

User's Guide

TRENDnet[®]



**Indoor/Outdoor 4MP H.265 PoE IR Bullet
Network Camera**

TV-IP328PI

Contents

Product Overview	4
Features	4
Package Contents	4
Warnings	5
Cautions	5
Plan for installation location	6
Viewing angle	6
Weather Conditions	6
Hardware Installation	7
Cabling	7
Waterproof cap	7
Mount your camera	7
Live View	8
Live View	8
Playback	9
Picture	10
Configuration	10
System – System Settings	10
Basic Information	10
Time Settings	11
DST	12
System – Maintenance	12
Upgrade & Maintenance	12
Log	14
System Service	14
System – Security	15

Authentication	15
IP Filter	15
Security Service	16
System – User Management	16
User Management	16
Online Users	16
Network – Basic Settings	17
TCP/IP	17
DDNS	18
PPPoE	18
Port	19
NAT	19
Network – Advanced Settings	20
SNMP	20
HTTPS	21
QoS	23
802.1x	23
Integration Protocol	24
Video/Audio	24
Video	24
ROI	27
Image	28
Display Settings	28
OSD Settings	31
Private Mask	32
Event - Basic Event	32
Motion Detection	32
Video Tampering	35
Exceptions	35

Email 36

 Storage – Schedule Settings 37

Record Schedule 37

Capture 39

 Storage – Storage Management..... 40

HDD Management 40

 Storage – Advanced Settings 42

FTP 42

Regulations.....44

 Federal Communication Commission Interference Statement 44

 RoHS 44

 Europe – EU Declaration of Conformity 45

Limited Warranty.....46

Product Overview



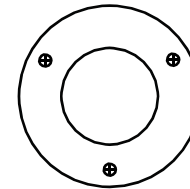
Features

TRENDnet's Indoor/Outdoor 4MP H.265 WDR PoE IR Bullet and Dome Network Cameras provide day and night surveillance with a night vision range of up to 30m (98 ft.) These compact network cameras deliver year-round surveillance, each with an IP67 weather rated housing to withstand harsh outdoor environments. Record up to 4MP HD video at 20fps in a space-saving H.265 compression format. Setup and view live video with included complimentary software and mobile apps.

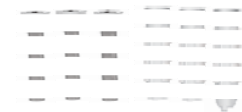
Package Contents

TV-IP328PI package includes:

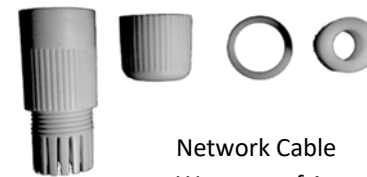
- TV-IP328PI
- Quick Installation Guide
- CD-ROM (Utility and User's Guide)
- Camera mounting hardware
- (Optional power adapter not included)



Drilling Template



Mounting Screws



Network Cable
Waterproof Accessories

If any package content is missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Warnings

Serious injury or death may be caused if any of these warnings are neglected. Follow these safety guards to prevent serious injury or death.

- If using the power adapter, please choose the power adapter that meets the safety extra low voltage (SELV) standard or IEC60950-1 and Limited Power Source standard.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. Disassembling the product will void the warranty and may cause harm or injury.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or water.
- The installation should be done by a qualified service person and should conform to all construction and electric regulations and other local codes.

Cautions

Injury or equipment damage may be caused if any of these cautions are neglected. Follow these precautions to prevent potential injury or material damage.

- Make sure the power supply voltage is correct before using the Camera.
- Do not drop the camera or subject to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as the Sun or an incandescent lamp. Strong light can damage the camera sensor.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor will not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -10°C to 60°C), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Keep out of water and any liquid.
- While shipping, the camera should be packed in its original packing.

Plan for installation location

Viewing angle

The TV-IP328PI is a bullet camera with a focused viewing angle (83° horizontal) that provides non-distorted and detailed images. Choose the location where has good angle to shoot the image you expect to see. The motion detection area should also be considered when installing the camera.

Weather Conditions

The TV-IP328PI is a small bullet camera, which fits most installations indoor and outdoor. The camera can work under a wide range of weather conditions. For severe weather conditions, a camera housing with temperature and moisture control is recommended. Using the camera in milder weather conditions will help extend the camera's product life and preserve the quality of the video image.

- **Moisture:** Avoid damp or moist environments whenever you can. The TV-IP328PI is an IP67 grade water proof camera, and it will work in moist environments. However, rain may affect the picture quality, especially at night, water may reflect the light from the infra-red illumination and degrade picture quality.
- **Temperature:** TV-IP328PI works within a specified temperature range. Areas with severe temperatures should be avoided when installing the camera. It's recommended that you use an enclosure with a heater and blower if you plan on using this camera outside of the specified temperature range.

- **Sunlight:** Avoid direct sun light exposure. Direct sun light will damage the image sensor. If sunlight is necessary for your viewing purposes, provide protection for the image sensor.
- **Lighting:** Consider installing your camera faces the same direction of the light sources. Shooting images with top-down position outdoor or next to the existing light source are good choices. Avoid the light source if it creates a shade that darkens the viewing area

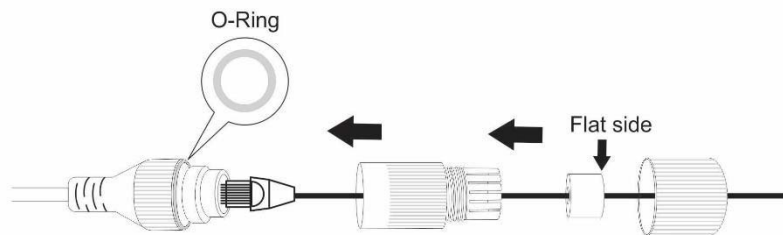
Hardware Installation

Cabling

It's recommended that the wiring the cable in your home or office by a professional. If you already have the cable deployed, make sure the cable and the connectors meet the category 5 Ethernet cable standards. At least 2 pairs of twisted lines are required for power and data. Poor cable quality may cause unexpected problems. Testing your cable or running a new cable is suggested for new camera installation.

Waterproof cap

The TV-IP328PI itself is IP66 grade water and dust proof. There is a set of network cable water proof caps that comes with the package as well. Run your cable going through the accessories, and then crimp the cable with an RJ45 module. Plug in the network cable and then tighten the waterproof cap to prevent water running into camera through the cable.



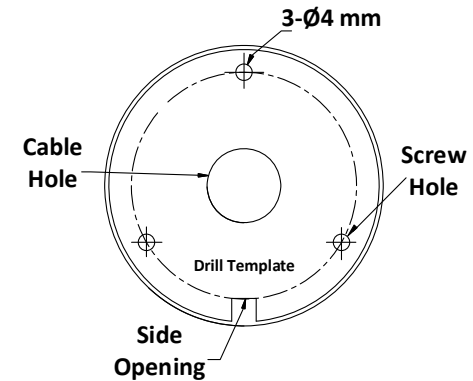
Mount your camera

Steps:

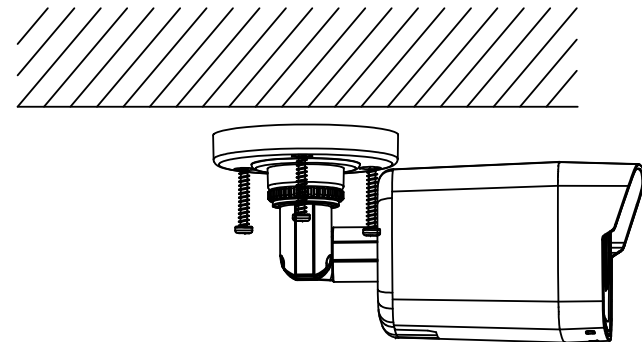
1. Paste the drill template to the desired mounting position on the ceiling.
2. Drill the screw holes in the ceiling according to the supplied drill template.

Note:

Drill the cable hole, if adopting ceiling outlet to route the cable.



3. Route the cables through the cable hole (optional), or the side opening.
4. Fix the camera on the ceiling with supplied screws.

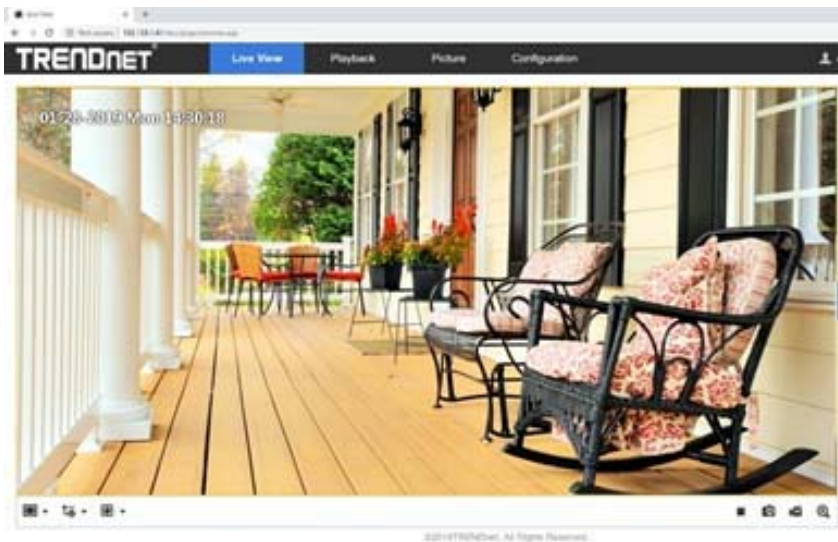


Live View

Use Mira app or VMS to activate and setup the camera, if you would like to access camera's configuration page, please find the camera IP from Camera Utility or Mira VMS to access it.

Live View

The live view page allows you to view the real-time video, capture images, and configure video parameters. Log in the network camera to enter the live view page, or you can click **Live View** on the menu bar of the main page to enter the live view page.



