TruVision Series 5 IP Camera Configuration Manual

P/N 1073340-EN • REV C • ISS 20NOV17

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

CE c UL us LISTED

Contact information

For contact information, see www.interlogix.com or www.utcfssecurityproducts.eu.

Content

Introduction

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

- TVB-5501 (3MPX IP bullet camera)
- TVB-5502 (8MPX IP bullet camera)

- TVT-5501 (3MPX IP turret camera)
- TVT-5502 (8MPX IP turret camera)

- TVD-5501 (3MPX IP dome camera)
- TVD-5502 (8MPX IP dome camera)

Network access

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

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

Checking your web browser security level

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

Configuring IE ActiveX controls

You should confirm the ActiveX settings of your web browser.

To change the web browser's security level:

1. In Internet Explorer click **Internet Options** on the **Tools** menu.
2. On the Security tab, click the zone to which you want to assign a web site under "Select a web content zone to specify its security settings".
3. Click **Custom Level**.
4. Change the **ActiveX controls and plug-ins** options that are signed or marked as safe to **Enable**. Change the **ActiveX controls and plug-ins** options that are unsigned to **Prompt** or **Disable**. Click **OK**.

   - or -

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

   Then click **OK** to the Internet Options Security tab window.
5. Click **Apply** in the **Internet Options** Security tab window.

Windows Internet Explorer

Internet Explorer operating systems have increased security measures to protect your PC from any malicious software being installed.

To have complete functionality of the web browser interface with Windows 7, 8 and 10, do the following:

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

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

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

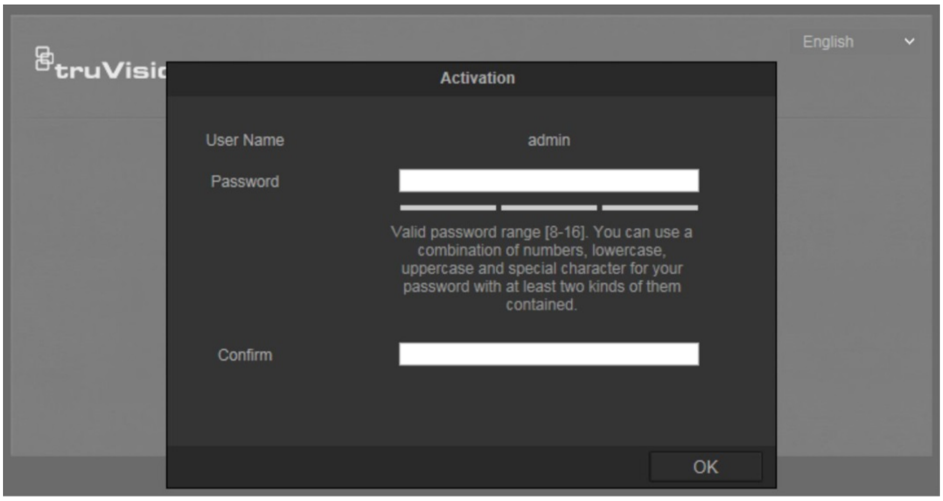
Activating the camera

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

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

Activation via the web browser:

1. Power on the camera and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface.



User Name admin

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Note:

- The default IP address of the camera is 192.168.1.70.
- For the camera to enable DHCP by default, you must activate the camera via TruVision Device Manager. Please refer to the following section, “Activation via TruVision Device Manager”.

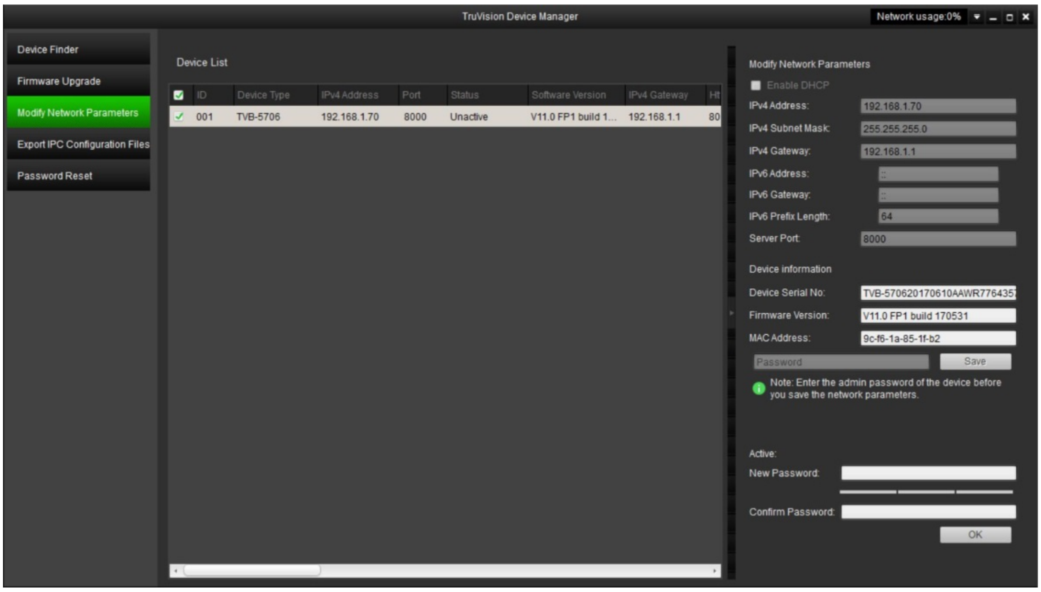
3. Enter the password in the password field.

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

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

Activation via *TruVision Device Manager*:

1. Run the *TruVision Device Manager* to search for online devices.
2. Check the device status from the device list, and select the inactive device.



Device List

☑	ID	Device Type	IPv4 Address	Port	Status	Software Version	IPv4 Gateway	Ht
✓	001	TVB-5706	192.168.1.70	8000	Unactive	V11.0 FP1 build 1...	192.168.1.1	80

Modify Network Parameters

□ Enable DHCP

IPv4 Address: 192.168.1.70

IPv4 Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 64

Server Port: 8000

Device information

Device Serial No: TVB-570620170610AAWR776435

Firmware Version: V11.0 FP1 build 170531

MAC Address: 9c-f6-1a-85-1f-b2

Password

Note: Enter the admin password of the device before you save the network parameters.

Active:

New Password:

Confirm Password:

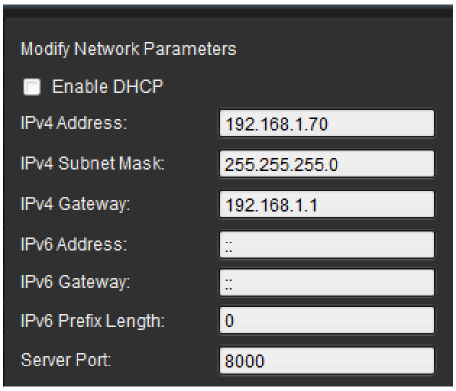
3. Enter the password in the password field, and confirm it.

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

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

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

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



Modify Network Parameters

□ Enable DHCP

IPv4 Address: 192.168.1.70

IPv4 Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

Server Port: 8000

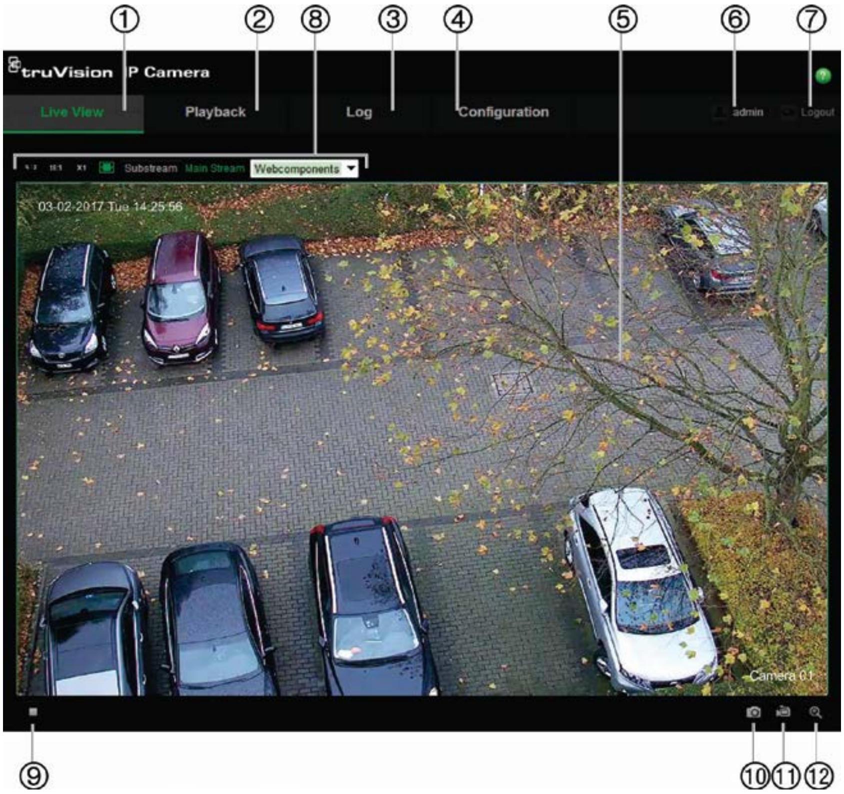
6. Input the password and click the **Save** button to activate your IP address modification.

Overview of the camera web browser

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

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

Figure 1: Web browser interface



Name	Description
1. Live view	Click to view live video.
2. Playback	Click to play back video.

Name		Description
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.	Display Control	Click each tab to adjust the layout and the stream type of the live view. You can also click the drop-down list to select the plug-in. For IE (internet explorer) users, web components and quick time are selectable. For non-IE users, web components, quick time, VLC, or MJPEG are selectable if they are supported by the web browser.
9.	Start/stop live view	Click to start/stop live view.
10.	Capture	Click to take a snapshot of the video. The snapshot will be saved to the default folder in JPEG or BMP format.
11.	Start/stop recording	Click to record live video.
12.	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.

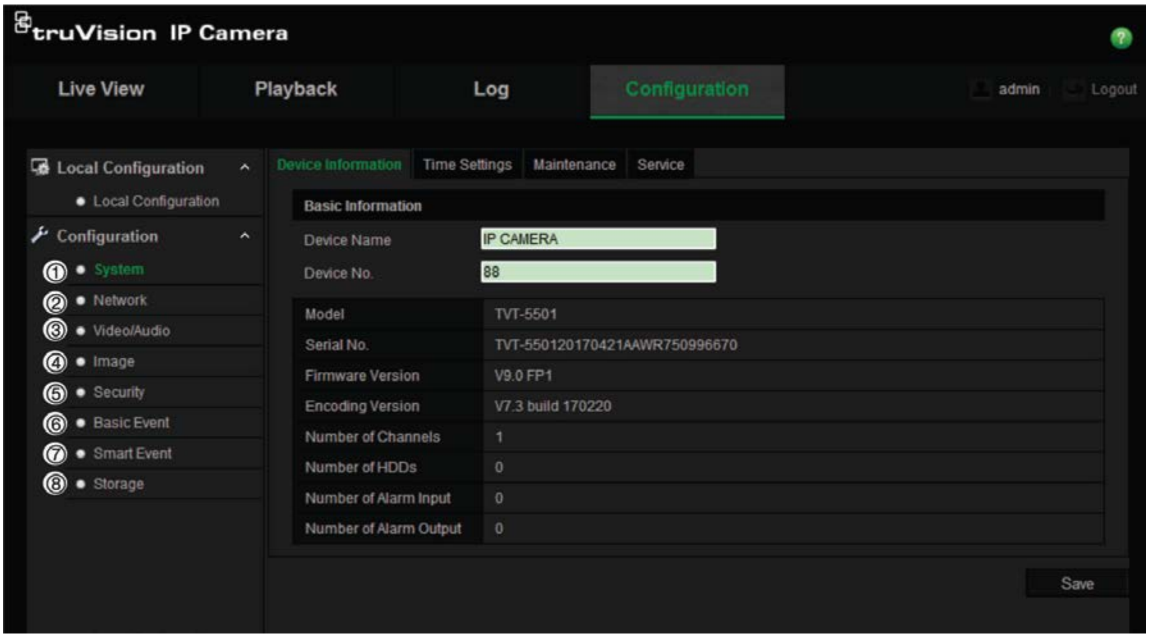
There are two main menus in the configuration panel:

- Local configuration
- Configuration

Configuration menu overview

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

Figure 2: Configuration window (Device Information tab selected)



Basic Information

Device Name	IP CAMERA
Device No.	88
Model	TVT-5501
Serial No.	TVT-550120170421AAWR750996670
Firmware Version	V9.0 FP1
Encoding Version	V7.3 build 170220
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	0
Number of Alarm Output	0

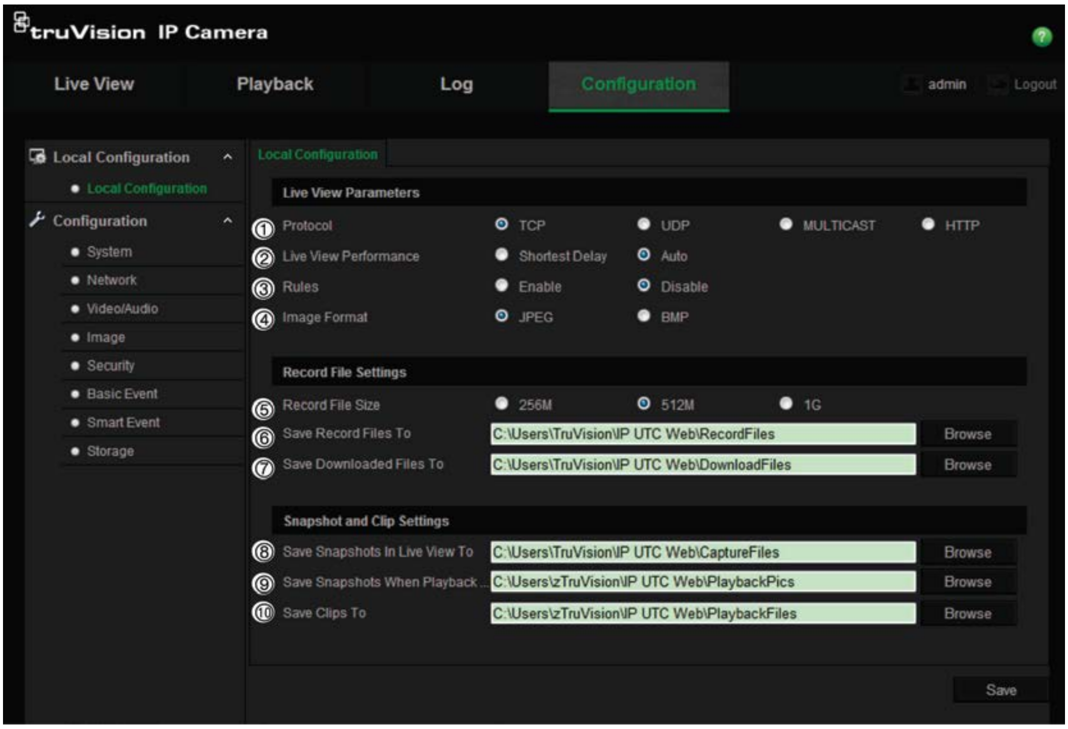
Configuration menus		Description
1.	System	Defines device basic information including SN and the current firmware version, time settings, maintenance, and serial port parameters. See "System time" on page 11 for further information.
2.	Network	Defines the network parameters required to access the camera over the internet. See "Network settings" on page 12 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 23 for further information on the setup.
5.	Security	Defines who can use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and telnet access.
6.	Basic Event	Defines motion detection, tamper-proof, alarm input/output, and exception. See “Motion detection alarms” on page 29, “Tamper-proof alarms” on page 35, and “Alarm inputs and outputs” on page 37.
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.

Local configuration

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

Figure 3: Example of the Local configuration window



Live View Parameters

1 Protocol ◉ TCP ● UDP ● MULTICAST ● HTTP

2 Live View Performance ● Shortest Delay ◉ Auto

3 Rules ● Enable ◉ Disable

4 Image Format ◉ JPEG ● BMP

Record File Settings

5 Record File Size ● 256M ◉ 512M ● 1G

6 Save Record Files To C:\Users\TruVision\IP UTC Web\RecordFiles

7 Save Downloaded Files To C:\Users\TruVision\IP UTC Web\DownloadFiles

Snapshot and Clip Settings

8 Save Snapshots In Live View To C:\Users\TruVision\IP UTC Web\CaptureFiles

9 Save Snapshots When Playback... C:\Users\zTruVision\IP UTC Web\PlaybackPics

10 Save Clips To C:\Users\zTruVision\IP UTC Web\PlaybackFiles

Parameters		Description
Live View Parameters		
1.	Protocol	Specifies the network protocol used. Options include: TCP, UDP, MULTICAST and HTTP.

