TruVision 360 Degree Multi-imager Camera Configuration Manual

P/N 1073688-EN • REV A • ISS 01APR20

Manufacturer UTC Building & Industrial Systems B.V.
Kelvinstraat 7, 6003 DH Weert, The Netherlands

Certification

Content

Introduction

This is the configuration manual for TruVision Multi-Imager 360 Degree IP Camera:

SKU	Description
TVS-5101	TruVision Multi-Imager 360 Degree IP Camera, 20MP/4 x 5MP image sensors, 2.8 to 12 mm motorized lenses, True D/N, WDR, 30 m IR, Audio, Alarm, Micro SD/SDHC /SDXC Slot, IP67, IK10, Heater, Hi-PoE/12 VDC

You can download the following manuals from our web site:

- TruVision 20MP (4 x 5MP) 360 Degree Multi-imager Camera Installation Guide
- TruVision 20MP (4 x 5MP) 360 Degree Multi-imager Camera Configuration Manual

The manuals are available in several languages on the EMEA web site.

Contact information and manuals /tools /firmware

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

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

Network access

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

TruVision IP cameras can be configured and controlled using Microsoft Internet Explorer (IE). 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 users

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" check 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.

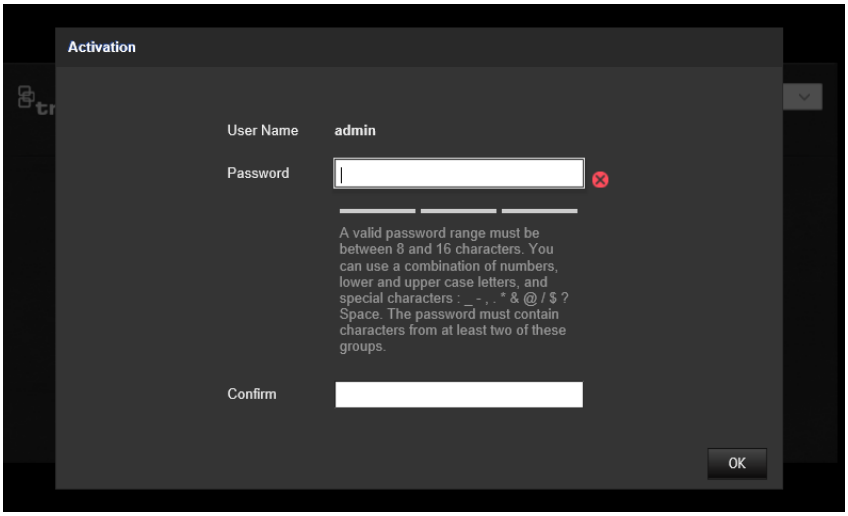
Activating the camera

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.

Activation via the web browser:

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



Note:

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

3. Enter the password in the password field.

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

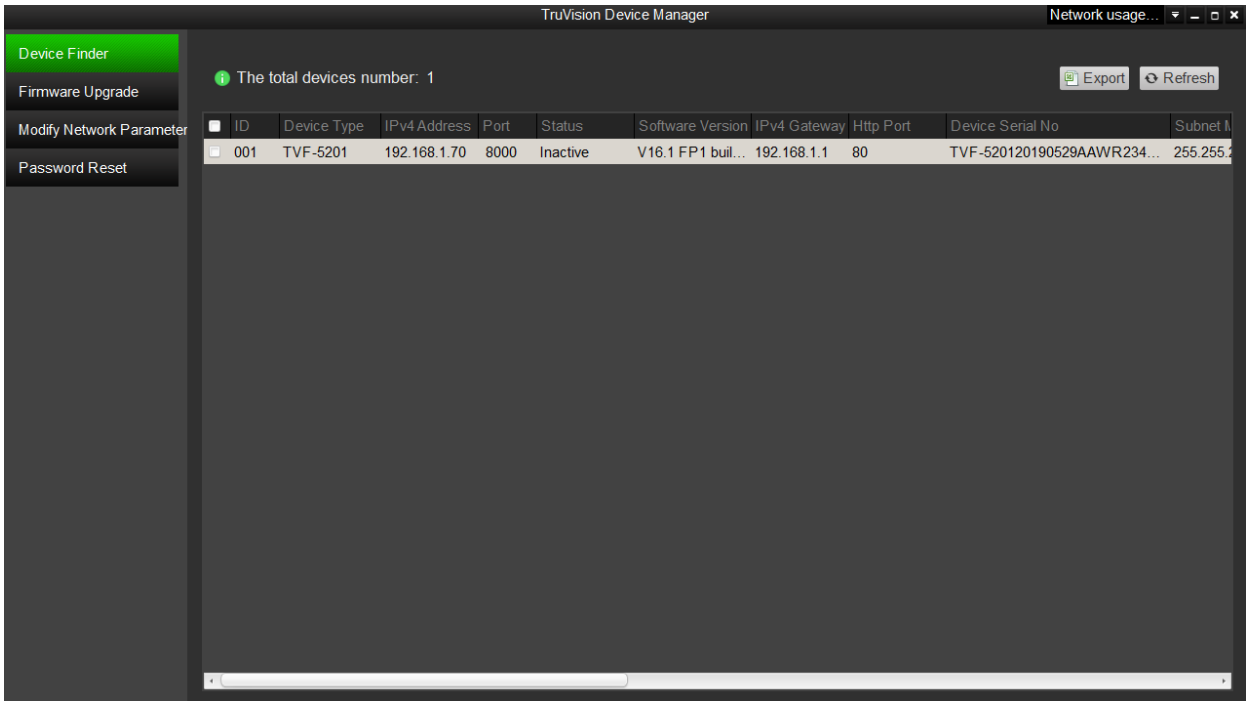
4. Confirm the password.

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

Activation via *TruVision Device Manager*:

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

2. Check the device status from the device list, and select the inactive device.



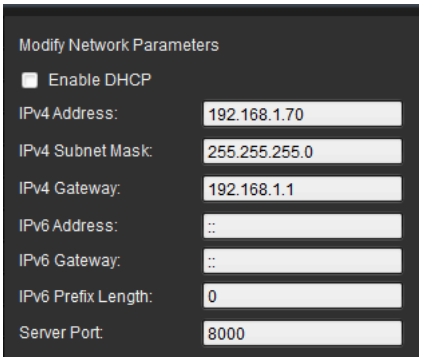
3. Enter the password in the password field, and confirm it.

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

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

   Use the pop-up window that 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.



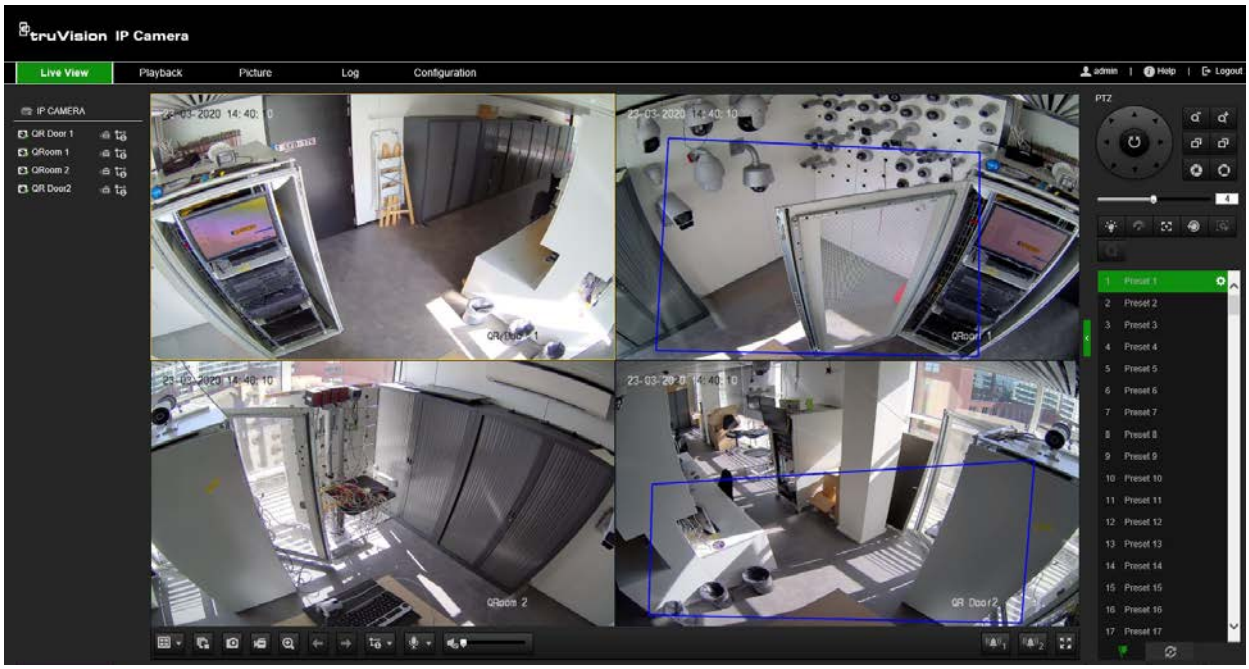
6. Input the password and click the **Save** button to activate your IP address modification.

Overview of the camera web browser

Use the camera web browser to view, record, and play back recorded videos as well as manage the camera from any PC with access to the same network as the camera. The browser's easy-to-use controls provide quick access to all camera functions.

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

Figure 1: Browser interface (Live view shown)



Name	Description
Live view	Click to view live video.
Playback	Click to play back video.
Picture	Click to search for recorded snapshots.
Log	Click to search for event logs.
Configuration	Click to access the configuration section of the camera.

Name	Description
Admin	Displays current user logged on.
Help	Click to open the camera help pages.
Logout	Click to log out from the system.

In the live view window, click the toolbar to start the live view of the camera.

Icon	Description
	Select desired camera multi-view layout
	Start/stop live view all channels
	Take a snapshot of selected camera channel
	Manually start/stop recording the selected camera channel
	Start/stop digital zoom function
	Show next or previous camera channel
	Switch between live main stream, sub stream and third stream
	Turn on/off microphone
	Audio on and adjust Volume/Mute
	Manual alarm output control
	Switch to full screen (hit ESC on PC keyboard to return to normal view)

Camera configuration

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

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

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

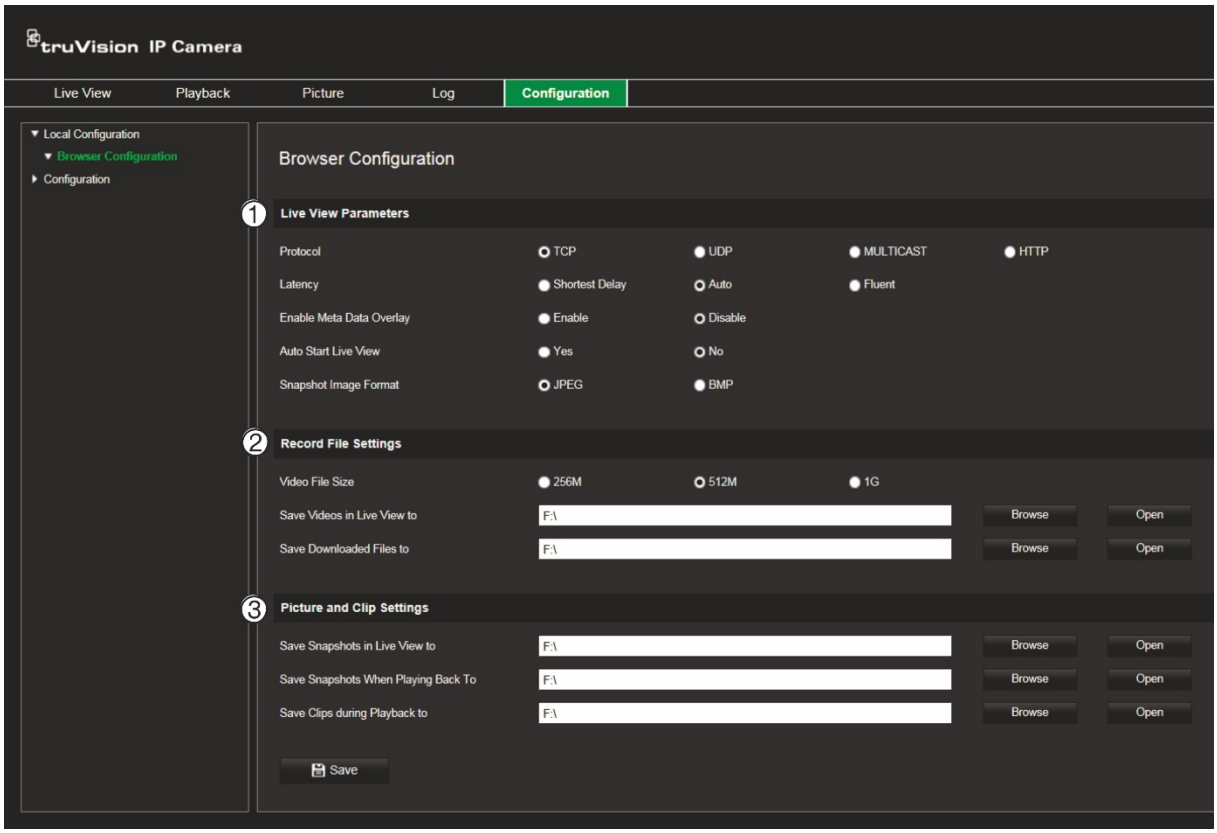
There are two main folders in the configuration panel:

- Local configuration
- Configuration

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 2 below for descriptions of the different menu parameters.

Figure 2: Local Configuration window

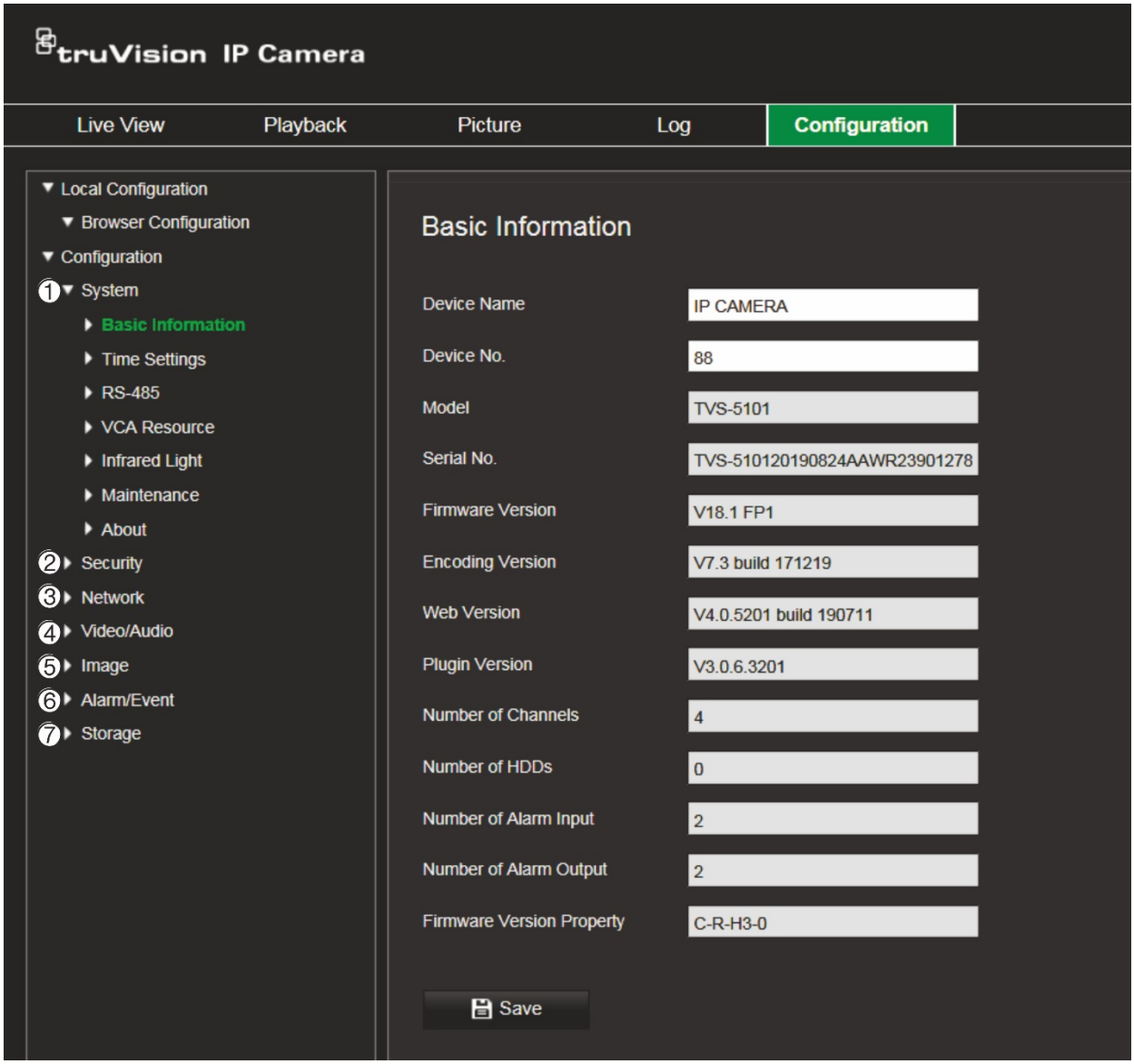


Parameters		Description
1.	**Live View Parameters**	
	Protocol	Specifies the network protocol used. Options include: TCP, UDP, MULTICAST and HTTP. **TCP:** Ensures complete delivery of streaming data and better video quality. However, real-time transmission will be affected. **UDP:** Provides real-time audio and video streams. **HTTP:** Allows the same quality as of TCP without setting specific ports for streaming under some network environments. **MULTICAST:** It is recommended to select MCAST type when using the Multicast function.
	Latency	Set the live view performance to Shortest Delay, Auto, Fluent or Custom. For Custom, you can set the frame rate for live view.
	Enable Meta Data Overlay	Enabling this function will dynamically display (detected) targets/objects/movements in the live image. The feature can be used to highlight motion or certain VCA features in the live view window.
	Auto Start Live View	Enable/disable automatic live view when opening the Live View page
	Snapshot Image Format	Specifies the snapshot format as JPEG or BMP.
2.	**Record File Settings**	
	Record File Size	Specifies the maximum file size for manually recorded video. Options include: 256 MB, 512 MB, and 1G.
	Save Record Files to	Specifies the directory for recorded files.
	Save Downloaded Files to	Specifies the directory for downloaded files.
3.	**Snapshot and Clip Settings**	
	Save Snapshots In Live View To	Specifies the directory for saving snapshots in live view mode.
	Save Snapshots When Playback To	Specifies the directory for saving snapshots in playback mode.
	Save Clips To	Specifies the directory for saving video clips in playback mode.

Configuration

Use the **Configuration** window to configure the camera system, network, video audio, alarms, users, transactions and other parameters such as upgrading the firmware. See Figure 3 on page 11 for descriptions of the configuration folders available.

Figure 3: Configuration window (Basic Information window selected)



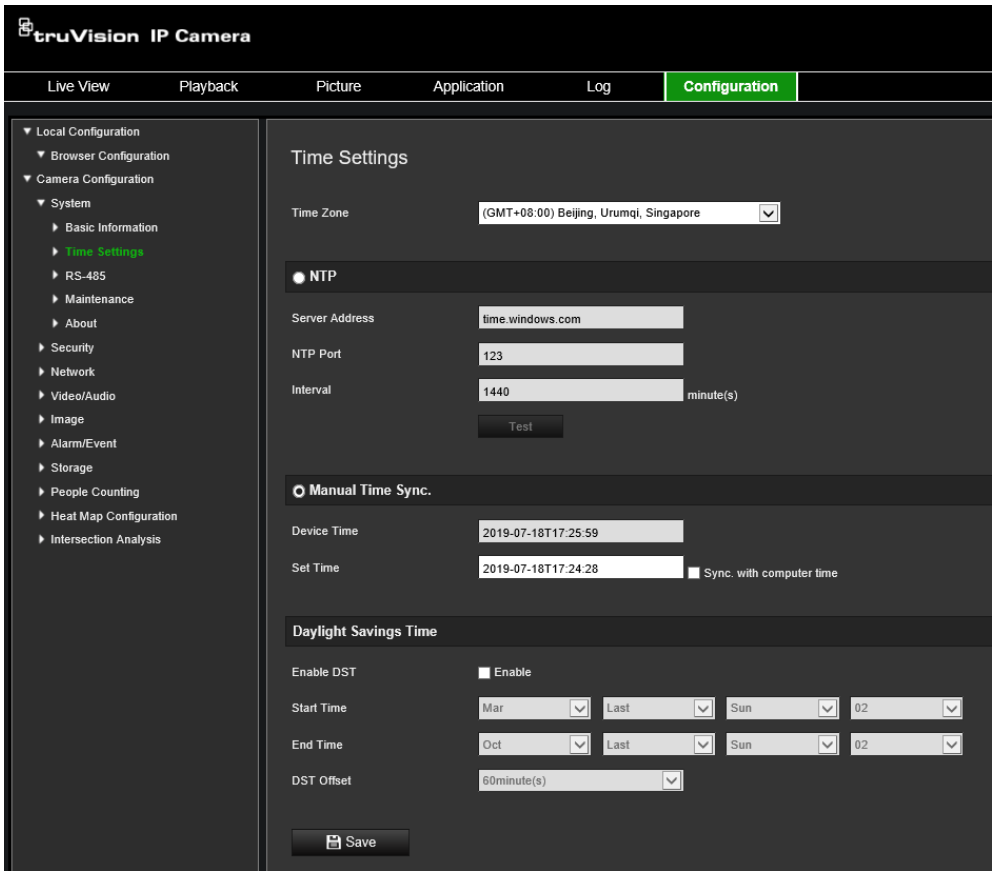
Parameters	Description
1. System	Displays the basic device information including serial number and the current firmware version, time settings, RS-485, VCA resources, infra red, and maintenance. See pages 12 to15 for further information.
2 Security	Defines who can use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and telnet access.
3 Network	Defines the network parameters required to access the camera over the internet. See page 23 for further information.
4 Video/Audio	Defines recording parameters. See page 30 for further information.
5. Image	Defines the image parameters, OSD settings, overlay text, and privacy masking. See page 34 for further information.
6. Alarm/Event	Defines motion detection, tamper-proof, alarm input/output, exception and snapshot configuration. See pages 41 to 61 for further information.
7. Storage	Defines recording schedule, storage management and NAS configuration. See pages 63 to 68 for further information.

