Legal considerations

Laws that can vary from country to country may prohibit camera surveillance. Please ensure that the relevant laws are fully understood for the particular country or region in which you will be operating this equipment. IndigoVision Ltd. accepts no liability for improper or illegal use of this product.

Copyright

Copyright © IndigoVision Limited. All rights reserved.

This manual is protected by national and international copyright and other laws. Unauthorized storage, reproduction, transmission and/or distribution of this manual, or any part of it, may result in civil and/or criminal proceedings.

IndigoVision is a trademark of IndigoVision Limited and is registered in certain countries. IndigoUltra, IndigoPro, IndigoLite and CyberVigilant are registered trademarks of IndigoVision Limited. Camera Gateway, Integra and Mobile Center are unregistered trademarks of IndigoVision Limited. All other product names referred to in this manual are trademarks of their respective owners and CyberVigilant are registered trademarks of IndigoVision Limited. Camera Gateway, and Integra are unregistered trademarks of IndigoVision Limited. All other product names referred to in this manual are trademarks of their respective owners.

Save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., this manual is provided without express representation and/or warranty of any kind. To the fullest extent permitted by applicable laws, IndigoVision Limited and IndigoVision, Inc. disclaim all implied representations, warranties, conditions and/or obligations of every kind in respect of this manual. Accordingly, save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., this manual is provided on an "as is", "with all faults" and "as available" basis. Please contact IndigoVision Limited (either by post or by e-mail at technical.support@indigovision.com) with any suggested corrections and/or improvements to this manual.

Save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., the liability of IndigoVision Limited and IndigoVision, Inc. for any loss (other than death or personal injury) arising as a result of any negligent act or omission by IndigoVision Limited and/or IndigoVision, Inc. in connection with this manual and/or as a result of any use of or reliance on this manual is excluded to the fullest extent permitted by applicable laws.

Contact address

IndigoVision Limited
Charles Darwin House,
The Edinburgh Technopole,
Edinburgh,
EH26 0PY
Safety notices

This guide uses the following formats for safety notices:

**Warning**

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

**Caution**

Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.

**Notice**

Indicates a hazardous situation which, if not avoided, may seriously impair operations.

**Additional information relating to the current section.**
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal considerations</td>
<td>2</td>
</tr>
<tr>
<td>Copyright</td>
<td>2</td>
</tr>
<tr>
<td>Contact address</td>
<td>2</td>
</tr>
<tr>
<td>Safety notices</td>
<td>3</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>6</td>
</tr>
<tr>
<td>2 Accessing the camera</td>
<td>8</td>
</tr>
<tr>
<td>Requirements</td>
<td>8</td>
</tr>
<tr>
<td>Powering up the camera</td>
<td>8</td>
</tr>
<tr>
<td>Logging in</td>
<td>8</td>
</tr>
<tr>
<td>3 Initial camera configuration</td>
<td>10</td>
</tr>
<tr>
<td>Set new password</td>
<td>10</td>
</tr>
<tr>
<td>Create new users</td>
<td>10</td>
</tr>
<tr>
<td>Modify IP address and network settings</td>
<td>10</td>
</tr>
<tr>
<td>Modify date and time settings</td>
<td>11</td>
</tr>
<tr>
<td>Modify camera settings</td>
<td>11</td>
</tr>
<tr>
<td>Configure CyberVigilant</td>
<td>11</td>
</tr>
<tr>
<td>4 Configuring analytics</td>
<td>14</td>
</tr>
<tr>
<td>Enable motion detection</td>
<td>14</td>
</tr>
<tr>
<td>Enable audio detection</td>
<td>14</td>
</tr>
<tr>
<td>Enable fire warning alarm</td>
<td>15</td>
</tr>
<tr>
<td>Define analytics period</td>
<td>15</td>
</tr>
<tr>
<td>Define a detection area (region of interest)</td>
<td>16</td>
</tr>
<tr>
<td>Monitor objects entering or leaving an area</td>
<td>16</td>
</tr>
<tr>
<td>Configure an analytics rule</td>
<td>17</td>
</tr>
</tbody>
</table>

