![interlogix - United Technologies]

TruVision Series 6 IP Camera Configuration Manual

Content

Index   65

Introduction

Product overview

This is the configuration manual for the following TruVision IP camera models:

- TVB-5601   (2MPX IP fixed lens bullet camera)
- TVB-5602   (4MPX IP fixed lens bullet camera)
- TVB-5603   (8MPX IP fixed lens bullet camera)

- TVB-5604   (2MPX IP motorized lens bullet camera)
- TVB-5605   (4MPX IP motorized lens bullet camera)
- TVB-5606   (8MPX IP motorized lens bullet camera)
- TVB-5604H   (2MPX IP motorized lens bullet camera)
- TVB-5605H   (4MPX IP motorized lens bullet camera)
- TVB-5606H   (8MPX IP motorized lens bullet camera)

- TVT-5601   (2MPX IP fixed lens turret camera, gray)
- TVT-5602   (2MPX IP fixed lens turret camera, white)
- TVT-5603   (2MPX IP fixed lens turret camera, black)
- TVT-5604   (4MPX IP fixed lens turret camera, gray)
- TVT-5605   (4MPX IP fixed lens turret camera, white)
- TVT-5606   (4MPX IP fixed lens turret camera, black)
- TVT-5607   (8MPX IP fixed lens turret camera, gray)

- TVT-5608   (2MPX IP motorized lens turret camera, gray)
- TVT-5609   (4MPX IP motorized lens turret camera, gray)
- TVT-5610   (4MPX IP motorized lens turret camera, white)
- TVT-5611   (8MPX IP motorized lens turret camera, gray)
- TVT-5608H   (2MPX IP motorized lens turret camera, gray)
- TVT-5609H   (4MPX IP motorized lens turret camera, gray)
- TVT-5610H   (4MPX IP motorized lens turret camera, white)
- TVT-5611H   (8MPX IP motorized lens turret camera, gray)

- TVD-5601   (2MPX IP fixed lens dome camera)
- TVD-5602   (4MPX IP fixed lens dome camera)

- TVD-5603   (8MPX IP fixed lens dome camera)

- TVD-5604   (2MPX IP motorized lens dome camera)
- TVD-5605   (4MPX IP motorized lens dome camera)
- TVD-5606   (8MPX IP motorized lens dome camera)
- TVD-5604H (2MPX IP motorized lens dome camera)
- TVD-5605H (4MPX IP motorized lens dome camera)
- TVD-5606H (8MPX IP motorized lens dome camera)

- TVW-5601   (2MPX IP fixed lens dome camera, 2.0 mm)
- TVW-5602   (2MPX IP fixed lens dome camera, gray)
- TVW-5603   (2MPX IP fixed lens dome camera, white)
- TVW-5604   (2MPX IP fixed lens dome camera, black)
- TVW-5605   (4MPX IP fixed lens dome camera, gray)

You can download the software and the following manuals from our web site:

- TruVision Series 6 IP Camera Installation Guide
- TruVision Series 6 IP Camera with Cable Harness Installation Guide

For contact information and to download the latest manuals, tools, and firmware, go to the web site of your region:

Americas:	interlogix.com
EMEA:	firesecurityproducts.com
	Manuals are available in several languages.
Australia/New Zealand:	utcfs.com.au

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 Internet Explorer

Internet Explorer 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, 8 and 10, 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.

Activating the camera

When you first start up the camera, the Activation window appears. You must define a high-security admin password before you can access the camera. There is no default password provided.

You can activate a password via a web browser and via TruVision Device Manager to find the IP address of the camera.

Activation via the web browser:

1. Power on the camera and connect the camera to the network.

2. Input the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface.


> **Note**:

> • The default IP address of the camera is 192.168.1.70.

> • For the camera to enable DHCP by default, you must activate the camera via TruVision Device Manager. Please refer to the following section, "Activation via TruVision Device Manager".

3. Enter the password in the password field.

Note: A valid password range must be between 8 and 16 characters. You can use a combination of numbers, lower and upper case letters, and special characters: _ - , . * & @ / $? Space. The password must contain characters from at least two of these groups. We also recommend that you reset your password regularly. For high security systems, it is particularly recommended to reset the password monthly or weekly for better protection.

4. Confirm the password.

5. Click **OK** to save the password and enter the live view interface.

Activation via TruVision Device Manager:

1. Run the *TruVision Device Manager* to search for online devices.

2. Select the device status from the device list, and select the inactive device.
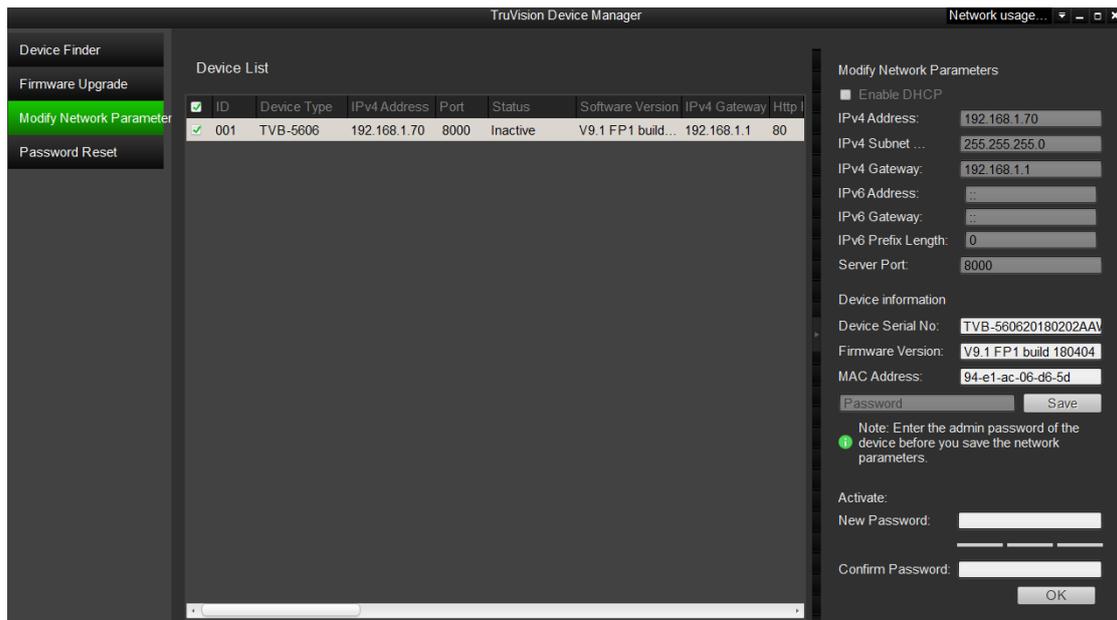
3. Enter the password in the password field, and confirm it.

Note: A valid password range must be between 8 and 16 characters. You can use a combination of numbers, lower and upper case letters, and special characters: _ - , . * & @ / $? Space. The password must contain characters from at least two of these groups. We also recommend that you reset your password regularly. For high security systems, it is particularly recommended to reset the password monthly or weekly for better protection.

4. Click **OK** to save the password.

   A pop-up window appears to confirm the activation. If activation fails, confirm that the password meets the requirements and try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or selecting the check box of Enable DHCP.

Modify Network Parameters
☐ Enable DHCP
IPv4 Address: 192.168.1.70
IPv4 Subnet Mask: 255.255.255.0
IPv4 Gateway: 192.168.1.1
IPv6 Address: ::
IPv6 Gateway: ::
IPv6 Prefix Length: 0
Server Port: 8000

6. Input the password and click the **Save** button to activate your IP address modification.

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 below.

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 window: Live view shown

	Name	Description
1.	Live view	Click to view live video.
2.	Playback	Click to play back video.
3.	Picture	Click to search snapshots.

	Name	Description
4.	Log	Click to search for event logs. There are three main types: Alarm, Exception, and Operation.
5.	Configuration	Click to display the configuration window for setting up the camera.
6.	Viewer	View live video. Time, date and camera name are displayed here.
7.	Admin	Displays current user logged on.
8.	Help	Click to find function.
9.	Logout	Click to log out from the system. This can be done at any time.
10.	Live view toolbar	▶/■ Click to start/stop live view
		📷 Click to manually capture the snapshot
		🎥 Click to manually start/stop recording
		🔍 Click to start/stop digital zoom function
		Live view with main stream or substream
		Click to select the third-party plug-in
		🎤 Turn on/off microphone
		🔊 ▼ Audio on and adjust Volume/Mute
		Manual alarm
		4:3 The window size is 4:3
		16:9 The window size is 16:9
		✕ The original window size
		Self-adaptive window size

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 menus in the configuration panel:

- Local configuration
- Camera Configuration

Configuration menu overview

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

Figure 2: Configuration window (Basic Information tab selected)
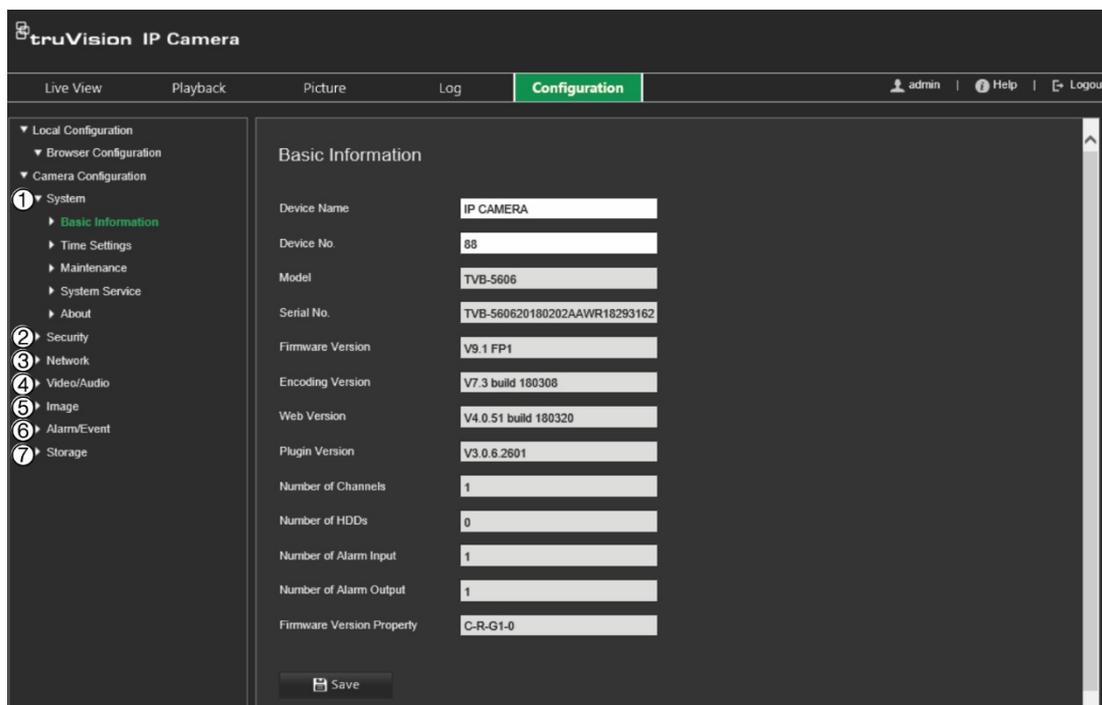
Configuration menus		Description
1.	System	Defines device basic information including SN and the current firmware version, time settings, maintenance, and serial port parameters. See "System time" on page 13 for further information.
		Device No.: It can be used for the SNMP or keypad to differentiate individual devices.
		Firmware Version Property:
		First Character: B-Baseline, C-Customization.
		Second Character: R-Release, F-Fault
		Third Character: G1-Platform
		Fourth Character: 0- Reserved.
2.	Security	Defines who can use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and telnet access.
3.	Network	Defines the network parameters required to access the camera over the internet. See "Network settings" on page 14 for further information on the setup.
4.	Video/Audio	Defines recording parameters.
5.	Image	Defines the image parameters, OSD settings, overlay text, and privacy mask. See "Video image" on page 25 for further information on the setup.
6	Alarm/Event	Defines motion detection, video tampering, alarm input/output, and exception. See "Alarm inputs and outputs" on page 38. Defines face detection, intrusion detection, cross line.
7.	Storage	Defines recording schedule, storage management, NAS configuration and snapshot.

Local configuration

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

Figure 3: Example of the Local configuration window
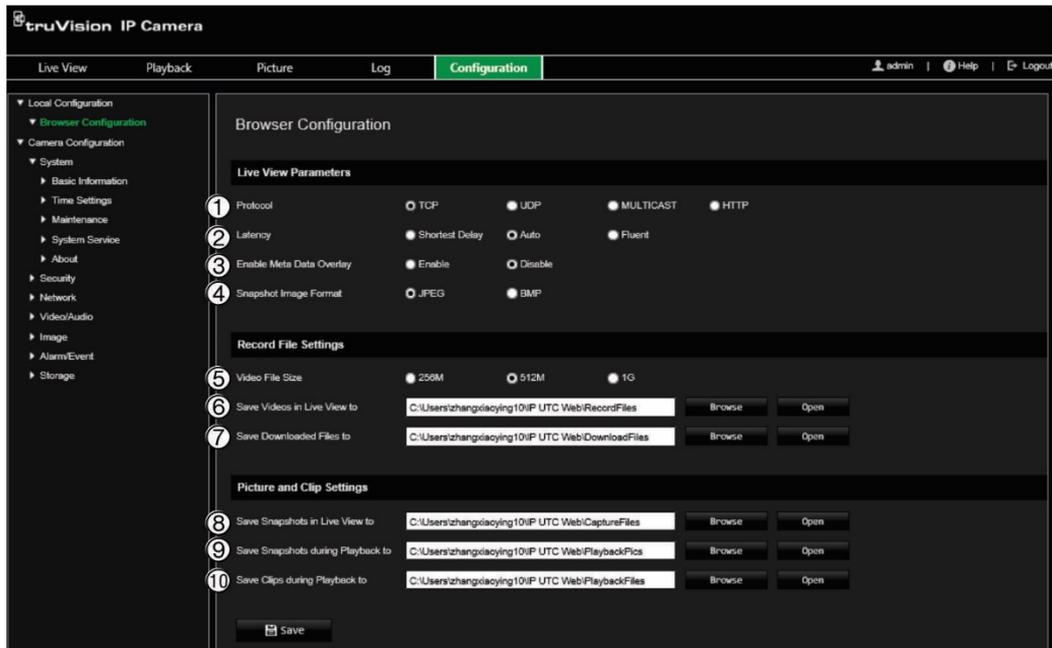
Parameters	Description
Live View Parameters	
1. Protocol	Specify the network protocol used. Options include: TCP, UDP, MULTICAST and HTTP.
2. Latency	Specify the transmission speed. Options include: Shortest Delay, Auto or Fluent.
3. Enable Meta Data Overlay	It refers to the rules on your local browser. 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. Snapshot Image Format	Choose the image format for a snapshot: JPEG or BMP.
Record File Settings	
5. Video File Size	Specify the maximum file size. Options include: 256 MB, 512 MB and 1G.
6. Save Videos in Live View to	Specify the directory for recorded files.
7. Save Downloaded Files to	Specify the directory for downloaded files.
Snapshot and Clip Settings	
8. Save Snapshots In Live View To	Specify the directory for saving snapshots in live view mode.
9. Save Snapshots during Playback To	Specify the directory for saving snapshots in playback mode.
10. Save Clips during Playback to	Specify 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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **System** > **Time Settings**.

