







TruVision Panoramic Wi-Fi Wedge IP Camera Configuration Manual

Copyright	© 2015 United Technologies Corporation. Interlogix is part of UTC Building & Industrial Systems, a unit of United Technologies Corporation. All rights reserved.
Trademarks and patents	Trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Manufacturer	Interlogix. 2955 Red Hill Avenue, Costa Mesa, CA 92626-5923, USA Authorized EU manufacturing representative: UTC Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, The Netherlands
Certification	  
FCC compliance	Class B: 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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
ACMA compliance	Notice! This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
European Union directives	2004/108/EC (EMC directive): Hereby, UTC Climate Controls & Security declares that this device is in compliance or with the essential requirements and other relevant provisions of Directive 2004/108/EC
	2006/66/EC (battery directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info .
Contact information	For contact information, see www.utcfireandsecurity.com or www.utcfssecurityproducts.eu .

Content

Introduction 3

Network access 4

Checking your web browser security level 4

Accessing the camera over the network 6

Overview of the camera web browser 6

Camera configuration 8

Configuration menu overview 8

Local configuration 9

System time 10

Network settings 12

Recording parameters 24

Video image 27

OSD (On Screen Display) 29

Overlay text 30

Privacy masks 31

Motion detection alarms 31

Tamper-proof alarms 35

Exception alarms 36

Alarm inputs and outputs 37

Cross line detection 38

Intrusion Detection 40

Snapshot parameters 41

NAS settings 43

Storage devices 44

Recording schedule 45

Camera management 48

User management 48

Authentication 50

IP address filter 51

Restore default settings 52

Import/export a configuration file 53

Upgrade firmware 54

Reboot camera 54

Camera operation 55

Logging on and off 55

Live view mode 55

Playing back recorded video 56

Searching event logs 58

Index 61

Introduction

This is the configuration manual for TruVision Panoramic Wedge IP camera models:

IP Wi-Fi panoramic wedge camera:

- TVW-1130 (3MPX Panoramic, 1.6 mm lens, Gray, Wi-Fi, PAL)
- TVW-3130 (3MPX Panoramic, 1.6 mm lens, Gray, Wi-Fi, NTSC)

Note: The camera has a horizontal viewing angle range between 127 and 160 degrees, depending on the resolution ratio settings.

Network access

This manual explains how to configure the camera over the network with a web browser.

TruVision IP cameras can be configured and controlled using Microsoft Internet Explorer (IE) and other browsers. The procedures described use Microsoft Internet Explorer (IE) web browser.

Checking your web browser security level

When using the web browser interface, you can install ActiveX controls to connect and view video using Internet Explorer. However, you cannot download data, such as video and images due to the increased security measure. Consequently you should check the security level of your PC so that you are able to interact with the cameras over the web and, if necessary, modify the Active X settings.

Configuring IE ActiveX controls

You should confirm the ActiveX settings of your web browser.

To change the web browser's security level:

1. In Internet Explorer click **Internet Options** on the **Tools** menu.
2. On the **Security** tab, click the zone to which you want to assign a web site under "Select a web content zone to specify its security settings".
3. Click **Custom Level**.

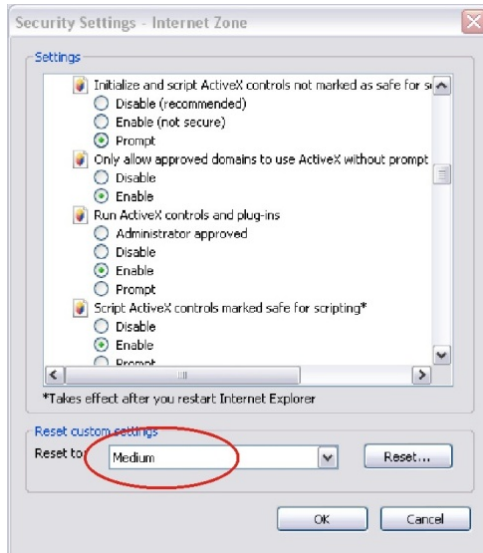


4. Change the **ActiveX controls and plug-ins** options that are signed or marked as safe to **Enable**. Change the **ActiveX controls and plug-ins** options that are unsigned to **Prompt** or **Disable**. Click **OK**.

- Or -

Under **Reset Custom Settings**, click the security level for the whole zone in the **Reset To** box, and select **Medium**. Click **Reset**.

Then click **OK** to the Internet Options Security tab window.



5. Click **Apply** in the **Internet Options Security** tab window.

Windows 7 and 8 users

Internet Explorer for Windows 7 and Windows 8 operating systems have increased security measures to protect your PC from any malicious software being installed.

To have complete functionality of the web browser interface with Windows 7 and Windows 8, do the following:

- Run the Browser interface as an administrator in your workstation
- Add the camera's IP address to your browser's list of trusted sites

To add the camera's IP address to Internet Explorer's list of trusted sites:

1. Open Internet Explorer.
2. Click **Tools**, and then **Internet Options**.
3. Click the **Security** tab, and then select the **Trusted sites** icon.
4. Click the **Sites** button.
5. Clear the "Require server verification (https:) for all sites in this zone" box.
6. Enter the IP address in the "Add this website to the zone" field.
7. Click **Add**, and then click **Close**.
8. Click **OK** in the Internet Options dialog window.
9. Connect to the camera for full browser functionality.

Accessing the camera over the network

Use the web browser to access and configure the camera over the network.

It is recommended that you change the administrator password once the setup is complete. Only authorized users should be able to modify camera settings. See “User management” on page 48 for further information.

To access the camera online:

1. In the web browser enter the camera’s IP address (default is 192.168.1.70). Use the tool, *TruVision Device Manager*, enclosed on the CD to find the IP address of the camera.

The Login dialog box appears.

Note: Ensure that the Active X controls are enabled.

2. Enter your user name and password.

User name: admin

Password: 1234

3. Click **Login**. The web browser window appears in live view mode.

Overview of the camera web browser

The camera web browser lets you view, record, and play back recorded videos as well as manage the camera from any PC with Internet access. The browser’s easy-to-use controls give you quick access to all camera functions. See Figure 1 on page 7.

If there is more than one camera connected over the network, open a separate web browser window for each individual camera.

Figure 1: Web browser interface

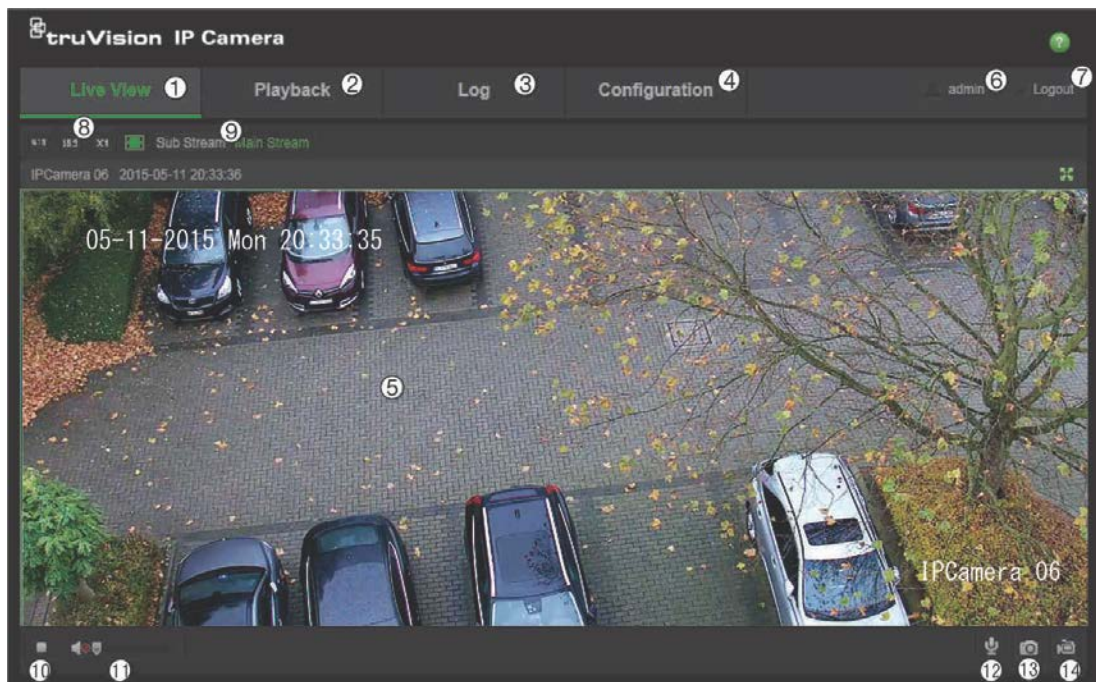


Table 1: Description of the web browser interface

Name	Description
1. Live view	Click to view live video.
2. Playback	Click to play back video.
3. Log	Click to search for event logs. There are three main types: Alarm, Exception and Operation.
4. Configuration	Click to display the configuration window for setting up the camera.
5. Viewer	View live video. Time, date and camera name are displayed here.
6. Current user	Displays current user logged on.
7. Logout	Click to log out from the system. This can be done at any time.
8. Aspect ratio	Select the aspect
9. Streaming	Switch between main stream and substream.
10. Start/stop live view	Click to start/stop live view.
11. Audio	Adjust volume.
12. Bidirectional audio	Turn on/off the microphone.
13. Capture	Click to take a snapshot of the video. The snapshot will be saved to the default folder in JPEG format.
14. Start/stop recording	Click to record live video.

Camera configuration

This chapter explains how to configure the cameras through a web browser.

Once the camera hardware has been installed, configure the camera's settings through the web browser. You must have administrator rights in order to configure the cameras over the internet.

The camera web browser lets you configure the camera remotely using your PC. Web browser options may vary depending on camera model.

There are two main folders in the configuration panel:

- Local configuration
- Configuration

Configuration menu overview

Use the **Configuration** panel to configure the network, camera, alarms, users, transactions and other parameters such as upgrading the firmware. See Figure 2 below for descriptions of the configuration folders available.

Figure 2: Configuration panel (Device Information tab selected)

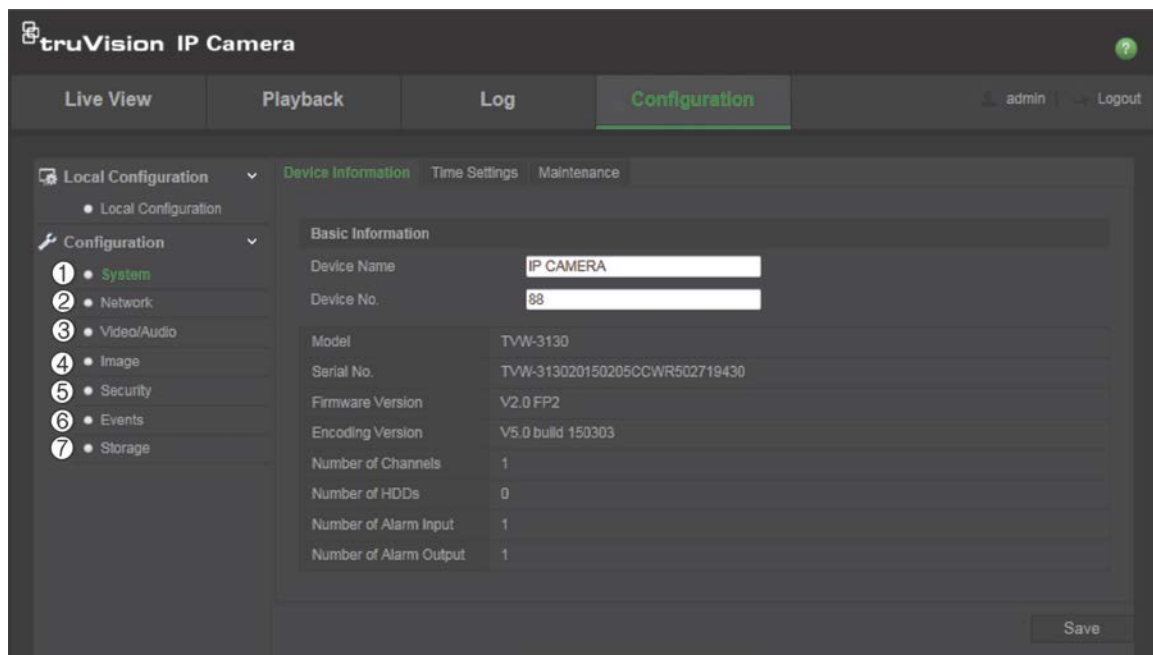


Table 2: Description of the Configuration parameters

Configuration folders	Description
1. System	Defines device basic information including SN and the current firmware version, time settings, maintenance, and serial port parameters. See “System time” on page 10, “Restore default settings” on page 52, and “Upgrade firmware” on page 54 for more information.
2. Network	Defines the network parameters required to access the camera over the internet. See “Network settings” on page 12 for more information.

Configuration folders	Description
3. Video/Audio	Defines recording parameters. See “Recording parameters” on page 24 for more information.
4. Image	Defines the image parameters, OSD settings, overlay text, and privacy mask. See “Video image” on page 27, “OSD (On Screen Display)” on page 29, “Overlay text” on page 30, and “Privacy masks” on page 31 for more information.
5. Security	Defines who can use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and telnet access. See “Camera management” on page 48 for more information.
6. Events	Defines motion detection, tamper-proof, alarm input/output, exception alarms, and snapshot configuration. See “Motion detection alarms” on page 31, “Tamper-proof alarms” on page 35, “Exception alarms” on page 36, and “Snapshot parameters” on page 41 for more information.
7. Storage	Defines recording schedule, storage management, and NAS configuration. See “NAS settings” on page 43, “Storage devices” on page 44, and “Recording schedule” on page 45 for more information.

Local configuration

Use the Local menu to manage the protocol type, rules of intelligence, live view performance, and local storage paths. In the Configuration panel, click **Local Configuration** to display the local configuration window. See Figure 3 and Table 3 below for descriptions of the different menu parameters.

Figure 3: Local configuration menu

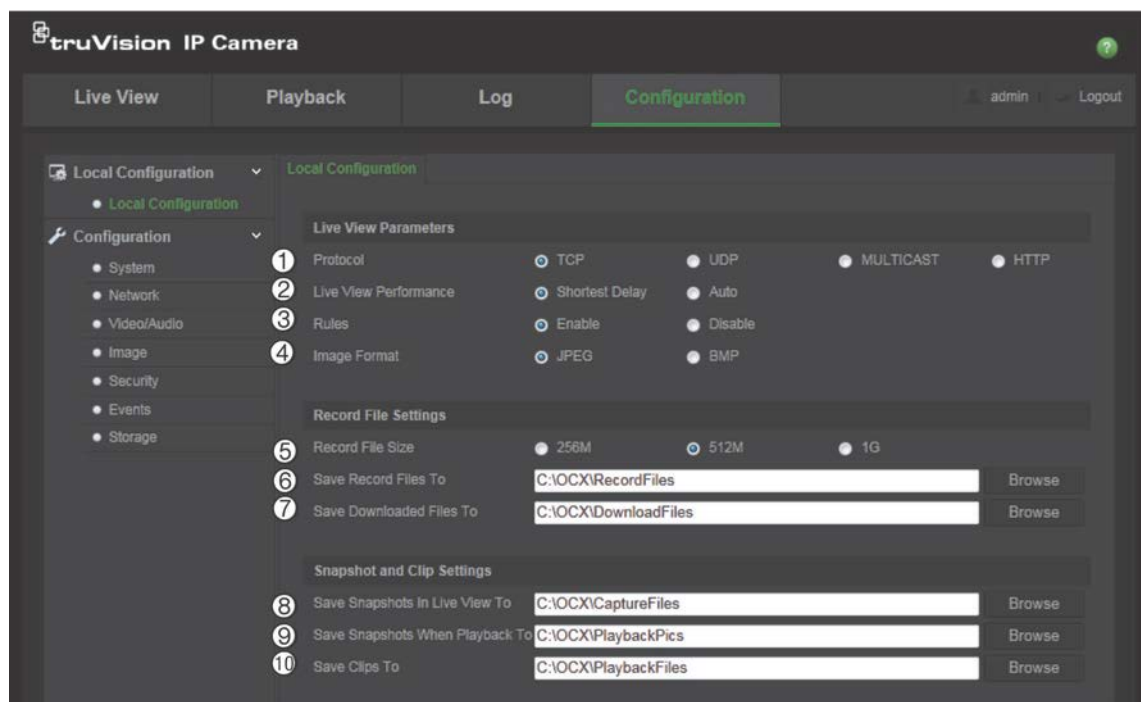


Table 3: Description of the local configuration parameters

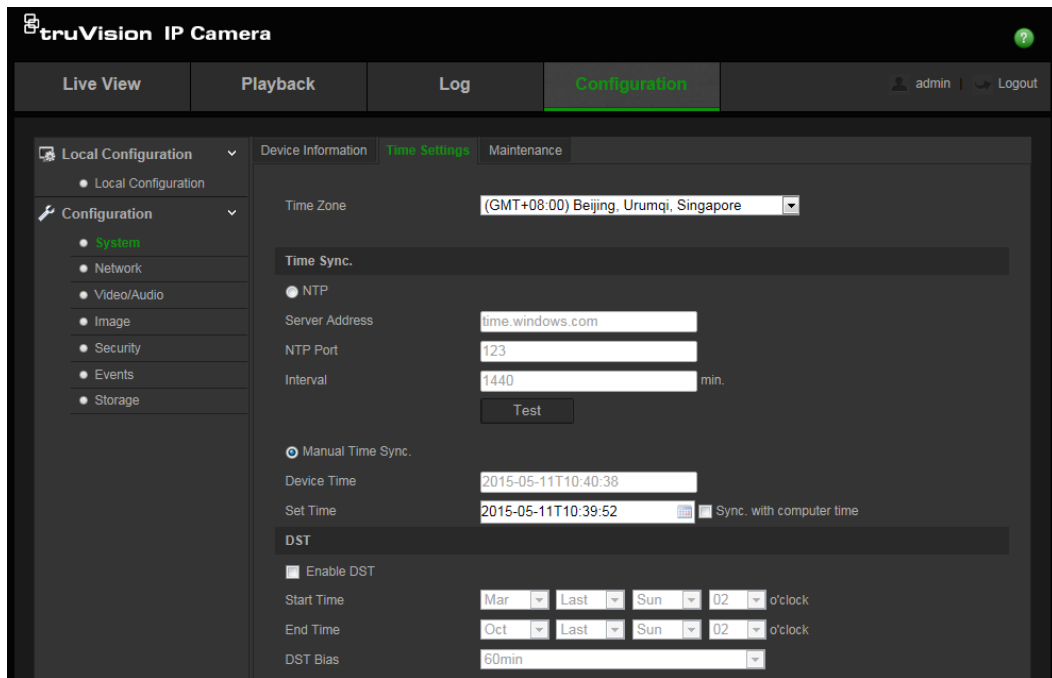
Parameters	Description
Live View Parameters	
1. Protocol	Specifies the network protocol used. Options include: TCP, UDP, MULTICAST and HTTP.
2. Live View Performance	Specifies the transmission speed. Options include: Shortest Delay or Auto.
3. Rules	It refers to the rules on your local browser. Specify whether or not to display the colored marks when motion detection, face detection, and intrusion detection are triggered. For example, when the rules option is enabled and a face is detected, the face will be marked with a green rectangle in live view.
4. Image Format	Choose the image format for a snapshot: JPEG or BMP.
Record File Settings	
5. Record File Size	Specifies the maximum file size. Options include: 256 MB, 512 MB and 1G.
6. Save Record Files to	Specifies the directory for recorded files.
7. Save Downloaded Files to	Specifies the directory for downloaded files.
Picture and Clip Settings	
8. Save Snapshots In Live View To	Specifies the directory for saving snapshots in live view mode.
9. Save Snapshots When Playback To	Specifies the directory for saving snapshots in playback mode.
10. Save Clips To	Specifies the directory for saving video clips in playback mode.


System time

NTP (Network Time Protocol) is a protocol for synchronizing the clocks of network devices, such as IP cameras and computers. Connecting network devices to a dedicated NTP time server ensures that they are all synchronized.

To define the system time and date:

1. In the **System** panel, click the **Time Settings** tab to open its window.



2. From the **Time Zone** drop-down menu, select the time zone that is the closest to the camera's location.
3. Under **Time Sync** check one of the options for setting the time and date:
Synchronize with an NTP server: Check the **NTP** enable box and enter the server NTP address. The time interval can be set from 1 to 10080 minutes.
- Or -
Set manually: Enable the **Manual Time Sync** function and then click  to set the system time from the pop-up calendar.
Note: You can also check the **Sync with computer time** check box to synchronize the time of the camera with the time of your computer.
4. Check **Enable DST** to enable the DST function, and set the date of the DST period.
5. Click **Save** to save changes.

