| Copyright | © 2016 United Technologies Corporation. Interlogix is part of UTC Climate, Controls & Security, a unit of United Technologies Corporation. All rights reserved. |
| Trademarks and patents | Trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products. |
| Manufacturer | Interlogix.  
2955 Red Hill Avenue, Costa Mesa, CA 92626-5923, USA  
Authorized EU manufacturing representative: UTC Fire & Security B.V.  
Kelvinstraat 7, 6003 DH Weert, The Netherlands |
| Contact information | For contact information, see www.utcfireandsecurity.com or www.utcfssecurityproducts.eu. |
## Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Network access</td>
<td>5</td>
</tr>
<tr>
<td>Checking your web browser security level</td>
<td>5</td>
</tr>
<tr>
<td>Accessing the camera over the internet</td>
<td>7</td>
</tr>
<tr>
<td>Overview of the camera web browser</td>
<td>7</td>
</tr>
<tr>
<td>Camera configuration</td>
<td>10</td>
</tr>
<tr>
<td>Configuration menu overview</td>
<td>10</td>
</tr>
<tr>
<td>Local configuration</td>
<td>11</td>
</tr>
<tr>
<td>System time</td>
<td>12</td>
</tr>
<tr>
<td>Network settings</td>
<td>14</td>
</tr>
<tr>
<td>Recording parameters</td>
<td>27</td>
</tr>
<tr>
<td>Video image</td>
<td>30</td>
</tr>
<tr>
<td>OSD (On Screen Display)</td>
<td>32</td>
</tr>
<tr>
<td>Overlay text</td>
<td>34</td>
</tr>
<tr>
<td>Privacy masks</td>
<td>34</td>
</tr>
<tr>
<td>Motion detection alarms</td>
<td>35</td>
</tr>
<tr>
<td>Tamper-proof alarms</td>
<td>39</td>
</tr>
<tr>
<td>Exception alarms</td>
<td>39</td>
</tr>
<tr>
<td>Alarm inputs and outputs</td>
<td>41</td>
</tr>
<tr>
<td>Cross line detection</td>
<td>43</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>45</td>
</tr>
<tr>
<td>Snapshot parameters</td>
<td>46</td>
</tr>
<tr>
<td>NAS settings</td>
<td>48</td>
</tr>
<tr>
<td>Storage devices</td>
<td>49</td>
</tr>
<tr>
<td>Recording schedule</td>
<td>49</td>
</tr>
<tr>
<td>Camera management</td>
<td>53</td>
</tr>
<tr>
<td>User management</td>
<td>53</td>
</tr>
<tr>
<td>RTSP authentication</td>
<td>55</td>
</tr>
<tr>
<td>IP address filter</td>
<td>56</td>
</tr>
<tr>
<td>Restore default settings</td>
<td>58</td>
</tr>
<tr>
<td>Import/export a configuration file</td>
<td>59</td>
</tr>
<tr>
<td>Upgrade firmware</td>
<td>59</td>
</tr>
<tr>
<td>Reboot camera</td>
<td>60</td>
</tr>
<tr>
<td>Camera operation</td>
<td>61</td>
</tr>
<tr>
<td>Logging on and off</td>
<td>61</td>
</tr>
<tr>
<td>Live view mode</td>
<td>61</td>
</tr>
<tr>
<td>Playing back recorded video</td>
<td>62</td>
</tr>
<tr>
<td>Searching event logs</td>
<td>64</td>
</tr>
</tbody>
</table>
Introduction

This is the user manual for TruVision 11/31 Series IP camera models:

**IP mini bullet camera:**
- TVB-1101 (1.3MPX Bullet, 6 mm lens, PAL)
- TVB-3101 (1.3MPX Bullet, 6 mm lens, NTSC)
- TVB-1102 (3MPX Bullet, 6 mm lens, PAL)
- TVB-3102 (3MPX Bullet, 6 mm lens, NTSC)
- TVB-1103 (1.3MPX Bullet, 4 mm lens, PAL)
- TVB-3103 (1.3MPX Bullet, 4 mm lens, NTSC)

**IP VF bullet camera:**
- TVB-1104 (1.3MPX Bullet, 2.8 to 12 mm VF Lens, PAL)
- TVB-3104 (1.3MPX Bullet, 2.8 to 12 mm VF Lens, NTSC)
- TVB-1105 (3MPX Bullet, 2.8 to 12 mm VF Lens, PAL)
- TVB-3105 (3MPX Bullet, 2.8 to 12 mm VF Lens, NTSC)

**IP mini dome camera:**
- TVD-1101 (1.3MPX Plastic Mini Dome, PoE, PAL)
- TVD-3101 (1.3MPX Plastic Mini Dome, PoE, NTSC)
- TVD-1102 (3MPX Plastic Mini Dome, PoE, PAL)
- TVD-3102 (3MPX Plastic Mini Dome, PoE, NTSC)
- TVD-1105 (1.3MPX IP IR Outdoor Mini Dome, PoE/12 VDC, PAL)
- TVD-3105 (1.3MPX IP IR Outdoor Mini Dome, PoE/12 VDC, NTSC)
- TVD-1106 (3MPX IP IR Outdoor Mini Dome, PoE/12 VDC, PAL)
- TVD-3106 (3MPX IP IR Outdoor Mini Dome, PoE/12 VDC, NTSC)

**IP VF mini dome camera:**
- TVD-1103 (1.3MPX VF Mini Dome, PAL)
- TVD-3103 (1.3MPX VF Mini Dome, NTSC)
- TVD-1104 (3MPX VF Mini Dome, PAL)
- TVD-3104 (3MPX VF Mini Dome, NTSC)

**IP wedge camera:**
- TVW-1101 (1.3MPX Wedge, 2.8 mm lens, Grey, PAL)
- TVW-3101 (1.3MPX Wedge, 2.8 mm lens, Grey, NTSC)
- TVW-1102 (3MPX Wedge, 2.8 mm lens, Grey, PAL)
- TVW-3102 (3MPX Wedge, 2.8 mm lens, Grey, NTSC)
- TVW-1117 (1.3MPX Wedge, 2 mm lens, Grey, PAL)
- TVW-3117 (1.3MPX Wedge, 2 mm lens, Grey, NTSC)
- TVW-1118 (1.3MPX Wedge, 2.8 mm lens, White, PAL)
- TVW-3118 (1.3MPX Wedge, 2.8 mm lens, White, NTSC)
- TVW-1119 (1.3MPX Wedge, 2.8 mm lens, Black, PAL)
- TVW-3119 (1.3MPX Wedge, 2.8 mm lens, Black, NTSC)