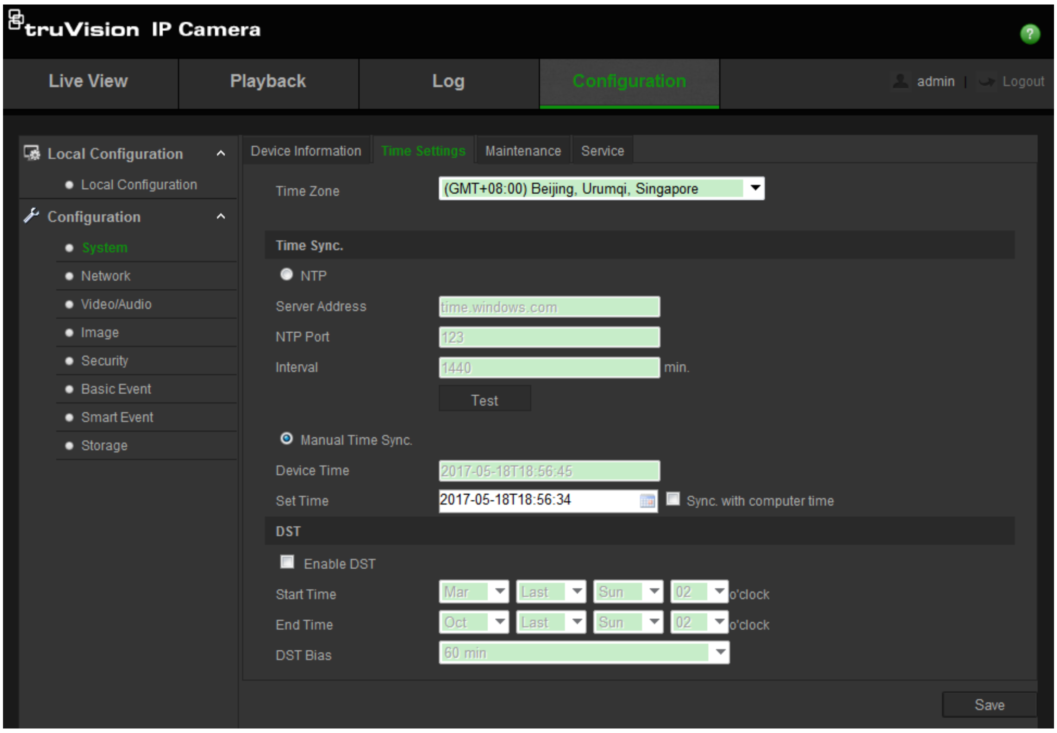
Parameters		Description
2.	Live View Performance	Specifies the transmission speed. Options include: Shortest Delay or Auto.
3.	Rules	It refers to the rules on your local browser. Specify whether or not to display the colored marks when motion detection, face detection, and intrusion detection are triggered.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

System time

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

To define the system time and date:

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



Time Zone: (GMT+08:00) Beijing, Urumqi, Singapore

Time Sync.

○ NTP

Server Address: time.windows.com

NTP Port: 123

Interval: 1440 min.

● Manual Time Sync.

Device Time: 2017-05-18T18:56:45

Set Time: 2017-05-18T18:56:34 □ Sync. with computer time

DST

□ Enable DST

Start Time: Mar Last Sun 02 o'clock

End Time: Oct Last Sun 02 o'clock

DST Bias: 60 min

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

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

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

   - Or -

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

   Note: You can also check the **Sync with computer time** check box to synchronize the time of the camera with the time of your computer.

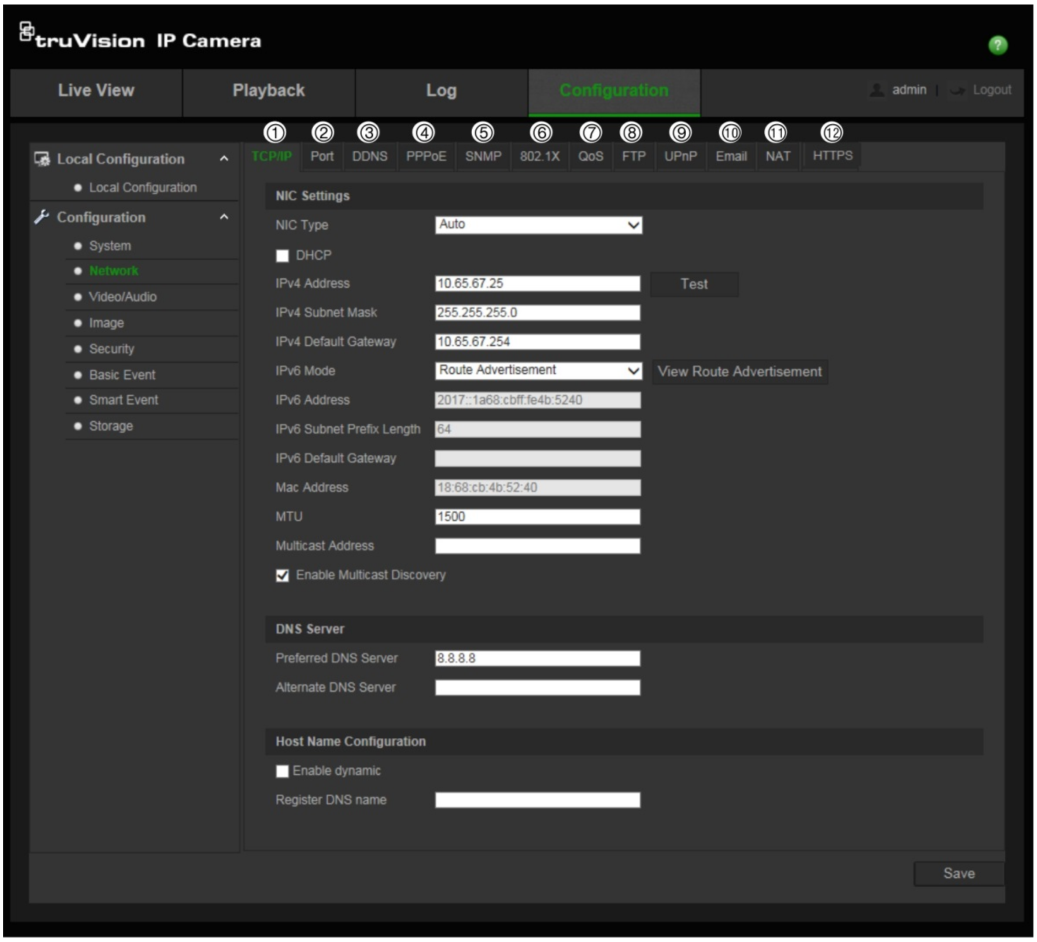
4. Check **Enable DST** to enable the DST (Daylight Savings Time) function, and set the date of the DST period.

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

Network settings

Accessing the camera through a network requires that you define certain network settings. Use the “Network” menu to define the network settings. See Figure 4 below for further information.

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



NIC Settings

NIC Type: Auto

□ DHCP

IPv4 Address: 10.65.67.25

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.65.67.254

IPv6 Mode: Route Advertisement

IPv6 Address: 2017::1a68:cbff:fe4b:5240

IPv6 Subnet Prefix Length: 64

IPv6 Default Gateway:

Mac Address: 18:68:cb:4b:52:40

MTU: 1500

Multicast Address:

☑ Enable Multicast Discovery

DNS Server

Preferred DNS Server: 8.8.8.8

Alternate DNS Server:

Host Name Configuration

□ Enable dynamic

Register DNS name:

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. See page 15 for setup information.

Menu tabs	Description
2. Port	**HTTP Port:** The HTTP port is used for remote internet browser access. Enter the port used for the Internet Explorer (IE) browser. Default value is 80. **RTSP Port:** RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. Enter the RTSP port value. The default port number is 554. **HTTPS Port:** HTTPS (Hyper Text Transfer Protocol Secure) allows video to be securely viewed when using a browser. Enter the HTTPS port, value. The default port number is 443. **Server Port:** This is used for remote client software access. Enter the server port value. The default port number is 8000. **Alarm Server IP**: Specifies the IP address of the alarm host. **Alarm Server Port**: Specifies the port of the alarm host. See page 15 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, DynDDNS.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 15 for setup information.
4. PPPoE	Retrieves a dynamic IP address. See page 16 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 16 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 16 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 16 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 17 for setup information.
10. Email	Enter the email address to which messages are sent when an alarm occurs. See page 17 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 18 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 the DHCP server is available, check **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server or Alternate DNS Server**.
5. Click **Save** to save changes.

To define the port parameters:

1. From the menu toolbar, click **Configuration** > **Network** > **Port**.
2. Set the HTTP port, RTSP port, HTTPS port and Server port of the camera.

   HTTP Port: The default port number is 80, 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 DNSS server address, members.ddns.org (which is used to notify DDNS about changes to your IP address), the host name for your camera, the port number (443 (HTTPS)), and your user name and password used to log

into your DDNS account. The domain name displayed under “Host Name” is that which you created on the DynDNS web site.

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

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

To define the PPPoE parameters:

1. From the menu toolbar, click **Configuration** > **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 setting the SNMP, please download the SNMP software and manage to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center. The SNMP version you select should be the same as that of the SNMP software.

To define the 802.1x parameters:

1. From the menu toolbar, click **Configuration** > **Network** > **802.1X**.
2. Check **Enable IEEE 802.1X** to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name, and password. The EAPOL version must be identical with that of the router or the switch.
4. Click **Save** to save changes.

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

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 is the higher the priority is.
3. Click **Save** to save changes.

To define the FTP parameters:

1. From the menu toolbar, click **Configuration** > **Network** > **FTP**.
2. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.

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

   Directory: In the Directory Structure field, you can select the root directory, 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.

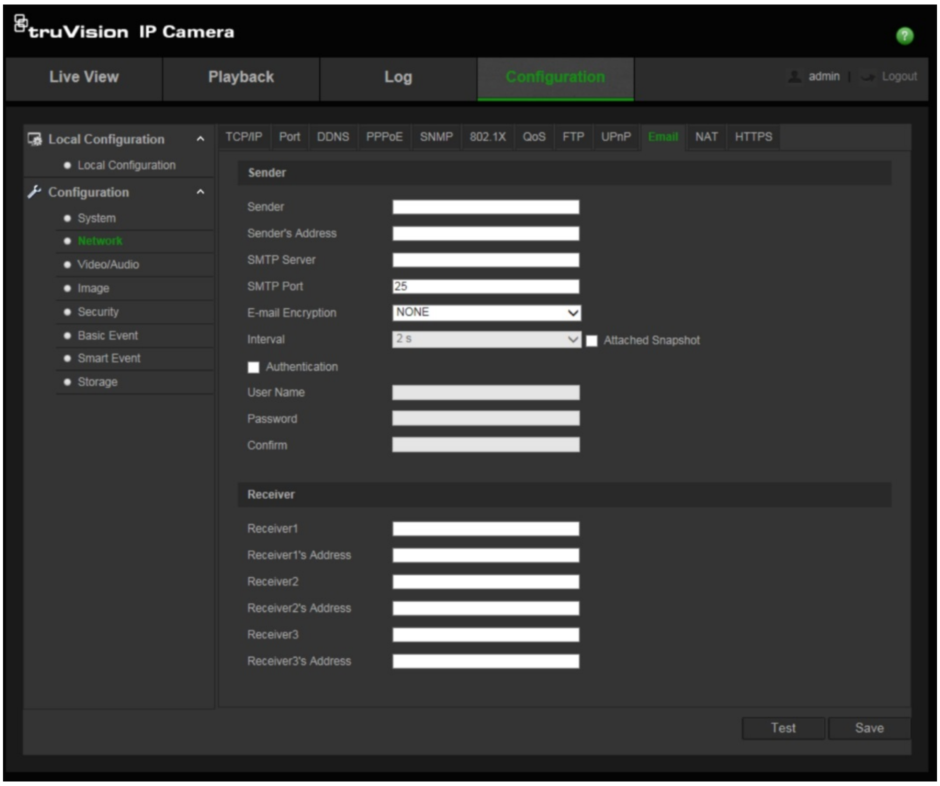
   Upload Type: To enable uploading the snapshots to the FTP server.
3. Click **Save** to save changes.

To define the UPnP parameters:

1. Click **Configuration** > **Network** > **UPnP**.
2. Check the check box 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.



Sender

Sender

Sender's Address

SMTP Server

SMTP Port 25

E-mail Encryption NONE

Interval 2 s □ Attached Snapshot

□ Authentication

User Name

Password

Confirm

Receiver

Receiver1

Receiver1's Address

Receiver2

Receiver2's Address

Receiver3

Receiver3's Address

2. Configure the following settings:

   Sender: The name of the email sender.

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

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

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

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

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

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

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

User Name: 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 user to be notified.

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

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

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

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

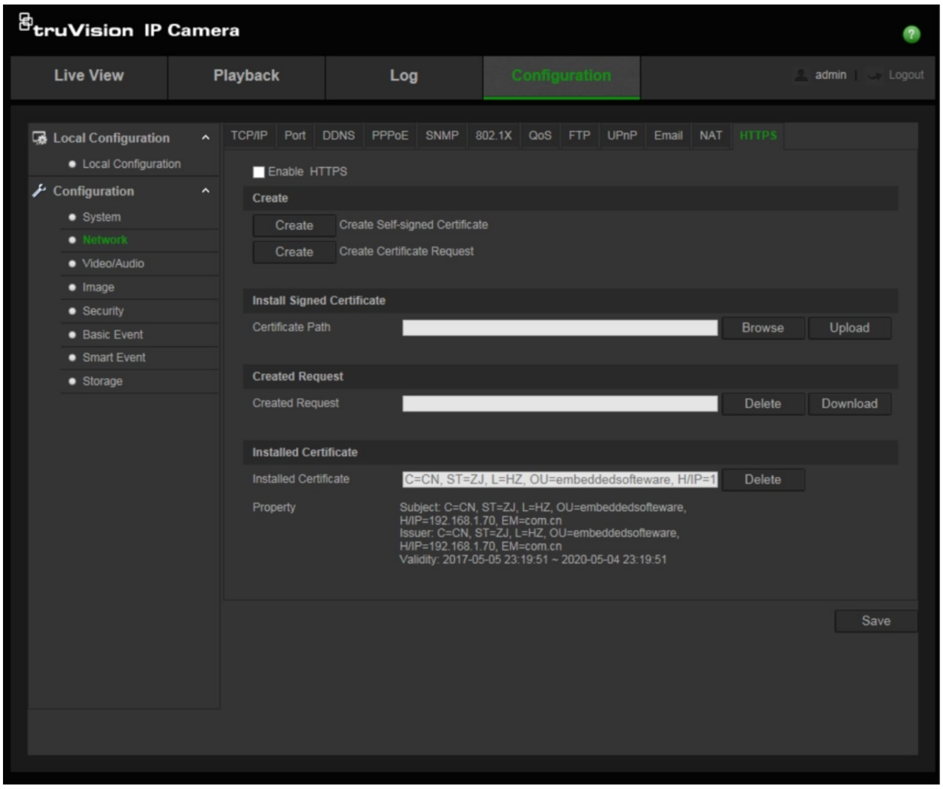
3. Click **Test** to test the email parameters set up.
4. Click **Save** to save changes.

To set up the NAT parameters:

1. Click **Configuration** > **Network** > **NAT**.
2. Check the check box to enable the NAT function.
3. Select **Port Mapping Mode** to be Auto or Manual. When you choose Manual mode, you can set the external port as you want.
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.



□ Enable HTTPS

Create

Create Self-signed Certificate

Create Certificate Request

Install Signed Certificate

Certificate Path

Created Request

Created Request

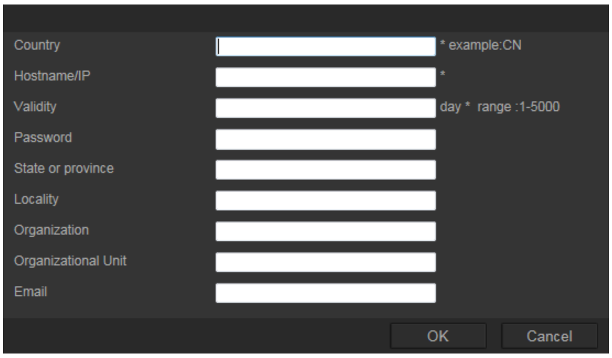
Installed Certificate

Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=1

Property: Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware,
H/IP=192.168.1.70, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware,
H/IP=192.168.1.70, EM=com.cn
Validity: 2017-05-05 23:19:51 ~ 2020-05-04 23:19:51

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.



Country * example:CN

Hostname/IP *

Validity day * range :1-5000

Password

State or province

Locality

Organization

Organizational Unit

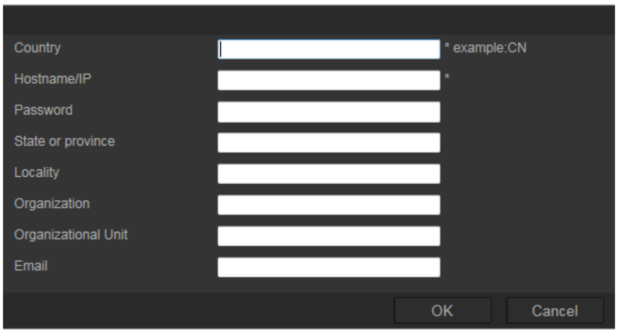
Email

   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.