Menu Bar:

Click each tab to enter Live View, Playback, Picture, and Configuration page respectively.

Live View Window:

Display the live video.

Toolbar:

Toolbar allows you to adjust the live view window size, the stream type, and the plug-ins. It also allows you to process the operations on the live view page, e.g., start/stop live view, capture, record, audio on/off, two-way audio, start/stop digital zoom, etc.

For IE (Internet Explorer) users, plug-ins as webcomponents and quick time are selectable. And for Non-IE users, webcomponents, quick time, VLC or MJPEG is selectable if they are supported by the web browser.

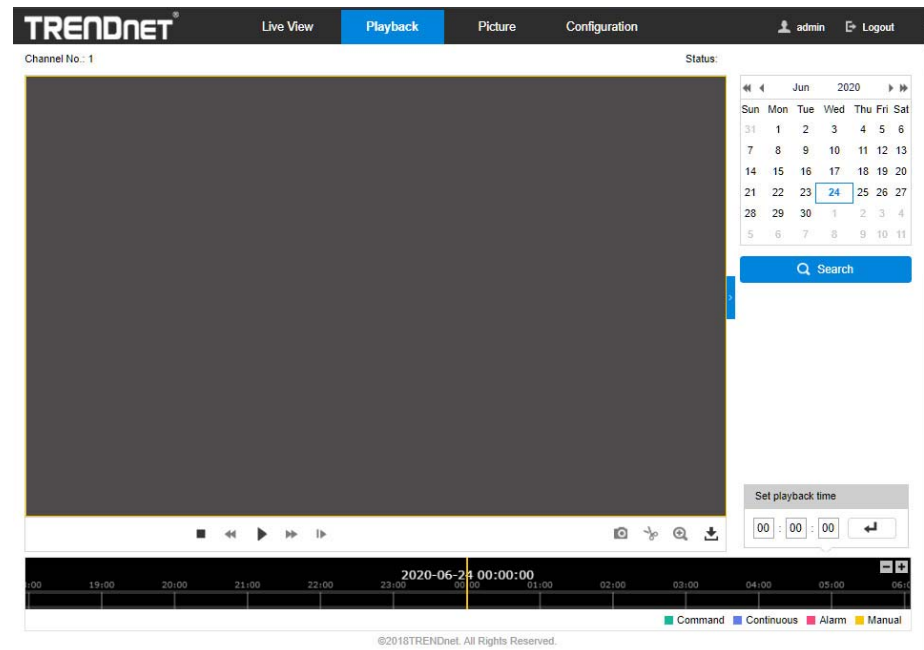
Note:

For camera that supports plug-in free live view, when Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version are used, plug-in installation is not required. But **Picture** and **Playback** functions are hidden. To use mentioned function via web browser, change to their lower versions, or change to Internet Explorer 8.0 and its above version.

Icon	Description
	Start/Stop live view.
	4:3 window size.
	16:9 window size.
	Original window size.
	Self-adaptive window size.
	Original ratio window size.
	Live view with the different video streams.
	Click to select the third-party plug-in.
	Manually capture the picture.
	Manually start/stop recording.
	Start/stop digital zoom function.

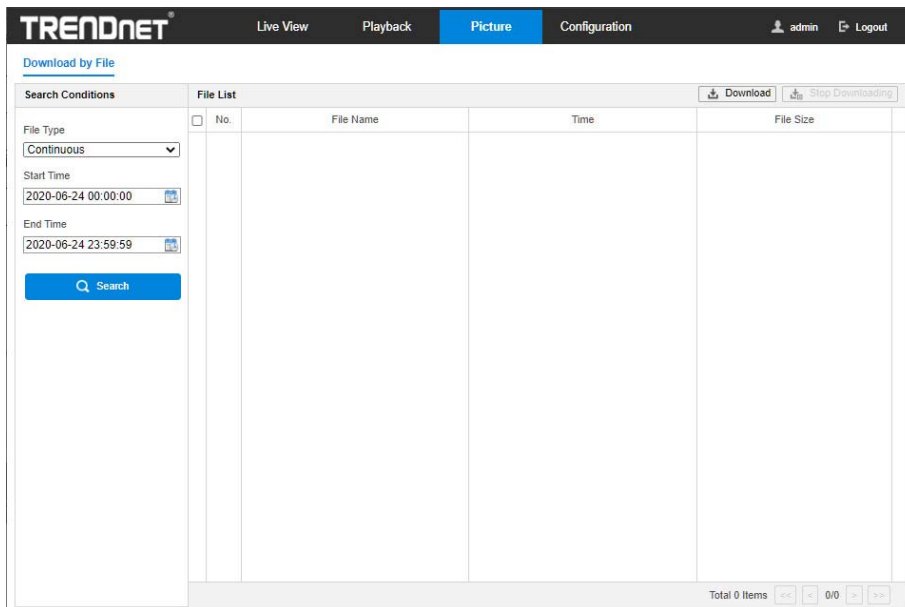
Playback

You can playback the video recording on the network storage and download the video clip and snapshots to your local computer.



Picture

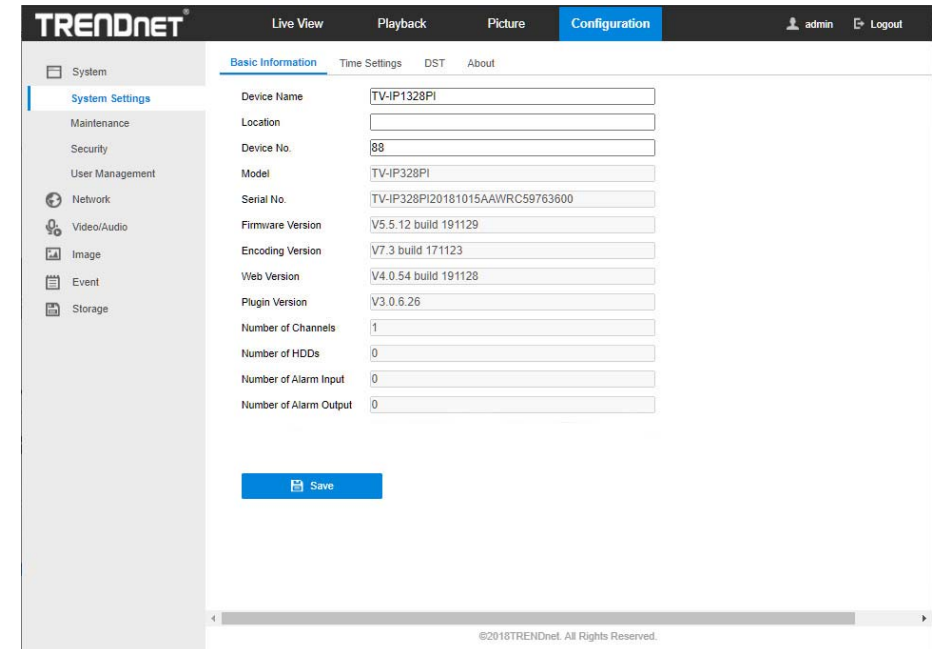
You can playback the snapshots on the network storage and download the images to your local computer.



Configuration

System – System Settings

Basic Information



In the **System Settings**, you can edit the Device Name and Device No. Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.

Time Settings

1. Select the Time Zone of your location from the drop-down menu.
2. Configure the NTP settings.
 - (1) Click to enable the **NTP** function.
 - (2) Configure the following settings:


Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP server.

- (3) (Optional) You can click the **Test** button to test the time synchronization function via NTP server.

Note: If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

- Configure the manual time synchronization.
 - (1) Check the **Manual Time Sync.** to enable the manual time synchronization function.
 - (2) Click the icon  to select the date, time from the pop-up calendar.
 - (3) (Optional) You can check **Sync. with computer time** item to synchronize the time of the device with that of the local PC.
- Click **Save** to save the settings.

DST

The screenshot shows the 'DST' configuration page. On the left is a sidebar menu with 'System Settings' selected. The main area has tabs for 'Basic Information', 'Time Settings', 'DST' (active), and 'About'. Under the 'DST' tab, there is a checkbox for 'Enable DST' which is checked. Below it are fields for 'Start Time' (Mar, Second, Sun, 02), 'End Time' (Nov, First, Sun, 02), and 'DST Bias' (60minute(s)). A blue 'Save' button is at the bottom.

Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Configure the DST according to your actual demand.

Steps:

1. Enter the DST configuration interface.

Configuration > System > System Settings > DST

2. Select the start time and the end time.
3. Select the DST Bias.
4. Click **Save** to activate the settings.

System – Maintenance

Upgrade & Maintenance

The screenshot shows the 'Upgrade & Maintenance' page. The top navigation bar includes 'Live View', 'Playback', 'Picture', and 'Configuration' (active). The left sidebar has 'Maintenance' selected. The main area contains several sections: 'Reboot' with a 'Reboot' button; 'Default' with 'Restore' and 'Default' buttons; 'Information Export' with 'Device Parameters' and 'Diagnose Informa...' buttons; 'Import Config. File' with a 'Device Parameters' input field and 'Browse'/'Import' buttons; and 'Status' with an 'Upgrade' section containing a 'Firmware' dropdown and a 'Browse'/'Upgrade' button.

The upgrade & maintenance interface allows you to process the operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

- **Reboot:** Restart the device.
- **Restore:** Reset all the parameters, except the IP parameters and user information, to the default settings.
- **Default:** Restore all the parameters to the factory default.
- **Information Export**
Device Parameters: click to export the current configuration file of the camera.

This operation requires admin password to proceed.

For the exported file, you also have to create an encryption password. The encryption password is required when you import the file to other cameras.

Diagnose Information: click to download log and system information.

- **Import Config. File**

Configuration file is used for the batch configuration of the cameras.

Steps:

1. Click **Browse** to select the saved configuration file.
2. Click **Import** and input the encryption password that you set during exporting.