Time settings

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. Click **Configuration** > **System** > **Time Settings**.



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

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

   - Or -

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

   Note: You can also check the **Sync with computer time** check box to synchronize the time of the camera with the time of your computer.
4. Check **Enable DST** to enable the DST function, and set the start and end dates of the DST period.
5. Click **Save** to save changes.

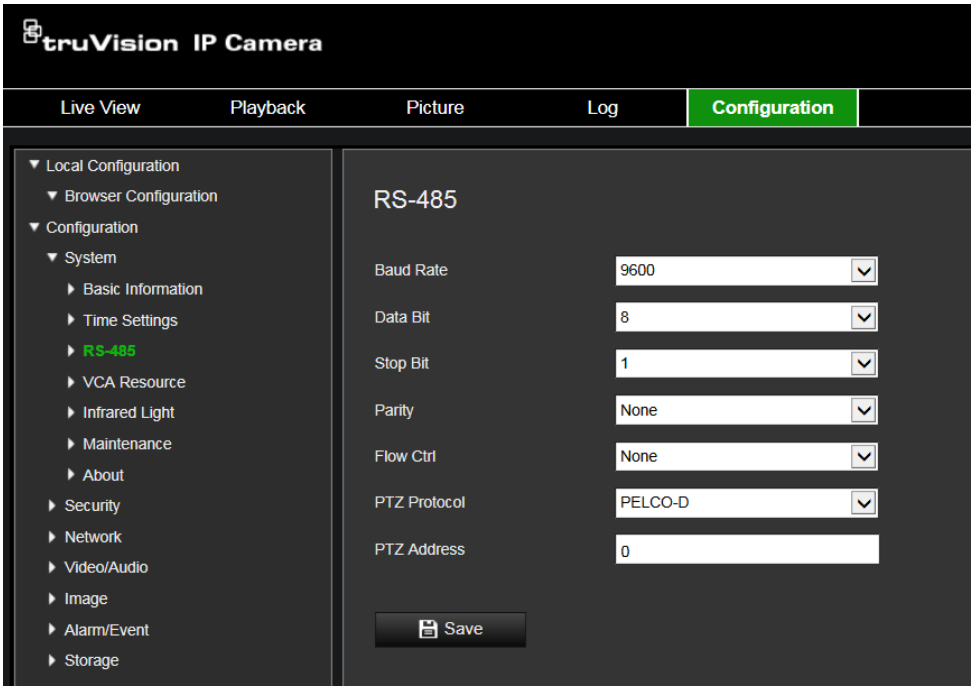
RS-485

The RS-485 serial port is used to control extra devices that support the 485 protocol (Pelco D or Pelco P), such as PTZ devices, lighting devices or other devices. You can also connect it to an analog PTZ camera, using a 360° camera to control PTZ movement.

You need to configure these parameters before connecting the camera to any devices.

To set up RS-485 settings:

1. Click **Configuration** > **System > RS485**.



2. Select the RS-485 port parameters.

   Note: The Baud Rate, PTZ Protocol, and PTZ Address parameters should be exactly the same as the PTZ camera parameters.

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

VCA resource

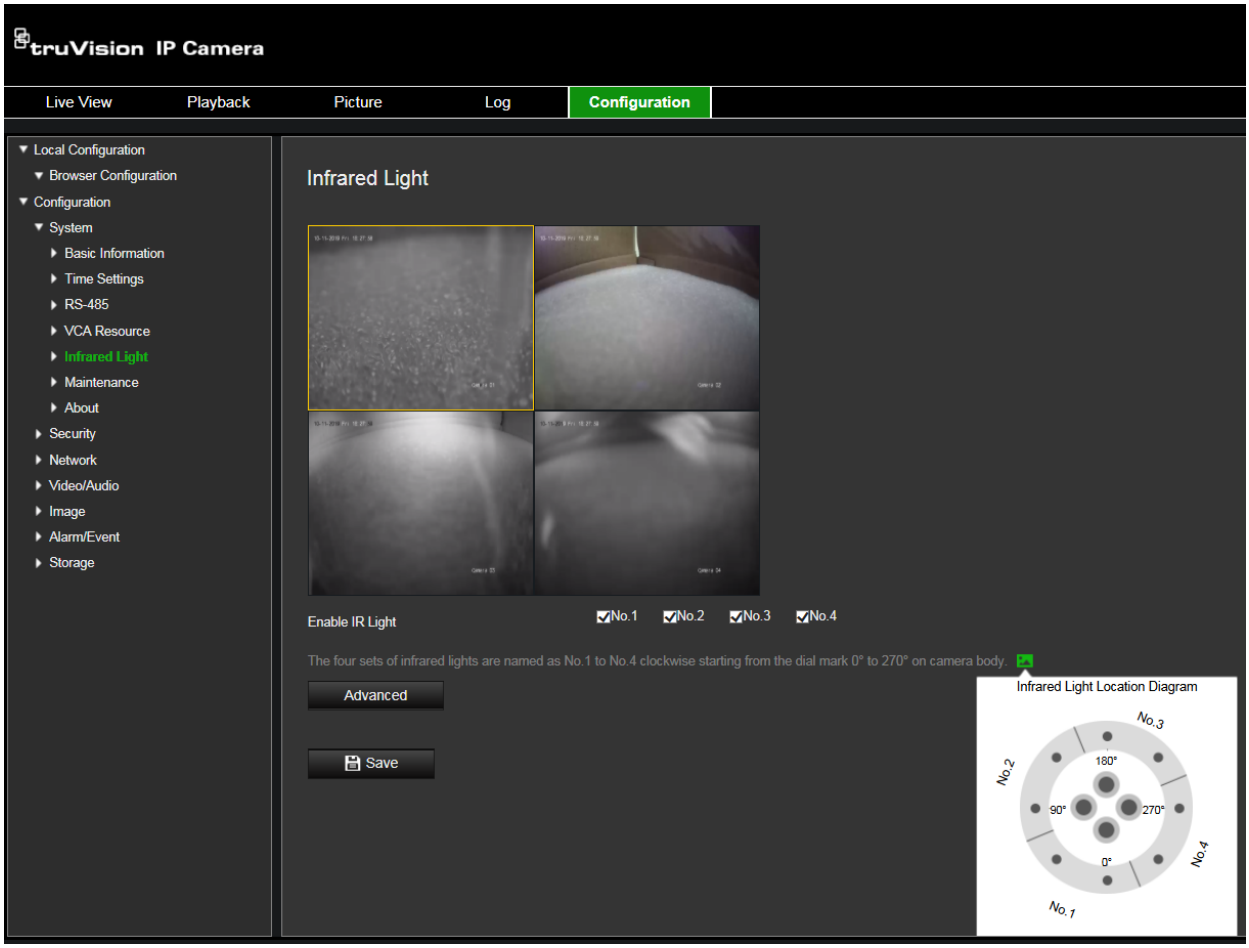
The camera has four lens in total. The four lens are named as Camera 01 to Camera 04 clockwise starting from the dial mark 0° to 270° on camera body. The smart events only work for the set of camera No. 01 and 03, or the set of camera No. 02 and 04.

Figure 4: Maintenance window

Infrared LEDs

The camera has four sets of infrared LEDs that can be enabled or disabled separately. The four sets of infrared LEDs are named No.1 to 4 clockwise starting from the dial mark 0° to 270° on camera body. You can hover on the icon to see the figure.

Figure 5: Infrared Light



One-to-One Control: With one-to-one control enabled, you can bind a certain set of IR LEDs to a specific camera channel. Thus the IR LED only works with the linked camera channel.

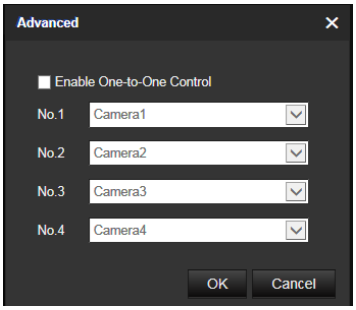
To link infra red LEDs to camera channels:

1. Select **Infrared Light** to enable certain sets of IR LEDs.

   Note: Without the one-to-one control, the enabled IR LEDs works as a group.

   A signal from any camera channel can control their on/off status.

2. Click **Advanced**.
3. Check **Enable One-to-One Control**.

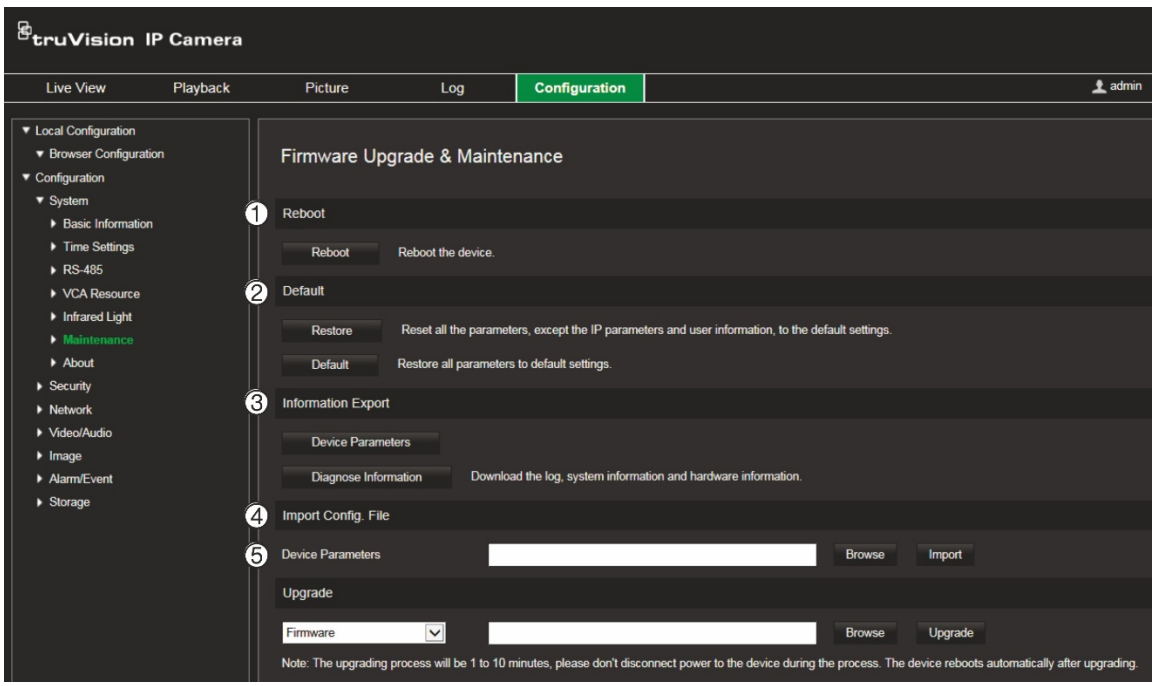


4. Link IR LEDs to the desired camera channels.
5. Click **OK** to save changes.

Maintenance

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

Figure 6: Maintenance window

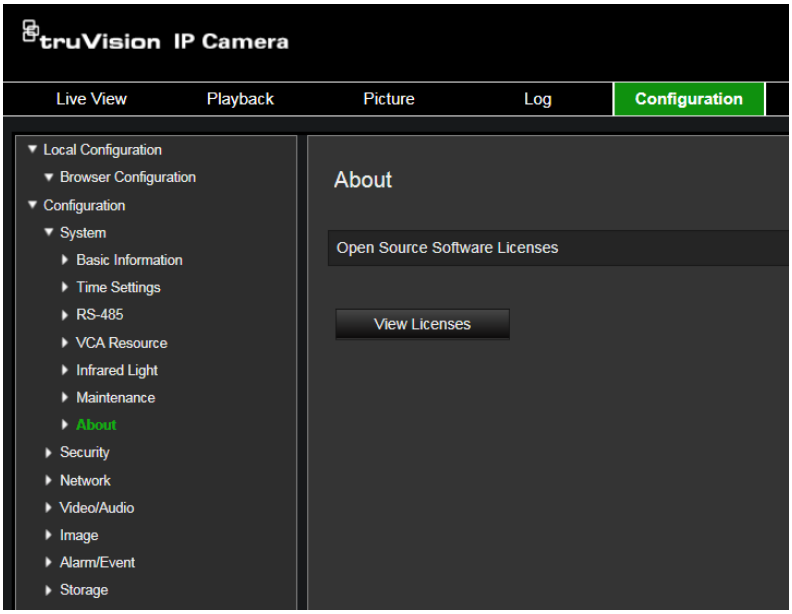


Parameters		Description	
1.	Reboot	Reboot the device	
2.	Default	Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.
		Default	Restore all the parameters to the factory default. **Notes:** • After restoring the default settings, the IP address is also restored to the default IP address. Please be careful using this function. • For cameras that support Wi-Fi, wireless dial, or WLAN function. This restore action does not restore the related settings of the mentioned functions to default.
3	Information Export	Device Parameters	Click to export the current configuration file of the camera. This operation requires the admin password to proceed.
		Diagnose Information	Click to download log and system information.
4	Import Config File	Configuration file is used for the batch configuration of the cameras **Note:** You need to reboot the camera after importing the configuration file	
5	Upgrade	Upgrade the camera to the latest available FW version. **Note:** The firmware upgrade process can take between 1 to 10 minutes. Do not disconnect power to the camera during the process. The camera reboots automatically after upgrade.	

Open source software licenses

Information about the open source software that applies to the IP camera can be checked, if required. Go to **Configuration** > **System Settings** > **About**.

Figure 7: Open Source Software Licenses



Security

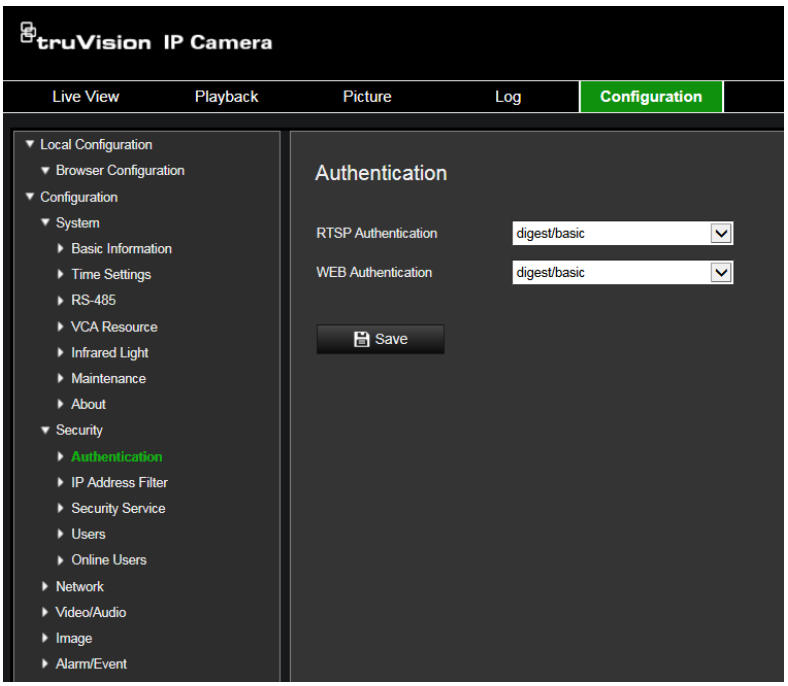
Security related parameters, such as user accounts and IP-address filter, can be managed via the camera menu **Configuration** > **Security**.

Authentication

You can secure the stream data of the live view.

To define RTSP authentication:

1. From the menu toolbar, click **Configuration** > **Security** > **RTSP Authentication**.



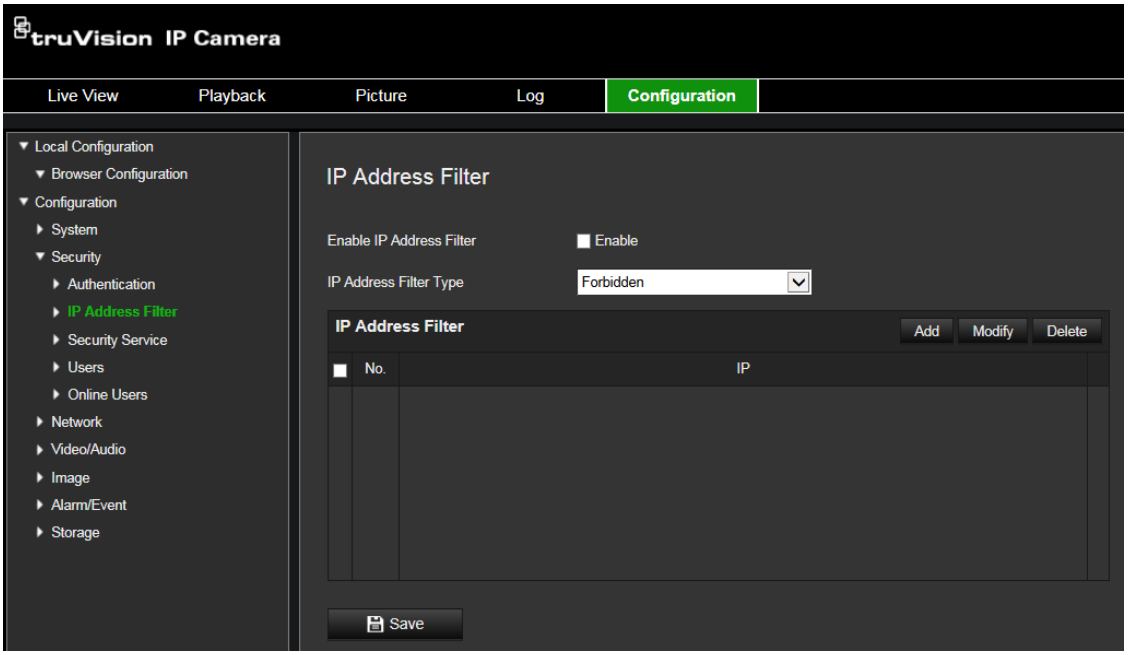
2. Select the **RTSP Authentication** type **Digest/basic** or **Digest** in the drop-down list
3. Select the **WEB Authentication** type **Digest/basic** or **Digest** in the drop-down list
4. Click **Save** to save the changes.

IP address filter

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

To define the IP address filter:

1. From the menu toolbar, click **Configuration** > **Security** > **IP Address Filter**.



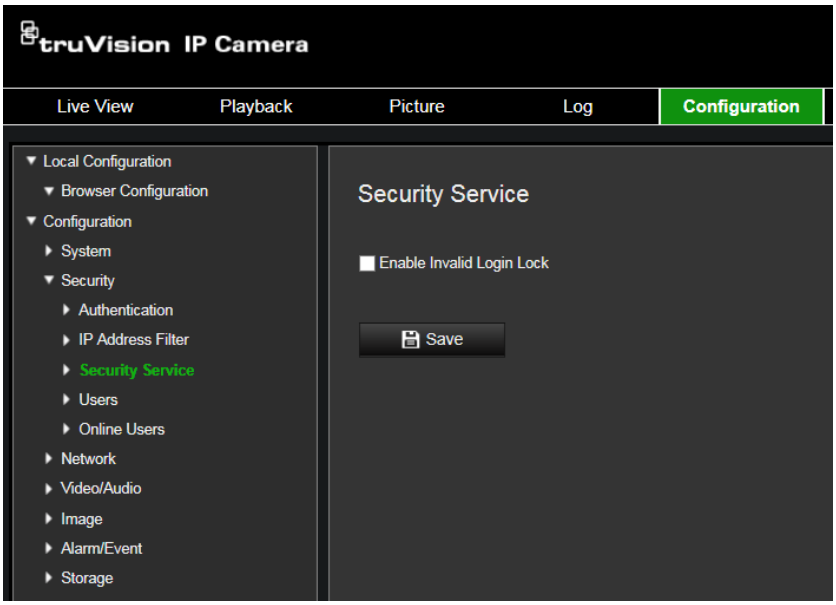
2. Select the **Enable IP Address Filter** check box**.**
3. Select the type of IP Address Filter in the drop-down list: Forbidden or Allowed.
4. Click **Add** to add an IP address and enter the address.
5. Click **Modify** or **Delete** to modify or delete the selected IP address**.**
6. Click **Clear**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

Security service

Enabling the *Invalid Login Lock* function will block the camera for a certain period after multiple incorrect login attempts.

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.

Notes:

A. The IP address will be locked if the admin user performs seven failed user name/password attempts (10 attempts for the operator/user).

