TruVision Series 4 IP Camera Configuration Manual

P/N 1073194-EN • REV D • ISS 09JUL19

Manufacturer

Interlogix
2955 Red Hill Avenue, Costa Mesa, CA 92626-5923, USA

Authorized EU manufacturing representative:
UTC Building & Industrial Systems B.V.
Kelvinstraat 7, 6003 DH Weert, The Netherlands

Certification

Contact information and manuals/ tools/ firmware

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

Americas: www.interlogix.com

EMEA: www.firesecurityproducts.com
Manuals are available in several languages.

Australia/New Zealand: www.utcfs.com.au

Content

Introduction

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

- TVC-5401 (2MPX low light camera)
- TVC-5402 (3MPX box camera)
- TVC-5403 (5MPX box camera)

- TVB-5401 (2MPX low light bullet camera)
- TVB-5402 (2MPX low light bullet camera)
- TVB-5403 (3MPX motorized lens bullet camera)
- TVB-5404 (3MPX motorized lens bullet camera)
- TVB-5405 (5MPX motorized lens bullet camera)

- TVD-5401 (2MPX low light indoor mini dome)
- TVD-5402 (3MPX motorized lens mini indoor dome)
- TVD-5403 (5MPX indoor mini dome)
- TVD-5404 (2MPX low light motorized lens dome)
- TVD-5405 (2MPX low light motorized lens dome)
- TVD-5406 (3MPX WDR motorized lens dome)
- TVD-5407 (3MPX WDR motorized lens dome)
- TVD-5408 (5MPX motorized lens mini dome)

Default settings to access the camera

Default credentials

The camera comes with a user account with administrative rights for configuring all options on the camera. The user name is “admin” and the password is “1234”. It is highly recommended that the default password be changed during initial setup for enhanced security.

Default network settings

The network settings are:

- IP address: 192.168.1.70
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.1.1

Ports used:

Browser	TruVision Navigator
RTSP: 554	RTSP: 554
HTTP: 80	Server/client control port: 8000

Please see “Overview of the camera web browser” on page 6 for further information.

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 may not be able to download data, such as video and images, due to the browser's security settings. Consequently you should check the security level of your browser 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 users

Internet Explorer for Windows 7, Windows 8, and Windows 10 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, Windows 8, and Windows 10 do the following:

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

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

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

Accessing the camera over the network

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

It is recommended that you change the administrator password once the setup is complete. Only authorized users should be able to modify camera settings. See "User management" on page 67 for further information.

To access the camera online:

1. In the web browser enter the camera's IP address (default is 192.168.1.70). Use the TruVision Device Manager included on the CD to find the IP address of the camera and assign it a new address on the local network, if desired.

   The Login dialog box appears.

   Note: Ensure that the Active X controls are enabled.
2. Enter your user name and password.

   User name: admin

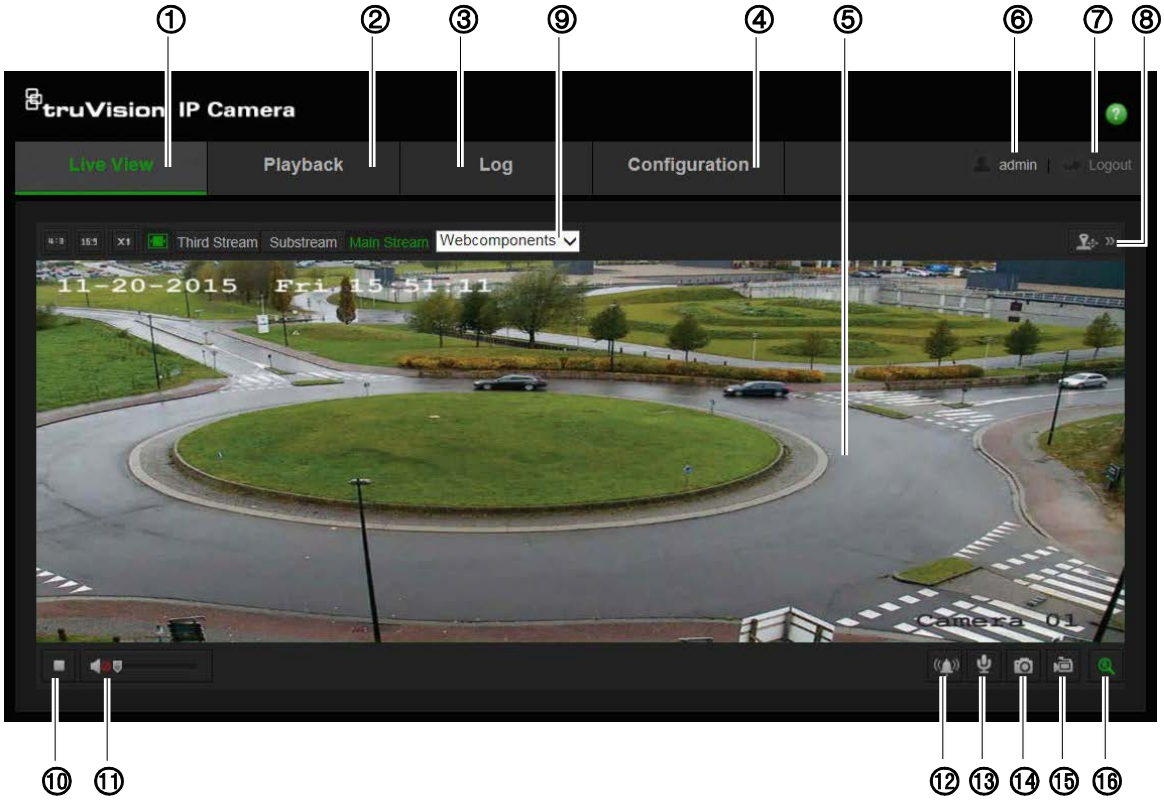
   Password: 1234
3. Click **Login**. The web browser window appears in live view mode.

Overview of the camera web browser

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

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

Figure 1: Web browser interface



Name		Description
1.	Live view	Click to view live video.
2.	Playback	Click to play back video.
3.	Log	Click to search for event logs. There are three main types: Alarm, Exception and Operation.
4.	Configuration	Click to display the configuration window for setting up the camera.
5.	Viewer	View live video. Time, date and camera name are displayed here.
6.	Current user	Displays current user logged on.
7.	Logout	Click to log out from the system. This can be done at any time.
8.	PTZ controls	Direction actions, zoom, focus, iris, light and wiper control. **Note**: Direction actions, light, and wiper control can be used if the camera supports RS-485 and external pan/tilt unit, light or wiper is installed.
9.	Display Control	Click each tab to adjust the layout and the stream type of the live view. You can also click the drop-down menu to select the plug-in. For IE (internet explorer) users, web components and QuickTime® are selectable. For non-IE users, web components, QuickTime, VLC or MJPEG are selectable, if they are supported by the web browser.
10.	Start/stop live view	Click to start/stop live view.
11.	Audio	Adjust the volume.
12.	Manual alarm	Turn on/off the alarm
13.	Bidirectional audio	Turn on/off the local microphone (if supported).
14.	Capture	Click to take a snapshot of the video. The snapshot will be saved to the default folder in JPEG or BMP format.

Name		Description
15.	Start/stop recording	Click to record live video.
16.	Digital zoom	Click to enable digital zoom.

Camera configuration

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

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

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

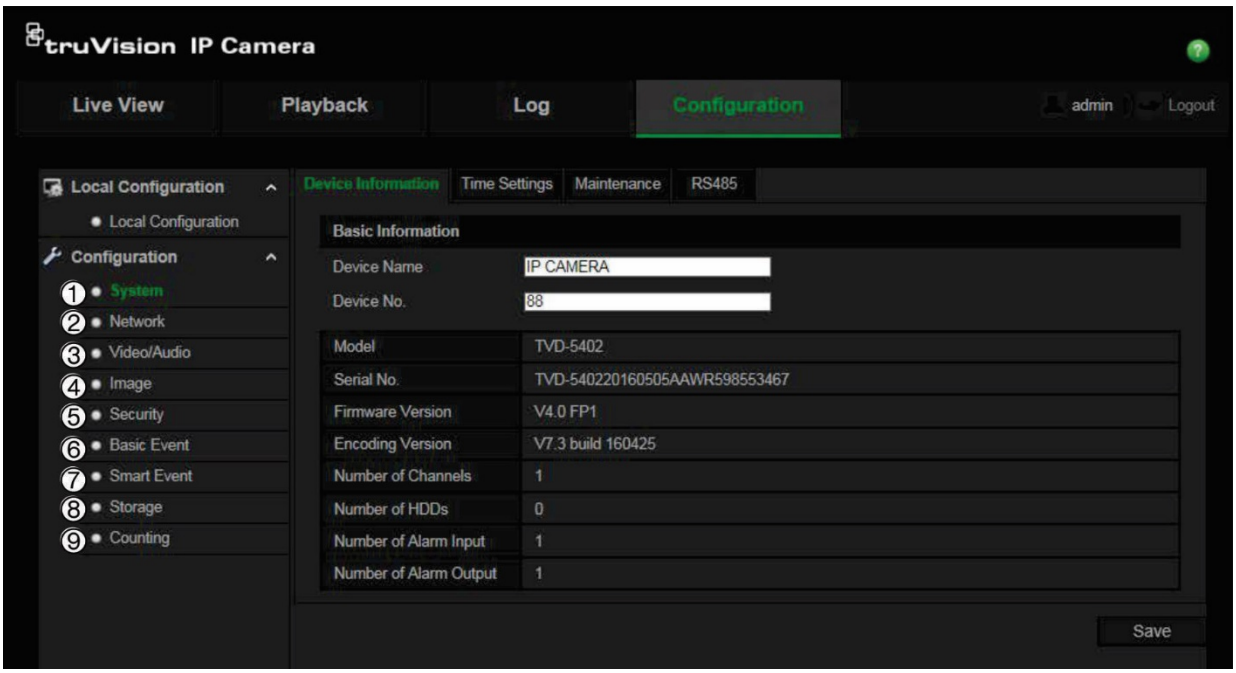
There are two main menus in the configuration panel:

- Local configuration
- Configuration

Configuration menu overview

Use the Configuration panel to configure the network, camera settings, 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 (Device Information tab selected)



Configuration menus		Description
1.	System	Defines basic device information including SN, the current firmware version, time settings, maintenance, and serial port parameters. See "System time" on page 12 for further information.
2.	Network	Defines the parameters required to access the camera over a network. See "Network settings" on page 13 for further information on the setup.
3.	Video/Audio	Defines recording parameters.

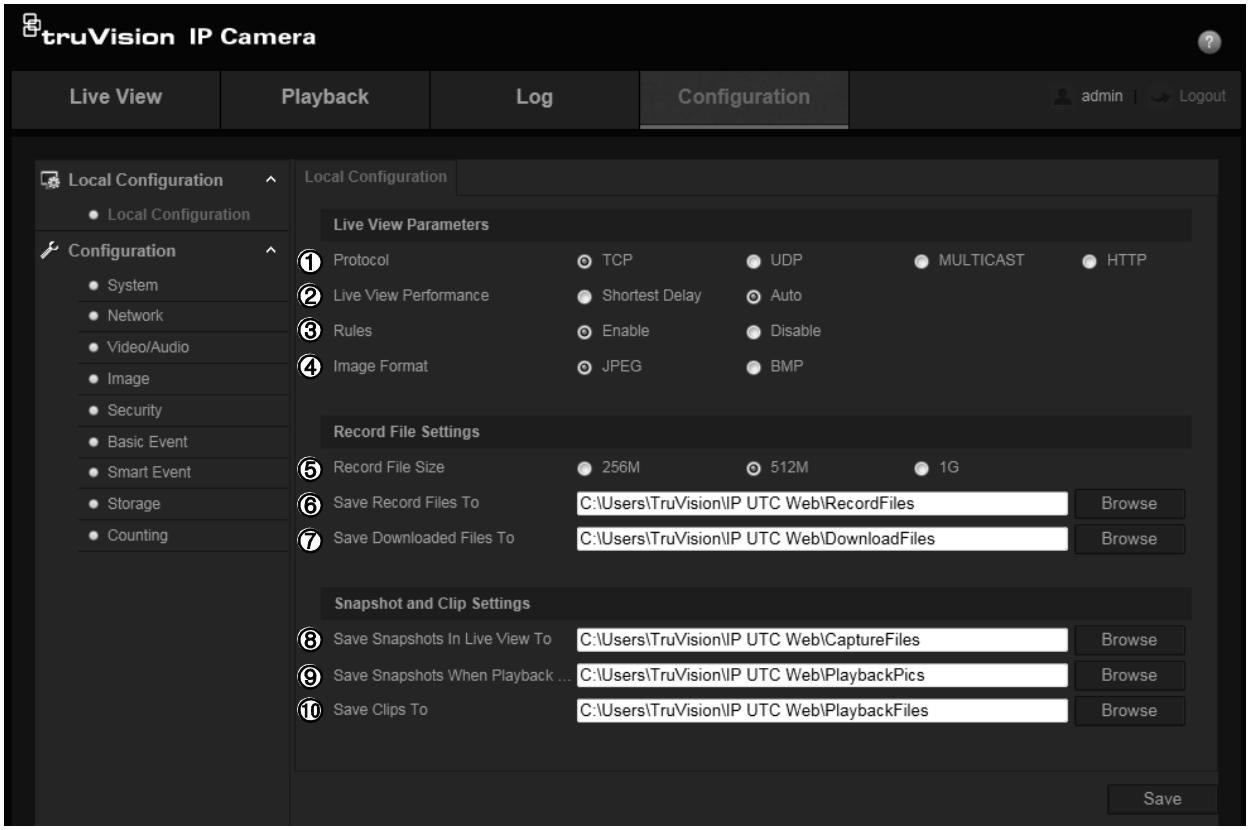
Configuration menus		Description
4.	Image	Defines the image parameters, OSD settings, overlay text, and privacy mask. See “Video image” on page 25 for further information on the setup.
5.	Security	Defines who can access and use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and SSH.
6.	Basic Event	Defines Motion Detection, Tamper-proof, Alarm Input/Output, and Exceptions. See “Motion detection alarms” on page 32, “Tamper-proof alarms” on page 38, and “Exception alarms” on page 39.
7.	Smart Event	Defines Defocus Detection, Scene Change Detection, Face Detection, Cross Line, Intrusion Detection, Region Entrance Detection, Region Exiting Detection, Unattended Baggage Detection, and Object Removal Detection.
8.	Storage	Defines recording schedule, storage management, NAS configuration and snapshot.
9.	Counting	Defines the people/object counting parameters.

Local configuration

Use the Local menu to manage the protocol type, live view performance, and local storage paths on your computer.

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



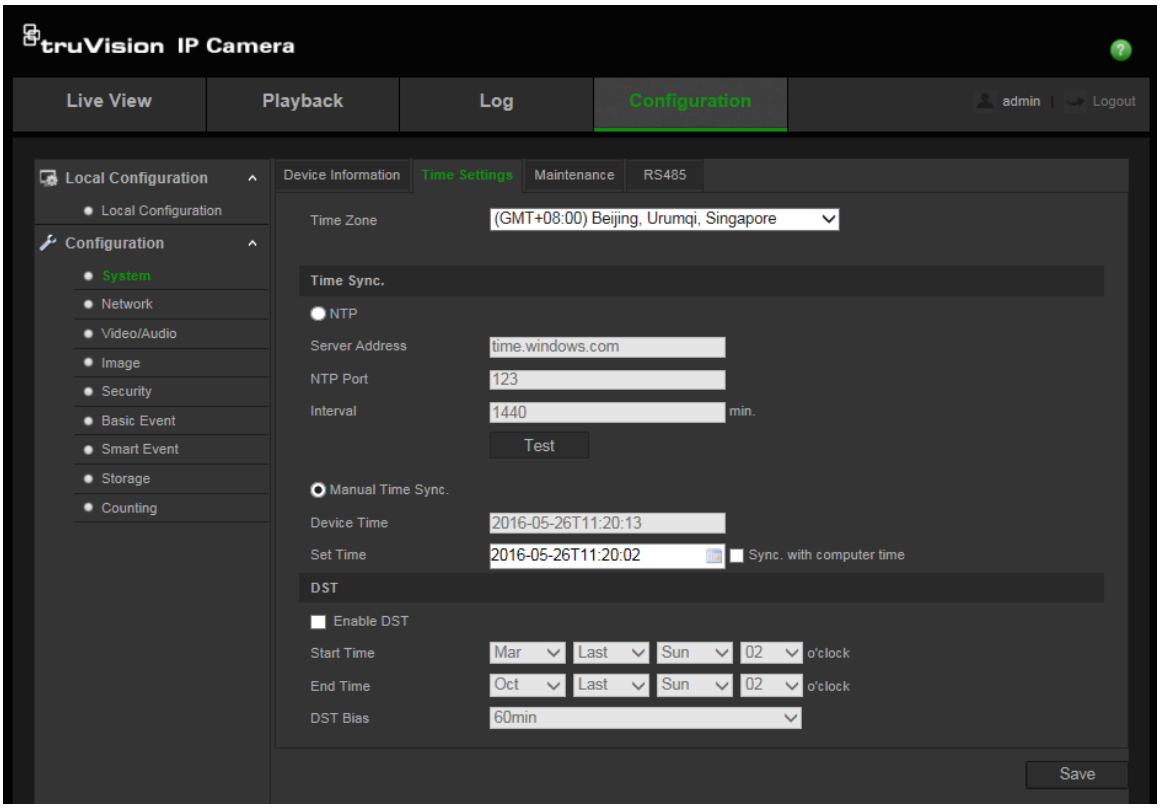
Parameters		Description
Live View Parameters		
1.	Protocol	Specifies the network protocol used. Options include: TCP, UDP, MULTICAST and HTTP.
2.	Live View Performance	Specifies the transmission speed. Options include: Shortest Delay or Auto.
3.	Rules	Enable or disable the display of intelligent metadata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

System time

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

To define the system time and date:

1. From the menu toolbar, click **Configuration** > **System** > **Time Settings**.



2. From the **Time Zone** drop-down menu, select the time zone that corresponds to the camera's location.
3. Under **Time Sync**, check one of the options for setting the time and date:

   Synchronize with an NTP server: Check the **NTP** enable box and enter the server NTP address. The time interval can be set from 1 to 10080 minutes.

   - or -

   Set manually: Enable the **Manual Time Sync** function and then click  to set the system time from the pop-up calendar.

   Note: You can also check the **Sync with computer time** checkbox to synchronize the time of the camera with the time of your computer.
4. Check **Enable DST** to enable the DST (Daylight Savings Time) function, and set the date of the DST period.
5. Click **Save** to save changes.

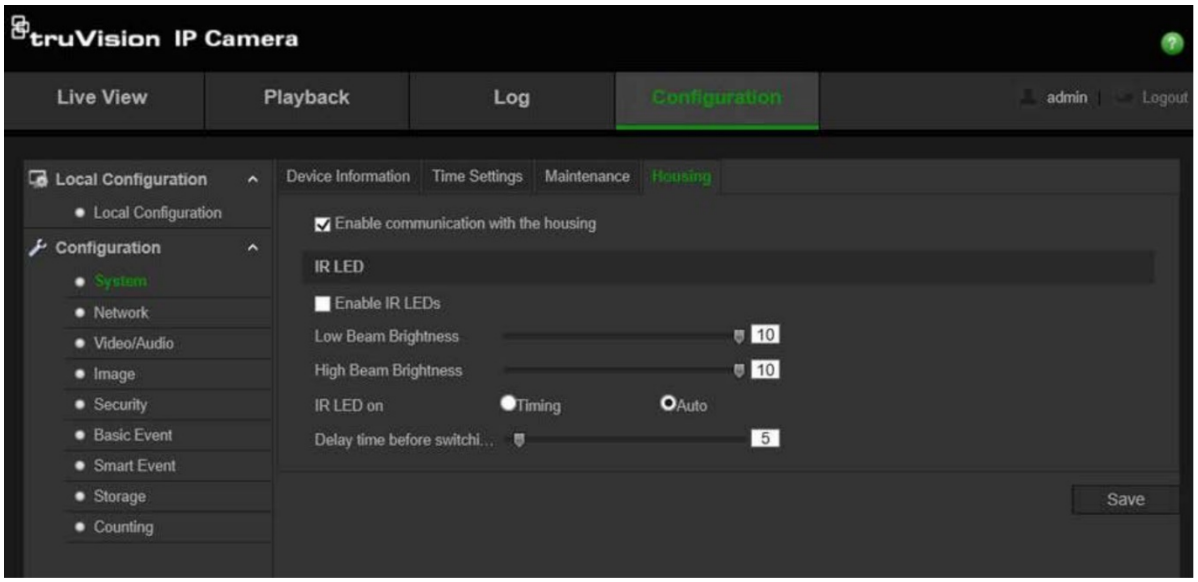
IR LED settings for the TVC-OH3-HT housing

You can control the IR illumination of the TVC-OH3-HT housing by selecting its brightness and when it turns on and off.

