IndigoVision

HD Ultra Range Camera

Web Configuration Guide

IndigoVision

THIS MANUAL WAS CREATED ON WEDNESDAY, FEBRUARY 20, 2019.

DOCUMENT ID: IU-CAM-MAN006-2

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

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

1 INTRODUCTION

This Web Configuration Guide contains information about configuring the HD Ultra Range cameras using the Web Configuration pages.

The guide covers accessing the camera, initial set up, and advanced configuration.

Cameras

This guide covers the following cameras:

- HD Ultra Bullet
- HD Ultra Minidome

2 ACCESSING THE CAMERA

This section contains instructions on how to access the HD Ultra Range cameras and log in to the Web configuration interface.

Requirements

The HD Ultra Range cameras support web configuration and management using a PC.

Before starting configuration, establish a network connection:

1. Ensure that the HD Ultra Range cameras are correctly connected to the network.
2. Ensure that the HD Ultra Range cameras 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.

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.

   For more information, *see "Set new password" on page 10*
3. Enter login and password on the **Login** page.

   The **Version** page is displayed.
4. Navigate to the **Live** page.

   An install dialog is displayed with details for downloading and installing the NPAPI plugin `webplugin.exe`.
5. 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 HD Ultra Range cameras settings which must be configured before first use.

Set new password

When the HD Ultra Range cameras are 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*

1. On the ***Setup > System > Account > Username*** screen, click ***Add User***.
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 date and time settings

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

To enable DST or NTP, check the appropriate checkbox and click ***Save***.

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 IP address and network settings

By default, the HD Ultra Range cameras use 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

Caution *Control Center requires that the IP address for a device in a site remains fixed. If the DHCP server has been configured to lease addresses from an address pool, rather than based on MAC address, the device will not work correctly with Control Center.*

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.

Notice *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**

Configure CyberVigilant

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

1. Click ***Setup > 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.

Caution

When specifying which PCs may access the device, make sure that you enter the address of the PC being used to configure the device before enabling IP address restrictions, otherwise your own access will be prevented.

4 CONFIGURING ANALYTICS

The HD Ultra Range cameras have video analytics capabilities. This section provides details about the capabilities available and how to configure them for common aplications.

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 ***Setup > 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 16*
   - **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 video tampering

Video tampering monitors the video input of the camera for any changes from what is typically seen by the camera. If any tampering or changes to the image are detected, the camera triggers an event that can be used to activate an alarm or trigger an action in Control Center.

Video tampering is configured on the ***Setup > Event > Video Detection > Video Tampering*** screen.

1. Select **Defocus Detect** to activate detection of the changes to the camera focus.
1. Alternatively, select **Video Tampering** to activate detection when there is a sudden change to the camera input.

   Video Loss is selected by default to activate detection when the video input is lost.
2. Configure the settings to suit your requirements:
   - ***Period*** defines when video tamper detection will be active.
   - ► *see "Define analytics period" on page 16*

- **Record** starts recording video to the local storage when video tamper is detected.
- **Relay out** triggers the binary output when video tamper is detected.
- **Send Email** sends an email to the configured email address when video tamper is detected.
- **Snapshot** saves a snapshot to the local storage when video tamper is detected.

Enable scene changing

Scene changing monitors the camera input and if there are any changes to the expected scene, the camera triggers an event that can be used to activate an alarm or trigger an action in Control Center.

Scene changing is configured on the ***Setup > Event > Video Detection > Scene Changing*** screen.

1. Select **Scene Change** to activate detection of changes to the current scene on the camera video input. When selected the following scene changes are also enabled:
   - ***Scene Occlusion*** triggers when a large portion of the scene is blocked off, hidden or undergoes a significant change in content. For example, the camera has been covered with spray paint or a hand covering the lens.

     For larger locations, scene occlusion could be a large object, close to the camera, blocking the view to most of the scene.
   - ***Field Of View Change*** detects if the camera has moved and no longer covers the original view area. This can happen, for example, if the camera is moved from its original position.
   - ***Bad Exposure Detect*** detects if the camera exposure changes to a point that prevents a clear image. This can happen, for example, from a reflection of direct sunlight.
2. Configure the settings to suit your requirements:
   - ***Period*** defines when scene change detection will be active.
   - ► *see "Define analytics period" on page 16*
   - **Record** starts recording video to the local storage when scene change is detected.
   - **Relay out** triggers the binary output when scene change is detected.
   - **Send Email** sends an email to the configured email address when scene change is detected.
   - **Snapshot** saves a snapshot to the local storage when scene change 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 ***Setup > 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 16*

- **Anti-dither** defines the time in seconds of `0` to `100`, during which audio abnormalities or changes only result in a single activation.
- **Record** starts recording video to the local storage when audio abnormalities or changes are detected.
- **Relay out** triggers the binary output when audio abnormalities or changes are detected.
- **Send Email** sends an email to the configured email address when audio abnormalities or changes are detected.
- **Snapshot** saves a snapshot to the local storage when audio abnormalities or changes are detected.

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 ***Setup > Event > Analytics > Rules based*** screen.

You can configure up to ten analytics rules.

1. Enable rules-based analytics by selecting the icon on the ***Setup > 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. On the ***Rules-based*** page click to add a new rule. A new rule is added to the list and selected.
3. Select the ***Rule Type*** as required.

   ► *see "Monitor objects entering or leaving an area" on page 17*
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 16*
6. Configure the parameters for the rule.
7. Click ***Save***.

Using ACF rate control

Using Activity Controlled Frame-rate (ACF) rate control allows video to be transmitted at a reduced frame rate when no **Event** is active, saving bandwidth, and recording disk space.

ACF requires **Rate Control** settings to be configured and an appropriate **Event** to be enabled.

Enable ACF

ACF is configured on the ***Setup > Camera > Video*** screen.

To enable and configure ACF:

1. Set **ACF** to ***On***.
   A warning dialog is displayed:
   `For ACF to operate, a Rate Control entry and related trigger Event should be configured and enabled.`
   This enables additional **Rate Control** entries: **ACF-Motion** and **ACF-Alarm**.
2. Click ***Save***.
3. Configure **General Rate Control** entry settings required for inactive periods, for example, reduced **Frame Rate** or **Bit Rate**, adjusted **Bit Rate Type** or **I-Frame Interval**.
4. Click ***Save***.
5. Configure **ACF-Motion Rate Control** entry settings required for **Analytics**-triggered active periods, for example, increased **Frame Rate** or **Bit Rate**, adjusted **Bit Rate Type** or **I-Frame Interval**.
6. Click ***Save***.
7. Configure **ACF-Alarm Rate Control** entry settings required for **Alarm**-triggered active periods, for example, increased **Frame Rate** or **Bit Rate**, adjusted **Bit Rate Type** or **I-Frame Interval**.
8. Click ***Save***.

ACF activation and duration

Activated **Analytic Events** will switch the camera to the **ACF-Motion** mode.

Activated **Alarm Events** will switch the camera to the **ACF-Alarm** mode.

The camera will then run in the ACF mode for the following times:

- The **Anti-Dither** time where available (e.g. **Digital Input Alarm**, **Motion Detection**, **Audio Intensity Change**)
- 120 s for other events

Encode Mode and **Resolution** are not supported for ACF. All **Rate Control** types will use the same values (from the **General** setting).

Priority varies according to the type of **Event**, which are supported in the following order, highest first:

1. **Digital Input Alarm**
2. **Motion Detection**
3. **Advanced Analytics** or **Tamper** or **Scene Change**