**IP wireless wedge camera:**
- TVW-1103 (1.3MPX wireless, 2.8 mm lens, Grey, PAL)
- TVW-3103 (1.3MPX wireless, 2.8 mm lens, Grey, NTSC)
- TVW-1104 (1.3MPX wireless, 2.8 mm lens, White, PAL)
- TVW-3104 (1.3MPX wireless, 2.8 mm lens, White, NTSC)
- TVW-1105 (3MPX wireless, 2.8 mm lens, Grey, PAL)
- TVW-3105 (3MPX wireless, 2.8 mm lens, Grey, NTSC)
- TVW-1106 (3MPX wireless, 2.8 mm lens, White, PAL)
- TVW-3106 (3MPX wireless, 2.8 mm lens, White, NTSC)
- TVW-1116 (3MPX wireless, 6 mm lens, White, PAL)
- TVW-3116 (3MPX wireless, 6 mm lens, White, NTSC)
Network access

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

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

Checking your web browser security level

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

Configuring IE ActiveX controls

You should confirm the ActiveX settings of your web browser.

To change the web browser's security level:

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

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

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

![Security Settings - Internet Zone](image)

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

**Windows users**

Internet Explorer for Windows 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, do the following:

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

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

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

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

It is recommended that you change the administrator password once the setup is complete. Only authorized users should be able to modify camera settings. See “User management” on page 53 for further information.

To access the camera online:

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

   The Login dialog box appears.

   **Note:** Ensure that the Active X controls are enabled.

2. Enter your user name and password.

   User name: admin

   Password: 1234

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

Overview of the camera web browser

The camera web browser lets you view, record, and play back recorded videos as well as manage the camera from any PC with Internet access. The browser’s easy-to-use controls give you quick access to all camera functions. See Figure 1 on page 8.

If there is more than one camera connected over the network, open a separate web browser window for each individual camera.
**Figure 1: Web browser interface**

![Image of web browser interface]

**Table 1: Overview of the web browser interface**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Live view</td>
<td>Click to view live video.</td>
</tr>
<tr>
<td>2. Playback</td>
<td>Click to play back video.</td>
</tr>
<tr>
<td>3. Log</td>
<td>Click to search for event logs. There are three main types: Alarm, Exception and Operation.</td>
</tr>
<tr>
<td>4. Configuration</td>
<td>Click to display the configuration window for setting up the camera.</td>
</tr>
<tr>
<td>5. Viewer</td>
<td>View live video. Time, date and camera name are displayed here.</td>
</tr>
<tr>
<td>6. Current user</td>
<td>Displays current user logged on.</td>
</tr>
<tr>
<td>7. Logout</td>
<td>Click to log out from the system. This can be done at any time.</td>
</tr>
<tr>
<td>8. Aspect ratio</td>
<td>Select the aspect</td>
</tr>
<tr>
<td>9. Streaming</td>
<td>Switch between main stream and substream.</td>
</tr>
<tr>
<td>10. Start/stop live view</td>
<td>Click to start/stop live view.</td>
</tr>
<tr>
<td>11. Audio</td>
<td>Adjust volume.</td>
</tr>
<tr>
<td>12. Manual Alarm</td>
<td>Click to trigger the alarm output.</td>
</tr>
<tr>
<td>13. Bidirectional audio</td>
<td>Turn on/off microphone.</td>
</tr>
<tr>
<td>14. Capture</td>
<td>Click to take a snapshot of the video. The snapshot will be saved to the default folder in JPEG format.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>15. Start/stop recording</td>
<td>Click to record live video.</td>
</tr>
<tr>
<td>16. Digital Zoom</td>
<td>Click to enable digital zoom.</td>
</tr>
</tbody>
</table>
Camera configuration

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

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

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

There are two main folders in the configuration panel:

- Local configuration
- Configuration

Configuration menu overview

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

Table 2: Overview of the Configuration panel

<table>
<thead>
<tr>
<th>Configuration folders</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. System</td>
<td>Defines the camera name and number. Displays basic information on the device including SN and the current firmware version, time settings, maintenance, and serial port parameters. See “System time” on page 12, “Restore default settings” on page 58, and “Upgrade firmware” on page 59 for more information.</td>
</tr>
<tr>
<td>2. Network</td>
<td>Defines the network parameters required to access the camera over the internet. See “Network settings” on page 14 for more information.</td>
</tr>
<tr>
<td>Configuration folders</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>3. Video/Audio</td>
<td>Defines recording parameters. See “Recording parameters” on page 27 for more information.</td>
</tr>
<tr>
<td>4. Image</td>
<td>Defines the image parameters, OSD settings, overlay text, and privacy mask. See “Video image” on page 30, “OSD (On Screen Display)” on page 32, “Overlay text” on page 34, and “Privacy masks” on page 34 for more information.</td>
</tr>
<tr>
<td>5. Security</td>
<td>Defines who can use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and Telnet access. See “Camera management” on page 53 for more information.</td>
</tr>
<tr>
<td>7. Smart Event</td>
<td>Defines cross line and intrusion detection.</td>
</tr>
<tr>
<td>8. Storage</td>
<td>Defines recording schedule, storage management, NAS configuration, and Snapshot parameters. See “NAS settings” on page 48, “Storage devices” on page 49, and “Recording schedule” on page 49 for more information, and “Snapshot parameters” on page 46 for more information.</td>
</tr>
</tbody>
</table>

**Local configuration**

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

**Figure 3: Example of a configuration window (Local configuration shown)**
Table 3: Overview of the Local configuration window

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

**System time**

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

**To define the system time and date:**

1. 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 date of the DST period.