**BX620-400NT Thermal Bullet - Camera**
1 INTRODUCTION

This Web Configuration Guide contains information about configuring the BX620-400NT Thermal Bullet Camera using the Web Configuration pages. The guide covers accessing the camera, initial set up, and advanced configuration.
2 ACCESSING THE CAMERA

This section contains instructions on how to access the BX620-400NT Thermal Bullet Camera and log in to the Web configuration interface.

Requirements

The BX620-400NT Thermal Bullet Camera supports web configuration and management using a PC.

Before starting configuration, establish a network connection:

1. Ensure that the BX620-400NT Thermal Bullet Camera is correctly connected to the network.
2. Ensure that the BX620-400NT Thermal Bullet Camera IP address and the PC IP address are in the same network segment.
3. If there is a router, set the corresponding gateway and subnet mask.
4. Use the command ping <IP address> to check the connection.

Powering up the camera

The camera is a Power Over Ethernet (PoE) - Class 0 powered device compliant with the IEEE802.3af standard.

If PoE is not available the camera can be powered using auxiliary power.

The camera can be powered by the following:

- Power over Ethernet (PoE) switch
- PoE injector/midspan (Part Number 130176)
- Auxiliary power supply
  - 24V AC / 12V DC with a maximum power of 8 Watts

A suitable power supply must be ordered separately. The camera should only be powered with the specified voltage.

Logging in

1. In a standard web browser, navigate to the IP address for the camera.
   For example, if your device IP is 10.5.1.10, enter http://10.5.1.10 in the address bar.
   The Device initialization page is displayed.
2. On your first login, you must set the password for the Admin user according to the instructions provided.
An install dialog is also displayed with details for downloading and installing the NPAPI plugin webplugin.exe.

3. Click **OK** to install the control.
   
   If you cannot download the file, lower your browser security levels to enable download.
3  INITIAL CAMERA CONFIGURATION

This section contains information about the BX620-400NT Thermal Bullet Camera settings which must be configured before first use.

Set new password
When the BX620-400NT Thermal Bullet Camera is accessed for the first time using the Web configuration pages, the Device initialization screen is displayed allowing you to set a new Admin password.

For security reasons, it is important that you set a secure password.

► For more information, please refer to the Control Center Security Hardening Guide

1. Enter a new Admin password in the Password and Confirm Password fields shown, following the displayed password requirements.
   You can also use the password strength indicators shown to ensure that you create a high-strength password.

2. Click Save to complete the configuration.

Create new users
For security reasons, you should create additional users with the appropriate level of access required.

► For more information, please refer to the Control Center Security Hardening Guide

2. Enter a Username and Password for the new user, following the password requirements.
   Use the password strength indicators shown to ensure that you create a high-strength password.
3. In the Group Name dropdown, select the User group.
   Alternatively, under the Group Name tab, you can add a new group with the required permissions, and assign this to the new user.
4. Select the required Authority from the available group permissions for this user.
5. Click Save to complete the creation of the new user.

Modify IP address and network settings
By default, the BX620-400NT Thermal Bullet Camera uses DHCP to get an IP address on initial startup. Alternatively, you can statically configure the IP address and network settings to allow the camera to work on the required network.

Use the Web configuration pages to change the IP address and network settings.
1. Enter the following network configuration on the **Setup > Network > TCIP/IP** menu if required:
   - IP address
   - Subnet mask
   - Default gateway
   - DNS servers

**Modify date and time settings**

You can use the Web configuration pages to change the date and time settings on the camera.

1. Enter the following network configuration on the **Setup > System > General > Date&Time** menu if required:
   - NTP server
   - Port
   - Interval
   - DST Type
   - Start Time
   - End Time

**Modify camera settings**

After the camera has been installed in its final location, you need to adjust the image settings to ensure that you have the best quality picture.