Network settings

Accessing the camera through a network requires that you define certain network settings. Use the Network panel to define the network settings. See Figure 4 and Table 4 below for further information.

Figure 4: Network window (TCP/IP tab shown)

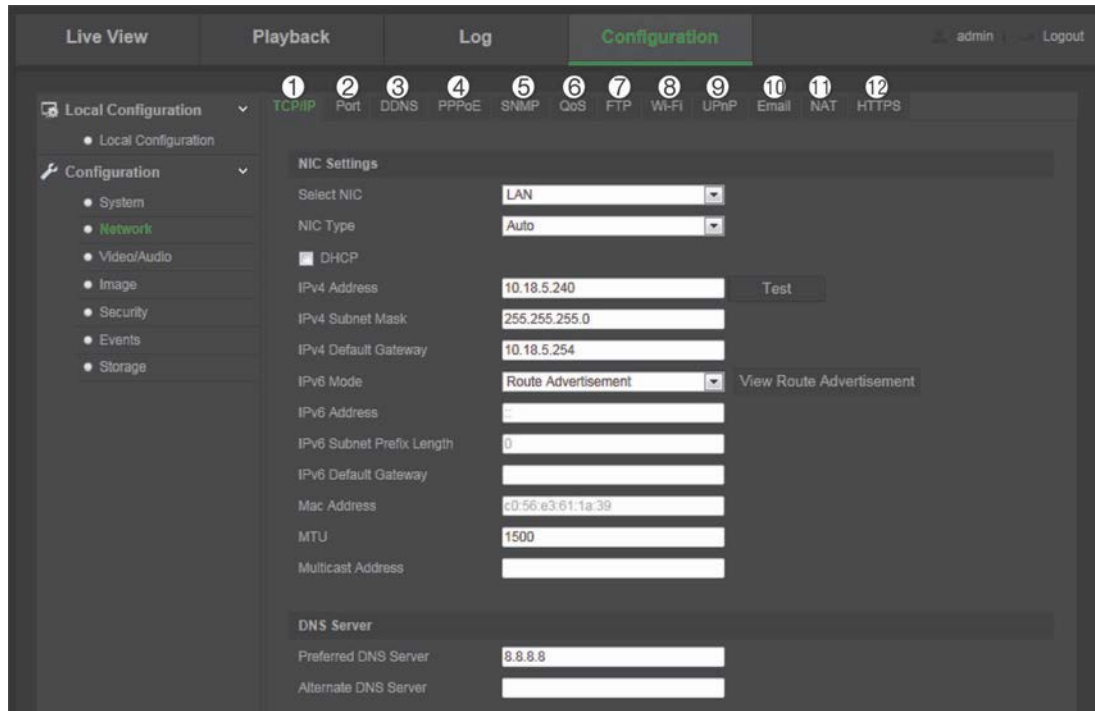


Table 4: Network parameters

Parameters	Description
1. TCP/IP	<p>Select NIC: Specifies LAN or WLAN for different network.</p> <p>NIC Type: Specifies the NIC type. Default is Auto. Other options include: 10M Half-dup, 10M Full-dup, 100M Half-dup and 100M Full-dup.</p> <p>DHCP: Enable to automatically obtain an IP address and other network settings from that server.</p> <p>IPv4 Address: Specifies the IPv4 address of the camera.</p> <p>IPv4 Subnet Mask: Specifies the IPv4 subnet mask.</p> <p>IPv4 Default Gateway: Specifies the IPv4 gateway IP address.</p> <p>IPv6 Mode: Specifies the IPv6 mode, including Manual, DHCP and Router Advertisement.</p> <p>IPv6 Address: Specifies the IPv6 address of the camera.</p> <p>IPv6 Subnet Prefix Length: Specifies the IPv6 prefix length.</p> <p>IPv6 Default Gateway: Specifies the IPv6 gateway IP address.</p> <p>Mac Address: Specifies the mac address of the camera.</p> <p>MTU: Specifies the valid value range of MTU. Default is 1500.</p> <p>Multicast Address: Specifies a D-class IP address between 224.0.0.0 to 239.255.255.255. Only specify this option if you are using the multicast function. Some routers prohibit the use of multicast function in case of a network storm.</p> <p>DNS server: Specifies the DNS server for your network.</p>

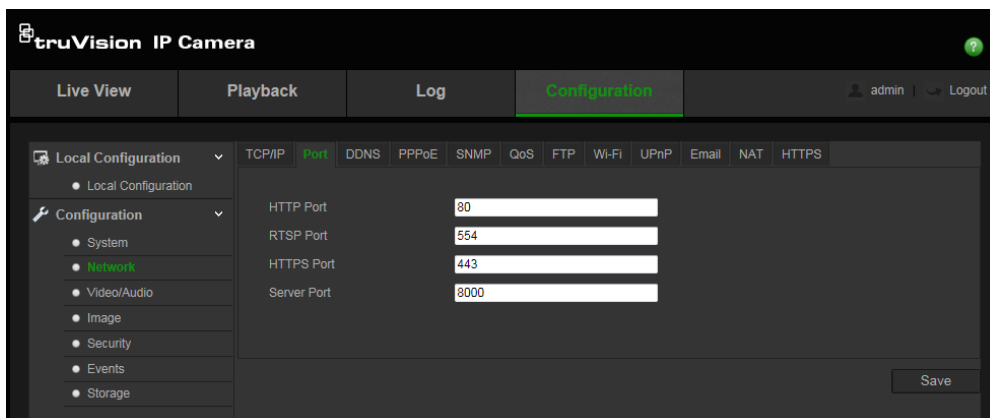
Parameters	Description
2. Port	<p>HTTP Port: The HTTP port is used for remote internet browser access. Enter the port used for the Internet Explorer (IE) browser. The default value is 80.</p> <p>RTSP Port: RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. Enter the RTSP port value. The default port number is 554.</p> <p>HTTPS Port: HTTPS (Hyper Text Transfer Protocol Secure) allows video to be securely viewed when using a browser. Enter the HTTPS port, value. The default port number is 443.</p> <p>Server Port: This is used for remote client software access. Enter the server port value. The default port number is 8000.</p>
3. DDNS	<p>DDNS is a service that maps Internet domain names to IP addresses. It is designed to support dynamic IP addresses, such as those assigned by a DHCP server.</p> <p>Specifies IP server, DynDNS, or ezDDNS.</p> <p>DynDNS (Dynamic DNS): Enter the user name and password registered to the DynDNS web site. The domain name is that of the DynDNS web site.</p> <p>ezDDNS: Enter the host name. It will automatically register it online.</p> <p>IPServer: Enter the address of the IP Server.</p>
4. PPPoE	Retrieves a dynamic IP address.
5. SNMP	SNMP is a protocol for managing devices on networks. Enable SNMP to get camera status and parameter related information.
6. QoS	<p>QoS (Quality of Service) can help solve network delay and network congestion by configuring the priority of data being sent.</p> <p>Enable the option to solve network delay and network congestion.</p>
7. FTP	Enter the FTP address and folder to which camera snapshots can be uploaded.
8. Wi-Fi	Specifies the Wi-Fi network connection parameters.
9. UPnP	<p>The UPnP (Universal Plug and Play) protocol allows devices to connect seamlessly and simplifies the implementation of networks in the home and corporate environments. With the function enabled, you do not need to configure the port mapping for each port, and the camera is connected to the Wide Area Network (WAN) via the router.</p> <p>Enable and then set the friendly name to be detected.</p>
10. Email	Specifies the email address to which messages are sent when an alarm occurs.
11. NAT	Enable NAT (Network address translation) to remap one IP address into another while the camera streams are transited across a private network and the internet.
12. HTTPS	Provides authentication of the web site and associated web server that one is communicating with, which protects against man-in-the-middle attacks.

To define the TCP/IP parameters:

1. In the **Network** panel, click the **TCP/IP** tab to open its window.
2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings, MTU settings, and Multicast Address.
3. If the DHCP server is available, check **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server** or **Alternate DNS Server**.
5. Click **Save** to save changes.

To define the port parameters:

1. In the **Network** panel, click the **Port** tab to open its window.



2. Set the HTTP Port, RTSP port, HTTPS port, and Server port of the camera.

HTTP Port: The default port number is 80, and it can be changed to any port number that is not occupied.

RTSP Port: The default port number is 554. It can be changed to any port number in the range from 1 to 65535.

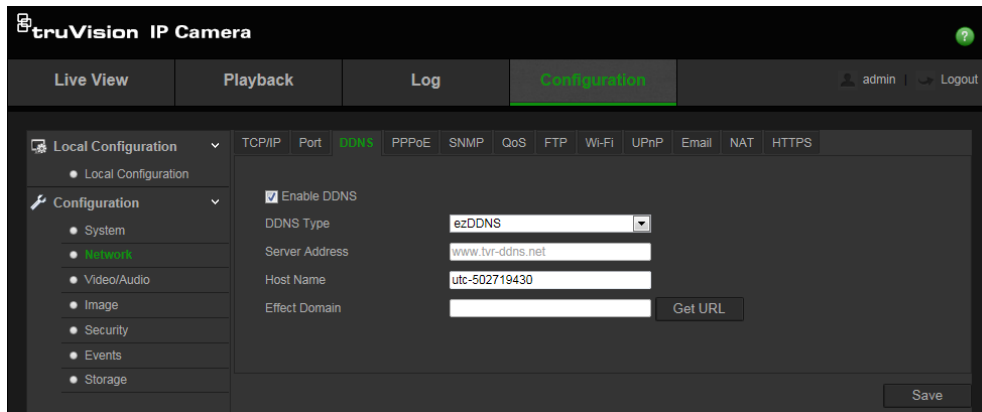
HTTPS Port: The default port number is 443. It can be changed to any port number that is not occupied.

Server Port: The default server port number is 8000. It can be changed to any port number in the range from 2000 to 65535.

3. Click **Save** to save changes.

To define the DDNS parameters:

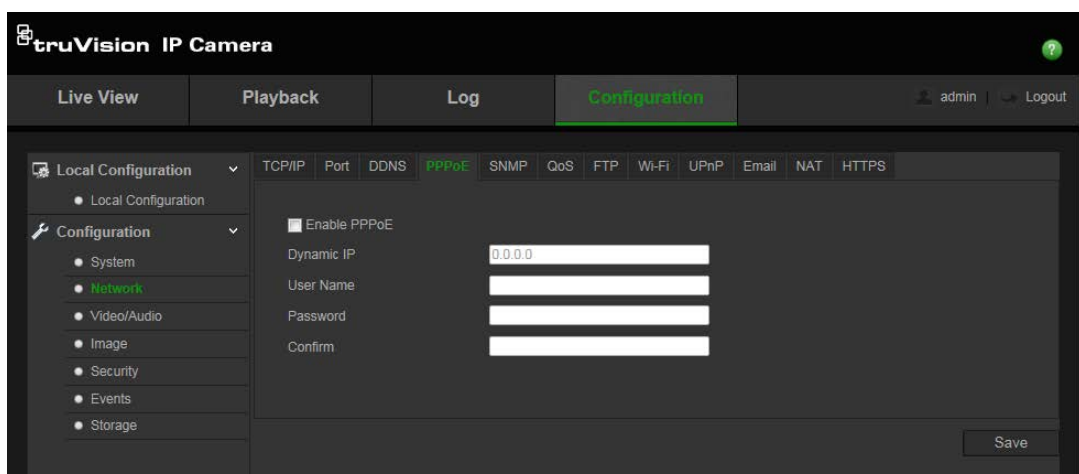
1. In the **Network** panel, click the **DDNS** tab to open its window.



2. Check **Enable DDNS** to enable this feature.
3. Select **DDNS Type**. Three options are available:
 - **DynDNS:** Enter the user name and password registered to the DynDNS web site. The domain name is that of the DynDNS web site.
 - **ezDDNS:** Enter the host name. It will automatically register it online.
 - **IPServer:** Enter the address of the IP Server.
4. Enter the host name.
5. Enter the Effect Domain address. Click the Get URL button to browse for the required address.
6. Click **Save** to save changes.

To define the PPPoE parameters:

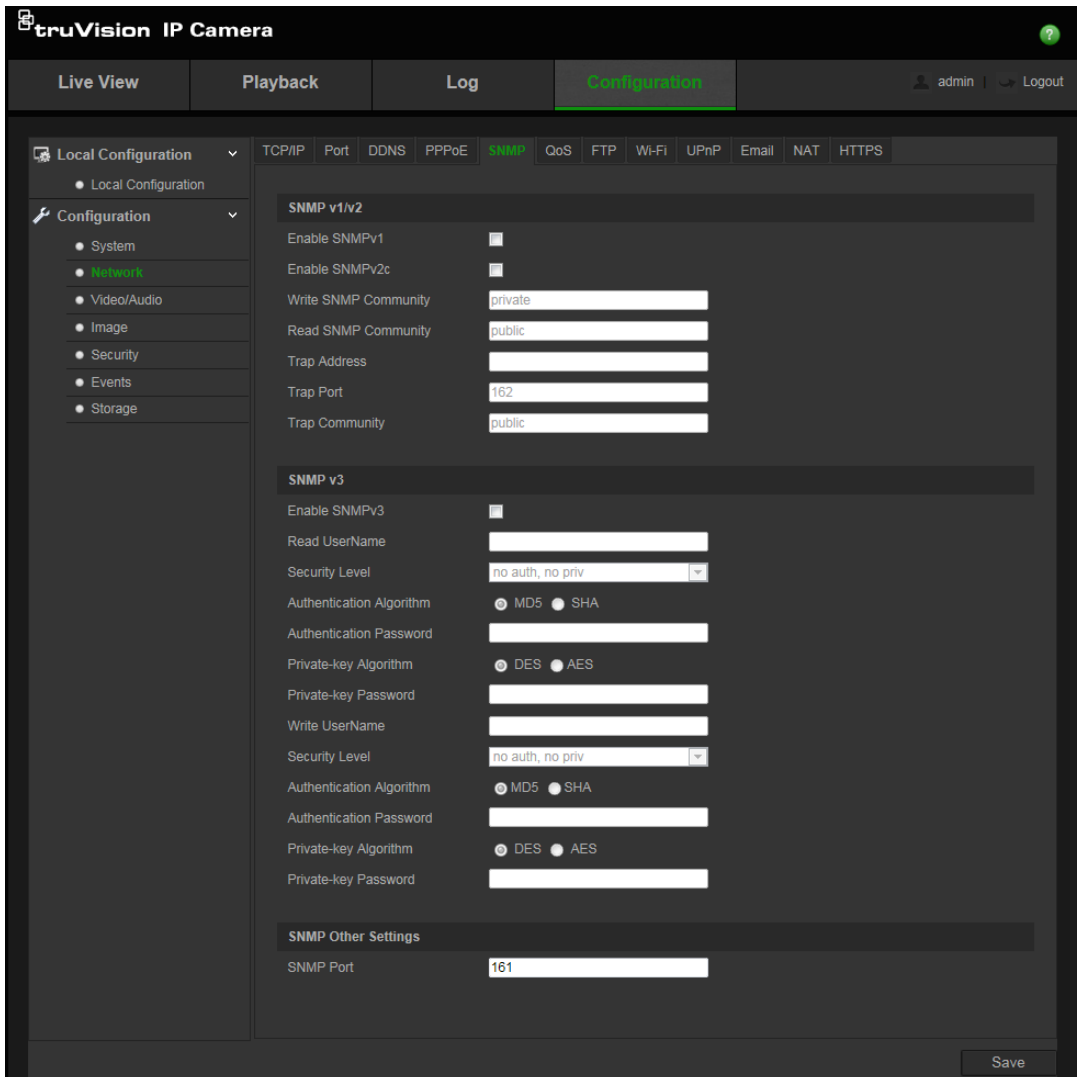
1. In the **Network** panel, click the **PPPoE** tab to open its window.



2. Check **Enable PPPoE** to enable this feature.
3. Enter User Name, Password, and Confirm password for PPPoE access.
4. Click **Save** to save changes.

To define the SNMP parameters:

1. In the **Network** panel, click the **SNMP** tab to open its window.

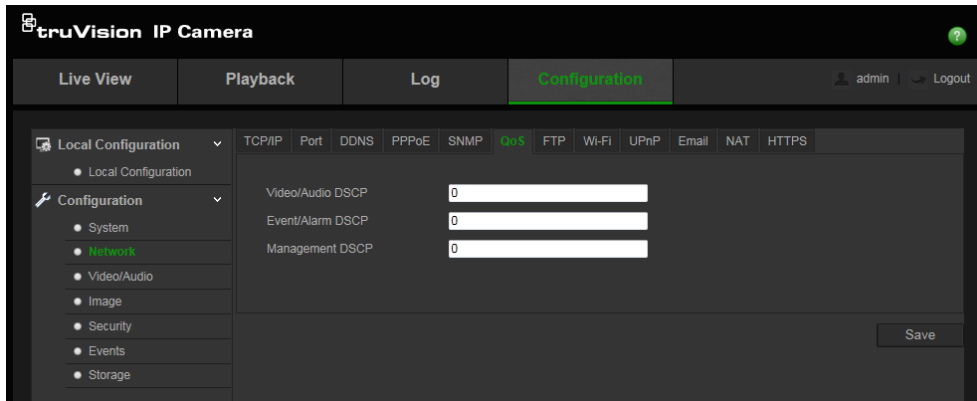


2. Select the corresponding version of SNMP: v1, v2c or v3.
3. Configure the SNMP settings. The configuration of the SNMP software should be the same as the settings you configure here.
4. Click **Save** to save changes.

Note: Before setting the SNMP, please download the SNMP software and manage to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the alarm recipient. The SNMP version you select should be the same as that of the SNMP software.

To define the QoS parameters:

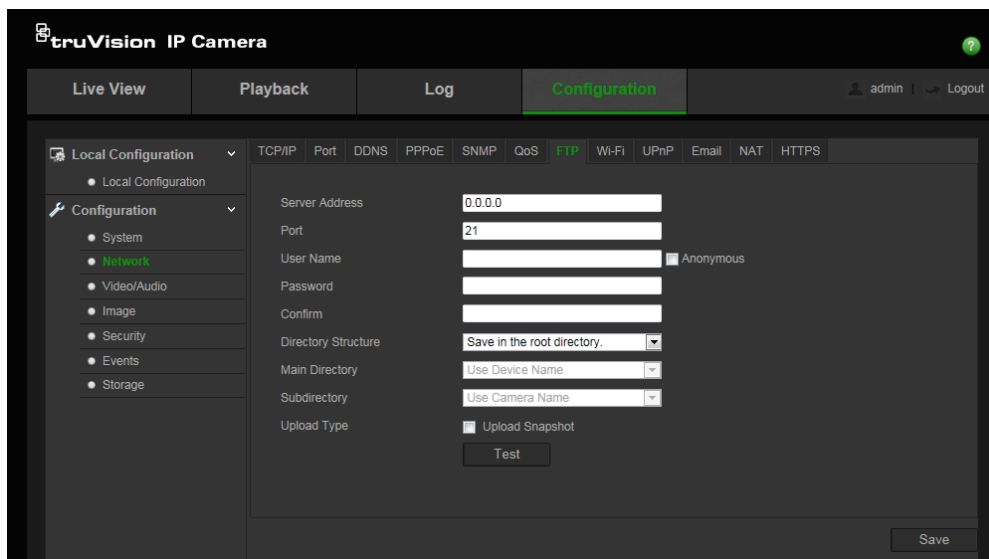
1. In the **Network** panel, click the **QoS** tab to open its window.



2. 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 larger the DSCP value is the higher the priority.
3. Click **Save** to save changes.

To define the FTP parameters:

1. In the **Network** panel, click the **FTP** tab to open its window.



2. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.

Anonymous: Check the check box to enable the anonymous access to the FTP server.

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.