Country * example:CN

Hostname/IP *

Password

State or province

Locality

Organization

Organizational Unit

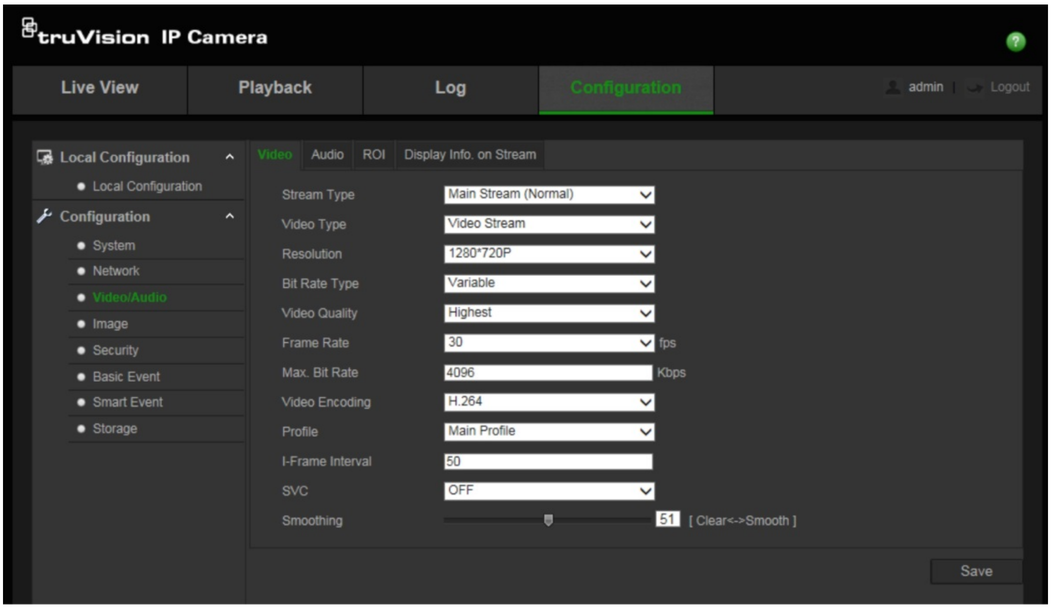
Email

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)



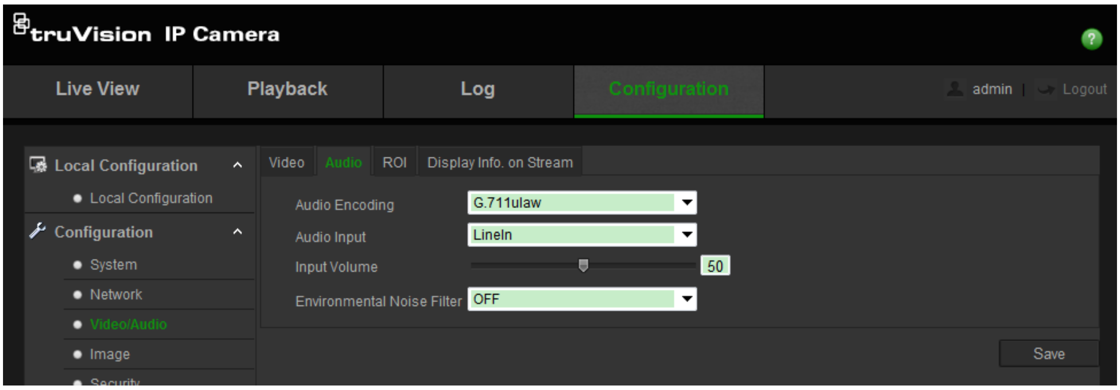
Stream Type: Main Stream (Normal)
Video Type: Video Stream
Resolution: 1280*720P
Bit Rate Type: Variable
Video Quality: Highest
Frame Rate: 30 fps
Max. Bit Rate: 4096 Kbps
Video Encoding: H.264
Profile: Main Profile
I-Frame Interval: 50
SVC: OFF
Smoothing: 51 [Clear<->Smooth]

Tab	Parameter descriptions
1. Video	**Stream Type**: Specifies the streaming method used. Options include: Main Stream (Normal), Sub Stream and Third stream. **Note**: The Third stream is only available when the this function is enabled in **System** > **Service**
	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.
	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 sub or third 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.

Tab	Parameter descriptions
	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 in its datasheet.
	Max bit rate: Specifies the maximum allowed bit rate. A high image resolution requires that a high bit rate must also be selected.
	Video Encoding: Specifies the video encoder used.
	Profile: Different profile indicates 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.
	Smoothing: Adjust the smoothness of the stream.
2. Audio	**Audio Encoding**: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726 and PCM are optional.
	Audio Input: Only “Linein” is available for the pickup microphone.
	Input Volume: Specifies the volume from 0 to 100.
	Environmental Noise Filter: Set it as OFF or ON. When you set the function on the noise detected can be filtered.
3. ROI	Enable to assign more encoding resources to the region of interest (ROI) to increase the quality of the ROI whereas the background information is less focused.
4. Display Info. On Stream	When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.

To configure audio settings:

1. From the menu toolbar, click **Configuration** > **Video/Audio** > **Audio**.



Audio Encoding: G.711ulaw

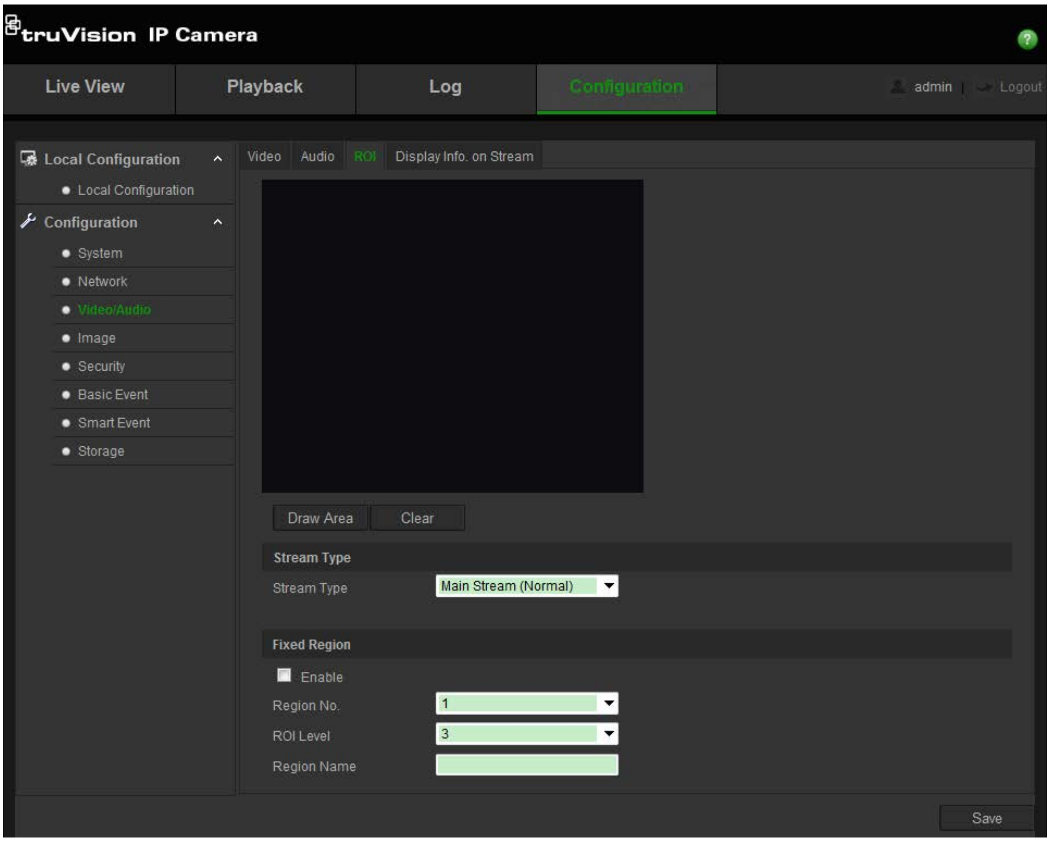
Audio Input: LineIn

Input Volume: 50

Environmental Noise Filter: OFF

To configure ROI settings:

1. From the menu toolbar, click **Configuration** > **Video/Audio** > **ROI**.



Stream Type

Stream Type: Main Stream (Normal)

Fixed Region

□ Enable

Region No.: 1

ROI Level: 3

Region Name:

2. Select the desired channel from the drop-down list.
3. Draw the region of interest on the image. Up to four regions can be drawn.
4. Choose the stream type to set the ROI encoding.
5. Enable **Fixed Region** to manually configure the area.

   Region No.: Select the region.

   ROI Level: Choose the image quality enhancing level.

   Region Name: Set the desired region name.

Dual-VCA (Video Content Analysis)

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

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

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

To define dual-VCA parameters:

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

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

Video image

You may need to adjust the camera image depending on the camera model or location background in order to get the best image quality. You can adjust the brightness, contrast, saturation, hue, and sharpness of the video image. See Figure 6 below for more information.

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

Figure 6: Camera image settings menu – Display Settings tab

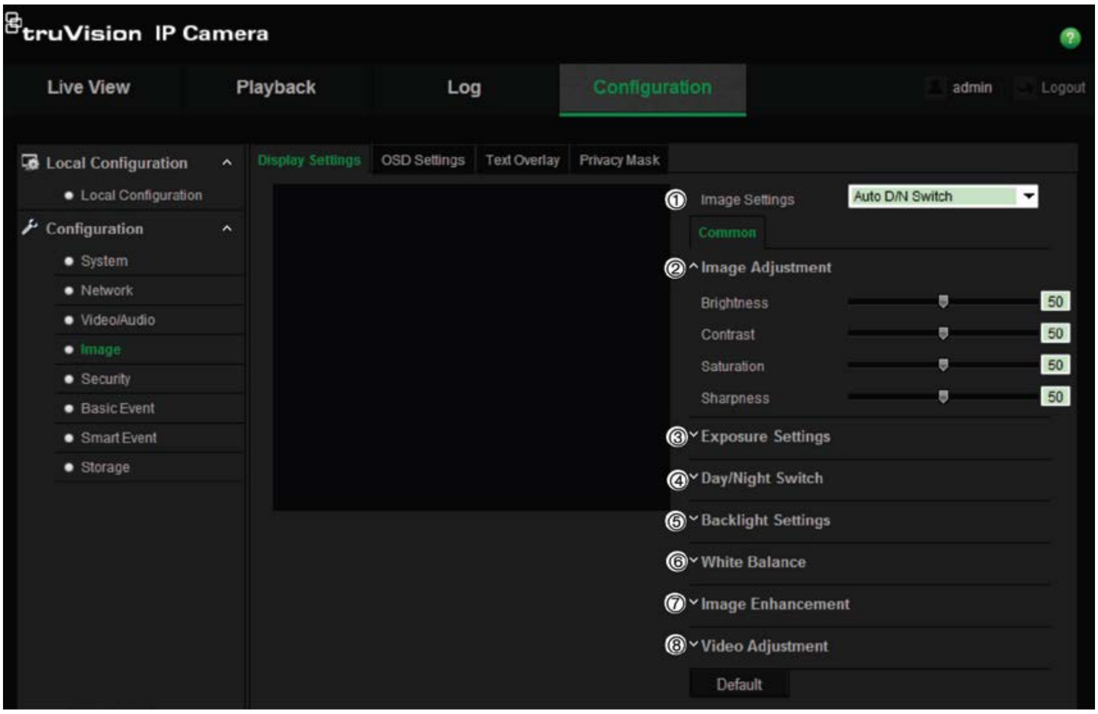


Image Settings: Auto D/N Switch

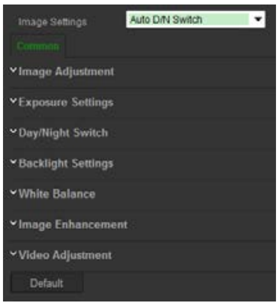
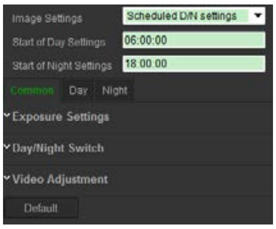
Image Adjustment

Brightness 50

Contrast 50

Saturation 50

Sharpness 50

Parameter	Description
1. Image Settings	
Auto D/N Switch	The camera automatically switches between day and night mode. All image settings remain the same for both modes. The image settings are: Image Adjustment, Exposure Settings, Day/Night Switch, Backlight Settings, White Balance, Image Enhancement, and Video Adjustment. *Common:* Set each image parameter individually for D/N switch. *Default*: Only use default settings.  Image Settings: Auto D/N Switch Common Image Adjustment Exposure Settings Day/Night Switch Backlight Settings White Balance Image Enhancement Video Adjustment Default
Custom 24-h settings	Customize the camera switch schedule for 24-hour settings. There are three tabs to configure the Custom 24-hour settings: *Common*, *Day*, *Night.* See "Scheduled D/N Switch" below for further information.
Scheduled D/N Switch	The camera switches between the day and night modes according to the schedule configured (see figure below). The start and end times shown are for day mode. The other time period is for night mode. There are three tabs to configure the day/night settings: *Common:* The settings are identical for both day and night modes for Exposure Settings, Day/Night Switch, and Video Adjustment. *Day*: Image Adjustment, Exposure Settings, Backlight Settings, White Balance, and Image Enhancement for day mode only. *Night*: Image Adjustment, Exposure Settings, Backlight Settings, White Balance, and Image Enhancement for night mode only.  Image Settings: Scheduled D/N settings Start of Day Settings: 06:00:00 Start of Night Settings: 18:00:00 Common Day Night Exposure Settings Day/Night Switch Video Adjustment Default
2. Image Adjustment	
Brightness, Contrast Saturation, Sharpness	Modify the different elements of picture quality by adjusting the values for each of parameter.

Parameter	Description
3. Exposure Settings	
Iris Mode	Select *Common* or *Manual iris mode*.
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. It can only be only selected for Day or Night mode of Scheduled D/N settings.
4. Day/Night Switch	
Day/Night Switch	Defines whether the camera is in day or night mode. The day (color) option could be used, for example, if the camera is located indoors where light levels are always good. Select one of the options: **Day**: Camera is always in day mode. **Night**: Camera is always in night mode. **Auto**: The camera automatically detects which mode to use. **Schedule**: The camera switches between day and night mode according to the configured time period. **Triggered by Alarm Input**: The camera switches to day or night mode after an 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. 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 between switchover the day/night switch. Set it between 5 and 120 s.
Smart IR	When enabled, it can avoid over exposure issue.
IR Light	Select On/OFF to Enable/disable IR. **Enable**: The IR LEDs are ON when the camera changes to night mode. **Disable**: The IR LEDs are OFF when the camera changes to night mode **Note**: The IR LEDs are always OFF in day mode.
5. Backlight Settings	
BLC Area	This function improves image quality when the background illumination is high. It prevents the object in the center of the image from appearing too dark. Select OFF, Up, Down, Left, Right, or Center. When WDR is enabled, BLC cannot be configured.
WDR	When enabled, wide dynamic range (WDR) provides clear images when there is high contrast between light and dark areas in the field of view of the camera. Both bright and dark areas can be displayed in the frame.

Parameter	Description
6. White Balance	
White Balance	White balance (WB) tells the camera what the color white looks like. Based on this information, the camera will then continue to display all colors correctly even when the color temperature of the scene changes such as from daylight to fluorescent lighting, for example. Select one of the options: **MWB:** Manually adjust the color temperature to meet your own requirements. **AWB1:** Apply for small range of 2500 to 9500K, for environments where the lighting is always stable. **Fluorescent Lamp:** For use where there are fluorescent lamps installed near the camera. **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.
7. Image Enhancement	
Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance. Select 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.
8. Video Adjustment	
Mirror	It mirrors the image so you can see it inversed. Select Left/Right, Up/Down, Center, or OFF. Default is OFF.
Hallway View	This function adjusts the image to suit long narrow scenes, such as corridors. Produces an image with a 9:16 ratio aspect to avoid including walls. During installing, 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.
Scene Mode	Select indoor or outdoor according to the current environment.
Video Standard	Select 50 Hz or 60 Hz. Select the value depending on the video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

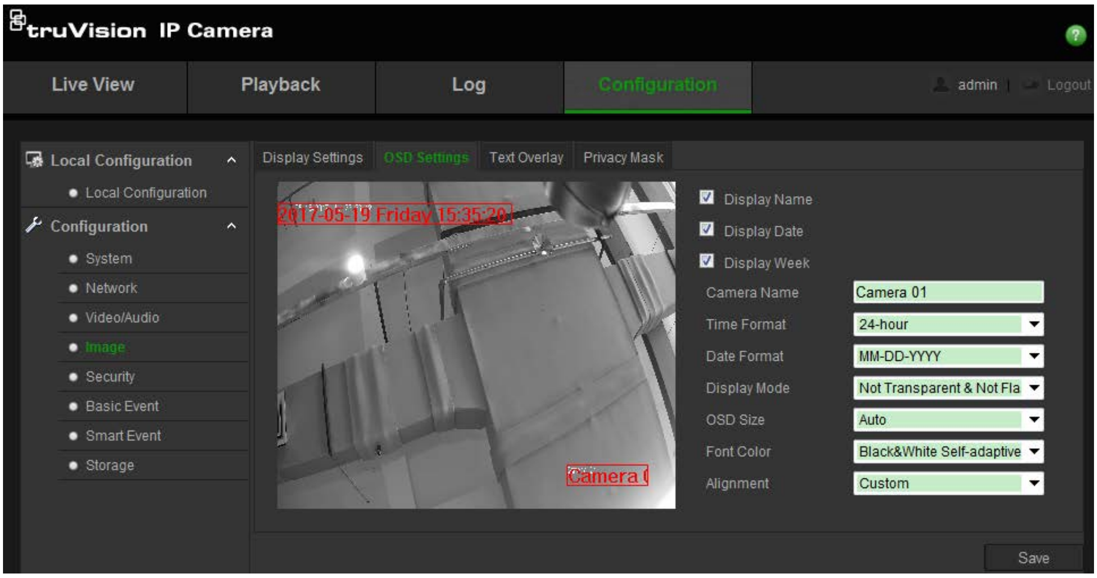
Note: Click the **Default** button to default all the image settings.

