PLEASE READ THIS MANUAL BEFORE USING YOUR CAMERAS, and always follow the instructions for safety and proper use. Save this manual for future reference.
CAUTION

FCC Caution: To assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

NOTE

This equipment has been tested and found to comply with the limits for a Class “A” digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

LEGAL NOTICE

Observint Technologies (Observint) products are designed to meet safety and performance standards with the use of specific Observint authorized accessories. Observint disclaims liability associated with the use of non-Observint authorized accessories.

The recording, transmission, or broadcast of any person’s voice without their consent or a court order is strictly prohibited by law.

Observint makes no representations concerning the legality of certain product applications such as the making, transmission, or recording of video and/or audio signals of others without their knowledge and/or consent. We encourage you to check and comply with all applicable local, state, and federal laws and regulations before engaging in any form of surveillance or any transmission of radio frequencies.

Alibi and the Alibi logo are trademarks of Observint.

Microsoft, Windows, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Android is a trademark of Google Inc. Use of this trademark is subject to Google Permissions. Apple, iPhone, iPod touch, and iPad are registered trademarks of Apple Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Observint disclaims any proprietary interest in trademarks and trade names other than its own.

No part of this document may be reproduced or distributed in any form or by any means without the express written permission of Observint, Inc.

© 2014, 2015 by Observint Technologies. All Rights Reserved.
11000 N. Mopac Expressway, Building 300, Austin, TX 78759
For Sales and Support, contact your distributor.
Regulatory information

FCC information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Preventive and Cautionary Tips

Before connecting and operating your cameras, please be advised of the following:

- Ensure environmental conditions meet factory specifications.
- Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an Uninterruptible Power Supply (UPS) if possible.

Safety Instructions

Read these instructions and keep them in a safe place for future reference.

- Please refer all work related to the installation of this product to qualified service personnel or system installers.
- Do not operate the appliance outside of its specified temperature, humidity or power source ratings.
- Install the unit away from heat sources such as radiators, heat registers and stoves.
- Installation of the unit near consumer electronics devices, such as stereo receiver/amplifiers and televisions, is permitted as long as the air surrounding the terminal does not exceed the above mentioned temperature range.
- Handle the camera with care. Do not drop or shake, as this may damage it.
- Do not use strong or abrasive detergents when cleaning the surfaces of this product. When dirt is hard to remove, use a mild detergent and wipe gently.
- Save your system configuration.
- Distributing, copying, disassembling, reverse compiling, reverse engineering, and exporting, in violation of export laws, the software provided with this product is expressly prohibited.
# Table of Contents

## SECTION 1 Overview

1. Typical application configurations ................................................................. i
  1.1 Camera is managed by an NVR or Network DVR ........................................... 1
  1.1.1 Camera is managed by a VMS ................................................................. 3
  1.2 PC requirements ........................................................................................... 3

## SECTION 2 Network Connection

2. Locating cameras on the network with Alibi Power Tools .................................. 4
  2.1.1 Restore Default Password ........................................................................ 7

## SECTION 3 Remote Access

3. Remote login .................................................................................................... 8
  3.2 Remote Live View screen .............................................................................. 11
    3.2.1 Remote Live View screen - ALI-IPV5060RP Fisheye camera ................. 13
  3.3 Playback screen ............................................................................................ 14
  3.4 Remote Log screen ........................................................................................ 18
  3.5 Remote SETUP screen ................................................................................... 19
    3.5.1 Local Setup menu .................................................................................. 19
    3.5.2 Camera Setup menus .............................................................................. 20