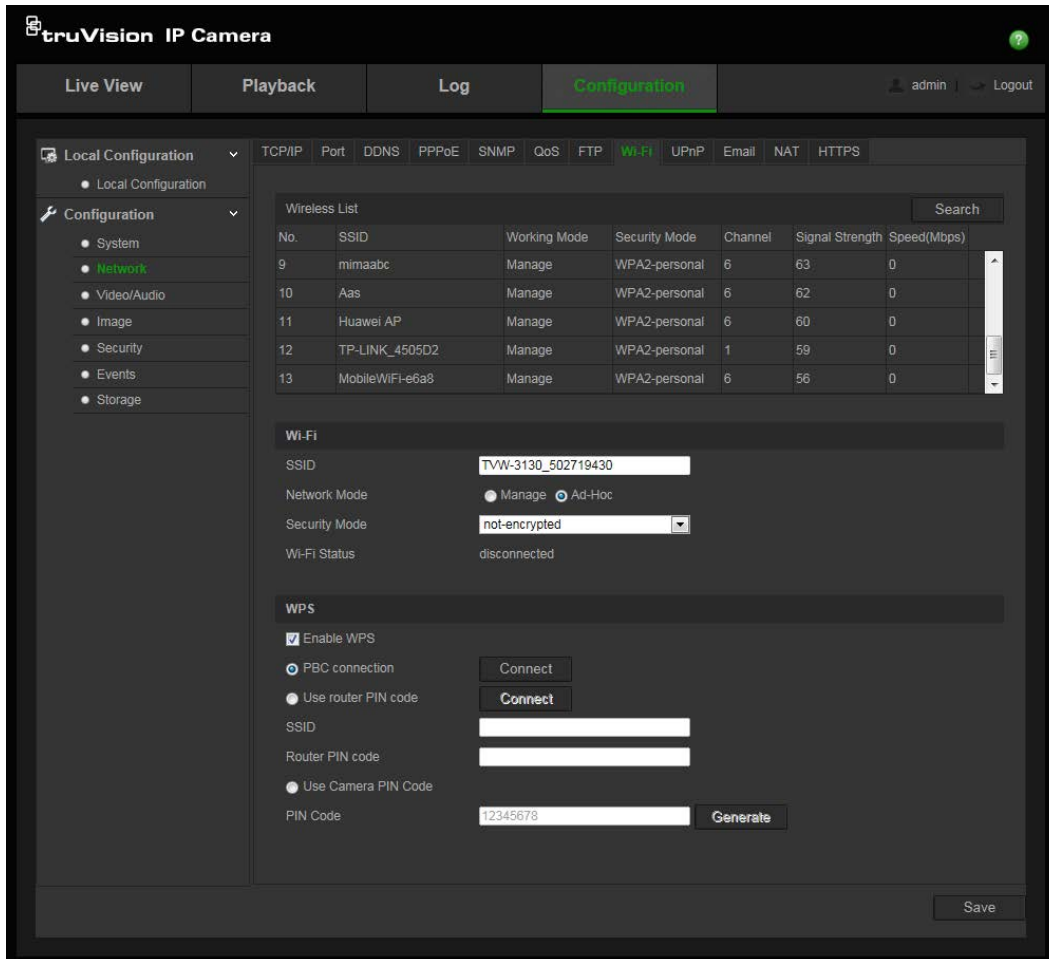
Upload type: To enable uploading the snapshots to the FTP server.

Test: Test whether the FTP address is accessible.

3. Click **Save** to save changes.

To define the parameters:

1. In the **Network** panel, click the **Wi-Fi** tab to open its window.



Note: When configuring the settings for the first time please connect the camera to a router via a network cable and open the web browser to complete the settings. When the **Status** changes from “Disconnected” to “Connected” the Wi-Fi connection has been set up successfully.

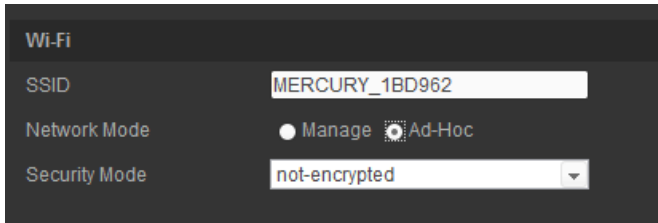
2. Click **Search** to search the online Wi-Fi connections.

3. Select a Wi-Fi connection from the list.

4. Select the Network Mode as **Manage** or **Ad-hoc**

When **Manage Mode** is selected, the Security Mode is automatically shown when you select a Wi-Fi connection from the list.

Select **Ad-Hoc Mode** when accessing the camera via a PC without going through a Wi-Fi router. You can identify the camera **SSID** and specify the **Security Mode** as needed.

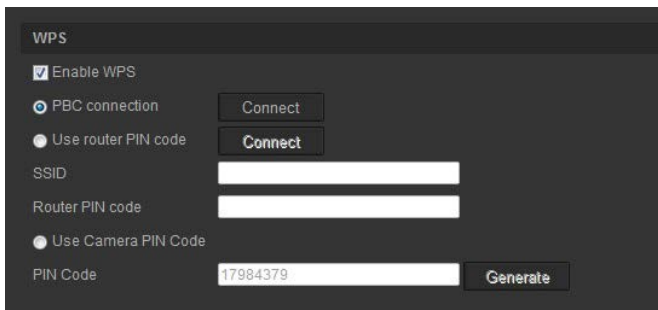


5. You can choose the **Security Mode** as not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, or WPA2-enterprise.
6. For quick setup, check the WPS check box to enable the WPS function.

PBC mode: Push the WPS button on the Wi-Fi router. The WPS indicator will flash (the WPS settings may differ per device. Please refer to the Wi-Fi router user manual for details). Check the **PBC connection** check box and click the **Connect** button. The camera and the Wi-Fi network router are connected automatically.

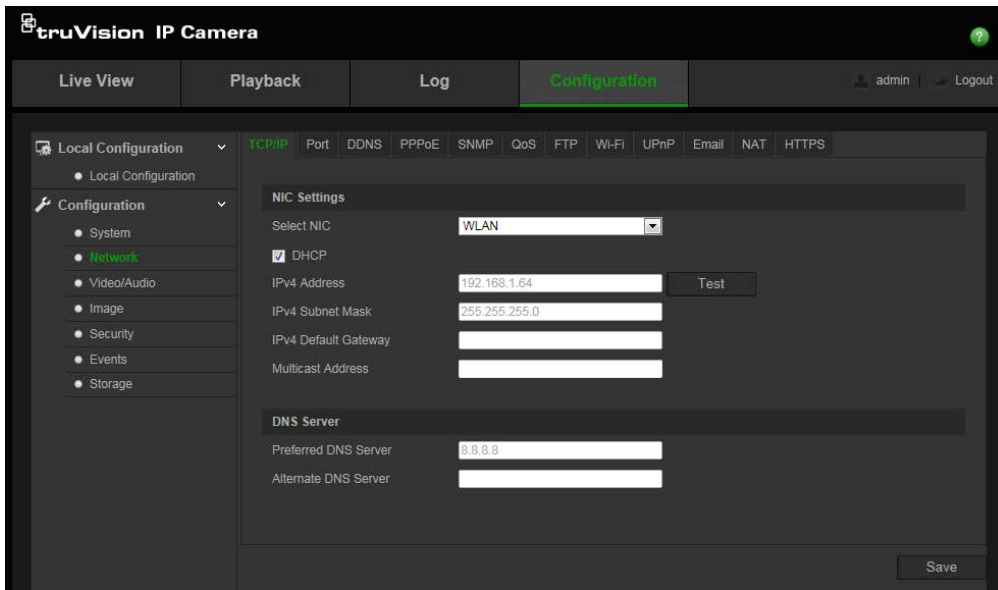
PIN Mode: Please check the Wi-Fi router device and find the PIN code, which is printed on a sticker or printed on the device. Enter the PIN code in the **Router PIN Code** text bar and check the **Use router PIN code**. Then click **Connect** to connect the camera to the Wi-Fi router.

You can generate the PIN code on the camera side and configure the Wi-Fi router to finish the connection setting (please refer to the Wi-Fi router user manual for details). Please note that the PIN code expiration time is 120 seconds.



To define the IP address settings:

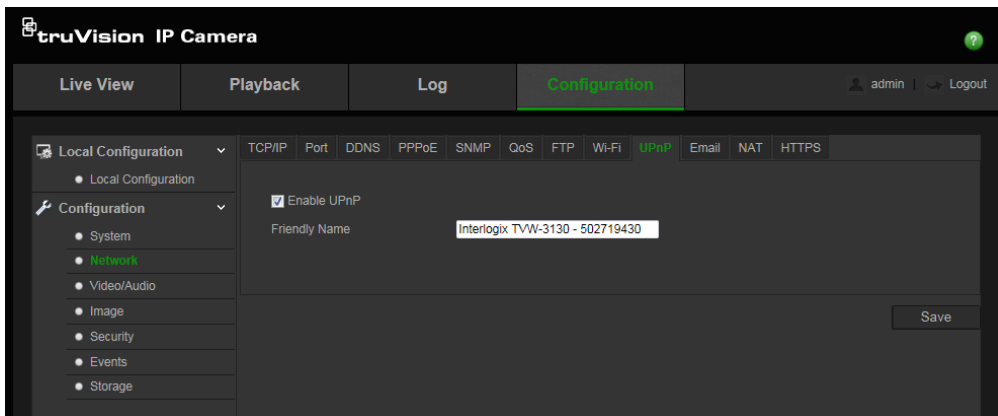
1. In the **Network** panel, click the **TCP/IP** tab to open its window.



2. Under **Select the NIC**, select WLAN.
3. Enter the IPv4 address, the IPv4 Subnet Mask, and the Default Gateway. If you want to be assigned the IP address, you can check the check box to enable the DHCP.

To define the UPnP parameters:

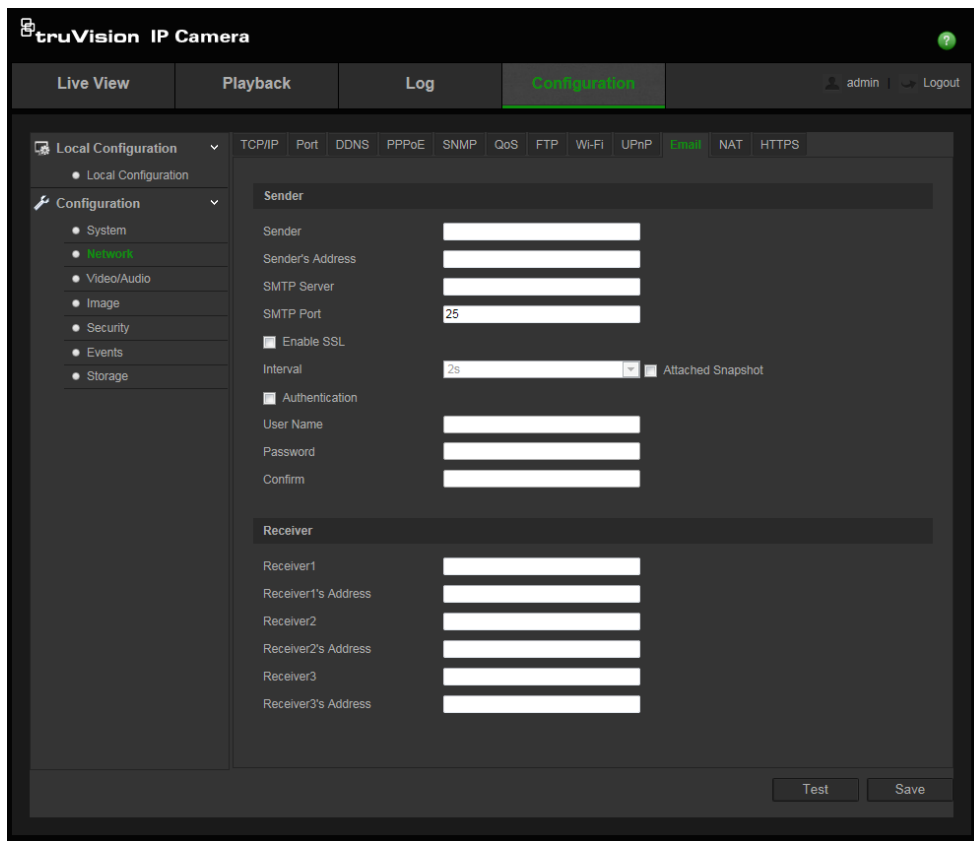
1. In the **Network** panel, click the **UPnP** tab to open its window.



2. Check the check box to enable the UPnP function. The name of the device when detected online can be edited.
3. Check the **Port Mapping**, and select Auto or Manual mode to modify the port number.
4. Click **Save** to save changes.

To set up the Email parameters:

1. In the **Network** panel, click the **Email** tab to open its window.



2. Configure the following settings:

Sender: Enter the name of the email sender.

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

SMTP Server: Enter the SMTP Server IP address or host name.

SMTP Port: Enter the SMTP port. The default is 25.

Enable SSL: Check the check box to enable SSL if it is required by the SMTP server.

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

Interval: This is the time between two actions when sending attached images.

Authentication: If your email server requires authentication, check this check box to use authentication to log in to this server. Enter the login user name and password.

User Name: This is the user name to log in to the server where the images are uploaded.

Password: Enter the password.

Confirm: Confirm the password.

Receiver1: Enter the name of the first user to be notified.

Receiver's Address1: The email address of the user to be notified.

Receiver2: Enter the name of the second user to be notified.

Receiver's Address2: Enter the email address of the second user to be notified.

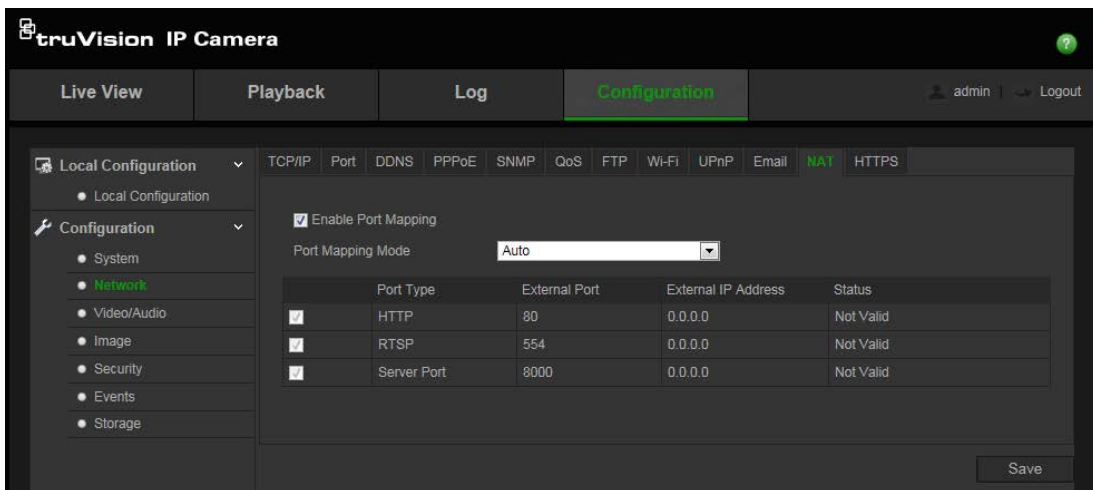
Receiver3: Enter the name of the third user to be notified.

Receiver's Address3: Enter the email address of the third user to be notified.

3. Click **Test** to test the email parameters set up.
4. Click **Save** to save changes.

To set up the NAT parameters:

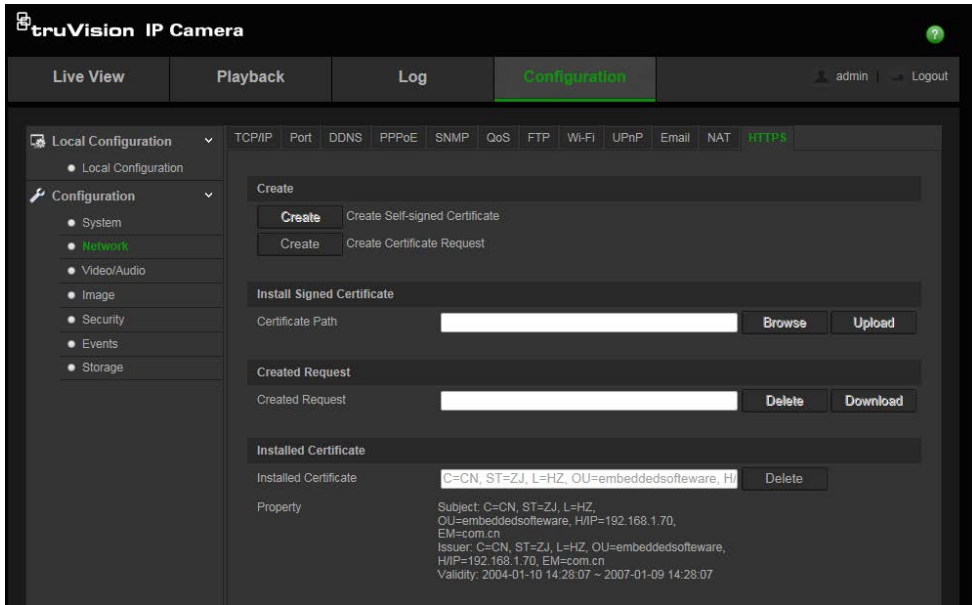
1. In the **Network** panel, click the **NAT** tab to open its window.



2. Check the check box to enable the NAT function.
3. Select **Port Mapping Mode** to be Auto or Manual. When you choose Manual mode, you can set the external port as desired.
3. Click **Save** to save changes.

To set up the HTTPS parameters:

1. In the **Network** folder, click the **HTTPS** tab to open its window.



2. To create a self-signed certificate:

Click the Create button beside **Create Self-signed Certificate**. Enter the country, host name/IP, validity and the other information requested.

Click **OK** to save the settings.

-Or-

To create a certificate request:

Click the Create button beside **Create Certificate Request**. Enter the country, host name/IP and the other information requested.

Click **OK** to save the settings. Download the certificate request and submit it to the trusted certificate authority for signature, such as Symantec or RSA. After receiving the signed valid certificate, upload the certificate to the device.

Recording parameters

You can adjust the video and audio recording parameters to obtain the image quality and file size best suited to your needs. Figure 5 and Table 5 below list the video and audio recording options you can configure for the camera.