5. Click Save to save changes.
Network settings

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

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. TCP/IP  | **Select NIC**: Specifies LAN or WLAN for different network.  
**NIC Type**: Specifies the NIC type. Default is Auto. Other options include: 10M Half-dup, 10M Full-dup, 100M Half-dup and 100M Full-dup.  
**DHCP**: Enable to automatically obtain an IP address and other network settings from that server.  
**IPv4 Address**: Specifies the IPv4 address of the camera.  
**IPv4 Subnet Mask**: Specifies the IPv4 subnet mask.  
**IPv4 Default Gateway**: Specifies the IPv4 gateway IP address.  
**IPv6 Mode**: Specifies the IPv6 mode, including Manual, DHCP and Router Advertisement.  
**IPv6 Address**: Specifies the IPv6 address of the camera.  
**IPv6 Subnet Prefix Length**: Specifies the IPv6 prefix length.  
**IPv6 Default Gateway**: Specifies the IPv6 gateway IP address.  
**Mac Address**: Specifies the mac address of the camera.  
**MTU**: Specifies the valid value range of MTU. Default is 1500.  
**Multicast Address**: Specifies a D-class IP address between 224.0.0.0 to 239.255.255.255. Only specify this option if you are using the multicast function. Some routers prohibit the use of multicast function in case of a network storm. |
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Multicast Discovery</strong>:</td>
<td>Enables the automatic detection of the online network camera via private multicast protocol in the LAN.</td>
</tr>
<tr>
<td><strong>DNS server</strong>:</td>
<td>Specifies the DNS server for your network.</td>
</tr>
<tr>
<td><strong>2. Port</strong></td>
<td><strong>HTTP Port</strong>: The HTTP port is used for remote internet browser access. Enter the port used for the Internet Explorer (IE) browser. Default value is 80. <strong>RTSP Port</strong>: 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. <strong>HTTPS Port</strong>: 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. <strong>Server Port</strong>: This is used for remote client software access. Enter the server port value. The default port number is 8000. <strong>Alarm Server IP</strong>: Specifies the IP address of the alarm host. <strong>Alarm Server Port</strong>: Specifies the port of the alarm host.</td>
</tr>
<tr>
<td><strong>3. DDNS</strong></td>
<td>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. Specifies IP server, DynDNS, and ezDDNS. <strong>DynDNS (Dynamic DNS)</strong>: Enter the user name and password registered to the DynDNS web site. The domain name is that of the DynDNS web site. <strong>ezDDNS</strong>: Enter the host name. It will automatically register it online. <strong>IPServer</strong>: Enter the address of the IP Server.</td>
</tr>
<tr>
<td><strong>4. PPPoE</strong></td>
<td>Retrieves a dynamic IP address.</td>
</tr>
<tr>
<td><strong>5. SNMP</strong></td>
<td>SNMP is a protocol for managing devices on networks. Enable SNMP to get camera status and parameter related information.</td>
</tr>
<tr>
<td><strong>6. QoS</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>7. FTP</strong></td>
<td>Enter the FTP address and folder to which snapshots of the camera can be uploaded.</td>
</tr>
<tr>
<td><strong>8. Wi-Fi</strong></td>
<td>Specifies the wireless network connection parameters.</td>
</tr>
<tr>
<td><strong>9. UPnP</strong></td>
<td>The UPnP (Universal Plug and Play) protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments. With the function enabled, you do not need to configure the port mapping for each port, and the camera is connected to the Wide Area Network (WAN) via the router. Enable and set the friendly name detected.</td>
</tr>
<tr>
<td><strong>10. Email</strong></td>
<td>Specifies the email address to which messages are sent when an alarm occurs.</td>
</tr>
</tbody>
</table>
11. **NAT**  
   The UPnP (Universal Plug and Play) protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments. With the function enabled, you do not need to configure the port mapping for each port, and the camera is connected to the Wide Area Network (WAN) via the router. 
   Enable and set the friendly name detected.

12. **HTTPS**  
   Specifies authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

**Parameters** | **Description**
--- | ---
11. **NAT** | The UPnP (Universal Plug and Play) protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments. With the function enabled, you do not need to configure the port mapping for each port, and the camera is connected to the Wide Area Network (WAN) via the router. Enable and set the friendly name detected.
12. **HTTPS** | Specifies authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

**To define the TCP/IP parameters:**

1. Click Configuration > Network > TCP/IP.

2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings, MTU settings, and Multicast Address.

3. If the DHCP server is available, check **DHCP**.

4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the Preferred DNS Server or Alternate DNS Server.

5. Click **Save** to save changes.
To define the port parameters:

1. 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. It can be changed to any port number that is not occupied.
   - **RTSP Port**: The default port number is 554. It can be changed to any port number in the range from 1 to 65535.
   - **HTTPS Port**: The default port number is 443. It can be changed to any port number that is not occupied.
   - **Server Port**: The default server port number is 8000. It can be changed to any port number in the range from 2000 to 65535.

3. Enter the IP address and port if you want to upload the alarm information to the remote alarm host. Also check the Notify Alarm Recipient option under Linkage Method of each Event page.

4. Click Save to save changes.

To define the DDNS parameters:

1. Click Configuration > Network > DDNS.
2. Check Enable DDNS to enable this feature.

3. Under 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: Enter the desired host name under “Host Name”. The default host name is utc-serial number. The new host name is registered when you click Save.
     
     **Note:** The default server address is www.tvr-ddns.net, which cannot be changed.
     
     - IPServer: Enter the address of the IP Server.

4. Click Save to save changes.

5. If you selected ezDDNS and changed the host name, click the Get URL button to confirm the domain name, which is displayed under Effect Domain.

**To define the PPPoE parameters:**

1. Click Configuration > Network > PPPoE.
2. Check Enable PPPoE to enable this feature.
3. Enter User Name, Password, and Confirm password for PPPoE access.
4. Click Save to save changes.
To define the SNMP parameters:
1. Click Configuration > Network > SNMP.

2. Select the corresponding version of SNMP: v1, v2c, v3, or “Other Settings”.

3. Configure the SNMP settings. The configuration of the SNMP software should be the same as the settings you configure here.

4. Click Save to save changes.

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

1. 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 to 63. The larger the DSCP value, the higher the priority.

3. Click Save to save changes.

To define the FTP parameters:

1. 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. When the subdirectory is selected, you can use the camera name or camera number as the name of the directory.
Upload type: To enable uploading the snapshots to the FTP server.

3. Click Save to save changes.

To define the Wi-Fi parameters:

1. Click Configuration > Network > Wi-Fi.

![Configuration Screen](image)

**Note:** When configuring the Wi-Fi settings for the first time, connect the camera to the router via a network cable and then open the web browser to complete the Wi-Fi setup by clicking Save. When the Wi-Fi Status changes from “Disconnected” to “Connected”, the wireless connection is successfully set up.

2. Click Search to search the online wireless connections.

3. Click a wireless connection on the list to select it.

4. Select the Network Mode as *Manage* or *Ad-hoc*.
Manage mode: The Security Mode is automatically shown when you select a wireless connection from the list.