When this feature is enabled, the RS-485 is then automatically set up by the camera. A confirmation dialog is displayed to confirm that the housing IR illumination has been enabled and the camera automatically reboots.

To define the IR LEDs of the TVC-OH3-HT housing:

1. From the menu toolbar, click **Configuration** > **System** > **Housing**.
2. Select **Enable communication with the housing**.



3. Select the **Enable IR LEDs** check box and then configure the IR illumination parameters.
   a. Adjust the low and high beam brightness, as required.
   b. Under *IR LED on:*

      Select **Auto** to control the IR LEDs by photoresistance and then adjust the filtering time to select the delay for switching the IR LEDS on/off when the light level changes. The range is between 0 to 120 seconds.

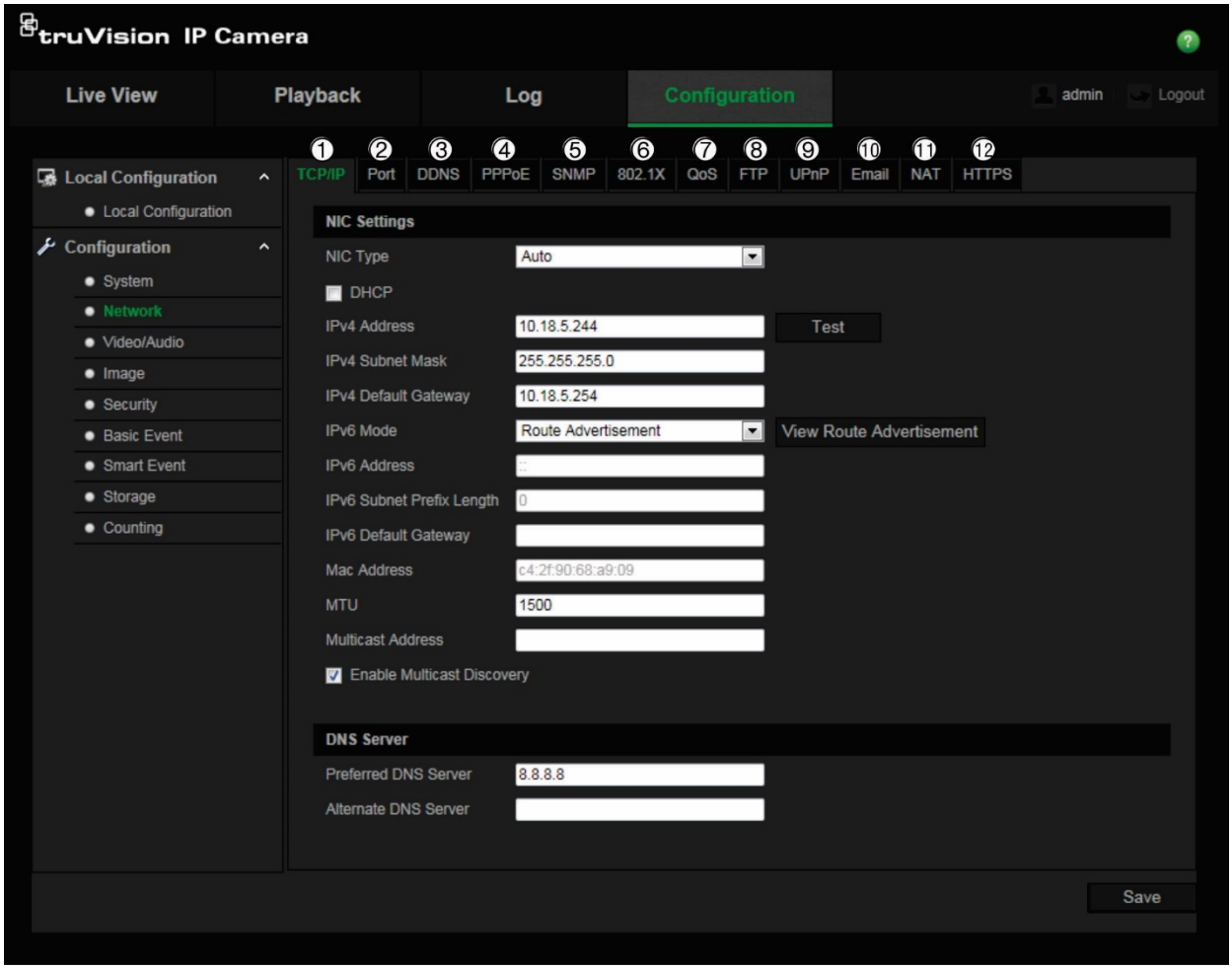
      – or –

      Select **Timing** to set up the start and end times of when the IR LEDs turn on.
4. 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 4 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. **Enable Multicast Discovery**: Enables the automatic detection of the online network camera via private multicast protocol in the LAN. **DNS server:** Specifies the DNS server for your network.

Menu tabs		Description
		See page 16 for setup information.
2.	Port	**HTTP Port:** The HTTP port is used for remote 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 Server IP**: Specifies the IP address of the alarm host. **Alarm Server Port**: Specifies the port of the alarm host. See page 16 for setup information.
3.	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 IP server, DynDNS, and ezDDNS. **DynDNS (Dynamic DNS**): Manually create your own host name. You will first need to create a user account using the hosting web site, DynDNS.org. **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. **IPServer**: Enter the address of the IP Server. See page 16 for setup information.
4.	PPPoE	Retrieves a dynamic IP address. See page 17 for setup information.
5.	SNMP	SNMP is a protocol for managing devices on networks. Enable SNMP to get camera status and parameter related information. See page 17 for setup information.
6.	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.
7.	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 18 for setup information.
8.	FTP	Enter the FTP address and folder to which snapshots of the camera can be uploaded. See page 17 for setup information.
9.	UPnP	The UPnP (Universal Plug and Play) protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments. With the function enabled, you do not need to configure the port mapping for each port, and the camera is connected to the Wide Area Network (WAN) via the router. Enable and set the friendly name detected. See page 19 for setup information.
10.	Email	Enter the email address to which messages are sent when an alarm occurs. See page 19 for setup information.

Menu tabs	Description
11. NAT	A NAT (Network Address Translation) is used for network connection. Select the port mapping mode: auto or manual. See page 20 for setup information.
12. HTTPS	Specifies authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

To define the TCP/IP parameters:

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

To define the port parameters:

1. In **Configuration** > **Network**, click the **Port** tab to open its window.
2. Set the HTTP port, RTSP port, HTTPS port and Server port of the camera.

   HTTP Port: The default port number is 80, and it can be changed to any port No. which 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 check the **Notify Alarm Recipient** option in the normal Linkage of each event page.
4. Click **Save** to save changes.

To define the DDNS parameters:

1. From the menu toolbar, click **Configuration** > **Network** > **DDNS**.
2. Check **Enable DDNS** to enable this feature.
3. Select **DDNS Type**. Two options are available: DynDNS and IPServer.

- Select **DDNS Type**. Select one of the follow options:
  - **DynDNS:** Enter the DDNS 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 DynDNS account. The domain name displayed under “Host Name” is that which you created on the DynDNS web site.

- **ezDDNS:** Enter the desired host name under “Host Name”. The default host name is utc-serial number. The new host name is registered when you click Save.

Note: The default server address is www.tvr-ddns.net, which cannot be changed.

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

To define the PPPoE parameters:

1. From the menu toolbar, click **Configuration** > **Network** > **PPPoE**.
2. Check **Enable PPPoE** to enable this feature.
3. Enter User Name, Password, and Confirm password for PPPoE access.
4. Click **Save** to save changes.

To define the SNMP parameters:

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

Note: Before configuring SNMP, test your SNMP monitoring software and attempt to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the SNMP monitoring software. The SNMP version you select should be the same as that supported by the SNMP software.

To define the 802.1x parameters:

1. From the menu toolbar, click **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 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.

To define the QoS parameters:

1. From the menu toolbar, click **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 bigger the DSCP value, the higher the priority.
3. Click **Save** to save changes.

To define the FTP parameters:

1. You must have an FTP server configured and available on the network in order to use the FTP feature
2. From the menu toolbar, click **Configuration** > **Network** > **FTP**.
3. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.

   Anonymous: Check the checkbox to enable the anonymous access to the FTP server.

   Directory: In the Directory Structure field, you can select the root directory, Main directory and Subdirectory. When the Main directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the

directory; and when the Subdirectory is selected, you can use the Camera Name or Camera No. as the name of the directory.

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

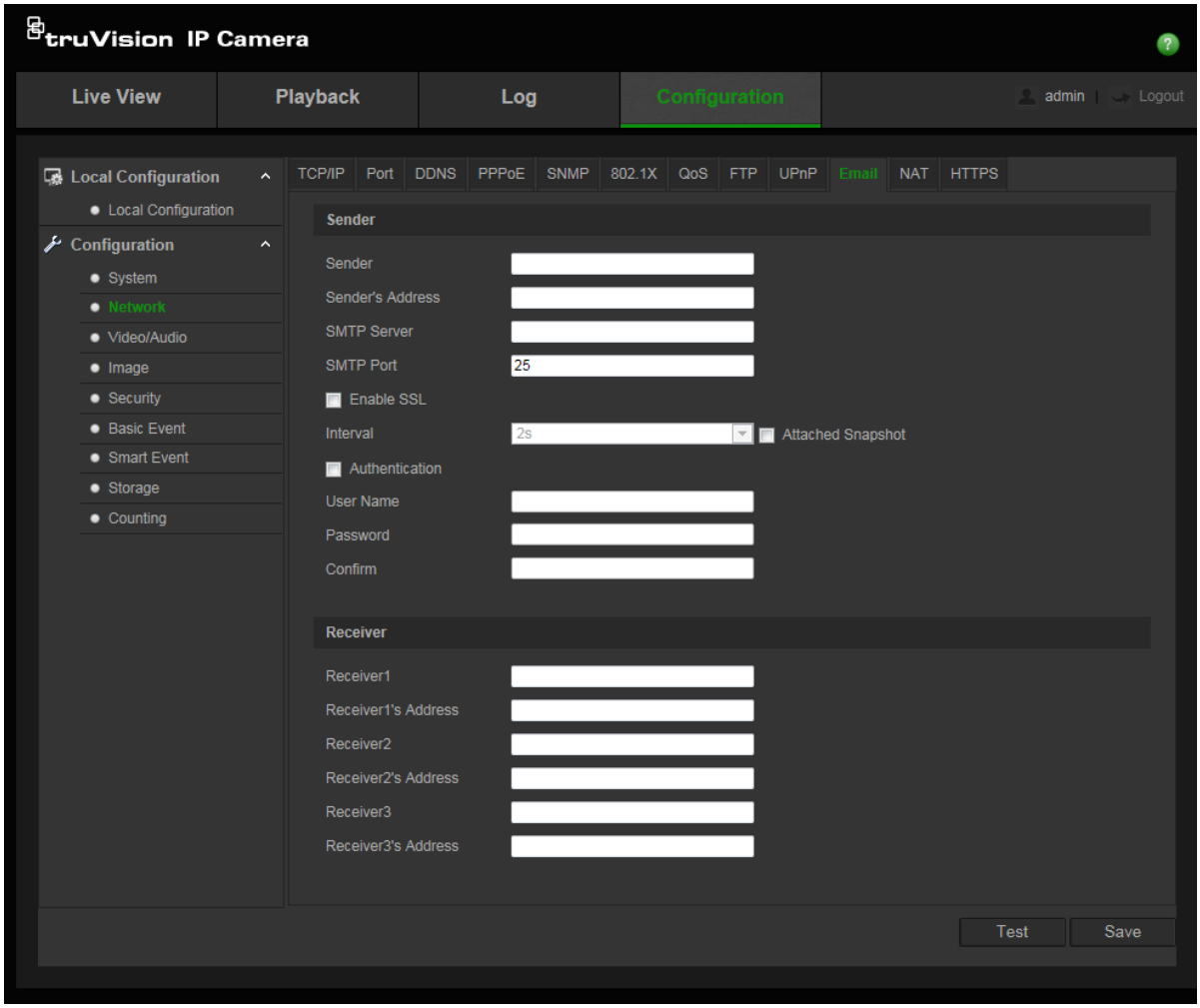
4. Click **Save** to save changes.

To define the UPnP parameters:

1. Click **Configuration** > **Network** > **UPnP**.
2. Check the checkbox to enable the UPnP function. The name of the device when detected online can be edited.
3. Click **Save** to save changes.

To set up the email parameters:

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



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.

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

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

I**nterval:** This is the time between two actions of sending attached images.

Authentication: If your email server requires authentication, check this checkbox 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 images 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 the first user to be notified.

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

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

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

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

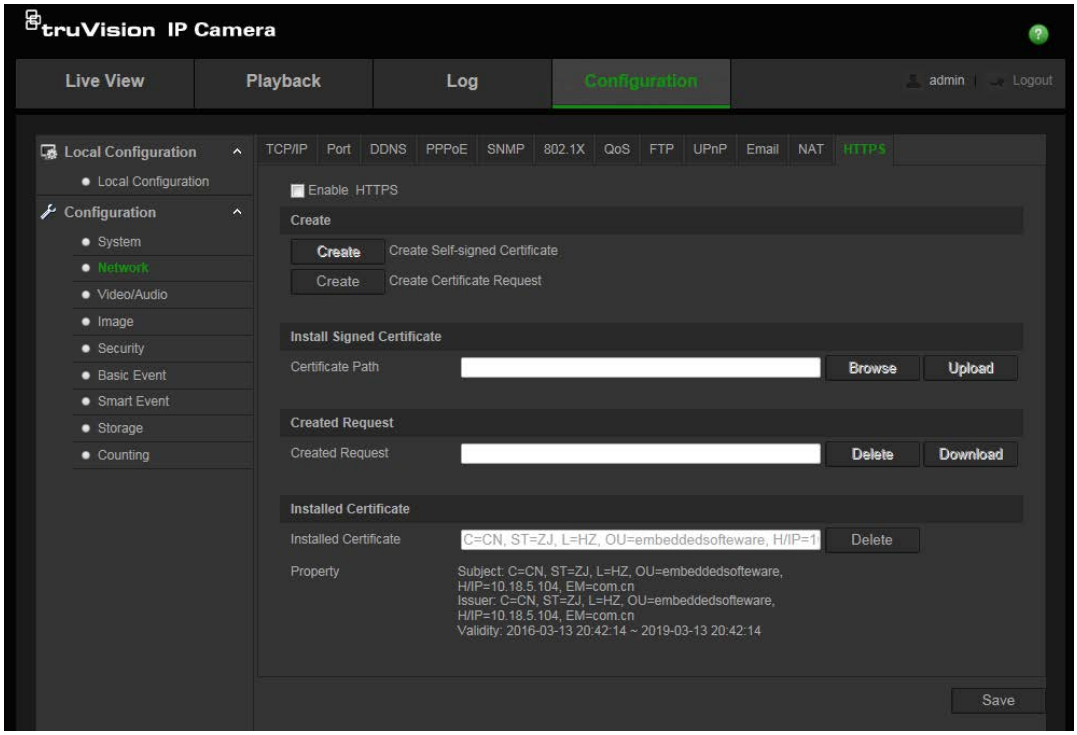
3. Click **Test** to test the email parameters.
4. Click **Save** to save changes.

To set up the NAT parameters:

1. Click **Configuration** > **Network** > **NAT**.
2. Check the checkbox to enable the NAT function.
3. Select **Port Mapping Mode** to be Auto or Manual. When you choose Manual mode, you can configure an external port of your choice.
4. Click **Save** to save changes.

To set up the HTTPS parameters:

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



2. **To create a self-signed certificate**:

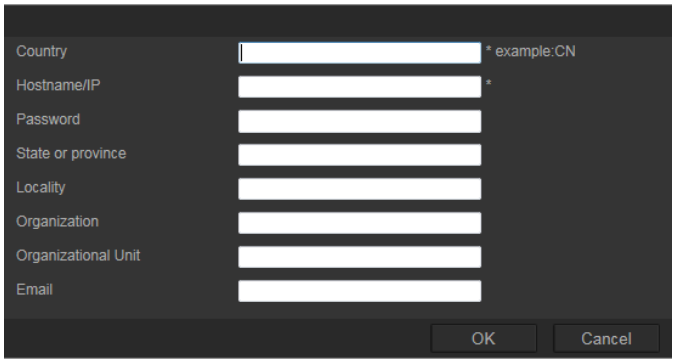
   Click the **Create** button beside “Create Self-signed Certificate”. Enter the country, host name/IP, validity and the other information requested.

   Click **OK** to save the settings.

   -Or-

   To create a certificate request:

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

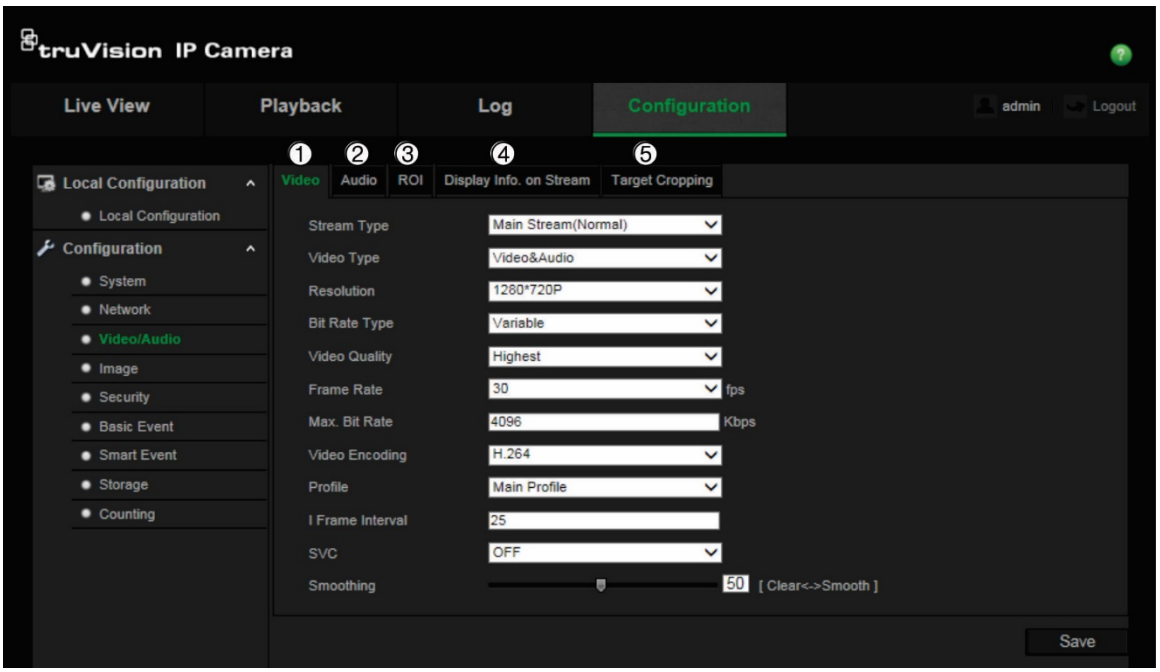


3. Click **OK** to save the settings. Download the certificate request and submit it to the trusted certificate authority for signature, such as Symantec or RSA. After receiving the signed valid certificate, upload the certificate to the device

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 5 below list the video and audio recording options you can configure for the camera.