## SECTION 4 Camera Setup Menus

4. System Setup menus ....................................................................................... 21
  4.1 Device Information ......................................................................................... 22
  4.1.1 Time Settings .......................................................................................... 22
  4.1.3 Maintenance ............................................................................................. 24
  4.1.4 RS485 ...................................................................................................... 26
  4.1.5 DST (Daylight Savings Time) .................................................................. 26
  4.1.6 Service ...................................................................................................... 27
  4.1.7 Fisheye Parameters (ALI-IPV5060RP camera only) ............................... 28
  4.2 Network menus ............................................................................................ 28
    4.2.1 TCP/IP .................................................................................................. 28
    4.2.2 Port ...................................................................................................... 29
    4.2.3 DDNS .................................................................................................... 30
    4.2.4 SNMP ................................................................................................... 33
    4.2.5 802.1X ................................................................................................. 34
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.6</td>
<td>QoS</td>
<td>34</td>
</tr>
<tr>
<td>4.2.7</td>
<td>FTP</td>
<td>35</td>
</tr>
<tr>
<td>4.2.8</td>
<td>UPnP™</td>
<td>36</td>
</tr>
<tr>
<td>4.2.9</td>
<td>Email</td>
<td>37</td>
</tr>
<tr>
<td>4.2.10</td>
<td>NAT</td>
<td>38</td>
</tr>
<tr>
<td>4.2.11</td>
<td>HTTPS</td>
<td>38</td>
</tr>
<tr>
<td>4.3</td>
<td>Video/Audio menus</td>
<td>40</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Video</td>
<td>40</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Audio</td>
<td>42</td>
</tr>
<tr>
<td>4.3.3</td>
<td>ROI</td>
<td>42</td>
</tr>
<tr>
<td>4.3.4</td>
<td>Display Info. on Stream</td>
<td>44</td>
</tr>
<tr>
<td>4.4</td>
<td>PTZ menus</td>
<td>44</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Basic menu</td>
<td>44</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Limit menu</td>
<td>46</td>
</tr>
<tr>
<td>4.4.3</td>
<td>Initial Position menu</td>
<td>47</td>
</tr>
<tr>
<td>4.4.4</td>
<td>Park Action menu</td>
<td>47</td>
</tr>
<tr>
<td>4.4.5</td>
<td>Privacy Mask menu</td>
<td>48</td>
</tr>
<tr>
<td>4.4.6</td>
<td>Scheduled Tasks menu</td>
<td>49</td>
</tr>
<tr>
<td>4.4.7</td>
<td>Clear Config menu</td>
<td>51</td>
</tr>
<tr>
<td>4.4.8</td>
<td>Smart Tracking menu</td>
<td>52</td>
</tr>
<tr>
<td>4.4.9</td>
<td>Prioritize PTZ menu</td>
<td>52</td>
</tr>
<tr>
<td>4.5</td>
<td>Image menus</td>
<td>53</td>
</tr>
<tr>
<td>4.5.1</td>
<td>Display Settings</td>
<td>53</td>
</tr>
<tr>
<td>4.5.2</td>
<td>OSD Settings</td>
<td>55</td>
</tr>
<tr>
<td>4.5.3</td>
<td>Text Overlay</td>
<td>56</td>
</tr>
<tr>
<td>4.5.4</td>
<td>Privacy Mask</td>
<td>57</td>
</tr>
<tr>
<td>4.6</td>
<td>Security menus</td>
<td>58</td>
</tr>
<tr>
<td>4.6.1</td>
<td>User</td>
<td>58</td>
</tr>
<tr>
<td>4.6.2</td>
<td>(RTSP) Authentication</td>
<td>60</td>
</tr>
<tr>
<td>4.6.3</td>
<td>Anonymous Visit</td>
<td>60</td>
</tr>
<tr>
<td>4.6.4</td>
<td>IP Address Filter</td>
<td>61</td>
</tr>
<tr>
<td>4.6.5</td>
<td>Security Service</td>
<td>63</td>
</tr>
<tr>
<td>4.7</td>
<td>Standard Events menus</td>
<td>63</td>
</tr>
<tr>
<td>4.7.1</td>
<td>Motion Detection</td>
<td>63</td>
</tr>
<tr>
<td>4.7.2</td>
<td>Video Tampering</td>
<td>66</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

| 4.7.3 Alarm Input | ................................................................. | 69 |
| 4.7.4 Alarm Output | ............................................................. | 72 |
| 4.7.5 Exception | ................................................................ | 74 |
| 4.8 VCA Event | ................................................................... | 75 |
| 4.8.1 Audio Exception Detection | ............................................... | 76 |
| 4.8.2 Face Detection | ......................................................... | 78 |
| 4.8.3 Line Crossing Detection | .................................................. | 79 |
| 4.8.4 Intrusion Detection | ......................................................... | 82 |
| 4.8.5 Region Entrance Detection | ........................................ | 85 |
| 4.8.6 Region Exiting Detection | ............................................... | 87 |
| 4.9 Storage menus | ..................................................................... | 89 |
| 4.9.1 Record Schedule | ......................................................... | 89 |
| 4.9.2 Storage Management | ...................................................... | 92 |
| 4.9.3 NAS | ...................................................................... | 93 |
| 4.9.4 Snapshot | ................................................................... | 95 |
SECTION 1
Overview