Ad-Hoc mode: This is used when accessing the camera via a PC without going through a wireless router. You can identify the camera SSID and specify the Security Mode required.

Note: The Ad-Hoc mode is default enabled with the camera serial number set as SSID.

5. Select the required Security Mode: Not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal (default), or WPA2-enterprise.

6. To quickly setup the Wi-Fi, check the Enable WPS check box to enable the WPS function and select one of the following methods:

   PBC mode: Push the WPS button on your wireless router device and the WPS indicator will start flashing. (The WPS settings may be different per device. Please refer to the wireless router User Manual for details). Then check the PBC Connection check box and click its Connect button. The camera and the wireless network router are connected automatically.

   - Or -

   Router PIN mode: Check your wireless router device and find the PIN code, which is printed on a sticker or printed on the device. Check the Use router PIN code and enter the PIN code in the Router PIN Code text box. Then click the “Use router PIN code” Connect button to connect the camera to the wireless router.

   - Or -

   Camera PIN mode: You can generate the PIN code on the camera side and configure the wireless router to finish the connection setting. (Please check the wireless router User Manual for details). Please note that the PIN code expiration time is 120 seconds.

7. Select the encryption type, TKIP or AES (default).

8. Enter the connection key value. Check the wireless status.

9. Click Save to save changes. Check the wireless status.

To define the IP address settings:

1. Click Configuration > Network > TCP/IP.
2. For “Select NIC”, select WLAN.

3. Set the IPv4 address, the IPv4 Subnet Mask, and the Default Gateway. If you want to be assigned the IP address, check the check box to enable the DHCP.

4. Click Save to save changes.

To define the UPnP parameters:

1. Click Configuration > Network > UPnP.

2. Check the check box to enable the UPnP function. You can edit the name of the device when detected online.

3. Click Save to save changes.

To set up the Email parameters:

1. Click Configuration > Network > Email.
2. Configure the following settings:

**Sender:** The name of the email sender.

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

**SMTP Server:** The SMTP server IP address or host name.

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

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

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

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

**Authentication:** If your email server requires authentication, 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 third user to be notified.
Receiver's Address3: The email address of user to be notified.

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

To set up the NAT parameters:

1. Click Configuration > Network > NAT.

2. Check the Enable Port Mapping check box to enable the NAT function.
3. Select Port Mapping Mode to be Auto or Manual. If you choose Manual mode, set the desired external port.
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.

   ![Create Self-signed Certificate](image)

   Click **OK** to save the settings.

   -Or-

   **To create a certificate request:**

   Click the **Create** button beside “Create Certificate Request”. Enter the country, host name/IP and the other information requested.
3. Click **OK** to save the settings. Download the certificate request and submit it to the trusted certificate authority for signature, such as Symantec or RSA. After receiving the signed valid certificate, upload the certificate to the device.

**Recording parameters**

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

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

**Table 5: Video and audio setting parameters**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Video</td>
<td><strong>Stream Type:</strong> Specifies the streaming method used. Options include: Main Stream (Normal) and Sub Stream.</td>
</tr>
<tr>
<td></td>
<td><strong>Video Type:</strong> Specifies the stream type you wish to record. Select Video Stream to record video stream only. Select Video&amp;Audio to record both video and audio streams.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Video&amp;Audio is only available for those camera models that support audio.</td>
</tr>
<tr>
<td>Tab</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Resolution</strong>: Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. The resolution options listed depend on the type of camera and on whether main or substream is being used. <strong>Note</strong>: Resolutions can vary depending on the camera model.</td>
<td></td>
</tr>
<tr>
<td><strong>Bitrate Type</strong>: Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.</td>
<td></td>
</tr>
<tr>
<td><strong>Video Quality</strong>: Specifies the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, Medium, Higher and Highest.</td>
<td></td>
</tr>
<tr>
<td><strong>Frame Rate</strong>: Specifies the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second. <strong>Note</strong>: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet.</td>
<td></td>
</tr>
<tr>
<td><strong>Max bit rate</strong>: Specifies the maximum allowed bit rate. A high image resolution requires that a high bit rate must also be selected.</td>
<td></td>
</tr>
<tr>
<td><strong>Video Encoding</strong>: Specifies the video encoder used. <strong>Profile</strong>: Different profile indicates different tools and technologies used in compression. Options include: Main Profile.</td>
<td></td>
</tr>
<tr>
<td><strong>I Frame Interval</strong>: A video compression method. It is strongly recommended not to change the default value 50.</td>
<td></td>
</tr>
<tr>
<td><strong>SVC</strong>: 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.</td>
<td></td>
</tr>
<tr>
<td><strong>2. Audio</strong>: <strong>Audio Encoding</strong>: G.722.1, G.711ulaw, G.711alaw, MP2L2 and G.726 are optional. <strong>Audio Input</strong>: “MicIn” is selectable for the built-in microphone. <strong>Input Volume</strong>: Specifies the volume from 0 to 100. <strong>Environmental Noise Filter</strong>: Set it as OFF or ON. When you set the function on the noise detected can be filtered.</td>
<td></td>
</tr>
<tr>
<td><strong>3. ROI</strong></td>
<td>Enable to assign more encoding resource to the region of interest to increase the quality of the ROI whereas the background information is less focused.</td>
</tr>
<tr>
<td><strong>4. Display Info. On Stream</strong></td>
<td>When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.</td>
</tr>
</tbody>
</table>
To define ROI parameters:

1. Click Configuration > Video/Audio > ROI.

2. Draw the region of interest on the image. It supports only one region.

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

4. Check the Fixed Region to manually configure the area. You can choose the Image Quality Enhancing level for ROI encoding, and you can also name the ROI area.