B. If the IP address is locked, you can try to log in to the device again after 30 minutes

To define SSH:

1. Click **Configuration** > **Security** > **Security Service**.
2. Click **Save** to save the changes.

Users

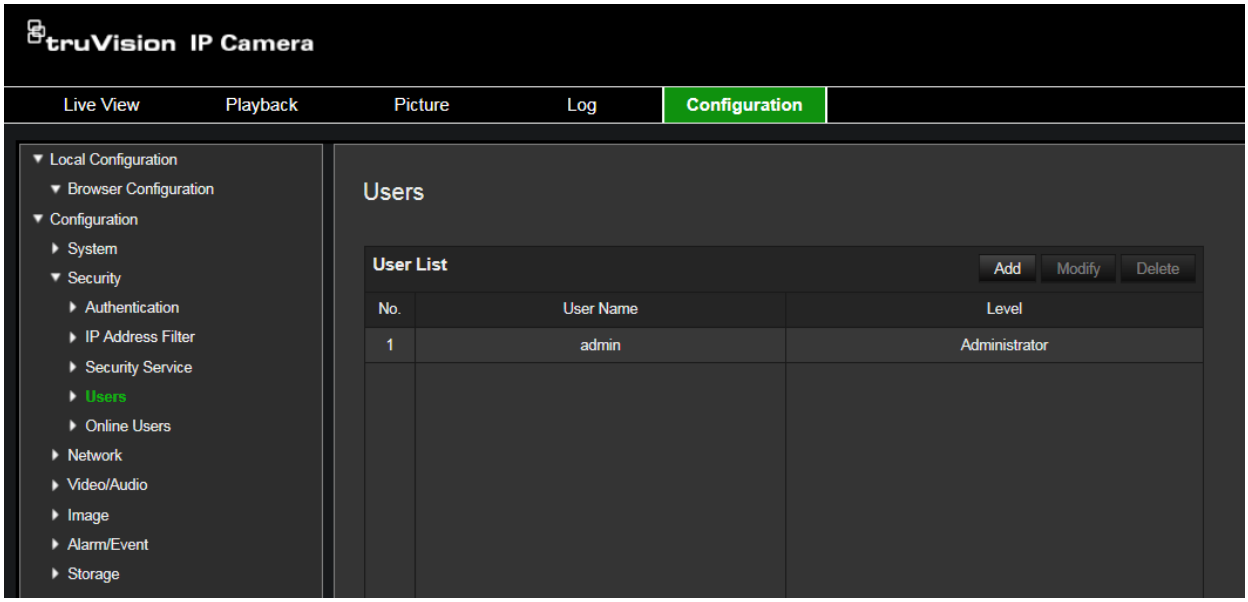
This section describes how to manage users. You can:

- 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 8 below.

Figure 8: User management window



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

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

Types of users

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

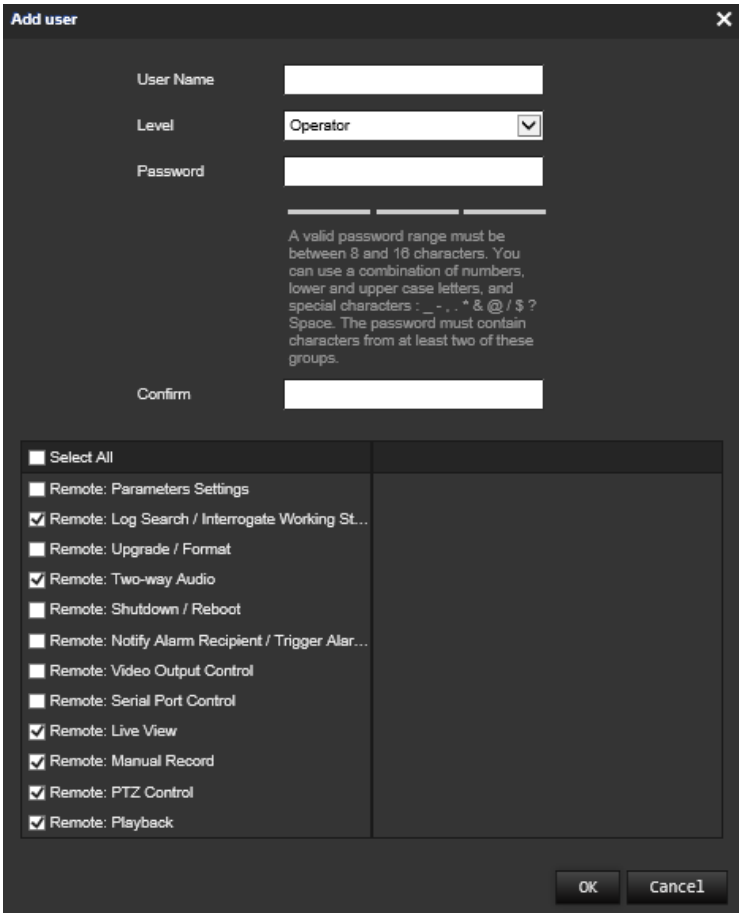
- **Admin**: This is the system administrator. The administrator can configure all settings. Only the administrator can create and delete user accounts. Admin cannot be deleted.
- **Operator**: This user can only change the configuration of his/her own account. An operator cannot create or delete other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

Add and delete users

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

To add a user:

1. From the menu toolbar, click **Configuration** > **Security** > **Users**.
2. Select the **Add** button. The user management window appears.



3. Enter a user name.
4. Assign the user a password. Passwords can have up to 16 alphanumeric characters.
5. Select the type of user from the drop-down list. The options are Viewer and Operator.
6. Assign permissions to the user. 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: Two-way Audio	Remote: Playback
Remote: Shutdown/Reboot	
Remote: Notify Alarm Recipient/Trigger Alarm Output	
Remote: Video Output Control	
Remote: Serial Port Control	

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

To delete a user:

1. Select the desired user under the **User** tab.
2. Click **Delete** button. A message box appears.

   Note: Only the administrator can delete a user.
3. Click **Save** to save the changes.

Modify user information

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

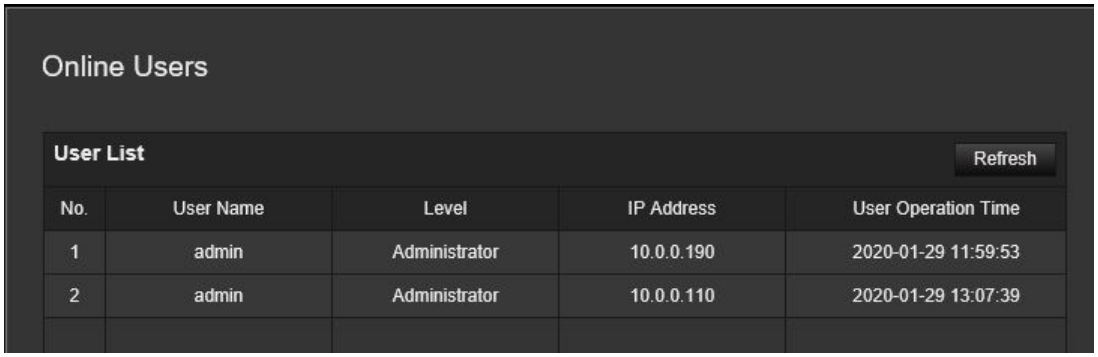
To modify user information:

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

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

Online users

The table displays the active network connections to the camera.

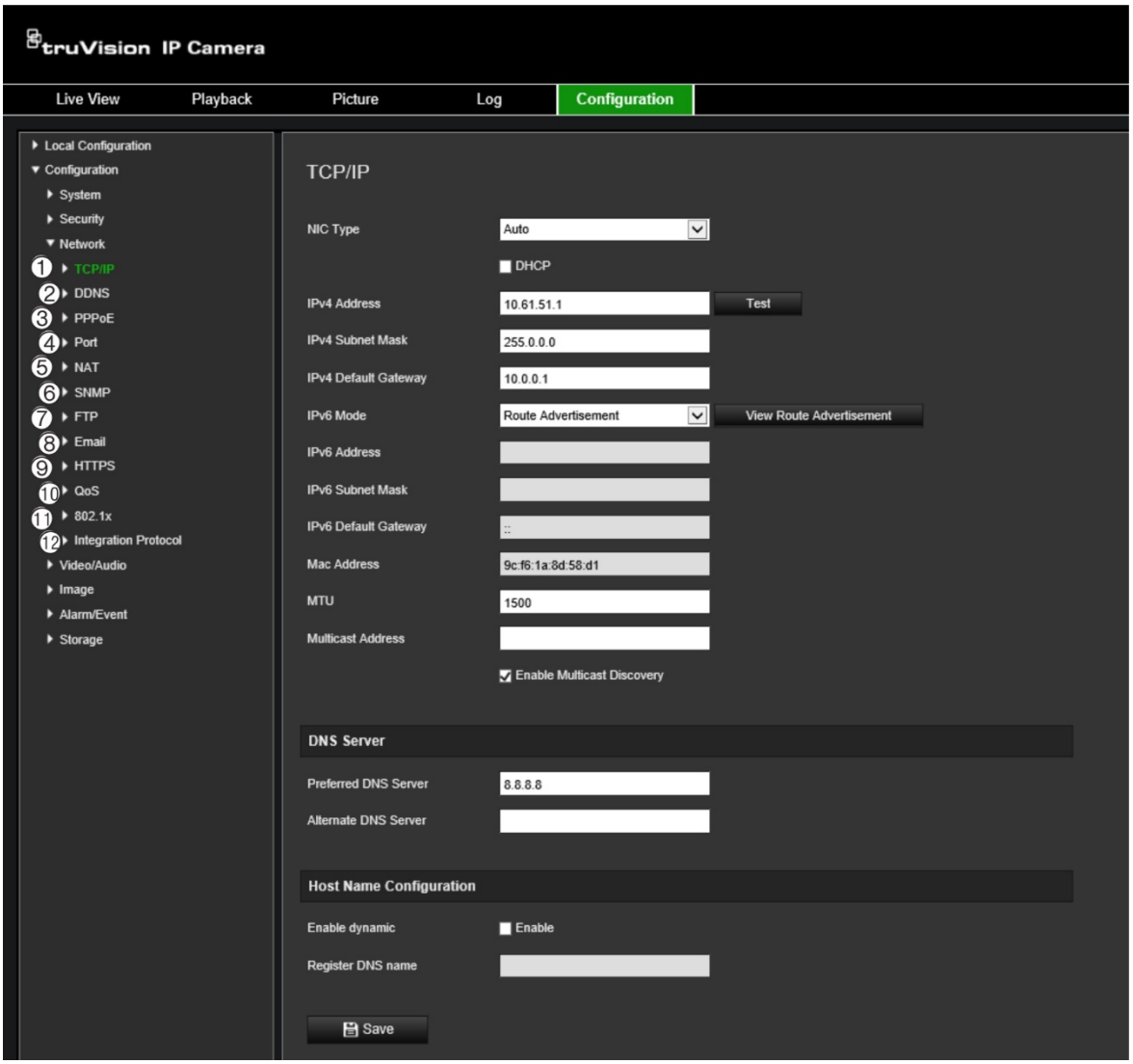


User name, user level, IP address and operation time are displayed. The refresh button reloads the page to check for active connections.

Network

Accessing the camera through a network requires that you define certain network settings. Use the “Network” folder to define the network settings. See Figure 9 below for further information.

Figure 9: Network window (TCP/IP window shown)



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

Menu tabs		Description
		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.
2.	DDNS	DDNS is a service that maps Internet domain names to IP addresses. It is designed to support dynamic IP addresses, such as those assigned by a DHCP server. Specify DynDNS, No-IP 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. **No-IP**: Enter the address of the NO-IP, host name for your camera, the port number, your user name and password. See page 25 for setup information.
3.	PPPoE	Retrieves a dynamic IP address. See page 26 for setup information.
4.	Port	**HTTP Port:** The HTTP port is used for remote internet browser access. Enter the port used for the Internet Explorer (IE) browser. Default value is 80. **RTSP Port:** RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. Enter the RTSP port value. The default port number is 554. **HTTPS Port:** HTTPS (Hyper Text Transfer Protocol Secure) allows video to be securely viewed when using a browser. Enter the HTTPS port, value. The default port number is 443. **Server Port:** This is used for remote client software access. Enter the server port value. The default port number is 8000. **Alarm Host IP**: Specifies the IP address of the alarm host. **Alarm Host Port**: Specifies the port of the alarm host. See page 25 for setup information.
5.	NAT	A NAT (Network Address Translation) is used for network connection. Select the port mapping mode: auto or manual. See page 26 for setup information.
6.	SNMP	SNMP is a protocol for managing devices on networks. Enable SNMP to get camera status and parameter related information. See page 26 for setup information.
7.	FTP	Enter the FTP address and folder to which snapshots of the camera can be uploaded. See page 27 for setup information.
8.	Email	Enter the email address to which messages are sent when an alarm occurs. See page 27 for setup information.
9.	HTTPS	Specifies authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

Menu tabs		Description
10.	QoS	QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending. Enable the option in order to solve network delay and network congestion by configuring the priority of data sending. See page 20 for setup information.
11.	802.1.X	When the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network. See page 27 for setup information.
12.	Integration protocol	If you need to access to the camera through the third party platform, you can enable STD-CGI function. And if you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

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 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, ezDDNS and NO-IP.

- 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.
  - **ezDDNS (preferred)**: Enter the host name. It will automatically register it online on the tvr-ddns.net server. You can define a host name for the camera. Make sure you entered a valid DNS server in the network settings and have the necessary ports forwarded in the router (HTTP, Server port, RSTP port).
  - **NO-IP:** Enter the address of the NO-IP, host name for your camera, the port number, your user name and password.

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

To define the PPPoE parameters:

1. From the menu toolbar, click **Configuration** > **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 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 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 define the SNMP parameters:

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

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

To define the FTP parameters:

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

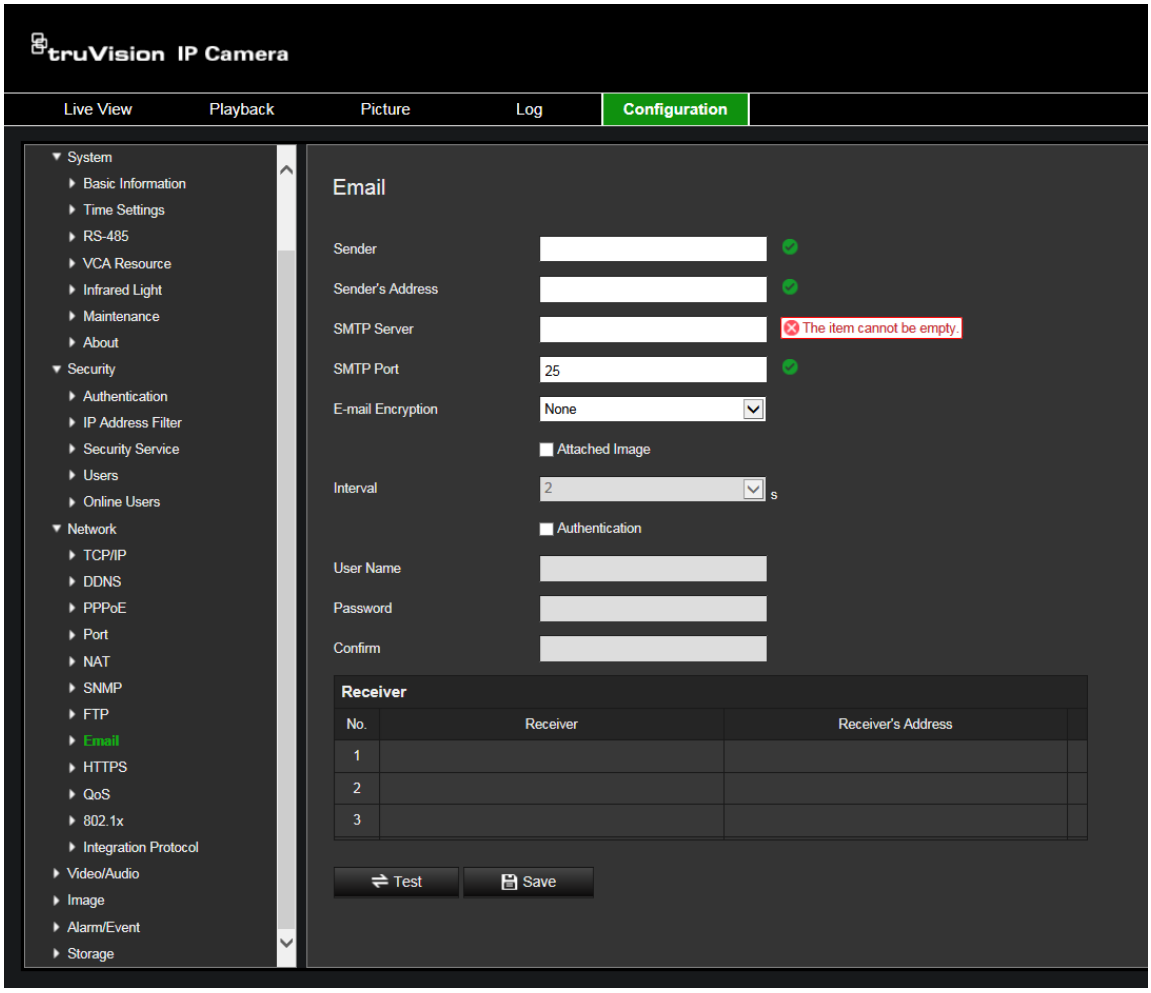
   Anonymous: Check the check box to enable the anonymous access to the FTP server.

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

To set up the email parameters:

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



2. Configure the following settings:

   Sender: The name of the email sender.

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

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

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

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.

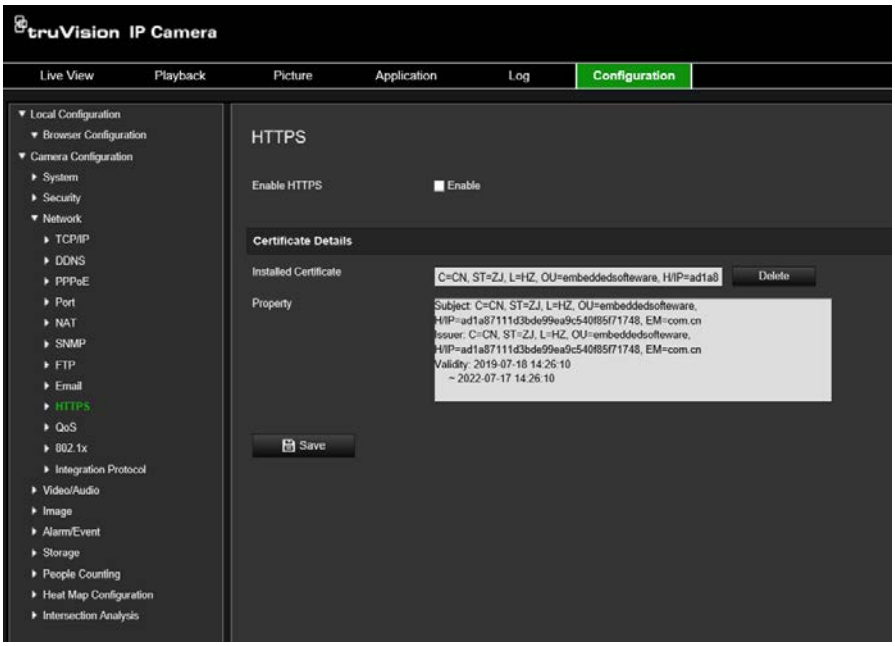
Receiver3: The name of the second user to be notified.

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.

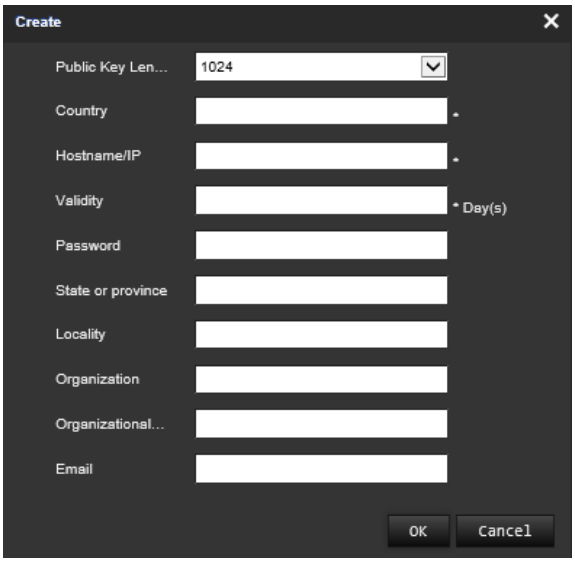
To set up the HTTPS parameters:

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



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

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



   Click **OK** to save the settings.

   -Or-

   To create a certificate request:

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

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

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 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 protocol, 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.