2. From the **Time Zone** drop-down list, select the time zone that is the closest to the camera's location.

3. Under **Time Settings**, select one of the options for setting the time and date:

   Synchronize with an NTP server: Select 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 select the **Sync with computer time** check box to synchronize the time of the camera with the time of your computer.

4. Select **Enable DST** to enable the DST (Daylight Savings Time) 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" menu to define the network settings. See Figure 2 below for further information.

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

Menu tabs	Description
1. TCP/IP	**NIC Type:** Enter the NIC type. Default is Auto. Other options include: 10M Half-dup, 10M Full-dup, 100M Half-dup and 100M Full-dup.
	DHCP: Enable to automatically obtain an IP address and other network settings from that server.
	IPv4 Address: Enter the IPv4 address of the camera.
	IPv4 Subnet Mask: Enter the IPv4 subnet mask.
	IPv4 Default Gateway: Enter the IPv4 gateway IP address.
	IPv6 Mode: Enter the IPv6 mode: Manual, DHCP or Router Advertisement.
	IPv6 Address: Enter the IPv6 address of the camera.
	IPv6 Subnet Prefix Length: Enter the IPv6 prefix length.
	IPv6 Default Gateway: Enter the IPv6 gateway IP address.
	Mac Address: Enter the MAC address of the devices.
	MTU: Enter the valid value range of MTU. Default is 1500.
	Multicast Address: Enter 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.

Menu tabs	Description
	Enable Multicast Discovery: Enable the automatic detection of the online network camera via private multicast protocol in the LAN. **DNS server:** Specify the DNS server for your network.
2. DDNS	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. Specify DynDNS, No-IP or ezDDNS. **DynDNS (Dynamic DNS**): Manually create your own host name. You will first need to create a user account using the hosting web site, DynDDNS.org. **No-IP**: Enter the address of the NO-IP, host name for your camera, the port number, your user name and password. **ezDDNS**: Activate the DDNS auto-detection function to set up a dynamic IP address. The server is set up to assign an available host name to your recorder. See page 16 for setup information.
3. PPPoE	Retrieve a dynamic IP address. See page 16 for setup information.
4. Port	**HTTP Port:** The HTTP port is used for remote internet browser access. Enter the port used for the Internet Explorer (IE) browser. Default value is 80. **RTSP Port:** RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. Enter the RTSP port value. The default port number is 554. **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. **Server Port:** This is used for remote client software access. Enter the server port value. The default port number is 8000. **Alarm Host IP**: Specify the IP address of the alarm host. **Alarm Host Port**: Specify the port of the alarm host. See page 16 for setup information.
5. NAT	NAT (Network Address Translation) is used for network connection. Select the port mapping mode: auto or manual. See page 17 for setup information.
6. SNMP	SNMP is a protocol for managing devices on networks. Enable SNMP to get the camera status and parameter related information. See page 17 for setup information.
7. FTP	Enter the FTP address and folder to which snapshots from the camera can be uploaded. See page 17 for setup information.
8. Email	Enter the email address to which messages are sent when an alarm occurs. See page 18 for setup information.
9. HTTPS	Specify the authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.
10. QoS	QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending. Enable the option in order to solve network delay and network congestion by configuring the priority of data sending. See page 20 for setup information.

Menu tabs	Description
11. 802.1.X	When the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network. See page 17 for setup information.
12. Integration protocol	If you need to access to the camera through the third party platform, you can enable STD-CGI function. The ONVIF protocol is enabled by default. If you do not need to access the camera through the third party platform, please deselect the checkbox *Enable ONVIF*.

To define the TCP/IP parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **TCP/IP**.

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, select **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 DDNS parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **DDNS**.

2. Select **Enable DDNS** to enable this feature.

3. Select **DDNS Type**. Three options are available: DynDNS, ezDDNS and NO-IP. Select one of the options:

   • **DynDNS:** Enter the DNSS server address, members.ddns.org (which is used to notify DDNS about changes to your IP address), the host name for your camera, the port number (443 (HTTPS)), and your user name and password used to log into your DDNS account. The domain name displayed under "Host Name" is that which you created on the DynDNS web site.

   • **ezDDNS**: Enter the host name. It will automatically register it online. You can define a host name for the camera. Make sure you entered a valid DNS server in the network settings and have the necessary ports forwarded in the router (HTTP, Server port, RSTP port).

   • **NO-IP:** Enter the address of the NO-IP, host name for your camera, the port number, your user name and password.

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

To define the PPPoE parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **PPPoE**.

2. Select **Enable PPPoE** to enable this feature.

3. Enter the user name, password, and confirm the password for PPPoE access.

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

To define the port parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **Port**.

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

   HTTP Port: The default port number is 80. 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. Enter the IP address and port if you want to upload the alarm information to the remote alarm host. Also select the **Notify Alarm Recipient** option in the normal Linkage of each event page.

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

To set up the NAT parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **NAT**.

2. Select 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.

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

To define the SNMP parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **SNMP**.

2. Select the corresponding version of SNMP: v1 or v2c.

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 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 surveillance center. The SNMP version you select should be the same as that of the SNMP software.

To define the FTP parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **FTP**.

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

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

   Directory: In the *Directory Structure* field, select the root directory, main directory and subdirectory. When the main directory is selected, you can use Device Name, Device Number, or Device IP for the name of the directory. When the subdirectory is selected, you can use the Camera Name or Camera No. as the name of the directory.

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

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

To set up the email parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **Email**.
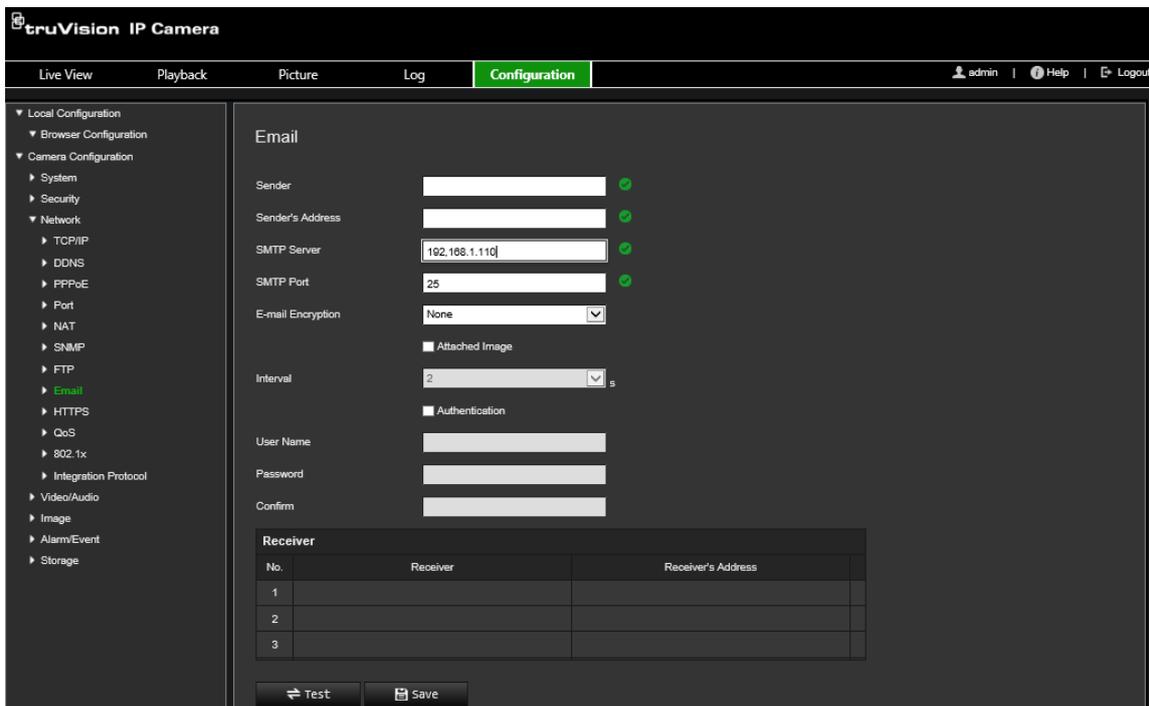
2. Configure the following settings:

   Sender: The name of the email sender.

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

   SMTP Server: The SMTP Server, IP address or host name.

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

   E-mail Encryption: Encrypt via SSL, TLS. NONE is default.

   Attached Image: Select the check box of **Attached Image** if you want to send emails with attached alarm snapshots.

   Interval: This is the time between two actions of sending attached snapshots.

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

User Name: The user name to log in to the server where the snapshots are uploaded.

Password: Enter the password.

Confirm: Confirm the password.

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

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

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

Receiver's Address2: The email address of user to be notified.

Receiver3: The name of the second user to be notified.

Receiver's Address3: The email address of user to be notified.

3. Click **Test** to test the email parameters set up.

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

To set up the HTTPS parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **HTTPS**.
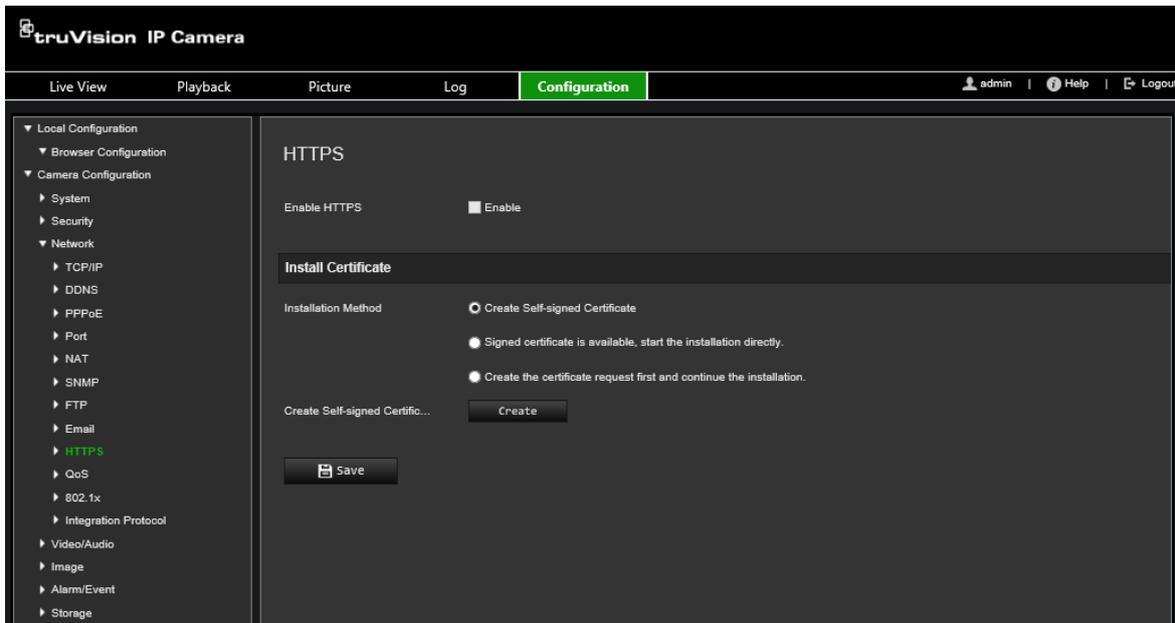
2. **To create a self-signed certificate**:

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.

3. 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.

To define the QoS parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **QoS**.

2. Configure the QoS settings, including Video / Audio DSCP, Event / Alarm DSCP and Management DSCP. The valid value range of the DSCP is 0-63. The larger the DSCP value, the higher the priority.

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

To define the 802.1x parameters:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Network** > **802.1X. 2.**
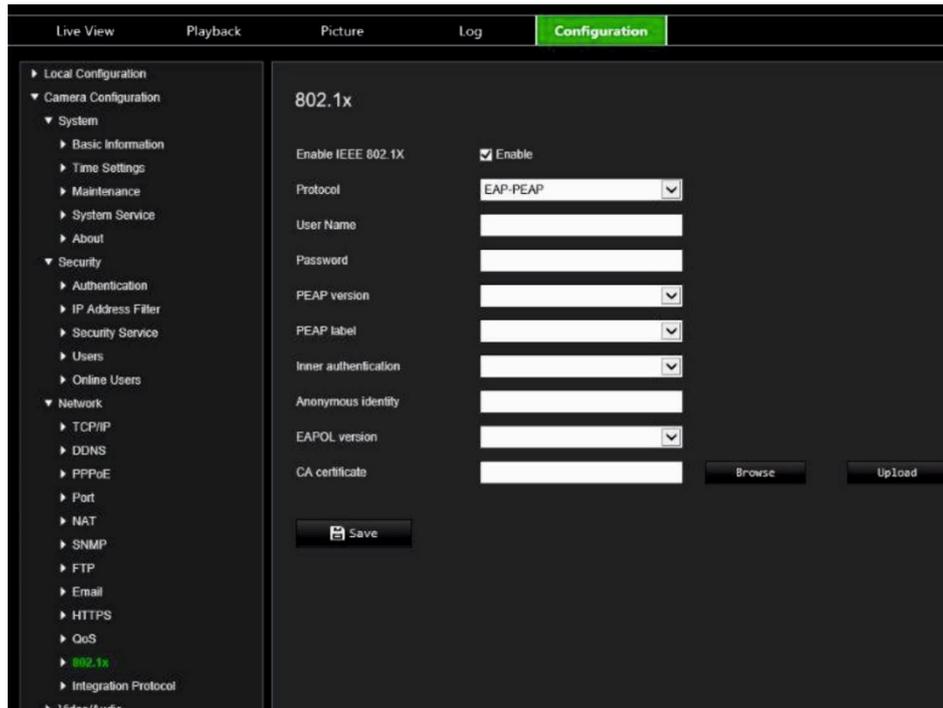
2. Select **Enable IEEE 802.1X** to enable the feature.

3. Select **EAP-PEAP** or **EAP-TLS** protocol, and configure all parameters for the selected protocol (see table below).

Protocol	EAP-PEAP
User Name	This is a valid username for the 802.1x server.
Password	This is a valid password for the username specified in the previous field.
PEAP version	Version 1 or 2; affects the format of the exchange with the RADIUS server.
PEAP label	This information will be available from the network administrator, as it will differ per network.
Inner authentication	MS-CHAPv2 - Microsoft Challenge-Handshake Authentication Protocol version 2, defined in RFC 2759. GTC - Generic Token Card, used when an automated device generates ASCII data to input for authentication. EAP - Extensible Authentication Protocol, defined in RFC 3748 and RFC 5247.
Anonymous identity	Used so the authenticator can choose the correct authentication server, with the actual identity sent in a second exchange (ex: anonymous@test.com).
EAPOL version	Indicate the version (1 or 2) that is being used; affects the format of the exchange with the RADIUS server.
CA certificate	This should be obtained from the network administrator, as network policies may differ.