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

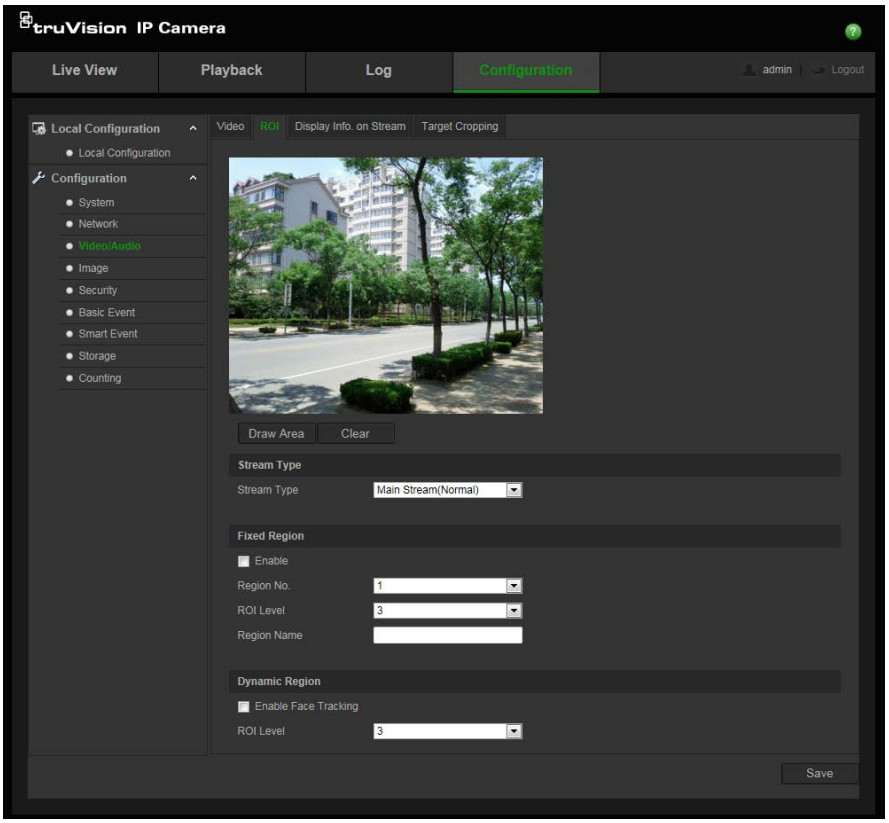


Tab		Parameter descriptions
1.	Video	**Stream Type**: Specifies the streaming method used. Options include: Main Stream (Normal), Sub Stream and Third stream.
		Video Type: Specifies the stream type you wish to record. Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams. **Note**: Video&Audio is only available for those camera models that support audio.

Tab		Parameter descriptions
		Resolution: Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. The resolution options listed depend on the type of camera and on whether main or sub stream is being used. **Note**: Resolutions can vary depending on the camera model.
		Bitrate Type: Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.
		Video Quality: Specifies the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, Medium, Higher and Highest.
		Frame Rate: Specifies the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second. **Note**: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications on its datasheet.
		Max bit rate: Specifies the maximum allowed bit rate. To maintain image quality for high image resolution, a high bit rate must also be selected.
		Video Encoding: Specifies the video encoding used.
		Profile: Different profile options indicate different tools and technologies used in compression. Options include: High Profile, Main Profile and Basic Profile.
		I Frame Interval: A video compression method. It is strongly recommended not to change the default value 50.
		SVC: 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. This setting allows for balancing of fluid movement with sharpness of resolution.
2.	Audio	**Audio Encoding**: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726 and PCM are optional.
		Audio Input: Select “LineIn” or “MicIn”
		Input Volume: Specifies the volume from 0 to 100.
		Environmental Noise Filter: Set it as OFF or ON. Enable the function to filter background ambient noise.
3.	ROI	Enable to assign more encoding resources to the region of interest to increase the quality of the ROI whereas the background information is less focused when network performance is less than optimal.
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.
5.	Target Cropping	You can specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

To configure ROI settings:

1. From the menu toolbar, click **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.
6. Enable **Dynamic Region** for face tracking. The ROI will change, depending upon where faces are detected in the scene.

   ROI Level: Choose the image quality enhancing level.
7. Click **Save** to save changes.

Dual-VCA (Video Content Analysis)

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

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

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

To define Dual-VCA parameters:

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

Target Cropping

You can specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

Note: Target cropping function varies according to different camera models.

To define Target Cropping:

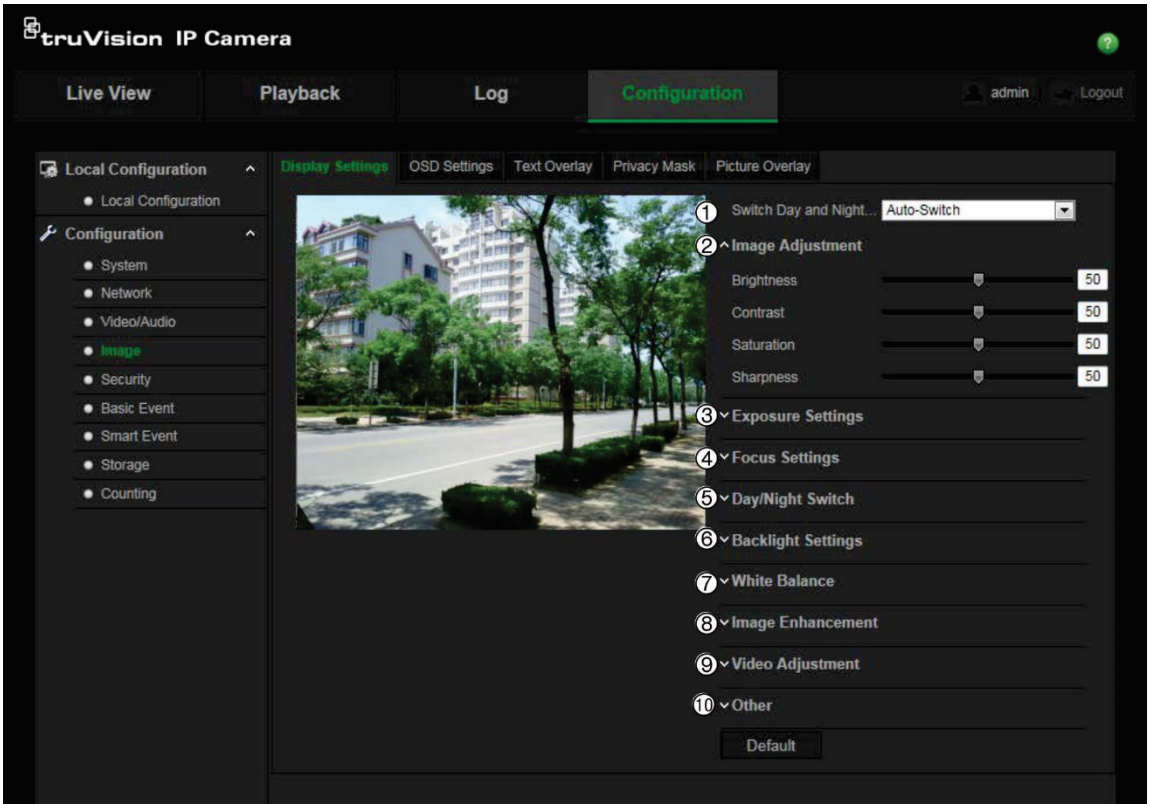
1. Enter the Target Cropping settings interface.
2. Check **Enable Target Cropping** checkbox to enable the function.
3. Set *Third Stream* as the stream type.
4. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
5. Click **Save** to save the settings.

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 6 below.

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. See Figure 6 below for more information.

Figure 6: Camera image settings menu – Display Settings tab



Parameter	Description
1. Switch Day and Night Settings	
Auto-Switch	The camera automatically switches between day and night mode. All image settings remain the same for both modes.
Scheduled 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 Image Adjustment, Exposure, Day/Night Switch, Video Adjustment, and Other. *Day*: Configure the Backlight, White Balance and Image Enhancement settings for day mode only. *Night*: Configure the Backlight, White Balance and Image Enhancement settings for night mode only.
2. Image Adjustment	
Brightness, Contrast Saturation, Hue, Sharpness	Modifies the different elements of picture quality by adjusting the sliders for each parameter.
3. Exposure Settings	
Iris Mode	There are two settings, Auto and Manual. The type of lens determines which setting is used. Default is Auto.
Auto Iris Level	Select the iris level, default is 50.

Parameter		Description
	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.
	Gain	Select the value to adjust the image brightness.
4.	**Focus Settings**	
	Focus mode	For cameras that support an electronic lens, you can set the focus mode as Auto, Manual or Semi-auto. If Auto is selected, the focus is adjusted automatically. If Manual is selected, you can control the lens by adjusting the zoom, focus, lens initialization, and auxiliary focus via the PTZ control interface. If semi-auto is selected, when you adjust focus manually, the camera will no longer focus automatically.
5.	**Day/Night Switch**	
	Day/Night Switch	Defines whether the camera is in day or night mode. The day (color) option should be used, for example, if the camera is located indoors where light levels are always good. 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 the day mode and the night mode according to the configured time period. **Triggered by Alarm Input**: The camera switches to the day mode or the night mode after the alarm is triggered.
	Sensitivity	Only available when Auto D/N switch mode is selected. It defines the sensitivity of the switch between day and night. You can set it between 0 and 7.
	Delay time	Only available when Auto D/N switch mode is selected. The filtering time refers to the interval time switching between day/night mode. You can set it between 5 and 120 s.
	Smart IR	When enabled, it can avoid over exposure of an image due to IR LED glare.
	IR Light	Select ON/OFF to Enable/disable IR. **Enable**: the IR illuminators will be ON when the camera switches to night mode. **Disable**: the IR illuminators will be OFF when the camera switches to night mode **Note**: The IR illuminators are always OFF in Daytime mode.
6.	**Backlight Settings**	
	BLC Area	If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates for the background light so that the image in the foreground is clear. OFF, Up, Down, Left, Right, and Center are selectable. When WDR is enabled, BLC cannot be configured.
	WDR	When enabled, this feature (wide dynamic range) allows you to see details of objects in shadows or details of objects in bright areas of frames that have high contrast between light and dark areas.

Parameter		Description
	HLC	High Light Compression function can be used when there are high light levels in the scene affecting the image quality.
7.	**White Balance**	
	White Balance	White balance (WB) sets the relative parameters for the color white in the camera. Based on this information, the camera will continue to display all colors correctly even when the color temperature of the scene changes such as from daylight to fluorescent lighting. Select one of the options: **MWB:** Manually adjust the color temperature to meet your requirements. **AWB1:** Adjust within a range of 2500 to 9500K, for environments where the lighting is always stable. **Locked WB:** Locks the WB to the current environment color temperature. **Incandescent Lamp:** For use with incandescent lighting. **Warm Light Lamp:** For use where the indoor light is warm. **Natural Light:** For use with natural light. **Fluorescent Lamp:** For use where there are fluorescent lamps installed near the camera.
8.	**Image Enhancement**	
	Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance. Options include: Normal Mode, Expert Mode, or OFF. Default is Normal.
	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.
	Time/Space DNR Level	Set the level of noise reduction level in Expert Mode. Default is 50. **Note**: If you set a higher value, the image may not be clear.
	Defog Mode	You can enable the defog function when the environment is foggy and obscures the image. It enhances the subtle details so that the image appears clearer.
	EIS	Electronic Image Stabilizer reduces the effects of camera vibration for the image.
	Grey Scale	You can choose the range of the grey scale from 0 to 255 or from16 to 235. Default is 0 to 255.
	Noise Reduction Level	Set the level of noise reduction. Higher value has a higher level of noise reduction. Default is 50.
9.	**Video Adjustment**	
	Mirror	Inverts the image. Options are Left/Right, Up/Down, Center, and OFF. Default is OFF.
	Hallway View	To invert the 16:9 aspect ratio, enable the rotate function. Best used when installing the camera in a scene with a narrow angle of view. During installation, turn the camera to 90 degrees or rotate the 3-axis lens to 90 degrees, and then set the rotate mode as 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.

Parameter	Description
Scene Mode	Choose the scene as indoor or outdoor according to the current environment.
Video Standard	50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.
Capture Mode	Set the desired frame rate to meet the different demands of field of view and resolution. A higher frame rate may be required in a location with a lot of movement (such as a money depot).
10. Other	
Local Output	Select ON or OFF to enable or disable the BNC output. Default is ON.

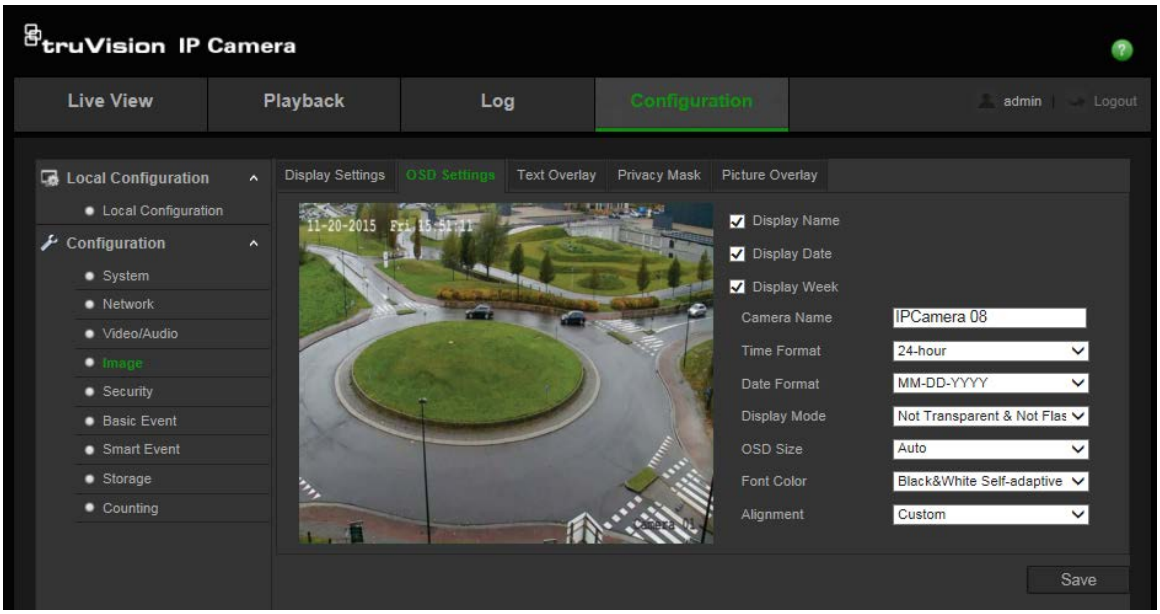
Note: Click the **Default** button to default all the image settings.

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** > **Image** > **OSD Settings**.



2. Check the **Display Name** box to display the camera's name on screen. You can modify the default name in the text box of **Camera Name**.
3. Check the **Display Date** box to display the date/time on screen.
4. Check the **Display Week** box to include the day of the week in the on-screen display.
5. In the **Camera Name** box, enter the camera name.
6. Select the time and date formats from the **Time format** and **Date format** list boxes.

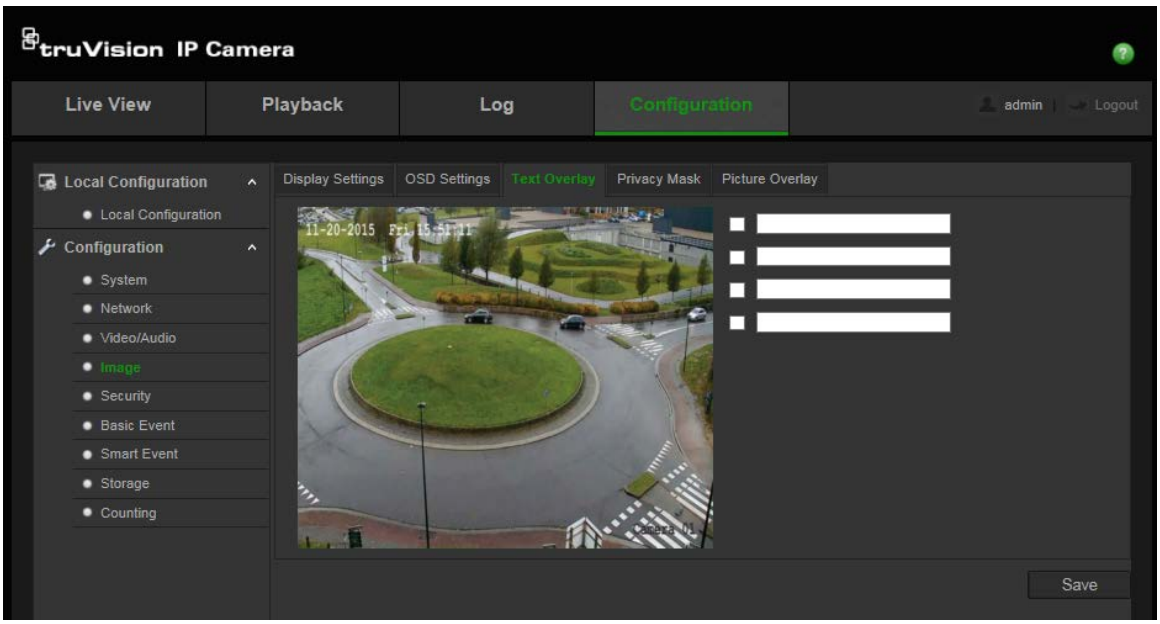
7. Select a display mode for the camera from the **Display Mode** list box. Display modes include:
   - **Transparent & Not flashing.** The image appears through the text.
   - **Transparent & Flashing**. **T**he image appears through the text. The text flashes on and off.
   - **Not transparent & Not 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 or Align Right).
11. Click **Save** to save changes.

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

Text overlay

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

Figure 7: Text overlay menu



To add on-screen text:

1. From the menu toolbar, click **Configuration** > **Image** > **Text Overlay**.
2. Check the box for the first line of text.
3. Enter the text in the text box.

4. Use the mouse to click and drag the red text in the live view window to adjust the text overlay position.
5. Repeat steps 2 to 4 for each extra line of text, selecting the next string number.