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** .



☑ Display Name

☑ Display Date

☑ Display Week

Camera Name: Camera 01

Time Format: 24-hour

Date Format: MM-DD-YYYY

Display Mode: Not Transparent & Not Fla

OSD Size: Auto

Font Color: Black&White Self-adaptive

Alignment: Custom

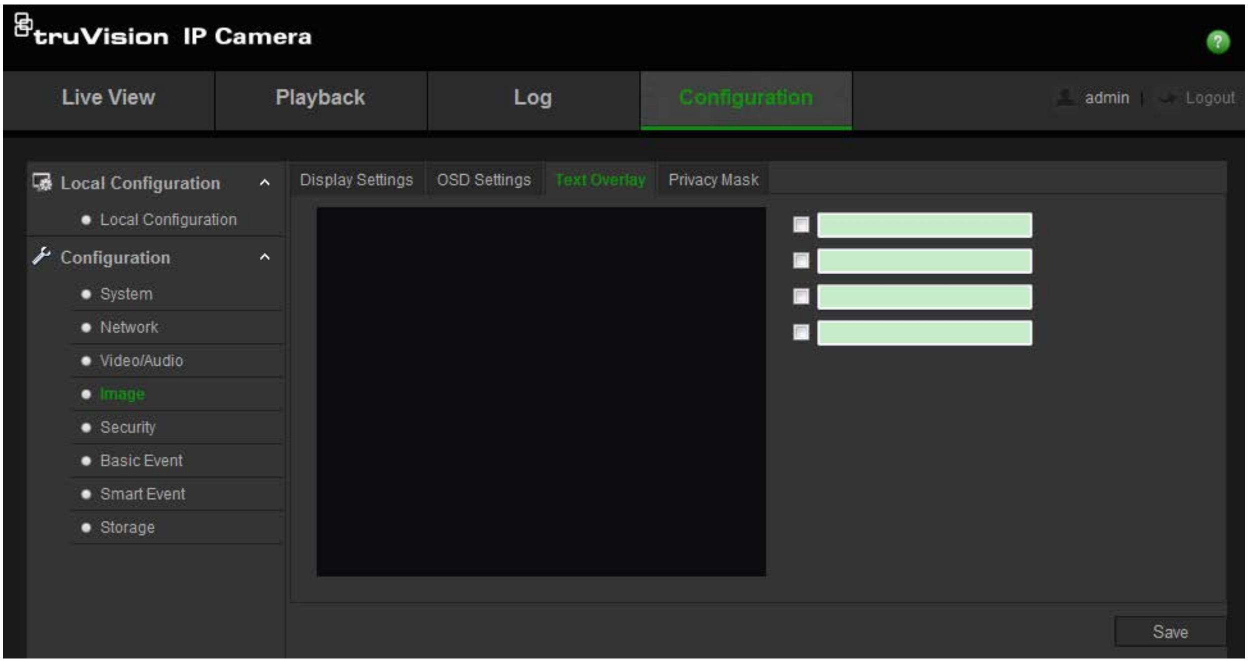
2. Check the **Display Name** box to display the camera's name on screen. You can modify the default name in the text box of **Camera Name**.
3. Select the **Display Date** check box to display the date/time on screen.
4. Select the **Display Week** check box to include the day of the week in the on-screen display.
5. In the **Camera Name** box, enter the camera name.
6. Select the time and date formats from the **Time format** and **Date format** drop-down list boxes.
7. Select a display mode for the camera from the **Display Mode** drop-down list box. Display modes include:
   - **Transparent & Not flashing.** The image appears through the text.
   - **Transparent & Flashing**. **T**he image appears through the text. The text flashes on and off.
   - **Not transparent & Not flashing.** The image is behind the text. This is default.
   - **Not transparent & Flashing**. The image is behind the text. The text flashes on and off.
8. Select the desired OSD size.
9. Select the desired font color.
10. Select the desired alignment (Custom or Align Right).
11. Click **Save** to save changes.

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

Text Overlay

Up to four lines of text can be added 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. Select the check box for the first line of text.
3. Enter the text in the text box.
4. Use the mouse to click and drag the red text in the live view window to adjust the text overlay position.
5. Repeat steps 2 to 4 for each extra line of text, selecting the next string number.

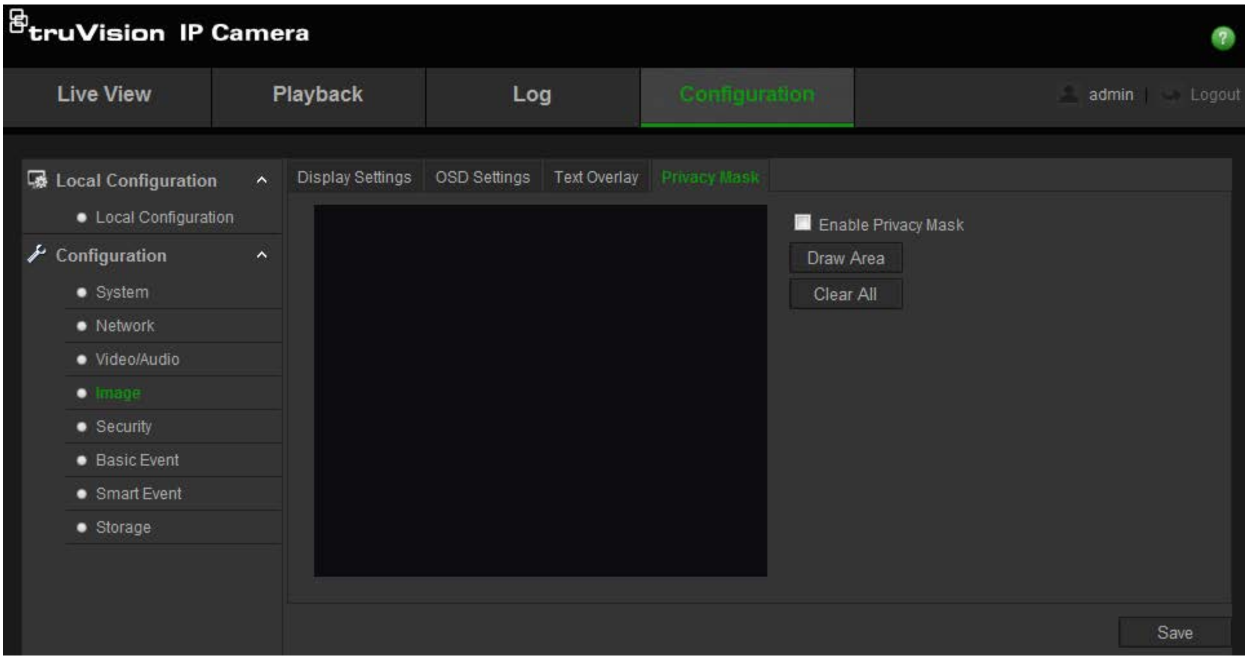
   Note: Remove an overlay text by deselecting its text line.
6. Click **Save** to save changes.

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 privacy mask area:

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

   Note: You are allowed to draw up to four areas on the same image.
5. Click **Stop Drawing** to finish drawing, or click **Clear All** to clear all of the areas you set without saving them.
6. Click **Save** to save changes.

Motion detection alarms

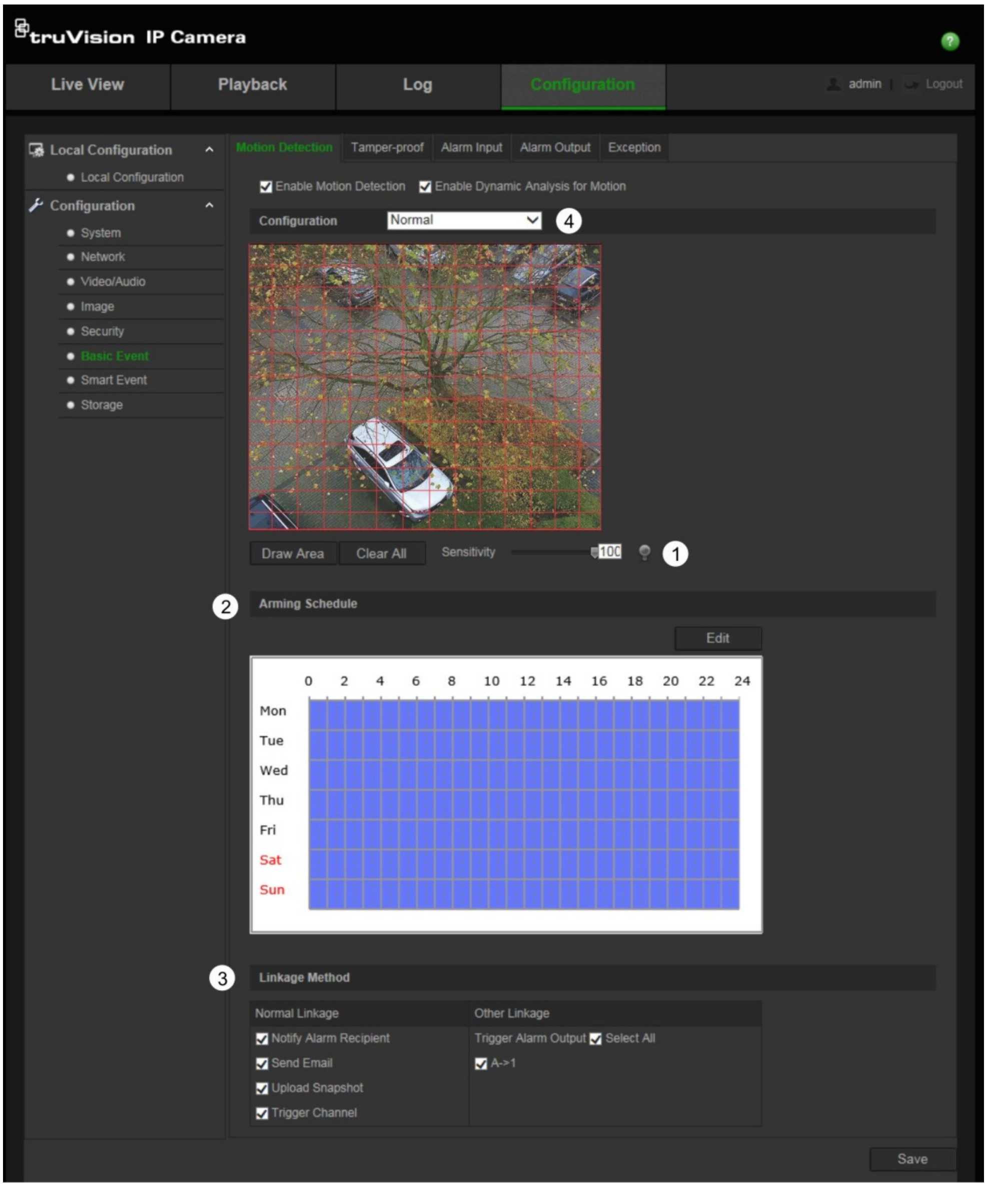
You can define motion detection alarms. A motion detection alarm refers to an alarm triggered when the camera detects motion. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

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

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

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

Figure 9: Motion detection window



☑ Enable Motion Detection ☑ Enable Dynamic Analysis for Motion

Configuration: Normal

Sensitivity: 100

Normal Linkage	Other Linkage
☑ Notify Alarm Recipient	Trigger Alarm Output ☑ Select All
☑ Send Email	☑ A->1
☑ Upload Snapshot	
☑ Trigger Channel	

Defining a motion detection alarm requires the following tasks:

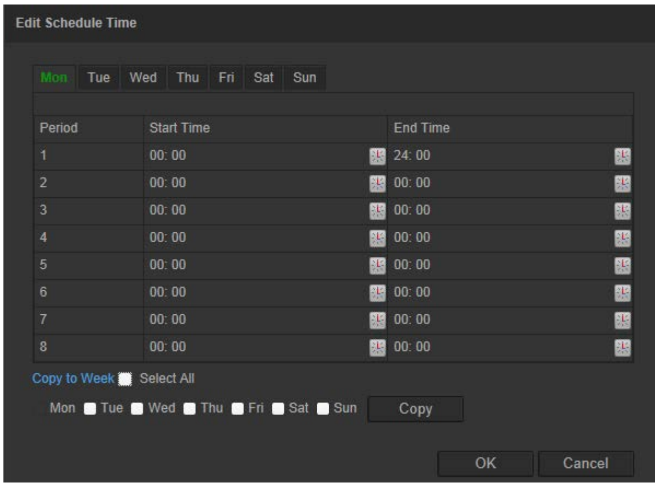
1. **Area settings**: Define the on-screen area that can trigger a motion detection alarm and the detection sensitivity level (see Figure 9, item 1).
2. **Arming schedule**: Define the schedule during which the system detects motion (see Figure 9, item 2).
3. **Recording schedule**: Define the schedule during which motion detection can be recorded. See “Recording Schedule” on page 51 for further information.
4. **Linkage**: Specify the method of response to the alarm (see Figure 9, item 3).
5. **Normal and advanced configuration**: Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 9, item 4). Advanced configuration gives you much more control over how motion is detected. It lets you set the sensitivity level as well as define the percentage of the motion detection area that the object must occupy, select day or night mode, and set up eight differently configured defined areas.

To set up motion detection in normal mode:

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

   Note: If you do not want the detected object to be marked with the green frame, select **Disable** from Configuration > Local Configuration > Live View Parameters > Rules.
3. Select **Normal** mode from the drop-down list.
4. Click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

   Note: You can draw up to 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, editable only if Enable Motion Detection. See the picture below for the editing interface of the arming schedule.



Period	Start Time	End Time
1	00: 00	24: 00
2	00: 00	00: 00
3	00: 00	00: 00
4	00: 00	00: 00
5	00: 00	00: 00
6	00: 00	00: 00
7	00: 00	00: 00
8	00: 00	00: 00

Copy to Week ☐ Select All

Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

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

Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 17 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.

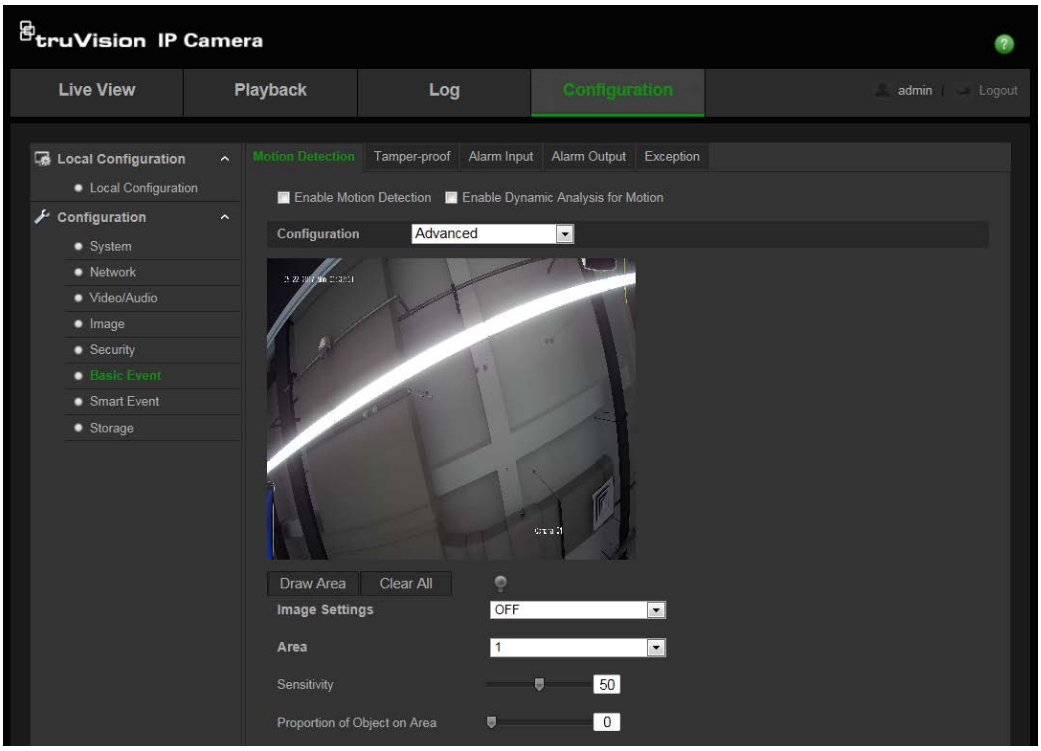
Upload Snapshot	Capture the image when an alarm is triggered and upload the picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 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 support 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 Configuration drop-down list.