Protocol	EAP-TLS
Identify	Obtain this information from the network administrator, if any.
Private Key Password	This should also be requested from the network administrator.
EAPOL version	Indicate the version (1 or 2) that is being used; changes the format of the exchange.
CA certificate	This should be obtained from the network administrator, as network policies may differ.

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

Note: The switch or router to which the camera is connected must also support the IEEE 802.1X standard, and a server must be configured. Please apply and register a user name and password for 802.1X in the server.

Recording parameters

You can adjust the video and audio recording parameters to obtain the picture quality and file size best suited to your needs. Figure 3 below lists the video and audio recording options you can configure for the camera.

Figure 5: Video/Audio Settings menu (Video tab shown)
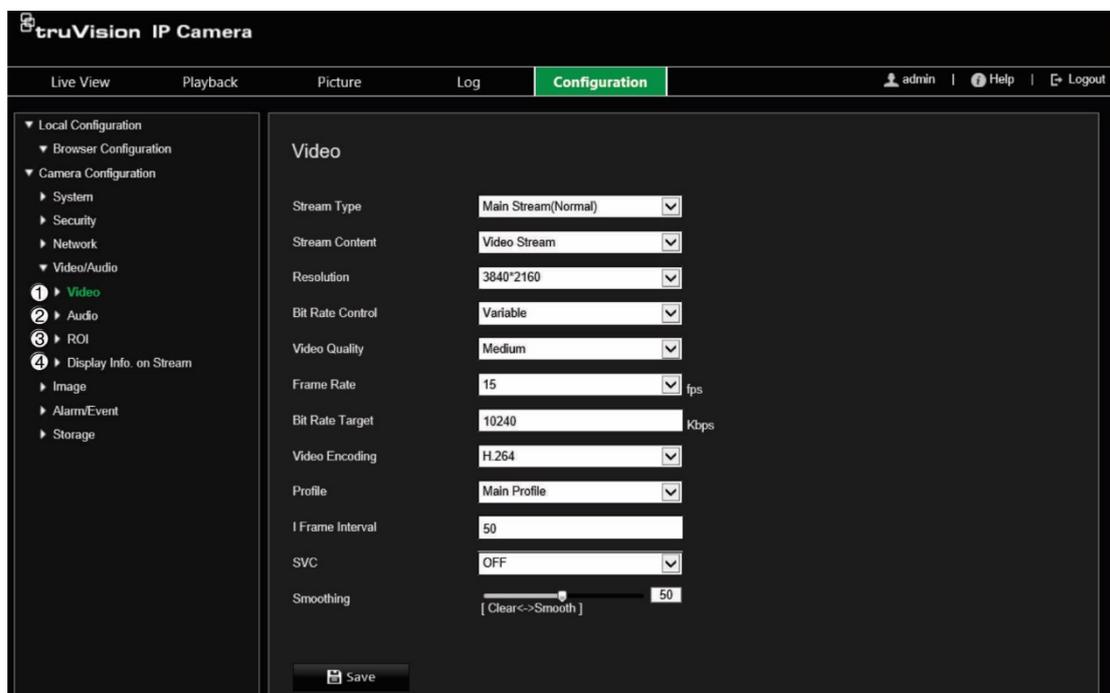
Tab	Parameter descriptions
1. Video	**Stream Type**: Specify the streaming method used.
	Options include: Main Stream (Normal), Substream.
	Note: The Third stream is only available when the this function is enabled in **System** > **System Service**.

Tab	Parameter descriptions
	Stream Control: Specify the stream type to record. Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams. **Note**: Video&Audio is only available for those camera models that support audio.
	Resolution: Specify 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 sub or third stream is being used. **Note**: Resolutions can vary depending on the camera model.
	Bit Rate Control: Specify whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.
	Video Quality: Specify the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, low, Medium, Higher and Highest.
	Frame Rate: Specify the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second. **Note**: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet.
	Video Encoding: Specify the video encoder used.
	Profile: Different profile indicates different tools and technologies used in compression. Options include: High Profile, and Main Profile.
	I Frame Interval: A video compression method. It is strongly recommended not to change the default value 50.
	SVC: Scalable Video Coding is an extension of the H.264/AVC 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: Adjust the smoothness of the stream.
2. Audio	**Audio Encoding**: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726 and PCM are optional.
	Audio Input: Mic In and Line In are selectable for the connected microphone and pickup respectively
	Input Volume: Specify the volume from 0 to 100.
	Environmental Noise Filter: Set to OFF or ON. Enable to filter the noise detected.
3. ROI	Enable to assign more encoding resources to the region of interest (ROI) to increase the quality of the ROI whereas the background information is less focused.
4. Display Info. On Stream	When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.

To configure audio settings:

From the menu toolbar, click **Configuration** > **Camera Configuration** > **Video/Audio** > **Audio**.
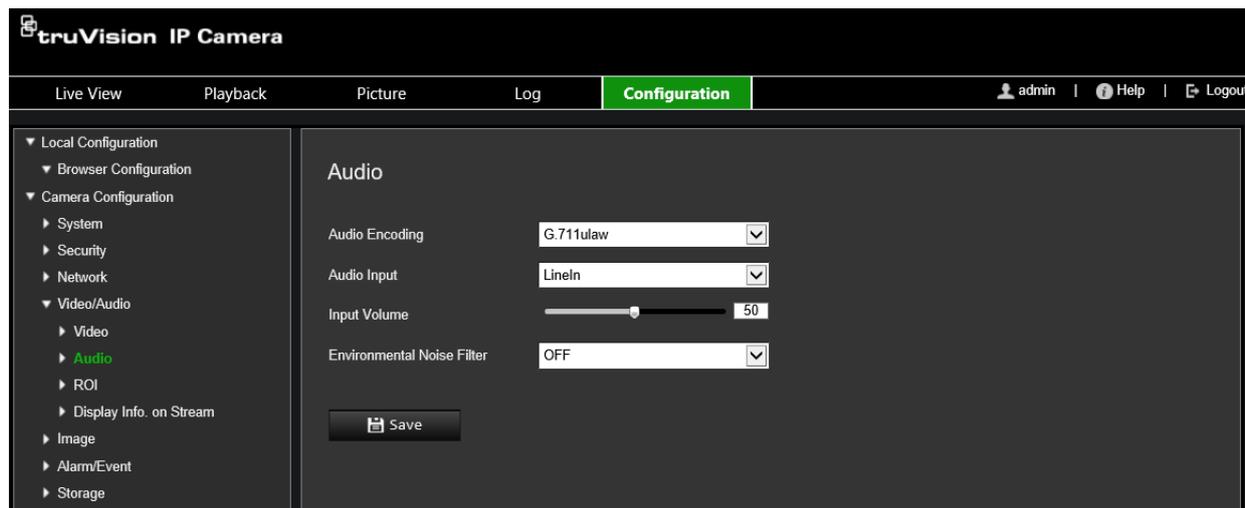
To configure ROI settings:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Video/Audio** > **ROI**.
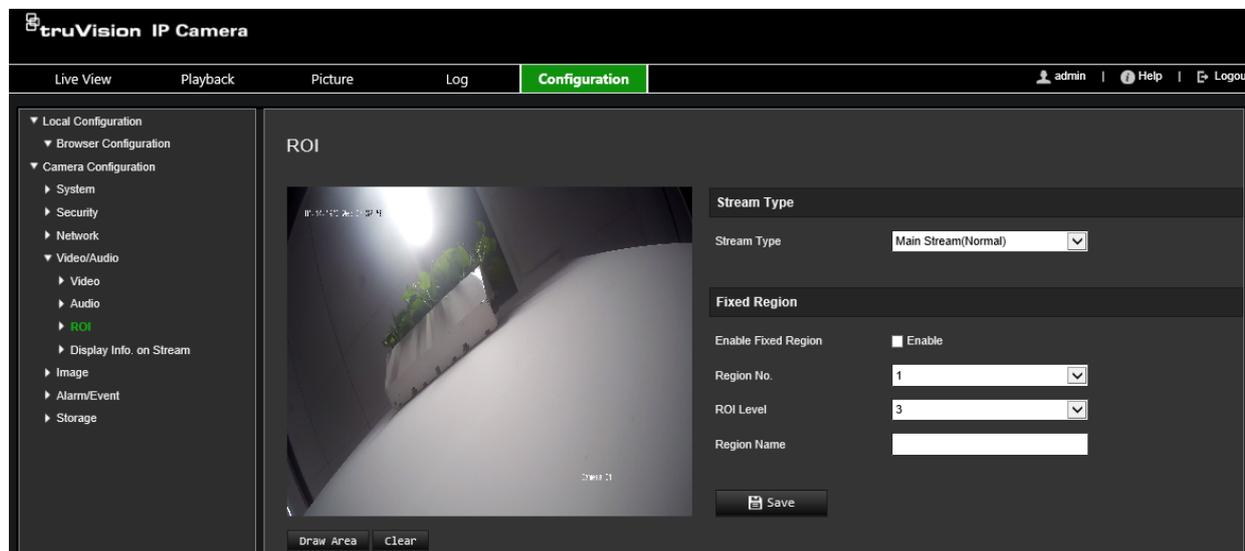
2. Select the desired channel from the drop-down list.

3. Draw the region of interest on the image. Up to four regions can be drawn.

4. Choose the stream type to set the ROI encoding.

5. Enable **Fixed Region** to manually configure the area.

    Region No.: Select the region.

    ROI Level: Choose the image quality enhancing level.

    Region Name: Set the desired region name.

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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Video/Audio** > **Display Info. On Stream**.

2. 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. See Figure 4 below for more information.

Use this menu to also adjust camera behavior parameters such as exposure time, iris mode, video standard, day/night mode, image flip, WDR, digital noise reduction, white balance, and indoor/outdoor mode.

Figure 6: Camera image settings menu – Display Settings tab
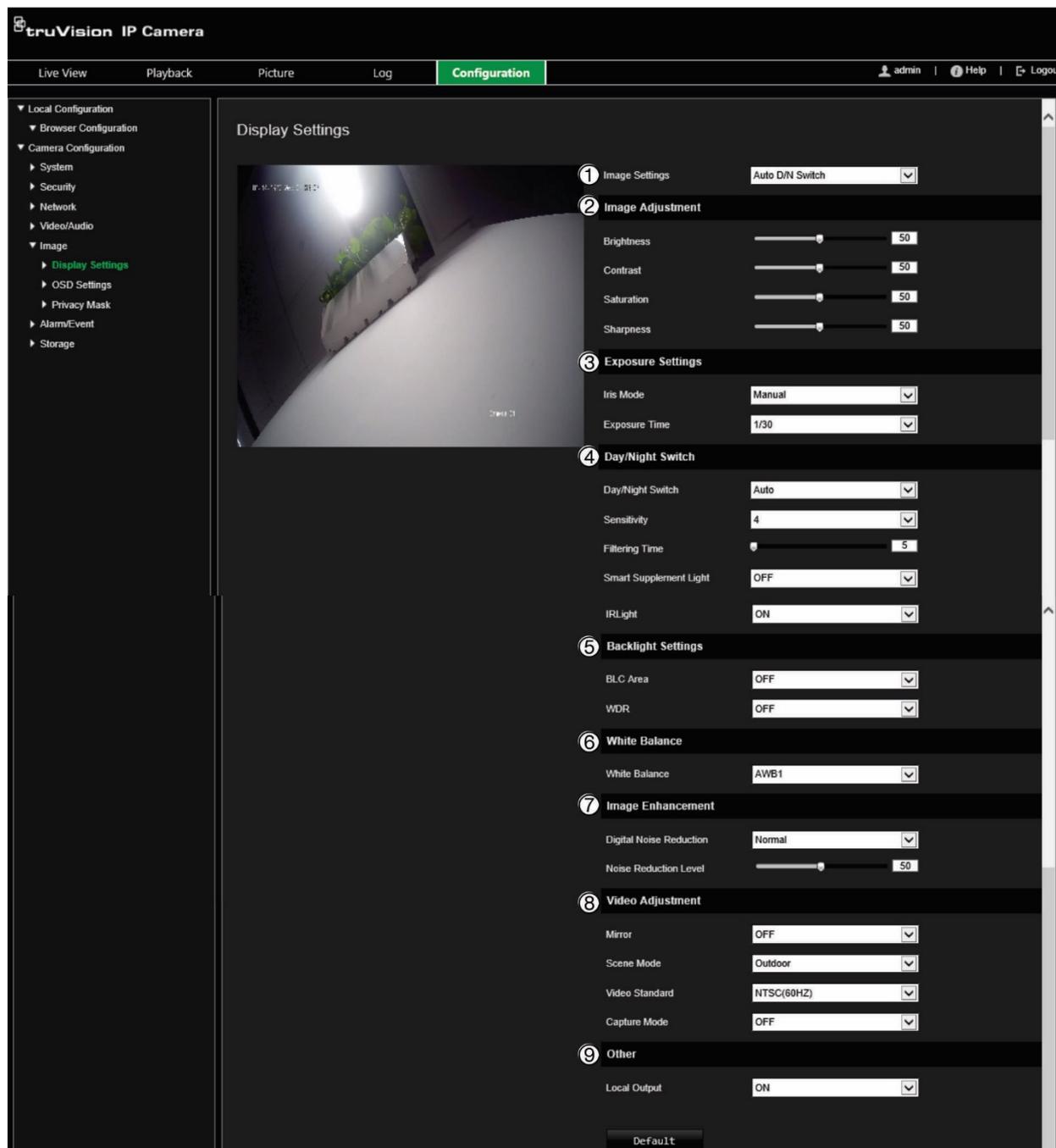
Parameter	Description
1. Image Settings	
Auto D/N Switch	The camera automatically switches between day and night modes. All image settings remain the same for both modes.
	The image settings are: Image Adjustment, Exposure Settings, Day/Night Switch, Backlight Settings, White Balance, Image Enhancement, and Video Adjustment.
	Common: Set each image parameter individually for D/N switch.
	Default: Only use default settings.

Parameter	Description
Custom 24-h settings	Customize the camera switch schedule for 24-hour settings.
	There are three tabs to configure the Custom 24-hour settings:
	Common, *Day*, *Night*.
	See "Scheduled D/N Switch" below for further information.
Scheduled D/N Switch	The camera switches between the day and night modes according to the schedule configured (see figure below). The start and end times shown are for day mode. The other time period is for night mode.
	There are three tabs to configure the day/night settings:
	Common: The settings are identical for both day and night modes for Exposure Settings, Day/Night Switch, and Video Adjustment.
	Day: Image Adjustment, Exposure Settings, Backlight Settings, White Balance, and Image Enhancement for day mode only.
	Night: Image Adjustment, Exposure Settings, Backlight Settings, White Balance, and Image Enhancement for night mode only.
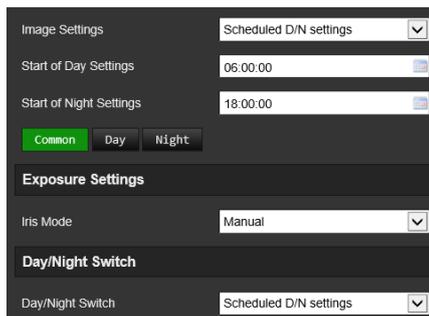
2. **Image Adjustment**

Brightness, Contrast, Saturation, Sharpness	Modify the different elements of picture quality by adjusting the values for each of parameter.