Use the Web configuration pages to change the camera settings.

1. Select the video standard for your region using the **Video Standard** option on the **Setup > System > General** menu.
   - Choose **PAL** for countries with 50Hz power frequency and **NTSC** for countries with 60Hz power frequency.
   - Changing this option causes the camera to reboot.

2. Adjust the image settings to fit the scene using the options on the **Setup > Camera > Conditions** menu.
   - Choose a predefined **Profile** for **Day** or **Night** use, or adjust the required settings manually, for example:
     - **Brightness**
     - **Contrast**
     - Orientation - using the **Mirror** and/or **Flip** options

**Configure CyberVigilant**

You can use the Web configuration pages to configure the CyberVigilant settings on the camera if required:

1. Click **Network > CyberVigilant > Add IP/MAC**.
2. Enter the IP address, IP range or MAC address for the authorised device.
3. Click **Save**.
4. Click **Save** on the main page.
   The new CyberVigilant list entries are saved.
5. Select **Enable CyberVigilant**.
6. Click **Save**.
   CyberVigilant functionality is now enabled.
Initial camera configuration

BX620-400NT Thermal Bullet - Camera
The BX620-400NT Thermal Bullet Camera has video analytics capabilities. This section provides details about the capabilities available and how to configure them for common applications.

Enable motion detection

Motion detection monitors the scene for any motion. When motion is detected, the camera triggers an event that can be used to activate an alarm or trigger an action in Control Center.

Motion detection is configured on the Event > Video Detection > Motion Detection screen.

1. Select Enable to activate motion detection.
2. Configure the settings to suit your requirements:
   • **Period** defines when motion detection will be active.
     ▶ see "Define analytics period" on page 15
   • **Anti-dither** defines the time in seconds of 0 to 100, during which detected motion only results in a single activation.
   • **Area** defines in the scene where motion will be monitored.
     ▶ see "Define a detection area (region of interest)" on page 16
   • **Record** starts recording video to the local storage when motion is detected.
   • **Relay out** triggers the binary output when motion is detected.
   • **Send Email** sends an email to the configured email address when motion is detected.
   • **Snapshot** saves a snapshot to the local storage when motion is detected.

Enable audio detection

Audio detection monitors the audio inputs of the camera for abnormalities and changes in intensity. When these are detected, the camera triggers an event that can be used to activate an alarm or trigger an action in Control Center.

Audio detection is configured on the Event > Audio Detection screen.

1. Select **Input Abnormal** to activate detection of abnormal audio on the camera inputs.
2. Alternatively, select **Intensity Change** to activate detection of changes in audio intensity, and configure the settings to suit your requirements:
   • **Sensitivity** controls the effect of detected audio on the camera input level. Larger values increase the sensitivity.
   • **Threshold** determines the camera input level at which an event is triggered. Larger values raise the threshold for triggering events.
   • **Period** defines when audio detection will be active.
     ▶ see "Define analytics period" on page 15
Enable fire warning alarm

The BX620-400NT Thermal Bullet Camera is able to detect heat, and, therefore, identify when a fire has started. Use the fire warning alarm to trigger an event that can be used to activate an alarm or trigger an action in Control Center.

The Fire warning alarm is configured on the **Smart Thermal > Fire Warning** screen.

1. Select **On** to activate fire warning and select the **Mode**.
2. Define the **Region** of interest in the scene in which the camera will detect fire.
   - You can define up to 4 regions, each indicated in the preview image with a different color.
   - Select a region by clicking the colored square, then click and drag over the scene to define the region of interest.
   - Specify a **Name** for the region if required.
   - Adjust the **Sensitivity** slider for the region.
3. Expand the **Alarm** section to configure the Alarm options:
   - **Period** defines when motion detection will be active.
     - see "Define analytics period" on page 15
   - **Anti-dither** defines the time in seconds of 0 to 100, during which detected motion only results in a single activation.
   - **Record** starts recording video to the local storage when motion is detected.
   - **Relay out** triggers the binary output when motion is detected.
   - **Send Email** sends an email to the configured email address when motion is detected.
   - **Snapshot** saves a snapshot to the local storage when motion is detected.