Integration protocol:

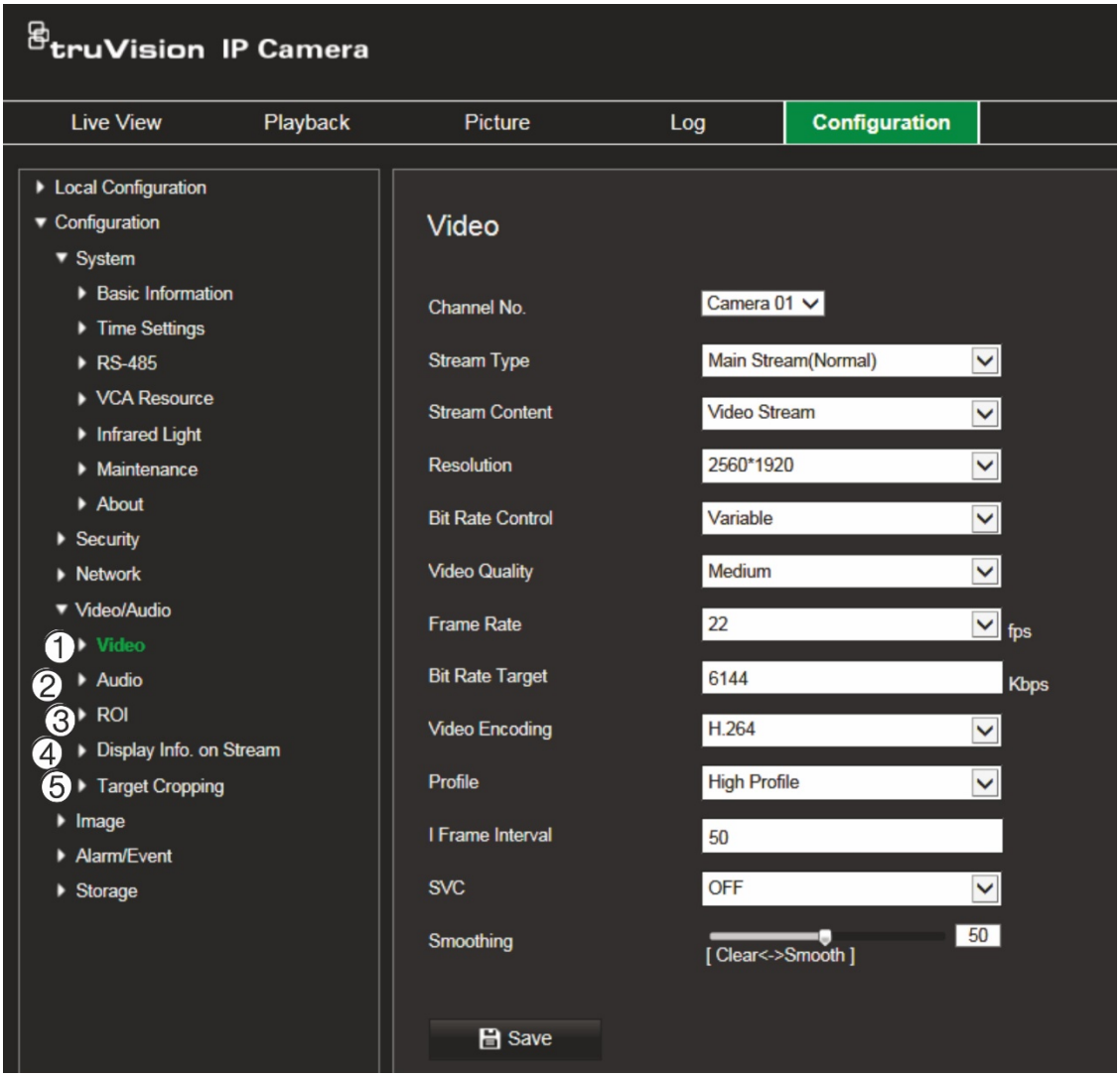
Enable STD-CGI and select desired authentication option for when using CGI.

Enable ONVIF to make the camera discoverable via ONVIF protocol.

Video/Audio

You can adjust the video and audio recording parameters to obtain the picture quality and file size best suited to your needs. Figure 10 below lists the video and audio recording options you can configure for the camera.

Figure 10: Video/Audio Settings menu (Video tab shown)

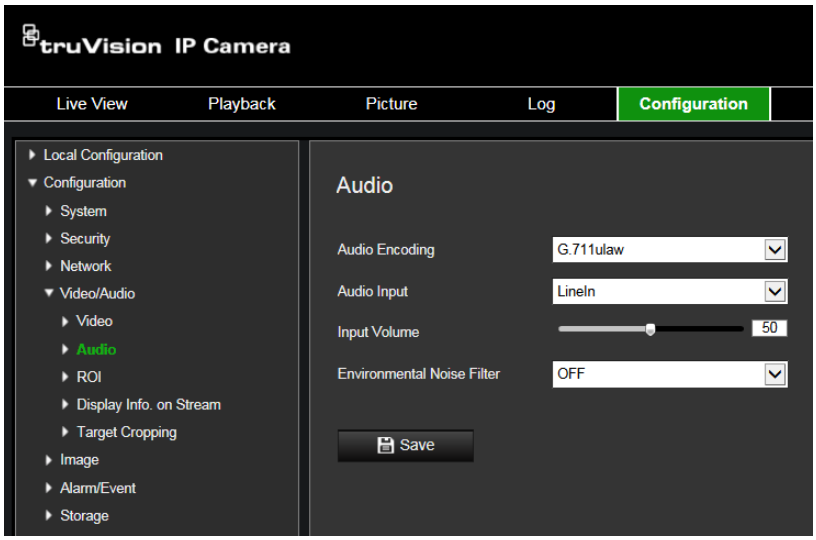


Tab		Parameter descriptions
1.	Video	**Channel No.:** First select camera channel to configure **Stream Type**: Specifies the streaming method used. Options include: Main Stream (Normal), Sub Stream. **Note**: The Third stream is only available when the this function is enabled in **System** > **System Service**
		Stream Content: Specifies the stream type(s) 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.
		Bit Rate Control: Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.

Tab		Parameter descriptions
		Video Quality: Specifies the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, low, Medium, Higher and Highest.
		Frame Rate: 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.
		Video Encoding: Specifies the video encoding used.
		Profile: Different profile indicates different tools and technologies used in compression. Options include: High Profile, Main Profile.
		I Frame Interval: A video compression method. It is strongly recommended not to change the default value 25.
		SVC: Scalable Video Coding is an extension of the H.264/AVC standard. Select OFF / ON to disable / enable the SVC function. Select Auto, and the device will automatically extract frames from the original video when the network bandwidth is insufficient.
		Smoothing: Adjust the smoothness of the stream.
2.	Audio	**Audio Encoding**: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726 and PCM are available.
		Audio Input: Line in can be used for an external 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) on 1 channel to an NVR or other platforms to generate a VCA alarm.
5.	Target Cropping	Specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

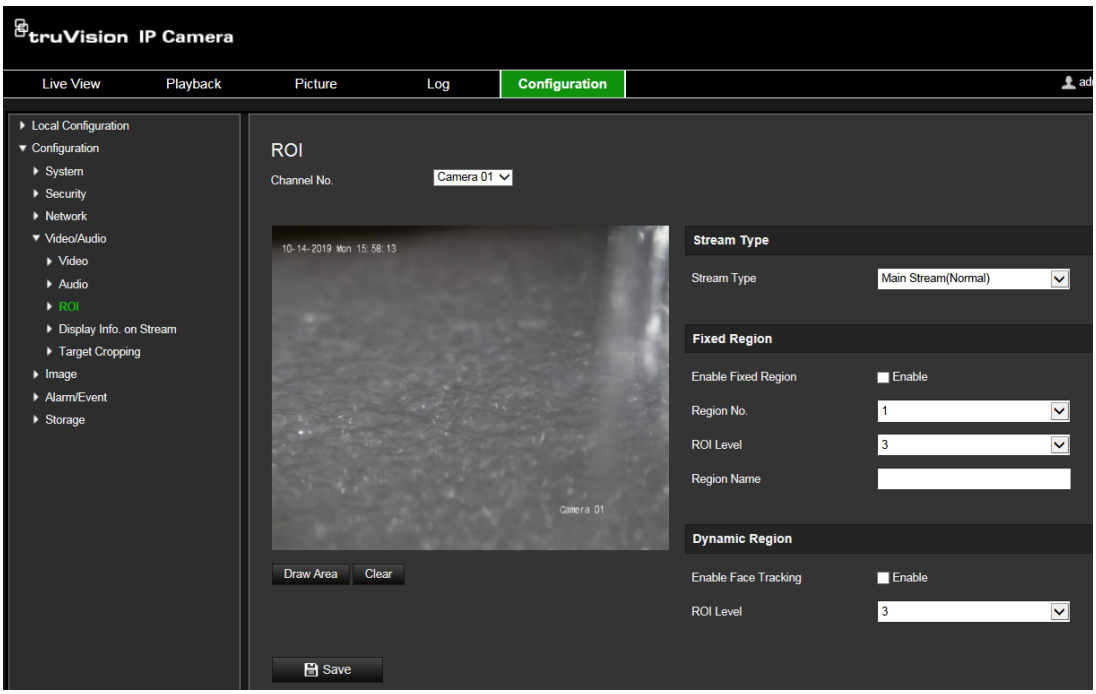
To configure audio settings:

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



To configure ROI settings:

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



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

   Region No.: Select the region.

   ROI Level: Choose the image quality enhancing level.

   Region Name: Set the desired region name.

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.

For example, with an TruVision NVR (please check our 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. Select the check box to enable **Dual-VCA**.
3. Click **Save** to save the changes.

Target Cropping:

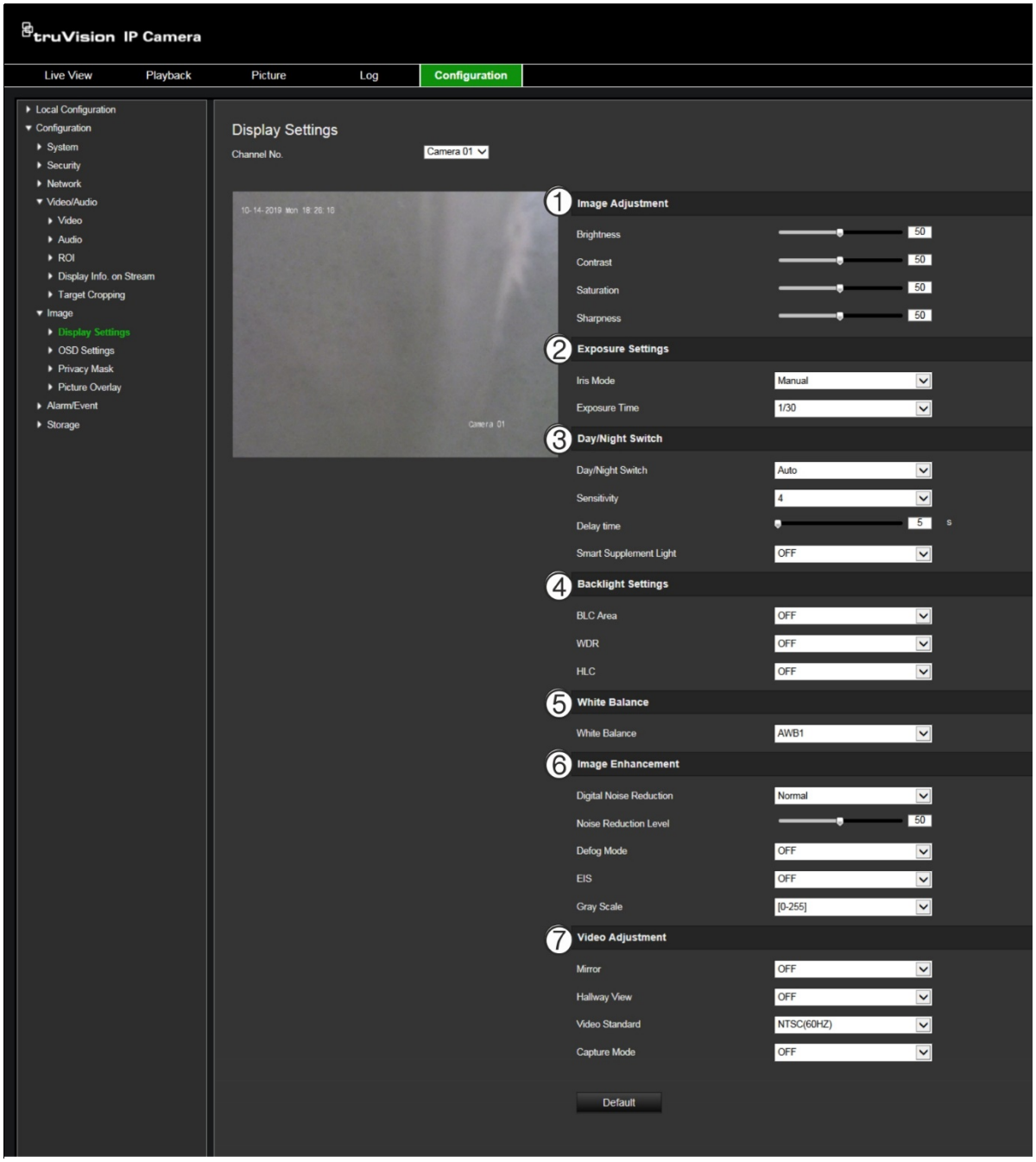
1. Select the **Enable Target Cropping** checkbox to enable the function.
2. Set **Third Stream** as the stream type.
3. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle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

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 11 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 11: Camera image settings menu – Display Settings tab



Parameter	Description
1. Image Adjustment	
Brightness, Contrast Saturation, Sharpness	Modify the different elements of picture quality by adjusting the values for each of parameter.
2. Exposure Settings	
Iris Mode	Only *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.

Parameter		Description
3.	**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, Center, Custom or Auto. When WDR is enabled, BLC cannot be configured.
	WDR	When enabled, wide dynamic range (WDR) provides clear images when there is high contrast between light and dark areas in the field of view of the camera. Both bright and dark areas can be displayed in the frame.
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.
	Filtering time	Only available when *Auto D/N switch* mode is selected. The filtering time refers to the interval time between switchover the day/night switch. Set it between 5 and 120 s.
	Smart Supplement Light	When enabled, it can avoid over exposure issue.
	IR Light	Select On/OFF to Enable/disable IR. **ON**: The IR LEDs are ON when the camera changes to night mode. **Off**: The IR LEDs are OFF when the camera changes to night mode **Note**: The IR LEDs are always OFF in day mode.
5.	**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.

Parameter		Description
		Locked WB: Locks the WB to the current environment color temperature. **Fluorescent Lamp:** For use where there are fluorescent lamps installed near the camera. **Incandescent Lamp:** For use with incandescent lighting. **Warm Light Lamp:** For use where the indoor light is warm. **Natural Light:** For use with natural light.
6.	**Image Enhancement**	
	Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance. Select Normal Mode, Advanced Mode, or OFF. Default is Normal.
	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.
7.	**Video Adjustment**	
	Mirror	It mirrors the image so you can see it inversed. Select Left/Right, Up/Down, Center, or OFF. 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.
	Capture Mode	It's the selectable video input mode to meet the different demands of field of view and resolution. Lens Distortion Correction: Select ON / OFF to enable / disable the lens distortion correction. The distorted image caused by the wide-angle lens can be corrected if this function enabled.

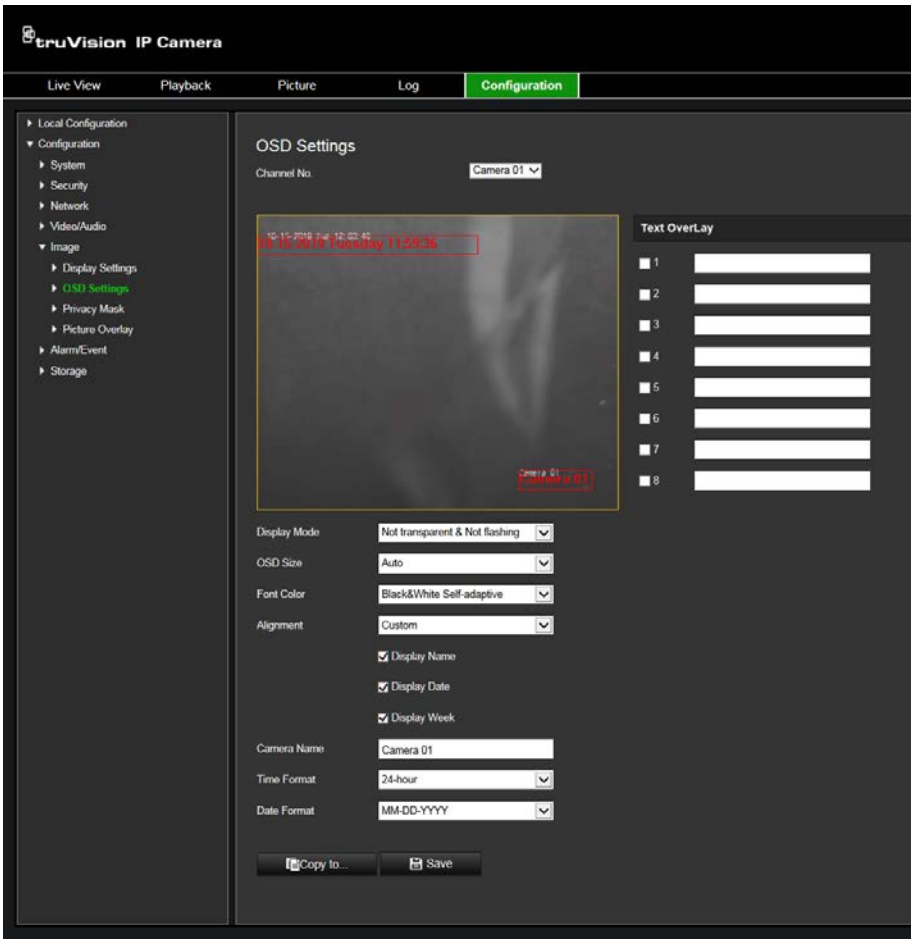
Note: Click the **Default** button to default all the image settings.

OSD settings (On Screen Display)

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

To position the date/time and name on screen:

1. From the menu toolbar, click **Configuration** > **Image** > **OSD Settings**.



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

- **Not transparent & Not flashing.** The image is behind the text. This is default.
- **Not transparent & Flashing**. The image is behind the text. The text flashes on and off.

8. Select the desired OSD size.
9. Select the desired font color.
10. Select the desired alignment (Custom, Align Left or Align Right).
11. Click **Save** to save changes.

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

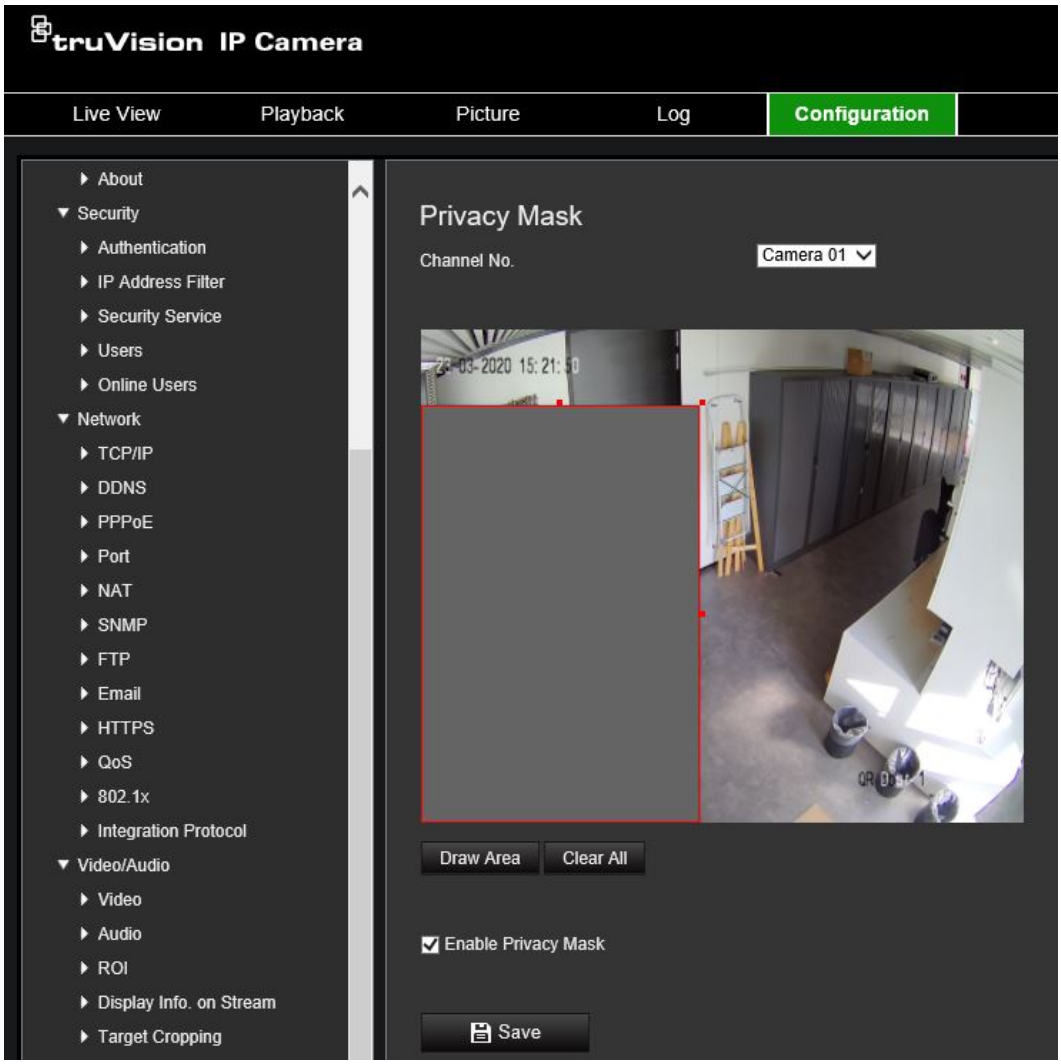
Privacy masks

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

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

To add a privacy mask area:

1. From the menu toolbar, click **Configuration** > **Image** > **Privacy Mask**.



2. Select **Enable Privacy Mask**.
3. Click **Draw Area**.
4. Click and drag the mouse in the live video window to draw the mask area.