Figure 5: Video/Audio Settings menu (Video tab shown)

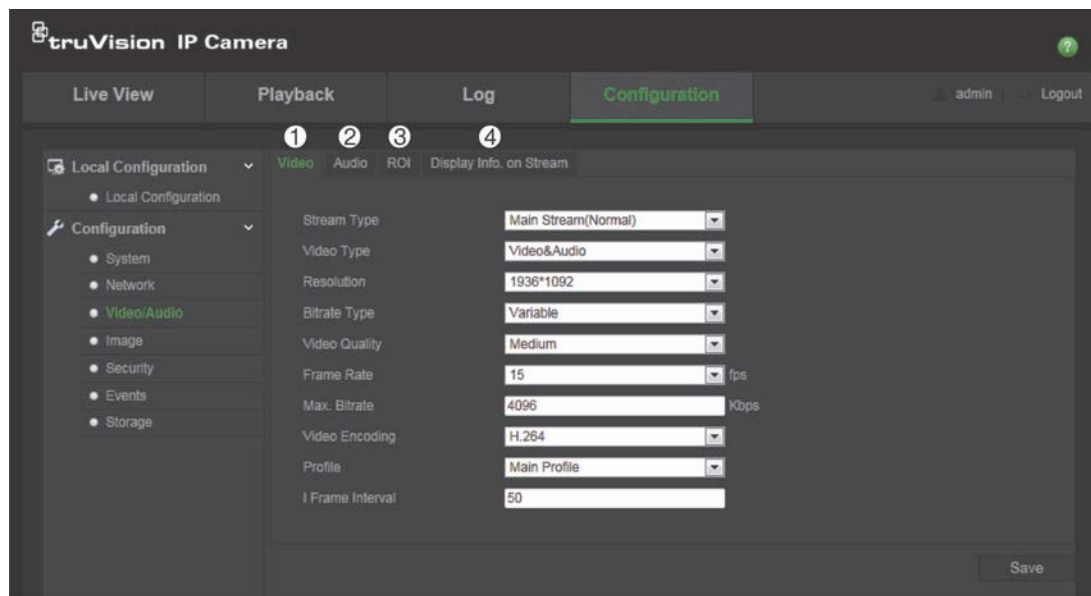


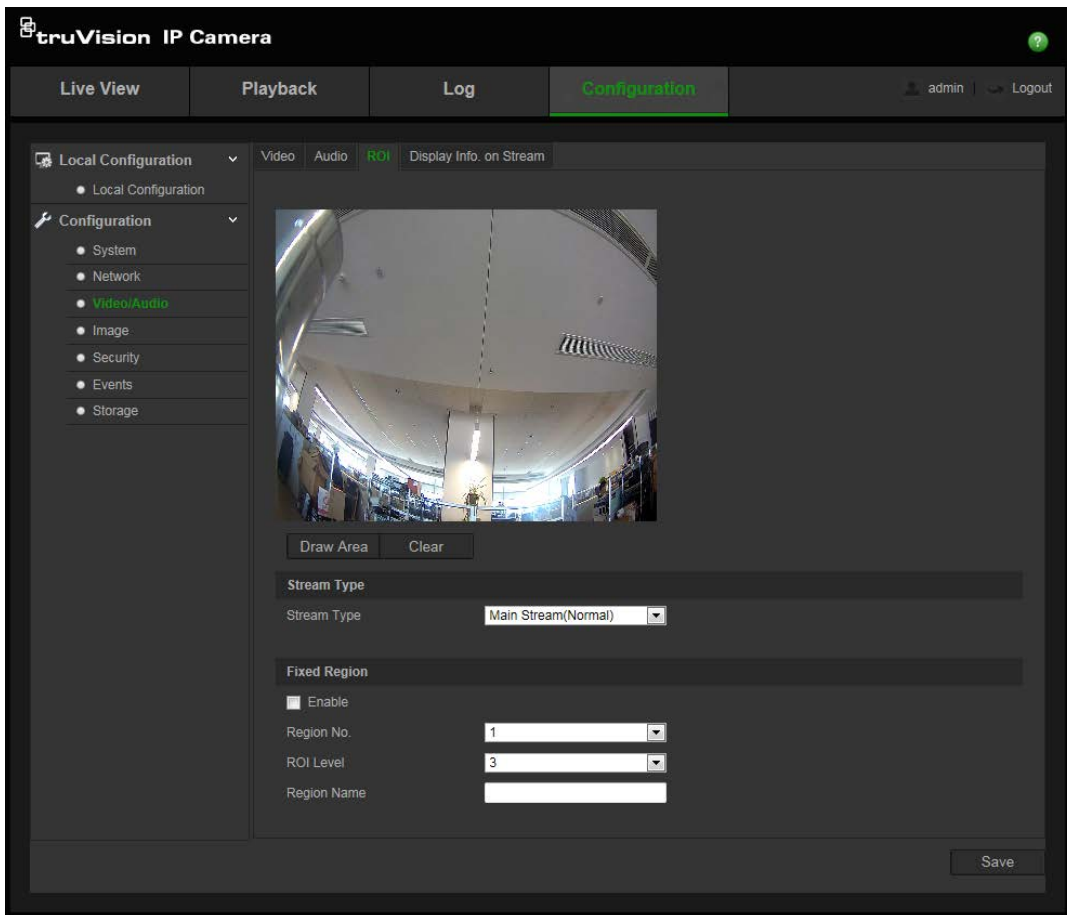
Table 5: Video setting parameters

Parameter	Description
1. Video	<p>Stream Type: Specifies the streaming method used. Options include: Main Stream (Normal) and Sub Stream.</p> <p>Video Type: Specifies the stream type you wish to record. Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams.</p> <p>Note: <i>Video</i> is default.</p> <p>Resolution: Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. The resolution options listed depend on the type of camera and on whether main or substream is being used.</p> <p>Note: Resolutions can vary depending on the camera model.</p> <p>Bitrate Type: Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.</p> <p>Video Quality: Specifies the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, Medium, Higher and Highest.</p>

Parameter	Description
	<p>Frame Rate: Specifies the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second.</p> <p>Note: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet.</p> <p>Max bit rate: Specifies the maximum allowed bit rate. A high image resolution requires that a high bit rate must also be selected.</p> <p>Video Encoding: Specifies the video encoder used.</p> <p>Profile: Different profile indicates different tools and technologies used in compression. Options include: Main Profile.</p> <p>I Frame Interval: A video compression method. It is strongly recommended not to change the default value 50.</p>
2. Audio	<p>Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2 and G.726 are optional.</p> <p>Audio Input: "MicIn" is selectable for the built-in microphone.</p> <p>Input Volume: Specifies the volume from 0 to 100.</p> <p>Environmental Noise Filter: Set it as OFF or ON. When you set the function on the noise detected can be filtered.</p>
3. ROI	<p>Enable to assign more encoding resource to the region of interest to increase the quality of the ROI whereas the background information is less focused.</p>
4. Display Info. On Stream	<p>When Dual-VCA mode is enabled, the camera sends video analytics results (meta data) to an NVR or other platforms to generate a VCA alarm.</p>

To define ROI parameters:

1. In the **Video/Audio** panel, click the **ROI** tab to open its window.



2. Draw the region of interest on the image. Only one region is supported.
3. Choose the stream type to set the ROI encoding.
4. Check the Fixed Region Enable box to manually configure the area. You can choose the image quality enhancing level for ROI encoding, and you can also name the ROI area.
5. Click **Save** to save changes.

Dual-VCA (Video Content Analysis)

When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.

For example, with an Interlogix NVR (please check Interlogix website for the latest NVR models supporting this feature), you can draw a virtual line in the NVR playback window, and search the objects or people crossing this virtual line.

Note: Only cross line and intrusion detection can support dual-VCA mode.

To define Dual-VCA parameters:

1. In the **Video/Audio** panel, click the **Display Info. On Stream** tab to open its window.
2. Check the check box to enable Dual-VCA.
3. Click **Save** to save changes.

Video image

You may need to adjust the camera image depending on the camera model or location background in order to get the best image quality. You can adjust the brightness, contrast, saturation, hue, and sharpness of the video image.

Use this menu to also adjust camera behavior parameters such as exposure time, iris mode, video standard, day/night switch, image flip, WDR, digital noise reduction, and white balance. See Figure 6 and Table 6 below for more information.

Figure 6: Camera image settings menu

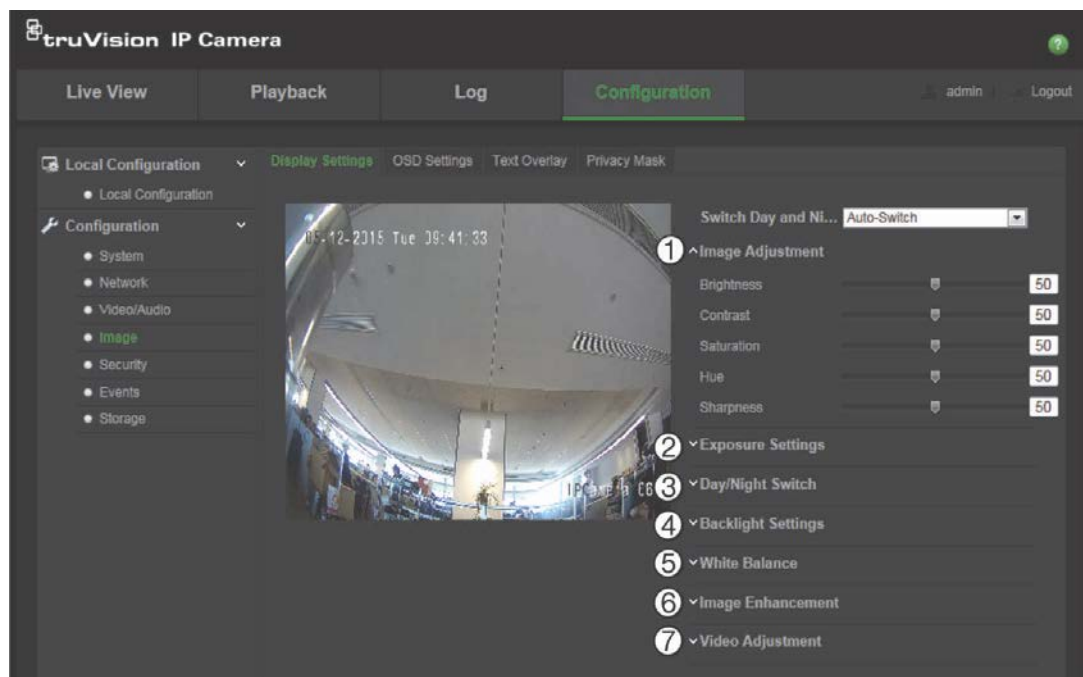


Table 6: Image parameters

Parameter	Description
1. Image Adjustment	
Brightness, Contrast, Saturation, Hue, Sharpness	Modifies the different elements of picture quality by adjusting the position of the values for each of parameter.
2. Exposure Settings	
Iris Mode	Only <i>Manual</i> is available.
Exposure Time	The exposure time controls the length of time that the aperture is open to let light into the camera through the lens. Select a higher value if the image is dark and a lower value to see fast moving object.

Parameter	Description
3. Day/Night Switch	
Day/Night Switch	<p>Defines whether the camera is in day or night mode. The day (color) option could be used, for example, if the camera is located indoors where light levels are always good.</p> <p>Options:</p> <p>Day: The camera is always in day mode.</p> <p>Night: The camera is always in night mode.</p> <p>Auto: The camera automatically detects which mode to use.</p> <p>Schedule: The camera switches between the day mode and the night mode according to the configured time period.</p> <p>Triggered by Alarm Input: The camera switches to the day mode or the night mode after the alarm is triggered.</p>
Sensitivity	If you choose <i>Auto Day/Night Switch</i> , select a sensitivity value from 0 to 7. The higher the value, the easier it is for the mode to switch.
Switch Time	Only available when Auto D/N switch mode is selected. The filtering time refers to the interval time between the day/night switch. You can set it between 5 and 120 s.
4. 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, and Center are selectable.
DWDR	When enabled, this feature (wide dynamic range) allows you to see details of objects in shadows or details of objects in bright areas of frames that have high contrast between light and dark areas.
5. White Balance	
White Balance	<p>White balance (WB) tells the camera what the color white looks like. Based on this information, the camera will then continue to display all colors correctly even when the color temperature of the scene changes such as from daylight to fluorescent lighting, for example. Select one of the options:</p> <p>AWB1: Apply for a small range of between 2500 to 9500K. For use in simple environments.</p> <p>Locked WB: Locks the WB to the current environment color temperature.</p> <p>Incandescent Lamp: For use with incandescent lighting.</p> <p>Warm Light Lamp: For use where the indoor light is warm.</p> <p>Natural Light: For use with natural light.</p> <p>Fluorescent Lamp: For use where there are fluorescent lamps installed near the camera.</p>
6. Image Enhancement	
Digital Noise Reduction	<p>Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance.</p> <p>Options include: ON or OFF.</p>
Noise Reduction Level	Set the level of noise reduction. Higher value has a stronger noise reduction. Default is 50.

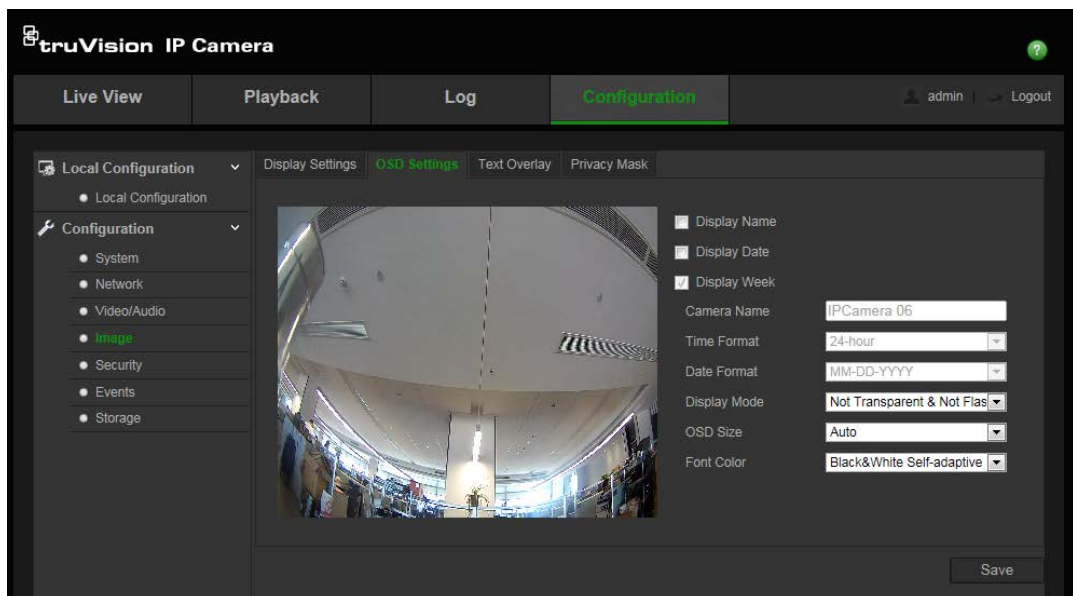
Parameter	Description
7. Video Adjustment	
Mirror	It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.
Video Standard	50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

OSD (On Screen Display)

In addition to the camera name, the camera also displays the system date and time on screen. You can also define how the text appears on screen.

To position the date/time and name on screen:

1. In the **Image** panel, click the **OSD Settings** tab to open its window.



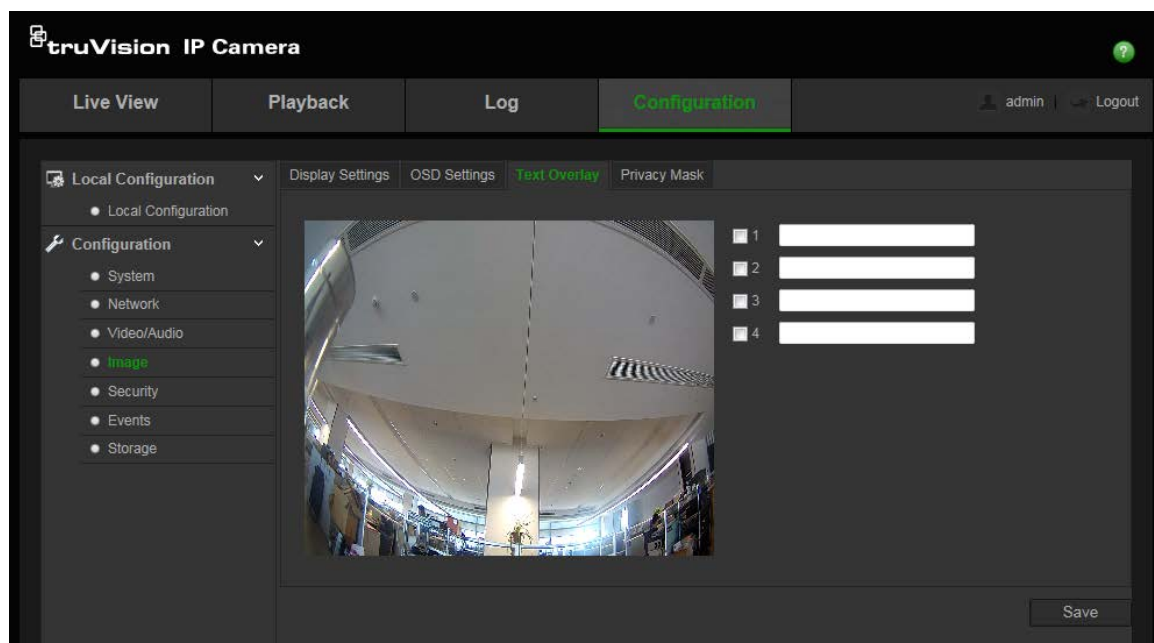
2. Check the **Display Name** box to display the camera's name on screen. You can modify the default name in the text box of **Camera Name**.
3. Check the **Display Date** box to display the date/time on screen.
4. Check the **Display Week** box to include the day of the week in the on-screen display.
5. In the **Camera Name** box, enter the camera name.
6. Select the time and date formats from the **Time format** and **Date format** list boxes.
7. Select a display mode for the camera from the **Display Mode** list box. Display modes include:
 - **Not transparent & Not Flashing**. The image is behind the text. This is default.

- **Not transparent & Flashing.** The image is behind the text. The text flashes on and off.
8. Select the OSD size that you want.
 9. Select the Font color that you want.
 10. Click **Save** to save changes.

Overlay text

You can add up to four lines of text on screen. This option can be used, for example, to display emergency contact details. Each text line can be positioned anywhere on screen. See Figure 7 below.

Figure 7: Text overlay menu



To add on-screen text:

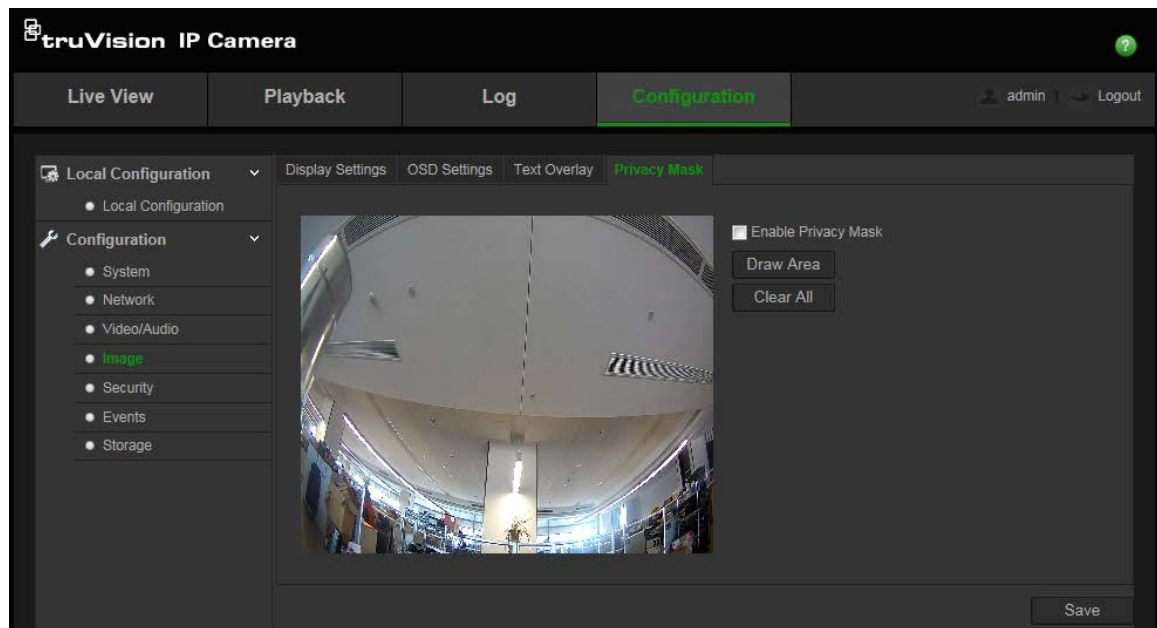
1. In the **Image** panel, click the **Text Overlay** tab to open its window.
2. Enable the check box for the first line of text.
3. Enter the text in the text box.
4. Use the mouse to click and drag the red text in the live view window to adjust the text overlay position.
5. Repeat steps 2 to 4 for each extra line of text, selecting the next string number.
6. Click **Save** to save changes.

Privacy masks

Privacy masks let you conceal sensitive areas (such as neighboring windows) to protect them from view on the monitor screen and in the recorded video. The masking appears as a blank area on screen. You can create up to four privacy masks per camera.

Note: There may be a small difference in size of the privacy mask area depending on whether local output or the web browser is used.

Figure 8: Privacy mask menu



To add privacy mask area:

1. In the **Image** panel, click the **Privacy Mask** tab to open its window.
2. Check the **Enable Privacy Mask**.
3. Click **Draw Area**.
4. Click and drag the mouse in the live video window to draw the mask area.

Note: You are allowed to draw up to four areas on the same image.

5. Click **Stop Drawing** to finish drawing, or click **Clear All** to clear all of the areas you set without saving them.
6. Click **Save** to save changes.

Motion detection alarms

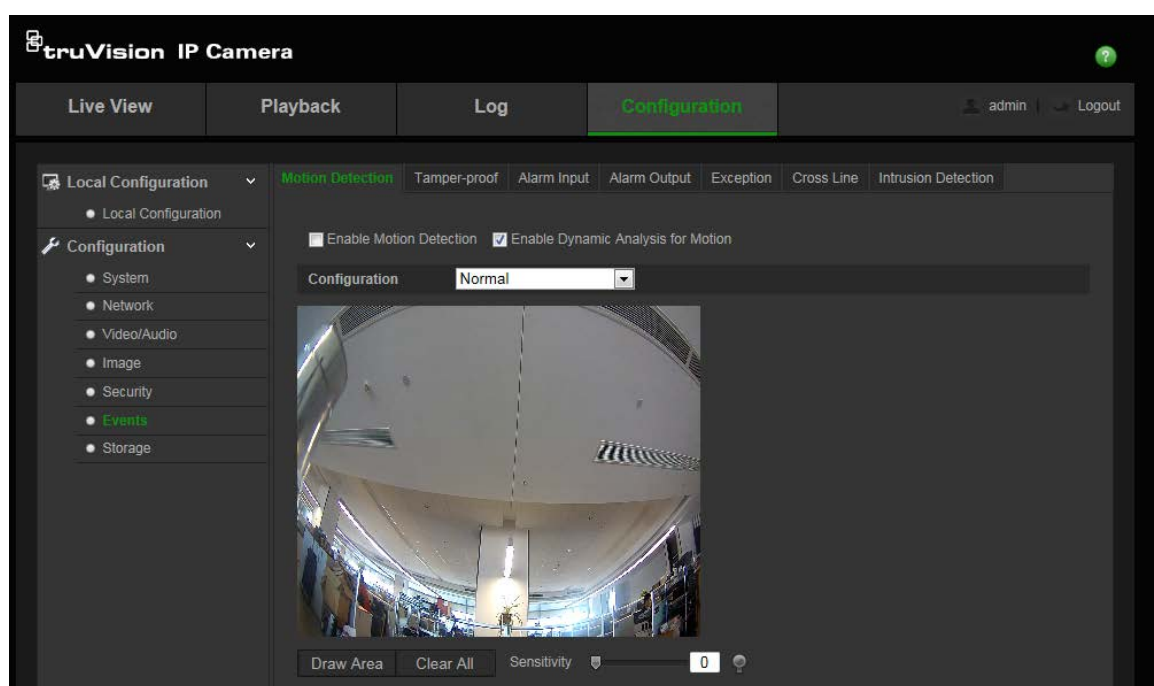
You can define motion detection alarms. A motion detection alarm refers to an alarm triggered when the camera detects motion. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

Select the level of sensitivity to motion as well as the target size so that only objects that could be of interest can trigger a motion recording. For example, the motion recording is triggered by the movement of a person but not that of a cat.