□ Enable Motion Detection □ Enable Dynamic Analysis for Motion

Configuration: Advanced

Image Settings: OFF

Area: 1

Sensitivity: 50

Proportion of Object on Area: 0

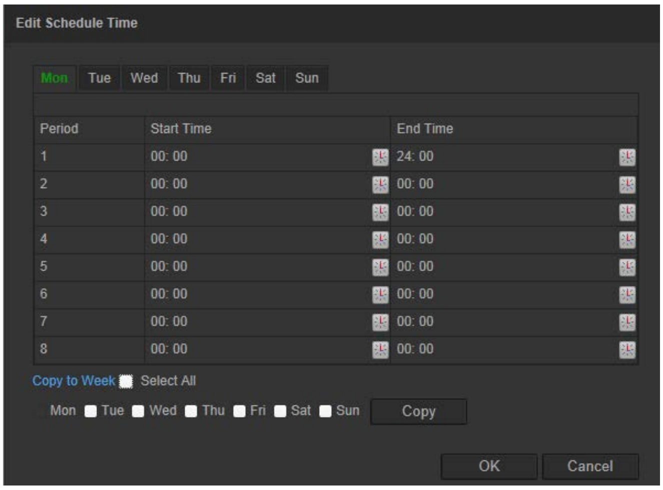
4. Under **Image Settings**, select OFF, Auto D/N Switch or Scheduled D/N settings. Default is OFF.

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

5. Select **Area No.** and click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

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

6. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
7. Move the **Sensitivity** slider to set the sensitivity of the detection for the selected areas.
8. Move the **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.



Edit Schedule Time

Period	Start Time	End Time
1	00: 00	24: 00
2	00: 00	00: 00
3	00: 00	00: 00
4	00: 00	00: 00
5	00: 00	00: 00
6	00: 00	00: 00
7	00: 00	00: 00
8	00: 00	00: 00

Copy to Week □ Select All

Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

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 when an event occurs. Check one or more response methods for the system when a motion detection alarm is triggered.

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

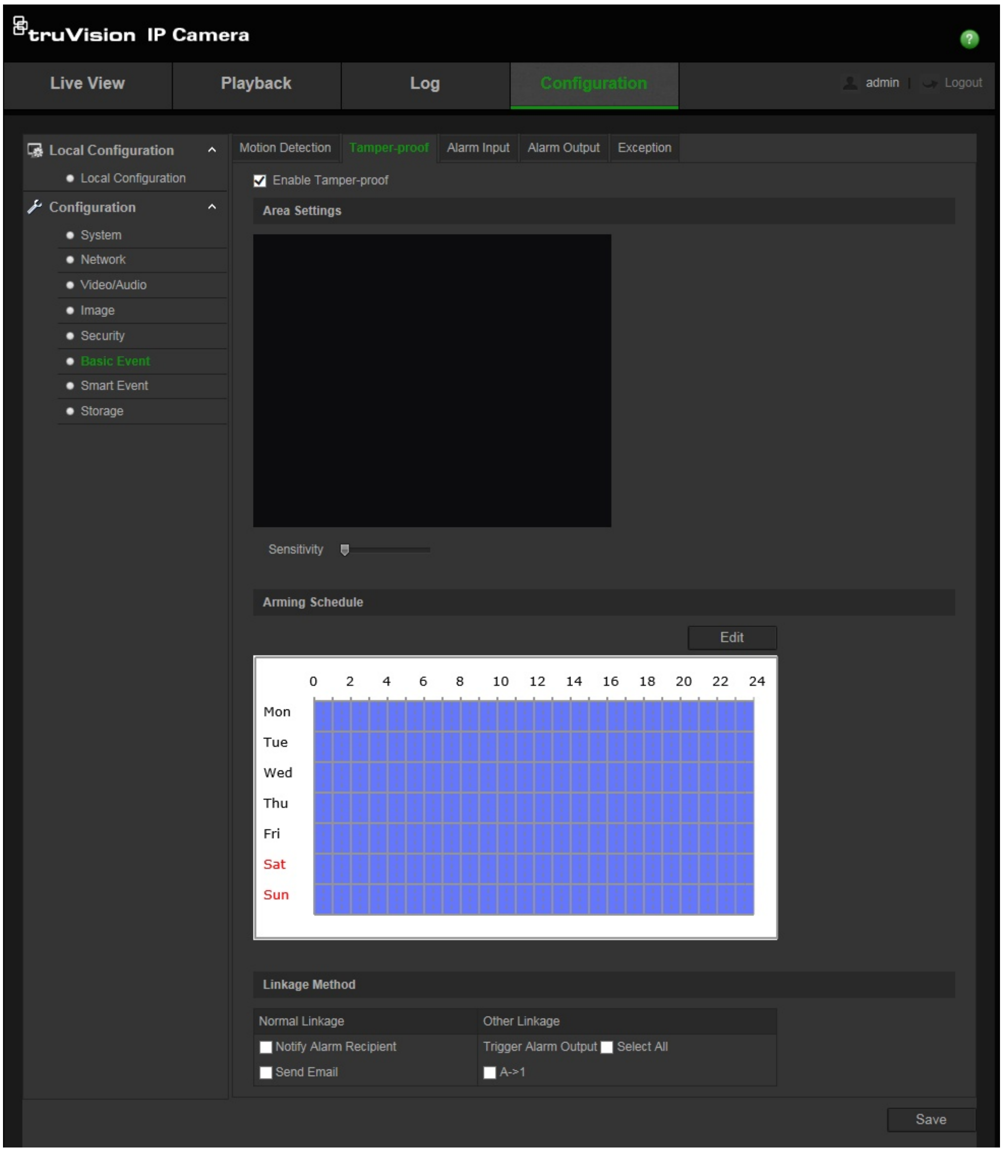
Send Email	Sends an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 17 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Upload Snapshot	Capture the image when an alarm is triggered and upload the picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 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 support 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 10: Tamper-proof alarm window



☑ Enable Tamper-proof

Normal Linkage	Other Linkage
□ Notify Alarm Recipient	Trigger Alarm Output □ Select All
□ Send Email	□ A->1

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 detection sensitivity.
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 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 17 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 support alarm output.

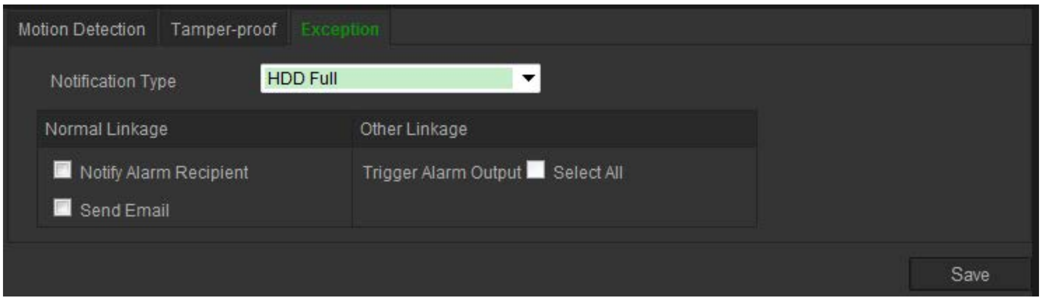
6. Click **Save** to save changes.

Exception alarms

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

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

Figure 11: Exception window



Notification Type: HDD Full

Normal Linkage	Other Linkage
□ Notify Alarm Recipient	Trigger Alarm Output □ Select All
□ Send Email	

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 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 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 picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 for further information.
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 support alarm output.

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

Alarm inputs and outputs

To define the external alarm input:

1. From the menu toolbar, click **Configuration** > **Basic Event** > **Alarm Input**.
2. Choose the **Alarm Input No.** and the **Alarm Type**. The alarm type can be NO (Normally Open) and NC (Normally Closed). Enter a name for the alarm input.
3. Click **Edit** to set the arming schedule for the alarm input. See “To set up motion detection” for more information.
4. Check the check box to select the linkage method.

Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Send Email	Sends an email to a specified address when there is 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 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 picture to NAS or FTP server. **Note:** To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 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 support alarm output.

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

To define alarm output:

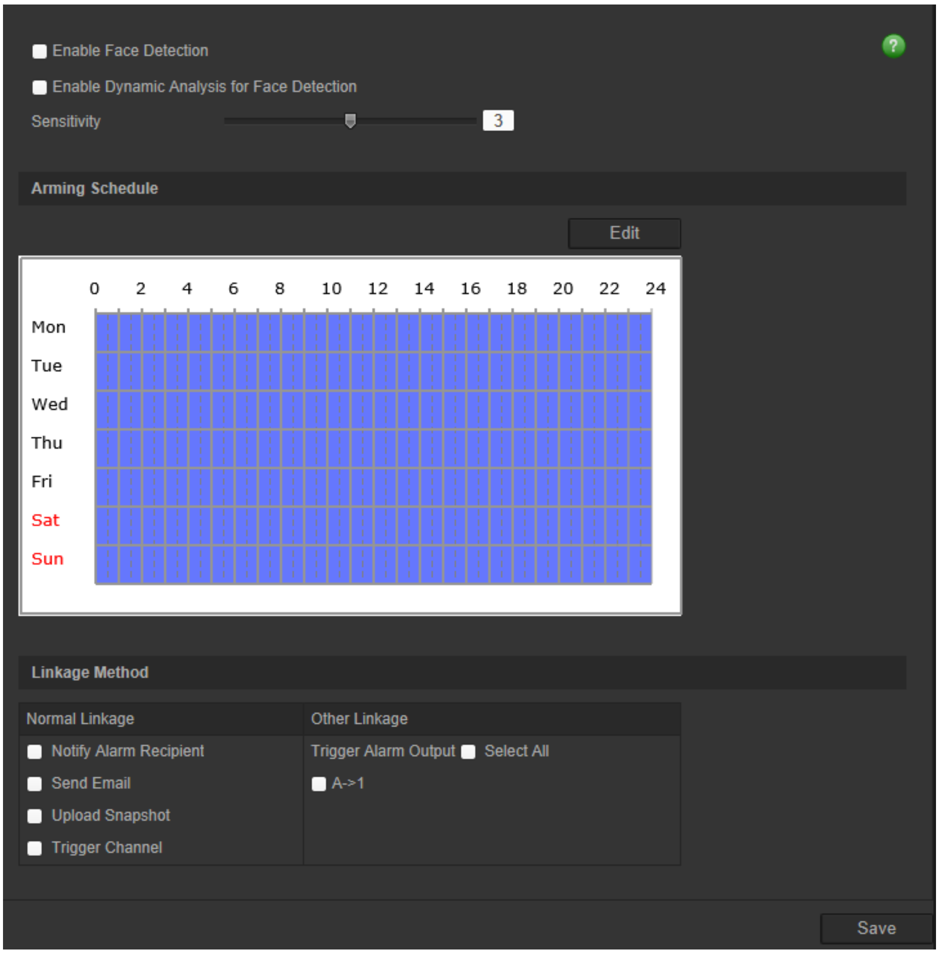
1. From the menu toolbar, click **Configuration** > **Basic Event** > **Alarm Output**.
2. Select one alarm output channel from the **Alarm Output** drop-down list. You can also set a name for the alarm output.
3. Set the delay time to 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min. The delay time refers to the time duration that the alarm output remains in effect after the 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 response. The camera can only detect a face looking directly into the camera, not side views. This feature is best suited when the camera is in front of a door or is located in a narrow corridor.

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

Figure 12: Face detection window



□ Enable Face Detection

□ Enable Dynamic Analysis for Face Detection

Sensitivity 3

Normal Linkage	Other Linkage
□ Notify Alarm Recipient	Trigger Alarm Output □ Select All
□ Send Email	□ A->1
□ Upload Snapshot	
□ Trigger Channel	

To define face detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Face Detection**.
2. Select the **Enable Face Detection** check box to enable the function.
3. Select the **Enable Dynamic Analysis** check box for **Face Detection** if you want the face detected to be marked with a green rectangle in live view.

   Note: If you do not want the detected face marked with the green frame, select **Disable** from Configuration > Local Configuration > Live View Parameters > 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 29 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 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 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 picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 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 support alarm output.

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

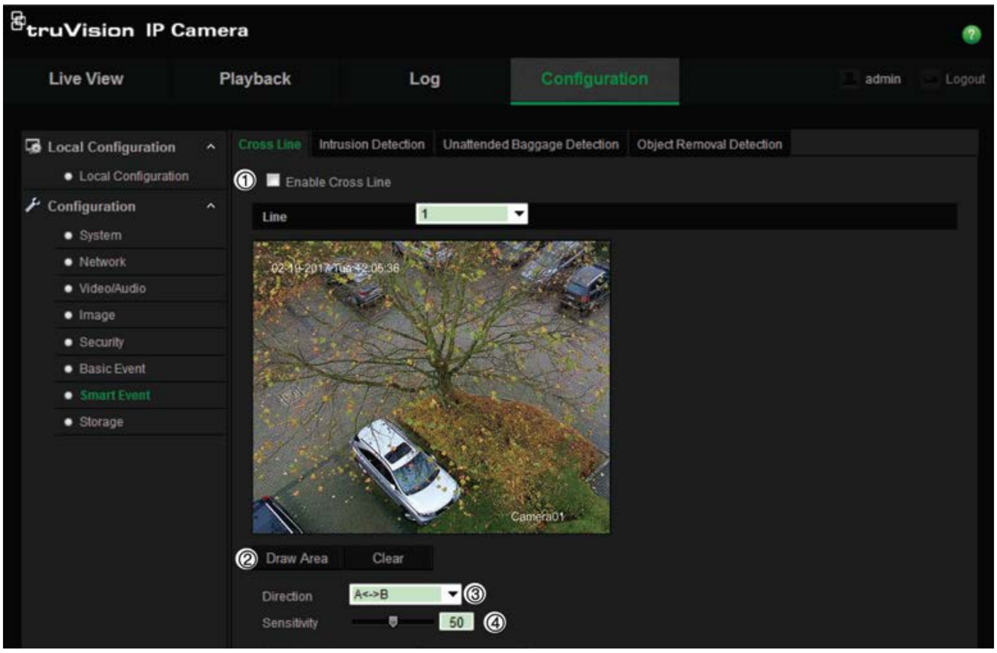
Cross line detection

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

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

To define cross line detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Cross Line**.



Line: 1

Direction: A<->B

Sensitivity: 50

2. Check the **Enable Cross Line** detection check box (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 list (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 29 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.

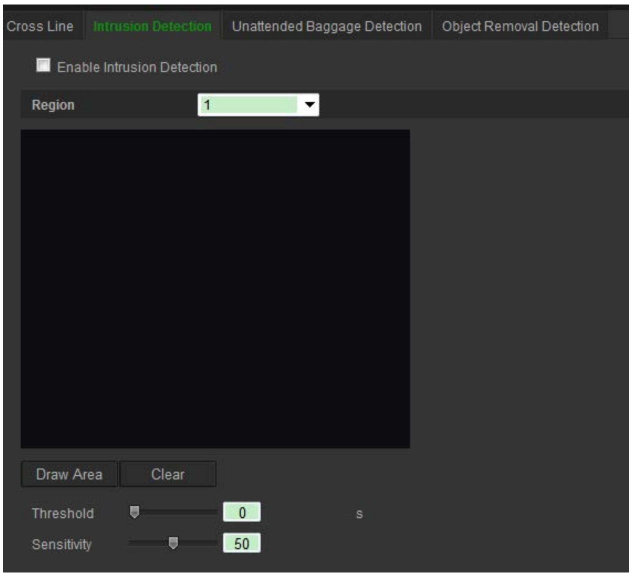
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Send Email	Send an email to a specified address when there is a cross line detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 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 picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 for further information.
Trigger Channel	Trigger 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 support 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. Up to four intrusion detection areas are supported. If someone enters the area, a set of alarm actions can be triggered.

Figure 13: Intrusion detection window



□ Enable Intrusion Detection

Region: 1

Threshold: 0 s

Sensitivity: 50

To define intrusion detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Intrusion Detection**.
2. Select the **Enable Intrusion Detection** check box to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the defense region.

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

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

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

   Sensitivity: The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, a small object can trigger an alarm. The range is between 1 and 100.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 29 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.

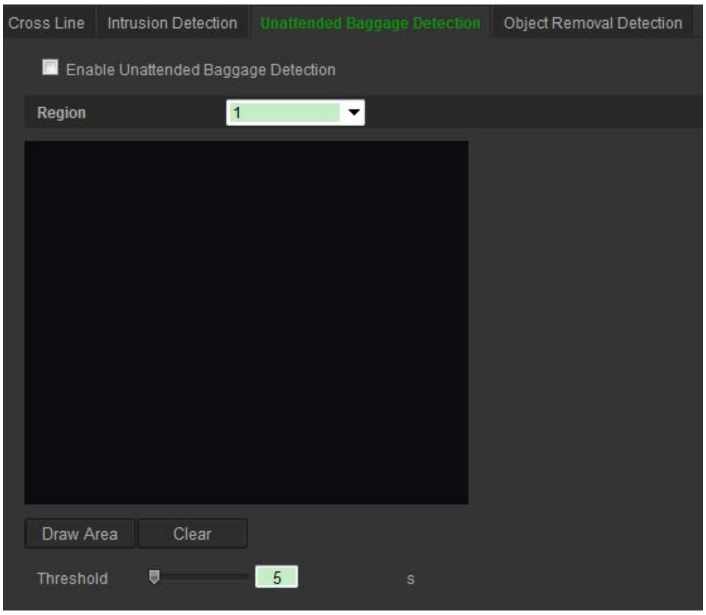
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Send Email	Send an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 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 picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 for further information.
Trigger Channel	Trigger 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 support alarm output.