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

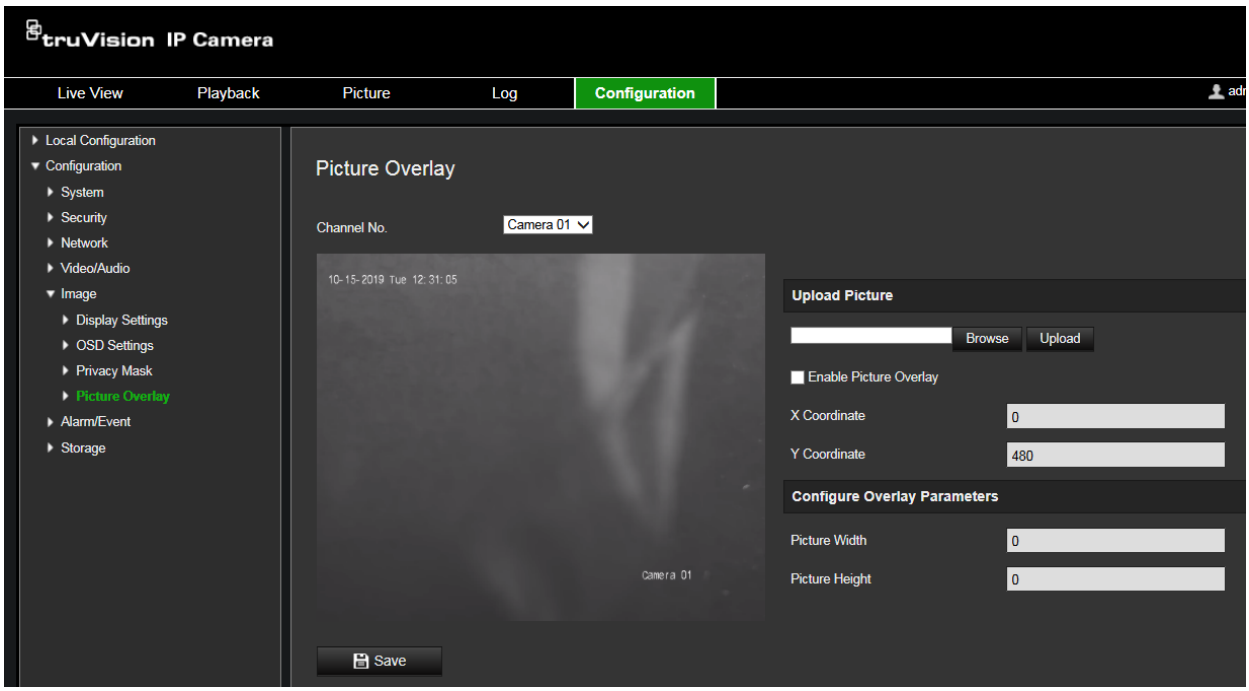
Picture overlay

Picture overlay enables you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image.

Note: The picture must be in RGB24 bmp format. The maximum picture size is 128*128.

To add picture overlay:

1. From the menu toolbar, click **Camera Configuration** > **Image** > **Picture Overlay**.



2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Select the **Enable Picture Overlay** checkbox to enable the function.
5. Drag the red rectangle to adjust the position.
6. Click **Save** to save settings.

Motion detection alarms

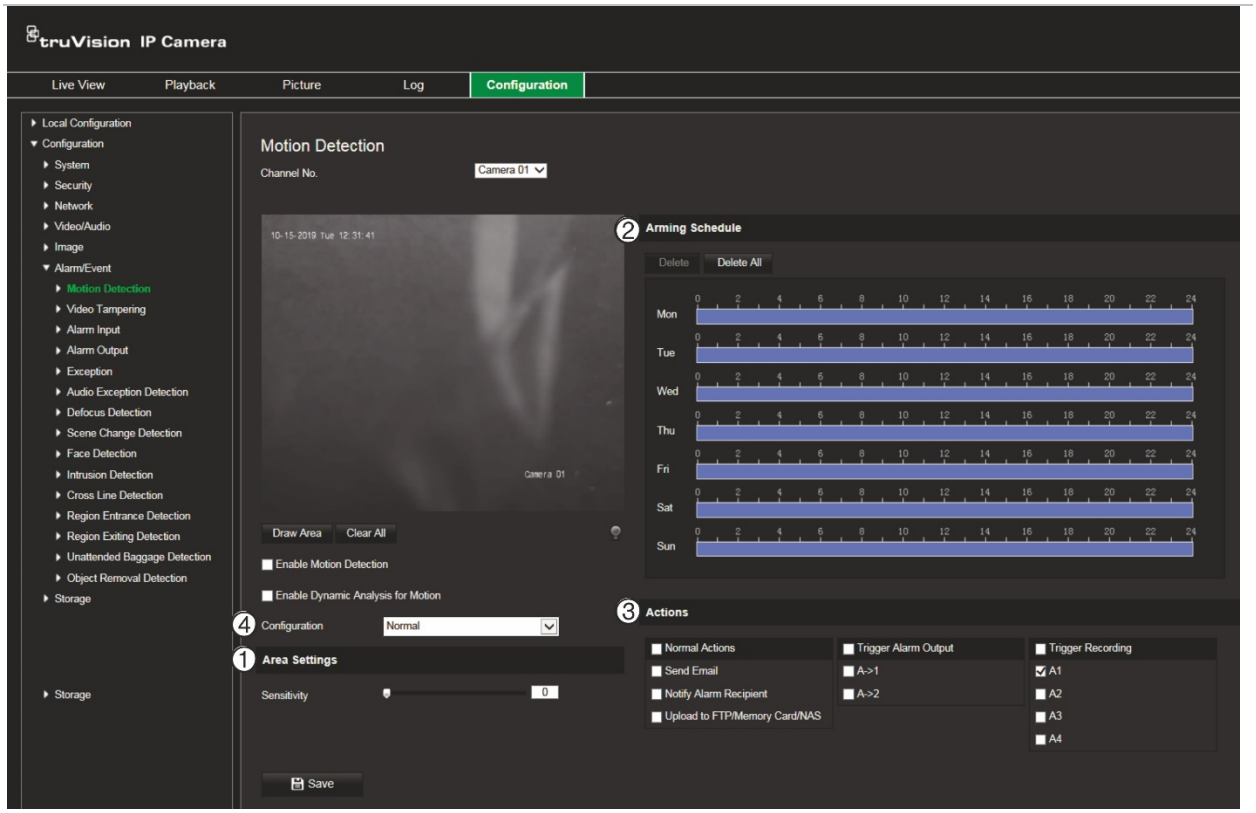
You can define motion detection alarms. A motion detection alarm refers to an alarm triggered when the camera detects motion. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

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 12: Motion detection window



Defining a motion detection alarm requires the following tasks:

1. **Area settings**: Define the on-screen area that can trigger a motion detection alarm and the detection sensitivity level (see Figure 12, item 1).
2. **Arming schedule**: Define the schedule during which the system detects motion (see Figure 12, item 2).
3. **Recording schedule**: Define the schedule during which motion detection can be recorded. See “Recording schedule” on page 63 for further information.
4. **Actions**: Specify the method of response to the alarm (see Figure 12, item 3).
5. **Normal and advanced configuration**: Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 12, 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:

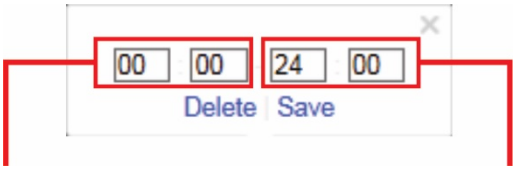
1. From the menu toolbar, click **Configuration** > **Alarm/Event** > **Motion Detection**.
2. Select the **Enable Motion Detection** check box. Select the **Enable Dynamic Analysis for Motion** check box if you want to see real-time motion events.

   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 > Enable Meta Data Overlay.
3. Select **Normal** mode from the drop-down list.

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

   Note: You can draw up to 8 motion detection areas on the same image.

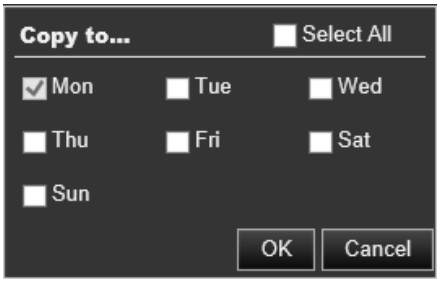
5. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
6. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.
7. Drag and click the time bar to edit the arming schedule.



Enter the start time (hour and minutes)

Enter the end time (hour and minutes)

8. Click  to copy the schedule to other days or to the whole week.



9. Click **OK** to save changes.
10. Specify the **linkage method** when an event occurs. Check one or more response methods for the system when a motion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 67 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 27 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” on page 65 for further information.

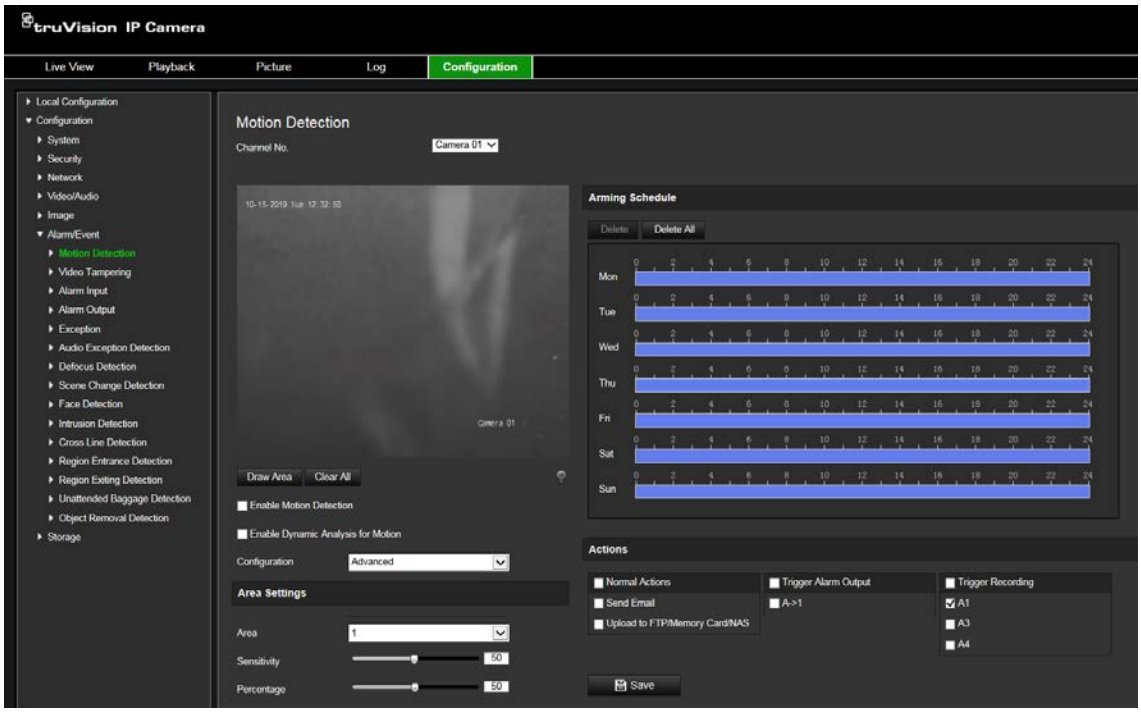
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note:** This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

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

To set up advanced motion detection:

1. From the menu toolbar, click **Configuration** > **Alarm/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 > Enable Meta Data Overlay > Disable if you do not want the detected objects displayed with the green rectangles.
3. Select **Advanced** mode from the Configuration drop-down list.



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

   Auto D/N Switch and Scheduled D/N settings allow you to set different settings for day and night as well as different periods.
5. Select **Area No.** and click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

   Note: You can draw up to eight motion detection areas on the same image. **Stop Drawing** shows up after **Draw Area** is clicked.
6. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.

7. Move the **Sensitivity** slider to set the sensitivity of the detection for the selected areas.
8. Move the **Percentage** slider to set the proportion of the object that must occupy the defined area to trigger an alarm.
9. Click **Save** to save the changes for that area.
10. Repeat steps 7 to 9 for each area to be defined.
11. Click **Edit** to edit the arming schedule. See the picture below for the editing interface of the arming schedule.

12. Click **OK** to save changes.
13. Specify the linkage method when an event occurs. Check one or more response methods for the system when a motion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See NAS” on page 67 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 27 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” on page 65 for further information.

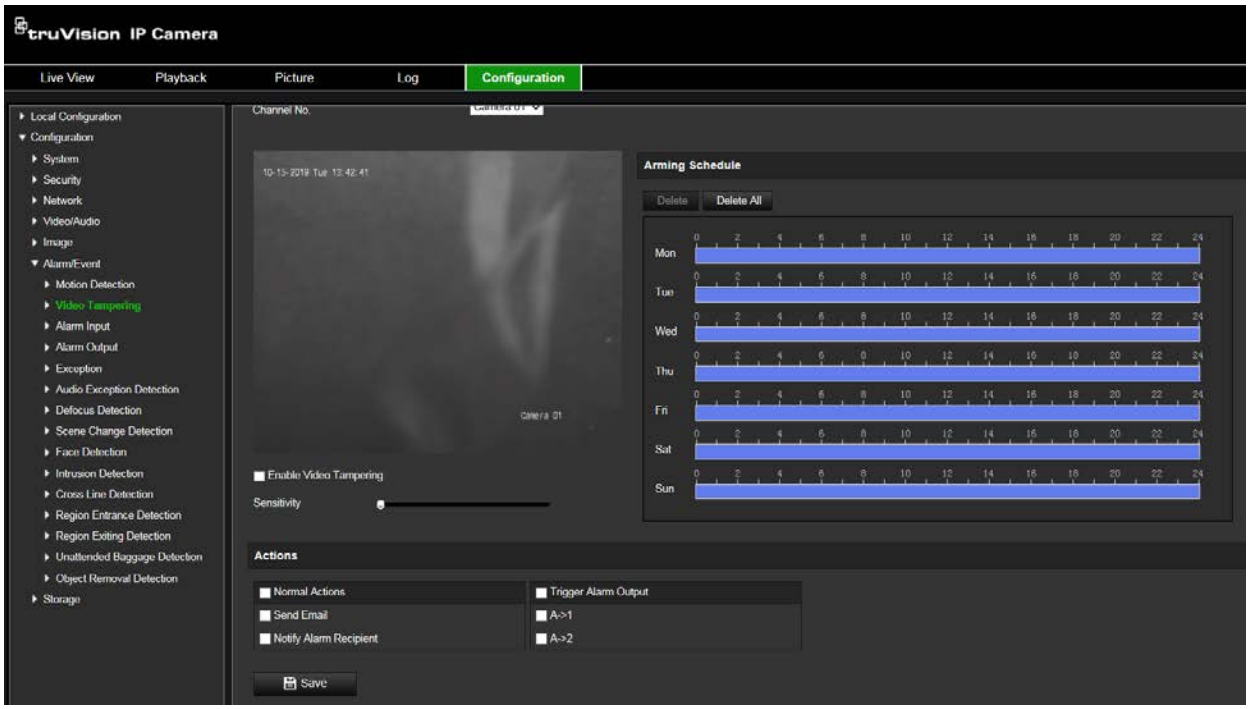
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note:** This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

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

Video tampering

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

Figure 13: Video Tampering window



To set up tamper-proof alarms:

1. From the menu toolbar, click **Configuration** > **Alarm Event** > **Video Tampering**.
2. Check the **Enable Video Tampering** box.
3. Move the **Sensitivity** slider to set the detection sensitivity.
4. Edit the arming schedule for video tampering. The arming schedule configuration is the same as that for motion detection. See “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 video tampering is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. 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.

Alarm inputs and outputs

To define the external alarm input:

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

Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. See NAS” on page 67 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 27 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” on page 65 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.

Trigger Recording	Triggers the recording to start in the camera.

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

To define alarm output:

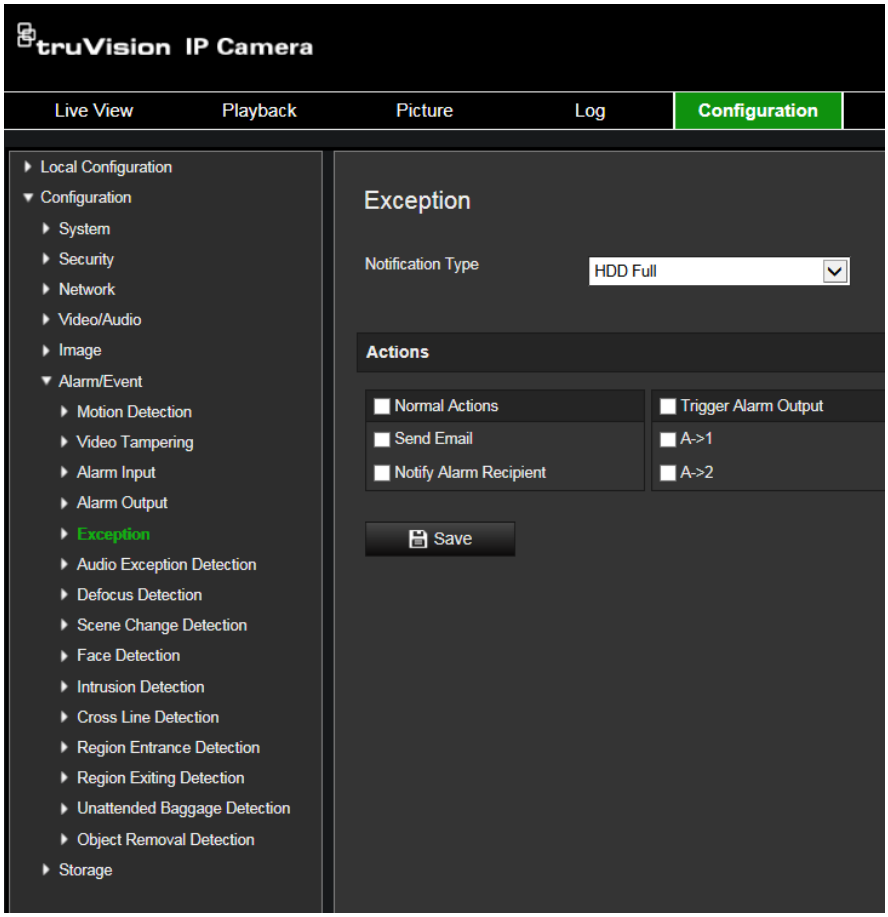
1. From the menu toolbar, click **Configuration** > **Basic Event** > **Alarm Output**.
2. Select one alarm output channel from the **Alarm Output** drop-down list. You can also set a name for the alarm output.
3. Set the delay time to 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min or manual. The delay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

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 14: Exception window



To define exception alarms:

1. From the menu toolbar, click **Configuration** > **Basic Event** > **Exception**.
2. Under **Exception Type**, select an exception type from the drop-down list.
3. Specify the linkage method when an event occurs. Check one or more response methods for the system when a tamper-proof alarm is triggered.

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 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. **Note:** This option is only supported by cameras that support alarm output.

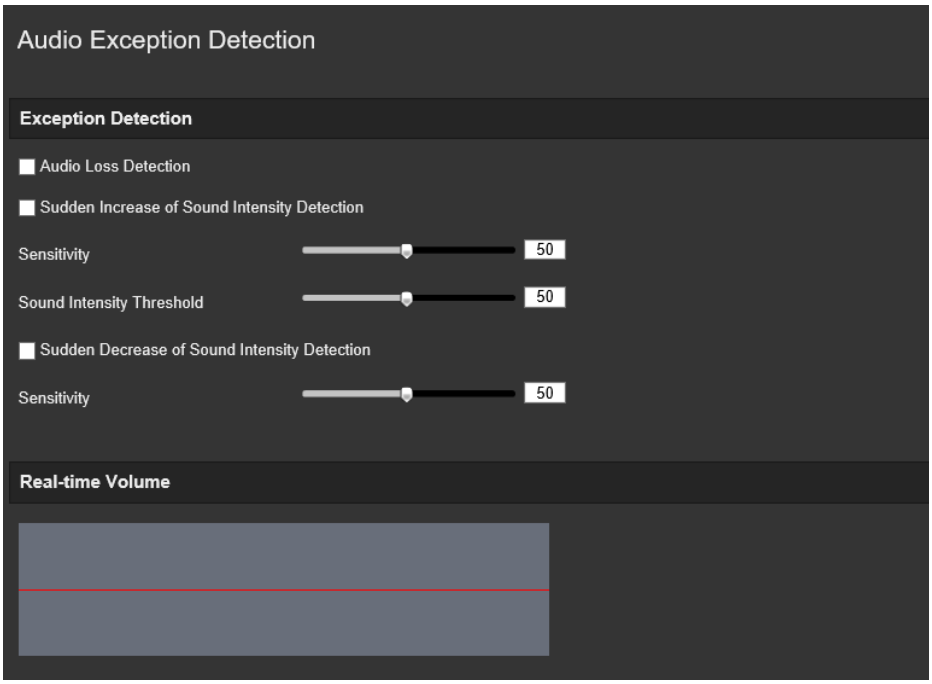
4. Click **Save** to save changes.

Audio exception detection

This function detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity. It can be set up to trigger a series of alarm actions.

To define Audio Exception detection:

1. From the menu toolbar, click **Configuration** > **Event** > **Smart Event** > **Audio Exception Detection**.



2. Check the checkbox of **Audio Loss Exception** to enable the audio loss detection function.
3. Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
4. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.

   Notes:

   Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.

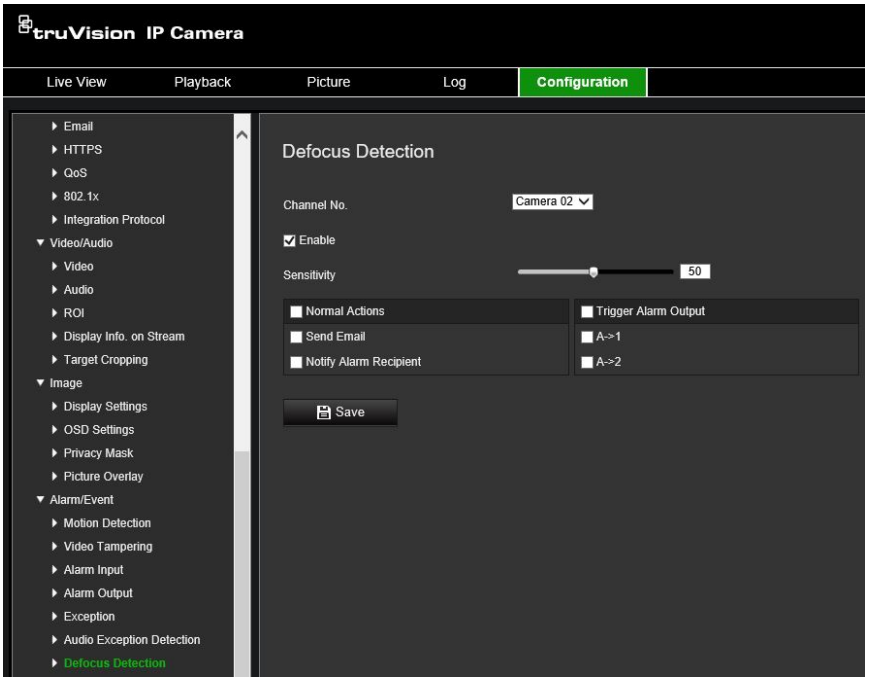
   Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

   You can view the real-time volume of the sound on the interface.
5. Click **Arming Schedule** to set the arming schedule.