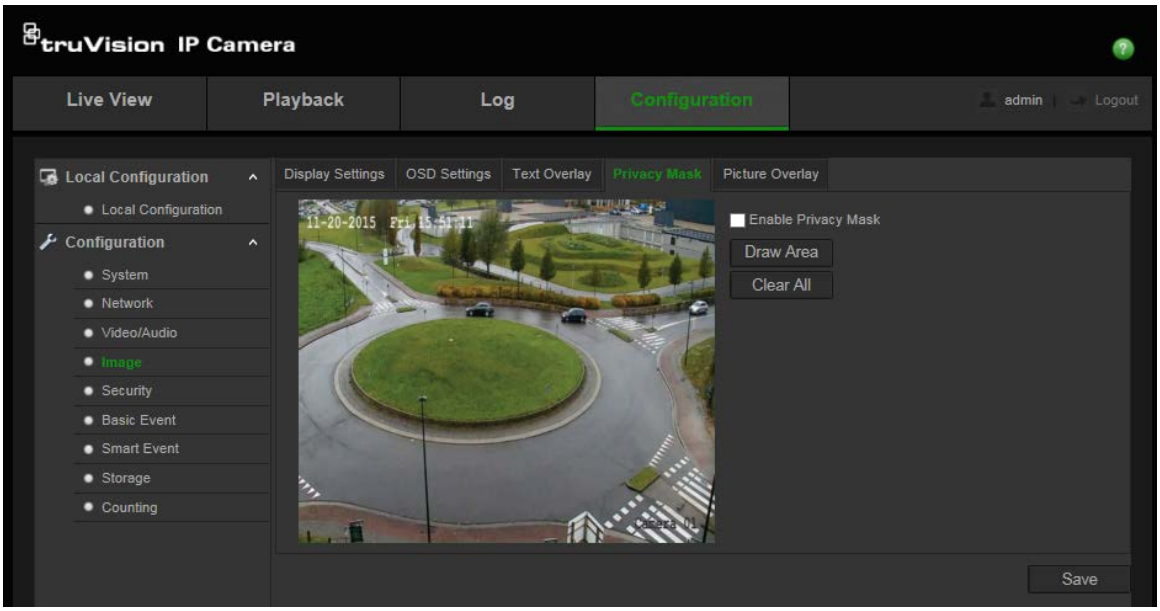
   Note: Remove an overlay text by deselecting its text line.
6. Click **Save** to save changes.

Privacy masks

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

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

Figure 8: Camera image settings menu – Privacy mask window



To add a privacy mask area:

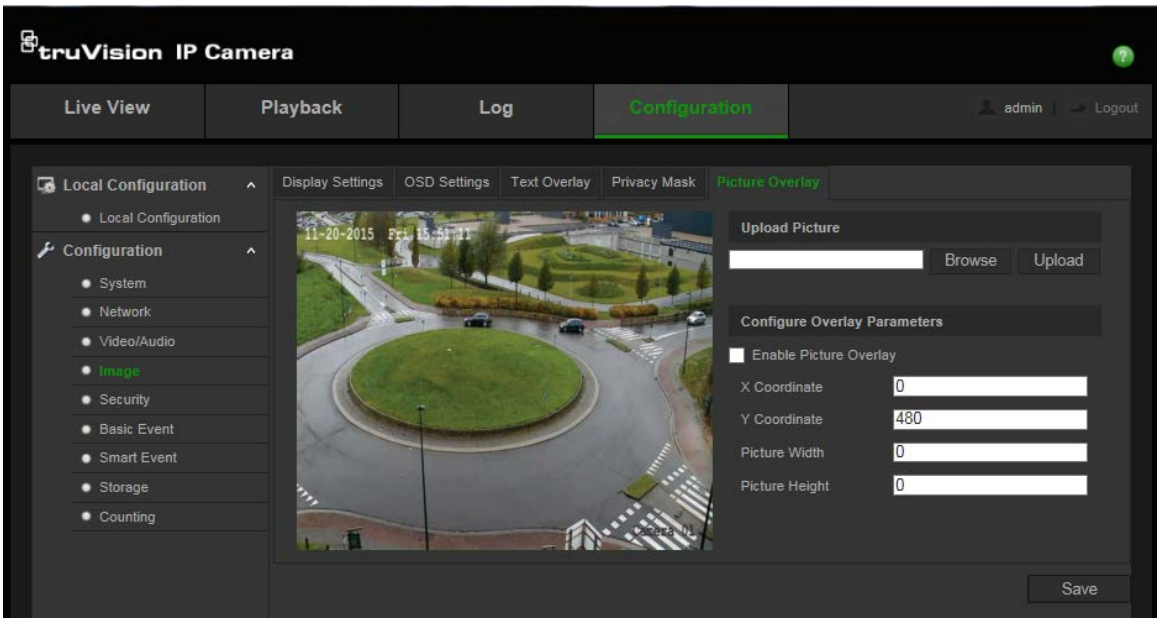
1. From the menu toolbar, click **Configuration** > **Image** > **Privacy Mask**.
2. Check **Enable Privacy Mask**.
3. Click **Draw Area**.
4. Click and drag the mouse in the live video window to draw the mask area.

   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.

Picture overlay

Picture overlay enables you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image. The picture must be in RGB24 bmp format and the maximum size of the picture is 128*128.

Figure 9: Camera image settings menu



To add a picture:

1. From the menu toolbar, click **Configuration** > **Image** > **Picture Overlay**.
2. Click **Browse** to select a picture and **Upload** to upload it.
3. Check **Enable Picture Overlay** checkbox to enable the function.

   Note: X coordinate and Y coordinate values are for the location of the picture on the image. The Picture width and height shows the size of the picture.

Motion detection alarms

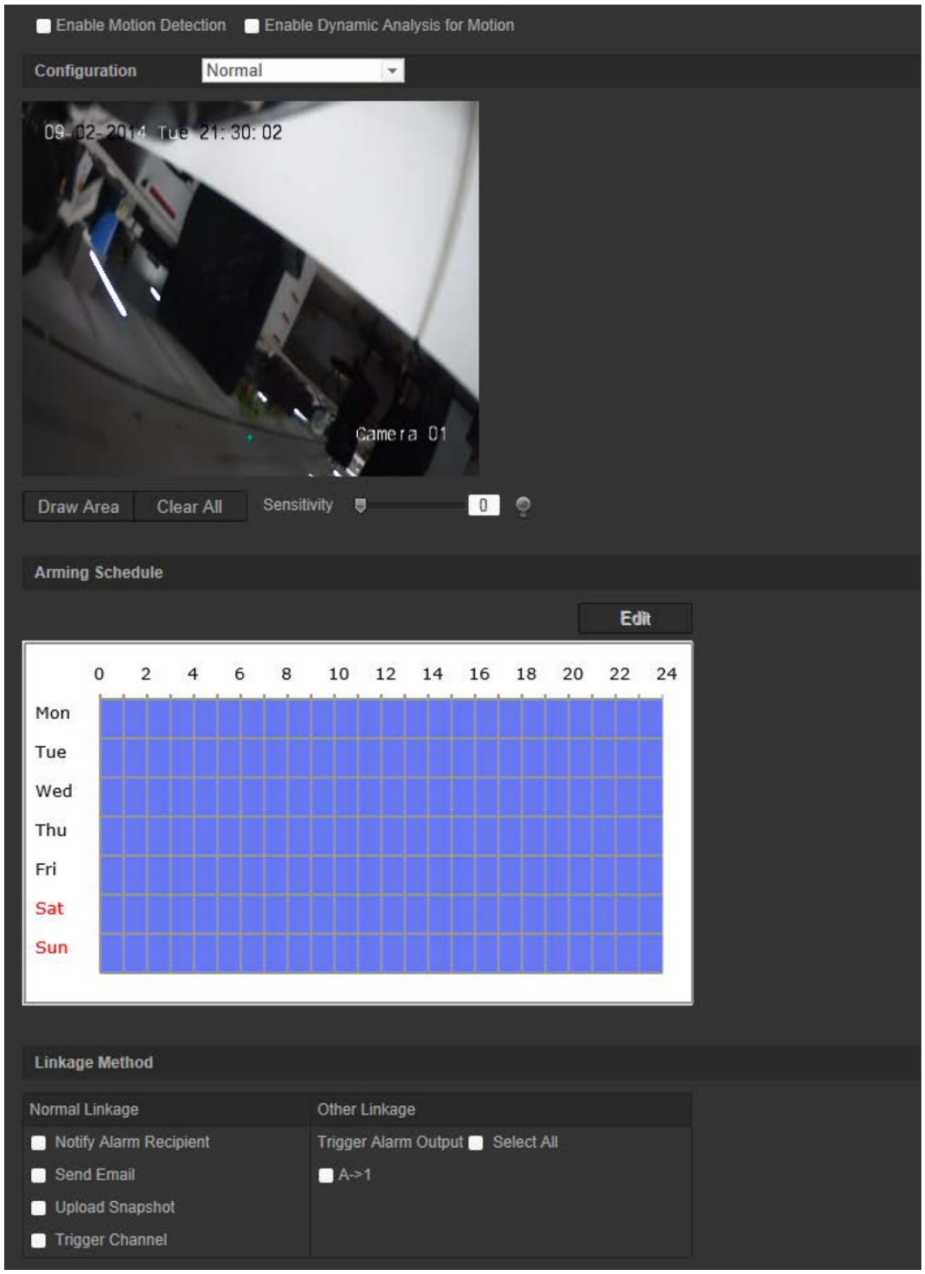
You can define motion detection alarms. A motion detection alarm refers to an alarm triggered when the camera detects motion. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

Select the level of sensitivity to motion as well as the target size so that only objects 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 small animal.

You can define the area on screen where the motion is detected, the level of sensitivity to motion, the schedule for the configured level of sensitivity 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 10: Motion detection window (Normal configuration mode shown)



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 10, item 1).
2. **Arming schedule**: Define the schedule during which the system detects motion (see Figure 10, item 2).
3. **Recording schedule**: Define the schedule during which motion detection will be recorded. See “Recording schedule” on page 62 for further information.
4. **Linkage**: Specify the method of response to the alarm (see Figure 10, item 3).
5. **Normal and advanced configuration**: Normal configuration allows you to set the sensitivity level of the motion detection. Advanced configuration gives you much more control over how motion is detected. It lets you set the sensitivity level as well

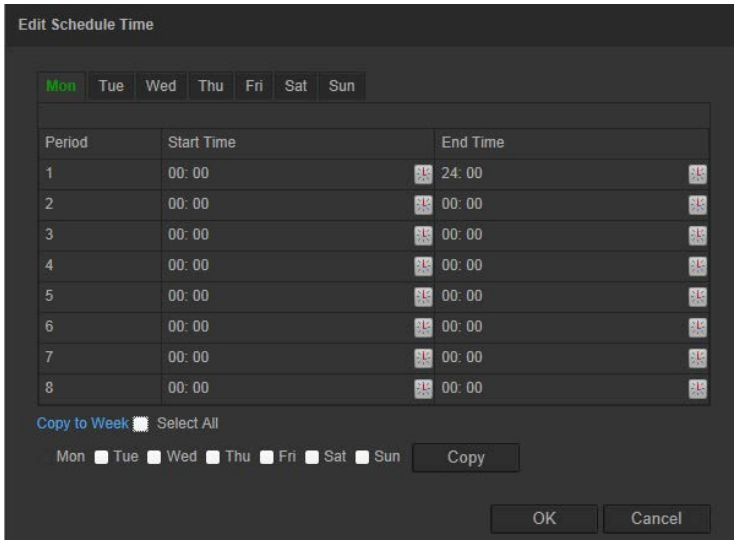
as define the percentage of the motion detection area that the object must occupy, select day or night mode, and set up eight differently configured defined areas.

To set up motion detection in normal mode:

1. From the menu toolbar, click **Configuration** > **Basic Event** > **Motion Detection**.
2. Check the **Enable Motion Detection** box. Check **Enable Dynamic Analysis for Motion** if you want to see real-time motion events.

   Note: Select **Disable** for rules in local configuration menu if you do not want the detected objected displayed with the rectangles.
3. Select **Normal** mode from the drop down menu.
4. Click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

   Note: You can draw up to 8 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. Click **Edit** to edit the arming schedule. See below for the editing interface of the arming schedule.



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

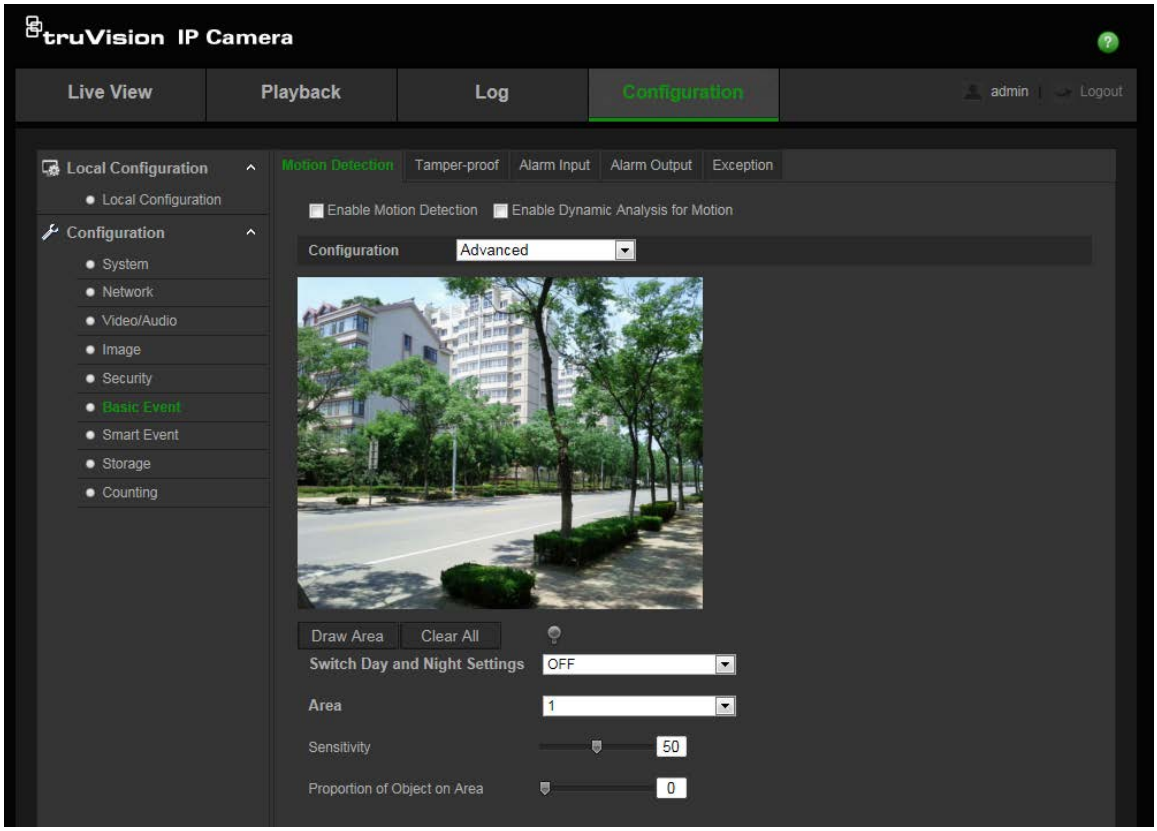
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera when an SD card is installed.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note:** This option is only supported by cameras that feature an alarm output.

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

To set up motion detection in advanced mode:

1. From the menu toolbar, click **Configuration** > **Basic Event** > **Motion Detection**.
2. Check the **Enable Motion Detection** box. Check **Enable Dynamic Analysis for Motion** if you want to see where motion occurs in real-time.

   Note: Select Local Configuration > Rules > Disable if you do not want the detected objects displayed with the green rectangles.
3. Select **Advanced** mode from the drop down menu.



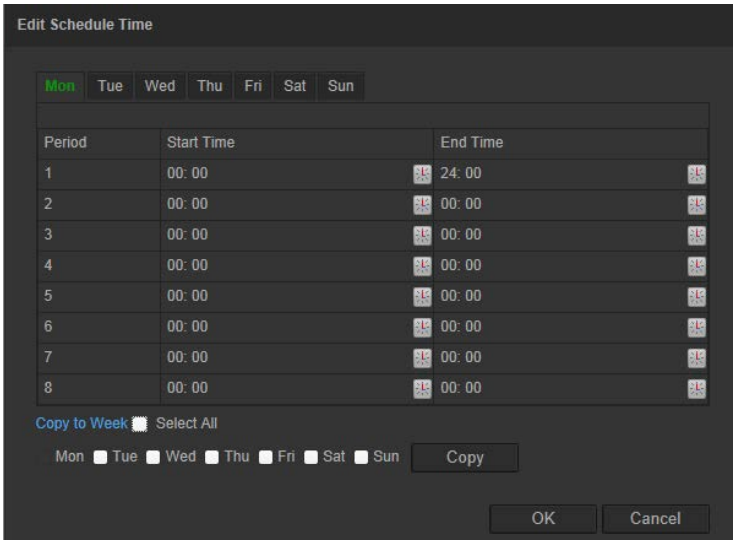
4. Under **Switch Day and Night Settings**, select OFF, Auto-switch or Scheduled-switch. Default is OFF.

   Auto-switch and Scheduled-switch 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.

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 **Proportion of Object on Area** 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. See the picture below for the editing interface of the arming schedule.



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

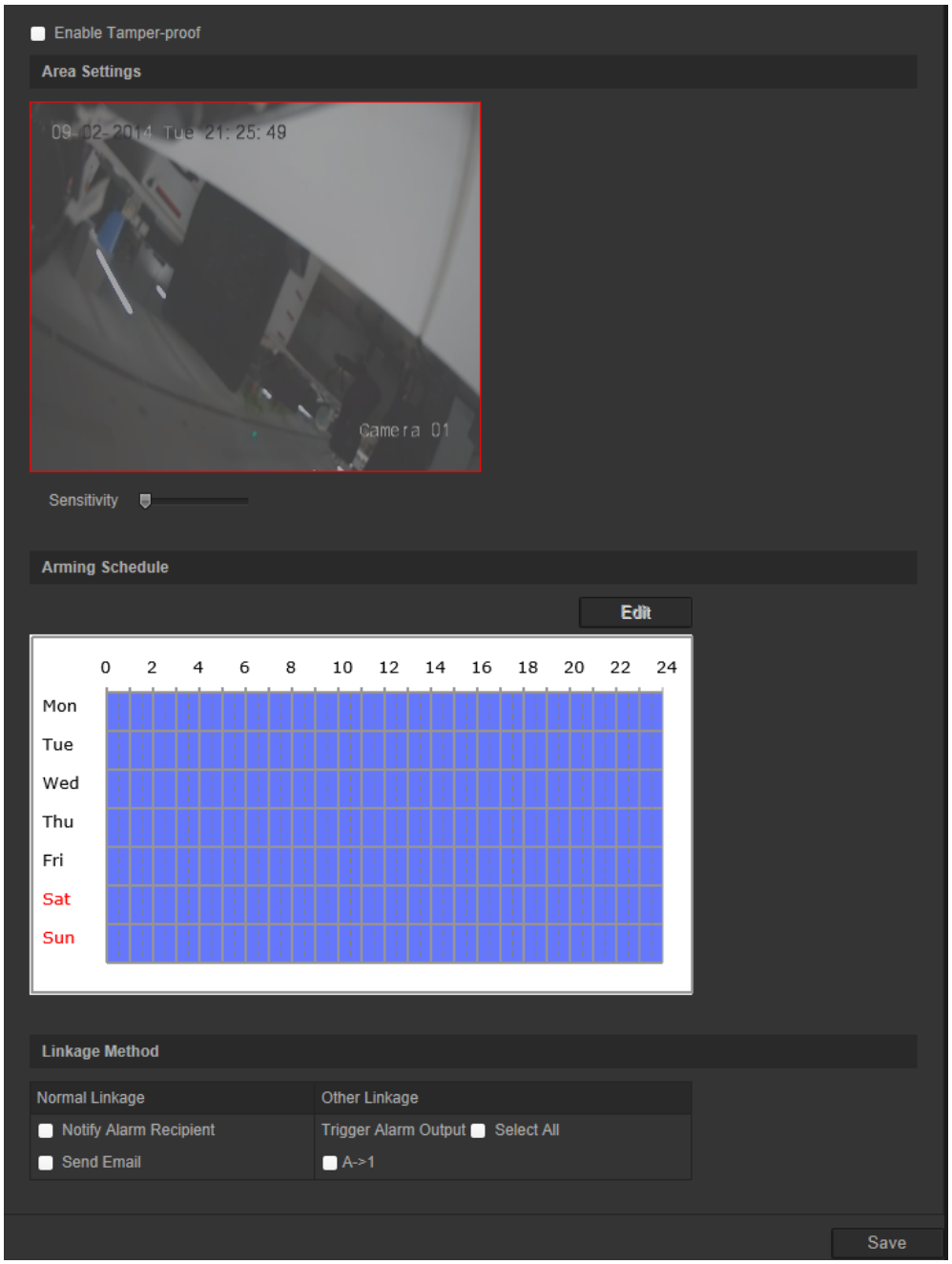
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

15. Click **Save** to save changes.

Tamper-proof alarms

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

Figure 11: Tamper-proof alarm window



To set up tamper-proof alarms:

1. From the menu toolbar, click **Configuration** > **Basic Event** > **Tamper-proof**.
2. Check the **Enable Tamper-proof** box.
3. Move the **Sensitivity** slider to set the sensitivity of the detection.