Congratulations on purchasing your new ALIBI™ IP camera! Your camera includes the following key features:

- Megapixel CMOS progressive scan sensor
- High definition video streaming
- Dual-stream video support
- Video stream compression using H.264 standard.
- 3D-DNR noise reduction
- Wide dynamic range (WDR)
- Backlight compensation
- IR sensors for night vision
- Dual power capable - Power over Ethernet (PoE) or 12 Vdc
- Weatherproof IP66 rated
- Vandal proof
- Mobile surveillance
- PTZ functionality (ALI-IPZ series only)
- Video Content Analytics (ALI-NS series only)

1.1 Typical application configurations

Your Alibi IP can function well in many different network configurations. The most common configurations are:

- Camera is installed on an IP network and managed by a Network Video Recorder (NVR)
- Camera is installed on an IP network and uses a network based storage device, such as a NAS or SMB/CIFS server, to archive recorded video and screen captures. The camera is managed by a PC with an Internet browser.
- Camera is installed on an IP network and connected directly by a PC with a Video Management System (VMS).

Since the Alibi camera is an IP based device, several other application configurations are also possible.

Important considerations

- Alibi cameras do not contain internal storage for video recording. Therefore, storage for this data must be in an external device such as an Network video Recorder (NVR), a Network Attached Storage device (NAS or SMB/CIFS device), or a PC with a Video Management System (VMS) that stores recorded video.
- Security devices on your network should be configured with static (fixed) IP addresses whenever possible. Using fixed IP addresses for these devices greatly simplifies the communication between the components of your security system.
- Alibi cameras include a web interface that enables remote access to the camera through an Internet browser such as Microsoft® Internet Explorer®, Mozilla® Firefox®, and Apple® Safari®. With this interface, you can watch live video and perform all camera configuration functions. You can also play back recorded video, download recordings, perform screen captures, and other functions. This document uses the web interface to show all functions of the camera.
**1.1.1 Camera is managed by an NVR or Network DVR**

The most typical application for the camera is to be installed with a compatible NVR or Network DVR (for analog and IP cameras). With the NVR or Network DVR, the camera can be installed anywhere on a network that is accessible to the recorder. Some Alibi NVRs include a built-in Ethernet switch.

![Diagram of Camera and NVR Setup]

**1.1.2 Camera uses network device for video storage**

Cameras that do not include internal data storage can be installed on an IP network and configured to store recorded video on a network-based storage device, such as a Network Attached Storage (NAS) device, or a device using Server Message Block (SMB) or Common Internet File System (CIFS) protocol. With this configuration, the camera is managed through a PC with an Internet browser and access to the LAN where the camera is installed, and recorded video can be played back either through the camera, or by direct access to the recorded video files on the storage device.

![Diagram of Camera and Storage Setup]
1.1.3 Camera is managed by a VMS

Cameras installed on a network can be managed through a PC with Video Management System (VMS, such as the Alibi CMS) software. In this configuration, storage of recorded video usually occurs internally in the PC. VMS software is not provided with your camera.

1.2 PC requirements

The PC you use to connect to your camera with an Internet browser should meet the following requirements:

- **Operating System**: Microsoft® Windows® XP SP1 and above, Windows Vista, 7, 8.x, 10, Server 2003, Server 2008 (32 bit)
- **CPU**: Intel® Pentium® IV 3.0 GHz or faster
- **RAM**: 1GB or more
- **Display**: 1024 × 768 resolution or higher
- **Internet Browser**: Microsoft® Internet Explorer® 7 and newer, Apple® Safari® 5.02 and newer, Mozilla® Firefox 3.5 and newer
SECTION 2

Network Connection

Alibi cameras use a standard RJ45 Ethernet interface to communicate with other devices. Whenever possible, configure the components of your security equipment on the LAN with static (fixed) IP addresses.