6. Click **Linkage Method** and select the linkage methods for audio exception, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording and Trigger Alarm Output.
7. Click **Save** to save the settings.

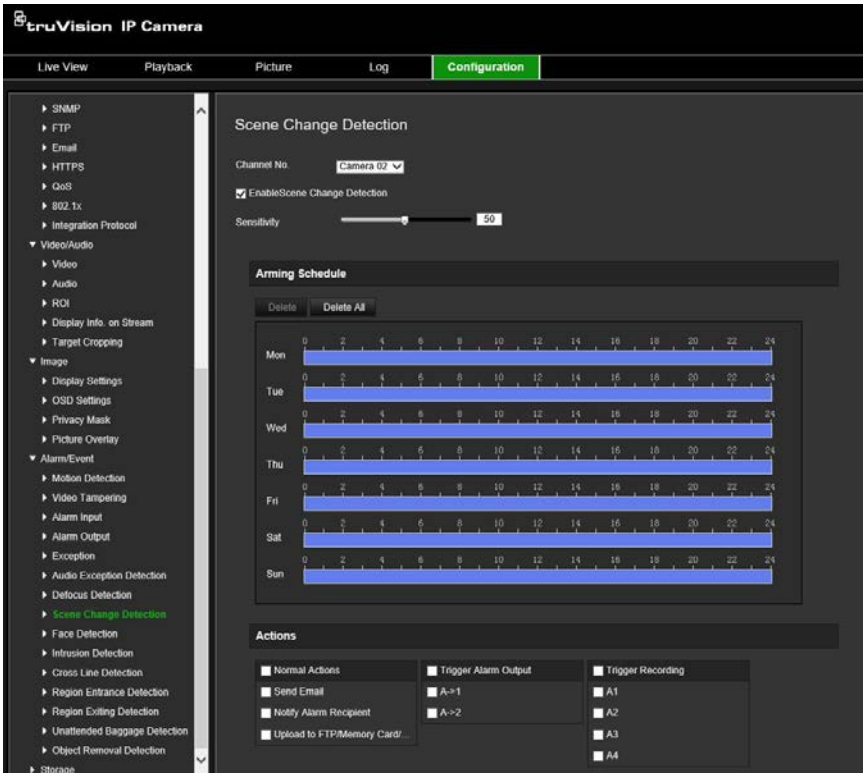
Defocus detection

Image blur is caused by defocusing the camera lens (e.g., someone interfering with the lens) can be detected. This can be set up to trigger a series of alarm actions.



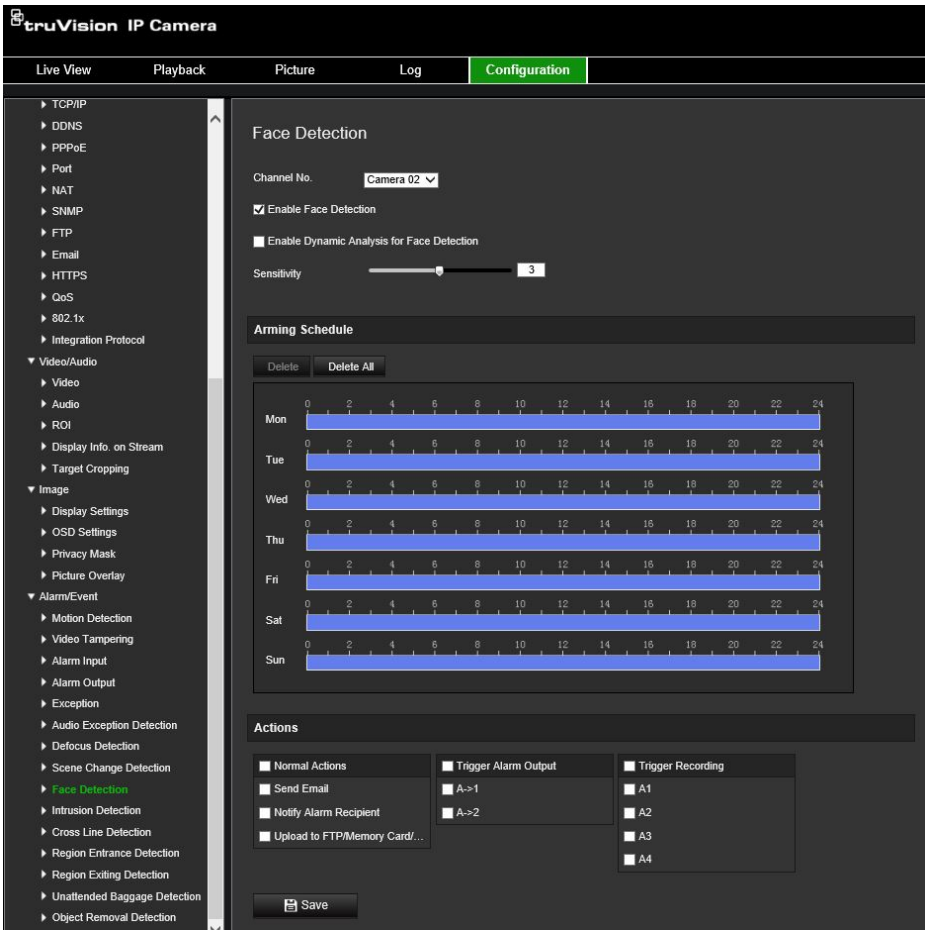
Scene change detection

This function detects the change of surveillance environment affected by the external factors, such as the intentional rotation of the camera. It can be set up to trigger a series of alarm actions.



Face detection

This function detects the face appears in the surveillance scene. It can be set up to trigger a series of alarm actions.



To define face detection:

1. From the menu toolbar, click **Configuration > Event > Smart Event > Face Detection**.
2. Select the **Enable Face Detection** checkbox to enable the function.
3. Select the **Enable Dynamic Analysis for Face Detection** checkbox. The detected face is marked with a green rectangle in live view mode.

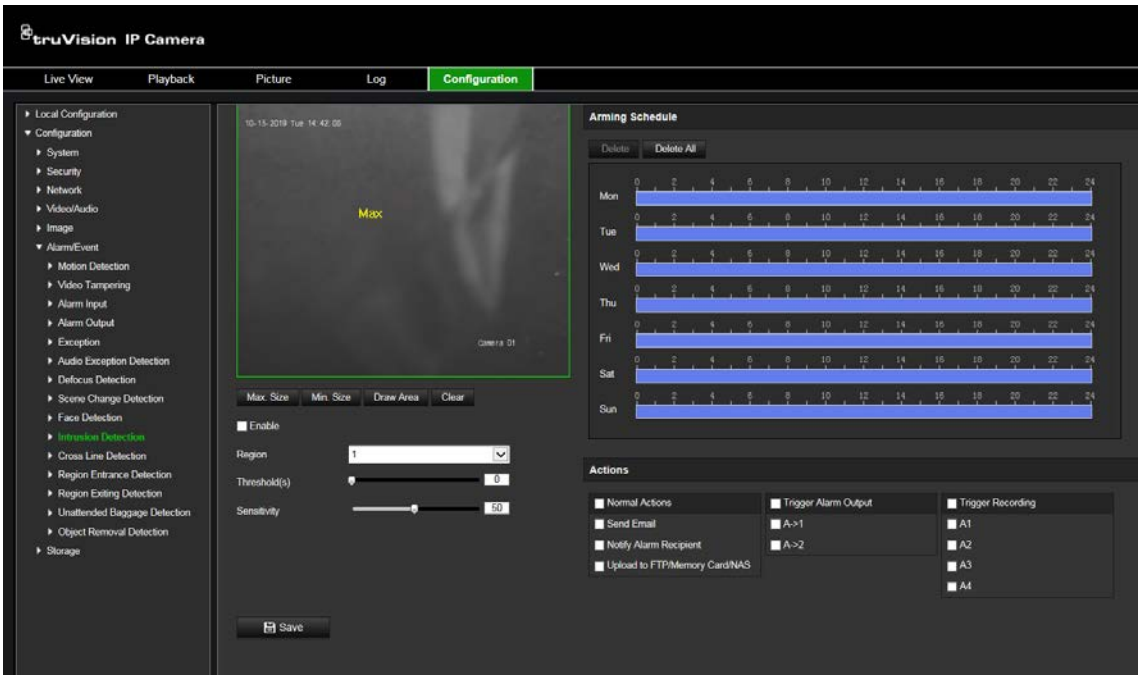
   Note: To be able to mark the detected face in live view mode, go to **Configuration** > **Local** to enable the rules.
4. Click-and-drag the slider to set the detection sensitivity. The Sensitivity ranges from 1 to 5. The higher the value is, the more easily the face can be detected.
5. Set the arming schedule for the alarm input. See “To set up motion detection” for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when an intrusion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 27 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” on page 65 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.
Trigger Recording	Triggers the recording to start in the camera.

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 15: Intrusion detection window



To define intrusion detection:

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

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

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

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

   Sensitivity: The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, a small object can trigger an alarm. The range is between 1 and 100.
5. Set the arming schedule for the alarm input. See “To set up motion detection” for more information.
6. Specify the linkage method when an event occurs. Check one or more response methods for the system when an intrusion detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. **Note:** You must configure email settings before enabling this option. See “To set up the email parameters” on page 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings.
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.
Trigger Recording	Triggers the recording to start in the camera.

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

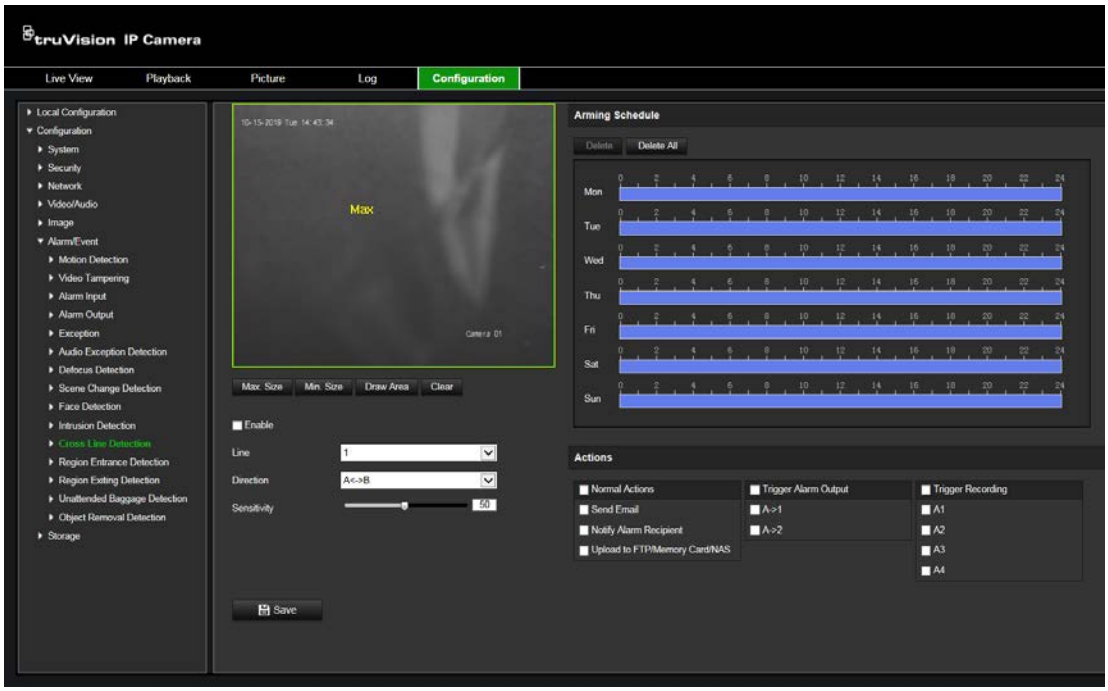
Cross line detection

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** > **Alarm Event** > **Cross Line**.



2. Check the **Enable Cross Line** detection check box to enable the function.
3. Click **Draw Area**, and a crossing plane will show on the image.
4. Click the line and two red squares appear at each end. Drag one of the red squares to define the arming area.

   Select the direction as A<->B, A ->B, or B->A from the drop-down list (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. The higher the value is, the more easily the line crossing action can be detected.
6. If desired, select another line crossing area to configure from the dropdown menu. Up to four line crossing areas can be configured.
7. Set the arming schedule for the alarm input. See “To set up motion detection” 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.

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 27 for further information. If you want to send the event snapshot together with the email, check the **Attached Snapshot** option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. **Note**: To upload the snapshot to NAS, you must first configure the NAS settings.
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.
Trigger Recording	Triggers the recording to start in the camera.

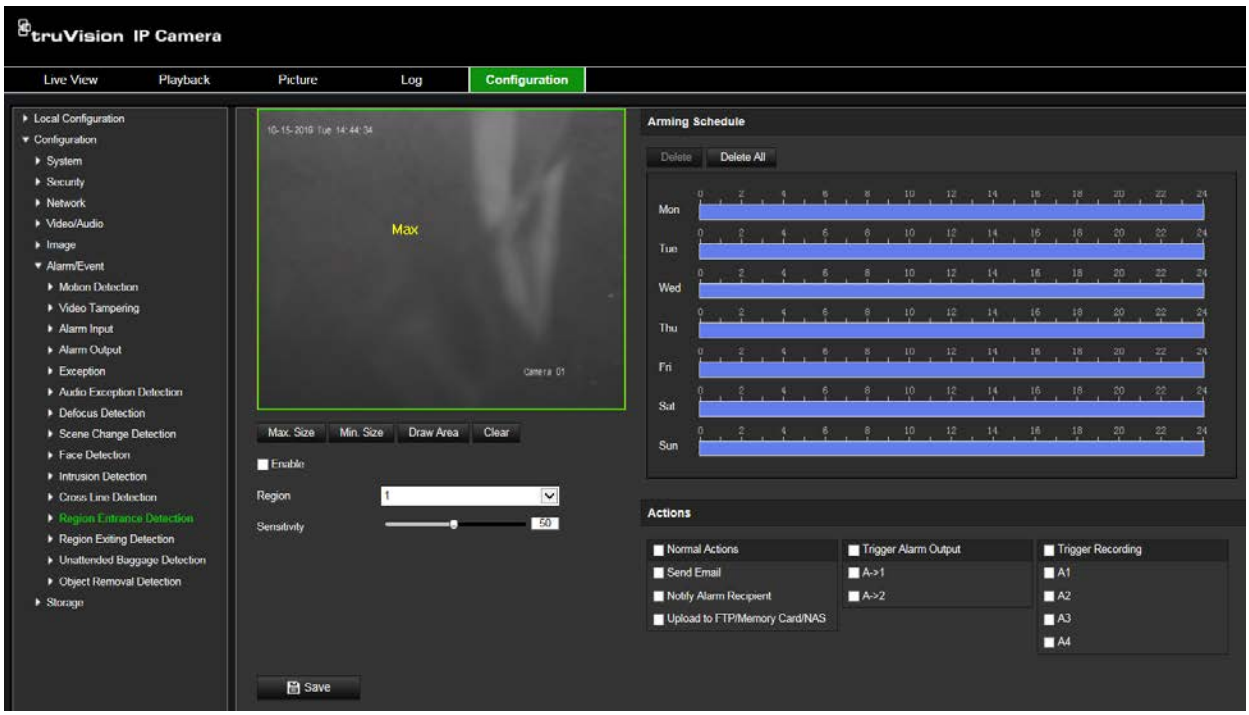
9. Click **Save** to save changes.

Region entrance detection

This function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place. It can be set up to trigger a series of alarm actions.

To define region entrance detection:

1. From the menu toolbar, click **Configuration** > **Event** > **Smart Event** > **Region Entrance Detection**.



2. Select the **Enable** checkbox to enable the function.

3. Select **Region** from the drop-down list to set up.
4. Click **Area Settings** and click **Draw Area** button to start the drawing area.
5. Click on the live video to specify the four vertexes of the detection region, and right-click to complete drawing.
6. Set the maximum and minimum sizes of valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finished drawing.
8. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = 100 – S1/ST*100

   S1 stands for the target body part that enters the pre-defined region ST stands for the complete target body.

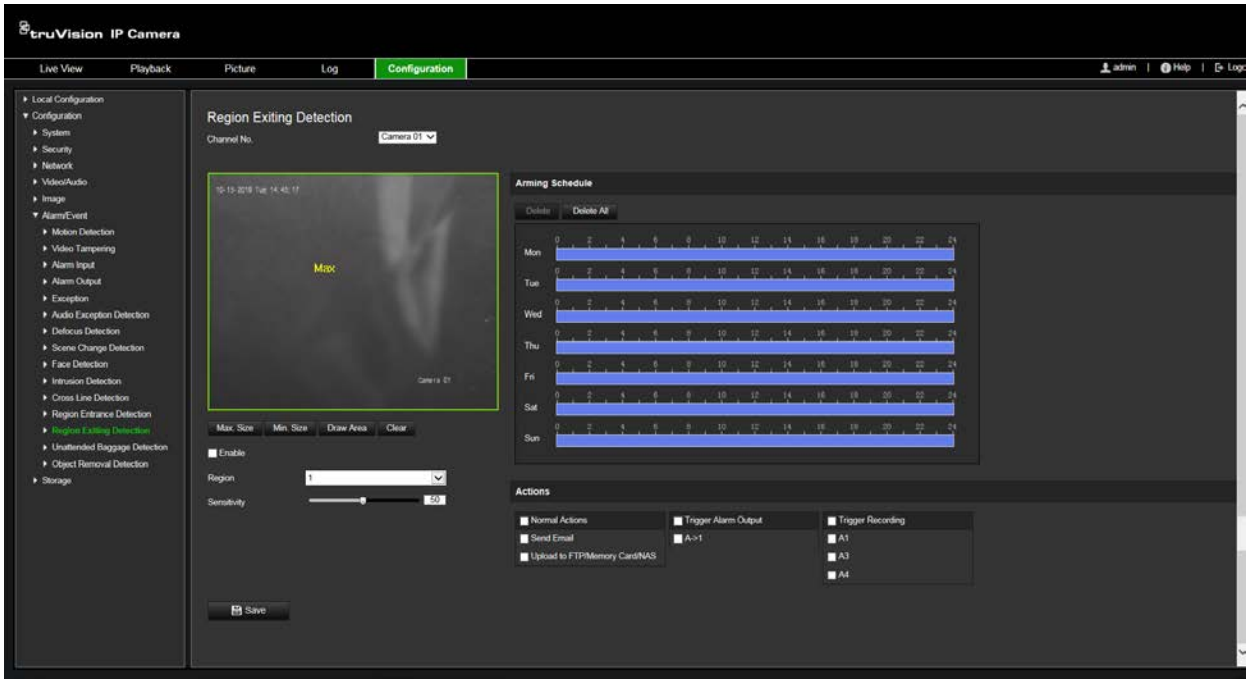
   Example: if you set the value as 60, the action can be counted as an region entrance action only when 40 percent body part enters the region.
9. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Linkage Method** to select the linkage methods.
12. Click **Save** to save the settings.

Region exiting detection

This function detects people, vehicle or other objects which exit from a pre-defined virtual region. It can be set up to trigger a series of alarm actions.

To define region exit detection:

1. From the menu toolbar, click **Configuration** > **Event** > **Smart Event** > **Region Exiting Detection**.



2. Select the **Enable** checkbox to enable the function.
3. Select **Region** from the drop-down list to set up.
2. Click **Area Settings** and click **Draw Area** button to start the drawing area.
3. Click on the live video to specify the four vertexes of the detection region, and right-click to complete drawing.
4. Set the maximum and minimum sizes of valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
5. Click **Stop Drawing** when finished drawing.
6. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = 100 – S1/ST*100

   S1 stands for the target body part that enters the pre-defined region ST stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as an region entrance action only when 40 percent body part enters the region.
7. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click **Arming Schedule** to set the arming schedule.
9. Click **Linkage Method** to select the linkage methods.