4. Click **Edit** to edit the arming schedule for tamper-proof alarms. The arming schedule configuration is the same as that for motion detection. See “To set up motion detection” for more information.
5. Specify the linkage method when an event occurs. Check one or more response methods for the system when a tamper-proof alarm is triggered.

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is an alarm triggered. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note:** This option is only supported by cameras that feature an alarm output.

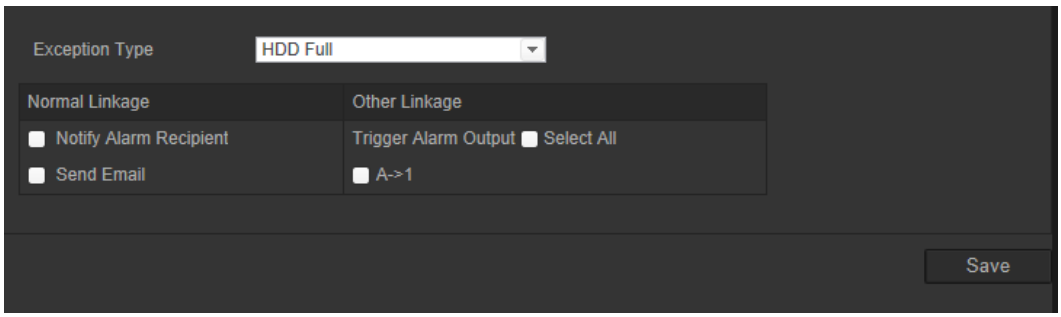
6. Click **Save** to save changes.

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

Figure 12: Exception window



To define exception alarms:

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

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

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is an exception alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 for further information. T To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. Note: This option is only supported by cameras that feature an 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** > **Basic Event** > **Alarm Input**.
2. Choose the **Alarm Input No.** and the **Alarm Type**. The alarm type can be NO (Normally Open) or NC (Normally Closed). Enter a name for the alarm input.
3. Click **Edit** to set the arming schedule for the alarm input. See “To set up motion detection” for more information.
4. Check the checkbox to select the linkage method.

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is an alarm input or output alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.

Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note:** To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note:** This option is only supported by cameras that feature an alarm output.

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

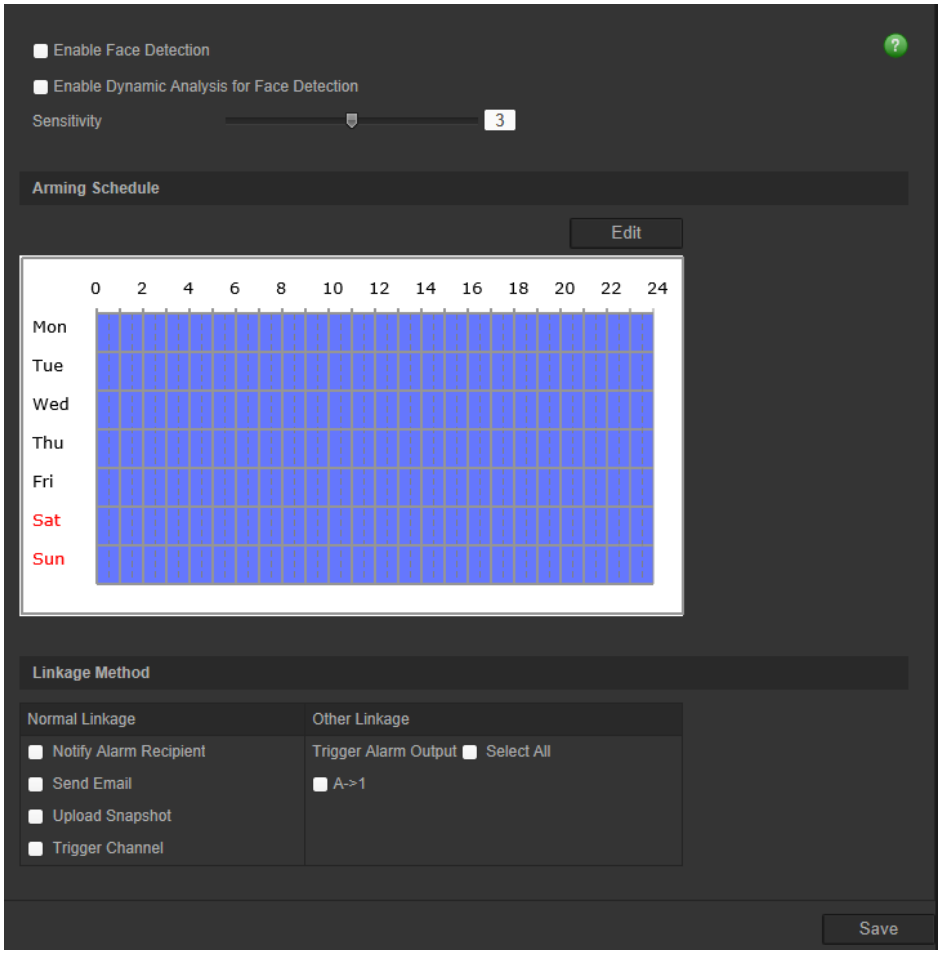
To define an alarm output:

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

Face detection

When the face detection function is enabled, the camera can detect a human face that is moving towards it, triggering a configurable 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.

Figure 13: Face detection window



To define face detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Face Detection**.
2. Check **Enable Face Detection** to enable the function.
3. Check **Enable Dynamic Analysis** 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 > Rules.
4. Configure the sensitivity of the face detection. The range is between 1 and 5.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when a face detection alarm is triggered.

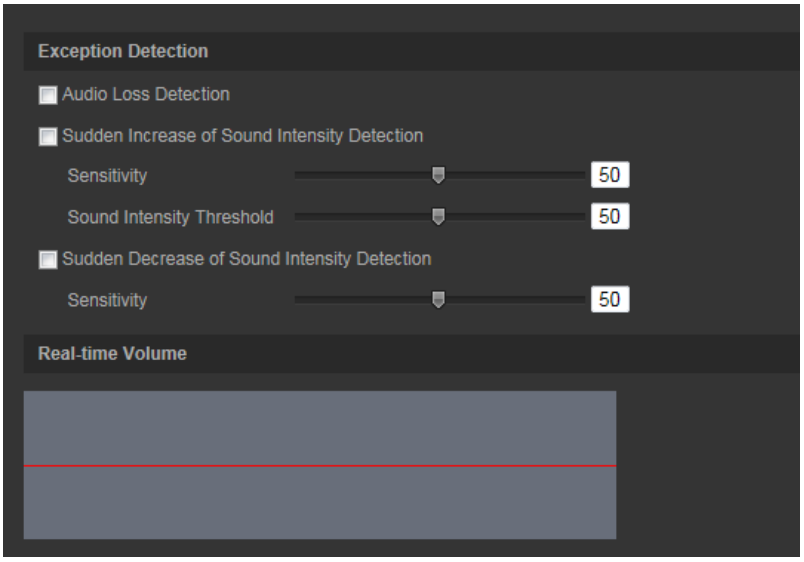
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a face detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Audio exception detection

Audio exception detection detects sounds that are above a selected threshold.

Figure 14: Audio exception detection window



To define audio exception detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Audio Exception Detection**.
2. Check **Audio Loss Exception** to activate the function.
3. Check **Sudden Increase of Sound Intensity Detection** to detect a steep rise in the sound level of the surveillance scene. You can set the detection sensitivity and threshold for a sudden increase.

   Sensitivity: The smaller the value, the larger the change should be to trigger the detection. The range is between 1 and 100.

   Sound Intensity Threshold: This option filters the sound in the environment. The louder the environmental sound, the higher the value. Adjust it according to the actual environment. The range is between 1 and 100.
4. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect a steep drop in the sound level of the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.

   Sensitivity: The smaller the value, the larger the change should be to trigger the detection. The range is between 1 and 100.

   Sound Intensity Threshold: This option filters the sound in the environment. The louder the environmental sound, the higher the value. Adjust it according to the actual environment. The range is between 1 and 100.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when an audio exception alarm is triggered.

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

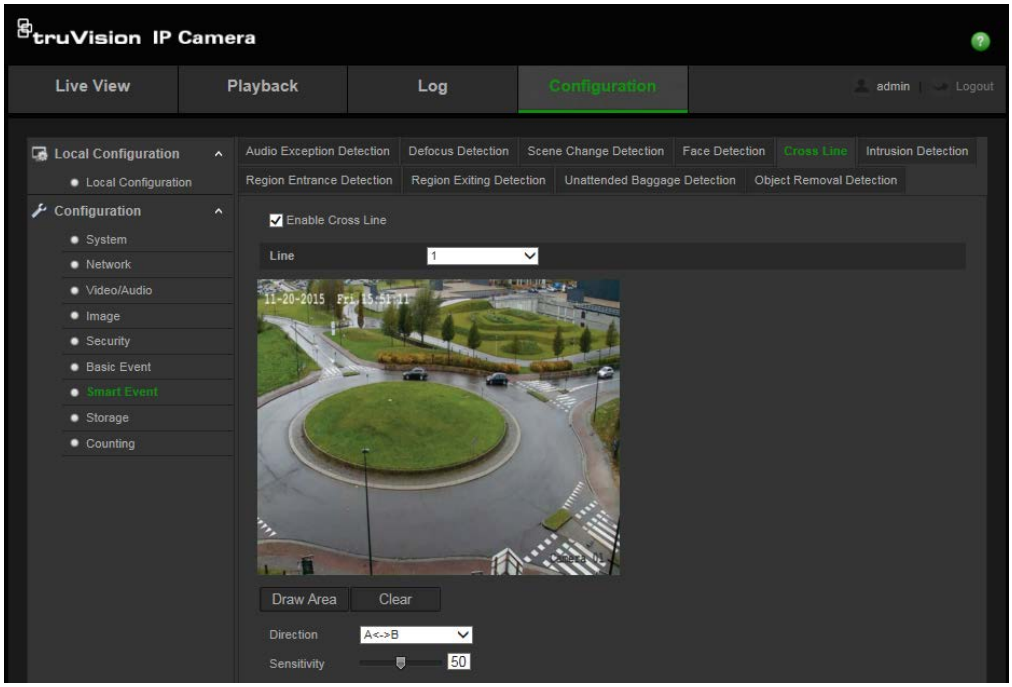
Cross line detection

This function can be used to detect people, vehicles and objects crossing a pre-defined line or an area on-screen. 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** > **Smart Event** > **Cross Line**.



2. Check the **Enable Cross Line Detection** checkbox (1) to enable the function.
3. Click **Draw Area** (2), 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 menu (3):

   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 (4) between 1 and 100.
6. If desired, select another line crossing area to configure from the dropdown menu. Up to four line crossing areas can be configured.
7. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.

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

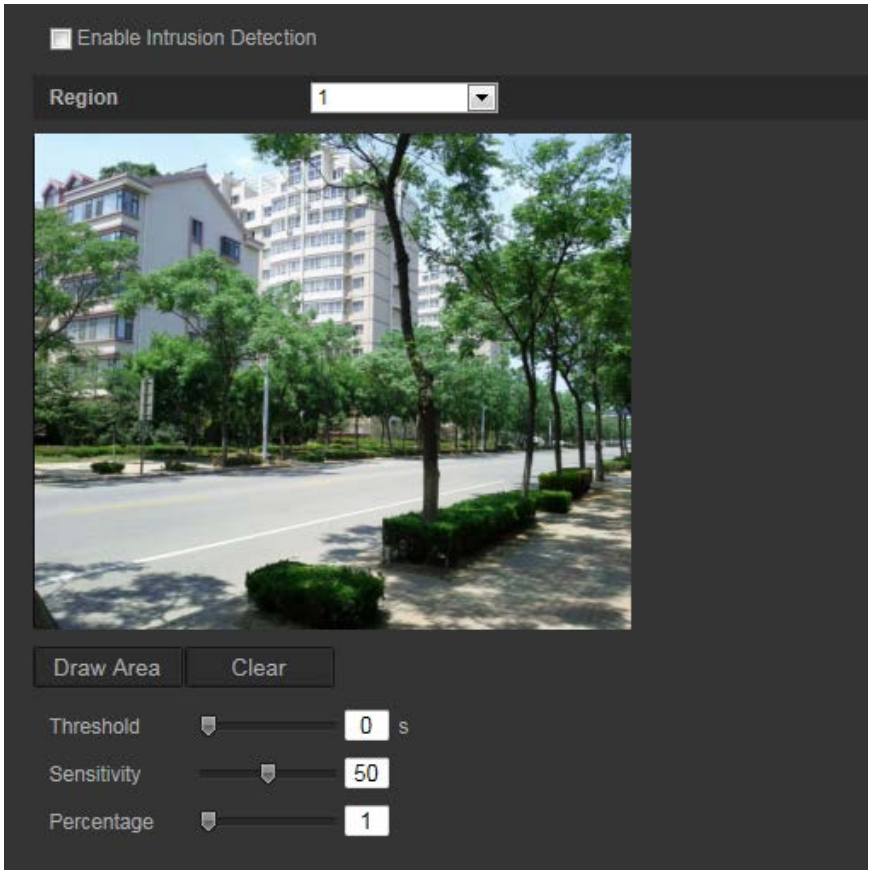
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a cross line detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

9. Click **Save** to save changes.

Intrusion detection

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

Figure 15: Intrusion detection window



To define intrusion detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Intrusion Detection**.
2. Check the **Enable Intrusion Detection** checkbox 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, the alarm is triggered immediately after the object enters the region. The range is between 0 and 100.

   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 the alarm. The range is between 1 and 100.

   Percentage: This defines the ratio of the in-region part of the object that can trigger an alarm. For example, when you set the percentage as 50%, half of the object entering the region will trigger the alarm. The range is between 1 and 100.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.

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

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

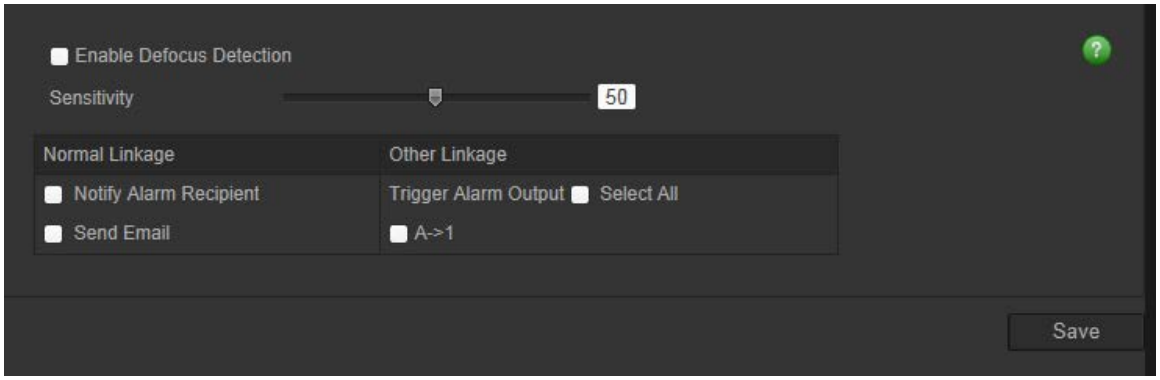
7. Click **Save** to save changes.

Defocus detection

The camera can detect image blur caused by defocusing of the lens, triggering a series of alarm actions.

The sensitivity level determines how much blur is tolerated by the camera before triggering an alarm. When enabled, the camera regularly checks the level of image focus (to allow for variations in light during the day) and then compares the current image to that of the reference image to see if there is a difference. A high sensitivity level means that there cannot be a large variance between the reference and current image.

Figure 16: Defocus detection window



To define defocus detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Defocus Detection**.
2. Check the **Enable Defocus Detection** checkbox to enable the function.

   Sensitivity: The range is between 1 and 100. The higher the sensitivity level, the smaller the defocus required to trigger an alarm.
3. Specify the linkage method when an event occurs. Check one or more response methods for the system when a defocus detection alarm is triggered.

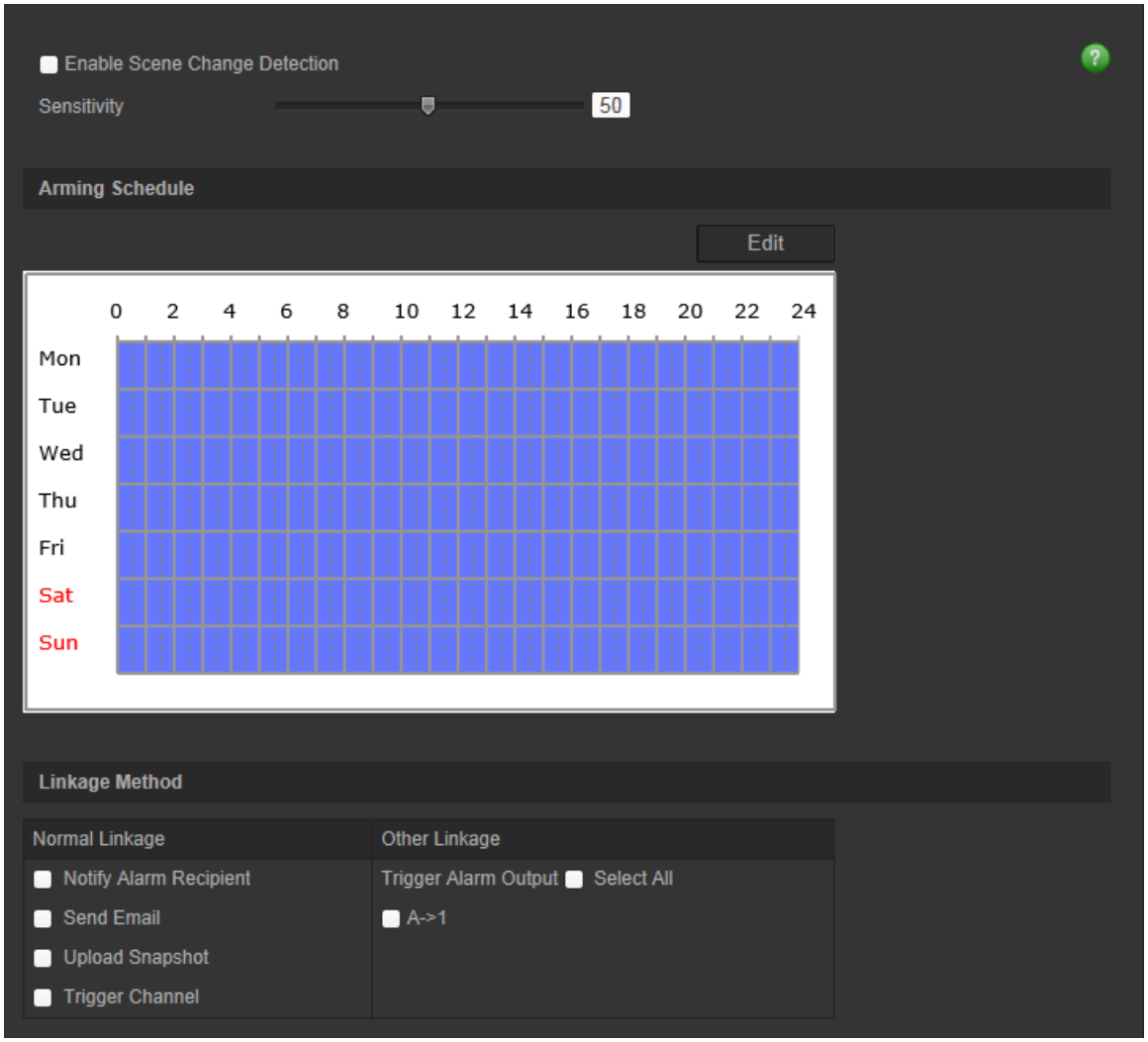
Notify Alarm Recipient	Sends an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Focus	Tries to refocus the camera by adjusting the back-focus. Only available on the box camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Scene change detection

You can configure the camera to trigger an alarm when the camera detects a change in the scene caused by a physical repositioning of the camera.