5. Click Save to save changes.

Dual-VCA (Video Content Analysis)

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

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

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

To define Dual-VCA parameters:

1. In the Video/Audio panel, click the Display Info. On Stream tab to open its window.

2. Check the check box to enable Dual-VCA.

3. Click Save to save changes.
Video image

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

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

Figure 6: Camera image settings menu (Auto-switch option selected for Switch Day and Night Settings)

Table 6: Image parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Switch Day and Night Settings</td>
<td></td>
</tr>
<tr>
<td>Auto-Switch</td>
<td>The camera automatically switches between day and night mode. All image settings remain the same for both modes.</td>
</tr>
<tr>
<td>Scheduled Switch</td>
<td>The camera switches between the day and night modes according to the schedule configured (see figure below). The start and end times shown are for day mode. The other time period is for night mode. There are three tabs to configure the day/night settings: Common: The settings are identical for both day and night modes for Image Adjustment, Exposure, Day/Night Switch, Video Adjustment, and Other. Day: Configure the Backlight, White Balance and Image</td>
</tr>
</tbody>
</table>
### Parameter Description

**Enhancement settings for day mode only.**

*Night:* Configure the Backlight, White Balance and Image Enhancement settings for night mode only.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Night</td>
<td>Configure the Backlight, White Balance and Image Enhancement settings for night mode only.</td>
</tr>
</tbody>
</table>

#### 2. Image Adjustment

- **Brightness, Contrast Saturation, Hue, Sharpness**
  - Modifies the different elements of picture quality by adjusting the position of the values for each of parameter.

#### 3. Exposure Settings

- **Iris Mode**
  - Only Manual is available.
- **Exposure Time**
  - The exposure time controls the length of time that the aperture is open to let light into the camera through the lens.
  - Select a higher value if the image is dark and a lower value to see fast moving object.
- **Gain**
  - Select the value to adjust the image brightness.

#### 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. There are three options:
    - *Auto:* Camera automatically detects which mode to use; *Day:* Camera is always in day mode; *Night:* Camera is always in night mode.
- **Switch 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. You can set it between 5 and 120 s.
- **Smart IR**
  - When enabled, it can avoid over exposure issue.
- **IR Light**
  - Select On/OFF to Enable/disable IR.
    - **Enable:** the IR illuminators will be ON, when the camera turns into night mode.
    - **Disable:** the IR illuminators will be OFF, when the camera turns into night mode
    - **Note:** The IR illuminators always are OFF in Daytime mode.

#### 5. Backlight Settings

- **BLC Area**
  - If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right, and Center are selectable.
### 6. White Balance

**White Balance**

White balance (WB) tells the camera what the color white looks like. Based on this information, the camera will then continue to display all colors correctly even when the color temperature of the scene changes such as from daylight to fluorescent lighting, for example.

Select one of the options:

- **AWB1:** Apply for small range of 2500 to 9500K, for simple environments.
- **Locked WB:** Locks the WB to the current environment color temperature.
- **Incandescent Lamp:** For use with incandescent lighting.
- **Warm Light Lamp:** For use where the indoor light is warm.
- **Natural Light:** For use with natural light.
- **Fluorescent Lamp:** For use where there are fluorescent lamps installed near the camera.

### 7. Image Enhancement

**Digital Noise Reduction**

Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance.

Options include: ON or OFF.

**Noise Reduction Level**

Set the level of noise reduction. Higher value has a stronger noise reduction. Default is 50.

### 8. Video Adjustment

**Mirror**

It mirrors the image so you can see it inverted. Left/Right, Up/Down, Center, and OFF are selectable. Default is OFF.

**Hallway View**

To make a complete use of the 16:9 aspect ratio, enable the rotate function when you use the camera in a narrow view scene.

During installing, turn the camera to 90 degrees or rotate the 3-axis lens to 90 degrees, and then set the rotate mode as On. You will get a normal view of the scene with 9:16 aspect ratio that ignores needless information such as the walls. Default is OFF.

**Video Standard**

50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

### 9. Other

**Local Output**

Select ON or OFF to enable or disable the BNC output. Default is ON.

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

### OSD (On Screen Display)

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

1. Click Configuration > Image > OSD Settings.

2. Check the **Display Name** box (1) to display the camera’s name on screen. You can modify the default name in the text box of **Camera Name**.

3. Check the **Display Date** box (2) to display the date/time on screen.

4. Check the **Display Week** box (3) to include the day of the week in the on-screen display.

5. In the **Camera Name** box (4), enter the camera name.

6. Select the time and date formats from the **Time format** and **Date format** list boxes (5).

7. Select a display mode for the camera from the **Display Mode** list box (6). Display modes include:
   - **Not transparent & Not Flashing**. The image is behind the text. This is default.
   - **Not transparent & Flashing**. The image is behind the text. The text flashes on and off.

8. Select the desired **OSD size** (7).

9. Select the desired font color (8).

10. Click **Save** to save changes.

**Note:**

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

2. When you enable motion detection, it is recommended not to select the flashing display option as overlay text may trigger a motion alarm.
Overlay text

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

Figure 7: Text overlay menu

To add on-screen text:
1. Click Configuration > Image > Text Overlay.
2. Check the text box for the first line of text.
3. Enter the text in the text box.
4. Use the mouse to click and drag the red text in the live view window to adjust the text overlay position.
5. Repeat steps 2 to 4 for each extra line of text, selecting the next string number.
6. Click Save to save changes.

Privacy masks

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

Note: There may be a small difference in size of the privacy mask area depending on whether local output or the web browser is used.
To add privacy mask area:
1. Click Configuration > Image > Privacy Mask.
2. Check Enable Privacy Mask.
3. Click Draw Area.
4. Click and drag the mouse in the live video window to draw the mask area.
   Note: You are allowed to draw up to four areas on the same image.
5. Click Stop Drawing to finish drawing, or click Clear All to clear all of the areas you set without saving them.
6. Click Save to save changes.

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.
Defining a motion detection alarm requires the following tasks:

1. **Area settings**: Define the on-screen area that can trigger a motion detection alarm and the detection sensitivity level.

2. **Arming schedule**: Define the schedule during which the system detects motion.

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

4. **Linkage**: Specify the method of response to the alarm.

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

**To set up motion detection as normal mode:**

1. Click **Configuration > Basic Event > Motion Detection**.

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

   **Note**: Select Disable for rules in local configuration menu if you don’t want the detected objected displayed with the rectangles.

3. Select **Normal** mode from the drop down menu.

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

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

6. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.
7. Click Edit to edit the arming schedule. See the picture below for the editing interface of the arming schedule.

