavlja, da je ta CAMERA v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2004/108/ES in 2006/95/ES.
Slovensky [Slovak]	TRENDnet vyhlasuje, že CAMERA spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2004/108/ES a 2006/95/ES.
Suomi [Finnish]	TRENDnet vakuuttaa täten että CAMERA tyyppinen laite on direktiivin 2004/108/EY ja 2006/95/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar TRENDnet att denna CAMERA står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2004/108/EG och 2006/95/EG.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TV-IP1514PI / TV-IP1515PI – 3 Years Warranty

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/>

[lgpl.txt](#) for specific terms of each license.

TRENDnet[®]

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA

Copyright ©2022. All Rights Reserved. TRENDnet.