Cameras should be installed on the same Ethernet subnetwork (subnet) that contains the NVR or PC with VMS used to manage them, or contains a network storage device for saving recordings.

2.1 Locating cameras on the network with Alibi Power Tools

Alibi Power Tools is a collection of useful utilities for use with your Alibi cameras and recorders. Included with these utilities is the Discovery Tool, used to find IP cameras and recorders attached to the physical network, even if they are configured for a subnet different from the recorder or PC where Alibi Power Tools is installed. Discovery Tool also provides an easy way to reconfigure their network configuration settings. Alibi Power Tools can be installed on a Microsoft® Windows® operating system.

To use Discovery Tool:

1. Insert the software CD provided with your camera into an optical drive on the Microsoft® Windows® computer you will use to access your camera on the LAN.

2. On the CD, find the folder that contains the Alibi Power Tools (Alibi Tools Utility).

3. Install Alibi Power Tools. Refer to the ALIBI™ Power Tools Installation and User Manual also provided on the CD. When the program opens, the following screen appears.

4. Double click on the Discovery Tool icon. The tool will automatically discover Alibi cameras and recorders installed on the network. In the example shown below, an ALI-NS1024VR camera was discovered. Notice that the IP address of the camera is 192.168.1.64 (default IP address).
5. To change the network settings of the camera to be compatible with the subnet where it is installed, do the following:

a. Click on the device to highlight it. Notice that the network parameters for the device populate the fields in the right frame.
SECTION 2: NETWORK CONNECTION

b. Modify the network settings to values compatible with the subnet where it is installed:

» If the IPv4 Address shown for the camera is 192.168.1.64 (default IP address) and the camera is new (un-configured) or was reset to its factory default state, the camera did not find a DHCP server on the network. Modify the parameters in the right pane to values you prefer and are compatible with the network. An example is shown in the screen below.

- If the IPv4 Address shown for the camera is something other than 192.168.1.64 (default IP address) and the camera is new or was reset to its factory default configuration, the camera did find a DHCP server on the network and acquired new network parameters that are compatible with the network. If necessary, change the parameters in the right pane to values that you prefer and are compatible with the network. An example is shown in the screen above.

c. Enter the admin password for the camera in the Password field. The default admin user password for Alibi cameras is 1111.

d. Click the Modify button. The new IP address, port, and other settings will change and appear in the list with the device you modified.
6. Close the Alibi Tools Utility by clicking the Close icon (X) in the upper-right corner of the screen.

2.1.1 Restore Default Password

Some Alibi cameras feature a Reset button that resets the camera to its factory default settings (including the password). To use this feature, refer to the user documentation provided with your camera.

The Alibi Power Tools Discovery Tool includes a Restore Default Password feature. This feature is a Support-only tool that allows them to reset the password of your camera if it was changed and lost. If you lost the password for your camera, contact your Support organization for assistance.
SECTION 3
Remote Access

When the camera is connected to a local network (LAN), you can access it from a computer on the LAN using Microsoft® Internet Explorer, Mozilla Firefox, or Apple Safari.

**NOTE** When connecting to an Alibi camera through Remote Access, you must enter a User Name and Password. User Names are assigned specific permissions. Depending on your permissions, some features of a camera may not be available.

When logging into the camera from a remote computer for the first time, you must install a plug-in program named WebComponents. The procedure for installing the program using Internet Explorer 11 is shown below. Subsequent log ins do not require you to reinstall WebComponents.

### 3.1 Remote login

To access the camera from a computer on the LAN:

1. Log into the operating system as a user with administrative privileges.

2. Open the Microsoft Internet Explorer browser on your computer and enter the IP address of the camera in the URL field. In the example below, the IP address of the camera is 192.168.75.76.
3. In the login window, enter a **User Name** and **Password** with Administrator privileges in the appropriate fields, then click **Login**. The default **User Name** and **Password** for Alibi cameras is **admin** and **1111**.

4. If the password you enter for your camera is a weak password, the following pop-up window will appear. Follow the instructions to create a “strong” **admin** password.