Figure 17: Scene change detection window



To define scene change detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Scene Change Detection**.
2. Check the **Enable Scene Change Detection** checkbox to enable the function.
3. Configure the sensitivity ranging from 1 to 100, the higher the sensitivity, the easier the change of scene can trigger the alarm.
3. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
4. Specify the linkage method when an event occurs. Check one or more response methods for the system when a scene change detection alarm is triggered.

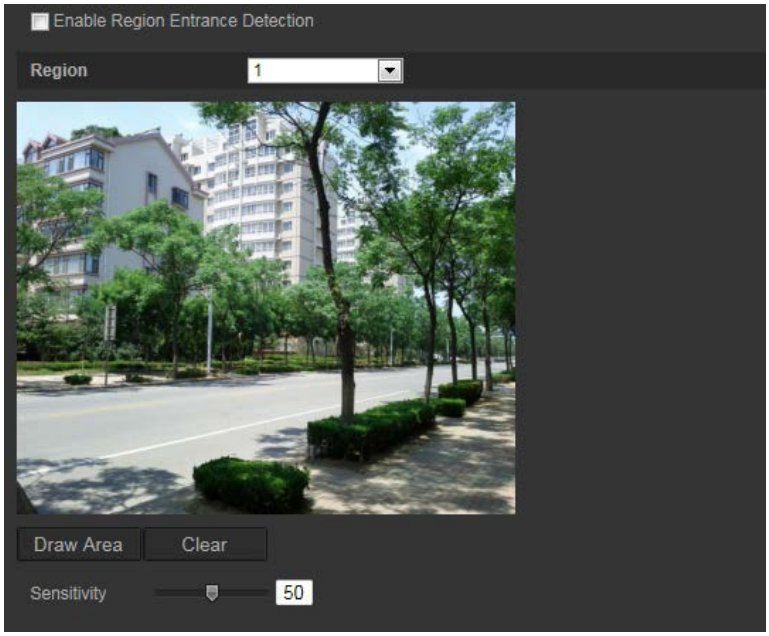
Notify Alarm Recipient	Sends an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a scene change detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 17 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Triggers external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Region entrance detection

This function detects people, vehicles or other objects that enter a designated region from outside the designated region. Certain actions can be configured to occur when the alarm is triggered.

Figure 18: Region entrance detection window



To define region entrance detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Region Entrance Detection**.
2. Check the **Enable Entrance Detection** checkbox to enable the function.
3. Choose the region number to be configured.
4. Click **Draw Area**, and then draw a rectangle on the image as the designated 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 designated region parameters can be set up separately.

   Note: The area can only be quadrilateral.
5. Set the sensitivity level.

   The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, a small object can trigger the alarm. The range is between 1 and 100.
6. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
7. Specify the linkage method when an event occurs. Check one or more response methods for the system when an intrusion detection alarm is triggered.

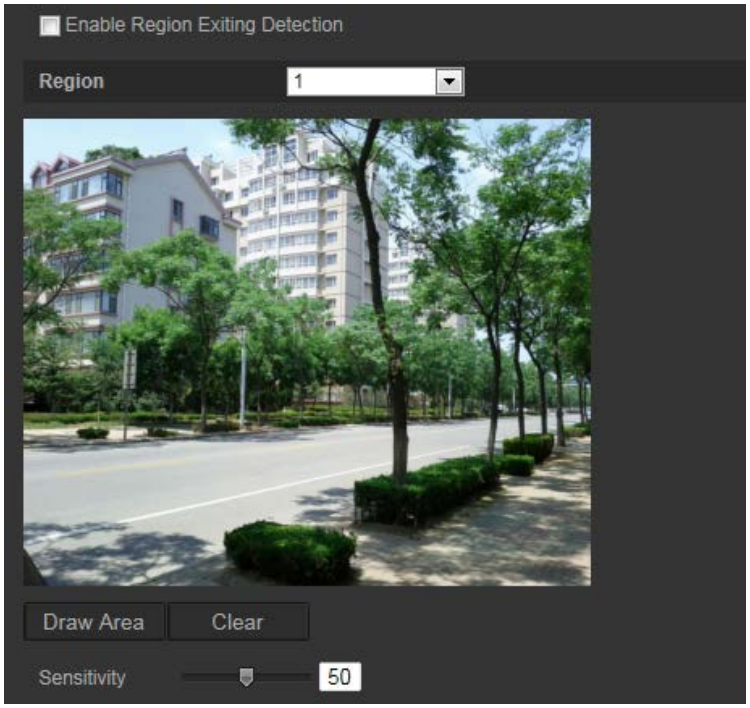
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Region exiting detection

Region exiting detection function detects people, vehicle or other objects that exit from a designated region, and certain actions can be configured to occur when the alarm is triggered.

Figure 19: Region exiting detection window



To define region exiting detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Region Exiting Detection**.
2. Check the **Enable Exiting Detection** checkbox to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the designated 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 designated region parameters can be set up separately.

   Note: The area can only be quadrilateral.
4. Choose the region to be configured.

   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 the alarm. The range is between 1 and 100.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when an intrusion detection alarm is triggered.

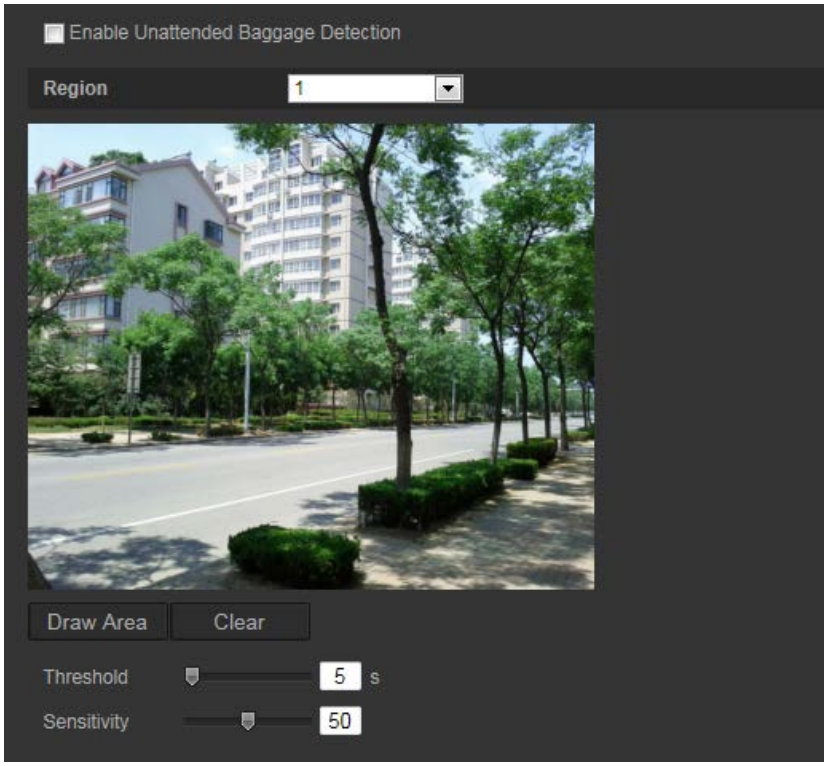
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Unattended baggage detection

Unattended baggage detection function detects the objects left in the designated region such as baggage, a purse, dangerous materials, etc. A series of actions can be configured to occur when the alarm is triggered.

Figure 20: Unattended baggage detection window



To define unattended baggage detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Unattended Baggage Detection.**
2. Check the **Enable Unattended Baggage Detection** checkbox to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the designated 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 designated region parameters can be set up separately.

   Note: The area can only be quadrilateral.
4. Choose the region to be configured.

   Threshold: the threshold for the time the objects remain left in the region. If you set the value as 10, an alarm is triggered after the object is left and remains in the region for 10s. The range is 5 and 20s.

   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 the alarm. The range is between 1 and 100.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when an unattended baggage alarm is triggered.

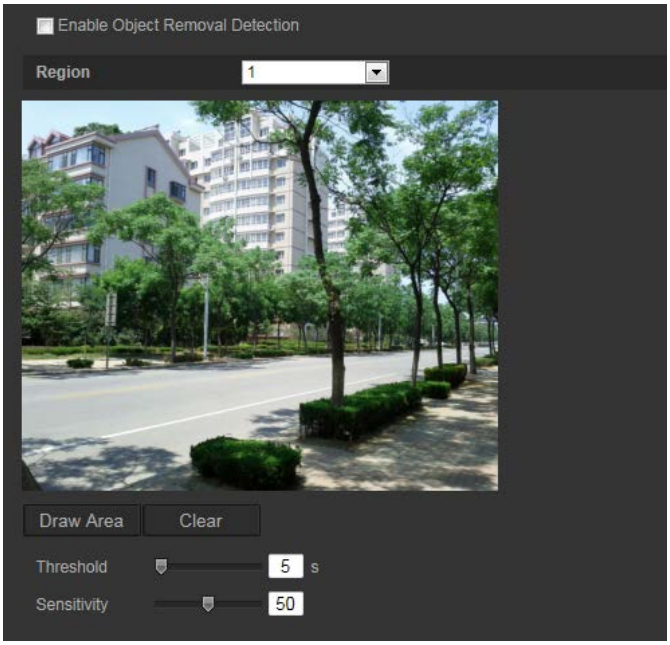
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 59 for further information.
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Object removal detection

Object removal detection function detects objects removed from a designated region, such as exhibits on display, and a series of actions can be configured to occur when the alarm is triggered.

Figure 20: Object removal detection window



To define object removal detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Object Removal Detection.**
2. Check the **Enable Unattended Baggage Detection** checkbox to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the designated 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 designated region parameters can be set up separately.

   Note: The area can only be quadrilateral.
4. Choose the region to be configured.

   Threshold: the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object is removed and absent from the region for 10s. The range is 5 and 20s.

   Sensitivity: The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, the removal of a small object can trigger the alarm. The range is between 1 and 100.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 32 for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when an object removal alarm is triggered.

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 19 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the snapshot to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 61 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 18 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 Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note**: This option is only supported by cameras that feature an alarm output.

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

Snapshot parameters

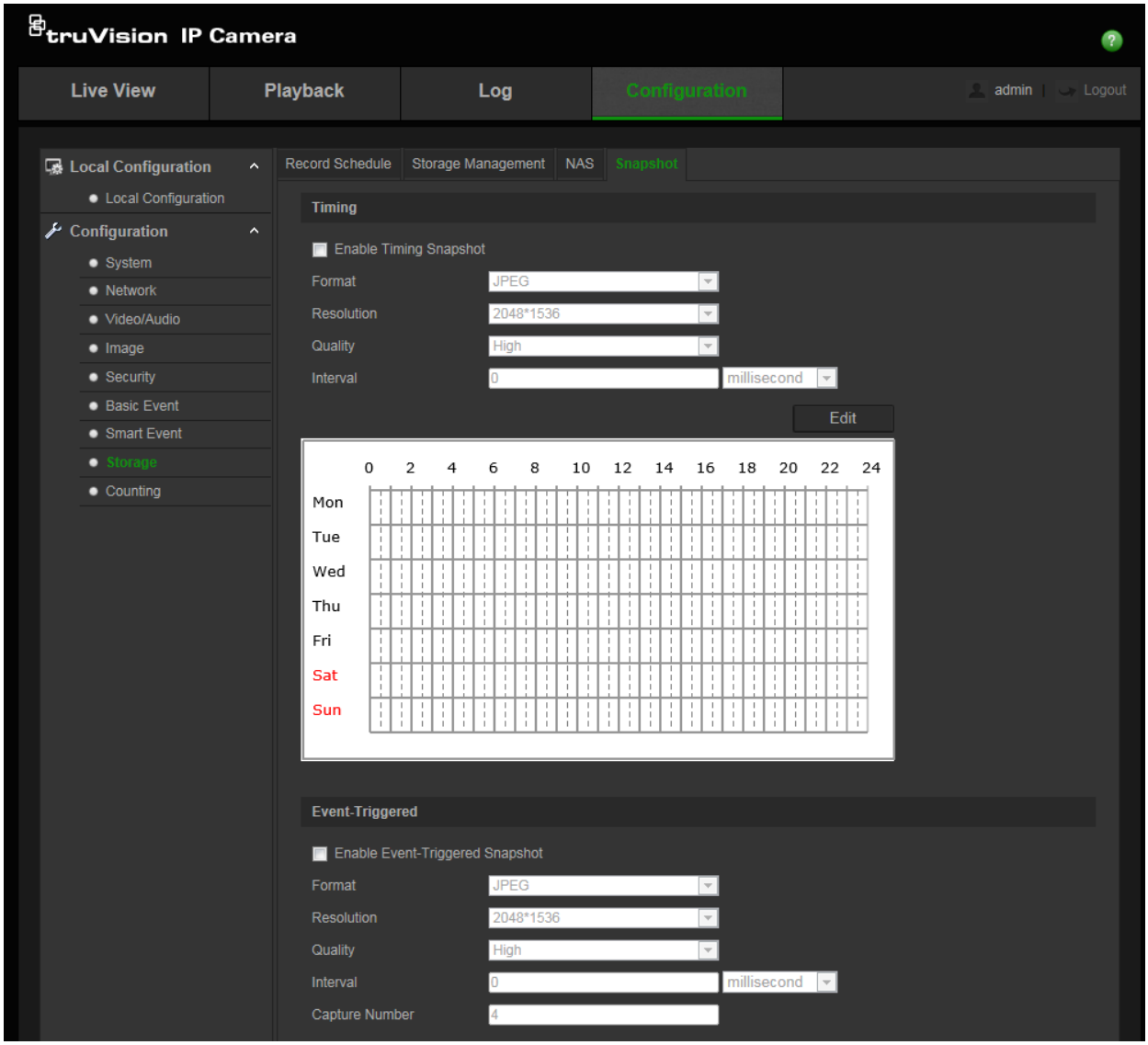
You can configure scheduled snapshots and event-triggered snapshots. The captured snapshots can be stored in the SD card (if supported) or in a NAS (if configured). You can also upload the snapshots to an FTP server.

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 checked **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/or NAS when motion detection or an alarm input is triggered. If you have configured the FTP settings and checked **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.

Figure 21: Snapshot window



To set up scheduled snapshots:

1. From the menu toolbar, click **Configuration** > **Storage** > **Snapshot**.
2. Check **Enable Timing Snapshot** to enable continuous snapshots.
3. Select the desired format of the snapshot, such as JPEG.
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. Click **Edit** and enter the desired schedule for each day of the week.
7. Click **Save** to save changes.

To set up event-triggered snapshots:

1. From the menu toolbar, click **Configuration** > **Storage** > **Snapshot**.
2. Check **Enable Event-triggered Snapshot** to enable event-triggered snapshots.

3. Select the desired format of the snapshot, such as JPEG.
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 should be taken.
7. Click **Save** to save changes.

NAS settings

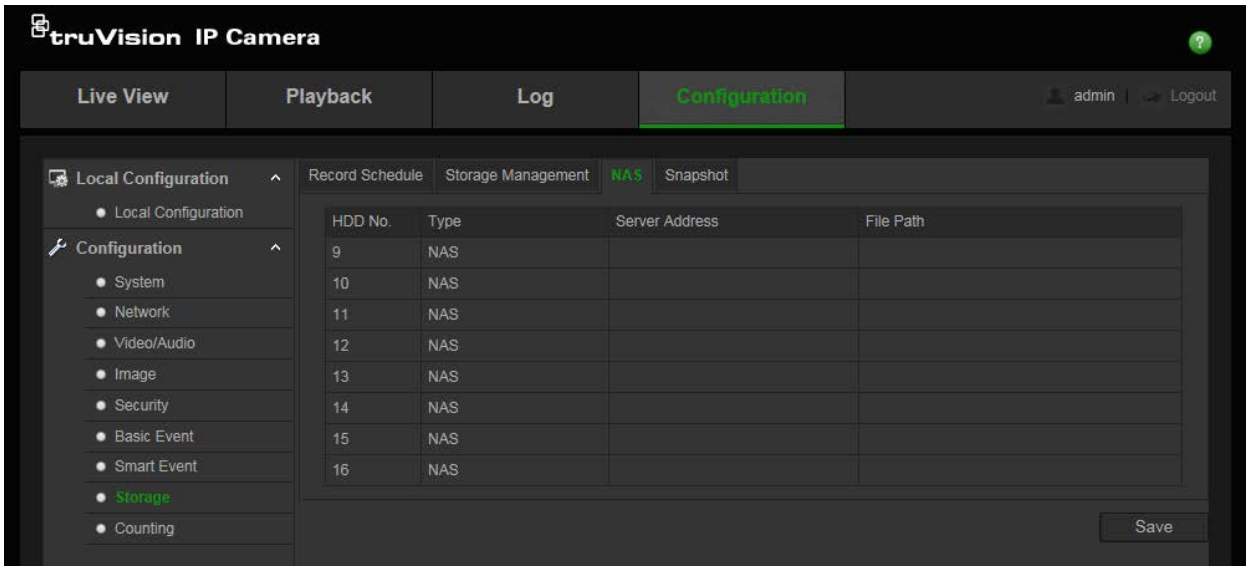
You can use a network attached storage (NAS) device to remotely store recordings.

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. Cameras can record to up to eight NAS devices.
2. The recommended capacity of NAS is between 9G and 2T; other capacities may cause a formatting failure.

Figure 22: NAS window



To set up a NAS system:

1. From the menu toolbar, click **Configuration** > **Storage** > **NAS**.
2. Enter the IP address of the network disk, and the NAS file path.
3. Click **Save** to save changes.

Storage devices

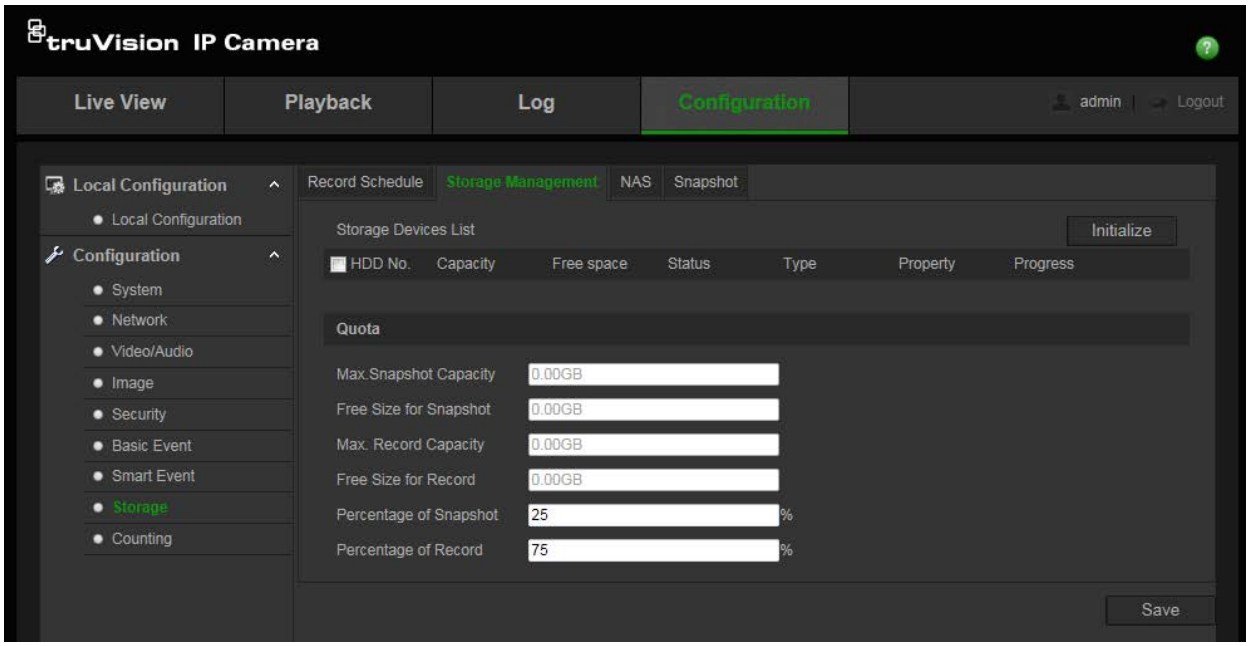
Use the storage management window to display the capacity, free space available, and the working status of the HDD of the NAS and the SD card in the camera (if supported). You must format these storage devices before first use.