You can define the area on screen where the motion is detected, the level of sensitivity to motion, the schedule when the camera is sensitive to detecting motion as well as which methods are used to alert you to a motion detection alarm.

You can also enable dynamic analysis for motion. When there is motion, the area will be highlighted as green.

Figure 9: Motion detection menu



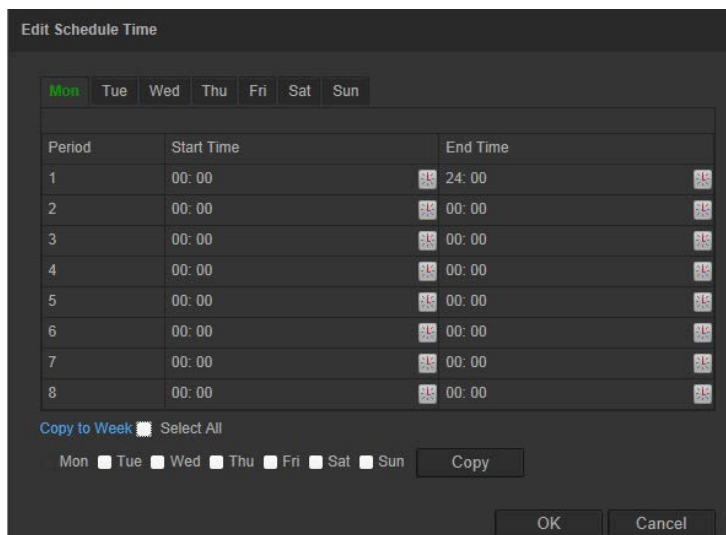
Defining a motion detection alarm requires the following tasks:


1. **Area Settings:** Define the on-screen area that can trigger a motion detection alarm and the detection sensitivity level.
2. **Arming Schedule:** Define the schedule during which the system detects motion.
3. **Linkage:** Specify the method of response to the alarm.

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

To set up motion detection as normal mode:

1. In the **Events** panel, click the **Motion Detection** tab to open its window.
2. Check the **Enable Motion Detection** box. Check **Enable Dynamic Analysis for Motion** if you want to see where has motion real-time.
Note: Select **Disable** for rules in local configuration menu if you don't want the detected objected displayed with the rectangles.
3. Select **Normal** mode from the drop down menu.
4. Click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.
5. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
6. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.
7. Click **Edit** to edit the arming schedule. See the picture below for the editing interface of the arming schedule.



8. Choose the day and click  to set the detailed time period. You can copy the schedule to other days.
9. Click **OK** to save changes.
10. Specify the linkage method when an event occurs. Check one or more response methods for the system when a motion detection alarm is triggered.

Notify Alarm Recipient

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

Send Email

Sends an email to a specified address when there is a motion detection alarm.

Note: You must configure email settings before check this option. See "To set up the Email parameters" on Page 22. If you want to send the event snapshot together with the email, you should check the Attached Snapshot option.

Upload Snapshot	Capture the image when an alarm is triggered and upload the picture to NAS or FTP server. Note: If you want to upload the snapshot to NAS, you must configure NAS settings, If you want to upload the snapshot to FTP, you must configure the FTP settings, please make sure the Upload type option is enabled.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs.

11. Click **Save** to save changes.

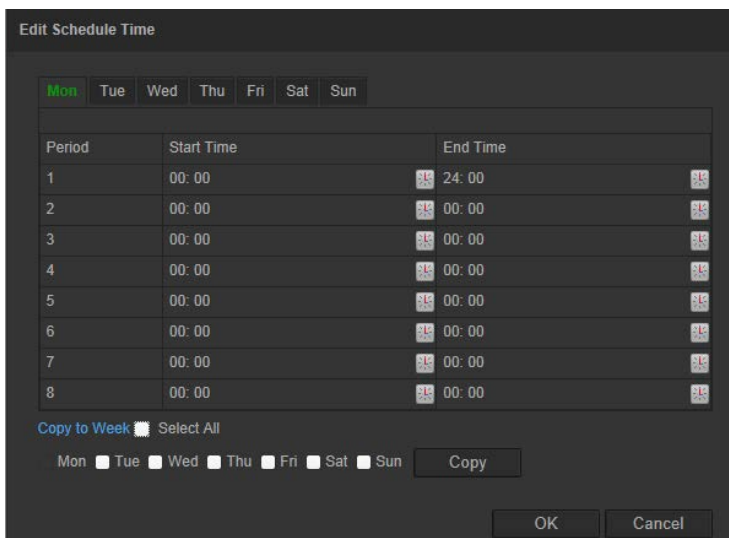
When you choose **Advanced** mode, you can set different sensitivity and proportion on different area. If you choose Auto-Switch or Schedule-Switch, you can also set different settings on day and night or different periods.


To set up motion detection as advanced mode:

1. In the **Events** panel, click the **Motion Detection** tab to open its window.
2. Check the **Enable Motion Detection** box. Check **Enable Dynamic Analysis for Motion** if you want to see where has motion real-time.

Note: Select Disable for rules in local configuration menu if you do not want the detected objected displayed with the rectangles.

3. Select **Advanced** from the drop down menu.
4. Select OFF, Auto-switch or Scheduled-switch.
5. Select **Area No.** and click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.
6. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
7. Move the **Sensitivity** and **Proportion of Object on Area** slider to set the sensitivity and proportion of the detection for different areas
8. Click **Edit** to edit the arming schedule. See the picture below for the editing interface of the arming schedule.



9. Choose the day and click  to set the detailed time period. You can copy the schedule to other days.
10. Click **OK** to save changes.
11. Specify the linkage method when an event occurs. Check one or more response methods for the system when a motion detection alarm is triggered.

Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm.
Upload Snapshot	Capture the image when an alarm is triggered and upload the picture to NAS or FTP server.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs.

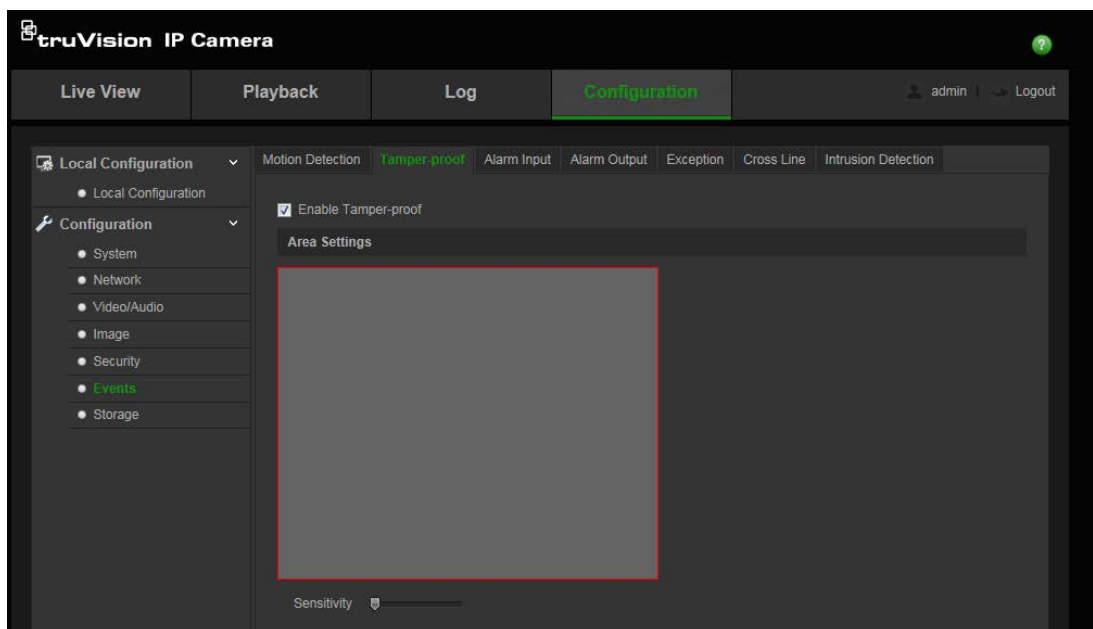
12. Click **Save** to save changes.

Tamper-proof alarms

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

To set up tamper-proof alarms:

1. In the **Events** panel, click the **Tamper-proof** tab to open its window.



2. Enable the **Enable Tamper-proof** box.
3. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.

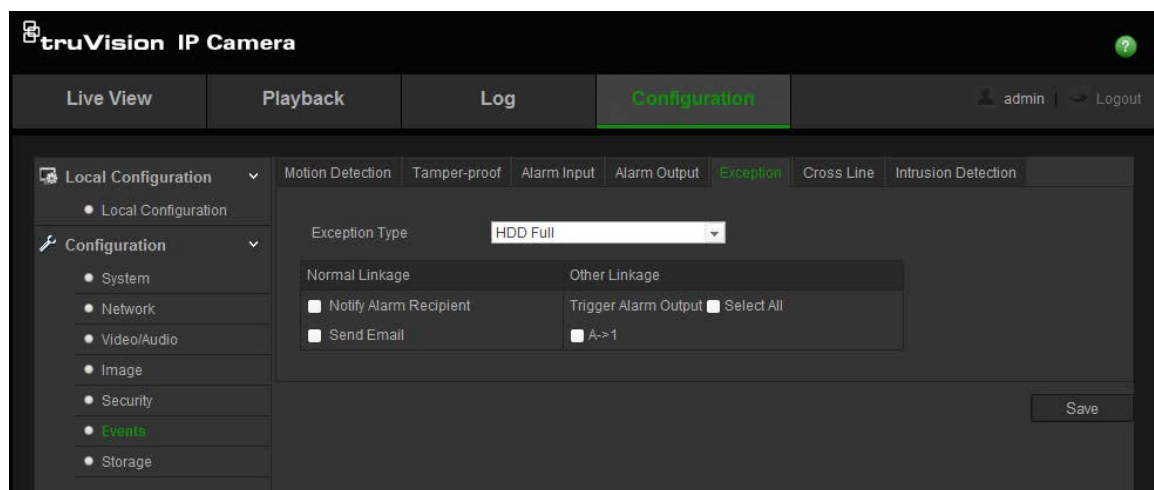
4. Click **Edit** to edit the arming schedule for tamper-proof alarms. The arming schedule configuration is the same as that for motion detection. See “Motion detection alarms” on page 31 for more information to set up motion detection.
5. Check the check box to select the linkage method taken for the tamper-proof.
6. Click **Save** to save changes.

Exception alarms

You can set up the camera to notify you when irregular events occur and how you should be notified. These exception alarms include:

- **HDD Full:** All recording space of NAS is full.
- **HDD Error:** Errors occurred while files were being written to the storage, no storage or storage had failed to initialize.
- **Network Disconnected:** Disconnected network cable.
- **IP Address Conflicted:** Conflict in IP address setting.
- **Invalid Login:** Wrong user ID or password used to login to the cameras.

Figure 10: Exception menu



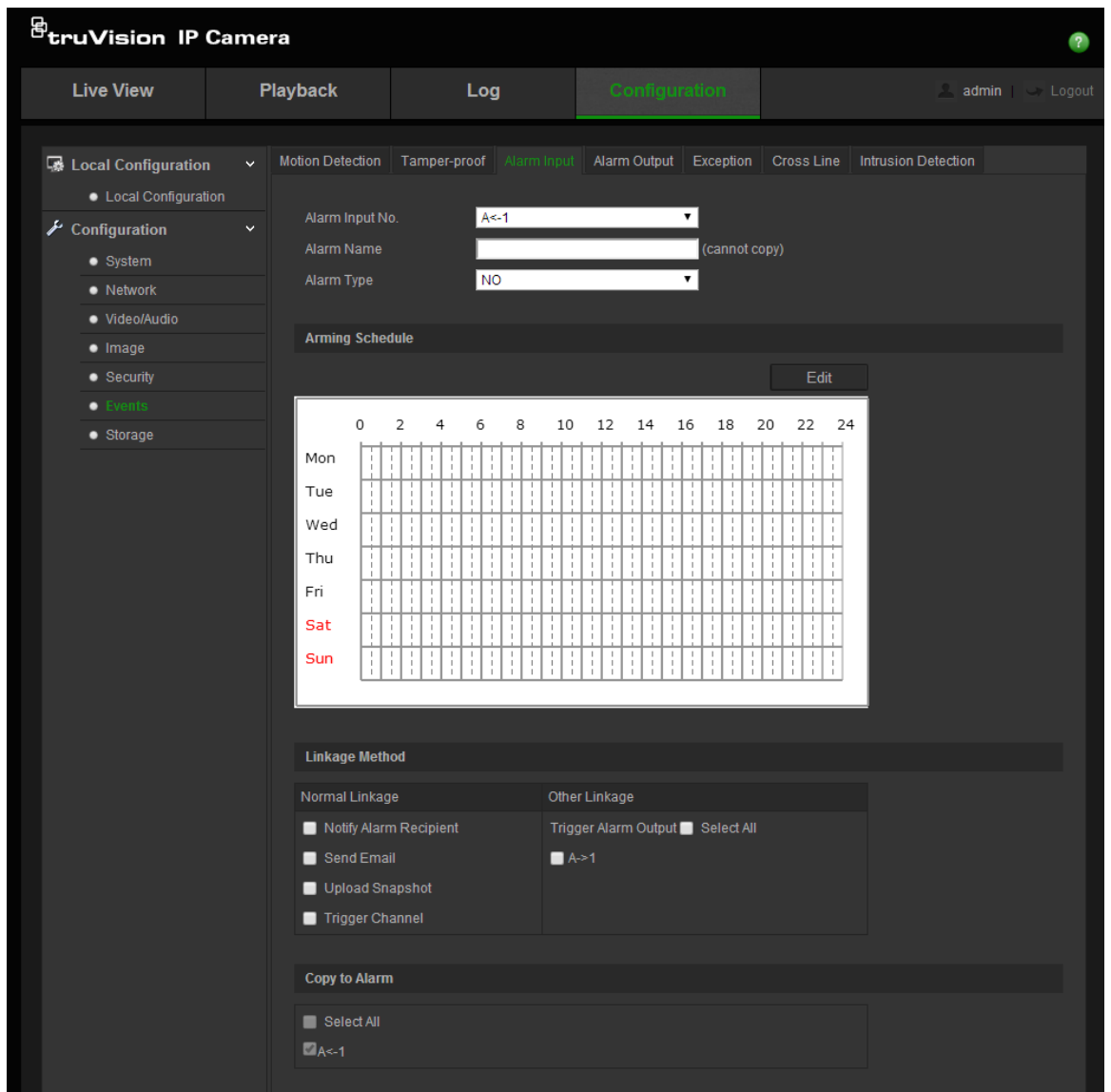
To define exception alarms:

1. In the **Events** panel, click the **Exception** tab to open its window.
2. Under **Notification Type**, select an exception alarm type from the drop-down list.
3. Check the check box to select the linkage method.
4. Click **Save** to save changes.

Alarm inputs and outputs

To define the external alarm input:

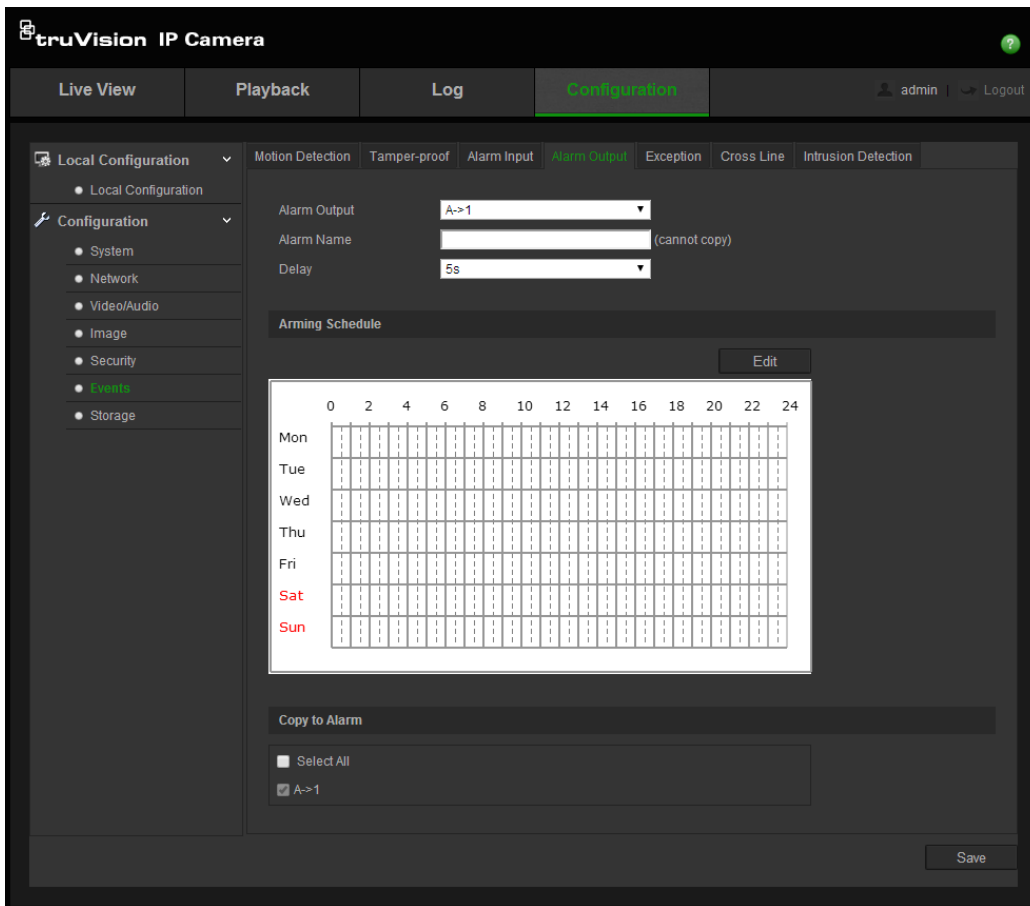
1. In the **Events** panel, click the **Alarm Input** tab to open its window.



2. Choose the **Alarm Input No.** and the **Alarm Type**. The alarm type can be NO (Normally Open) and NC (Normally Closed). Enter a name for the alarm input.
3. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 31 for more information to set up motion detection.
4. Check the check box to select the linkage method.
5. Click **Save** to save changes.