5. If this is the first time you are logging into a camera and you are using Internet Explorer 10 or newer, a message may appear at the bottom of the window to use ActiveX Controls. Click **Allow**.
SECTION 3: REMOTE ACCESS

6. If this login is the first login to an Alibi camera from your computer and browser, continue with the following sub-steps to install WebComponents:

   a. After a successful login to the camera, a message will appear in the middle of the Live View window requiring you to load a plug-in. Click on the message to continue, then click Run in the pop-up block at the bottom of the screen.

   ![Screenshot of Alibi camera Live View window with a message to load a plug-in]

   Some computer security software may attempt to block you from running WebComponents.exe. If necessary, open the Internet Explorer downloads list, right click on the WebComponents.exe file name, then click Run Anyway.

   ![Screenshot of Internet Explorer downloads list with Run Anyway option]

   "NOTE"

   b. In the Setup - WebComponents window opens, click Next to continue.
Installing the WebComponents plugin may require that you close the browser. Follow the on-screen instructions, then restart your browser after the installation is finished.

c. Allow the plug-in installation to complete. When the following window appears, click Finish.

### 3.2 Remote Live View screen

**NOTE** When connecting to an Alibi camera through Remote Access, you must enter a User Name and Password. User Names are assigned specific permissions. Depending on your permissions, some features of a camera may not be available.

After logging into the camera, the Live View - Main stream window initially appears. In this screen, you can:

- Change the viewing options. Click the appropriate button to select a 4:3 or 16:9 aspect ratio, full size (X1 button), and Sub Stream or Main Stream.
• Live view displays for PTZ cameras have additional controls. A PTZ control panel can be opened and closed by clicking the PTZ panel button.
* For cameras with PTZ capability only.

— For cameras with PTZ capability, click the PTZ control panel button to open the frame shown above on the right.

— Each PTZ camera can be configured to include up to 128 “Presets”, each of which can be quickly set and called. Presets are used to quickly reposition the camera for specific views (pan, tilt, zoom, focus). The list of Presets is presented beneath the control panel on the right side of the screen.

- Capture the screen or start and stop recording. Captures and recordings are saved on the local HDD as configured in Local Setup menu.
- Switch from window mode to full screen mode by double clicking anywhere in the Live View video window. To return to window mode, double click anywhere.
- For cameras with Audio capability, select Mute and adjust the audio volume.

3.2.1 Remote Live View screen - ALI-IPV5060RP Fisheye camera

The ALI-IPV5060RP fisheye camera provides up to 4 different images simultaneously. These images can include:

- Single 360 degree fisheye video stream
- Single panoramic video stream (2 streams)
- Simultaneous fisheye video stream of three PTZ camera video streams
- Simultaneous panorama video stream and three PTZ camera video streams
- Simultaneous four PTZ camera video streams
- One fisheye video stream and 3 PTZ camera video streams
- Full screen view of one of 4 individual PTZ camera streams
Viewing options for ALI-IPV5060RP camera are configurable in a special menu. See “4.1.7 Fisheye Parameters (ALI-IPV5060RP camera only)” on page 28.

### 3.3 Playback screen

**NOTE** When connecting to an Alibi camera through Remote Access, you must enter a User Name and Password. User Names are assigned specific permissions. Depending on your permissions, some features of a camera may not be available.

Open the Playback screen by clicking the **Playback** tab. The Playback screen allows you to review video recorded from one camera or several cameras concurrently. Also, video can be downloaded to your local computer.
To playback recorded video:

- Click the day on the calendar when the video was recorded. In the example above, February 5, 2014 was selected.
- Click the **Search** button. Recorded video is indicated by a colored band on the timeline. The color legend is shown below the timeline. You can expand or contract the timeline with the icons on the right.
- At the bottom of the screen, drag the timeline left or right to position the video clip you want to play at the yellow Playback timestamp line.
- In the play controls, click the **Play** button (►) to begin playing video. When the video is playing, the Play button changes to a **Pause** button (II).
SECTION 3: REMOTE ACCESS

- Use the Audio play / mute controls to adjust the audio level (audio capable cameras only).

To save a portion of recorded video

- While playing back video, advance the playback to the beginning of the portion of the video you want to save.
- Click the Start / Stop clipping icon (black scissors). The icon will change to a Stop clipping icon (red scissors).
- When the playback the end of the portion you want to save, clip the Stop clipping icon.
- Playback the video clip you saved. The clip is saved to the location on your local HDD specified in the Setup (tab) | Local Setup menu. See “3.5.1 Local Setup menu” on page 19 for more information.