Note: You need to reboot the camera after importing configuration file.

- **Upgrade:** Upgrade the device to a certain version.

Steps:

1. Select firmware or firmware directory to locate the upgrade file.

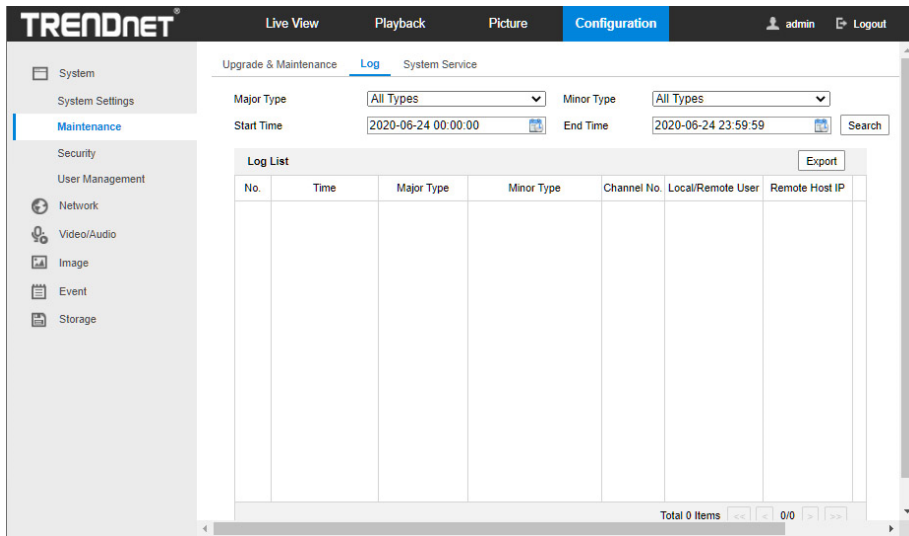
Firmware: Locate the exact path of the upgrade file.

Firmware Directory: Only the directory the upgrade file belongs to is required.

2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

Note: The upgrading process will take 1 to 10 minutes. Please don't disconnect power of the camera during the process, and the camera reboots automatically after upgrade.

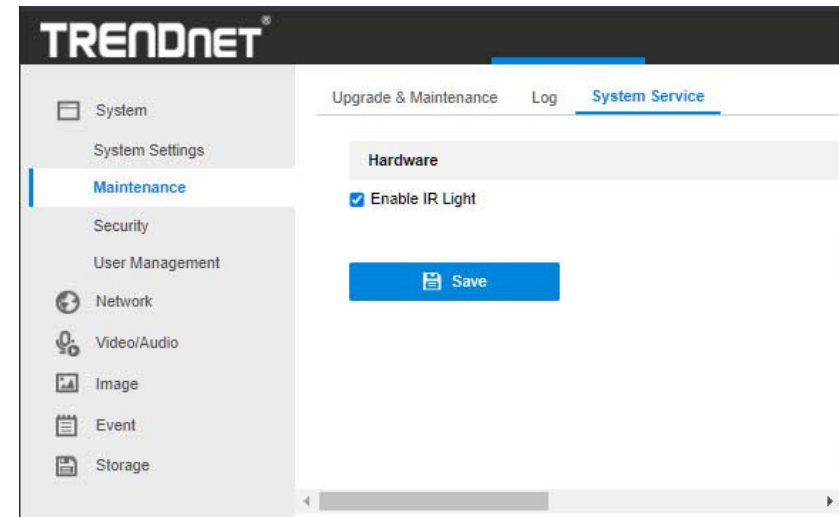
Log



The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

1. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
2. Click **Search** to search log files. The matched log files will be displayed on the log list interface.
3. To export the log files, click **Export** to save the log files.

System Service



System service settings refer to the software and hardware service the camera supports. Supported functions vary according to the different cameras. For the cameras support IR LED, ABF (Auto Back Focus), Auto Defog, or Status LED, you can select to enable or disable the corresponding service according to the actual demands.

System – Security

Authentication

The screenshot shows the TRENDnet web interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', and 'Configuration'. The left sidebar has 'System', 'System Settings', 'Maintenance', 'Security' (selected), 'User Management', and 'Network'. The main content area is titled 'Authentication' and contains two dropdown menus: 'RTSP Authentication' and 'WEB Authentication', both set to 'digest'. A blue 'Save' button is located at the bottom.

You can specifically secure the stream data of live view.

1. Set up authentication method for RTSP authentication and WEB authentication.

Caution:

Digest is the recommended authentication method for better data security. You must be aware of the risk if you adopt basic as the authentication method.

2. Click **Save** to save the settings.

IP Filter

The screenshot shows the TRENDnet web interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', and 'Configuration'. The left sidebar has 'System', 'System Settings', 'Maintenance', 'Security' (selected), 'User Management', and 'Network'. The main content area is titled 'IP Address Filter' and contains a checkbox 'Enable IP Address Filter', a dropdown 'IP Address Filter Type' set to 'Forbidden', and a table for the IP Address Filter list. A blue 'Save' button is located at the bottom.

1. Check the checkbox of **Enable IP Address Filter**.
2. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
3. Set the IP Address Filter list.

- Add an IP Address

Steps:

- (1) Click the **Add** to add an IP.
- (2) Input the IP Address.
- (3) Click the **OK** to finish adding.

- Modify an IP Address

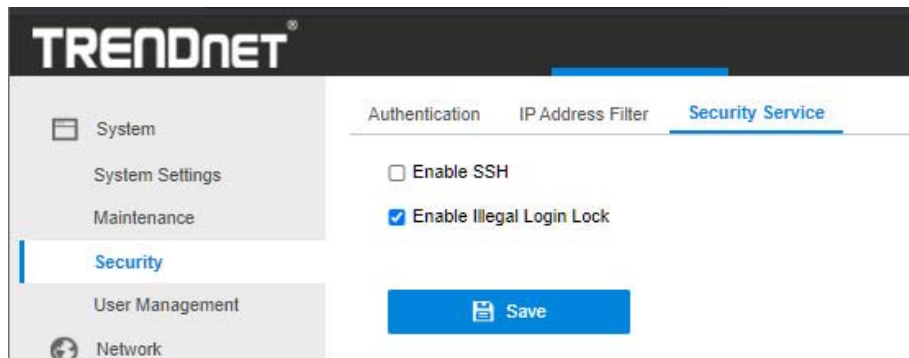
Steps:

- (1) Left-click an IP address from filter list and click **Modify**.
- (2) Modify the IP address in the text filed.
- (3) Click the **OK** to finish modifying.

- Delete an IP Address or IP Addresses.
Select the IP address (es) and click **Delete**.

4. Click **Save** to save the settings.

Security Service

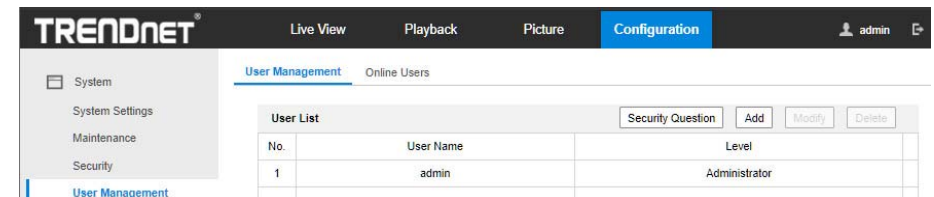


Illegal Login Lock: it is used to limit the user login attempts. Login attempt from the IP address is rejected if admin user performs 7 failed user name/password attempts (5 times for the operator/user).

Note: If the IP address is rejected, you can try to login the device after 30 minutes.

System – User Management

User Management



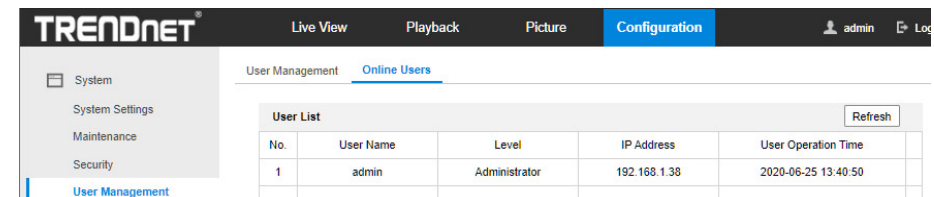
The *admin* user has all permissions by default and can create/modify/delete other accounts.

The *admin* user cannot be deleted and you can only change the *admin* password.

Notes:

- Up to 31 user accounts can be created.
- Users of different levels own different default permissions.
Operator and user are selectable.

Online Users



You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address, and operation time, is displayed in the User List.

Network – Basic Settings

TCP/IP

The screenshot displays the 'Configuration' tab of the TRENDnet web interface, specifically the 'TCP/IP' settings. The left sidebar shows a navigation menu with 'Network' selected, leading to 'Basic Settings'. The main panel contains the following configuration options:

- TCP/IP** (selected tab), with sub-tabs for DDNS, PPPoE, Port, and NAT.
- NIC Type**: Auto (dropdown menu).
- DHCP**: Checked checkbox.
- IPv4 Address**: 192.168.1.53 (text field) with a **Test** button.
- IPv4 Subnet Mask**: 255.255.255.0 (text field).
- IPv4 Default Gateway**: 192.168.1.254 (text field).
- IPv6 Mode**: Route Advertisement (dropdown menu) with a **View Route Advertisement** button.
- IPv6 Address**: (empty text field).
- IPv6 Subnet Mask**: (empty text field).
- IPv6 Default Gateway**: (empty text field).
- Mac Address**: 44:47:cc:6d:12:a7 (text field).
- MTU**: 1500 (text field) with a **byte** unit indicator.
- Multicast Address**: (empty text field).
- Enable Multicast Discovery**: Checked checkbox.
- DNS Server** section:
 - Preferred DNS Server**: 192.168.1.249 (text field).
 - Alternate DNS Server**: (empty text field).
- Save** button at the bottom.

1. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
2. (Optional) Check the checkbox of **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
3. Configure the DNS server. Input the preferred DNS server, and alternate DNS server.
4. Click **Save** to save the above settings.

Notes:

- The valid value range of MTU is 1280 to 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.
- A reboot is required for the settings to take effect.

DDNS

The screenshot shows the DDNS configuration page in the TRENDnet web interface. The 'DDNS' tab is selected. The 'Enable DDNS' checkbox is unchecked. The 'DDNS Type' dropdown is set to 'NO-IP'. The 'Server Address' field contains 'dynupdate.no-ip.com'. The 'Domain', 'User Name', 'Port', 'Password', and 'Confirm' fields are empty. A 'Save' button is at the bottom.

1. Check the **Enable DDNS** checkbox to enable this feature.
2. Select **DDNS Type**. NO-IP.

Steps:

- (1) Enter the Server Address as www.noip.com
- (2) Enter the Domain name you registered.
- (3) Enter the User Name and Password.
- (4) Click **Save** and then you can view the camera with the domain name.

PPPoE

The screenshot shows the PPPoE configuration page in the TRENDnet web interface. The 'PPPoE' tab is selected. The 'Enable PPPoE' checkbox is unchecked. The 'Dynamic IP' field contains '0.0.0.0'. The 'User Name', 'Password', and 'Confirm' fields are empty. A 'Save' button is at the bottom.

1. Check the **Enable PPPoE** checkbox to enable this feature.
2. Enter **User Name**, **Password**, and **Confirm** password for PPPoE access.

Note: The User Name and Password should be assigned by your ISP.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
 - *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*
3. Click **Save** to save and exit the interface.

Port

The screenshot shows the 'Port' configuration page in the TRENDnet web interface. The left sidebar contains a menu with 'System', 'Network', 'Basic Settings' (selected), 'Advanced Settings', 'Video/Audio', 'Image', 'Event', and 'Storage'. The main content area has tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port' (selected), and 'NAT'. Under the 'Port' tab, there are four input fields: 'HTTP Port' with value 80, 'RTSP Port' with value 554, 'HTTPS Port' with value 443, and 'Server Port' with value 8000. A blue 'Save' button is located at the bottom of the form.

HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP Port: The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.

Server Port: The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

NAT

The screenshot shows the 'NAT' configuration page in the TRENDnet web interface. The left sidebar is the same as the Port page. The main content area has tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT' (selected). Under the 'NAT' tab, there is a checkbox for 'Enable UPnP™' which is checked. Below it is a 'Friendly Name' field with the value 'TV-IP328PI - C59763600'. A 'Port Mapping Mode' dropdown menu is set to 'Auto'. Below this is a table with the following data:

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid

A blue 'Save' button is located at the bottom of the form.

NAT interface allows you to configure the UPnP™ parameters.

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

1. Check the checkbox to enable the UPnP™ function.

Note:

Only when the UPnP™ function is enabled, ports of the camera are active.

2. Choose a friendly name for the camera, or you can use the default name.
3. Select the port mapping mode. Manual and Auto are selectable.

Note:

If you select Auto, you should enable UPnP™ function on the router.

If you select Manual, you can customize the value of the external port and complete port mapping settings on router manually.

4. Click **Save** to save the settings.

Network – Advanced Settings

SNMP

TRENDnet Live View Playback Picture Configuration

System Network Basic Settings **Advanced Settings** Video/Audio Image Event Storage

SNMP HTTPS QoS 802.1x Integration Protocol

SNMP v1/v2

☐ Enable SNMPv1

☐ Enable SNMP v2c

Read SNMP Community public

Write SNMP Community private

Trap Address

Trap Port 162

Trap Community public

SNMP v3

☐ Enable SNMPv3

Read UserName

Security Level no auth, no priv

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key password

Write UserName

Security Level no auth, no priv

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key password

SNMP Other Settings

SNMP Port 161

Save

You can set the SNMP function to get camera status, parameters and alarm related information, and manage the camera remotely when it is connected to the network.

Before you start:

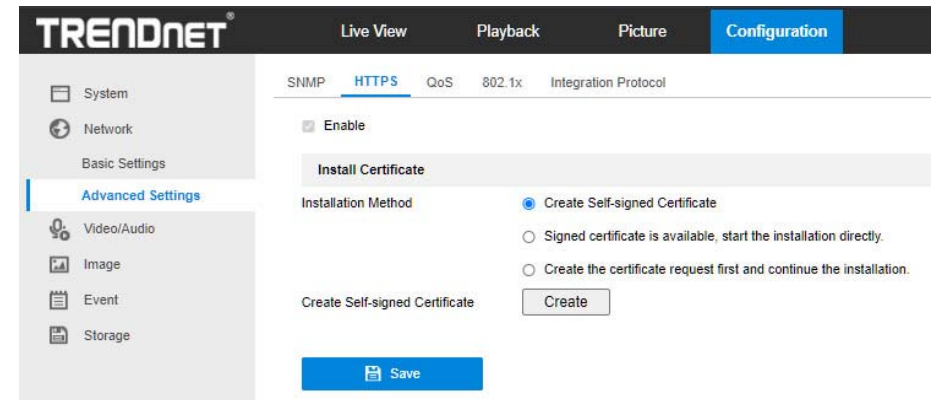
Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Note: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

Notes:

- A reboot is required for the settings to take effect.
- To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.

HTTPS



HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

Note:

- For the camera that supports plug-in free live view, when you use HTTPS to visit the camera, you should enable **Websockets** for live view. Go to **Configuration > Network > Advanced Settings > Network Service**.
- If HTTPS is enabled by default, the camera creates an unsigned certificate automatically. When you visit the camera via HTTPS, the web browser will send a notification about the certificate issue. Install a signed-certificate to the camera to cancel the notification.
 1. Check **Enable** to access the camera via HTTP or HTTPS protocol.
 2. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.

3. Create the self-signed certificate or authorized certificate.

- Create the self-signed certificate

- (1) Select **Create Self-signed Certificate** as the Installation Method.
- (2) Click **Create** button to enter the creation interface.
- (3) Enter the country, host name/IP, validity and other information.
- (4) Click **OK** to save the settings.

Note: If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

- Create the request and import the authorized certificate

- (1) Select **Create the certificate request first and continue the installation** as the Installation Method.
- (2) Click **Create** button to create the certificate request. Fill in the required information in the popup window.
- (3) Click **Download** to download the certificate request and submit it to the trusted certificate authority for signature.
- (4) After receiving the signed valid certificate, you can import the certificate in two ways:
 - a) Select **Signed certificate is available, Start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
 - b) Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate

to the device.

4. There will be the certificate information after your successfully creating and installing the certificate.

5. Export and save the certificate for verification when adding the device to client software.

Note:

The exported certificate should be saved in the certificate folder of your client software before adding the device to your PC client.

6. Click the **Save** button to save the settings.

QoS

The screenshot shows the TRENDnet web interface with the 'QoS' tab selected. The left sidebar has 'Advanced Settings' highlighted. The main content area shows three DSCP settings: Video/Audio DSCP, Event/Alarm DSCP, and Management DSCP, each with a text input field containing the value '0'. A blue 'Save' button is at the bottom right.

1. Configure the QoS settings, including Video/Audio DSCP, Event/Alarm DSCP and Management DSCP.

The valid value range of the DSCP is 0 to 63. The bigger the DSCP value is, the higher the priority is.

Note: DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

2. Click **Save** to save the settings.

802.1x

The screenshot shows the TRENDnet web interface with the '802.1x' tab selected. The left sidebar has 'Advanced Settings' highlighted. The main content area shows the 'Enable IEEE 802.1X' checkbox, which is unchecked. Below it are fields for 'Protocol' (set to EAP-MD5), 'EAPOL version' (set to 1), 'User Name', 'Password', and 'Confirm'. A blue 'Save' button is at the bottom right.

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

Before you start:

The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

1. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
2. Configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

Note: The **EAPOL version** must be identical with that of the router or the switch.

3. Enter the user name and password to access the server.
4. Click **Save** to finish the settings.

Integration Protocol

The screenshot shows the 'Integration Protocol' configuration page. It includes a sidebar with 'System', 'Network', and 'Video/Audio' sections. The 'Integration Protocol' tab is active, showing a checkbox for 'Enable ONVIF' and a 'User List' table. The table has columns for 'No.', 'User Name', and 'Level'. A 'Save' button is located at the bottom of the page.

If you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

1. Check the Enable ONVIF checkbox to enable the function.
2. Add ONVIF users. Up to 32 users are allowed.
Set the user name and password, and confirm the password. You can set the user as media user, operator, and administrator.

Note: ONVIF user account is different from the camera user account. You have set ONVIF user account independently.

3. Save the settings.

Note: User settings of ONVIF are cleared when you restore the camera.

Video/Audio

Video

The screenshot shows the 'Video/Audio' configuration page. It includes a sidebar with 'System', 'Network', and 'Video/Audio' sections. The 'Video' tab is active, showing various settings for video streaming. The settings include Stream Type (Main Stream(Normal)), Video Type (Video Stream), Resolution (1920*1080P), Bitrate Type (Variable), Video Quality (Medium), Frame Rate (20 fps), Max. Bitrate (6144 Kbps), Video Encoding (H.264), H.264+ (OFF), Profile (Main Profile), I Frame Interval (50), and Smoothing (50). A 'Save' button is located at the bottom of the page.

Video Type:

Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

Resolution:

Select the resolution of the video output.

Bitrate Type:

Select the bitrate type to constant or variable.

Video Quality:

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Frame Rate:

Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate:

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Note: The maximum limit of the max. bitrate value varies according to different camera platforms. For certain cameras, the maximum limit is 8192 Kbps or 12288 Kbps.