You can also use the **Smart Thermal > Hot Trace** screen to view the hottest and coldest point in the scene in case of fire. Select **On** to activate Hot Trace, and configure the required **Color Mode**.

Define analytics period

The analytics period is a schedule that defines the times that an analytics rule is active. You can define a up to six periods for each day.

Configure the active periods using the visual display.

1. Click the Period **Setup** button on the appropriate analytics rule page, for example, Motion Detection. The **Period** dialog opens.
   - The green bars indicate the active periods for each day of the week.
2. Click **Set** next to the day you want to configure the active periods.
The day being configured is highlighted in red and the check box for that day is automatically selected below the display.

- Select additional check boxes or All below the display to configure the same active periods for several days.

3. Click a green bar for that day to remove it, or click and drag in the area below the bar to add an active period.
   As you configure the active periods, they are reflected in the entry fields below the display.
4. Click Save to apply any changes you have made, or Cancel to cancel the changes.
5. On return to the main Analytics page, click Save to save the settings.

Define a detection area (region of interest)
The detection area, or region of interest, is the part of the camera scene that is analyzed for activity.

1. Click Setup on the appropriate analytics rule page, for example, Motion Detection, to configure the detection area.
   You can configure 4 regions, each indicated in the preview image with a different color.
2. Click a colored square to select a region to configure.
3. Specify a Name for the region if required, and adjust the Sensitivity and Threshold sliders for the region.
4. Click and drag on the preview image to configure the region.
   Click and drag within an already selected region to deselect that part of the region.
5. Click Save to apply any changes you have made, or click Cancel to cancel the changes.
6. On return to the main Analytics page, click Save to save the settings.

Monitor objects entering or leaving an area
The analytics rules of the camera can be used to identify when a person or object enters or leaves an area. This is can be used for both security and safety purposes, for example, a person crossing from a train platform on to the train tracks, or a person entering a restricted area.

The device supports the following analytics rule types:

- **Tripwire**
  Tripwire triggers an event when a defined line in a scene is crossed in one direction, or both directions.
  This can be used to identify when a person or object performs a dangerous maneuver, for example, crossing to the wrong side of a highway.

- **Intrusion**
  Intrusion triggers an event when a person or object enters or leaves the defined area, such as crossing the boundary.
  This can be used to identify when a person or object enters a dangerous area, for example, the area where heavy machinery is operating.

- **Abandoned Object**
  Abandoned Object triggers an event when a person or object enters and remains left in the detection area for longer than a defined period of time.
This can be used to identify when a car has stopped in a restricted area, or if a vehicle has broken down on a road.

- **Missing Object**
  Missing Object triggers an event when an object is removed from the detection area for longer than a defined period of time.
  This can be used to identify when something has been stolen, a painting for example, or if a door has been left open.

### Configure an analytics rule

Analytics rules are configured on the **Event > Analytics > Rules based** screen.

You can configure up to ten analytics rules.

1. Enable rules-based analytics by selecting the icon on the **Event Analytics** page.
   When enabled, the icon is highlighted in a light blue color. When disabled, the icon appears in a gray background color.
2. Click to add a new rule. A new rule is added to the list and selected.
3. Select the **Rule Type** you required.
   - see “Monitor objects entering or leaving an area” on page 16
4. Define the region of interest for the rule on the camera scene.
   - Click **Draw** and click on the scene to start drawing
   - Move the cursor and continue to click to add points on the line
   - Right-click to complete the line or area
5. Configure the **Period** when the rule will be active.
   - see “Define analytics period” on page 15
6. Configure the parameters for the rule.
7. Click **Save**.