To define alarm output:

1. In the **Events** panel, click the **Alarm Output** tab to open its window.

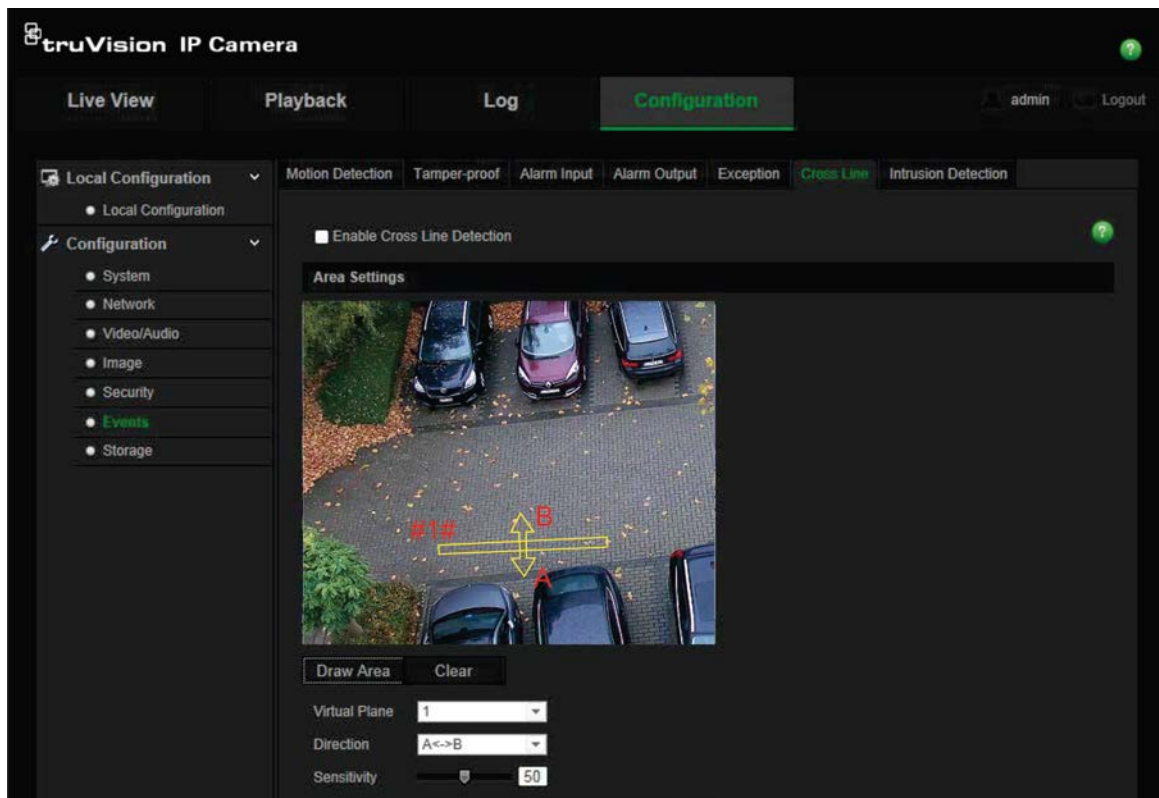


2. Select one alarm output channel from the **Alarm Output** drop-down list. You can also set a name for the alarm output.
3. The delay time can be set to 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
4. Click **Edit** to set the arming schedule for the alarm input. See “To set up motion detection” for more information.
5. Click **Save** to save changes.

Cross line detection

This function can be used for detecting people, vehicles and objects crossing a pre-defined line or an area. The line crossing direction can be set as bidirectional, that is, from left to right or from right to left. A series of linkage methods can be triggered if an object crossing behavior is detected.

Figure 11: Cross line detection menu



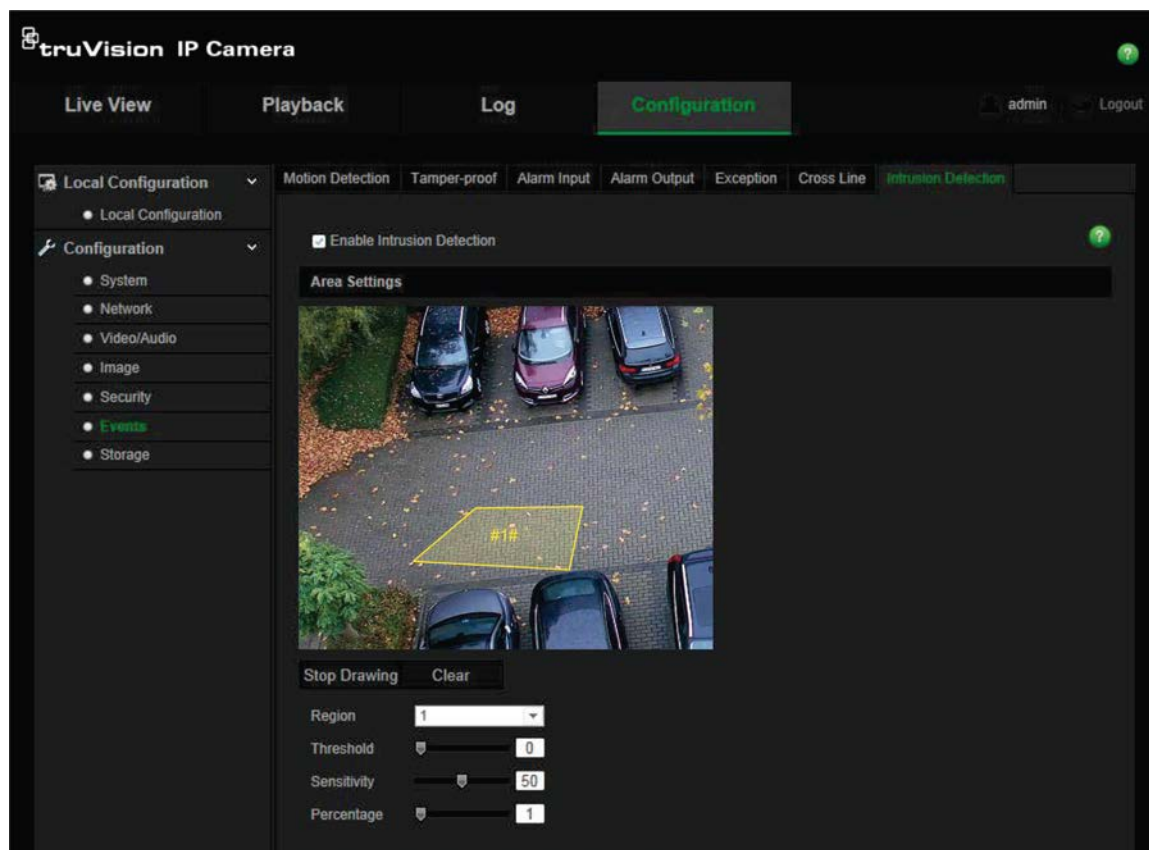
To define cross line detection:

1. In the **Events** panel, click the **Cross Line** tab to open its window.
2. Enable the **Enable Cross Line Detection** check box.
3. Click **Draw Area**. A crossing plane appears on the image.
4. Click on the line. You will see two red squares on each end. Drag one of the red squares to define the arming area.
Select the direction as A<->B, A ->B, or B->A from the drop down menu.
A<->B: Only the arrow on the B side is shown. Only objects crossing the configured line in both directions can be detected and alarms triggered.
A->B: Only objects crossing the configured line from the A side to the B side can be detected and alarms triggered.
B->A: Only objects crossing the configured line from the B side to the A side can be detected and alarms triggered.
5. Set the sensitivity level between 1 and 100.
6. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 31 for more information to set up motion detection.
7. Configure the linkage action.
8. Click **Save** to save changes.

Intrusion Detection

Intrusion detection allows you to set up an area in the surveillance scene. If someone enters the area a set of alarm action can be triggered.

Figure 12: Intrusion detection menu



To define intrusion detection:

1. In the **Events** panel, click the **Intrusion Detection** tab to open its window.
2. Enable the **Enable Intrusion Detection** check box.
3. Click **Draw Area**. Draw a rectangle on the image as a defense region. All lines of the rectangle drawn must connect end-to-end to each other. Only one area is supported. Click **Clear** to clear the area drawn.
4. Select the **Region** to be configured, and set the threshold, sensitivity and percentage trigger area of the region.

Threshold: Range [0-10 s]. This is the time threshold that the object loiters in the region. If you set the value as 0, an alarm is triggered immediately after the object enters the region.

Sensitivity: Range [1-100]. This is the sensitivity value that defines the size of the object that can trigger an alarm. When the sensitivity is high, a very small object can trigger the alarm.

Percentage: Range [1-100]. This is the percentage ratio of the in-region part of the object that can trigger an alarm. For example, when you set the percentage as 50%, half of the object entering the region will trigger the alarm.

5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 31 for more information to set up motion detection.
6. Configure the linkage action.
7. Click **Save** to save changes.

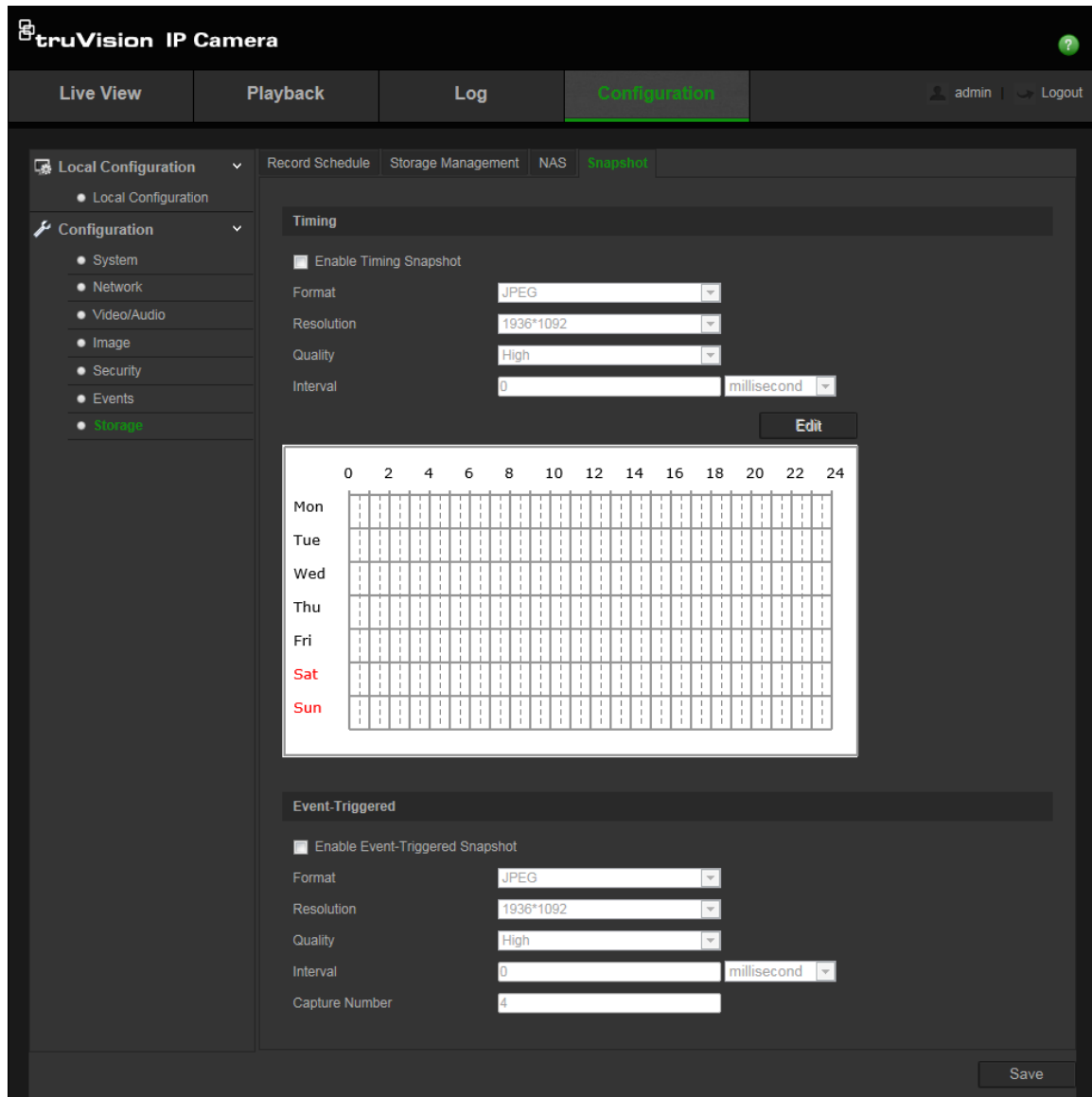
Snapshot parameters

You can configure scheduled snapshots and event-triggered snapshots. The captured snapshots can be stored in the SD card (if supported) or the NAS. You can also upload the snapshots to an FTP server.

You can set up the format, resolution and quality of the snapshots. The quality can be low, medium or high. See Figure 13 below.

If you want snapshots to be uploaded to the FTP, you should configure the FTP settings and check **Upload Type** in the Network > FTP menu. If you want snapshots to be uploaded to the storage, you should configure the storage settings to have normal NAS or SD card.

Figure 13: Snapshot menu



To set up scheduled snapshots:

1. In the **Storage** panel, click the **Snapshot** tab to open its window.
2. Enable **Enable Timing Snapshot**.
3. Select the desired format of the snapshot.
Note: Only JPEG is available.
4. Select the desired resolution of the snapshot.
Note: Only the resolution of the current main stream is available.
5. Select the desired quality of the snapshot: High, Medium or Low.
6. Enter the time interval between two snapshots. Select the unit of time from the dropdown list: milliseconds, seconds, minutes, hour, or day.
7. Set the schedule for when you want snapshots to be taken. Click **Edit** and desired schedule for each day of the week.

8. Click **Save** to save changes.

To set up event-triggered snapshots:

1. In the **Storage** panel, click the **Snapshot** tab to open its window.



The screenshot shows a configuration window titled "Event-Triggered". It contains the following settings:

- Enable Event-Triggered Snapshot
- Format: JPEG
- Resolution: 1936*1092
- Quality: High
- Interval: 0 milliseconds
- Capture Number: 4

2. Enable **Enable Event-Triggered Snapshot**.

3. Select the desired format, resolution and quality of the snapshot.

4. Enter the time interval between two snapshots. Select the unit of time from the dropdown list: milliseconds, seconds, minutes, hour, or day.

5. Under **Capture Number** enter the total number of snapshots that can be taken. If you set it as 4, the total number of the snapshot will be a multiple of four.

6. Click **Save** to save changes.

NAS settings

You can use a network storage system (NAS) to remotely store recordings

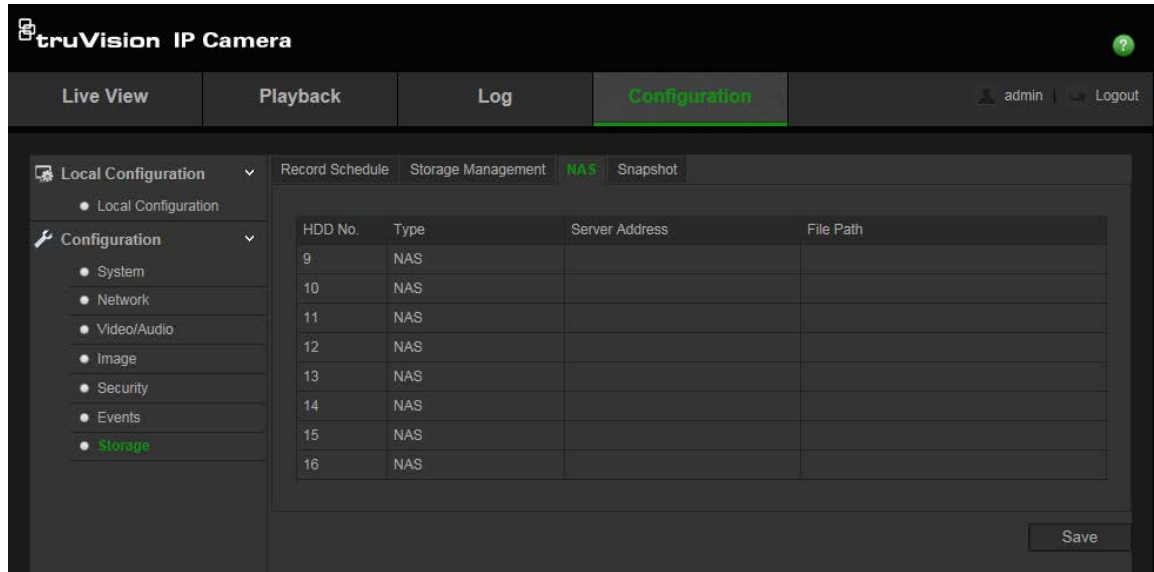
To configure record settings, please ensure that you have the network storage device within the network. The NAS disk should be available within the network and correctly configured to store the recorded files, log files, etc.

Notes:

1. Up to eight NAS disks can be connected to the camera.

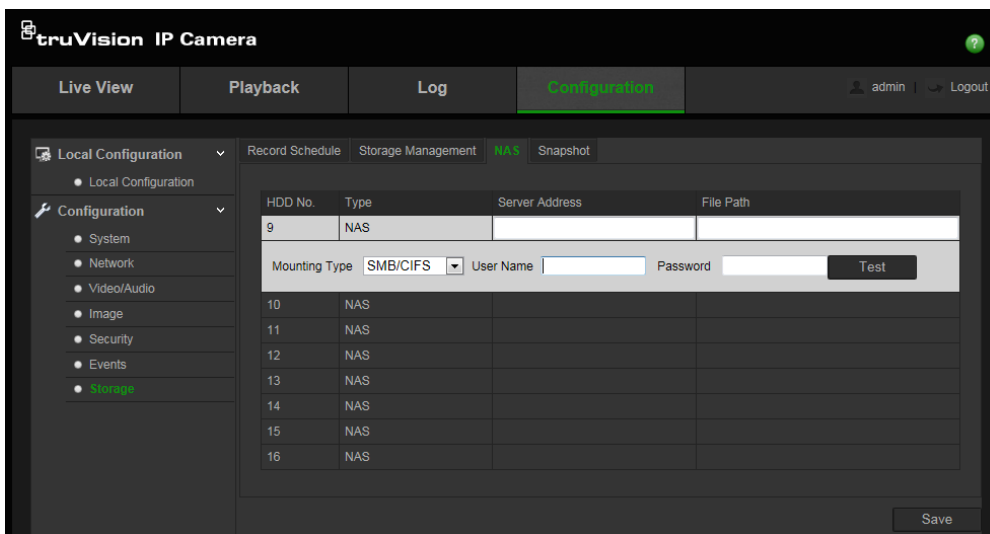
2. The recommended capacity of NAS should be between 9G and 2T as otherwise it may cause formatting failure.

Figure 14: NAS menu



To set up a NAS system:

1. In the **Storage** panel, click the **NAS** tab to open its window.
2. Enter the IP address of the network disk, and the NAS file path.
3. Configure the Mounting Type as NFS or SMB/CIFS. If you select SMB/CIFS, you can enter the user name and password.



4. Click **Save** to save changes.

Storage devices

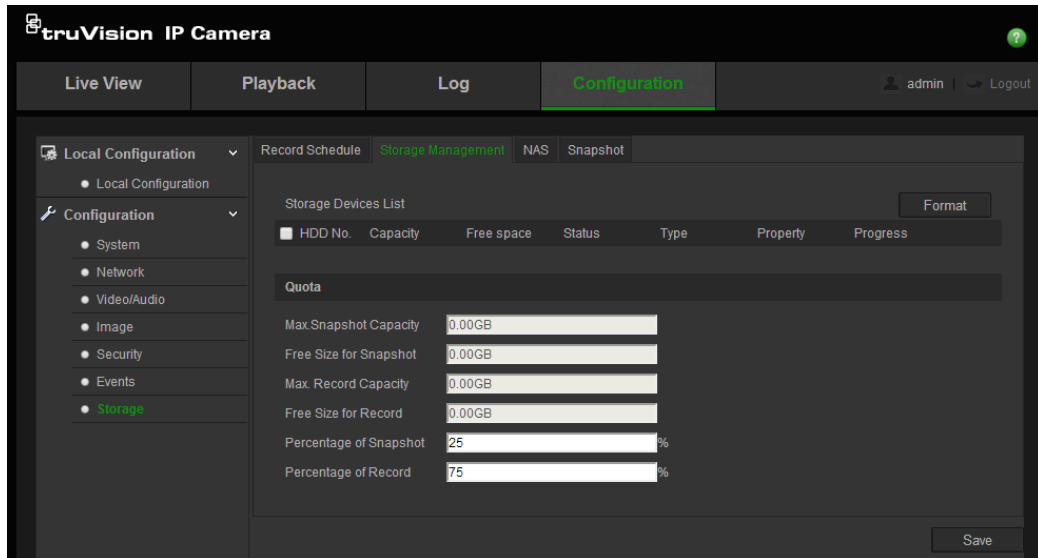
Use the storage management window to display the capacity, free space available and the working status of the NAS HDD and SD card in the camera. You can also format these storage devices.

Before formatting the storage device, stop all recording. Once formatting is completed, reboot the camera as otherwise the device will not function properly.

If *Overwrite* is enabled, the oldest files are overwritten when the storage becomes full.

To format the storage devices:

1. In the **Storage** panel, click the **Storage Management** tab to open its window.



2. Enable the **HDD Number** column to select the storage.
3. Define the quota percentage for snapshots and recordings by modifying the values for each in **Percentage of Snapshot** and **Percentage of Record**.
4. Click **Format**. A window appears to confirm your formatting permission.
5. Click **OK** to start formatting.

Recording schedule

You can define a recording schedule for the camera in the “Record Schedule” window. The recording is saved on to the SD card or NAS in the camera. The camera’s SD card provides a backup in case of network failure.