![Editing Interface](image)

8. Choose the day and click 🔄 to set the detailed time period. You can copy the schedule to other days.

9. Click OK to save changes.

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

<table>
<thead>
<tr>
<th>Notify Alarm Recipient</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Email</td>
<td>Sends an email to a specified address when there is a motion detection alarm. <strong>Note:</strong> You must configure email settings before check this option. See “To set up the Email parameters:” on page 23. If you want to send the event snapshot together with the email, you should check the Attached Snapshot option.</td>
</tr>
</tbody>
</table>

| Upload Snapshot        | Capture the image when an alarm is triggered and upload the picture to NAS or FTP server. **Note:** If you want to upload the snapshot to NAS, you must configure NAS settings. If you want to upload the snapshot to FTP, you must configure the FTP settings. Please ensure that the Upload Type option is enabled. |

| Trigger Channel        | Triggers the recording to start in the camera. |
| Trigger Alarm Output   | Trigger external alarm outputs when an event occurs. **Note:** This option is only supported by cameras that support alarm output. |

11. Click Save to save changes.

When you choose Advanced mode, you can set different sensitivities and proportions on different areas. If you choose Auto-Switch or Schedule-Switch, you can also set different settings for day and night or different periods.
To set up motion detection as advanced mode:

1. Click Configuration > Basic Event > Motion Detection.

2. Check the Enable Motion Detection box. Check Enable Dynamic Analysis for Motion if you want to see where has motion real-time.

   **Note:** Select Disable for rules in local configuration menu if you don’t want the detected objected displayed with the rectangles.

3. Select Advanced mode from the drop down menu.

4. Select OFF, Auto-switch or Scheduled-switch.

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

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

7. Move the Sensitivity and Proportion of Object on Area slider to set the sensitivity and proportion of the detection for different areas.

8. Click Edit to edit the arming schedule. See the picture below for the editing interface of the arming schedule.

![Edit Schedule Time](image)

9. Choose the day and click [ ] to set the detailed time period. You can copy the schedule to other days.

10. Click OK to save changes.

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

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify Alarm Recipient</td>
<td>Send an exception or alarm signal to remote management software when an event occurs.</td>
</tr>
<tr>
<td>Send Email</td>
<td>Sends an email to a specified address when there is a motion detection alarm.</td>
</tr>
<tr>
<td>Upload Snapshot</td>
<td>Capture the image when an alarm is triggered and upload the picture to NAS or FTP server.</td>
</tr>
<tr>
<td>Trigger Channel</td>
<td>Triggers the recording to start in the camera.</td>
</tr>
</tbody>
</table>
Trigger Alarm Output  
Trigger external alarm outputs when an event occurs.  
Note: This option is only supported by cameras that support alarm output.

12. Click Save to save changes.

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

To set up tamper-proof alarms:
1. Click Configuration > Basic Event > Tamper-proof.
2. Check the Enable Tamper-proof box (1).
3. Move the Sensitivity slider (2) to set the sensitivity of the detection. All areas will have the same sensitivity level.
4. Click Edit to edit the arming schedule for tamper-proof alarms. The arming schedule configuration is the same as that for motion detection. See “To set up motion detection” for more information.
5. Check the check box to select the linkage method taken for the tamper-proof.
6. Click Save to save changes.

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

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

Figure 10: Exception menu

To define exception alarms:

1. Click **Configuration > Basic Event > Exception**.
2. Under **Notification Type**, select an exception alarm type from the drop-down list.
3. Check the check box to select the linkage method.
4. Click **Save** to save changes.
Alarm inputs and outputs

To define the external alarm input:

1. Click Configuration > Basic Event > Alarm Input.

2. Choose the Alarm Input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed). Enter a name for the alarm input.

3. Click Edit to set the arming schedule for the alarm input. See “Motion detection alarms” on page 35 for more information.

4. Check the desired check box to select the linkage method.

5. Click Save to save changes.
To define the alarm output:

1. Click Configuration > Basic Event > Alarm Output.

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

3. The delay time can be set to 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.

4. Click Edit to set the arming schedule for the alarm input. See “Motion detection alarms” on page 35 for more information.

5. 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. The line crossing direction can be set as bi-directional, for example, from left to right or from right to left. A series of linkage methods can also be triggered if an object crossing the line is detected.

Figure 11: Cross line menu

To define Cross Line Detection:
1. Click Configuration > Smart Event > Cross Line.
2. Check the Enable Cross Line check box to enable the function.
3. Click Draw Area. A crossing plane appears on the image.
4. Click on the line. Two red squares appear at each end of the line. Drag one of the red squares to define the arming area.
   Select the direction as A<->B, A->B, or B->A from the drop down menu.
   **A<->B:** Only the arrow on the B side is displayed. When an object crosses the plane in both directions, it is detected and alarms are triggered.
   **A->B:** Only an object crossing the configured line from the A side to the B side can be detected.
   **B->A:** Only the object crossing the configured line from the B side to the A side can be detected.
5. Set the sensitivity [1 to 100].
6. Click Edit to set the arming schedule for the alarm input. See “Motion detection alarms” on page 35 for more information.

7. Configure the linkage action.

8. Click Save to save changes.
Intrusion detection

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

Figure 12: Intrusion Detection menu

To define intrusion detection:

1. Click Configuration > Smart Event > Intrusion Detection.
2. Check the Enable Intrusion Detection check box to enable the function.
3. Click Draw Area, and then draw a rectangle on the image as a defense region. When you draw the rectangle, all lines should connect end-to-end to each other. Up to four areas are supported. You can click Clear to clear the areas you have drawn. The defense region parameters can be set up separately.
4. Configure the settings of threshold, sensitivity.

   **Threshold:** Range [0 to 10 s]. This is the time threshold of the object to loiter in the region. If you set the value as 0, an alarm is triggered immediately when the object enters the region.

   **Sensitivity:** Range [1 to 100]. The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, a small object can trigger the alarm.

   **Percentage:** Range [1 to 100]. This defines the ratio of the in-region part of the object that can trigger an alarm. For example, when you set the percentage to 50%, half of the object entering the region will trigger the alarm.
5. Click Edit to set the arming schedule for the alarm input. See “Motion detection alarms” on page 35 for more information.

6. Configure the linkage action.

7. Click Save to save changes.

Snapshot parameters

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

You can set up the format, resolution and quality of the snapshots. The quality can be below, 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. Click Configuration > Storage > Snapshot.
2. Check Enable Timing Snapshot to enable continuous snapshots.
3. Select the desired format of the snapshot, such as JPEG.
4. Select the desired resolution of the snapshot.
5. Select the desired quality of the snapshot: High, Medium, or Low.
6. Enter the time interval between two snapshots. Select the unit of time from the dropdown list: milliseconds, seconds, minutes, hour, or day.
7. Set the schedule for when you want snapshots to be taken. Click Edit and the desired schedule for each day of the week.
8. Click Save to save changes.
To set up event-triggered snapshots:

1. Click Configuration > Storage > Snapshot.

2. Check Enable Timing Snapshot to enable continuous snapshots.

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

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

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

6. Click Save to save changes.

NAS settings

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

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

Notes:

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

Figure 14: NAS menu
To set up a NAS system:
1. Click Configuration > Storage > NAS.
2. Enter the IP address of the network disk, and the NAS file path.
3. Click Save to save changes.