3. **Exposure Settings**

Iris Mode	Only *Manual iris mode* 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 objects.

4. **Day/Night Switch**

Day/Night Switch	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.
	Select one of the options:
	Day: Camera is always in day mode.
	Night: Camera is always in night mode.
	Auto: The camera automatically detects which mode to use.
	Schedule: The camera switches between day and night modes according to the configured time period.
	Triggered by Alarm Input: The camera switches to day or night mode after an alarm is triggered.

Parameter	Description
Sensitivity	Only available when *Auto D/N switch* mode is selected. It defines the sensitivity of the switch between day and night. Set it between 0 and 7.
Filtering time	Only available when *Auto D/N switch* mode is selected. The filtering time refers to the interval time between switchover the day/night switch. Set it between 5 and 120 s.
Smart IR	When enabled, the camera can avoid over exposure issues by automatically adjusting the IR LED. Set the Smart IR to **ON** and select either **Auto** or **Manual** as IR mode. Select **AUTO** so the camera automatically adjusts the IR LED illumination depending on the actual luminance. For example, if the current scene is bright enough, then the IR LED adjusts itself to a lower illumination. If the scene is too dark, the IR LED adjusts to a higher illumination. Select **Manual** so the camera automatically adjusts the IR LED illumination depending on the object's distance from the camera. For example, if the object is near the camera, the camera adjusts the IR LED to a lower illumination. If the object is far away, the IR LED adjusts to a higher illumination.
IR Light	Select On/OFF to Enable/disable IR. **ON**: The IR LEDs are ON when the camera changes to night mode. **Off**: The IR LEDs are OFF when the camera changes to night mode **Note**: The IR LEDs are always OFF in day mode.

5. Backlight Settings

Parameter	Description
BLC Area	This function improves image quality when the background illumination is high. It prevents the object in the center of the image from appearing too dark. Select OFF, Up, Down, Left, Right, Center, Custom or Auto. When WDR is enabled, BLC cannot be configured.
WDR	When enabled, wide dynamic range (WDR) provides clear images when there is high contrast between light and dark areas in the field of view of the camera. Both bright and dark areas can be displayed in the frame.

6. White Balance

Parameter	Description
White Balance	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: **MWB:** Manually adjust the color temperature to meet your own requirements. **AWB1**: Apply within a narrow range between 2500 to 9500K for environments where the lighting is always stable. **Locked WB:** Locks the WB to the current environment color temperature. **Fluorescent Lamp:** For use where there are fluorescent lamps installed near the camera. **Incandescent Lamp:** For use with incandescent lighting.

| Parameter	Description
	Warm Light Lamp: For use where the indoor light is warm.
	Natural Light: For use with natural light.
7. Image Enhancement	
Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance.
	Select Normal Mode, Advanced Mode, or OFF. Default is Normal Mode.
Noise Reduction Level	Only available when DNR is set to Normal Mode. Set the level of noise reduction in the Normal Mode. Higher value has a stronger noise reduction. Default is 50.
8. Video Adjustment	
Mirror	It mirrors the image so you can see it inversed.
	Select Left/Right, Up/Down, Center, or OFF. Default is OFF.
Hallway View	This function adjusts the image to suit long narrow scenes, such as corridors. It produces an image with a 9:16 ratio aspect to avoid including walls.
	During installation, turn the camera to 90 degrees or rotate the 3-axis lens to 90 degrees, and then set the rotate mode to ON. You will get a normal view of the scene with 9:16 aspect ratio that ignores needless information such as the walls. Default is OFF.
	Note: It is not supported by 8MPx cameras.
Scene Mode	Select indoor or outdoor according to the current environment.
Video Standard	Select 50 Hz or 60 Hz.
	Select the value depending on the video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.
Capture Mode	It is the selectable video input mode to meet the different demands of field of view and resolution.
	Lens Distortion Correction: Select ON / OFF to enable / disable the lens distortion correction. The distorted image caused by the wide-angle lens can be corrected if this function is enabled.
9. Other	
Local output	Select ON or OFF to enable or disable the BNC output. Default is ON.

Note: Click the **Default** button to default all the image settings.

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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Image** > **OSD Settings**.
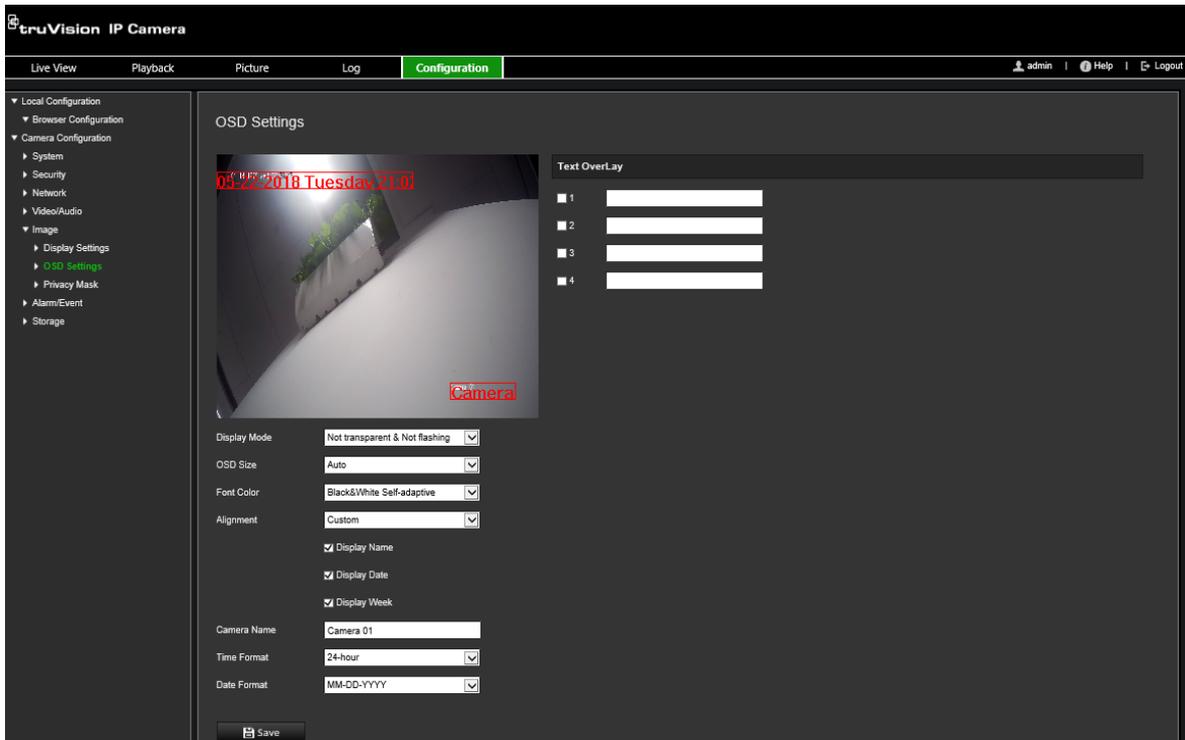
2. Select the **Display Name** box to display the camera's name on screen. You can modify the default name in the text box of **Camera Name**.

3. Select the **Display Date** check box to display the date/time on screen.

4. Select the **Display Week** check 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** drop-down list boxes.

7. Select a display mode for the camera from the **Display Mode** drop-down list box. Display modes include:

   • **Transparent & Not flashing.** The image appears through the text.

   • **Transparent & Flashing**. **T**he image appears through the text. The text flashes on and off.

   • **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 desired OSD size.

9. Select the desired font color.

10. Select the desired alignment (Custom, Align Left or Align Right).

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

Note: If the display mode sets as transparent, the text varies according the background. With some backgrounds, the text may be not easily readable.

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.

To add a privacy mask area:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Image** > **Privacy Mask**.
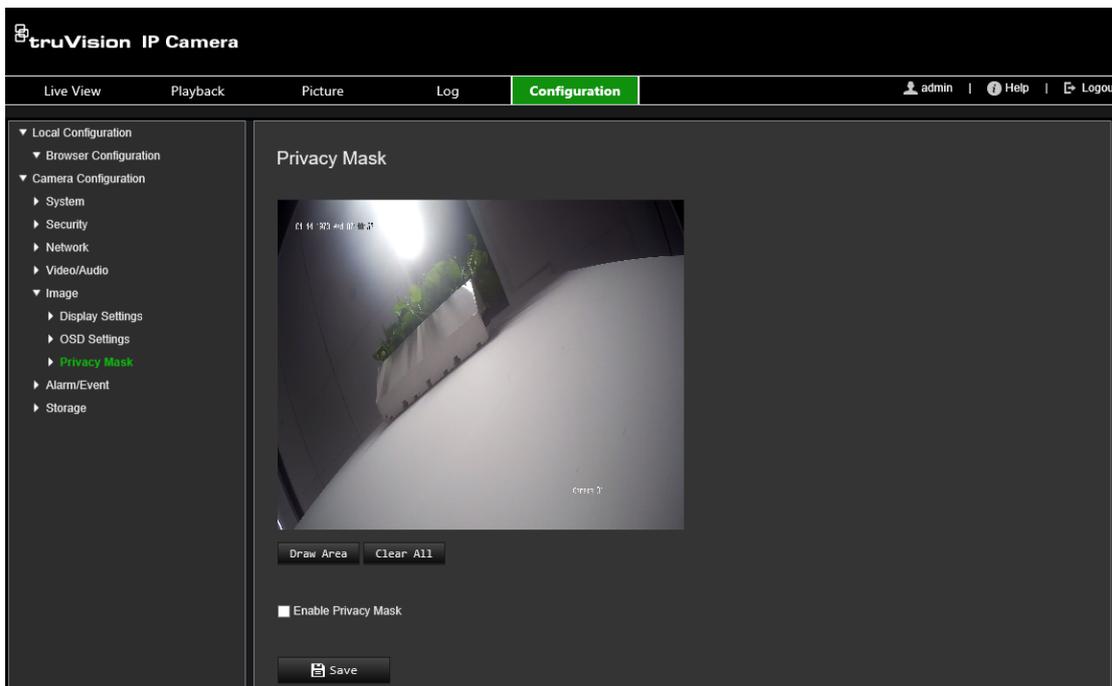
2. Select the **Enable Privacy Mask**.

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 7: Motion detection window**
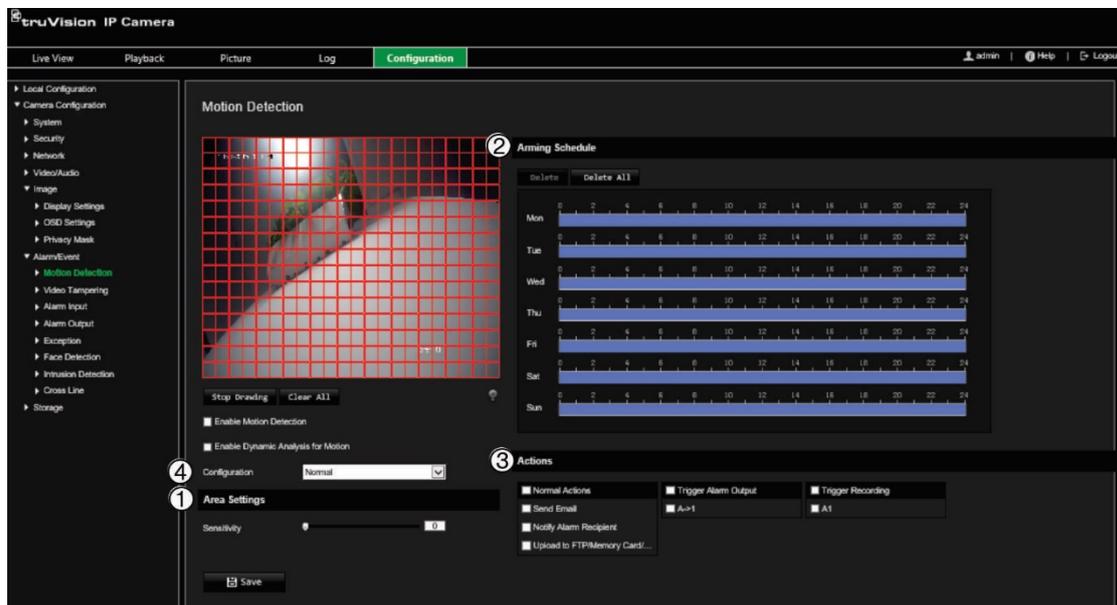
Defining a motion detection alarm requires the following tasks:

1. **Area settings**: Define the on-screen area that can trigger a motion detection alarm and the detection sensitivity level (see Figure 7, item 1).

2. **Arming schedule**: Define the schedule during which the system detects motion (see Figure 7, item 2).

3. **Recording schedule**: Define the schedule during which motion detection can be recorded. See "Recording Schedule" on page 49 for further information.

4. **Actions**: Specify the method of response to the alarm (see Figure 7, item 3).

5. **Normal and advanced configuration**: Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 7, item 4). Advanced configuration gives you much more control over how motion is detected. It lets you set the sensitivity level as well as define the percentage of the motion detection area that the object must occupy, select day or night mode, and set up eight differently configured defined areas.

To set up motion detection in normal mode:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/Event** > **Motion Detection**.

TruVision Series 6 IP Camera Configuration Manual

2. Select the **Enable Motion Detection** check box. Select the **Enable Dynamic Analysis for Motion** check box if you want to see real-time motion events.

   Note: If you do not want the detected object to be marked with the green frame, select **Disable** from Configuration > Local Configuration > Live View Parameters > Enable Meta Data Overlay.

3. Select **Normal** mode from the drop-down list.

4. Click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

   Note: You can draw up to eight motion detection areas on the same image.

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. Drag and click the time bar to edit the arming schedule.

Enter the start time (hour and minutes)   Enter the end time (hour and minutes)

8. Click ![icon] to copy the schedule to other days or to the whole week.
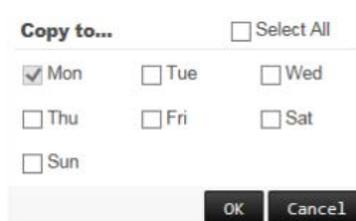
9. Click **OK** to save changes.

10. Specify the **linkage method** when an event occurs. Select one or more response methods for the system when a motion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.

|	
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.
	Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "NAS settings" on page 47 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 17 for further information. Enable the **Upload Type** option.
	To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See "Snapshot parameters" on page 45 for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

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

To set up motion detection in advanced mode:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/Event** > **Motion Detection**.

2. Select the **Enable Motion Detection** box. Select **Enable Dynamic Analysis for Motion** if you want to see where motion occurs in real-time.

   Note: Select Local Configuration > Enable Meta Data Overlay > Disable if you do not want the detected objects displayed with the green rectangles.