The selected recording schedule applies to all alarm types.

Pre-record time

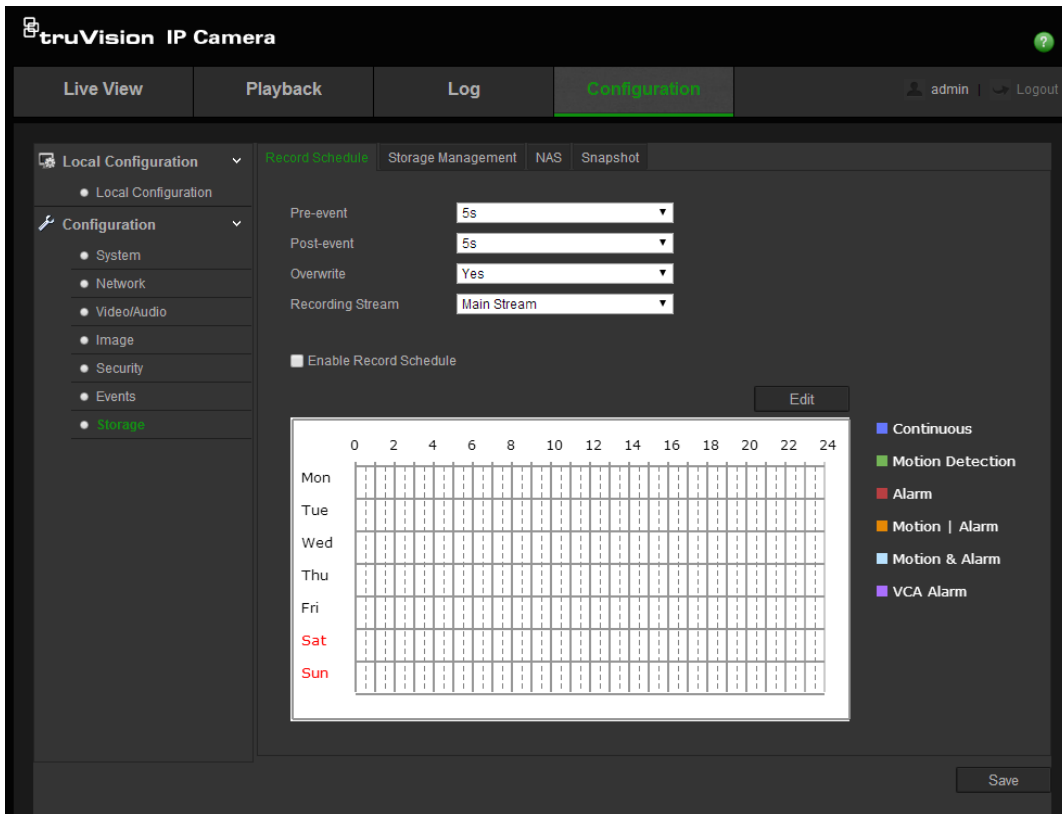
The pre-record time is set to start recording before the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record the event at 9:59:55. The pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s, or not limited.

Post- record time

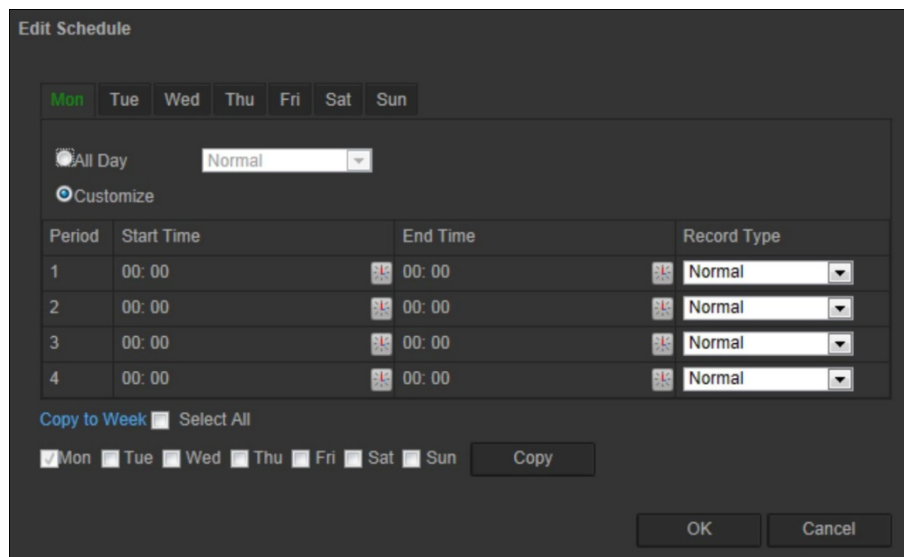
The post-record time is set to stop recording after the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05. The post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, or 10 min.

To set up a recording schedule:

1. In the **Storage** panel, click the **Record Schedule** tab to open its window.



2. Enable the **Enable Record Schedule** box to permit recording.
Note: To disable recording, deselect the option.
3. Click **Edit** to edit the recording schedule. The following window appears:



4. Select whether the recording will be for the whole week (**All Day** recording) or for specific days of the week.

If you have selected "All day", select one of the record types to record from the drop-down list box:

- **Normal:** This is continuous recording.
 - **Motion detection:** The video is recorded when the motion is detected.
 - **Alarm:** The video is recorded when the alarm is triggered via the external alarm input.
 - **Motion | Alarm:** The video is recorded when the external alarm is triggered or the motion is detected.
 - **Motion & Alarm:** The video is recorded when motion and alarms are triggered at the same time.
 - **Cross line:** Video is recorded when the pre-defined line on-screen is crossed.
 - **Intrusion Detection:** Video is recorded when an intrusion is detected.
 - **All Events:** Video is recorded when any events are detected.
5. If you selected “Customize”, click the day of the week required and then for period 1 set the start and end times during which you want the camera to begin and end recording.

From the drop-down list box, select one of the record types to record.

Repeat for additional periods in the day. Up to eight time periods can be selected.

Note: The eight time periods cannot overlap.

6. Set the recording periods for the other days of the week if required.
Click **Copy** to copy the recording periods to another day of the week.
7. Click **OK** and **Save** to save changes.

Note: If you set the record type to “Motion detection”, “Alarm”, “Cross Line” or “Intrusion detection” you must also define all the settings of the event and check the option **Trigger Channel** in order to trigger the recording.

Camera management

This chapter describes how to use the camera once it is installed and configured. The camera is accessed through a web browser.

User management

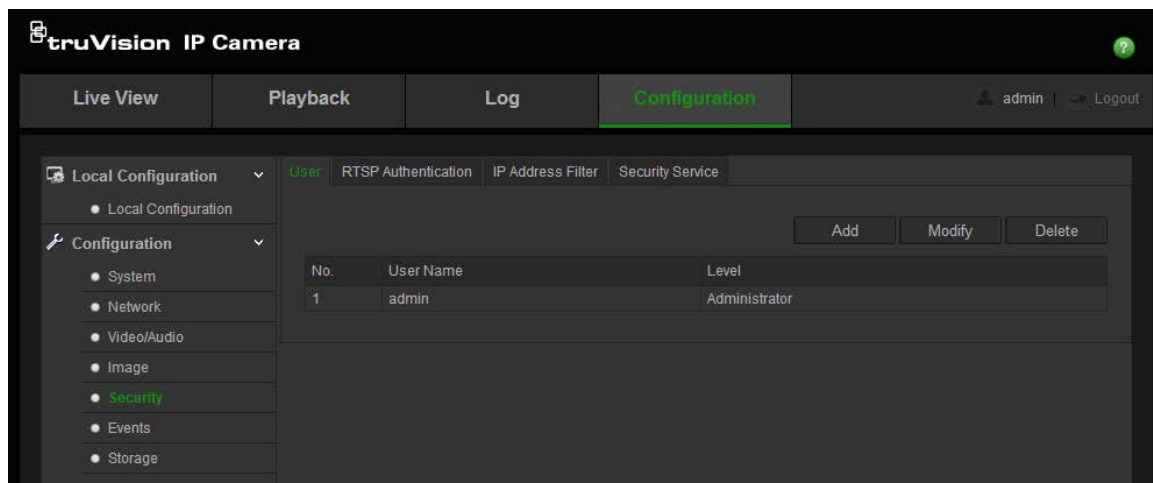
This section describes how to manage users. You can:

- Add or delete users
- Modify permission
- Modify passwords

Only the administrator can manage users. The administrator can create up to 31 individual users for the cameras listed in this manual. For TruVision IP open standard cameras, the administrator can create up to 15 individual users.

When new users are added to the list, the administrator can modify permissions and password of each user. See Figure 15 below.

Figure 15: User management window



Passwords limit access to the camera and the same password can be used by several users. When creating a new user, you must give the user a password. There is no default password provided for all users. Users can modify their passwords.

If you enter a password more than five times in a row, this user account will be locked for 10 minutes. If you use IE browser, it will be locked if you enter a password three times.

Note: Keep the admin password in a safe place. If you forget it, please contact technical support.

Types of users

A user's access privileges to the system are automatically defined by their user type. There are three types of user:

- **Admin:** This is the system administrator. The administrator can configure all settings. Only the administrator can create and delete user accounts. Admin cannot be deleted.
- **Operator:** This user can only change the configuration of his/her own account. An operator cannot create or delete other users.
- **Viewer:** This user has the permission to live view, play back and search logs. However, they cannot change any configuration settings.

Add and delete users

The administrator can create up to 15 users. Only the system administrator can create or delete users.

To add a user:

1. In the **Security** panel, click the **User** tab to open its window.
2. Select the **Add** button. The user management window appears.

3. Enter a user name.
4. Select the type of user from the drop-down list. The options are Viewer and Operator.
5. Assign the user a password. Passwords can have up to 16 alphanumeric characters. It will identify the complexity of the password as Low, Normal or High.
6. Assign permissions to users.
7. Click **OK** to save the settings.

To delete a user:

1. In the **Security** panel, click the **User** tab to open its window.
2. Select a user in the **User** tab.
3. Click the **Delete** button. A message box appears asking you to confirm that you want to delete this user. .

Note: Only the administrator can delete a user.

4. Click **OK** to delete the user.

Modify user information

You can easily change the information about a user such as their name, password and permissions.

To modify user information:

1. In the **Security** panel, click the **User** tab to open its window.
2. Select a user in the **User** tab.
3. Click the **Modify** button. The user management window appears
4. Change the information required.

Note: You can only change the password of admin.

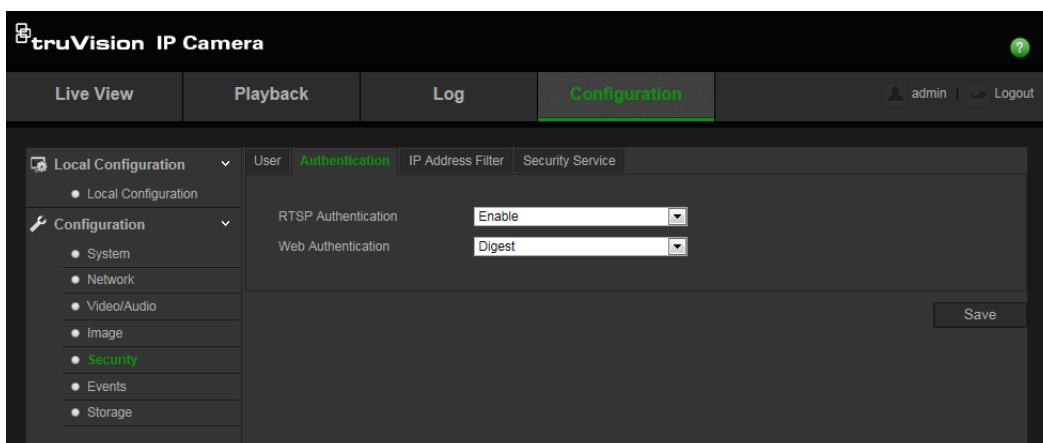
5. Click **OK** to save the changes.

Authentication

You can specifically secure the stream data of live view.

To define authentication parameters:

1. In the **Security** panel, click the **Authentication** tab to open its window.



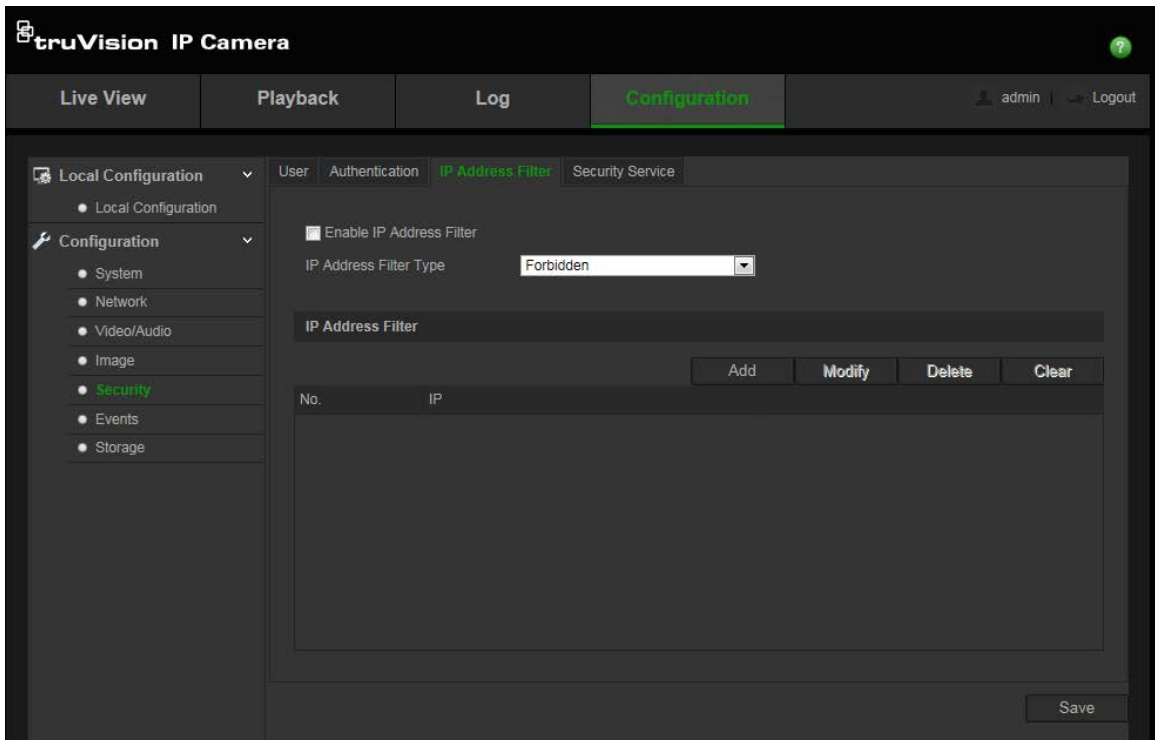
2. Under **RTSP Authentication** select **Enable** or **Disable** from the drop-down list to enable or disable the RTSP authentication.

Note: If "RTSP Authentication" is disabled, although the user has no permission for "Remote Live View", he can still see live view images.

3. Under **Web Authentication** select **Digest** or **Basic** from the drop-down list.
4. Click **Save** to save the changes.

IP address filter

This function makes it possible for access control.

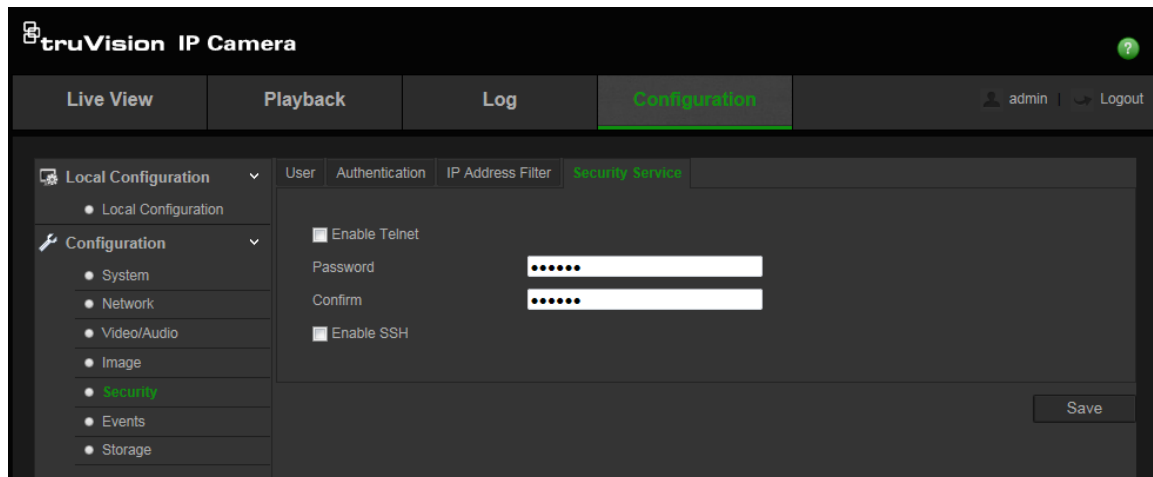


To define the IP address filter:

1. In the **Security** panel, click the **IP Address Filter** tab.
2. Enable **Enable IP Address Filter**.
3. Select the type of IP address filter from the drop-down list: **Forbidden** or **Allowed**.
4. Click **Add** to add an IP address.
-Or -
Click **Modify** or **Delete** to modify or delete the selected IP address.
-Or -
Click **Clear** to delete all the IP addresses.
5. Click **Save** to save the changes.

Defining the security service

To enable remote login, and improve the data communication security, the camera provides the security service for better user experience.



To define Telnet:

1. In the **Security** panel, click the **Security Service** tab to open its window.
2. Enable **Enable Telnet**.
3. Click **Save** to save the changes.

Note:

1. The Telnet user name is root as default and cannot be changed.
2. The default Telnet password is “ab12!”
3. The password should have least four characters with at least one letter and one number.

To define SSH:

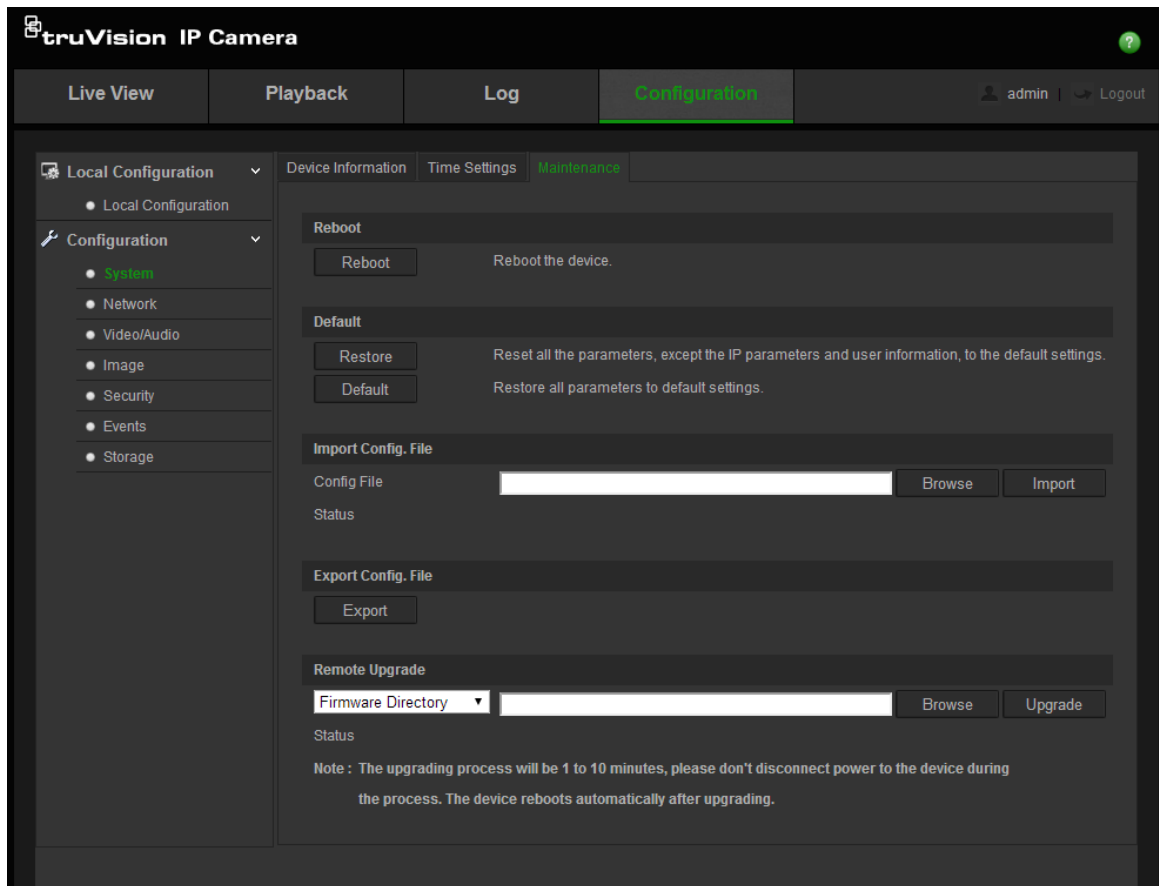
1. In the **Security** panel, select the **Security Service** tab to open its window.
2. Check the check box of **Enable SSH**.
3. Click **Save** to save the changes.