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

Before formatting the storage device, stop all recording. Once formatting is completed, reboot the camera 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 Number column to select the storage.
3. Define the quota percentage for snapshots and recordings, modify the values for each in Percentage of Snapshot and Percentage of Record.
4. Click Format. A window appears to check your formatting permission.
5. Click OK to start formatting.

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

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

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

To set up a recording schedule:
1. Click Configuration > Storage > Record Schedule.

2. Click the Enable Record Schedule box to enable recording.
   Note: To disable recording, deselect the option.

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

**All Day recording**: Select one of the record types to record from the drop-down list box:

- **Normal**: This is continuous recording.
- **Motion Detection**: The video is recorded when the motion is detected.
- **Alarm**: The video is recorded when the alarm is triggered via the external alarm input.
- **Motion | Alarm**: The video is recorded when the external alarm is triggered or the motion is detected.
- **Motion & Alarm**: The video is recorded when motion and alarms are triggered at the same time.
- **Cross Line**: Video is recorded when the pre-defined line on-screen is crossed.
- **Intrusion Detection**: Video is recorded when an intrusion is detected.

- Or -

**Customize recording**: Click the day of the week required and then for period 1 set the start and end times during which you want the camera to begin and end recording. From the drop-down list box, select one of the record types to record. Repeat for additional periods in the day. Up to four time periods can be selected.

**Note**: The eight time periods cannot overlap.
Set the customized recording periods for the other days of the week, if required. Click Copy to copy the recording periods to another day of the week.

5. Click OK and Save to save changes.

**Note:** If you set the record type to “Motion detection”, “Alarm”, “Cross Line” or “Intrusion Detection” you must also define the arming schedule in order to trigger the recording.
Camera management

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

User management

This section describes how to manage users. You can:

- Add or delete users
- Modify permission
- Modify passwords

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

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

Figure 15: User management window

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

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

Types of users

A user’s access privileges to the system are automatically defined by their user type. There are three types of user:
• **Admin**: This is the system administrator. The administrator can configure all settings. Only the administrator can create and delete user accounts. Admin cannot be deleted.

• **Operator**: This user can only change the configuration of his/her own account. An operator cannot create or delete other users.

• **Viewer**: This user has the permission to live view, play back and search logs. However, Viewers cannot change any configuration settings.

Add and delete users

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

**To add a user:**

1. Click the User folder to open its window.
2. Select the Add button. The user management window appears.

3. Enter a user name. The name can have up to 16 alphanumeric characters.
4. Assign the user a password. Passwords can have up to 16 alphanumeric characters.

**Note**: We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

5. Select the type of user from the drop-down list. The options are Viewer and Operator.
6. Assign permissions to users. The options are:

<table>
<thead>
<tr>
<th>Basic Permission</th>
<th>Camera Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote: Parameters Settings</td>
<td>Remote: Live View</td>
</tr>
</tbody>
</table>

TruVision 11/31 Series IP Camera FW 5.2 Configuration Manual
Basic Permission | Camera Configuration
---|---
Remote: Log Search/Interrogate Working Status | Remote: PTZ Control
Remote: Upgrade/Format | Remote: Manual Record
Remote: Bidirectional Audio | Remote: Playback
Remote: Shutdown / Reboot | Remote: Video Output Control
Remote: Notify Alarm Recipient / Trigger Alarm Output | Remote: Serial Port Control
Remote: Video Output Control | Remote: PTZ Control
Remote: Serial Port Control | Remote: Manual Record
Remote: PTZ Control | Remote: Video Output Control
Remote: Manual Record | Remote: Serial Port Control
Remote: Playback | Remote: PTZ Control
Remote: Video Output Control | Remote: Manual Record
Remote: Serial Port Control | Remote: Playback

7. Click OK to save the settings.

To delete a user:
1. Select one user in 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 one user in the User tab.
2. Click the Modify button. The user management window appears
3. Change the information required.
   
**Note:** The user “Admin” can only be changed by entering the admin password.
4. Click Save to save the changes.

RTSP authentication
You can specifically secure the stream data of live view.
To define RTSP authentication:

1. Click Configuration > Storage > RTSP Authentication.

2. Under “RTSP Authentication”, select Enable or Disable in the drop-down list to enable or disable the RTSP authentication.

3. Click Save to save the changes.

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

**IP address filter**

This function makes access control possible.

Figure 16: IP address filter window

To define IP Address Filter:

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

Defining the security service
The camera provides a security service by allowing you to enable remote login and to improve data communication security.

Figure 17: Enable Telnet window

To define Telnet:
2. Check the Enable Telnet check box.
3. Click Save to save the changes.

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

To define SSH:
2. Check the Enable SSH check box.
3. Click Save to save the changes.

To enable the illegal login lock:
2. Check the Enable Illegal Login Lock check box
3. Click Save to save the changes.

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

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. 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 a camera, or if you want to make a backup of the settings.

To import/export configuration file:
1. Click Configuration > System > Maintenance.
2. Click Browse to select the local configuration file and then click Import to start importing configuration file.
3. Click Export and set the saving path to save the configuration file.

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

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

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

To upgrade firmware version:
1. Download on to your computer the latest firmware from our web site at:
   - Or -
   www.utcfssecurityproductspages.eu/videoupgrades/
2. When the firmware file is downloaded to your computer, extract the file to the desired destination.
   **Note:** Do not save the file on your desktop.
3. Click Configuration > System > Maintenance.
4. Select the Firmware or Firmware Directory option. Then click the Browse button to locate latest firmware file on your computer.
• **Firmware directory** – Locate the upgrading folder of Firmware files. The camera will choose the corresponding firmware file automatically.

• **Firmware** – Locate the firmware file manually for the camera.

  **Note:** Please select Interlogix_Gen_3_ipc.dav for product models listed in “Introduction” on page 3.

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

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

### Reboot camera

The camera can be easily rebooted remotely.