3. Select **Advanced** mode from the Configuration drop-down list.
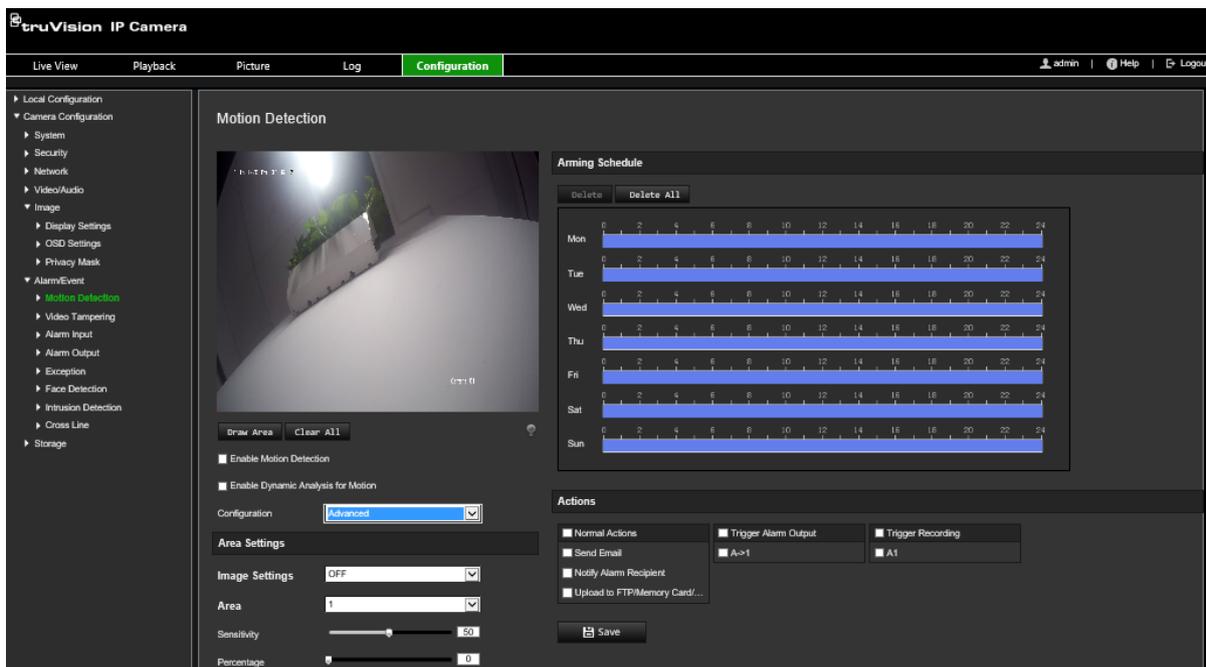

4. Under **Image Settings**, select OFF, Auto D/N Switch or Scheduled D/N settings. Default is OFF.

Auto D/N Switch and Scheduled D/N settings allow you to set different settings for day and night as well as different periods.

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.

   Note: You can draw up to eight motion detection areas on the same image. **Stop Drawing** shows up after **Draw Area** is clicked.

6. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.

7. Move the **Sensitivity** slider to set the sensitivity of the detection for the selected areas.

8. Move the **Percentage** slider to set the proportion of the object that must occupy the defined area to trigger an alarm.

9. Click **Save** to save the changes for that area.

10. Repeat steps 7 to 9 for each area to be defined.

11. Click **Edit** to edit the arming schedule. The following pop-up screen appears.
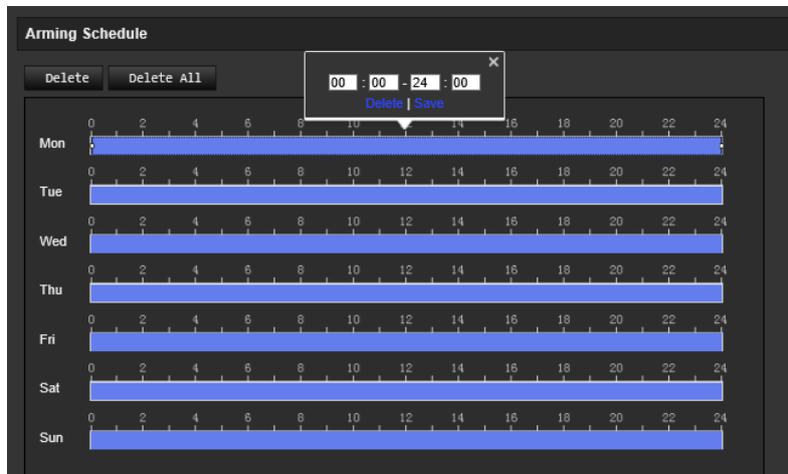
12. Click **OK** to save changes.

13. Specify the linkage method when an event occurs. Select one or more response methods for the system when a motion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.
	Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "NAS settings" on page 47 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 17 for further information. Enable the **Upload Type** option.
	To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See "Snapshot parameters" on page 45 for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

14. Click **Save** to save changes.

Video tampering

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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm Event** > **Video Tampering**.
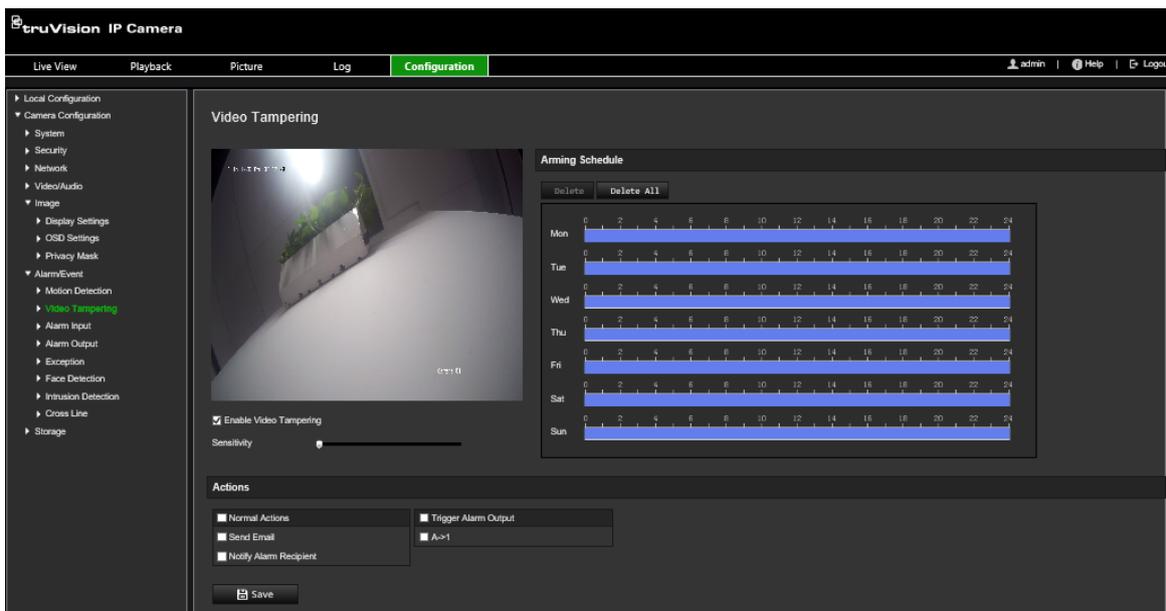
2. Select the **Enable Video Tampering** box.

3. Move the **Sensitivity** slider to set the detection sensitivity.

4. Edit the arming schedule for video tampering. The arming schedule configuration is the same as that for motion detection. See "Motion detection alarms" on page 31 for more information.

5. Specify the linkage method when an event occurs. Select one or more response methods for the system when a video tampering is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.

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 the 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.

To define exception alarms:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/ Event** > **Exception**.
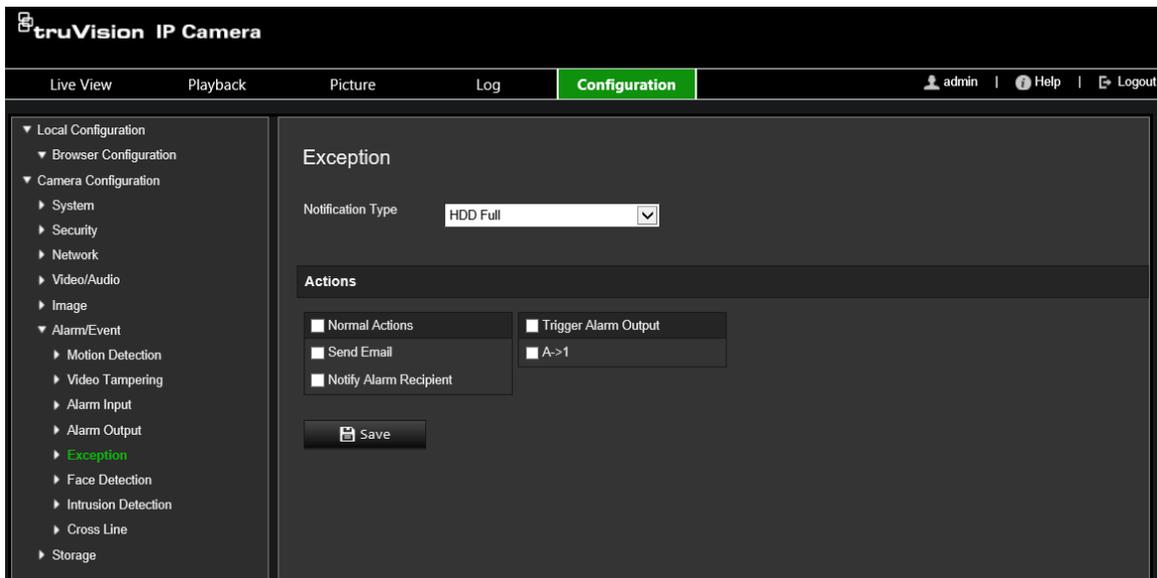
2. Under **Notification Type**, select an exception type from the drop-down list.

3. Specify the linkage method when an event occurs. Select one or more response methods for the system when a tamper-proof alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.

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

Alarm inputs and outputs

To define the external alarm input:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/Event** > **Alarm Input**.

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. Set the arming schedule for the alarm input. See "Motion detection alarms" on page 31 for more information.

4. Select the check box to enable the linkage method.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.
	Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "NAS settings" on page 47 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 17 for further information. Enable the **Upload Type** option.
	To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See "Snapshot parameters" on page 45 for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

5. Click **Save** to save changes.

To define an alarm output:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Basic Event** > **Alarm Output**.

2. Select one alarm output channel from the **Alarm Output** drop-down list. You can also set a name for the alarm output.

3. Set the delay time 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 the alarm occurs.

4. Set the arming schedule for the alarm input. See "To set up motion detection" for more information.

5. Click **Save** to save changes.

Face detection

When the face detection function is enabled, the camera can detect a human face that is moving towards it, triggering a response. The camera can only detect a face looking directly into the camera, not side views. This feature is best suited when the camera is in front of a door or is located in a narrow corridor.

Note: This function is only available when the third stream is disabled in **System** > **System Service**.

To define face detection:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/Event** > **Face Detection**.
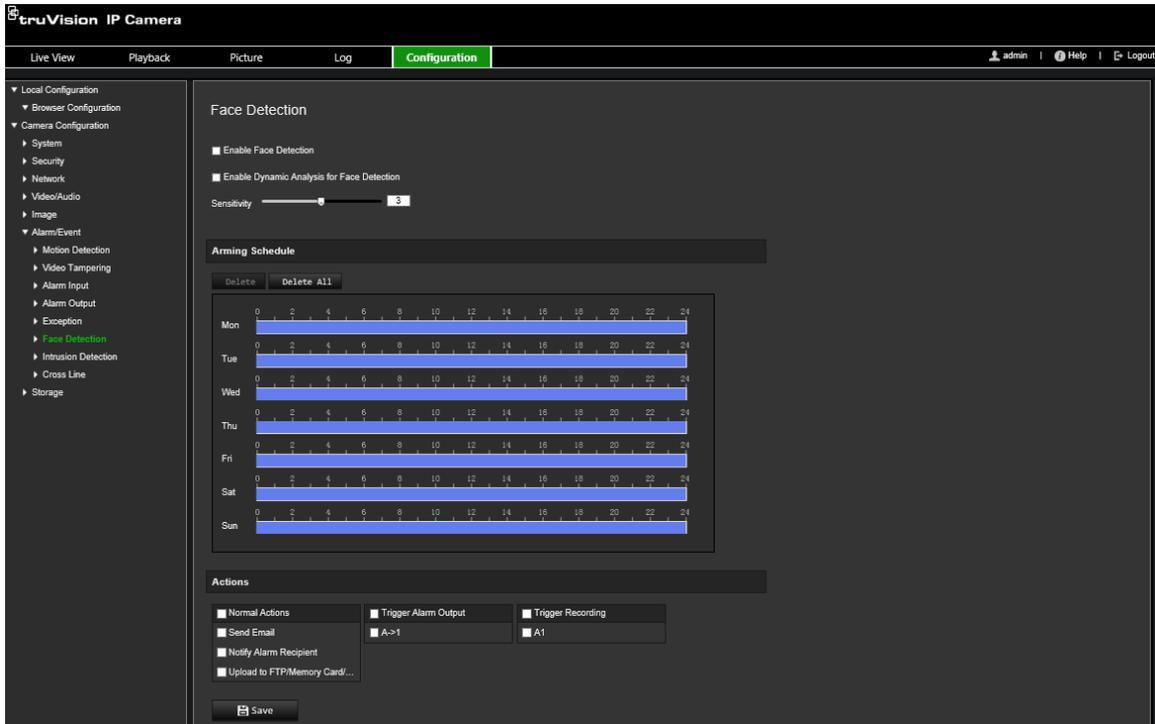
2. Select the **Enable Face Detection** check box to enable the function.

3. Select the **Enable Dynamic Analysis** check box for **Face Detection** if you want the face detected to be marked with a green rectangle in live view.

   Note: If you do not want the detected face marked with the green frame, select **Disable** from Configuration > Local Configuration > Live View Parameters > Enable Meta Data Overlay.

4. Configure the sensitivity of the face detection. The range is between 1 and 5.

5. Set the arming schedule for the alarm input. See "Motion detection alarms" on page 31 for more information.

6. Specify the linkage method when an event occurs. Select one or more response methods for the system when a face detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.
	Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "NAS settings" on page 47 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 17 for further information. Enable the **Upload Type** option.
	To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See "Snapshot parameters" on page 45 for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

7. Click **Save** to save changes.

Intrusion detection

You can set up an area in the surveillance scene to detect when intrusion occurs. Up to four intrusion detection areas are supported. If someone enters the area, a set of alarm actions can be triggered.