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

Unattended Baggage Detection

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc. A series of actions can be taken when the alarm is triggered.

Figure 20: Unattended baggage detection window



□ Enable Unattended Baggage Detection

Region: 1

Threshold: 5 s

To define unattended baggage detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Unattended Baggage Detection.**
2. Select the **Enable Unattended Baggage Detection** check box to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the defense region.

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

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

   Threshold: the amount of the time an object is left in the region. If you set the value as 10, alarm is triggered after the object is in the region for 10 seconds. The range is from 5 to 100 s.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 29 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.

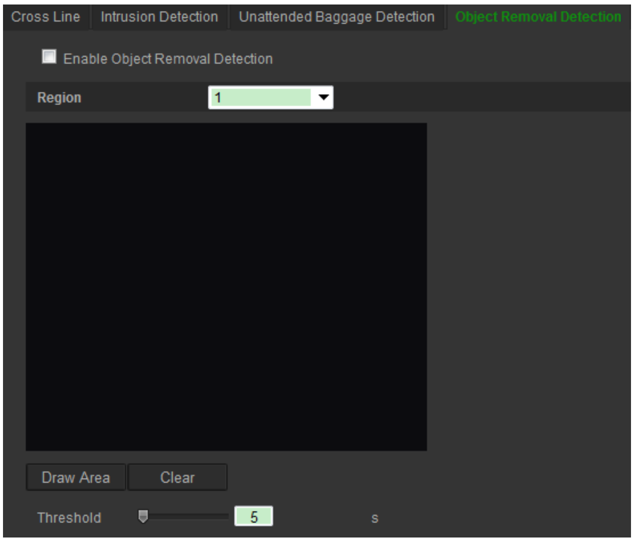
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Send Email	Send an email to a specified address when there is a motion detection alarm. **Note**: You must configure email settings before enabling this option. See “To set up the email parameters” on page 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 picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 for further information.
Trigger Channel	Trigger 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 support alarm output.

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

Object Removal Detection

Object removal detection function detects the objects removed from the pre-defined region, such as exhibits on display, and a series of actions can be taken when the alarm is triggered.

Figure 20: Object removal detection window



□ Enable Object Removal Detection

Region 1

Threshold 5 s

To define object removal detection:

1. From the menu toolbar, click **Configuration** > **Smart Event** > **Object Removal Detection.**
2. Select the **Enable Unattended Baggage Detection** check box to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the defense region.

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

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

   Threshold: The amount of time after an object is removed from the region. If you set the value as 10, alarm is triggered 10 seconds after the object is removed from the region. The range is from 5 to 100 s.
5. Click **Edit** to set the arming schedule for the alarm input. See “Motion detection alarms” on page 29 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 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 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 picture to NAS or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS settings” on page 49 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 17 for further information. Enable the **Upload Type** option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable **Enable Event-triggered Snapshot** under the snapshot parameters. See “Snapshot parameters” on page 48 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 support alarm output.

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

Snapshot parameters

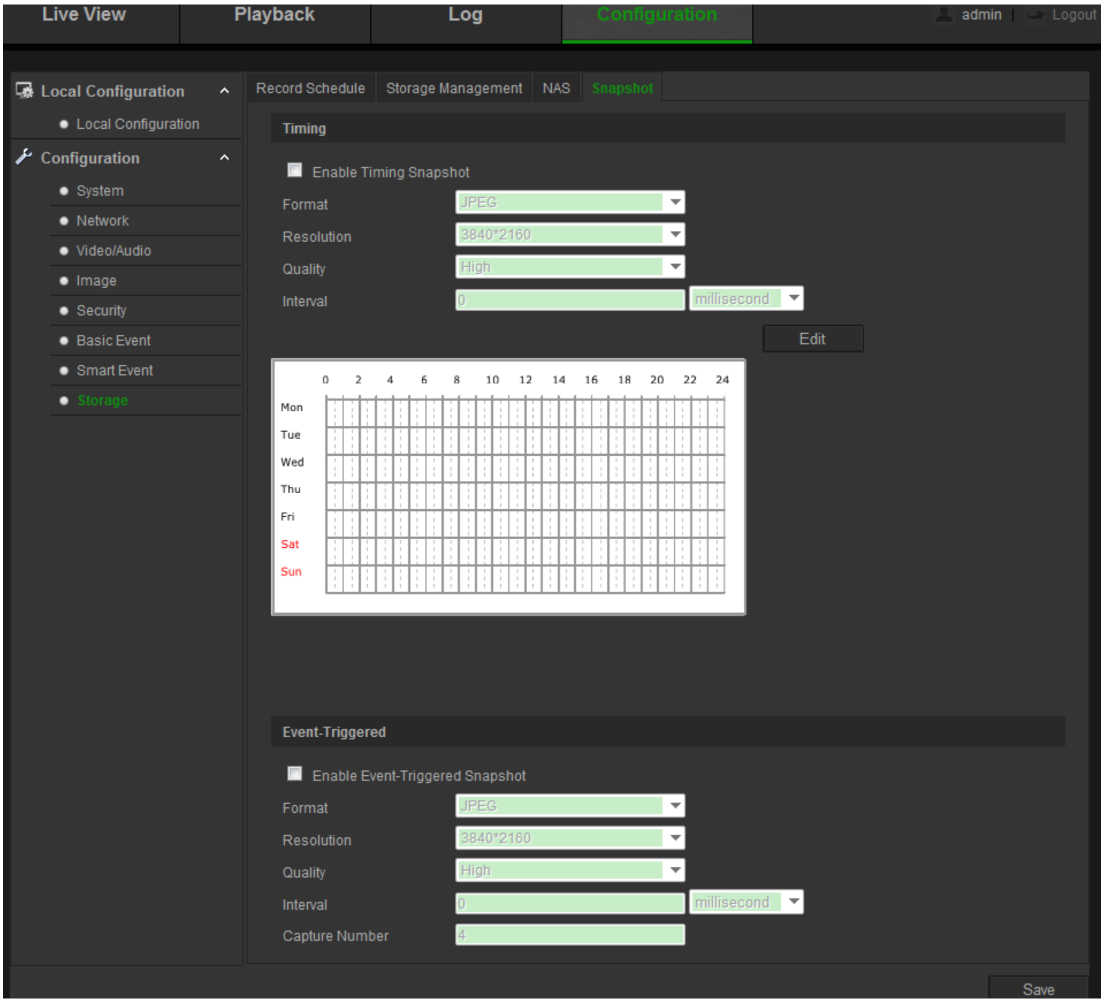
You can configure scheduled snapshots and event-triggered snapshots. The captured snapshots can be stored in the SD card (if supported) or the NAS. You can also upload the snapshots to an FTP server.

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

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 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 menu



Timing

☐ Enable Timing Snapshot

Format JPEG

Resolution 3840*2160

Quality High

Interval 0 millisecond

Edit

Event-Triggered

☐ Enable Event-Triggered Snapshot

Format JPEG

Resolution 3840*2160

Quality High

Interval 0 millisecond

Capture Number 4

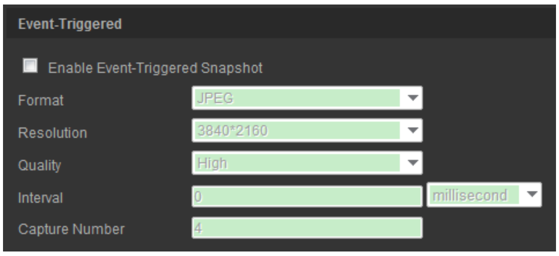
Save

To set up scheduled snapshots:

1. From the menu toolbar, click **Configuration** > **Storage** > **Snapshot**.
2. Select **Enable Timing Snapshot** check box to enable continuous snapshots.
3. Select the desired format of the snapshot, such as JPEG.
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. Select the **Enable Event-triggered Snapshot** check box to enable event-triggered snapshots.



Event-Triggered

□ Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 3840*2160

Quality: High

Interval: 0 millisecond

Capture Number: 4

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 can be taken.
7. Click **Save** to save changes.

NAS settings

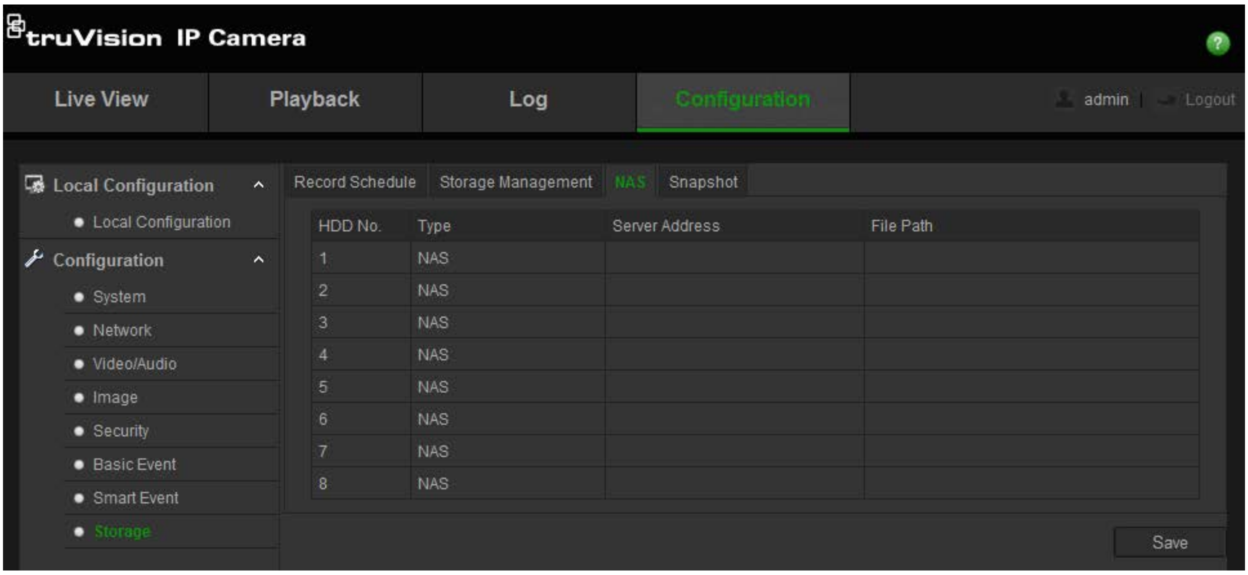
You can use a network storage system (NAS) to remotely store recordings.

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

Notes:

1. Up to eight NAS disks can be connected to a camera.
2. The recommended capacity of NAS is between 9G and 2T as otherwise it may cause formatting failure.

Figure 22: NAS menu



HDD No.	Type	Server Address	File Path
1	NAS		
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

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.

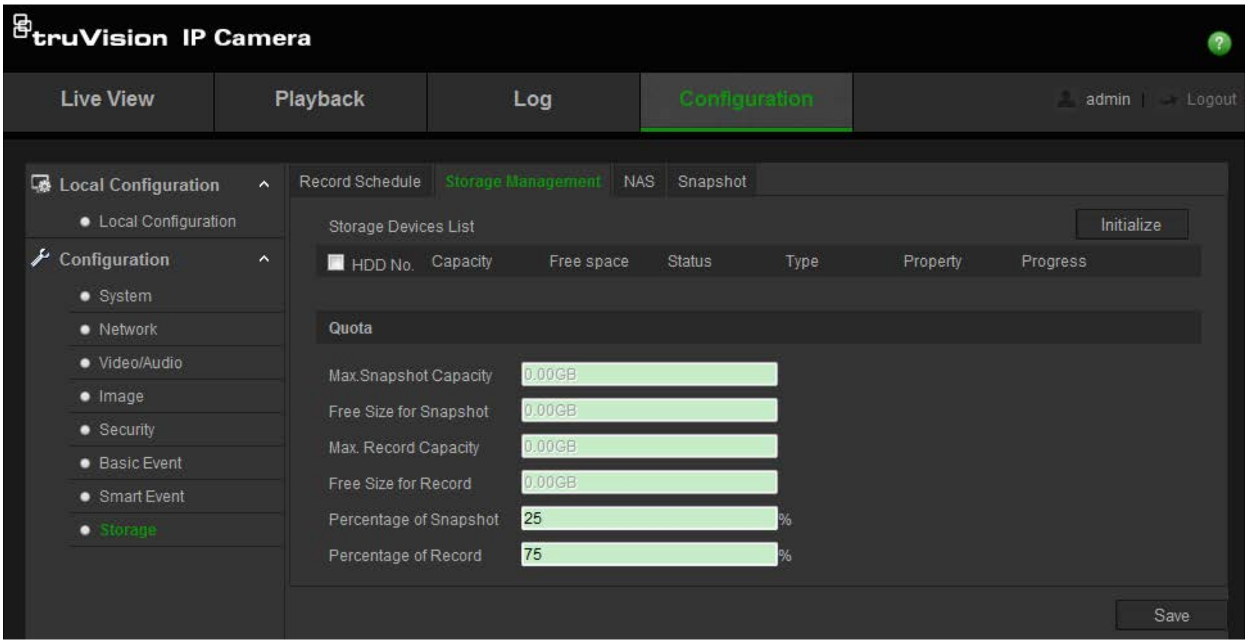
Storage devices

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. You can also format these storage devices.

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.

Figure 14: Storage window



Storage Devices List

□ HDD No.	Capacity	Free space	Status	Type	Property	Progress

Quota

Max.Snapshot Capacity 0.00GB

Free Size for Snapshot 0.00GB

Max. Record Capacity 0.00GB

Free Size for Record 0.00GB

Percentage of Snapshot 25 %

Percentage of Record 75 %

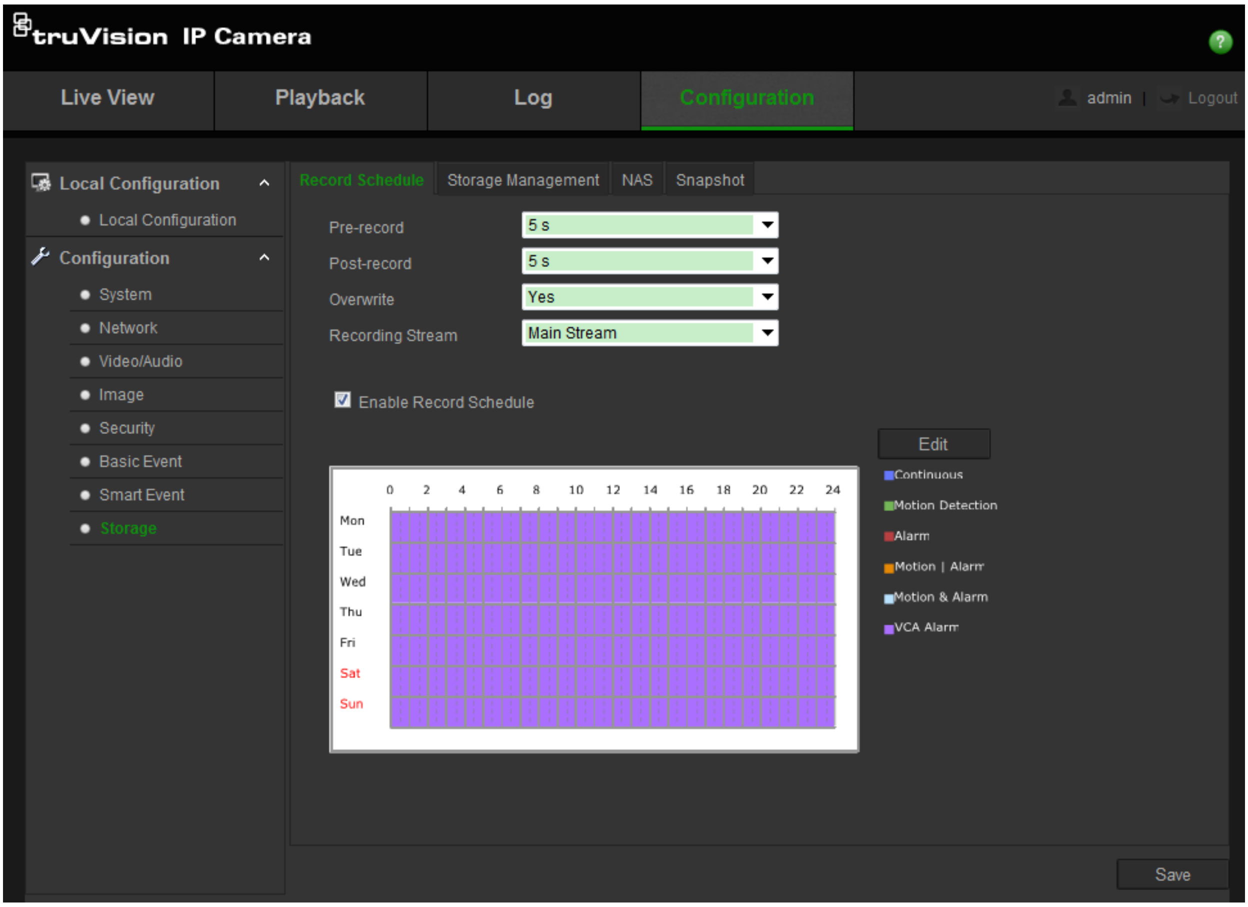
To format the storage devices:

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 permission.
5. Click **OK** to start formatting.