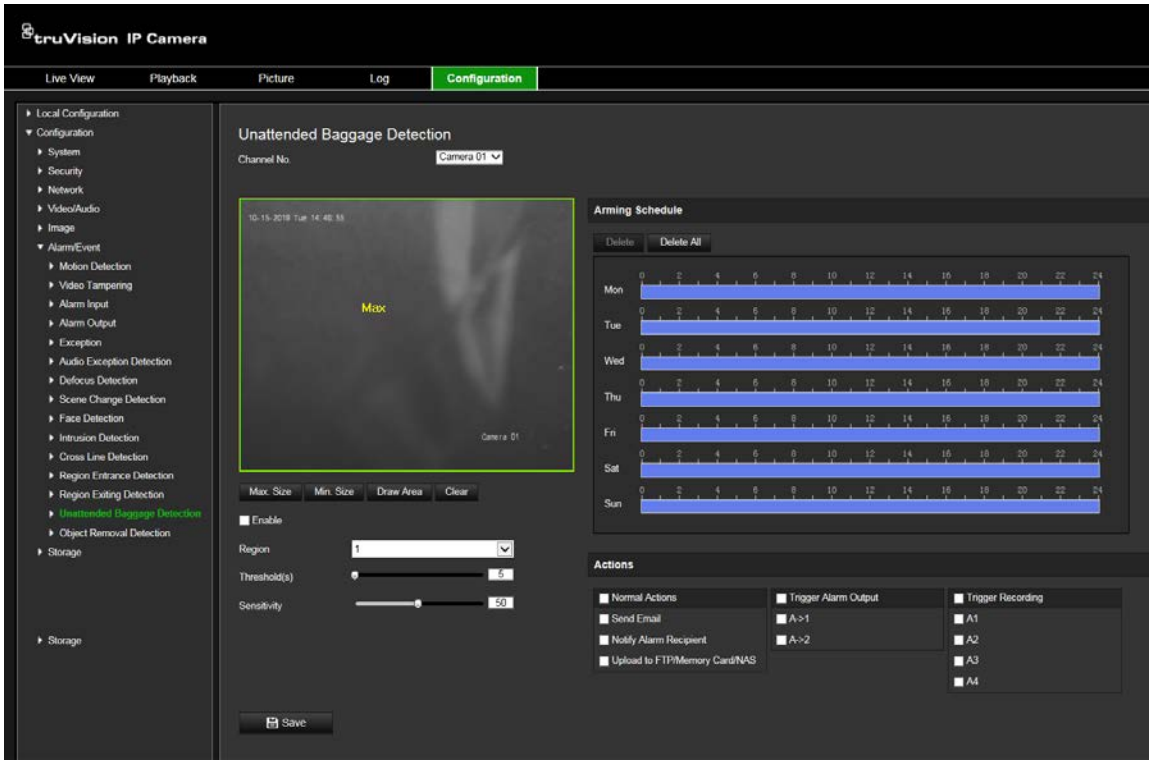
10. Click **Save** to save the settings.

Unattended baggage detection

This function detects the objects left behind in the pre-defined region such as a suitcase, purse, dangerous materials, etc. It can be set up to trigger a series of alarm actions. Please note that this feature is not able to properly detect unattended objects in complex and low contrast environments.

To define unattended baggage detection:

1. From the menu toolbar, click **Configuration** > **Event** > **Smart Event** > **Unattended Baggage Detection**.



2. Select the **Enable** checkbox to enable the function.
3. Select **Region** from the drop-down list to set up.
4. Click **Area Settings** and click **Draw Area** button to start the drawing area.
5. Click on the live video to specify the four vertexes of the detection region, and right-click to complete drawing.
6. Set the maximum and minimum sizes of valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finished drawing.

8. Set the time threshold and detection sensitivity for unattended baggage detection.

   Threshold: Range [5-100s], the threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object is left and stay in the region for 10s.

9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = 100 – S1/ST*100

   S1 stands for target body part that enters the pre-defined region. ST stands for the complete target body.

   Example: if you set the value as 60, a target is possible to be counted as an unattended baggage only when 40 percent body part of the target enters the region.

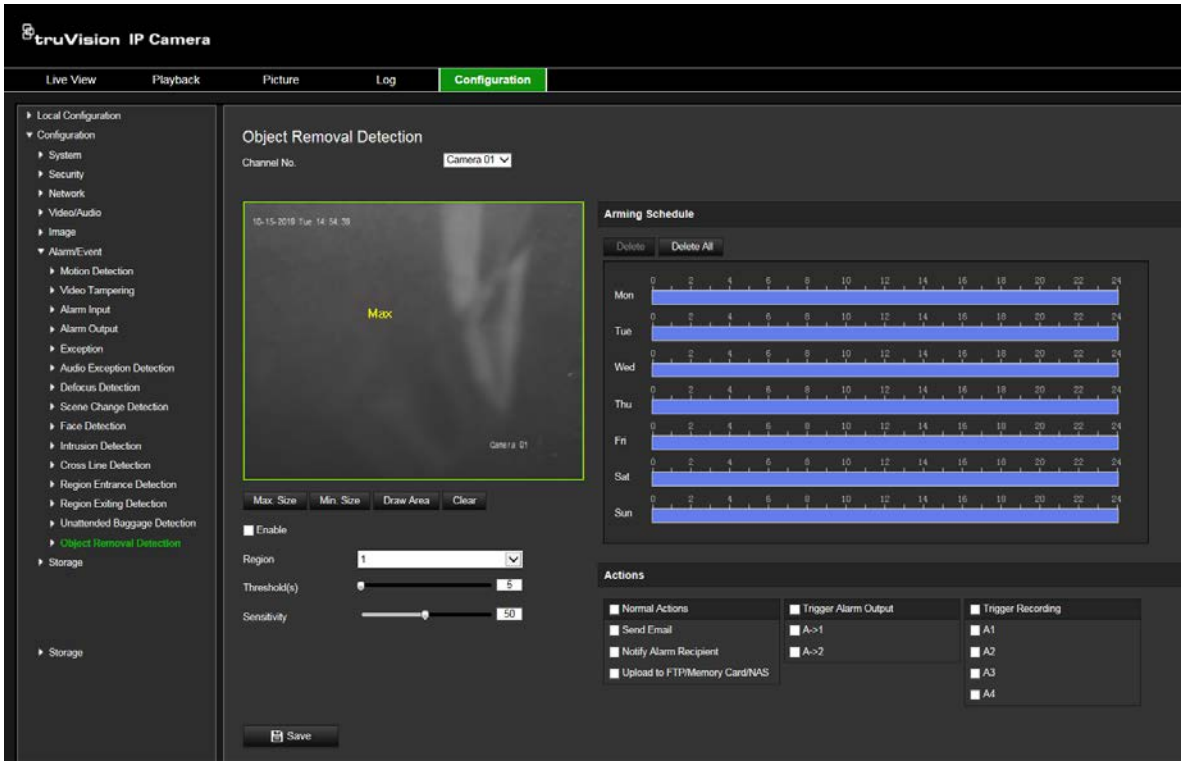
10. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods.
13. Click **Save** to save the settings.

Object removal detection

This function detects the objects removed from the pre-defined region, such as the exhibits on display It can be set up to trigger a series of alarm actions. Please note that this feature is not able to properly detect removed objects in complex and low contrast environments.

To define object removal detection:

1. From the menu toolbar, click **Configuration** > **Event** > **Smart Event** > **Object Removal Detection**.



2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the maximum and minimum sizes of valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for object removal detection.

   Threshold: Range [5-100s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.
9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. It stands for the percentage of the body part of an acceptable target that leaves the pre-defined region.

   Sensitivity = 100 – S1/ST*100

   S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body.

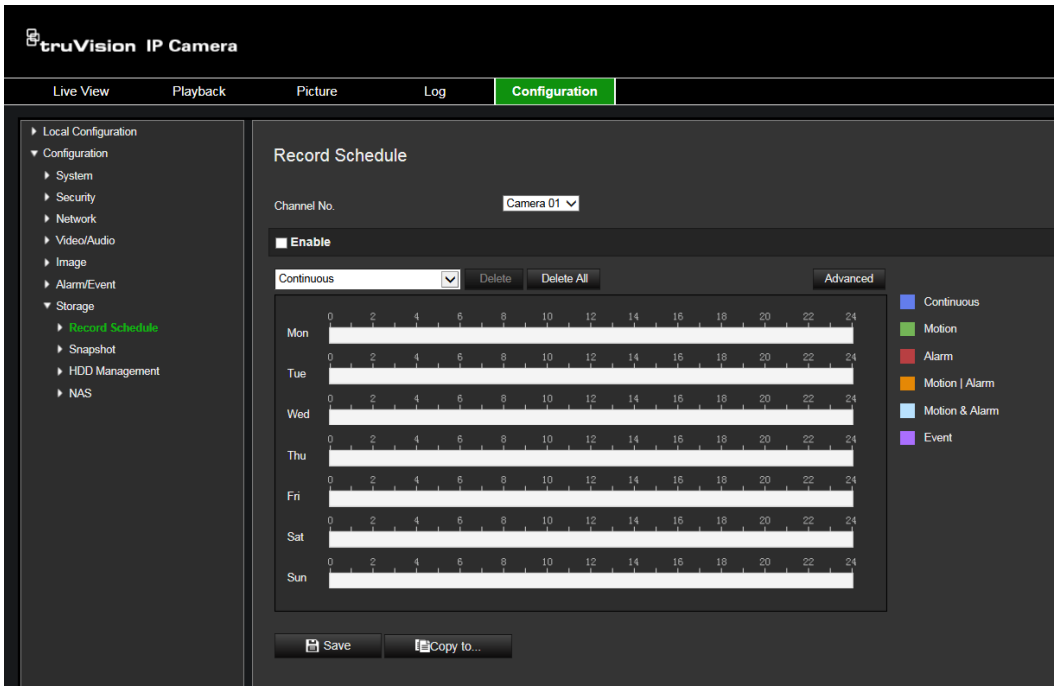
Example: if you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region.

10. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods.
13. Click **Save** to save the settings.

Recording schedule

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

The selected recording schedule applies to all alarm types.



Pre-record time

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

Post-record time

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

Overwrite

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

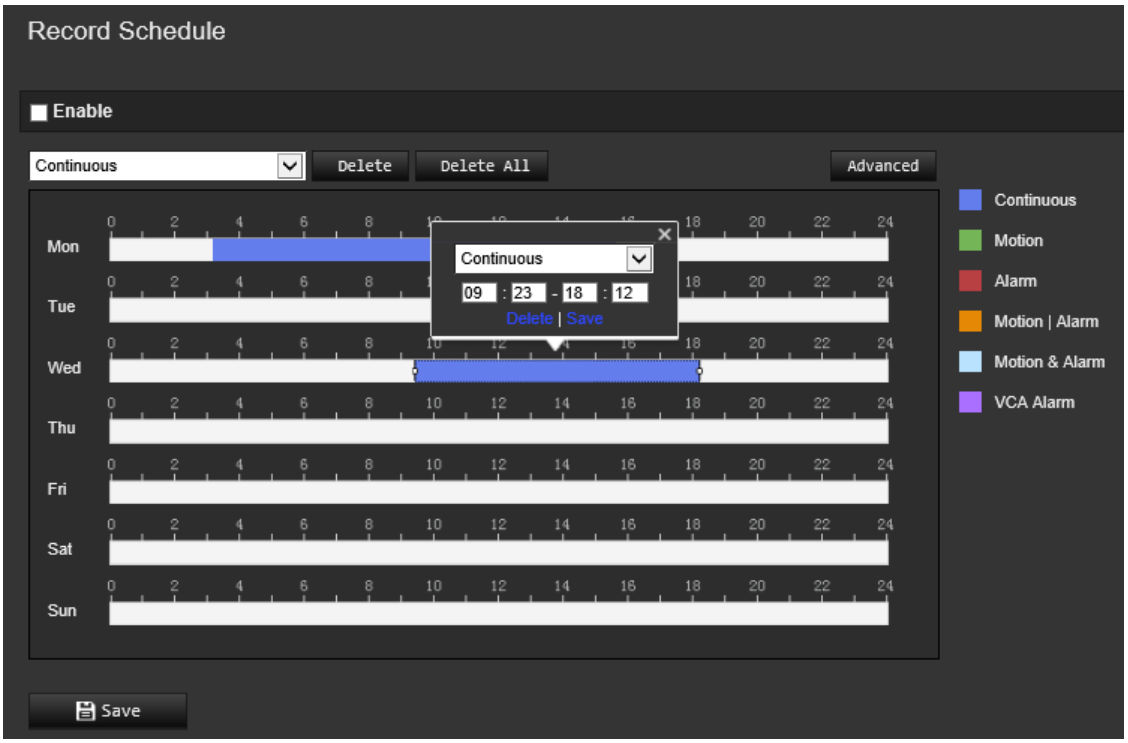
Recording stream

There are two options to select for the recording stream: Main Stream (Normal) and Substream.

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. Edit the recording schedule. The following window appears:



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

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

   - **Continuous**: This is continuous recording.
   - **Motion:** Video is recorded when the motion is detected.
   - **Alarm:** Video is recorded when the alarm is triggered via the external alarm input channels. Besides configuring the recording schedule, you have to set the Alarm Type and check the checkbox of Trigger Channel in the Linkage Method of Alarm Input Settings interface. For detailed information, please refer to Section Alarm Input.

- **Motion | Alarm:** Video will be recorded when the external alarm is triggered or the motion is detected. Besides configuring the recording schedule, you have to configure the settings on the Motion Detection and Alarm Input Settings interfaces.
- **Motion & Alarm:** Video will be recorded when the motion and alarm are triggered at the same time. Besides configuring the recording schedule, you have to configure the settings on the Motion Detection and Alarm Input Settings interfaces.
- **VCA events:** Video will be recorded when the either of the VCA events is triggered. Besides configuring the recording schedule, you have to configure the settings on the VCA interface.

Note: Up to eight record types can be selected.

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

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

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

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

Snapshot

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.

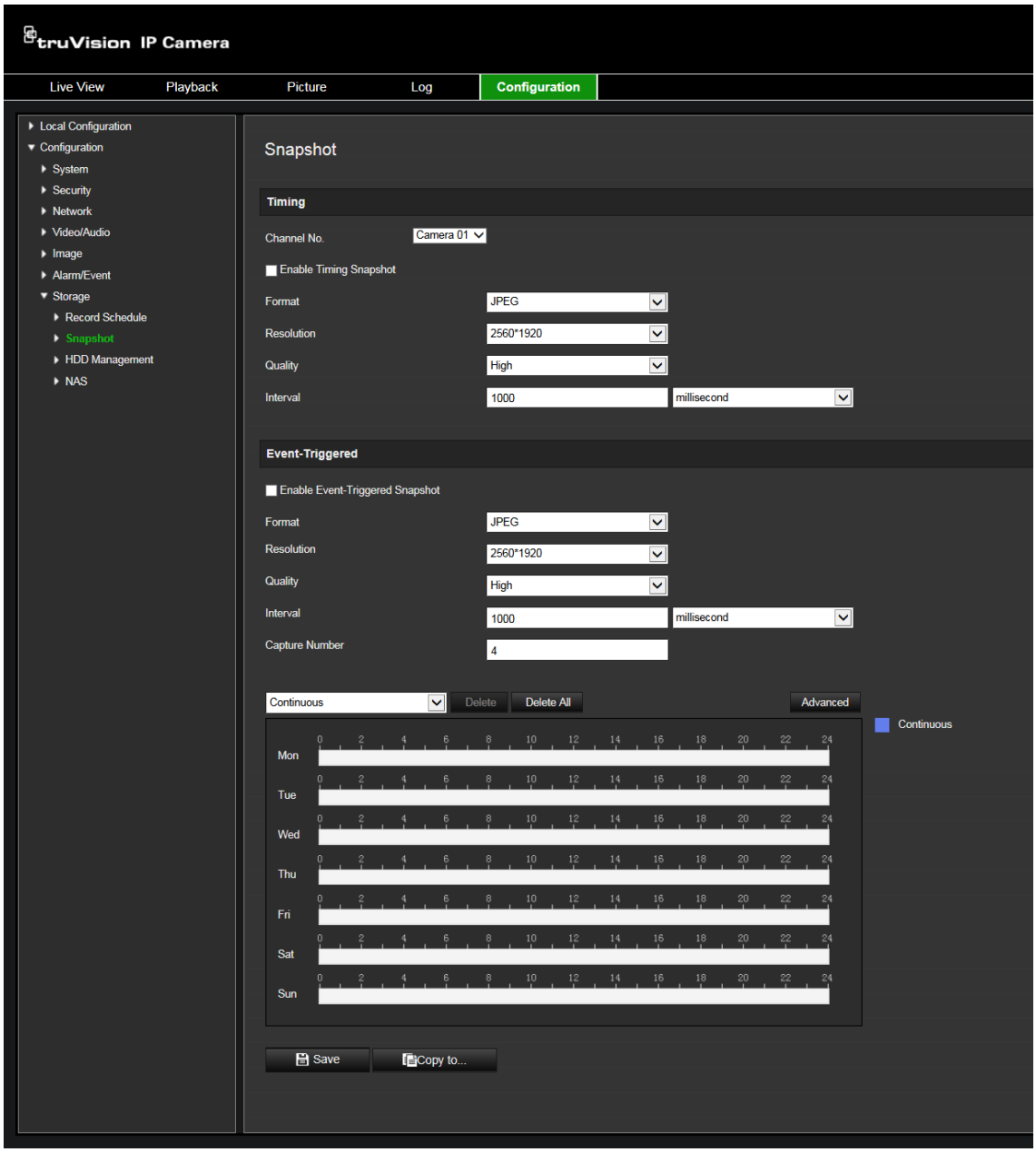
You can set up the format, resolution and quality of the snapshots. The quality can be low, medium, or high.

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.

To set up scheduled snapshots:

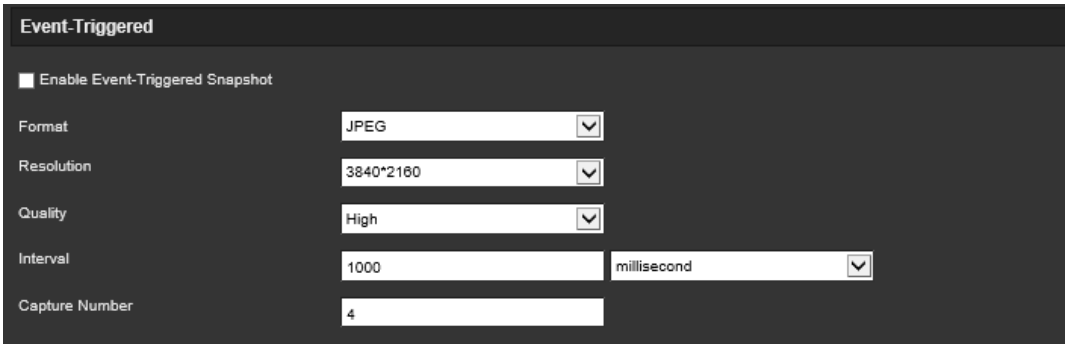
1. From the menu toolbar, click **Configuration** > **Storage** > **Snapshot**.



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. Enter the desired schedule for each day of the week. Click advanced to select stream type, such as main stream (Normal).
7. Click **Save** to save changes.

To set up event-triggered snapshots:

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



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

HDD management

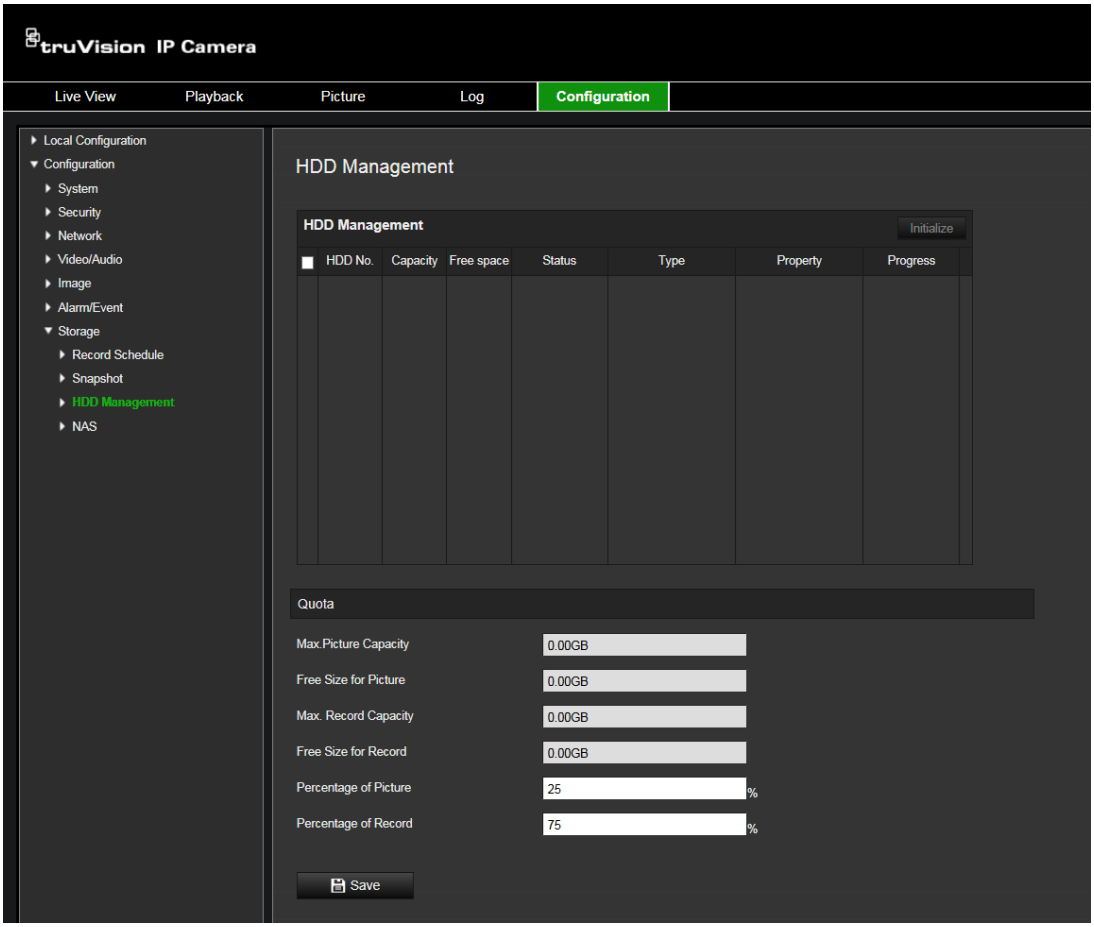
Use the storage management window to display the capacity, free space available, and the working status of the HDD of the NAS and the SD card in the camera. You can also format these storage devices.

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

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

To format the storage devices:

1. Click **Configuration** > **Storage** > **Storage Management**.



2. Check the **HDD No.** tab to select the storage.
3. Click **Format**. A window appears to check your formatting permission.
4. Click **OK** to start formatting.

To define the quota for record and snapshots:

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

NAS

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

To configure record settings, please ensure that you have the network storage device within the network.