To define intrusion detection:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/Event** > **Intrusion Detection**.
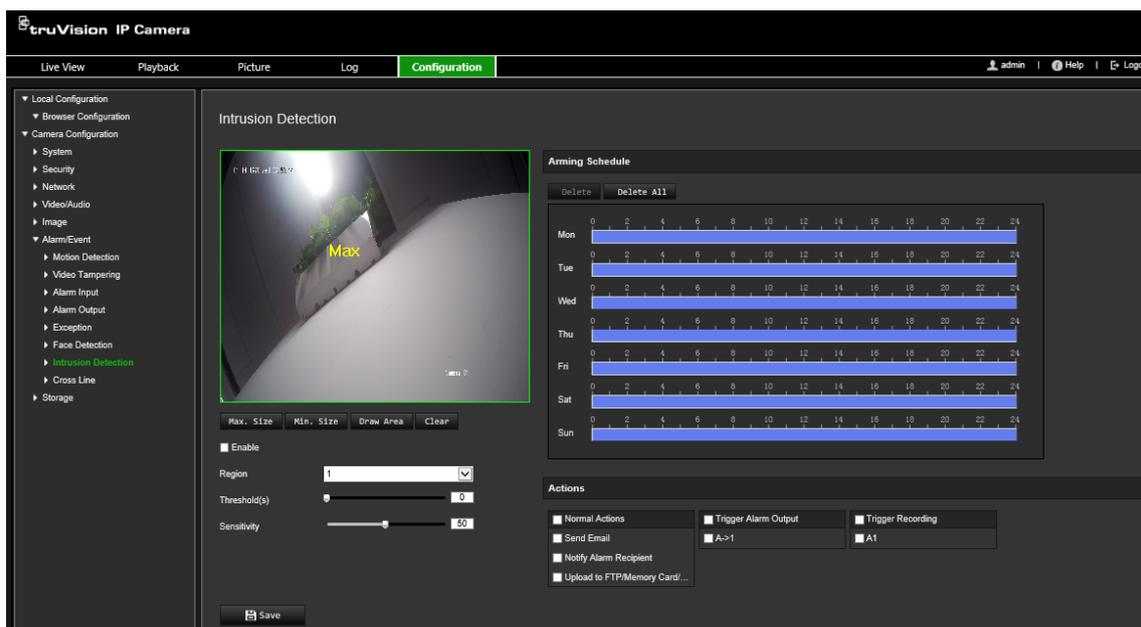
2. Select the **Enable Intrusion Detection** check box to enable the function.

3. Click **Draw Area**, and then draw a rectangle on the image as the defense region.

   When you draw the rectangle, all lines should connect end-to-end to each other. Up to four areas are supported. Click **Clear** to clear the areas you have drawn. The defense region parameters can be set up separately.

   Note: The area can only be quadrilateral.

4. Choose the region to be configured.

   Threshold: This is the time threshold that the object remains in the region. If you set the value as 0 s, the alarm is triggered immediately after the object enters the region. The range is between 0 and 10.

   Sensitivity: The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, a small object can trigger an alarm. The range is between 1 and 100.

5. Set the arming schedule for the alarm input. See "To set up motion detection" for more information.

6. Specify the linkage method when an event occurs. Select one or more response methods for the system when an intrusion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.
	Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "NAS settings" on page 47 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 17 for further information. Enable the **Upload Type** option.
	To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See "Snapshot parameters" on page 45 for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

7. Click **Save** to save changes.

Cross line detection

This function is used to detect people, vehicles, and objects crossing a pre-defined line or an area on-screen. Up to four cross lines are supported. The line crossing direction can be set as unidirectional or bidirectional. Unidirectional is crossing the line from left to right or from right to left. Bidirectional is crossing the line from both directions.

A series of linkage methods can be triggered if an object is detected crossing the line.

To define cross line detection:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Alarm/ Event** > **Cross Line**.
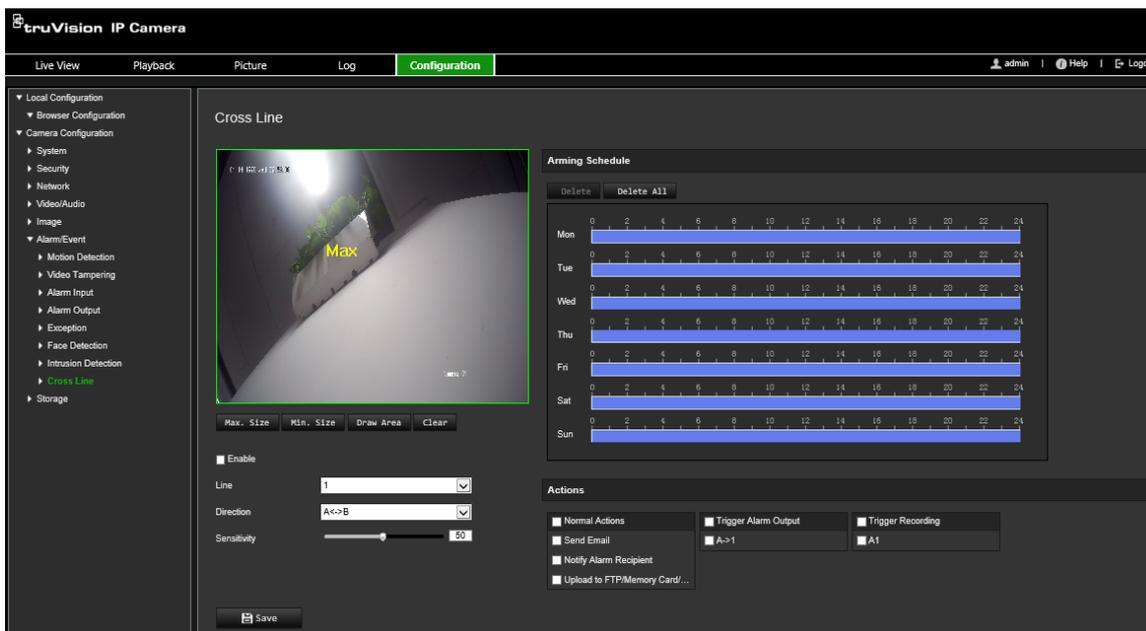
2. Select the **Enable** check box to enable the cross line detection function.

3. Click **Draw Area**, and a crossing plane will show on the image.

4. Click the line and two red squares appear at 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 list:

   A<->B: Only the arrow on the B side is displayed. When an object moves across the plane in both directions, it is detected and alarms are triggered.

   A->B: Only an object crossing the pre-defined line from the A to the B side can be detected and trigger an alarm.

   B->A: Only an object crossing the pre-defined line from the B to the A side can be detected and trigger an alarm.

5. Set the sensitivity level between 1 and 100. The higher the value is, the more easily the line crossing action can be detected.

6. If desired, select another line crossing area to configure from the dropdown menu. Up to four line crossing areas can be configured.

7. Set the arming schedule for the alarm input. See "Motion detection alarms" on page 31 for more information.

8. Specify the linkage method when an event occurs. Select one or more response methods for the system when a line cross detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm.
	Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 18 for further information. If you want to send the event snapshot together with the email, select the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.
	Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "NAS settings" on page 47 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 17 for further information. Enable the **Upload Type** option.
	To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See "Snapshot parameters" below for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.
	Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

9. 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 in a 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.

You must enable the option **Enable Timing Snapshot** if you want snapshots to be uploaded to the FTP. If you have configured the FTP settings and selected **Upload Type** in the Network > FTP tab, the snapshots will not be uploaded to the FTP if the **Enable Timing Snapshot** option is disabled.

You must enable the option **Enable Event-Triggered Snapshot** if you want snapshots to be uploaded to the FTP and NAS when motion detection or an alarm input is triggered. If you have configured the FTP settings and selected **Upload Type** in the Network > FTP tab for motion detection or an alarm input, the snapshots will not be uploaded to the FTP if this option is disabled.

To set up scheduled snapshots:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Storage** > **Snapshot**.
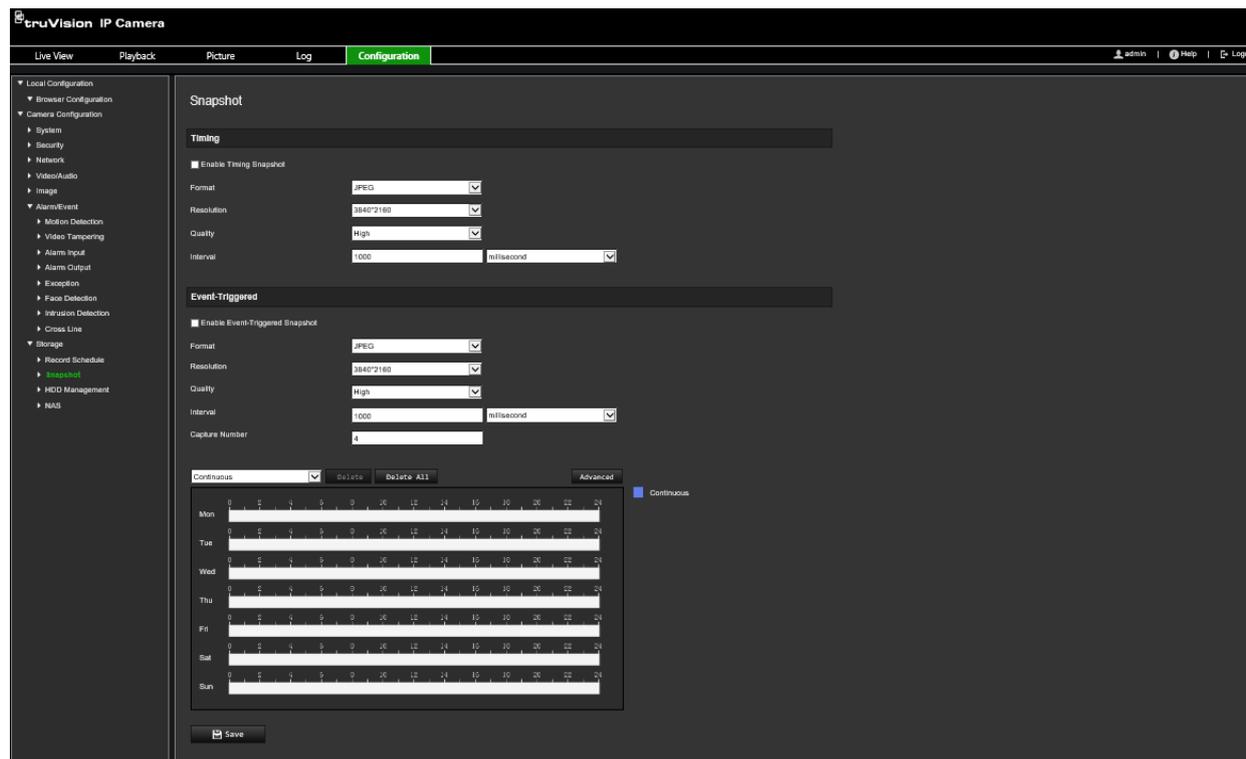
2. Select **Enable Timing Snapshot** check box to enable continuous snapshots.

3. Select the desired format of the snapshot, such as JPEG (default).

4. Select the desired resolution and quality of the snapshot.

5. Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds, seconds, minutes, hour, or day.

6. Set the schedule for when you want snapshots to be taken. Enter the desired schedule for each day of the week. Click **Advanced** to select the stream type, such as main stream (Normal).

7. Click **Save** to save changes.

To set up event-triggered snapshots:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Storage** > **Snapshot**.

2. Select the **Enable Event-triggered Snapshot** check box to enable event-triggered snapshots.

3. Select the desired format of the snapshot, such as JPEG (default).

4. Select the desired resolution and quality of the snapshot.

5. Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds or seconds.

6. Under **Capture Number**, enter the total number of snapshots that can be taken.

7. Click **Save** to save changes.

NAS settings

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

To configure recording 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 a camera.

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

To set up a NAS system:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Storage** > **NAS**.
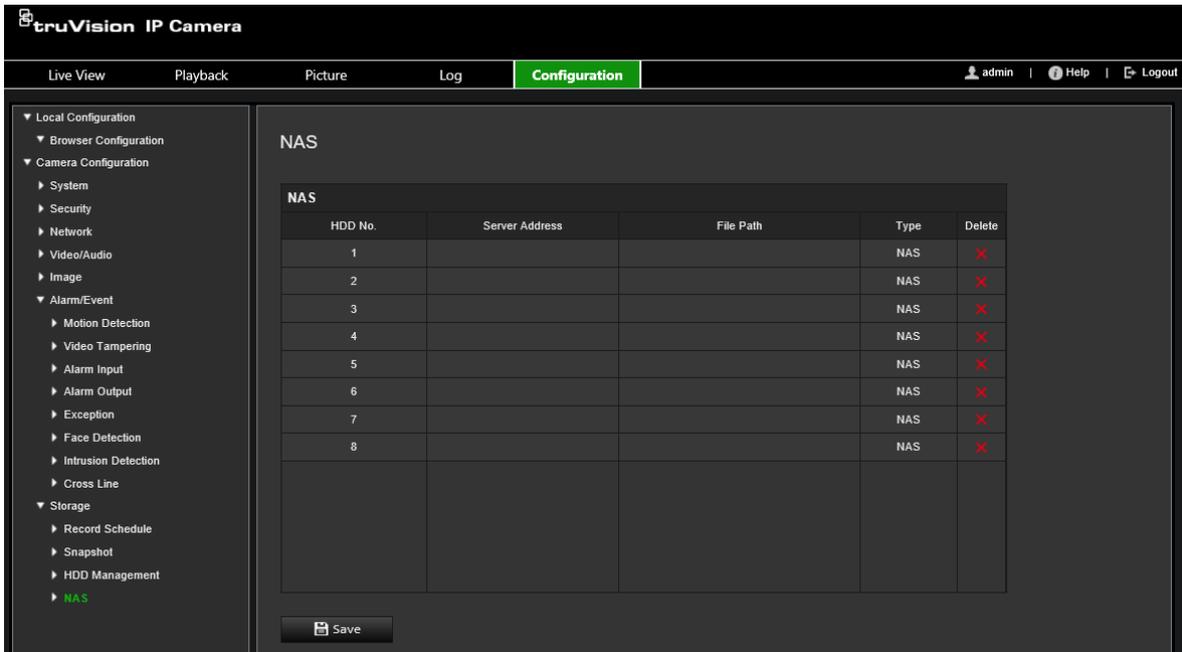
2. Enter the IP address of the network disk, and the NAS file path.