Video Encoding:

The camera supports multiple video encodings types, such as H.264, H.265, MJPEG, and MPEG4. Supported encoding type for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate and image quality.

Note: Selectable video encoding types may vary according to different camera modes.

H.264+ and H.265+:

- **H.264+:** If you set the main stream as the stream type, and H.264 as the video encoding, you can see H.264+ available. H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.
- **H.265+:** If you set the main stream as the stream type, and H.265 as the video encoding, you can see H.265+ available. H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

You need to reboot the camera if you want to turn on or turn off the H.264+/H.265+. If you switch from H.264+ to H.265+ directly, and vice versa, a reboot is not required by the system.

Notes:

- Upgrade your video player to the latest version if live view or playback does not work properly due to compatibility.
- With H.264+/H.265+ enabled, the parameters such as profile, I frame interval, video quality, and SVC are greyed out.
- With H.264+/H.265+ enabled, some functions are not supported. For those functions, corresponding interfaces will be hidden.
- H.264+/H.265+ can spontaneously adjust the bitrate distribution according the requirements of the actual scene in order to realize the set maximum average bitrate in the long term. The camera needs at least 24 hours to adapt to a fixed monitoring scene.

Max. Average Bitrate:

When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.

Profile:

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to camera models.

I Frame Interval:

Set I Frame Interval from 1 to 400.

SVC:

Scalable Video Coding is an extension of the H.264/AVC and H.265 standard. Select OFF/ON to disable/enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Smoothing:

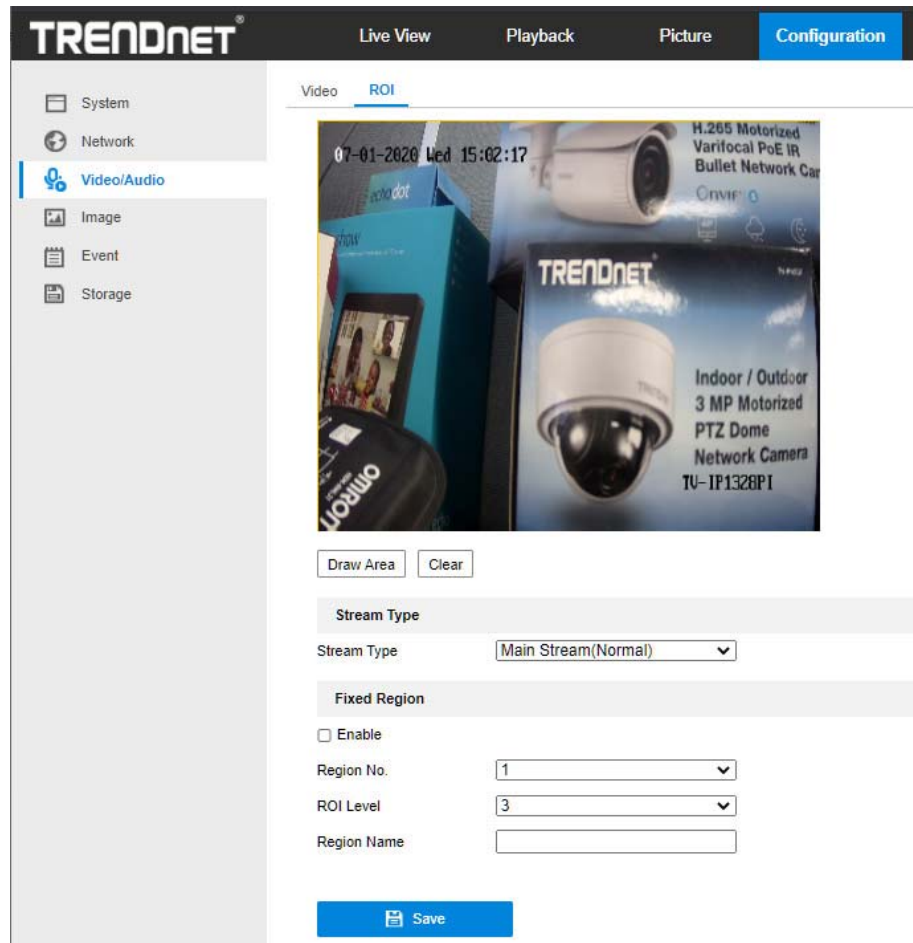
It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

1. Click **Save** to save the settings.

Note:

The video parameters vary according to different camera models. Refer to the actual display page for camera functions.

ROI



ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression, which means, the technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Note: ROI function varies according to different camera models.

Steps:

1. Enter the ROI settings interface: **Configuration > Video/Audio > ROI**.
2. Select the Stream Type for ROI encoding.
3. Check the checkbox of **Enable** under Fixed Region item.
4. Set **Fixed Region** for ROI.
 - (1) Select the Region No. from the drop-down list.
 - (2) Check the **Enable** checkbox to enable ROI function for the chosen region.
 - (3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.
 - (4) Select the ROI level.
 - (5) Enter a region name for the chosen region.
 - (6) Click **Save** the save the settings of ROI settings for chosen fixed region.
 - (7) Repeat steps (1) to (6) to setup other fixed regions.
5. Set **Dynamic Region** for ROI.
 - (1) Check the checkbox to enable **Face Tracking**.

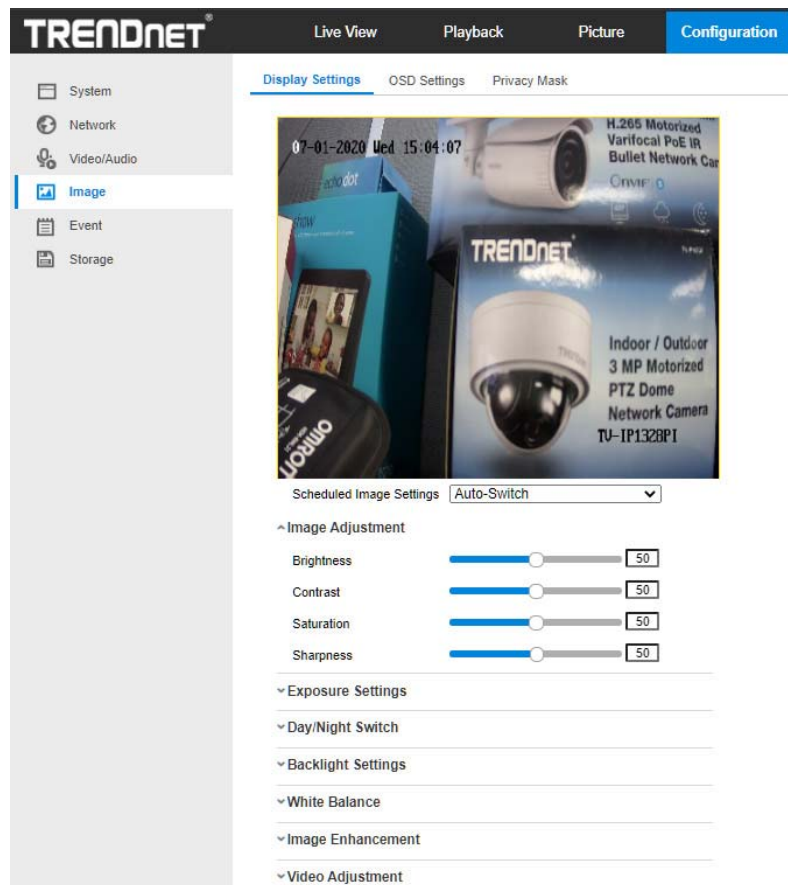
Note: To enable face tracking function, the face detection function should be supported and enabled.
 - (2) Select the ROI level.

6. Click **Save** to save the settings.

Note: ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

Image

Display Settings



● Image Adjustment

Brightness describes bright of the image, which ranges from 1 to 100.

Contrast describes the contrast of the image, which ranges from 1 to 100.

Saturation describes the colorfulness of the image color, which ranges from 1 to 100.

Sharpness describes the edge contrast of the image, which ranges from 1 to 100.

● Exposure Settings

If the camera is equipped with the fixed lens, only **Manual** is selectable, and the iris mode is not configurable.

If **Auto** is selected, you can set the auto iris level from 0 to 100.

The **Exposure Time** refers to the electronic shutter time, which ranges from 1 to 1/100,000s. Adjust it according to the actual luminance condition.

Gain of image can also be manually configured from 0 to 100. The bigger the value is, the brighter would the image be, and the noise would also be amplified to a larger extent.

- **Day/Night Switch**

Select the Day/Night Switch mode according to different surveillance demand.

Day, Night, Auto, Scheduled-Switch, and Triggered by alarm input are selectable for day/night switch.

Day: the camera stays at day mode.

Night: the camera stays at night mode.

Auto: the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0 to 7, the higher the value is, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.

Scheduled-Switch: Set the start time and the end time to define the duration for day/night mode.

Triggered by alarm input: The switch is triggered by alarm input. You can set the triggered mode to day or night.

Smart Supplement Light: Set the supplement light as ON, and Auto and Manual are selectable for light mode.

Select Auto, and the supplement light changes according to the actual luminance. E.g., if the current scene is bright enough, then the supplement light adjusts itself to lower power; and if the scene is not bright enough, the light adjusts itself to higher power.

Select Manual, and you can adjust the supplement by adjusting the distance. E.g., if the object is near the camera, the device adjusts the supplement light to lower power, and the light is in higher power if the object is far away.

- **Backlight Settings**

BLC Area: If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right, Center, Auto, and Custom are selectable.

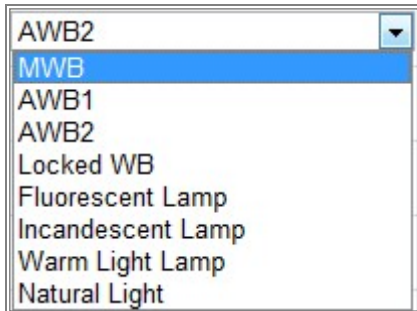
Note: If BLC mode is set as Custom, you can draw a red rectangle on the live view image as the BLC area.