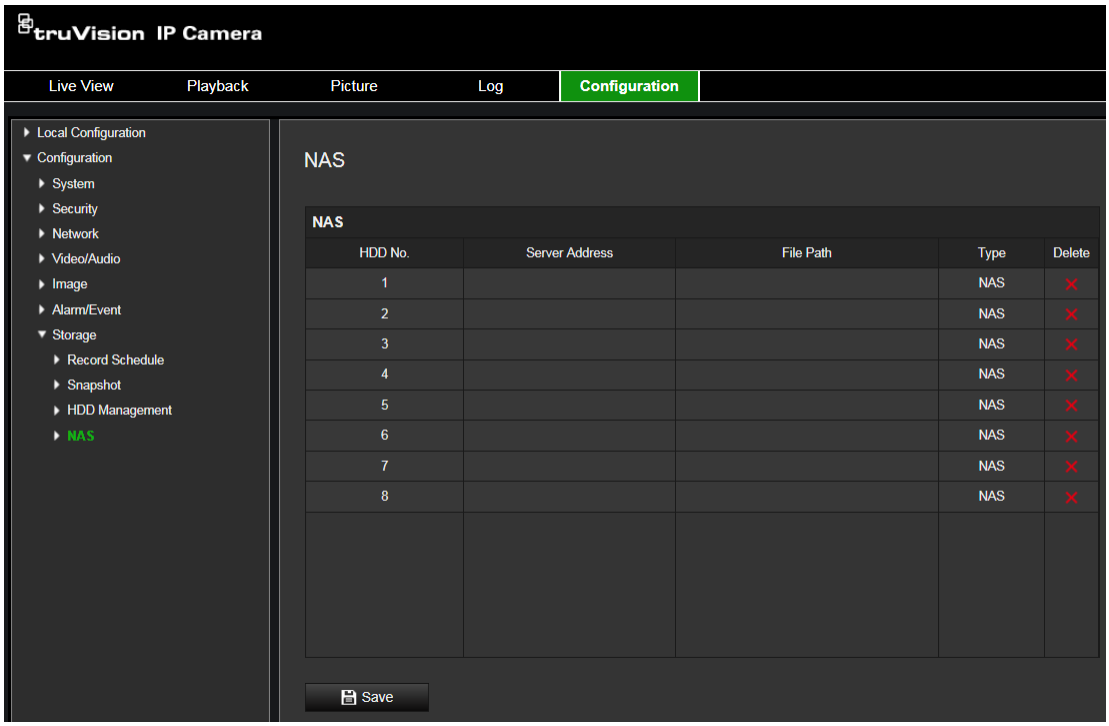
The NAS disk should be available within the network and correctly configured to store the recorded files, log files, etc.

Notes:

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

To set up a NAS system:

1. Click **Configuration** > **Storage** > **NAS**.



2. Enter the IP address of the network disk, and the NAS folder path.
3. Click **Save** to save changes.

Camera management

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

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 **Camera 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 **Device Parameters** and set the saving path to save the configuration file.

Upgrade firmware

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

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

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

To upgrade firmware version:

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

   firesecurityproducts.com

2. When the firmware file is downloaded to your computer, extract the file to the desired destination.

   Note: Do not save the file on your desktop.

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

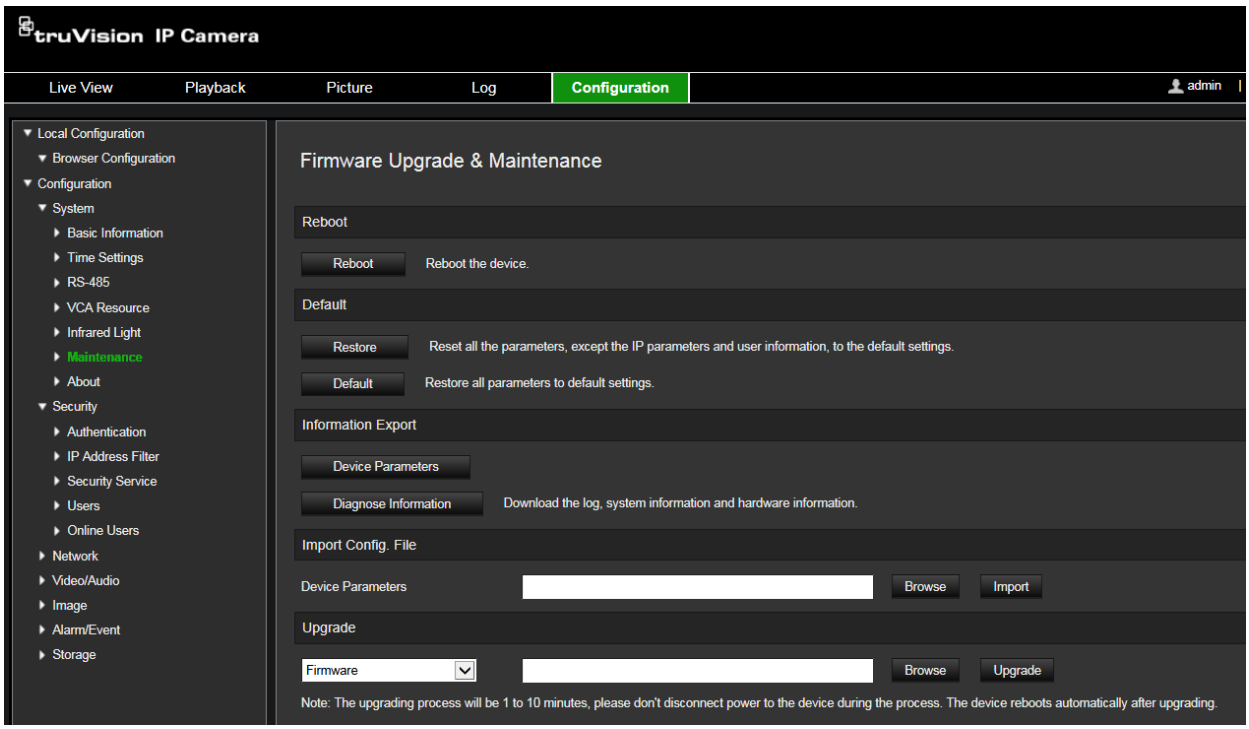
   - **Firmware directory** – Locate the upgrading folder of Firmware files. The camera will choose the corresponding firmware file automatically.
   - **Firmware** – Locate the firmware file manually for the camera.

4. Click **Update**. You will receive a prompt asking you to reboot the camera.

5. When the upgrade is finished, the device will reboot automatically. The browser will also be refreshed.

To upgrade the firmware via TruVision Device Manager:

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



2. Click the browse 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**.

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

Reboot camera

It is easy to reboot the camera remotely.

To reboot the camera through the web browser:

1. In **Camera 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.

On the upper left corner of the logon window, you can select the language of the Browser. It supports English, Chinese, Spanish, German, Russian, French, and Portuguese.

Figure 16: Login dialog box

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.

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.

Taking a snapshot

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

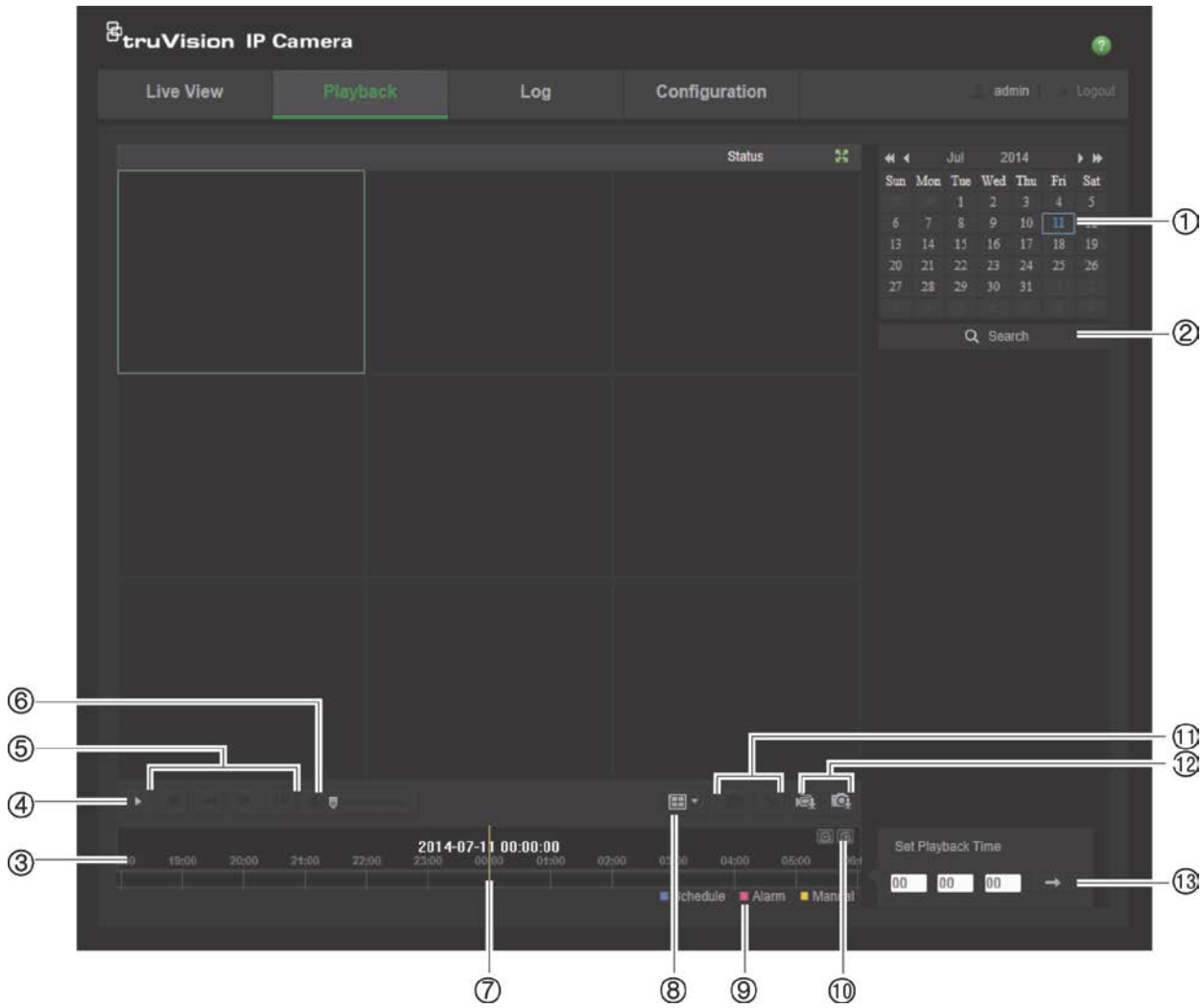
Playing back recorded video

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

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

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

Figure 17: Playback window



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

Name		Description
6.	Audio control	Modify the audio level.
7.	Time moment	Vertical bar shows where you are in the playback recording. The current time and date are also displayed.
8.	Layout	Click to select the number of video tiles you want to use for playback.
9.	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.
10.	Zoom in/out	Click to zoom in or out of the timeline bar.
11.	Archive functions	Click these buttons for the following archive actions:  Capture a snapshot image of the playback video.  Start/Stop clipping video files.
12.	Download functions	 Download video files.  Download captured images.
13.	Set playback time	Input the time and click  to locate the playback point.

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.

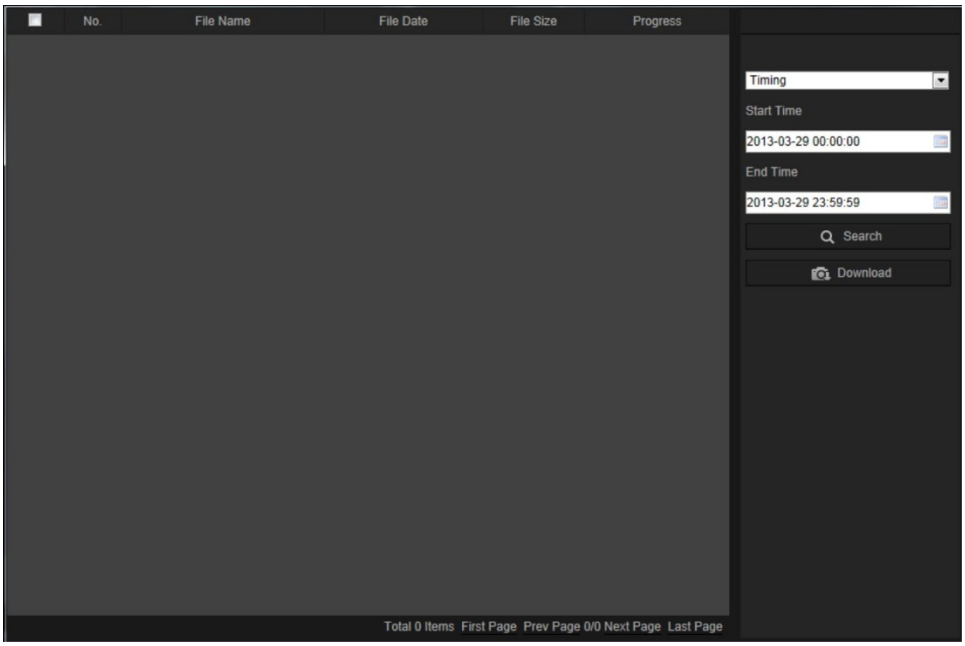
   Note: You must have playback permission to playback recorded images. See “Modify user information” on page 22 for more information.
3. Select the date and click the **Search** button to search for the required recorded file.
4. Click  to search the video file.
5. In the pop-up window, check the box of 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.



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.

Snapshots

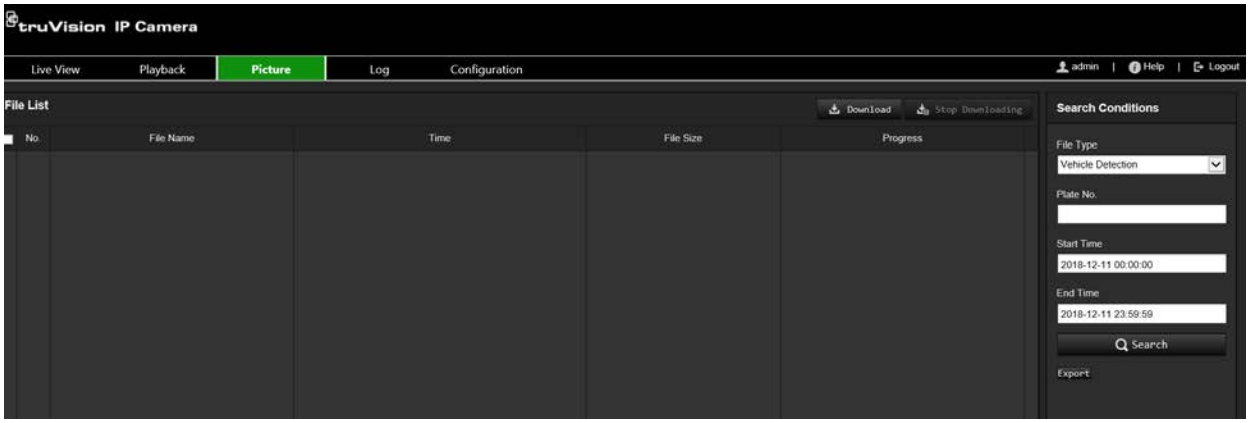
Click **Picture** to enter the snapshot searching interface. You can search, view, and download the snapshots stored in the local storage or network storage.

Notes:

Make sure HDD, NAS or memory card are properly configured before you process the snapshot search.

Make sure a snapshot schedule/method is configured. Go to **Configuration** > **Storage** > **Snapshot** to set the capture schedule.

Figure 25: Picture window



Steps:

1. From the drop-down list, select the file type for which you want to search. Continuous, Motion, Alarm, Face Detection, Cross Line Detection and other supported VCA types are selectable.
2. Set the start time and end time.
3. Click **Search** to search for recorded snapshots matching your search criteria.
4. In the list of snapshots you can check the checkbox of each snapshot and then click the **Download** button to download the selected pictures.

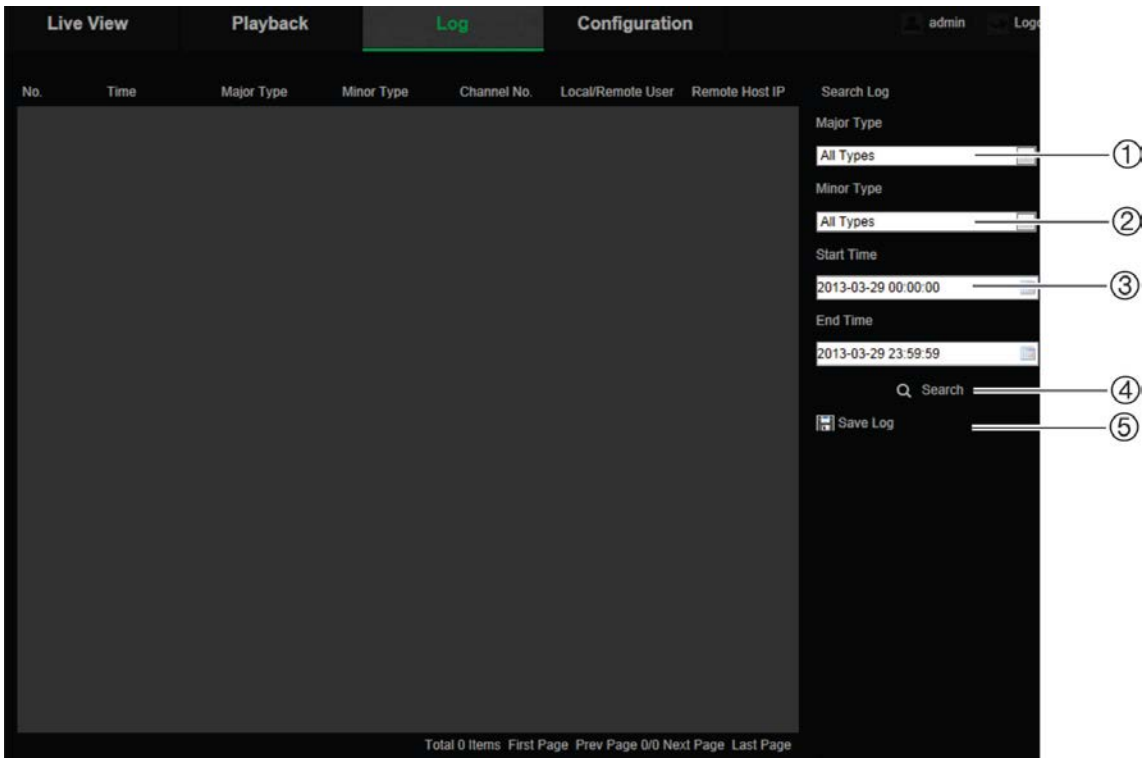
Search event logs

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

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

Note: You must have view log access rights to search and view logs. See “Modify user information” on page 22 for more information.

Figure 18: Log window



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

You can search for recorded logs by the following criteria:

Major type: There are three types of logs: Alarm, Exception, and Operation. You can also search All. See Table 1 below for their descriptions.

Minor type: Each major type 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

Log type	Description of events included
Alarm	Start Motion Detection, Stop Motion Detection, Start Tamper-proof, Stop Tamper-proof
Exception	Invalid Login, HDD Full, HDD Error, Network Disconnected and IP Address Conflicted
Operation	Power On, Unexpected Shutdown, Remote Reboot, Remote Login, Remote Logout, Remote Configure parameters, Remote upgrade, 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, 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.

Use the PTZ control

On the right-hand side of the live view page, you can click ‹ or › to hide or show the PTZ control panel. Some of the PTZ functions, such as pan/tilt, are not available because they are not supported by the camera hardware.

Figure 19: PTZ control panel

Icon	Description
	Directional buttons
	Zoom in/out
	Focus -/+
	Iris -/+
	Pan/tilt speed adjustment
	Enable/disable light
	Enable/disable wiper
	Auxiliary focus
	Lens initialization
	Start manual tracking
	Start 3D zoom

Presets and Preset Tours

A preset is a preconfigured action for the camera that will run automatically after a defined dwell time.

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

Figure 20: Preset and Preset Tour panel

To set a preset:

1. Click the icon to select the preset configuration interface.
2. Use the directional and zoom buttons on the PTZ control panel to move the camera to the desired position.
3. Select a preset number from the preset list.
4. Click the icon to save the current PTZ view as the preset.

   The preset name turns from grey to black.

To call up a preset:

1. Click the icon to select the preset configuration interface.
2. Select the desired preset number from the list.
3. Click the icon to call the selected preset.

   The selected PTZ View will move to the pre-defined preset scene.

To delete a preset:

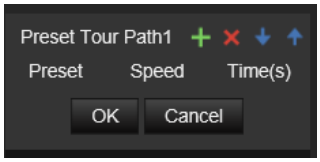
1. Select the preset number from the list.
2. Click the icon to delete the selected preset.

   The preset name turns from black to grey.

To set a preset tour:

Note: At least two presets are required to set a preset tour.

1. Click the icon to enter the preset tour configuration interface.



2. Select a preset tour path number from the drop-down list, and click the icon to configure the path.

3. Click  to add a preset into the path, and click  to delete a preset.
4. Set the preset number, speed and lingering time at each preset. You can adjust the order of presets by using  and  .
5. Click **OK** to save preset tour path.

   Note: Up to 32 preset tour paths can be set. Each path can support up to 16 steps.

To call a preset tour:

1. Click the icon  to enter the preset tour configuration interface.
2. Select the preset tour path number from the drop-down list.
3. Click the icon  to start the selected preset tour and  to stop it.

To delete a preset tour:

1. Select the preset tour path number from the drop-down list.
2. Click the icon  to delete the preset tour path.

Index