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

HDD management

Use the storage management window to display the capacity, free space available, and the working status of the HDD of the NAS and of the 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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Storage** > **HDD Management**.
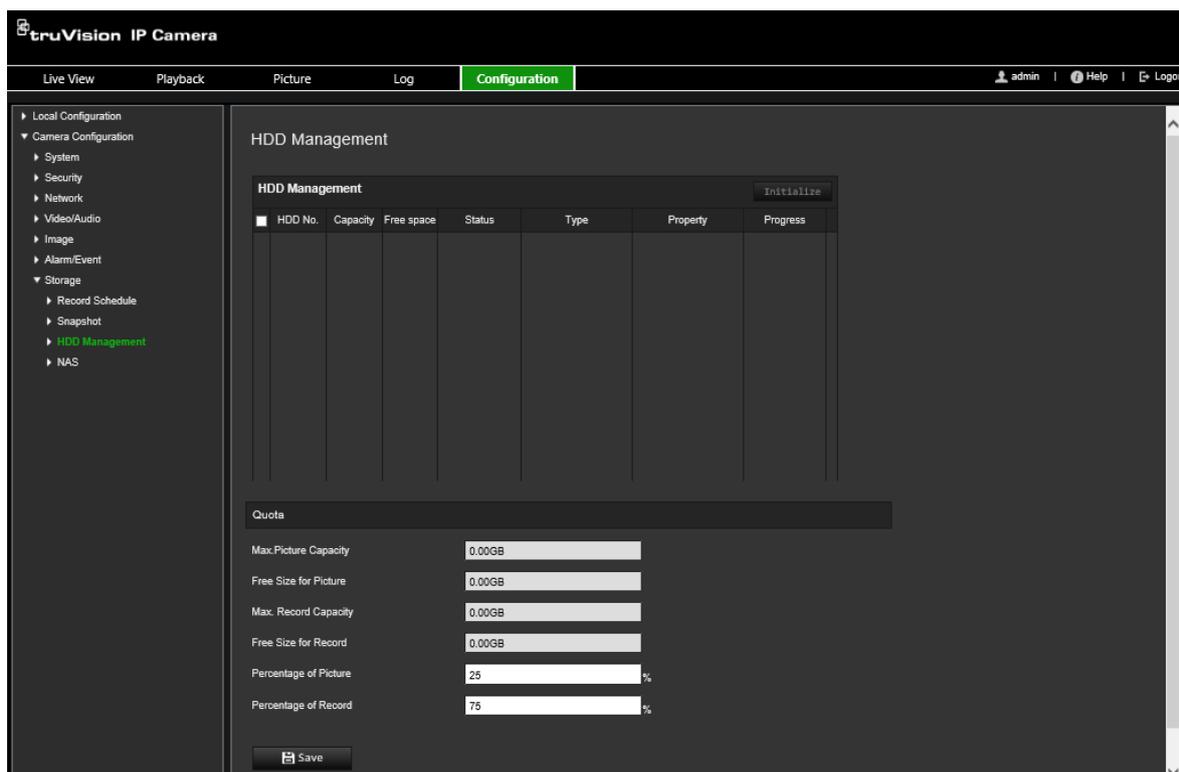
2. Select the **HDD Number** column to select the storage.

3. Define the quota percentage for snapshots and recordings, modify the values for each in **Percentage of Picture** and **Percentage of Record**.

4. Click **Format**. A window appears to select 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 SD card is not provided with the camera.

The selected recording schedule applies to all alarm types.
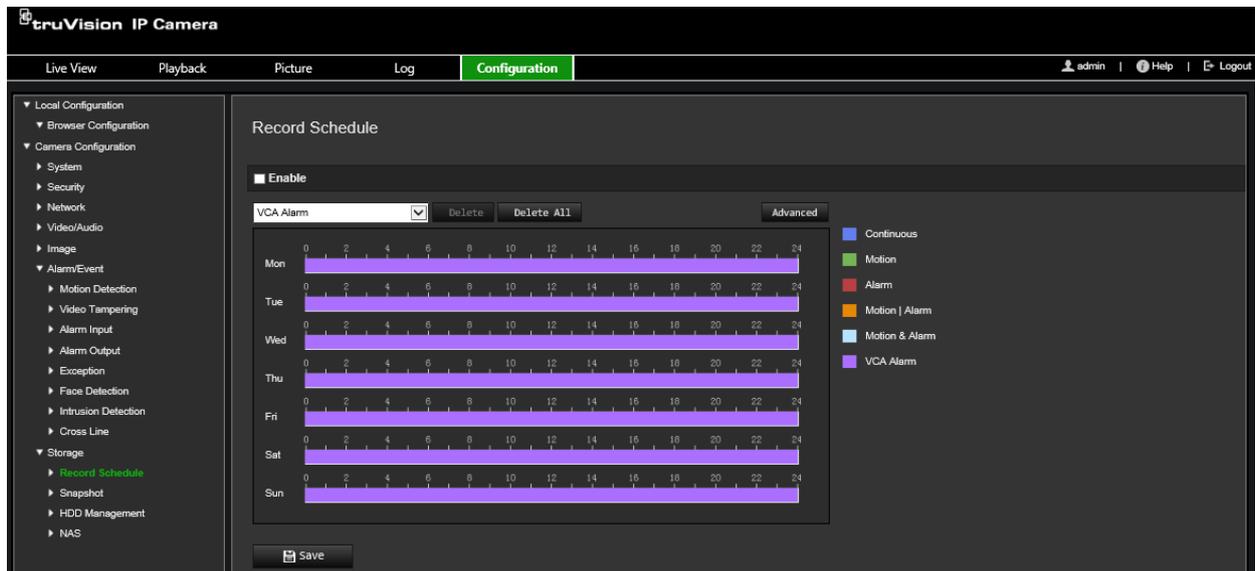
Pre-record time

The pre-record time is set to start recording before the scheduled time or event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set to 5 seconds, the camera starts to record 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 scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set to 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.

Overwrite

Enable *Overwrite* to overwrite the camera recording.

Recording Stream

Select Main Stream (Normal) or Substream for the recording stream.

To set up a recording schedule:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Storage** > **Record Schedule**.

2. Select the **Enable Record Schedule** check box to enable recording.

   Note: To disable recording, deselect the option.

3. Edit the recording schedule. The following window appears:
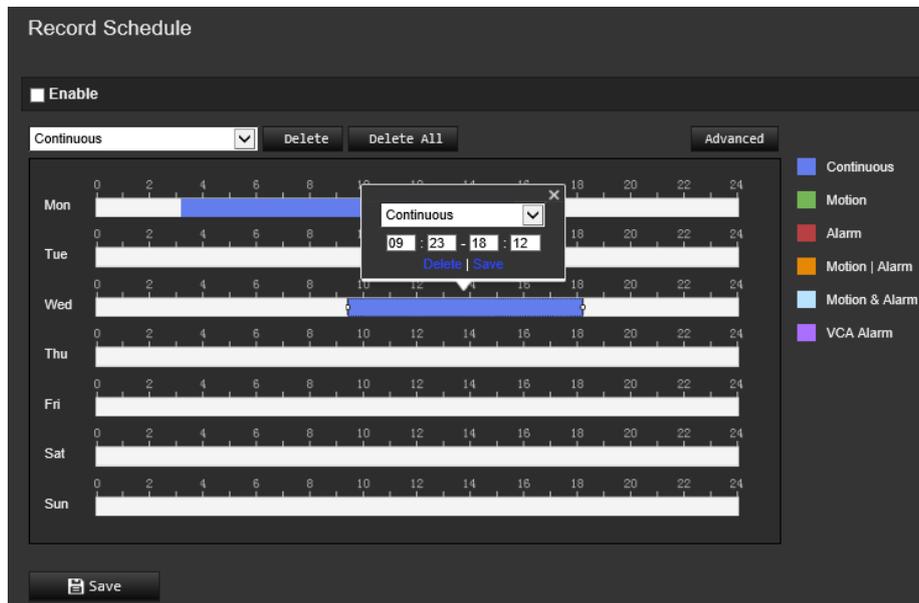
4. Select whether the recording will be for the whole week (**All Day** recording) or for specific days of the week.

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

   • **Continuous**: This is continuous recording.

   • **Motion:** Video is recorded when the motion is detected.

   • **Alarm:** Video is recorded when an alarm is triggered via the external alarm input channels. As well as configuring the recording schedule, you also have to set the alarm type and select *Trigger Alarm Output* as the linkage method for an external alarm input (see page 38).

   • **Motion | Alarm:** Video is recorded when an external alarm is triggered or motion is detected. As well as configuring the recording schedule, you also have to configure the settings for motion detection (see page 31) and for an external alarm input (see page 38).

   • **Motion & Alarm:** Video is recorded when both motion and alarm are triggered at the same time. As well as configuring the recording schedule, you have to configure the settings for motion detection (see page 31) and for an external alarm input (see page 38).

   • **VCA events:** Video is recorded when the either of the VCA events is triggered. Besides configuring the recording schedule, you have to configure the settings on the VCA interface.

5. 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.

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

Note: If you set the record type to "Motion detection" or "Alarm", you must also define the arming schedule in order to trigger motion detection or alarm input 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.

When new users are added to the list, the administrator can modify permissions and password of each user. See Figure 6 below.

Figure 8: User management window
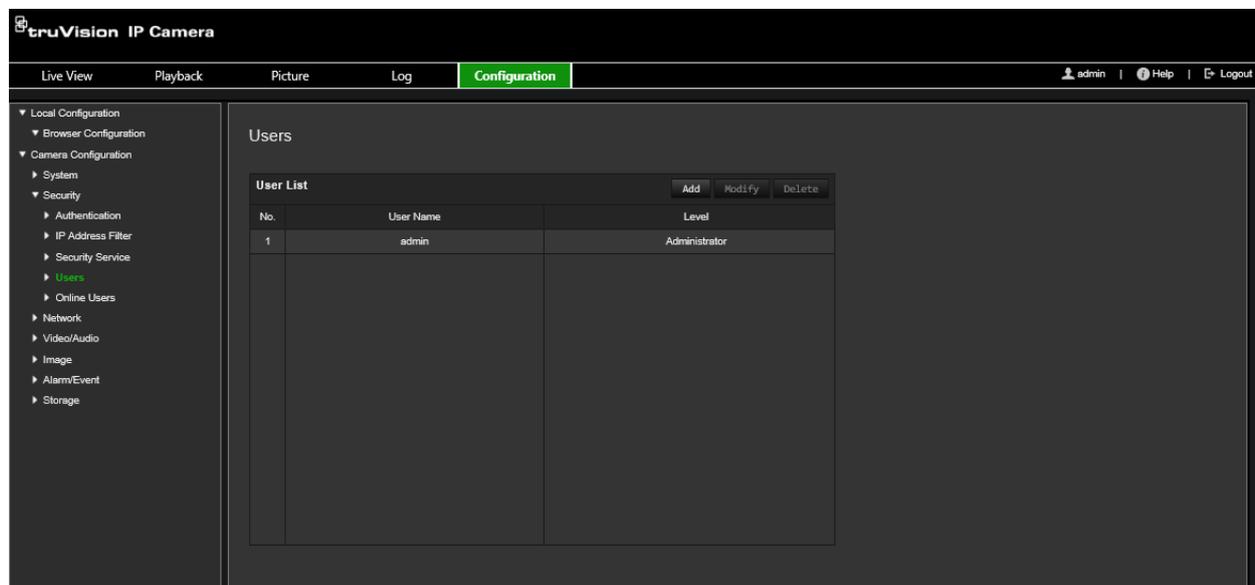
Passwords limit access to the camera and the same password can be used by several users. When creating a new user, you must give the user a password. There is no default password provided for all users. Users can modify their passwords.

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.

- **User**: This user has the permission of live view, playback and log search. However, they cannot change any configuration settings.

Add and delete users

The administrator can create up to 31 users. Only the system administrator can create or delete users.

To add a user:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Security** > **Users**.

2. Select the **Add** button. The user management window appears.

3. Enter a user name.

4. Assign the user a password. Passwords can have up to 16 alphanumeric characters.

5. Select the type of user from the drop-down list. The options are Viewer and Operator.

6. Assign permissions to the user. Select the desired options:

Basic Permissions	Camera Configuration
Remote: Parameters Settings	Remote: Live View
Remote: Log Search/Interrogate Working Status	Remote: Manual Record
Remote: Upgrade/Format	Remote: PTZ Control
Remote: Two-way Audio	Remote: Playback
Remote: Shutdown/Reboot	
Remote: Notify Alarm Recipient/Trigger Alarm Output	
Remote: Video Output Control	
Remote: Serial Port Control	

7. Click **OK** to save the settings.

To delete a user:

1. Select the desired user under the **User** tab.

2. Click **Delete** button. A message box appears.

   Note: Only the administrator can delete a user.

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

Modify user information

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

To modify user information:

1. Select the desired user under the **User** tab.

2. Click the **Modify** button. The user management window appears.

3. Change the information required.

   Note: The user "Admin" can only be changed by entering the admin password.

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

RTSP authentication

You can specifically secure the stream data of the live view.

To define RTSP authentication:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Security** > **RTSP Authentication**.
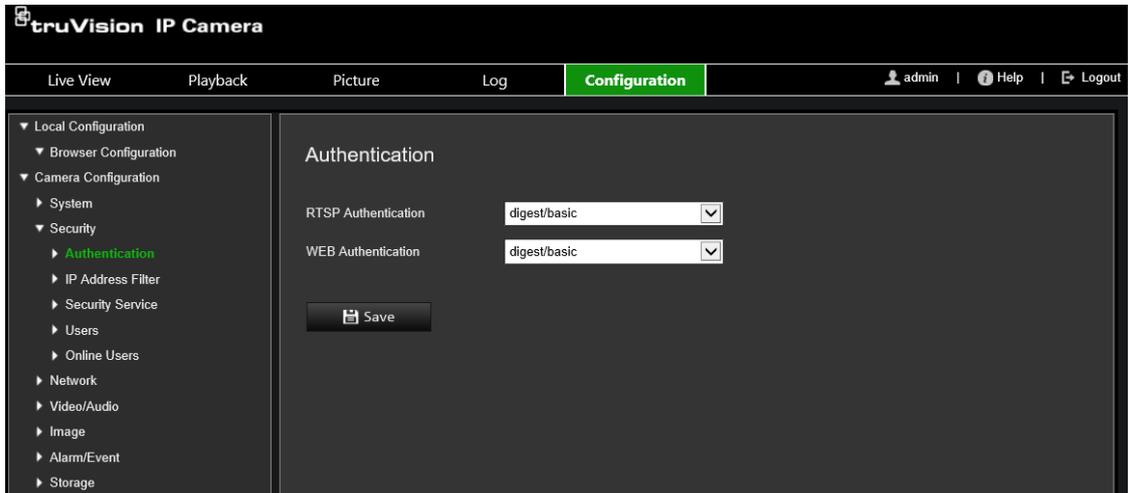
2. Select the **RTSP Authentication** type **Digest/basic** or **Digest** in the drop-down list

3. Select the **WEB Authentication** type **Digest/basic** or **Digest** in the drop-down list

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

IP address filter

This function allows you to give or deny access rights to defined IP addresses. For example, the camera is configured so that only the IP address of the server hosting the video management software is allowed to be accessed.