Recording Schedule

You can define a recording schedule for the camera in the “Record Schedule” window. The recording is saved on to the SD card or NAS in the camera. The camera’s SD card provides a backup in case of network failure. The SD card is not provided with the camera.

The selected recording schedule applies to all alarm types.



Pre-record: 5 s

Post-record: 5 s

Overwrite: Yes

Recording Stream: Main Stream

☑ Enable Record Schedule

Pre-record time

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

Post-record time

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

Overwrite

The camera record can be overwritten when *Overwrite* is enabled.

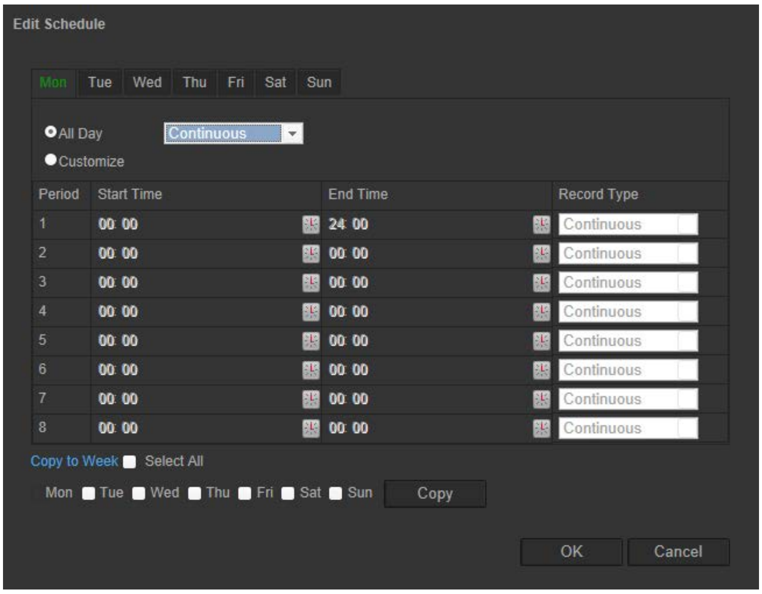
Recording Stream

Main Stream and Substream are alternative for the recording stream.

To set up a recording schedule:

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

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



● All Day   Continuous

○ Customize

Period	Start Time	End Time	Record Type
1	00:00	24:00	Continuous
2	00:00	00:00	Continuous
3	00:00	00:00	Continuous
4	00:00	00:00	Continuous
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Copy to Week □ Select All

Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

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

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

   - **Continuous**: This is continuous recording.
   - **Motion Detection:** Video is recorded when the 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 38 for more information.
   - **Cross Line**: Video is recorded when the pre-defined line on-screen in crossed. See “Cross line detection” on page 40 for more information.
   - **Intrusion Detection**: Video is recorded when an intrusion is detected. See “Intrusion detection” on page 42 for more information.
   - **Unattended Baggage Detection**: Video is recorded when the object is left on the pre-defined area.
   - **Object Removal Detection**: Video is recorded when the object is taken away from the pre-defined area.

5. If you enable “Custom”, 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 to record (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 the arming schedule in order to trigger motion detection or alarm input recording.

Camera management

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

User management

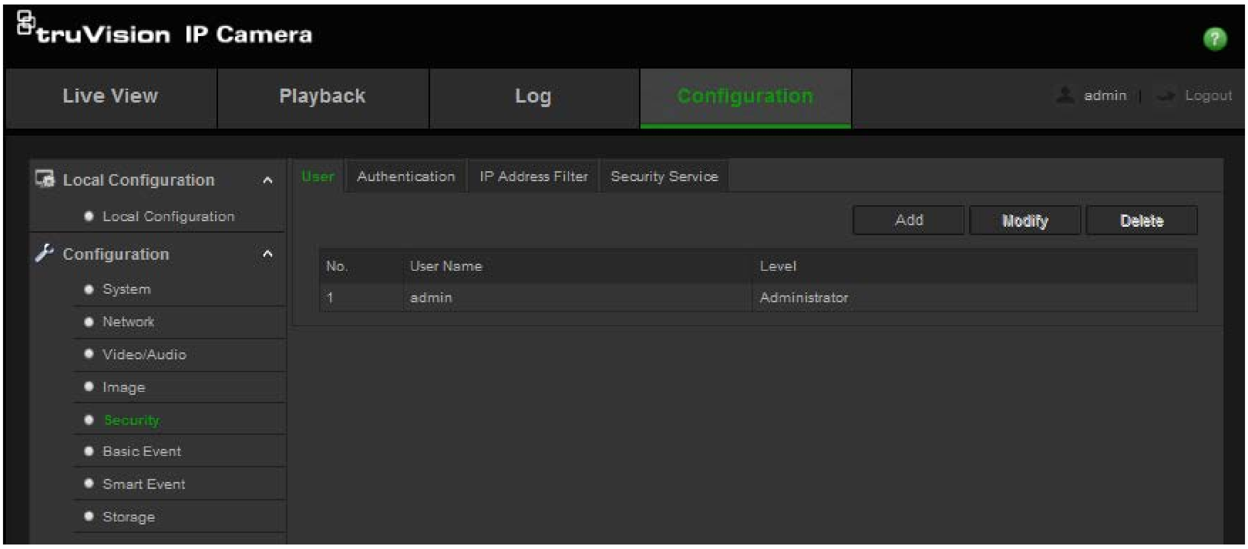
This section describes how to manage users. You can:

- Add or delete users
- Modify permission
- Modify passwords

Only the administrator can manage users. The administrator can create up to 31 individual users for the cameras listed in this manual.

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

Figure 15: User management window



No.	User Name	Level
1	admin	Administrator

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.

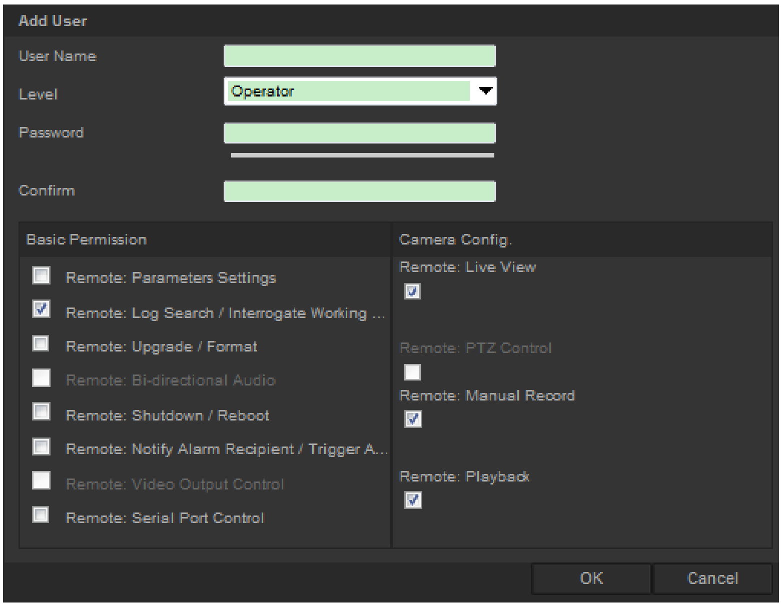
- **Operator**: This user can only change the configuration of his/her own account. An operator cannot create or delete other users.
- **Viewer**: This user has the permission of live view, playback and log search. However, they cannot change any configuration settings.

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.



Add User

User Name

Level: Operator

Password

Confirm

Basic Permission	Camera Config.
☐ Remote: Parameters Settings	Remote: Live View ☑
☑ Remote: Log Search / Interrogate Working ...	Remote: PTZ Control ☐
☐ Remote: Upgrade / Format	Remote: Manual Record ☑
☐ Remote: Bi-directional Audio	Remote: Playback ☑
☐ Remote: Shutdown / Reboot	
☐ Remote: Notify Alarm Recipient / Trigger A...	
☐ Remote: Video Output Control	
☐ Remote: Serial Port Control	

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:

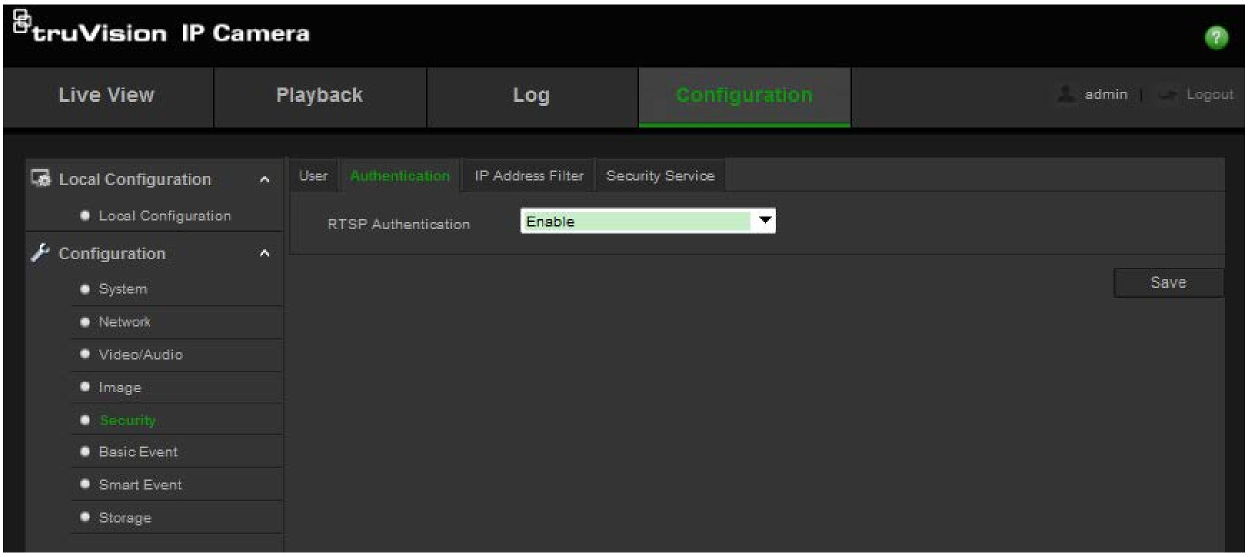
1. Select the desired user under the **User** tab.
2. Click the **Modify** button. The user management window appears
3. Change the information required.

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

RTSP authentication

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

Figure 16: RTSP authentication window



RTSP Authentication: Enable

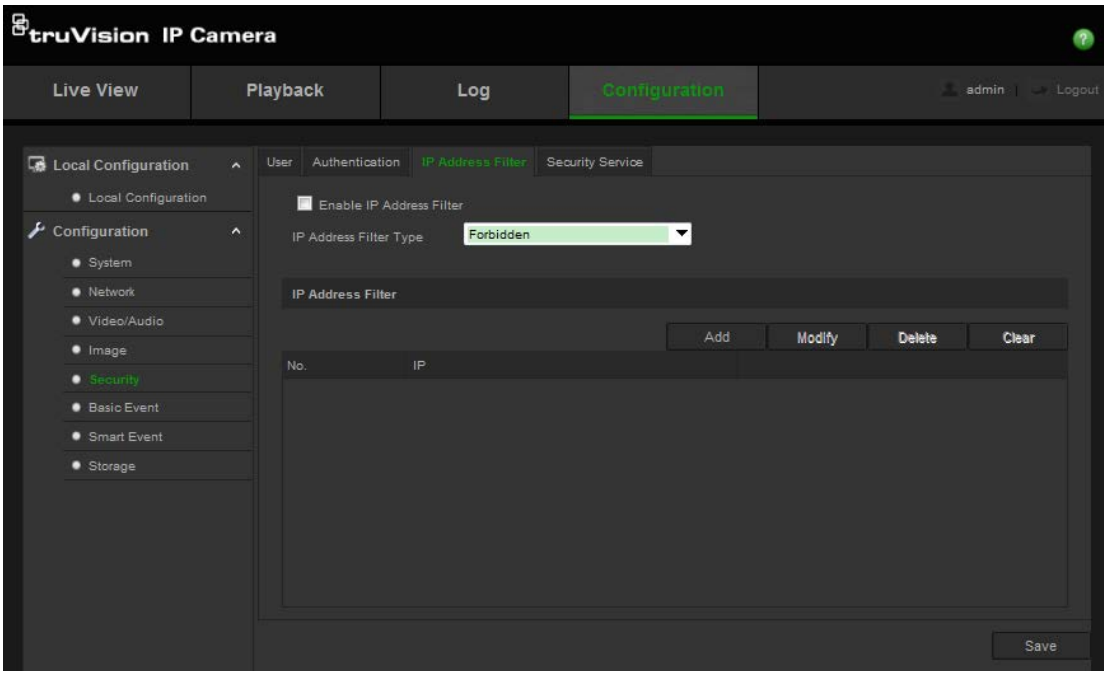
To define RTSP authentication:

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

IP address filter

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

Figure 17: IP address filter window



□ Enable IP Address Filter

IP Address Filter Type: Forbidden

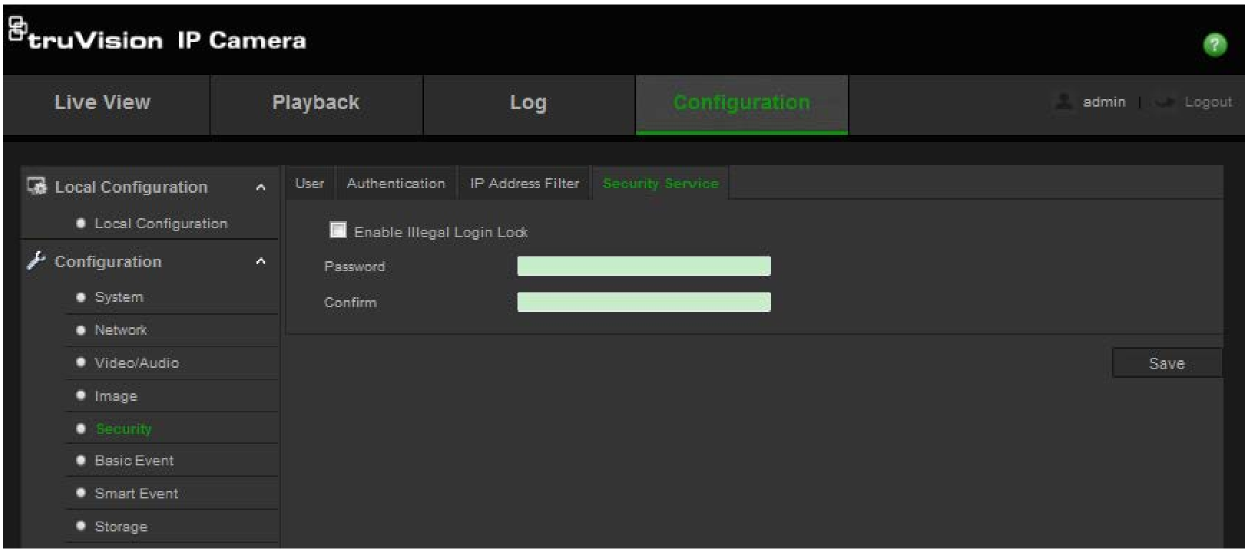
To define the IP address filter:

1. From the menu toolbar, click **Configuration** > **Security** > **IP Address Filter**.
2. Select the **Enable IP Address Filter** check box**.**
3. Select the type of IP Address Filter in the drop-down list: Forbidden or Allowed.
4. Click **Add** to add an IP address and enter the address.
5. Click **Modify** or **Delete** to modify or delete the selected IP address**.**
6. Click **Clear** to delete all the IP addresses.
7. Click **Save** to save the changes.

Defining the security service

This function enables Telnet and let you define its password. It is only used by Technical Support.

Figure 18: Security service window



□ Enable Illegal Login Lock

Password

Confirm

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

Restore default settings

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

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

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

To restore default settings:

1. From the menu toolbar, click **Configuration** > **System**> **Maintenance**.
2. Click either **Restore** or **Default**. A window showing user authentication appears.
3. Enter the admin password and click OK.
4. Click **OK** in the pop-up message box to confirm restoring operation.

Import/export a configuration file

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

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

To import/export configuration file:

1. 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 on to your computer the latest firmware from our web site at:

   www.interlogix.com/video/product/truvision-ip-open-standards-outdoor-cameras/

   - Or -

   www.utcfssecurityproductspages.eu/videoupgrades/
2. When the firmware file is downloaded to your computer, extract the file to the desired destination.

   Note: Do not save the file on your desktop.