Before formatting the storage device, stop all recording. Once formatting is completed, reboot the camera, 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** > **Storage** > **Storage Management**.



2. Check 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 Snapshot** and **Percentage of Record**.
4. Click **Format**. A window appears to check your formatting permissions.
5. Click **OK** to start formatting.

Accessing the files saved on the SD card and NAS storage

For security reasons you cannot directly open snapshots and video files saved on the SD card and NAS storage using a file browser. You can read these files via the camera browser or via TruVision Navigator. See “Playing back recorded video” on page 76 for information on how to play back recorded files.

Recording schedule

You can define a recording schedule for the camera in the “Record Schedule” window. The recording is saved to the NAS or SD card configured 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 as 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.

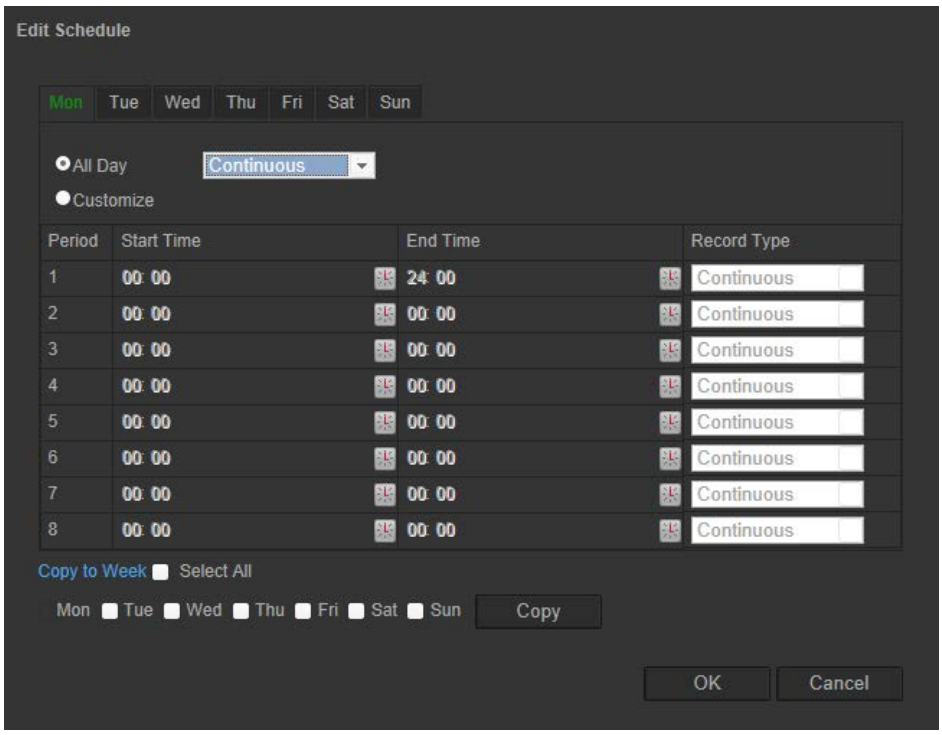
Post-record time

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 as 5 seconds, the camera records until 11:00:05. The post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, or 10 min.

To set up a recording schedule:

1. From the menu toolbar, click **Configuration** > **Storage** > **Record Schedule**.
2. Click the **Enable Record Schedule** box to enable recording.

   Note: To disable recording, deselect the option.
3. Click **Edit** to edit the recording schedule. The following window appears:



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

If you select “All Day”, select one of the record types from the drop-down list box:

- **Continuous**: For continuous recording.
- **Motion detection:** Video is recorded when the motion is detected.
- **Alarm:** Video is recorded when the alarm is triggered via the external alarm input.
- **Motion | Alarm:** Video is recorded when an external alarm is triggered or motion is detected.
- **Motion & Alarm:** Video is recorded when motion and alarms are triggered at the same time.
- **Face Detection**: Video is recorded when a face is detected. See “Face detection” on page 41 for more information.
- **Cross line**: Video is recorded when the pre-defined line on-screen is crossed. See “Cross line detection” on page 45 for more information.
- **Intrusion Detection**: Video is recorded when an intrusion is detected. See “Intrusion detection” on page 46 for more information.
- **Scene Change detection**: Video is recorded when a change in the camera scene is detected. See “Scene change detection” on page 49 for more information.
- **Region entrance detection**: Video is recorded when a person or object enters the pre-defined area.
- **Region exiting detection**: Video is recorded when a person or object leaves the pre-defined area.
- **Unattended baggage detection**: Video is recorded when the object is left within the pre-defined area.
- **Object removal detection**: Video is recorded when the object is removed from the pre-defined area.

5. If you enable “Customize”, click the day of the week required. For period 1, set the start and end times during which you want the camera to begin and end recording.

   From the drop-down list box, select one of the record types (see the list above).

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

   Note: The eight time periods cannot overlap.

6. Set the recording periods for the other days of the week if required.

   Click **Copy** to copy the recording periods to another day of the week.

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

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

RS-485 settings

The RS-485 serial port is used to control the PTZ of the camera or connect to light and wiper devices. Configuration of these parameters should be done before you connect to any devices.

Note: Only the box camera and VF mini dome support RS-485.

To set up RS-485 settings:

1. From the menu toolbar, click **Configuration** > **System** > **RS485**.
2. Select the RS-485 port parameters.

   Note: The Baud Rate, PTZ Protocol, and PTZ Address parameters should be exactly the same as the PTZ camera parameters.
3. Click **Save** to save changes.

Object counting

This function helps to calculate the number of people or objects entering or exiting a configured area and is primarily used with entrances or exits.

Note: It is recommended to install the camera directly above the entrance/exit and aimed down at the entry/exit point to improve counting accuracy.

To set up object counting:

1. From the menu toolbar, click **Configuration** > **Counting**.
2. Check the **Enable Object Counting** checkbox to enable the function.
3. Check the **Enable OSD Overlay** checkbox. The real-time number of people entered and exited is superimposed on the live video view.
4. Set the detection line.

   Draw an orange detection line on the live video to detect and count the objects entering or exiting through the line.

   1) Click **Draw Line** to draw a detection line. An orange detection line will appear on the image.

      Note:

      - The detection line should be drawn directly below the camera and it should cover the entire entrance/exit region.
      - Draw the detection line where people do not linger to improve the accuracy of the count.

   2) Click and drag the detection line to adjust its position.
   3) Click and drag the two end points of the detection line to adjust its length.
   4) Click **Delete Line** to delete the detection line.
   5) Click **Change Direction** to change the direction.
5. Click the **Reset Counter** button to clear the number of entries/exits to zero.

6. Enter the arming schedule interface and click-and-drag the mouse on the time bar to set the time during which object counting will be active.
7. Select the linkage method.
8. Click **Save** to save the settings.

To set up counting statistics:

Note: An SD card must be installed and configured for use with the camera in order to save count data and generate reports.

1. Select the report type: Daily report, Weekly report, Monthly report, and Annual report.

   Daily report calculates the data on the selected date. Weekly report calculates for the week of the selected date. Monthly report calculates for the month of the selected date. Annual report calculates for the year of the selected date.
2. Select the statistics type: People entered and people exited.
3. Select the statistics time.
4. Select Table, Bar, Chart or Line Chart to display the result. If you select the table to list the statistics, there is an Export button to export the data in an Excel file.
5. Click **Counting** to list the object counting result.

Camera management

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

User management

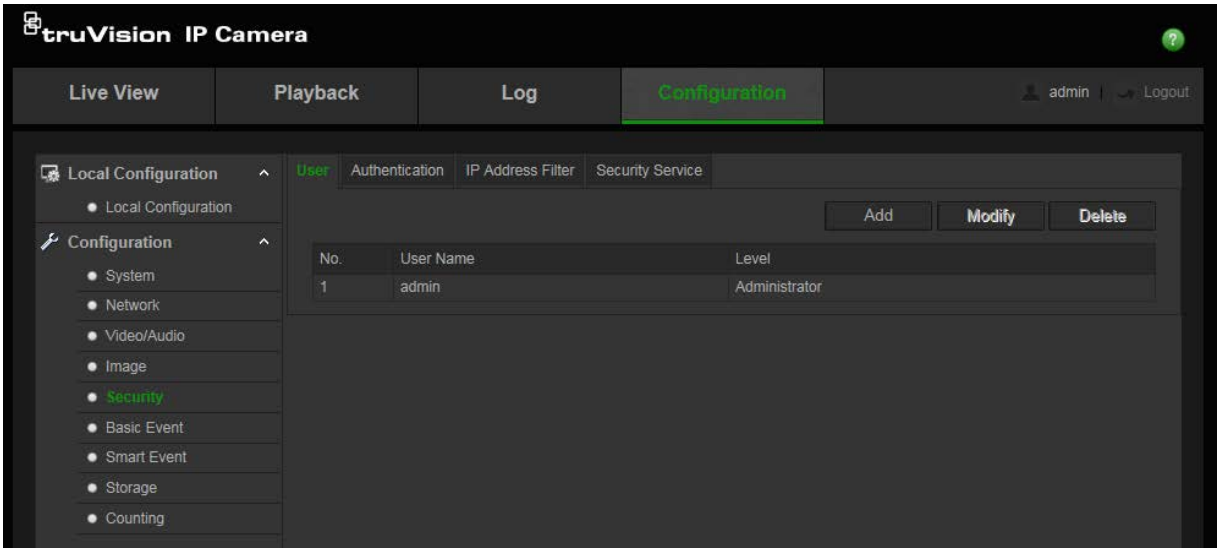
This section describes how to manage users. You can:

- Add or delete users
- Modify permissions
- 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 passwords for each user. See Figure 18 below.

Figure 18: 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.

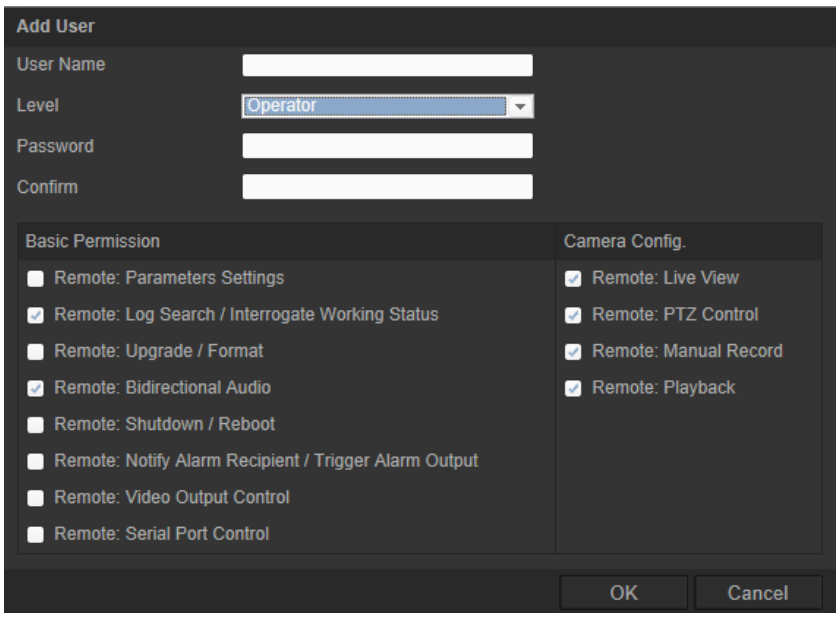
- **Operator**: This user can only change the configuration of his/her own account. An operator cannot create or delete other users.
- **Viewer**: This user has the permission of live view, playback and log search. However, they cannot change any configuration settings.

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** > **Security** > **User**.
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. Check the desired options:

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

Basic Permissions	Camera Configuration
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:

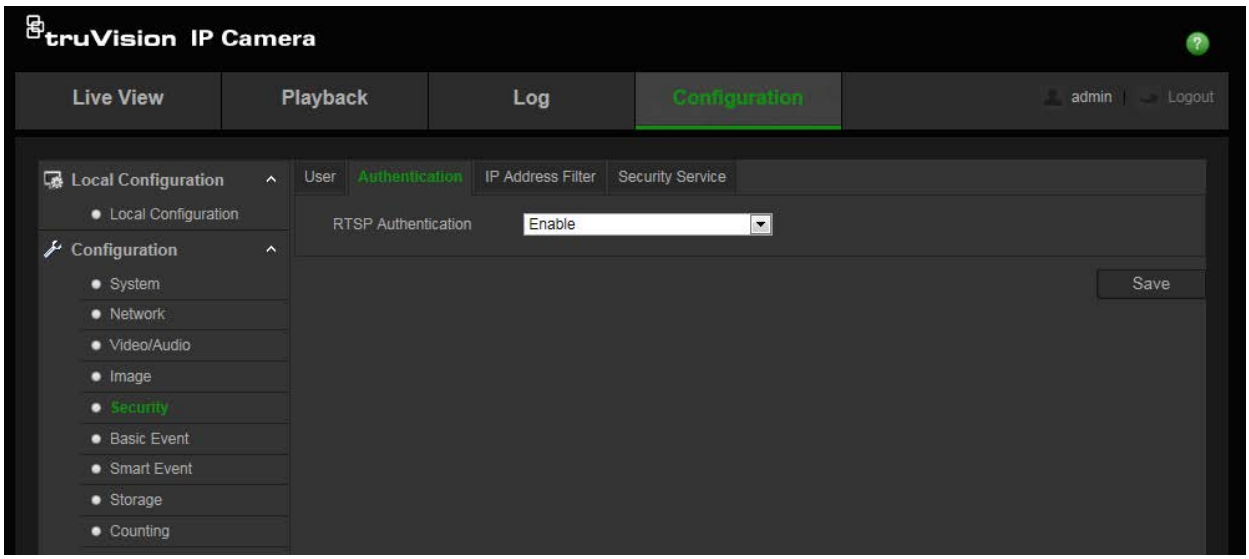
1. Select the desired user under the **User** tab.
2. Click the **Modify** button. The user management window appears
3. Change the information required.

   Note: The user “Admin” can only be changed by entering the admin password.
4. Click **Save** to save the changes.

RTSP authentication

You can secure the RTSP stream of the live view.

Figure 19: RTSP authentication window



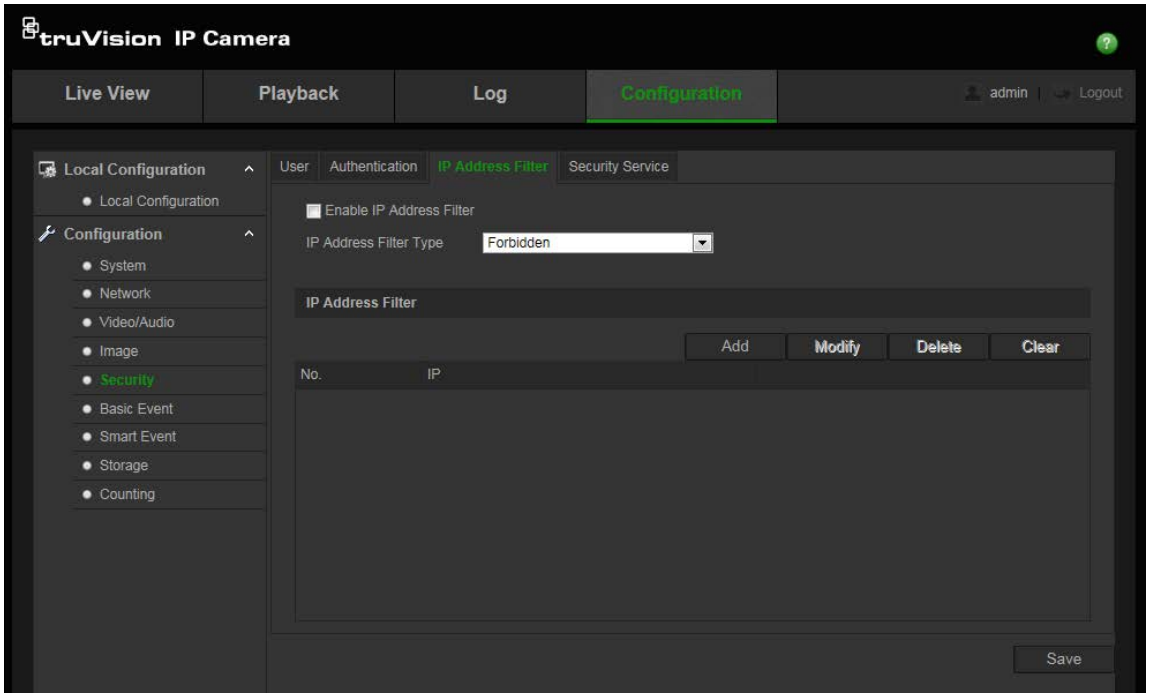
To define RTSP authentication:

1. From the menu toolbar, click **Configuration** > **Security** > **RTSP Authentication**.
2. Select the **Authentication** type **Enable** or **Disable** in the drop-down list to enable or disable the RTSP authentication. The authentication credentials are the same as the Admin user.
3. Click **Save** to save the changes.

IP address filter

This function allows you to allow or deny access rights to defined IP addresses. For example, the camera can be configured so that only the IP address of the server hosting the video management software is allowed to be accessed, and attempts by users at any other IP addresses would be denied access.

Figure 20: IP address filter window



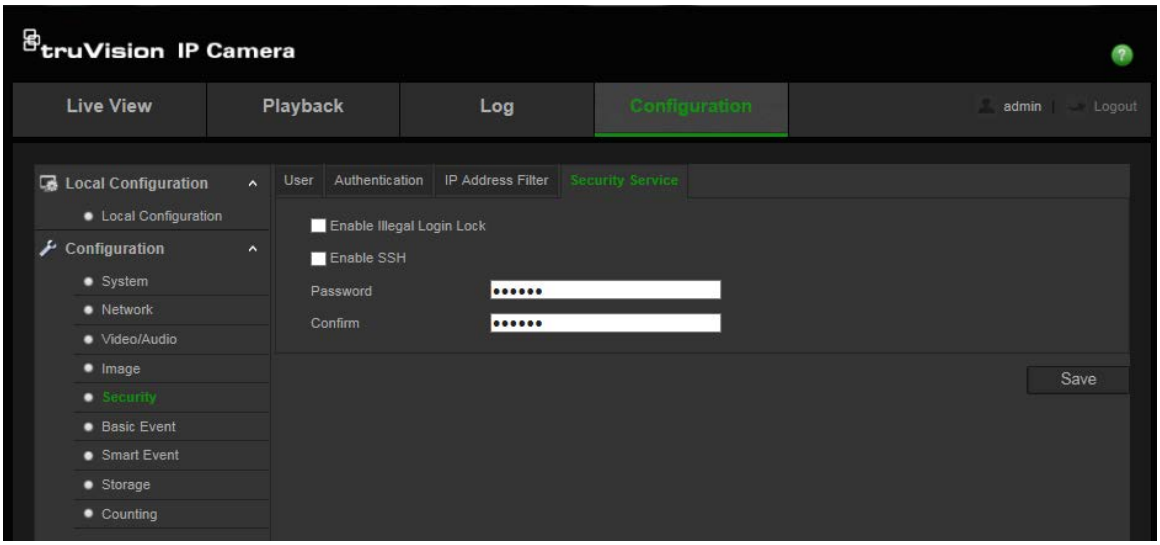
To define IP Address Filter:

1. From the menu toolbar, click **Configuration** > **Security** > **IP Address Filter**.
2. Check the checkbox of **Enable IP Address Filter.**
3. Select the type of IP Address Filter in the drop-down list: Forbidden or Allowed.
4. Click **Add** to add an IP 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.