WDR: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

HLC: High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

- **White Balance**

White balance is the white rendition function of the camera used to adjust the color temperature according to the environment.



- **Image Enhancement**

Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal and Expert are selectable. Set the DNR level from 0 to 100 in Normal Mode. Set the DNR level from both space DNR level [0-100] and time DNR level [0-100] in Expert Mode.

Defog Mode: You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.

EIS (Electrical Image Stabilizer): EIS reduces the effects of vibration in a video.

Grey Scale: You can choose the range of the grey scale as [0-255] or [16-235].

- **Video Adjustment**

Mirror: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.

Rotate: To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.

When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.

Scene Mode: Choose the scene as indoor or outdoor according to the real environment.

Video Standard: 50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

Lens Distortion Correction: For cameras equipped with motor-driven lens, image may appear distorted to some extent. Turn on this function to correct the distortion.

OSD Settings

TRENDnet Live View Playback Picture **Configuration**

Display Settings **OSD Settings** Privacy Mask

System
Network
Video/Audio
Image
Event
Storage

07-01-2020 Wed 15:07:35

Display Mode: Not transparent & Not flashing

OSD Size: Auto

Font Color: Black&White Self-adaptive

Alignment: Custom

☐ Display Name

☐ Display Date

☐ Display Week

Camera Name: TV-IP1328PI

Time Format: 24-hour

Date Format: MM-DD-YYYY

Text OverLay

☐ 1

☐ 2

☐ 3

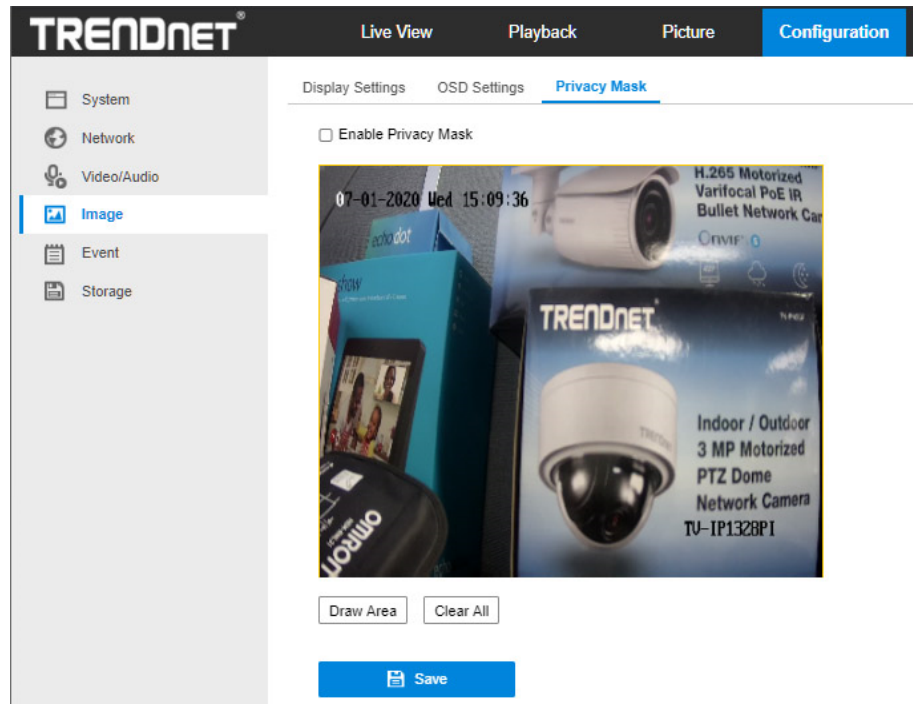
☐ 4

Save

1. Check the corresponding checkbox to select the display of camera name, date or week if required.
2. Edit the camera name in the text field of **Camera Name**.
3. Select from the drop-down list to set the time format and date format.
4. Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.
5. Configure the text overlay settings.
 - (1) Check the checkbox in front of the textbox to enable the on-screen display.
 - (2) Input the characters in the textbox.

Note: Up to 8 text overlays are configurable.
6. Adjust the OSD position and alignment.
7. Character align right, character align left, all align right, all align left and custom are selectable. If you select character align right, character align left, all align left or all align right, you can set the left and right margins and up and down margins. 1 Character, 2 character and none are available. If you select custom, you can use the mouse to click and drag text frames in the live view window to adjust their positions.
8. Click **Save** to save the settings.

Private Mask



1. Check the checkbox of **Enable Privacy Mask** to enable this function.
2. Click **Draw Area**.
3. Click and drag the mouse in the live video window to draw the mask area.
Note: You are allowed to draw up to 4/8 areas on the same image. The supported number of the areas vary with the camera model.
4. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
5. Click **Save** to save the settings.

Event - Basic Event

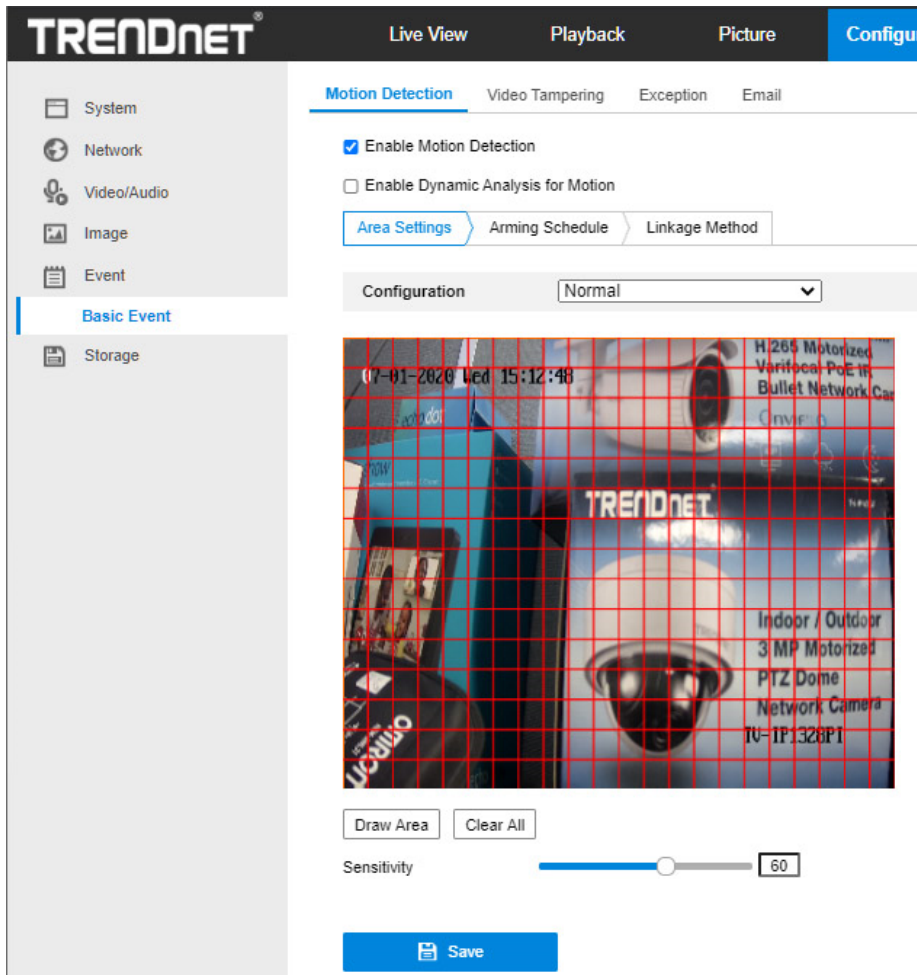
You can configure the basic events by following the instructions in this section, including motion detection, video tampering, alarm input, alarm output, and exception, etc. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, etc.

Note: Check the checkbox of Notify Surveillance Center if you want the alarm information to be pushed to PC or mobile client software as soon as the alarm is triggered.

Motion Detection

Motion detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

In order to detect the moving objects accurately and reduce the false alarm rate, normal configuration and expert configuration are selectable for different motion detection environment.



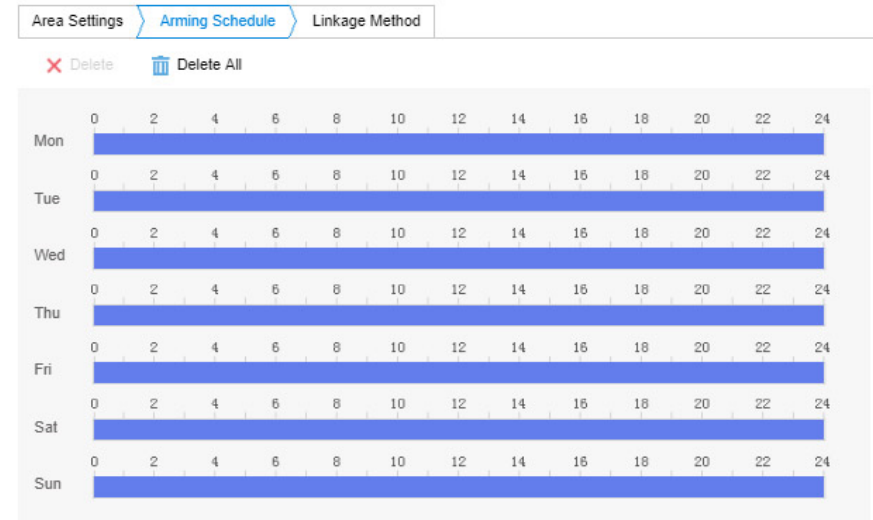
1. Check the checkbox of **Enable Motion Detection**.
2. Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles.

Note: Select Disable for rules if you don't want the detected object displayed with the green rectangles. Select disable rules from **Configuration > Local Configuration > Live View Parameters-rules**.

3. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.
4. (Optional) Click **Clear All** to clear all of the areas.
5. (Optional) Move the slider to set the sensitivity of the detection.

Steps:

1. Click **Arming Schedule** to edit the arming schedule.
2. Click on the time bar and drag the mouse to select the time period.



Note: Click on the selected time period, you can adjust the time period to the desired time by either moving the time bar or input the

exact time period.

3. (Optional) Click Delete to delete the current arming schedule, or click Save to save the settings.
4. Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.
5. Click **Save** to save the settings.

Note: The time of each period can't be overlapped. Up to 8 periods can be configured for each day.

Task 3: Set the Linkage Method for Motion Detection

Check the checkbox to select the linkage method. Audible Warning, Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output are selectable. You can specify the linkage method when an event occurs.

Area Settings > Arming Schedule > Linkage Method	
<input type="checkbox"/> Normal Linkage	<input checked="" type="checkbox"/> Trigger Recording
<input type="checkbox"/> Send Email	<input checked="" type="checkbox"/> A1
<input checked="" type="checkbox"/> Notify Surveillance Center	
<input type="checkbox"/> Upload to FTP/Memory Card/...	

Note: The linkage methods vary according to the different camera models.

- **Send Email**

Send an email with alarm information to a user or users when an event occurs.

- **Notify Surveillance Center**

Send an exception or alarm signal to remote management software when an event occurs.

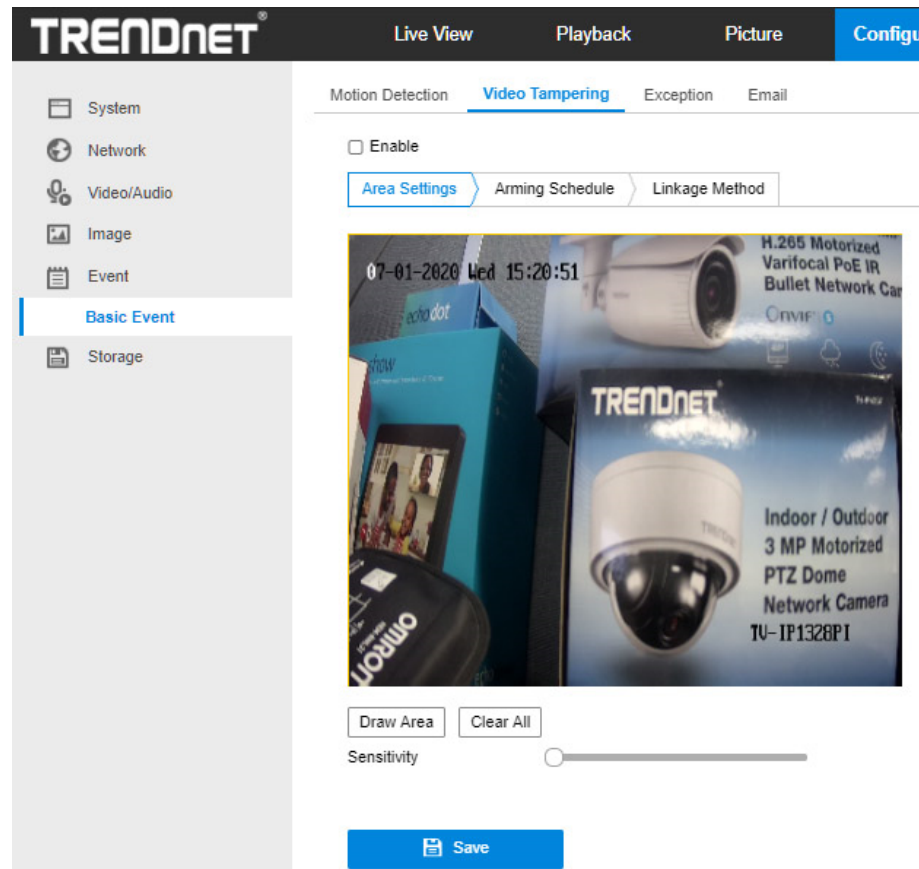
- **Upload to FTP/ NAS**

Capture the image when an alarm is triggered and upload the picture to a FTP server.

Notes:

- Set the FTP address and the remote FTP server first
- Go to **Configuration > Storage > Schedule Settings> Capture > Capture Parameters** page, enable the event-triggered snapshot, and set the capture interval and capture number.
- The captured image can also be uploaded to the available SD card or network disk.

Video Tampering

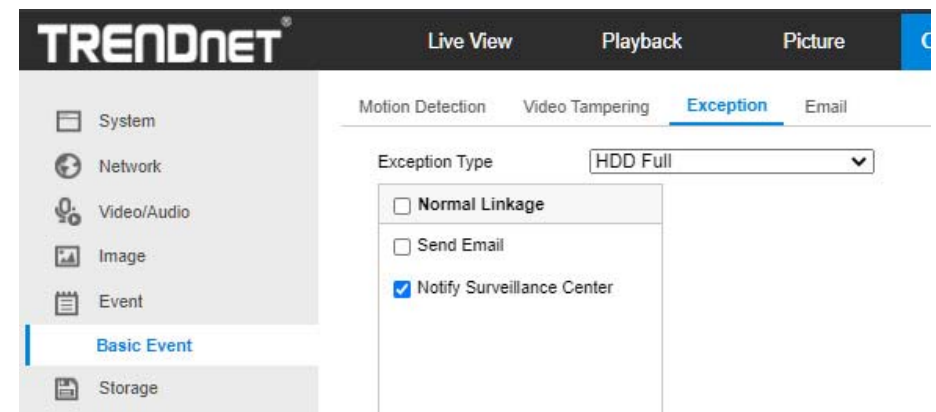


You can configure the camera to trigger the alarm when the lens is covered and take certain alarm response actions.

Detection area for this alarm is the whole screen.

1. Check **Enable Video Tampering** checkbox to enable the video tampering detection.
2. Click **Edit** to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Check the checkbox to select the linkage method taken for the video tampering.
3. Click **Save** to save the settings.

Exceptions



The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the cameras.

Email

TRENDnet Live View Playback Picture **Configuration** admin

Motion Detection Video Tampering Exception **Email**

System Network Video/Audio Image Event **Basic Event** Storage

Sender:

Sender's Address:

SMTP Server:

SMTP Port:

E-mail Encryption:

☐ Attached Image

Interval:

☐ Authentication

User Name:

Password:

Confirm:

No.	Receiver	Receiver's Address	Test
1			<input type="button" value="Test"/>
2			
3			

Steps:

1. Enter the TCP/IP Settings (**Configuration > Network > Basic Settings > TCP/IP**) to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.
2. Enter the Email Settings interface: **Configuration > Network > Advanced Settings > Email**.
3. Configure the following settings:

Sender: The name of the email sender.

Sender's Address: The email address of the sender.

SMTP Server: IP address or host name (e.g., smtp.263xmail.com) of the SMTP Server.

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.

Email Encryption: None, SSL, and TLS are selectable. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS. The SMTP port should be set as 465 for this encryption method. When you select SSL or TLS and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

Note: If you want to use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check the Enable STARTTLS checkbox when the protocol is not supported by your e-mail sever, your e-mail will not be encrypted.

Attached Image: Check the checkbox of Attached Image if you want to send emails with attached alarm images.

Interval: The interval refers to the time between two actions of sending attached pictures.

Authentication (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and input the login user name and password.

- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

The **Receiver** table: Select the receiver to which the email is sent. Up to 3 receivers can be configured.

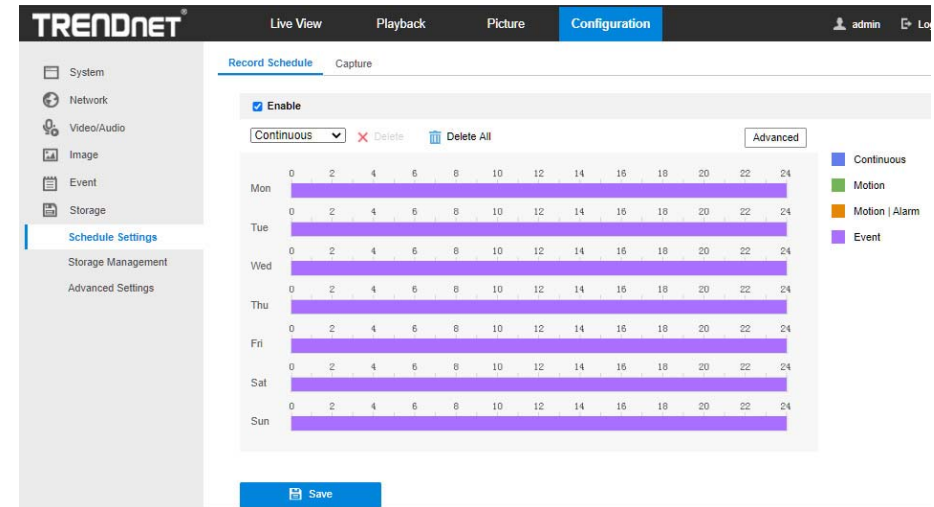
Receiver: The name of the user to be notified.

Receiver's Address: The email address of user to be notified.

4. Click **Save** to save the settings.

Storage – Schedule Settings

Record Schedule



Steps:

1. Check the checkbox of **Enable** to enable scheduled recording.
2. Click **Advanced** to set the camera record parameters.
 - **Pre-record:** The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.
The Pre-record time can be configured as No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s or not limited.
 - **Post-record:** The time you set to stop recording after the scheduled

time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

The Post-record time can be configured as 5s, 10s, 30s, 1 min, 2 min, 5 min or 10 min.

- **Stream Type:** Select the stream type for recording.

Note: The record parameter configurations vary depending on the camera model.

3. Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.

- **Continuous**

If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.