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

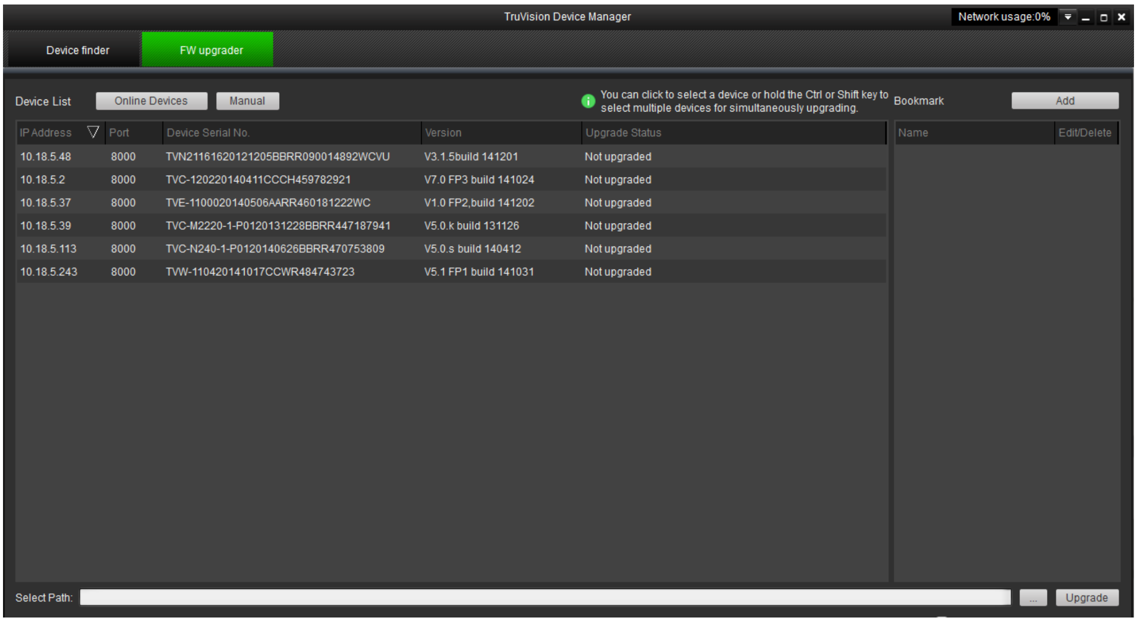
    - **Firmware directory** – Locate the upgrading folder of Firmware files. The camera will choose the corresponding firmware file automatically.
    - **Firmware** – Locate the firmware file manually for the camera.

    Note: Please select Interlogix_Gen_3_ipc.dav for camera models listed in the "Introduction" on page 3.

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

To upgrade the firmware via TruVision Device Manager:

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



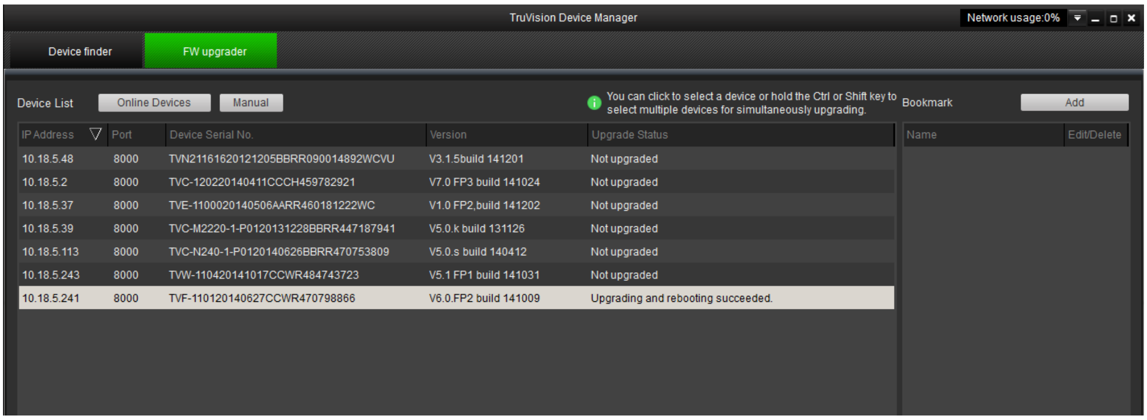
You can click to select a device or hold the Ctrl or Shift key to select multiple devices for simultaneously upgrading.

IP Address	Port	Device Serial No.	Version	Upgrade Status
10.18.5.48	8000	TVN21161620121205BBRR090014892WCVU	V3.1.5build 141201	Not upgraded
10.18.5.2	8000	TVC-120220140411CCCH459782921	V7.0 FP3 build 141024	Not upgraded
10.18.5.37	8000	TVE-1100020140506AARR460181222WC	V1.0 FP2,build 141202	Not upgraded
10.18.5.39	8000	TVC-M2220-1-P0120131228BBRR447187941	V5.0.k build 131126	Not upgraded
10.18.5.113	8000	TVC-N240-1-P0120140626BBRR470753809	V5.0.s build 140412	Not upgraded
10.18.5.243	8000	TVW-110420141017CCWR484743723	V5.1 FP1 build 141031	Not upgraded

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.



You can click to select a device or hold the Ctrl or Shift key to select multiple devices for simultaneously upgrading.

IP Address	Port	Device Serial No.	Version	Upgrade Status
10.18.5.48	8000	TVN21161620121205BBRR090014892WCVU	V3.1.5build 141201	Not upgraded
10.18.5.2	8000	TVC-120220140411CCCH459782921	V7.0 FP3 build 141024	Not upgraded
10.18.5.37	8000	TVE-1100020140506AARR460181222WC	V1.0 FP2,build 141202	Not upgraded
10.18.5.39	8000	TVC-M2220-1-P0120131228BBRR447187941	V5.0.k build 131126	Not upgraded
10.18.5.113	8000	TVC-N240-1-P0120140626BBRR470753809	V5.0.s build 140412	Not upgraded
10.18.5.243	8000	TVW-110420141017CCWR484743723	V5.1 FP1 build 141031	Not upgraded
10.18.5.241	8000	TVF-110120140627CCWR470798866	V6.0.FP2 build 141009	Upgrading and rebooting succeeded.

Reboot camera

It is easy to reboot the camera 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

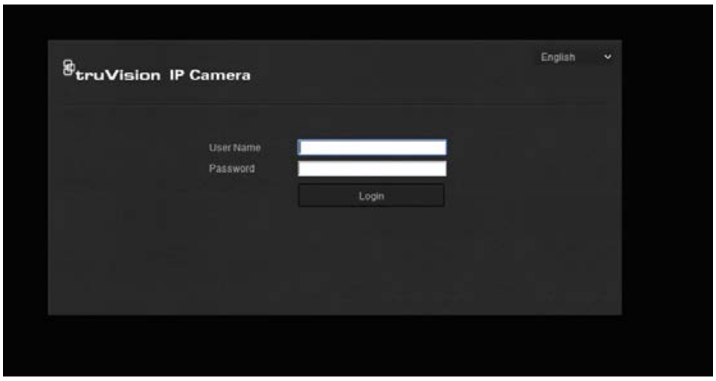
This chapter describes how to use the camera once it is installed and configured.

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 19: Login dialog box



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

Live view mode

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

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

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

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

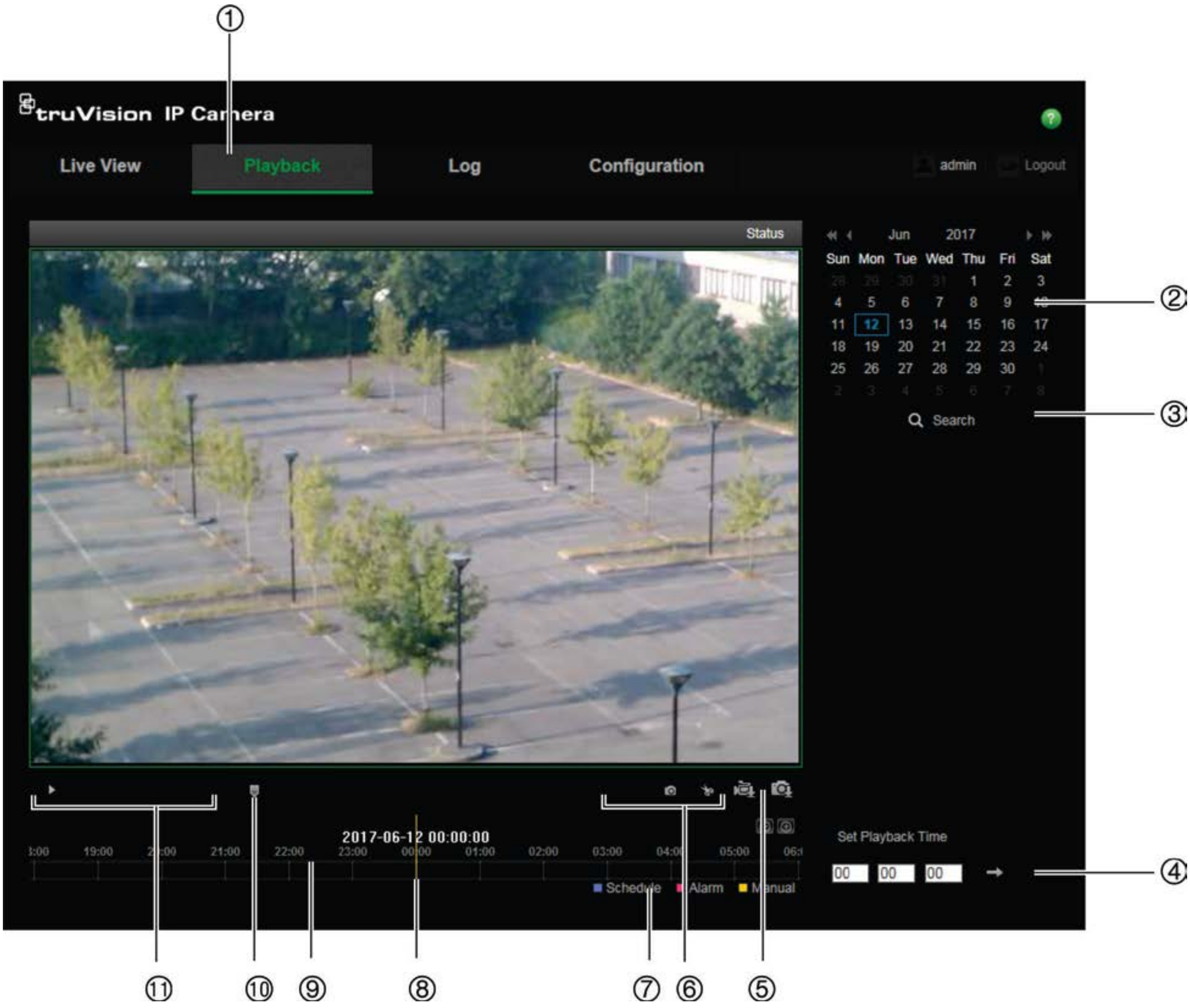
Playing back recorded video

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

Note: You must configure the NAS or insert an SD card in the dome camera to be able to use the playback functions. See “Storage devices” on page 50 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 20 below.

Figure 20: 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 where you are in 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 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.

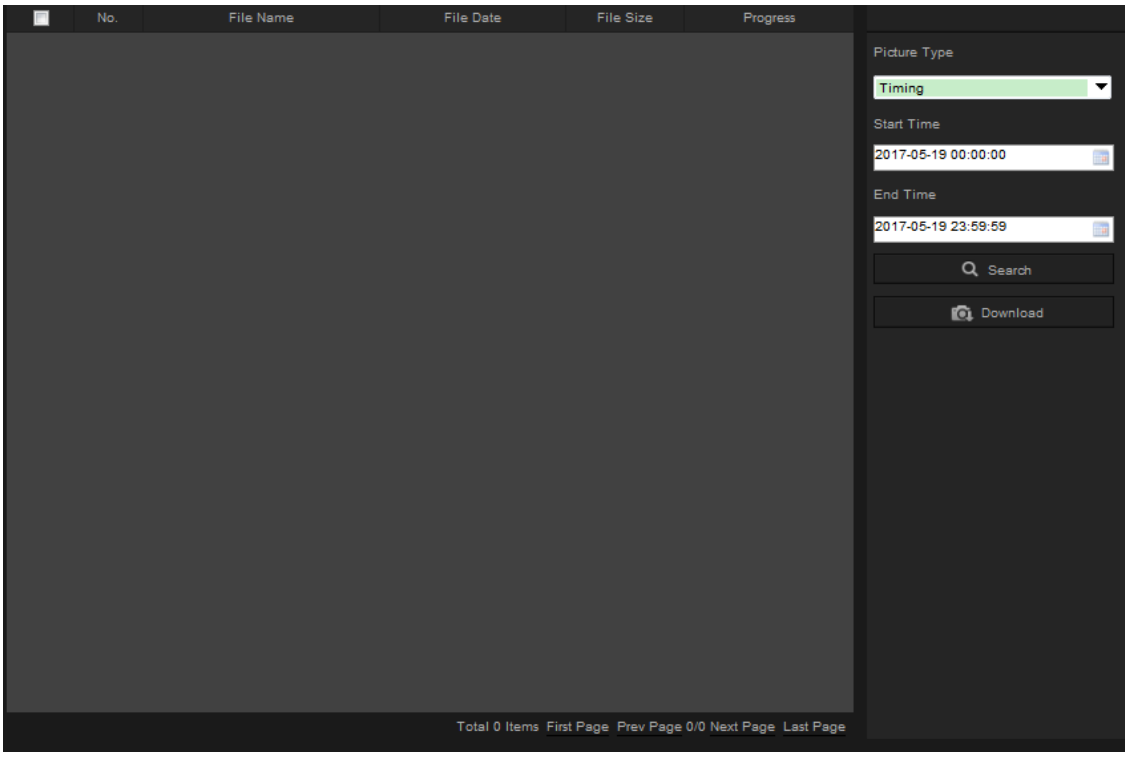
   Note: You must have playback permission to play back recorded images. See “Modify user information” on page 57 for more information.
3. Select the date and click the **Search** button to search for the required recorded file.
4. Click 🎞 to search the video file.
5. In the pop-up window, check the box 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 snapshots search window.



□	No.	File Name	File Date	File Size	Progress

Total 0 Items First Page Prev Page 0/0 Next Page Last Page

Picture Type: Timing

Start Time: 2017-05-19 00:00:00

End Time: 2017-05-19 23:59:59

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

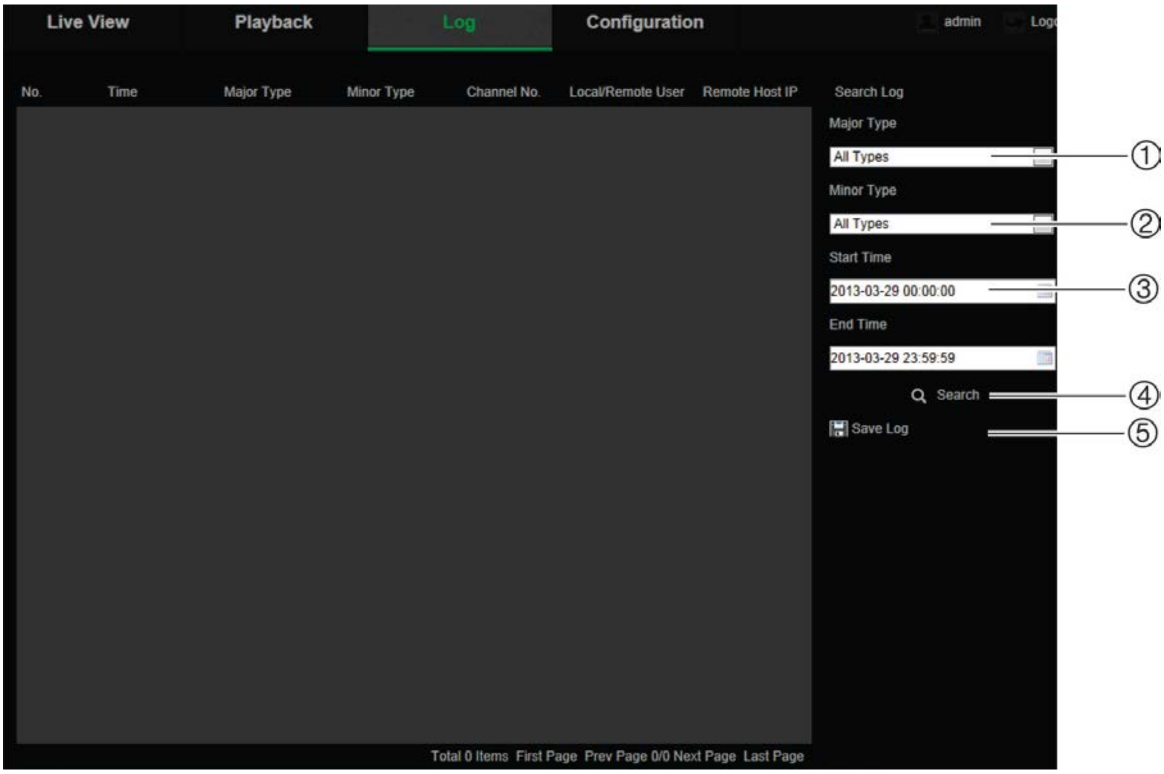
Searching event logs

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

The number of event logs that can be stored on NAS or SD card depends on the capacity of the storage devices. When this capacity is reached, the system starts deleting older logs. To view logs stored on storage devices, click **Log** on the menu toolbar. The Log window appears. See Figure 21 on page 67.

Note: You must have view log access rights to search and view logs. See “Modify user information” on page 57 for more information.

Figure 21: Log window



Major Type: All Types

Minor Type: All Types

Start Time: 2013-03-29 00:00:00

End Time: 2013-03-29 23:59:59

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 Table 1 below for their descriptions.

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

Index