Defining the security service

This function enables SSH and allows you to define its password. It is only used by Technical Support.

Figure 21: Security service window



To enable the illegal login lock:

1. Click **Configuration** > **Security** > **Security Service**.
2. Check the **Enable Illegal Login Lock** check box
3. Click **Save** to save the changes.

Note:

1. The IP address will be locked if the admin user performs 7 failed user name/password attempts (10 attempts for the operator/user).
2. If the IP address is locked, you can try to login the device after 5 minutes

To define SSH:

1. Click **Configuration** > **Security** > **Security Service**.
2. Check the **Enable SSH** check box.
3. Click **Save** to save the changes.

Restore default settings

Use the Default menu to restore factory 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** > **Security** > **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 the 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 from an existing camera to a new 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. In **Configuration** > **System**, click the **Maintenance** tab to open its window.
2. Click **Browse** to select the local configuration file and then click **Import** to start importing configuration file.
3. Click **Export** and set the saving path to save the configuration file.

Upgrade firmware

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

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

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

To upgrade firmware version:

1. Download the latest firmware version from our web site at:

   http://www.interlogix.com/video/category/ip-cameras

   - or -

   www.utcfssecurityproductspages.eu/videoupgrades/

2. When the firmware file has downloaded, extract the file to the desired destination.

   Note: Do not save the file on your desktop.

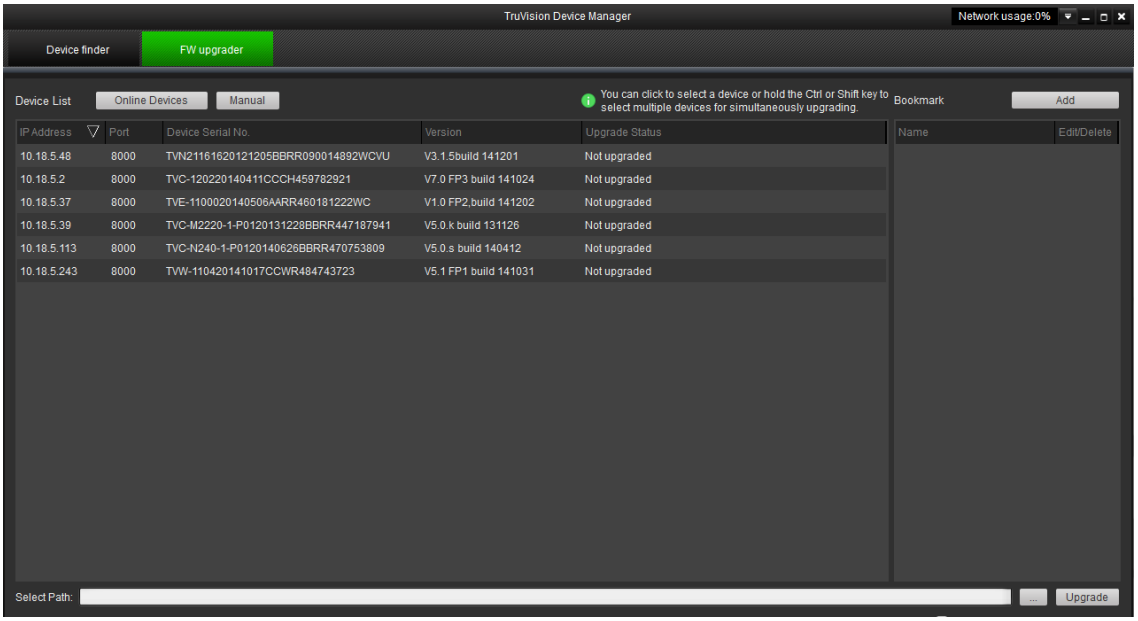
3. From the menu toolbar, click **Configuration** > **Security** > **Maintenance**. Select the **Firmware** or **Firmware Directory** option. Then click the Browse button to locate latest firmware file on your computer.

- **Firmware directory**: Locate the folder containing the firmware file. The camera will choose the appropriate firmware file automatically.
- **Firmware**: Locate the firmware file manually for the camera.

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:

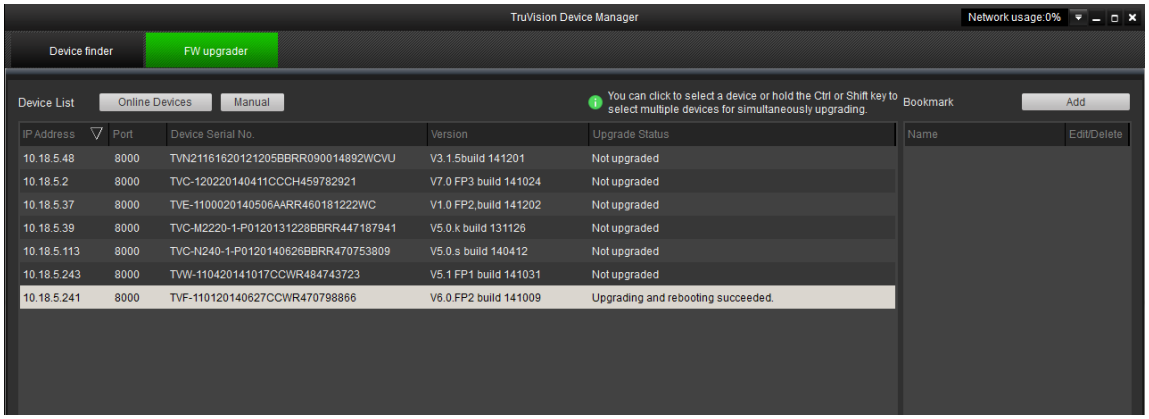
1. In the **FW upgrader** panel, select a device or hold the Ctrl or Shift key to select multiple devices for simultaneous upgrading.



2. Click the browse button  to locate the firmware file to use.

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

3. Click **Upgrade**.
4. When the upgrading is completed, the updated version information on the devices is listed.



Reboot camera

The camera can be easily rebooted remotely.

To reboot the camera through the web browser:

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

Camera operation

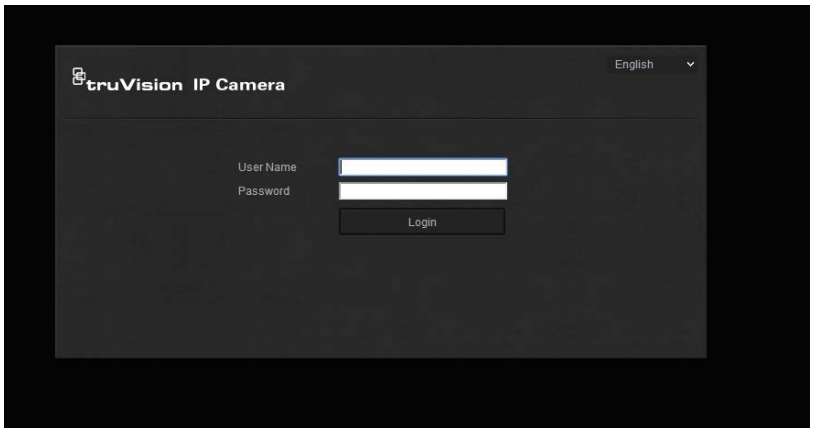
This chapter describes how to use the camera once it is installed and configured.

Logging on and off

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

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

Figure 22: Login dialog box



If you do not change the default password of admin, a message will always pop up requesting you to do so. It is highly recommended to change the Admin password upon first use for enhanced security.

Live view mode

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

Start/stop live view: You can stop and start live view by clicking the Start/stop live view button on the bottom of the window.

Record: You can record live video and store it in the directory you have configured. In the live view window, click the **Record** button at the bottom of the window. To stop recording, click the button again.

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

Playing back recorded video

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

Note: You must configure the NAS or insert an SD card in the dome camera to be able to use the playback functions. See “Storage devices” on page 62 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 23 on page 76.

Figure 23: Playback window

Name		Description
1.	Playback button	Click to open the Playback window.
2.	Search calendar	Click the day required to search.
3.	Search	Start search.
4.	Set playback time	Input the time and click → to locate the playback point.
5.	Download functions	Download video files. Download captured images.
6.	Archive functions	Click these buttons for the following archive actions:

Name		Description
		 Enable digital zoom.  Capture a snapshot image of the playback video.  Start/Stop clipping video files.
7.	Recording type	The color code displays the recording type. Recording types are schedule recording, alarms recording and manual recording. The recording type name is also displayed in the current status window.
8.	Time moment	Vertical bar shows the current position within the playback recording. The current time and date are also displayed.
9.	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 on the timeline bar.
10.	Audio control	Control level of audio.
11.	Control playback	Click to control how the selected file is played back: play, stop, slow, and fast forward playback.

To play back recorded video:

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

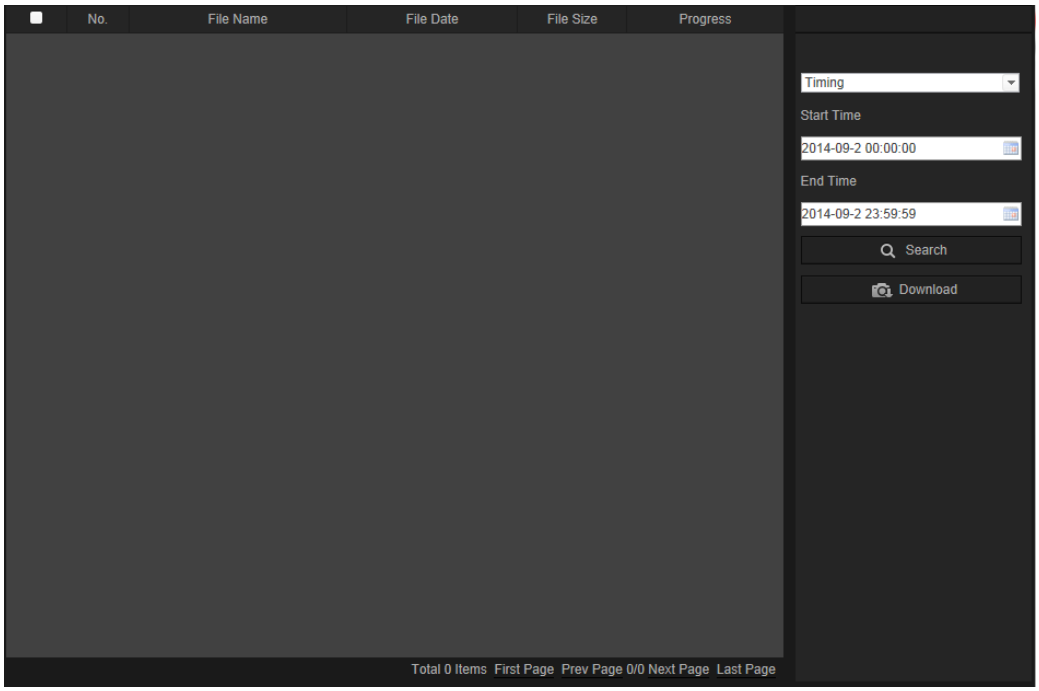
   Note: You must have playback permission to play back recorded images. See “Modify user information” on page 69 for more information.
3. Select the date and click the **Search** button to search for the required recorded file.
4. Click  to search the video file.
5. In the pop-up window, check the box of the video file and click **Download** to download the video files.

To archive a recorded video segment during playback:

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

To archive recorded snapshots:

1. Click  to open the snapshot search window.



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

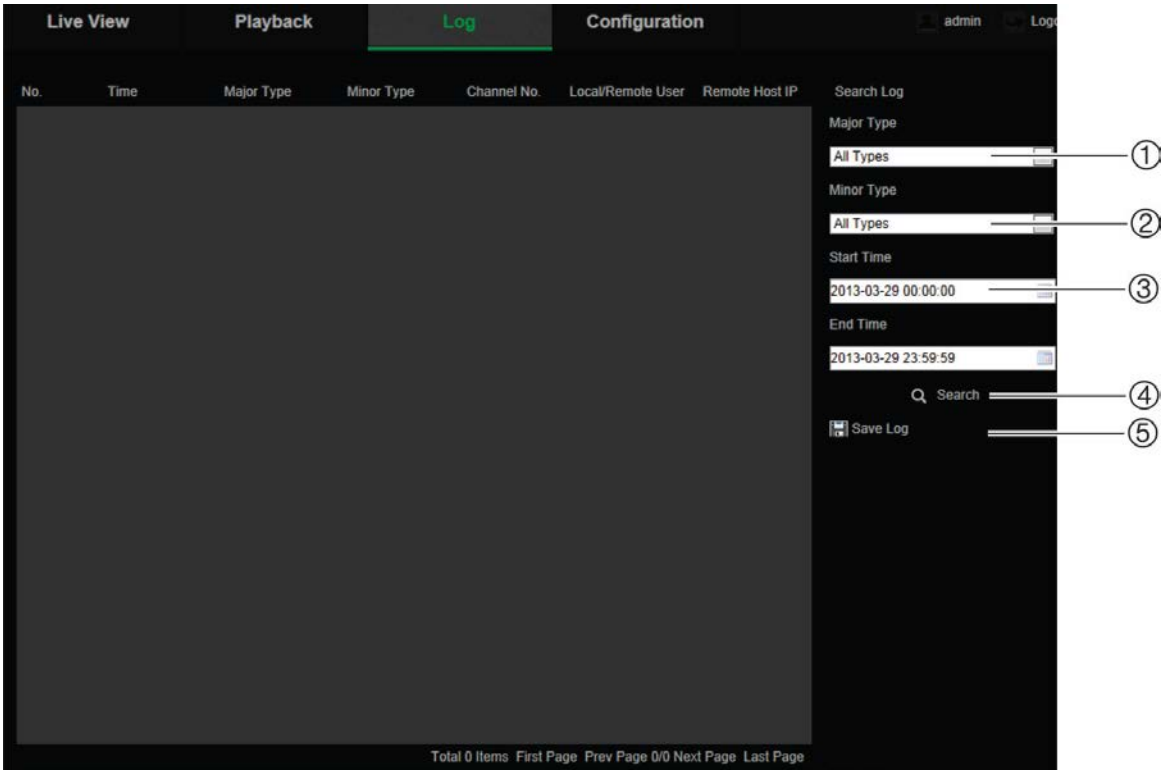
Searching event logs

You must configure a NAS or 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 events. To view logs stored on storage devices, click **Log** on the menu toolbar. The Log window appears. See Figure 24 on page 79.

Note: You must have view log access rights to search and view logs. See “Modify user information” on page 69 for more information.

Figure 24: Log window



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

You can search for recorded logs by the following criteria:

Major type: There are four types of logs: All Types, Alarm, Exception, and Operation. See 802.1x parameters below for their descriptions. “Major type” indicates the general category of the logged event.

Minor type: “Minor type” indicates the specific type of event logged. See 802.1x parameters below for descriptions.

Date and Time: Logs can be searched by start and 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

Main log type	Minor log types: Description of events included
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 logs:

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

Operating PTZ control

In the live view interface, you can use the PTZ control buttons to control pan/tilt/zoom and other functions of the camera (where supported).

PTZ control panel

In live view, click « / » to display/hide the PTZ control panel.

Figure 25: PTZ control panel

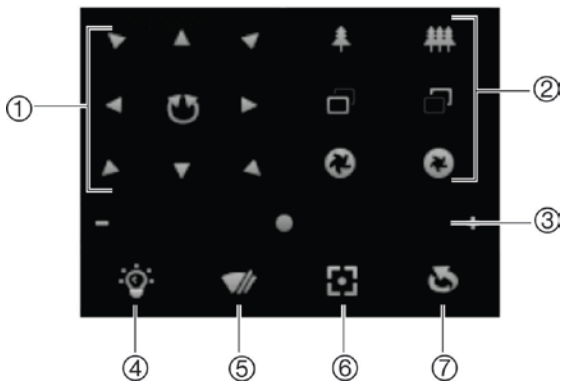


Table 2: Description of the PTZ control panel

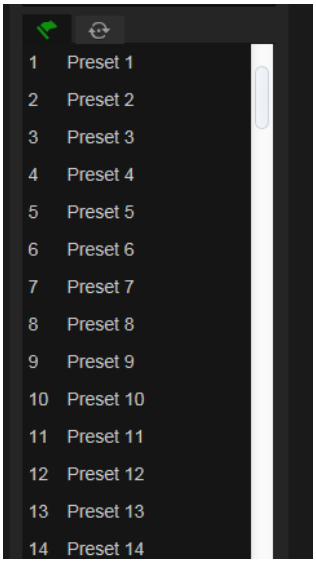
	Description
1.	**Directional buttons**: Controls the movements and directions of the PTZ. Center button is used to start auto-pan by the PTZ dome camera.
2.	**Zoom, focus and iris**: Adjusts zoom, focus and iris.
3.	**PTZ movement**: Adjusts the speed of PTZ movement.
4.	Turns on/off the light. This function is supported by cameras with a RS-485 port.
5.	Turns on/off camera wiper. This function is supported by cameras with a RS-485 port.
6.	Auto focus
7.	Initializes the lens

Note:

1. To do pan/tilt movement using the direction buttons, the camera connected to the network must support RS-485 and a pan/tilt unit must be installed in the camera. Please properly set the PTZ parameters on the RS-485 Settings page referring to Defining RS-485 settings
2. To control the lens, such as zoom or focus, the camera must support auto focus.

To set a preset:

1. Select a preset number from the preset list.



2. Use the PTZ directional buttons to move the camera to the desired position.
3. Click to finish the setting of the current preset.
4. You can click to delete the preset.

To call a preset:

1. Select a defined preset from the list.
2. Click to call the preset.

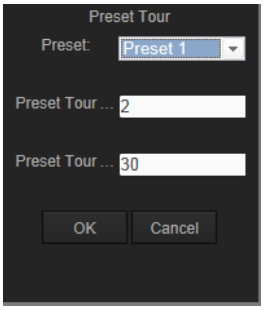
Using preset tours

A preset tour is a memorized series of preset functions. The camera stays at a step for a set dwell time before moving on to the next step. The steps are defined by presets. A preset tour can be configured with up to 32 presets.

You can configure up to eight preset tours.

To set a preset tour:

1. In the PTZ control panel, click to enter the tour settings interface.
2. Select a preset tour number from the drop-down list.
3. Click to enter the adding interface of preset.



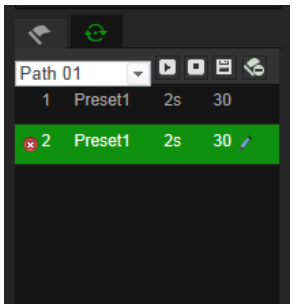
4. Configure the preset number, preset tour time and preset tour speed.

Preset Tour Duration:	The dwell time. The length of time in seconds for which a camera stays at a preset before moving to the next preset.
Preset Tour Speed:	The speed the camera moves from one preset to another.

5. Click **OK** to save a preset into the preset tour.
6. Repeat the steps from 3 to 5 to add more presets.
7. Click to save all the preset tour settings.

To call a preset tour:

In the PTZ control panel, select a defined preset tour from the drop-down list and click to call the preset tour.



Index

O

P

R

S

T

U

V

W