**To reboot the camera through the web browser:**

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

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

Logging on and off

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

Figure 18: Login dialog box

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

Live view mode

Once logged in, click “Live View” on the menu toolbar to access live view mode. See Figure 1 on page 8 for the description of the interface.

- **Start/stop live view:** You can stop and start live view by clicking the Start/stop live view button on the bottom of the window.
- **Record:** You can record live video and stored it in the directory you have configured. In the live view window, click the Record button at the bottom of the window. To stop recording, click the button again.
Take a snapshot: You can take a snapshot of a scene when in live view. Simply click the Capture button located at the bottom of the window to save an image. The image is in JPEG format. Snapshots are saved on the hard drive.

Playing back recorded video

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

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

To search recorded video stored on the camera’s storage device for playback, click Playback on the menu toolbar. The Playback window appears. See Figure 19.

Figure 19: Playback window

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Playback button</td>
<td>Click to open the Playback window.</td>
</tr>
<tr>
<td>2. Search calendar</td>
<td>Click the day required to search.</td>
</tr>
<tr>
<td>3. Search</td>
<td>Start search.</td>
</tr>
<tr>
<td>4. Set playback time</td>
<td>Input the time and click ▶️ to locate the playback point.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5. Control playback</td>
<td>Click to control how the selected file is played back: play, stop, slow and fast forward playback.</td>
</tr>
<tr>
<td>6. Timeline bar</td>
<td>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 playback. Click  to zoom out/in the timeline bar.</td>
</tr>
<tr>
<td>7. Time moment</td>
<td>Vertical bar shows where you are in the playback recording. The current time and date are also displayed.</td>
</tr>
<tr>
<td>8. Download functions</td>
<td>Download video files.</td>
</tr>
<tr>
<td></td>
<td>Download captured images.</td>
</tr>
<tr>
<td>9. Recording type</td>
<td>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.</td>
</tr>
<tr>
<td>10. Archive functions</td>
<td>Click these buttons for the following archive actions:</td>
</tr>
<tr>
<td></td>
<td>Capture a snapshot image of the playback video.</td>
</tr>
<tr>
<td></td>
<td>Start/Stop clipping video files.</td>
</tr>
</tbody>
</table>

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 55 to archive recorded video files.

3. Select the date and click the Search button to search for the required recorded file.

4. Click  to search the video file.

5. In the pop-up window, check the box of the video file and click Download to download the video files.

To archive a recorded video segment during playback:

1. While playing back a recorded file, click  to start clipping. Click it again to stop clipping. A video segment is created.

2. Repeat step 1 to create additional segments. The video segments are saved on your computer.
To archive recorded snapshots:

1. Click 📸 to open the snapshots search window.

2. Select the snapshot type as well as the start and end time.

3. Click Search to search for the snapshots.

4. Select the desired snapshots, and click Download to download them.

Searching event logs

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

The number of event logs that can be stored on NAS or SD card depends on the capacity of the storage devices. When this capacity is reached, the system starts deleting older logs. To view logs stored on storage devices, click Log on the menu toolbar. The Log window appears. See Figure 20 on page 65.

Note: You must have view log access rights to search and view logs. See “Modify user information” on page 55 for more information.
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 7 below for their descriptions.

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

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

### Table 7: Types of logs

<table>
<thead>
<tr>
<th>Log type</th>
<th>Description of events included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Alarm Input, Alarm output, Start Motion Detection, Stop Motion Detection, Start Tamper-proof, Stop Tamper-proof, Cross Line Detection Started, Cross Line Detection Stopped, Intrusion Detection Started, Intrusion Detection stopped</td>
</tr>
<tr>
<td>Exception</td>
<td>Invalid Login, HDD Full, HDD Error, Network Disconnected and IP Address Conflicted</td>
</tr>
<tr>
<td>Log type</td>
<td>Description of events included</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------</td>
</tr>
</tbody>
</table>

**To search logs:**

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

A
Alarm inputs
set up, 41
Alarm outputs
set up, 41
Alarm types
motion detection, 35
Archived files
play back, 63
Archiving files
recorded files, 63
snapshots of recorded files, 63
Audio parameters, 27

B
Bit rate, 27

C
Camera image
configuring, 30
Camera name
display, 32
Configuration file
import/export, 59
Configuration settings, 10

D
Date format set up, 32
DDNS parameters
set up, 17
Default settings
restore, 58
Display information on screen set up, 32

E
Email parameters
set up, 23
Events
search logs, 64

F
Firmware upgrade, 59
Frame rate, 27
FTP parameters
set up, 20

H
HDD
capacity, 49
formatting, 49
HDD error alarm, 39
HDD full alarm, 39
Illegal login alarm, 39
IP address
finding IP address of a camera, 7
IP address conflicted alarm, 39
Live view
manual recording, 61
snapshots, 62
start/stop, 61
Live view parameters, 11
Local camera parameters, 11
Logging on and off, 61
Logs
information type, 65
search logs, 64
view logs, 64
Motion detection
configuring, 35
marking the detection areas, 36, 38

N
NAS settings, 48
Network, 39
Network settings
set up, 14
NTP synchronization, 12

P
Passwords
modify, 55
Playback
play back recorded files, 63
screen, 62
search recorded video, 62
Port parameters
set up, 17
Post-recording times
description, 50
PPPoE parameters
set up, 18
Pre-recording times
description, 50
Privacy masks, 34
Q
QoS parameters
   set up, 20

R
Reboot camera, 60
Record file settings, 11
Recording
   define recording schedule, 49
   manual recording, 61
   parameters, 27
   playback, 62
Resolution, 27
RTSP authentication, 55

S
SDHC card
   capacity, 49
   card full, 49
   formatting, 49
   free space available, 49
Snapshot and clip settings, 11
Snapshots
   archive snapshots from recorded files, 63
   save during live view mode, 62
   set up, 46
SNMP parameters
   set up, 19
System time
   set up, 12

T
Tamper-proof alarms
   set up, 39
TCP/IP settings
   set up, 16
Text
   add extra lines of text on screen, 34
Text display on screen
   appearance, 32
Time format set up, 32
TruVision Device Finder, 7

U
UPnP parameters
   set up, 21, 23
User settings, 53
Users
   adding new users, 54
   deleting a user, 55
   modify a password, 55
   modify computer ID, 55
   types of users, 53

V
Video parameters, 27
Video quality, 30

W
Web browser
   accessing the camera, 7
   overview of the interface, 7
Web browser security level
   checking, 5