Restore default settings

Use the Default menu to restore default settings to the camera. There are two options available:

- **Restore:** Restore all the parameters, except the IP parameters, to the default settings.
- **Default:** Restore all the parameters to the default settings.

Note: If the video standard is changed, it will not be restored to its original setting when **Restore** or **Default** is used.



To restore default settings:

1. In the **System** panel, click the **Maintenance** tab to open its window.
2. Click either **Restore** or **Default**. A window showing user authentication appears.
3. Enter the admin password and click OK.
4. Click **OK** in the pop-up message box to confirm restoring operation.

Import/export a configuration file

The administrator can export and import configuration settings from the camera. This is useful if you want to copy the configuration settings to camera, or if you want to make a backup of the settings.

To import/export configuration file:

1. In the **System** panel, click the **Maintenance** tab to open its window.
2. Click **Browse** to select the local configuration file and then click **Import** to start importing configuration file.
3. Click **Export** and set the saving path to save the configuration file.

Upgrade firmware

The camera firmware is stored in the flash memory. Use the upgrade function to write the firmware file into the flash memory.

You need to upgrade firmware when it has become outdated. When you upgrade the firmware, all existing settings are unchanged. Only the new features are added with their default settings.

The camera will select the corresponding firmware file automatically. Cookies and data in the web browser are automatically deleted when the firmware is updated.

To upgrade firmware version:

1. Download on to your computer the latest firmware from our web site at:
www.interlogix.com/library
- Or -
www.utcssecurityproductspages.eu/videoupgrades/
2. When the firmware file is downloaded to your computer, extract the file to the desired destination.

Note: Do not save the file on your desktop.

3. In the **System** panel, click the **Maintenance** tab. Select the **Firmware** or **Firmware Directory** option. Then click the Browse button to locate latest firmware file on your computer.
 - **Firmware directory** – Locate the upgrading folder of Firmware files. The camera will choose the corresponding firmware file automatically.
 - **Firmware** – Locate the firmware file manually for the camera.

Note: Please select the correct firmware for the product models listed in “Introduction” on page 3.

4. Click **Update**. You will receive a prompt asking you to reboot the camera.
5. When the upgrade is finished, the device will reboot automatically. The browser will also be refreshed.

Reboot camera

The camera can be easily rebooted remotely.

To reboot the camera through the web browser:

1. In the **System** panel, click the **Maintenance** tab.
2. Click the **Reboot** button to reboot the device.
3. Click **OK** in the pop-up message box to confirm reboot operation.

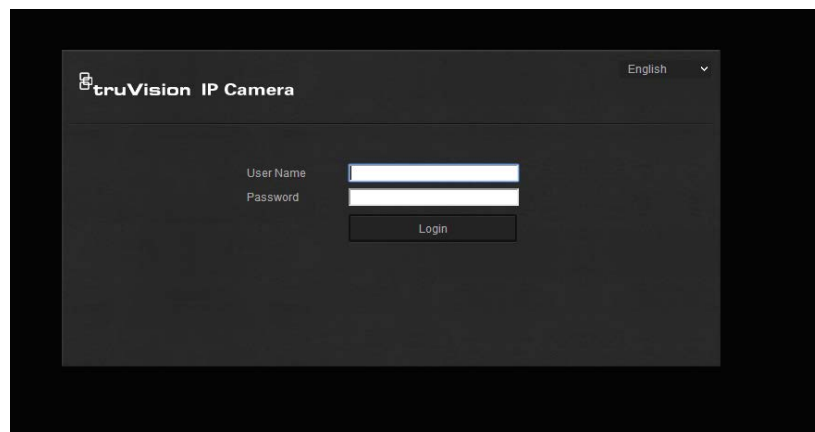
Camera operation

This chapter describes how to use the camera once it is installed and configured.

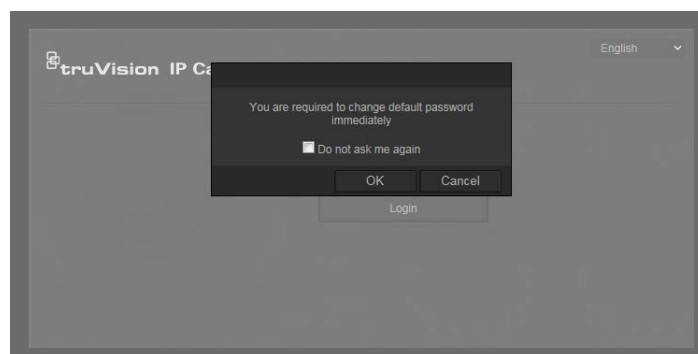
Logging on and off

You can easily log out of the camera browser window by clicking the Logout button on the menu toolbar. You will be asked each time to enter your user name and password when logging in.

Figure 16: Login dialog box





If you do not change the default password of admin, a message will always pop up requesting that you to do so.



Live view mode

Once logged in, click "Live View" on the menu toolbar to access live view mode. See Figure 1 on page 7 for the description of the interface.

-  **Start/stop live view:** You can stop and start live view by clicking the Start/stop live view button on the bottom of the window.
-  **Record:** You can record live video and stored it in the directory you have configured. In the live view window, click the **Record** button at the bottom of the window. To stop recording, click the button again.



Take a snapshot: You can take a snapshot of a scene when in live view. Simply click the **Capture** button located at the bottom of the window to save an image. The image is in JPEG format. Snapshots are saved on the hard drive.

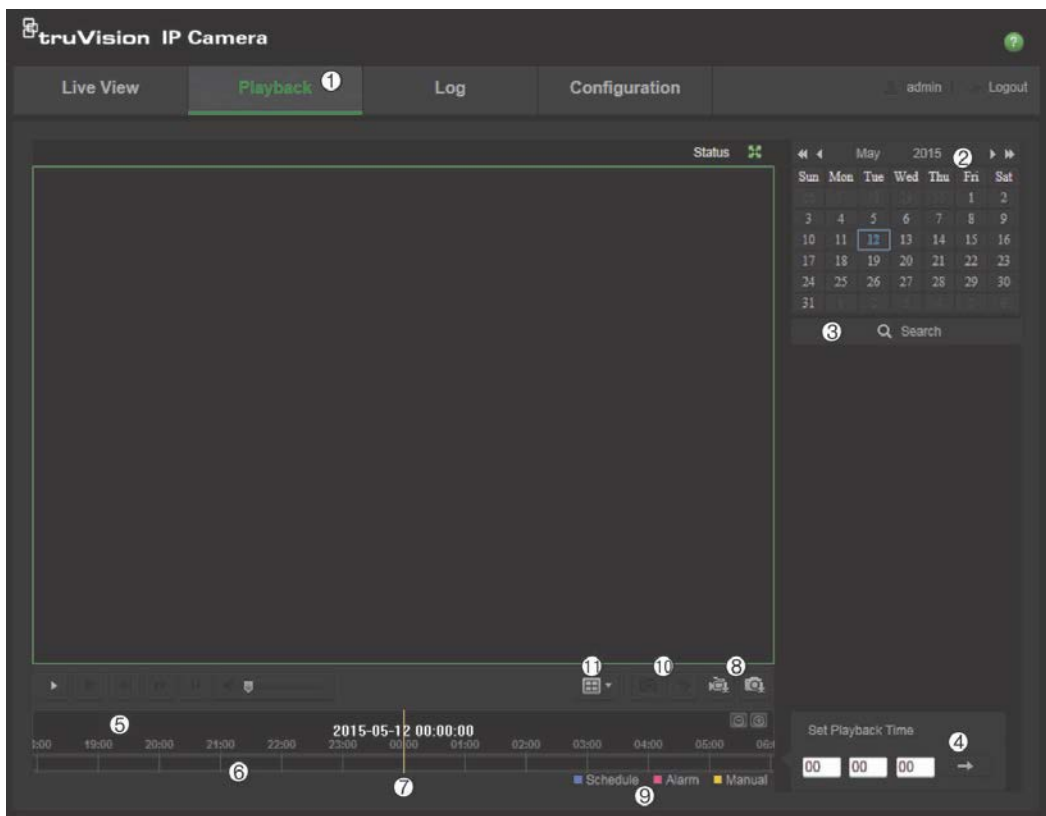
Playing back recorded video


You can easily search and play back recorded video in the playback interface.







Note: You must configure NAS or insert the SD card in the dome camera to be able to use the playback functions.

To search recorded video stored on the camera's storage device for playback, click **Playback** on the menu toolbar. The Playback window displays. See Figure 17 below.

Figure 17: Playback window




Name	Description
1. Playback button	Click to open the Playback window.
2. Search calendar	Click the day required to search.
3. Search	Start search.
4. Set playback time	Input the time and click  to locate the playback point.
5. Control playback	Click to control how the selected file is played back: play, stop, slow and fast forward playback.

Name	Description
6. Timeline bar	<p>The timeline bar displays the 24-hour period of the day being played back. It moves left (oldest) to right (newest). The bar is color-coded to display the type of recording.</p> <p>Click a location on the timeline to move the cursor to where you want playback to start. The timeline can also be scrolled to earlier or later periods for play back.</p> <p>Click   to zoom out/in the timeline bar.</p>
7. Time moment	Vertical bar shows where you are in the playback recording. The current time and date are also displayed.
8. Download functions	<p> Download video files.</p> <p> Download captured images.</p>
9. Recording type	<p>The color code displays the recording type. Recording types are schedule recording, alarms recording and manual recording.</p> <p>The recording type name is also displayed in the current status window.</p>
10. Archive functions	<p>Click these buttons for the following archive actions:</p> <p> Capture a snapshot image of the playback video.</p> <p> Start/Stop clipping video files.</p>
11. Playback mode	Specifies different playback modes.


To play back recorded video

1. Click **Playback** in the toolbar. Select the date and click the **Search** button. The searched video is displayed in the timeline.
2. Click **Play** to start playback. While playing back a video, the timeline bar displays the type and time of the recording. The timeline can be manually scrolled using the mouse.


Note: You must have playback permission to playback recorded images. See “Modify user information” on page 50 to archive recorded video files.

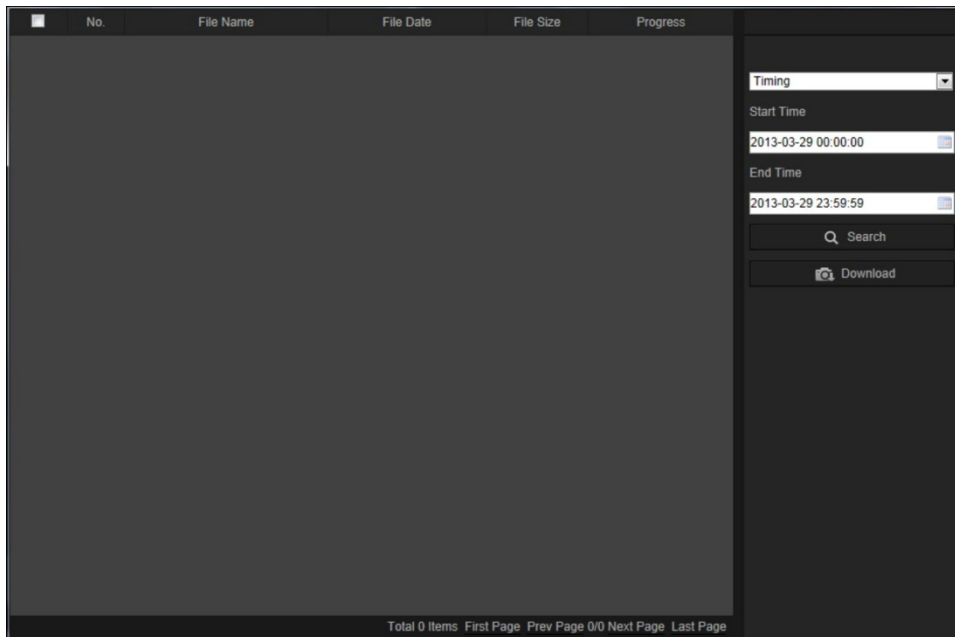
3. Select the date and click the **Search** button to search for the required recorded file.
4. Click  to search and download the video file.
5. In the pop-up window, check the box of the video file and click **Download** to download the video files.

To archive a recorded video segment during playback:

1. While playing back a recorded file, click  to start clipping. Click it again to stop clipping. A video segment is created.
2. Repeat step 1 to create additional segments. The video segments are saved on your computer.

To archive recorded snapshots:

1. Click  to open the snapshots search window.



2. Select the snapshot type as well as the start and end time.
3. Click **Search** to search for the snapshots.
4. Select the desired snapshots, and click **Download** to download them.

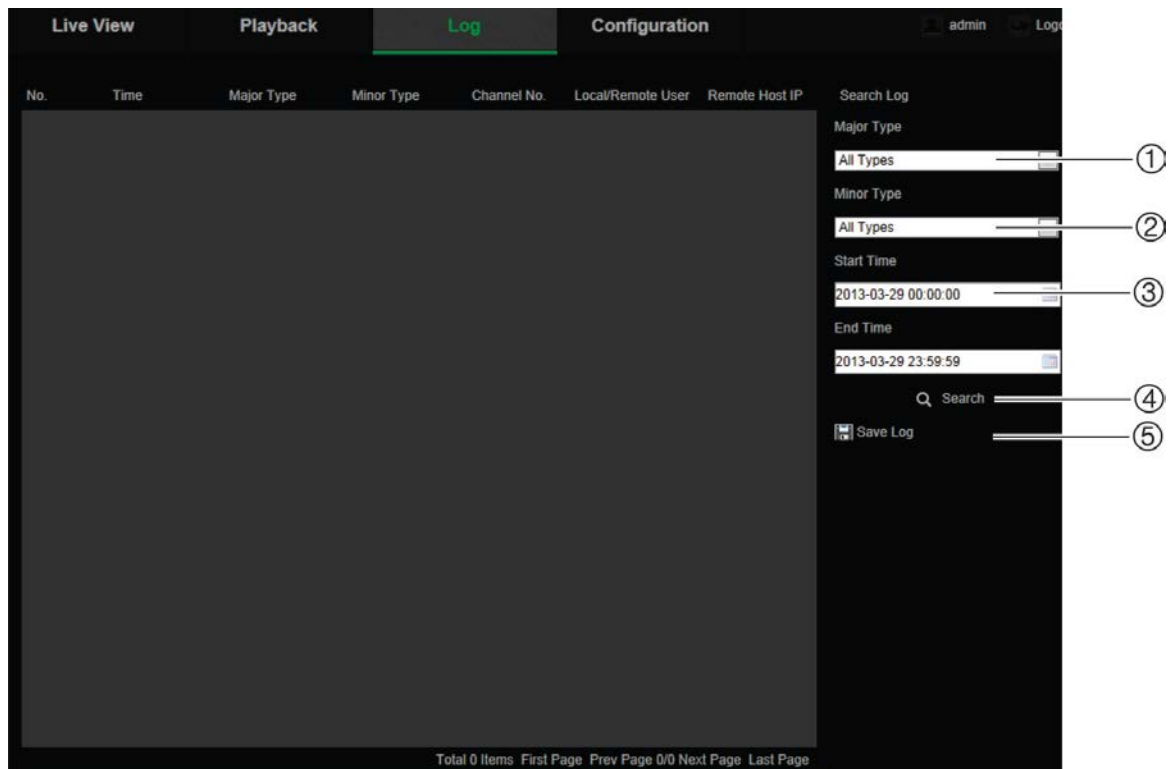
Searching event logs

You must configure NAS or insert a SD card in the camera to be able to use the log functions.

The number of event logs that can be stored on NAS or SD card depends on the capacity of the storage devices. When this capacity is reached, the system starts deleting older logs. To view logs stored on storage devices, click **Log** on the menu toolbar. The Log window appears. See Figure 18 on page 59.

Note: You must have view log access rights to search and view logs. See “Modify user information” on page 50 for more information.

Figure 18: Log window



1. Major Type
2. Minor Type
3. Start and end search time
4. Start search
5. Save searched logs

You can search for recorded logs by the following criteria:

Major type: There are three types of logs: Alarm, Exception, and Operation. You can also search **All Type**. See Table 7 below for their descriptions.

Minor type: Each major type has some minor types. See Table 7 below for their descriptions.

Date and Time: Logs can be searched by start and end recording time.

Table 7: Types of logs

Log type	Description of events included
Alarm	Alarm Input, Alarm output, Start Motion Detection, Stop Motion Detection, Start Tamper-proof, Stop Tamper-proof, Cross Line Detection Started, Cross Line Detection Stopped, Intrusion Detection Started, Intrusion Detection stopped
Exception	Invalid Login, HDD Full, HDD Error, Network Disconnected and IP Address Conflicted

Log type	Description of events included
Operation	Power On, Unexpected Shutdown, Remote Reboot, Remote Login, Remote Logout, Remote Configure parameters, Remote Upgrade, Remote Start Record, Remote Stop Record, Remote Initialize HDD, Remote Playback by File, Remote Playback by Time, Remote Export Config file, Remote import config file, Remote Get Parameters, Remote Get Working Status, Start Bidirectional Audio, Stop Bidirectional Audio, Remote Alarm Arming, Remote Alarm Disarming

To search logs:

1. Click **Log** in the menu toolbar to display the Log window.
2. In the Major Type and Minor Type drop-down list, select the desired option.
3. Select start and end time of the log.
4. Click **Search** to start your search. The results appear in the left window.

Index

A

- Alarm inputs
 - set up, 37
- Alarm outputs
 - set up, 37
- Alarm types
 - motion detection, 31
- Archived files
 - play back, 57
- Archiving files
 - snapshots, 57

B

- Bit rate, 24
- Brightness setup, 27

C

- Camera image
 - configuring, 27
- Camera name
 - display, 29
- Configuration file
 - import/export, 53
- Configuration settings, 8
- Contrast setup, 27

D

- Date format set up, 29
- DDNS parameters
 - set up, 15
- Default settings
 - restore, 52
- Display information on screen set up, 29

E

- Email parameters
 - set up, 21
- Events
 - search logs, 58

F

- Firmware upgrade, 54
- Frame rate, 24
- FTP parameters
 - set up, 17

H

- HDD
 - capacity, 44
 - formatting, 44
- HDD error alarm, 36

- HDD full alarm, 36

I

- I-frame interval, 24
- Illegal login alarm, 36
- IP address conflicted alarm, 36

L

- Live view parameters, 9
- Local camera parameters, 9
- Logging on and off, 55
- Logs
 - information type, 59
 - search logs, 58
 - view logs, 58

M

- Motion detection
 - configuring, 31
 - marking the detection areas, 33, 34

N

- NAS settings, 43
- Network, 36
- Network settings
 - set up, 12
- NTP synchronization, 10

P

- Passwords
 - modify, 50
- Playback
 - play back recorded files, 57
 - search recorded video, 56
- Port parameters
 - set up, 14
- Post-recording times
 - description, 45
- PPPoE parameters
 - set up, 15
- Pre-recording times
 - description, 45
- Privacy masks, 31

Q

- QoS parameters
 - set up, 17

R

- Reboot camera, 54
- Record file settings, 9
- Recording

- define recording schedule, 45
- parameters, 24

Resolution, 24

RTSP authentication, 50

S

Saturation setup, 27

SDHC card

- capacity, 44
- card full, 44
- formatting, 44
- free space available, 44

Sharpness setup, 27

Snapshot and clip settings, 9

Snapshots

- archive, 57
- set up, 41

SNMP parameters

- set up, 16

Stream type, 24

System time

- set up, 10

T

Tamper-proof alarms

- set up, 35

TCP/IP settings

- set up, 14

Text

- add extra lines of text on screen, 30

Text display on screen

- appearance, 29

Time format set up, 29

TruVision Device Finder, 6

U

UPnP parameters

- set up, 18, 20

User settings, 48

Users

- adding new users, 49
- deleting a user, 50
- modify a password, 50
- modify computer ID, 50
- types of users, 48

V

Video quality, 27

W

Web browser

- accessing the camera, 6
- overview of the interface, 6

Web browser security level

- checking, 4