- **Record Triggered by Motion Detection**

If you select **Motion Detection**, the video will be recorded when the motion is detected.

Besides configuring the recording schedule, you have to set the motion detection area and check the checkbox of Trigger Channel in the Linkage Method of Motion Detection Settings interface. For detailed information.

- **Record Triggered by Alarm**

If you select **Alarm**, the video will be recorded when the alarm is triggered via the external alarm input channels.

Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method** of **Alarm Input Settings** interface. **Record Triggered by Motion & Alarm**

If you select **Motion & Alarm**, the video will be recorded when the motion and alarm are triggered at the same time.

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. **Record Triggered by Motion | Alarm**

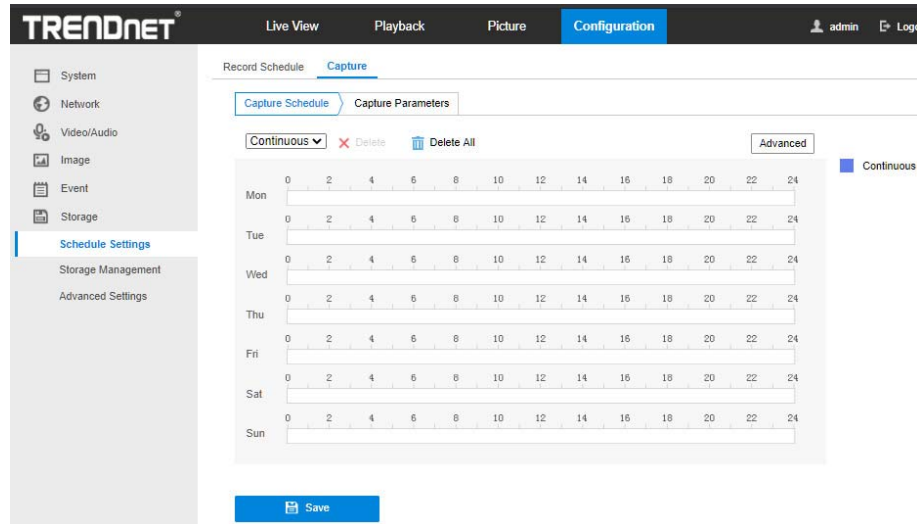
If you select **Motion | Alarm**, the video will be recorded when the external alarm is triggered or the motion is detected.

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. **Record Triggered by Events**

If you select **Event**, the video will be recorded if any of the events is triggered. Besides configuring the recording schedule, you have to configure the event settings.

4. Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.
5. Click **Save** to save the settings.

Capture



You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the local storage or network storage.

Steps:

1. Enter the Capture Settings interface: **Configuration > Storage > Storage Settings > Capture**.
2. Go to **Capture Schedule** tab to configure the capture schedule by click-and-drag the mouse on the time bar. You can copy the record schedule to other days by clicking the green copy icon on the right of each time

bar.

3. Click **Advanced** to select stream type.
4. Click **Save** to save the settings.
5. Go to **Capture Parameters** tab to configure the capture parameters.
 - (1) Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.
 - (2) Select the picture format, resolution, quality and capture interval.
 - (3) Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
 - (4) Select the picture format, resolution, quality, capture interval, and capture number.

TRENDnet Live View Playback Picture **Configuration**

Record Schedule **Capture**

Capture Schedule Capture Parameters

Timing

☐ Enable Timing Snapshot

Format: JPEG

Resolution: 1920*1080

Quality: High

Interval: 1000 milliseconds

Event-Triggered

☐ Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 1920*1080

Quality: High

Interval: 1000 milliseconds

Capture Number: 4

Save

6. Set the time interval between two snapshots.
7. Click **Save** to save the settings.

Storage – Storage Management

HDD Management

TRENDnet Live View Playback Picture **Configuration** admin Logout

HDD Management Net HDD

HDD Management

HDD No.	Capacity	Free space	Status	Type	Property	Progress

Quota

Max. Picture Capacity: 0.00GB

Free Size for Picture: 0.00GB

Max. Record Capacity: 0.00GB

Free Size for Record: 0.00GB

Percentage of Picture: 25%

Percentage of Record: 75%

Save

The network disk should be available within the network and properly configured to store the recorded files, log files, pictures, etc.

Steps:

1. Add Net HDD.
 - (1) Enter the Net HDD settings interface, **Configuration > Storage > Storage Management > Net HDD**.
 - (2) Enter the IP address of the network disk, and enter the file path.

- (3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

Note: Please refer to the *NAS User Manual* for creating the file path.

- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- (4) Click **Save** to add the network disk.

2. Initialize the added network disk.

- (1) Enter the HDD Settings interface, **Configuration > Storage > Storage Management > HDD Management**, in which you can view the capacity, free space, status, type and property of the disk.
- (2) If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.

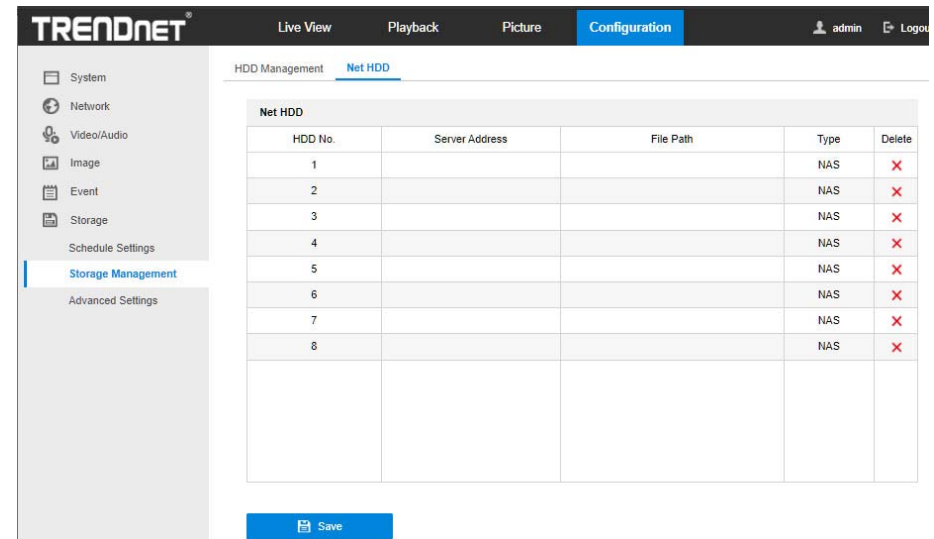
When the initialization completed, the status of disk will become **Normal**.

3. Define the quota for record and pictures.

- (1) Input the quota percentage for picture and for record.
- (2) Click **Save** and refresh the browser page to activate the settings.

Note:

Up to 8 NAS disks can be connected to the camera.



Storage – Advanced Settings

FTP

The screenshot shows the TRENDnet web interface for the TV-IP328PI device. The 'Configuration' tab is active, and the 'FTP' sub-tab is selected. The left sidebar lists various system settings, with 'Advanced Settings' under the 'Storage' category highlighted. The main configuration area for FTP includes fields for Server Address (0.0.0.0), Port (21), User Name, Password, and Confirm. It also features a 'Directory Structure' dropdown set to 'Save in the root directory', a 'Picture Filing Interval' dropdown set to 'OFF', and a 'Picture Name' dropdown set to 'Default'. There are checkboxes for 'Anonymous' and 'Upload Picture', and a 'Test' button. A large blue 'Save' button is positioned at the bottom right of the configuration area.

You can configure the FTP/SFTP server related information to enable the uploading of the captured pictures to the FTP/SFTP server. The captured pictures can be triggered by events or a timing snapshot task.

1. Select the FTP protocol.
2. Input the server address and port.
3. Configure the FTP/SFTP settings; and the user name and password are required for the FTP server login.

- For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Set the directory structure and picture filing interval.

Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

Picture Filing Interval: For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

Picture Name: Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is,

IP address_channel number_capture time_event type.jpg

Or you can customize it by adding a **Custom Prefix** to the default naming rule.

5. Check the Upload Picture checkbox to enable the function.

Upload Picture: To enable uploading the captured picture to the FTP server.

Anonymous Access to the FTP Server (in which case the user name and password won't be required.): Check the **Anonymous** checkbox to enable the anonymous access to the FTP server.

Note: The anonymous access function must be supported by the FTP server.

6. Click **Save** to save the settings.

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 TV-IP328PI 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 TV-IP328PI 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 TV-IP328PI 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 TV-IP328PI vastavust direktiivi 2004/108/EÜ ja 2006/95/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, TRENDnet, declares that this TV-IP328PI 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 TV-IP328PI 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 ΤΟ TV-IP328PI ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2004/108/ΕΚ, 2006/95/ΕΚ και.

Français [French]	Par la présente TRENDnet déclare que l'appareil TV-IP328PI 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 TV-IP328PI è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2004/108/CE e 2006/95/CE.
Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TV-IP328PI atbilst Direktīvas 2004/108/EK un 2006/95/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruojama, kad šis TV-IP328PI atitinka esminius reikalavimus ir kitas 2004/108/EB ir 2006/95/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TV-IP328PI 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 TV-IP328PI jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2004/108/KE u 2006/95/KE.
Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozik, hogy a TV-IP328PI megfelel a vonatkozó alapvető követelményeknek és az 2004/108/EK és a 2006/95/EK irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym TRENDnet oświadcza, że TV-IP328PI jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2004/108/WE i 2006/95/.
Português [Portuguese]	TRENDnet declara que este TV-IP328PI 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 TV-IP328PI v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2004/108/ES in 2006/95/ES.
Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TV-IP328PI spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2004/108/ES a 2006/95/ES.
Suomi [Finnish]	TRENDnet vakuuttaa täten että TV-IP328PI 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 TV-IP328PI 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-IP328PI – 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 DATA, 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.

2/15/2020

TV-IP328PI 1.0



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