To define the IP address filter:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **Security** > **IP Address Filter**.
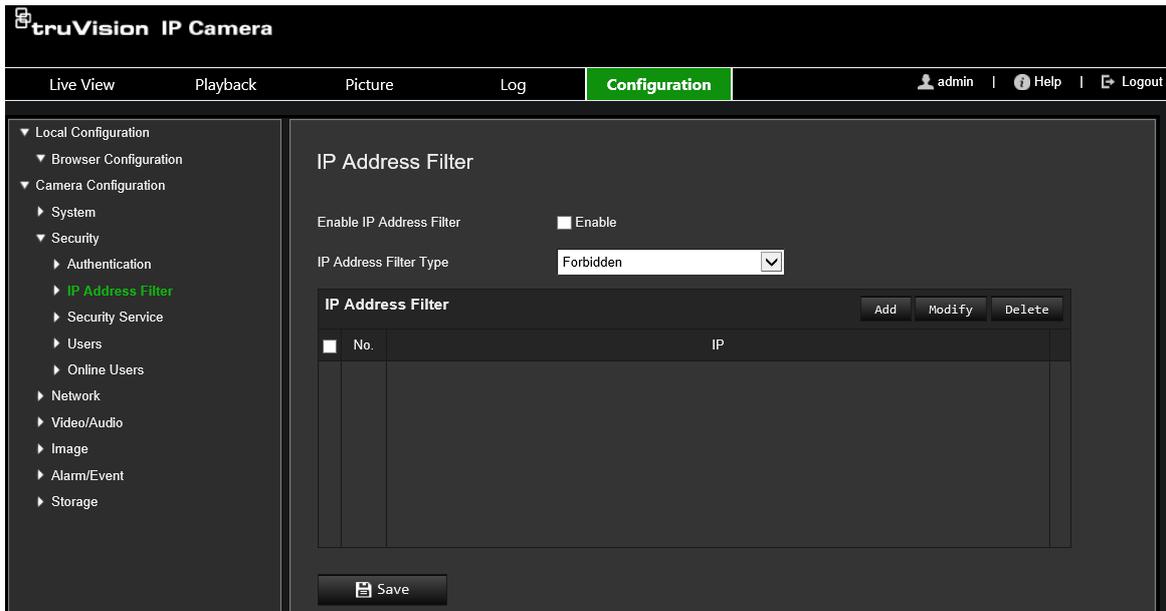
2. Select the **Enable IP Address Filter** check box**.**

3. Select the type of IP Address Filter in the drop-down list: Forbidden or Allowed.

4. Click **Add** to add an IP address and enter the address.

5. Click **Modify** or **Delete** to modify or delete the selected IP address**.**

6. Click **Clear** to delete all the IP addresses.

7. Click **Save** to save the changes.

Illegal login lock

This function allows you to enable the invalid login lock which locks the system when there have been too many failed login attempts.

The IP address will be locked if the administrator performs seven failed user name/password attempts (5 attempts for the operator/user). If the IP address is locked, you can log in to the device after five minutes.

Figure 9: Security service window
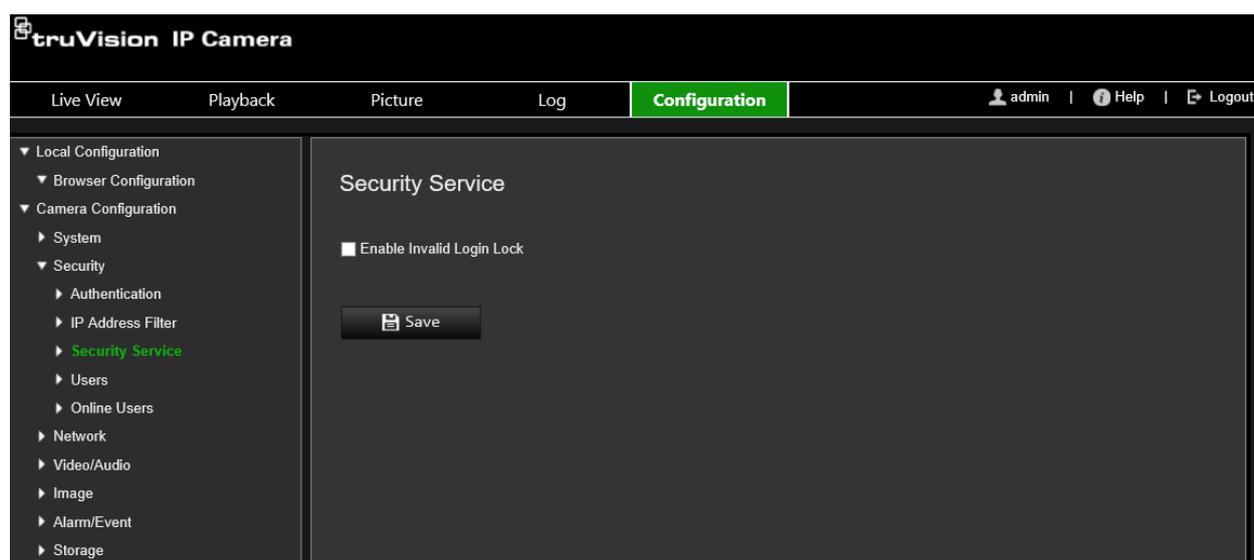
To enable the illegal login lock:

1. Click **Configuration** > **Camera Configuration** > **Security** > **Security Service**.

2. Select the **Enable Illegal Login Lock** check box.

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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **System**> **Maintenance**.

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.

Note: Only the administrator can import/export configuration files.

To import/export configuration file

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **System** > **Maintenance**.

2. Click **Browse** to select the local configuration file and then click **Import** to start importing configuration file.

3. Click **Device Parameters** 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/video

   — or —

   www.firesecurityproducts.com

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. From the menu toolbar, click **Configuration** > **Camera Configuration** > **System** > **Maintenance**. 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 Interlogix_Gen_3_ipc.dav for camera models listed in the "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.

To upgrade the firmware via TruVision Device Manager:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **System** > **Maintenance**.
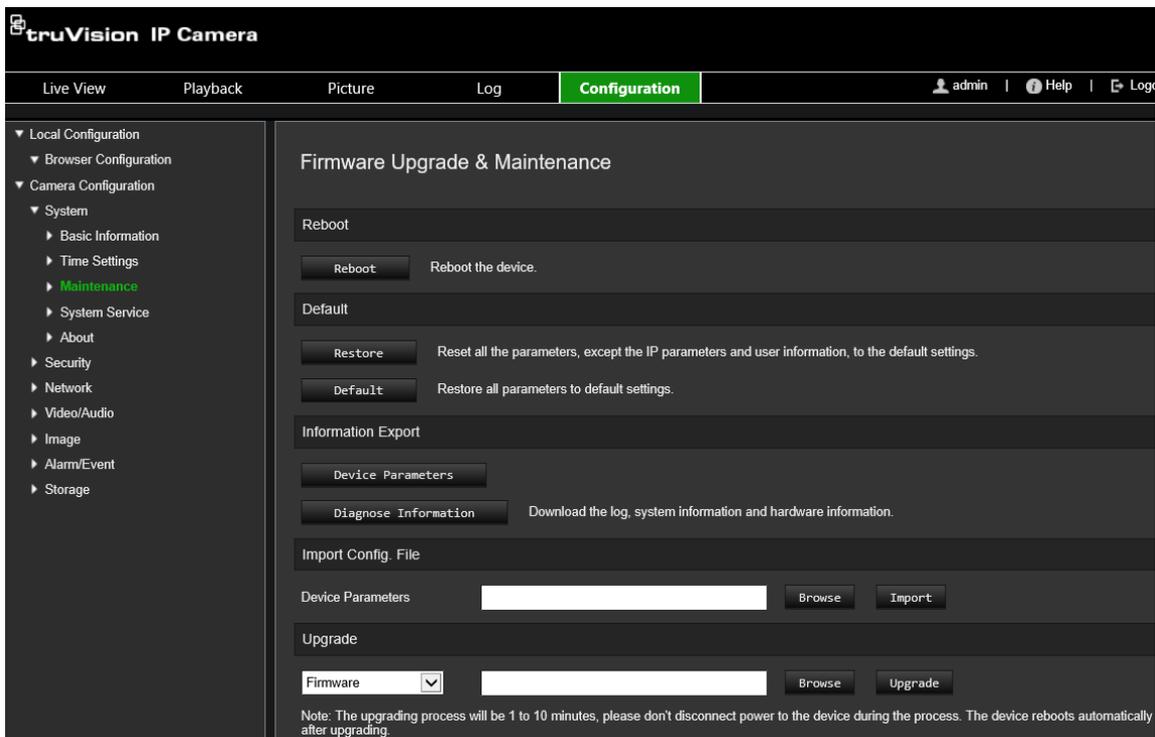
2. Click the Browse button to locate the firmware file to use.

   If you want the device to automatically reboot after the upgrade, select **Reboot the device after upgrading**. When selected, it will also display **Restore default settings** option. Check it if you want to restore all parameters.

3. Click **Upgrade**.

   Note: The upgrading process will be 1 to 10 minutes. Please do not disconnect power to the device during the upgrade process. The device reboots automatically after upgrading.

Reboot camera

It is easy to reboot the camera remotely.

To reboot the camera through the web browser:

1. From the menu toolbar, click **Configuration** > **Camera Configuration** > **System** > **Maintenance**.

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.

Log in and out

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.

Note: When an incorrect user name or password has been entered, a message appears showing how many login attempts remain ("Incorrect user name or password. The device will be locked after xxx failed login attempts."). However, in order for this error message to appear, you must first enable **Enable Illegal Login Lock** under **Configuration** > **Camera Configuration** > **Security** > **Security Service**. See "Illegal login lock" on page 56 for further information.

You can change the language of the interface from the drop-down menu in the top right corner of the window.

Figure 10: Login dialog box

If you do not change the default password for *admin*, a message will always pop up requesting 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 8 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.

Play back recorded video

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

Note: You must configure the NAS or insert an SD card in the dome camera to be able to use the playback functions. See "HDD management" on page 48 for more information.

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 8 below.

Note: You must have playback permission to play back recorded images. See "Modify user information" for more information.

Figure 11: 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 ![arrow] 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. ![stop] Stop ![speed down] Speed down

Name	Description
	▶ Play
	▶▶ Speed up
	▶ Playback by frame
6. Archive functions	Click these buttons for the following archive actions:
	📷 Capture and download a snapshot image of the playback video.
	✂ Start/Stop clipping video files.
7. Digital zoom	Click to enable digital zoom.
8. Audio control	Control level of audio. Drag to adjust the volume.
9. Time moment	Vertical bar shows where you are in the playback recording. The current time and date are also displayed.
10. Timeline bar	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.
	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.
	Click ▬▬ to zoom out/in the timeline bar.
11. Download functions	⤓ Download video files.
12. Recording type	The color code displays the recording type. Recording types are Continuous recording (blue), Alarm recording (red), and manual recording (yellow).
	The recording type name is also displayed in the current status window.

To play back recordings:

1. Click **Playback** on the menu bar to enter the playback interface.

2. Select the date in the calendar and click **Search**.

3. Click ▶ to play the video files found on this date.

   Use the toolbar on the bottom of playback interface to control the playing process. See Figure 11 above for information on what the icons mean.

   Note: You can choose the file paths locally for downloaded playback video files and snapshots under *Local Configuration.*

   To play back from a specific time, enter the time and click ➡ to locate the playback point.

4. 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. Click ▬▬ to zoom out/in of the timeline bar.

5. To download video files, click ⤓.

Search event logs

You must configure NAS or insert a SD card in the dome 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 9 below.

Note: You must have view log access rights to search and view logs. See "Modify user information"

Figure 12: Log window
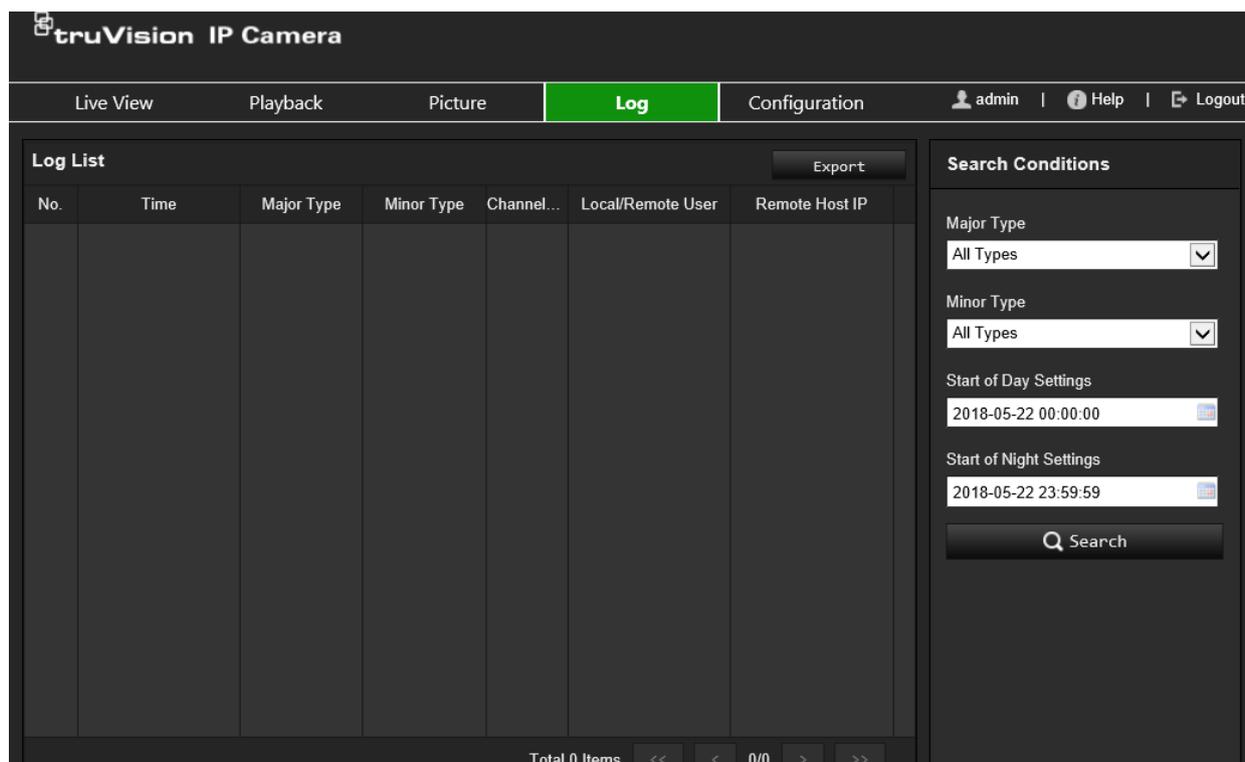
You can search for recorded logs by the following criteria:

Major type: There are four types of logs: All Types, Alarm, Exception, Operation or Information. See Table 1 below for their descriptions.

Minor type: Each major type log has some minor types. See Table 1 below for their descriptions.

Start of day settings: Logs can be searched by start recording time.

Start of night settings: Logs can be searched by end recording time.

Table 1: Types of logs

Main log type	Minor log types: Description of events included
Alarm	Alarm Input, Alarm output, Start Motion Detection, Stop Motion Detection, Start Tamper-proof, Stop Tamper-proof, Face Detection Started, Face Detection Stopped, Cross Line Detection Started, Cross Line Detection Stopped, Intrusion Detection Started, Intrusion Detection stopped, Defocus Detection Started, Defocus Detection stopped, Audio input Exception, Sudden change of sound Intensity Detection.
Exception	Invalid Login, HDD Full, HDD Error, Network Disconnected and IP Address Conflicted
Operation	Power On, Abnormal Shutdown, Remote Reboot, Remote Login, Remote Logout, Remote Configure parameters, Remote Start Record, Remote Stop Record, Remote PTZ Control, 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, Establish Transparent Channel, Disconnect Transparent Channel, Start Bidirectional Audio, Stop Bidirectional Audio, Remote Alarm Arming, Remote Alarm Disarming

To search the 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 times of the log.

4. Click **Search** to start your search. The results appear in the left window.

Index