To download a video recording

- In the Playback screen, Click the Download recording icon.
- In the options on the right panel, select the type of video recording you want to download, the Start Time and the End Time when the recording was made.
- Click the Search button. A list of video recordings meeting the search criterion is shown in the window. **NOTE:** Video recordings that are larger than the Record File Size selected on the Setup (tab) | Local Setup menu (see “3.5.1 Local Setup menu” on page 19) appear in the list as multiple video segments.

- Check the box(es) for the video recording(s) you want to download, then click the Download button. The progress of the download(s) is indicated in the column on the right.
Playback the video recording you downloaded. The recording is saved to the location on your local HDD specified in the Setup (tab) | Local Setup menu. See “3.5.1 Local Setup menu” on page 19 for more information.

To download images

- In the Playback screen, Click the Download images icon.
- In the options on the right panel, select the type of images you want to download, the Start Time and the End Time when the recording was made.
- Click the Search button. A list of video images meeting the search criterion is shown in the window.

Check the box(es) for the image(s) you want to download, then click the Download button. The progress of the download(s) is indicated in the column on the right.
• Open the image(s) you downloaded. The image(s) is saved to the location on your local HDD specified in the Setup (tab) | Local Setup menu. See “3.5.1 Local Setup menu” on page 19 for more information.

### 3.4 Remote Log screen

Open the Log screen by clicking Log in the screen header. The camera log report is created by specifying a search criteria using the menu in the right frame (or using the default options), then clicking the Search button. The search criteria menu includes filters to search for Major and Minor type events, and specify the start and end time of the report.

Log reports can be saved in either text or Excel formats by clicking the Save Log icon.
3.5 Remote SETUP screen

NOTE When connecting to an Alibi camera through Remote Access, you must enter a User Name and Password. User Names are assigned specific permissions. Depending on your permissions, some features of a camera may not be available.

Open the Configuration screen by clicking the Configuration tab. The Configuration menus are organized in two sections: one for Local Setup, and one for Camera Setup. The Local Setup section defines the Live View Parameters, Record File (local PC) Settings, and Picture and Clip Settings. Camera Setup includes all configurable features of the camera, including the System, Network, Storage locations, etc. Users who log into the camera through the remote connection may or may not be allowed to view or change the configuration of the local settings or camera, depending on the permissions granted to their user name by admin user.

3.5.1 Local Setup menu

The local configuration includes parameters of Live View, Record Files (local PC settings), and Picture and Clip Settings. The record files and captured pictures are created using your web browser and saved on the PC running the browser.

To open the Local Setup screen, go to Setup tab | Local Setup.

<table>
<thead>
<tr>
<th>Live View</th>
<th>Playback</th>
<th>Log</th>
<th>Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Setup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera Setup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video/Audio</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard Event</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VGA Event</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuration settings are defined below:

Live View Parameters: Set the protocol type and live view performance.
- **Protocol Type**: Select either TCP, UDP, MULTICAST or HTTP.
  - TCP: Ensures complete delivery of streaming data and better video quality. Real-time transmission is affected.
  - UDP: Provides real-time audio and video streams.
— **HTTP**: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.
— **MULTICAST**: See TCP/IP settings for more information.

- **Live View Performance**: Set the live view performance to Shortest Delay or Auto. Depending on your camera, other options may be available.
- **Rules**: Reserved for future use.
- **Image Format**: Select the file format for captured images (JPEG or BMP).

**Record File Settings**: Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.

- **Record File Size**: Select the segment size of the manually recorded and downloaded video files. Options are 256MB, 512MB or 1GB.
- **Save record files to**: Set the saving path for the manually recorded video files.
- **Save downloaded files to**: Set the saving path for the downloaded video files in playback mode.

**Picture and Clip Settings**: Set the saving paths on your PC of the captured pictures and clipped video files with the web browser.

- **Save snapshots in live view to**: Set the saving path of the manually captured pictures in Live View mode.
- **Save snapshots when playback to**: Set the saving path of the captured pictures in playback mode.
- **Save clips to**: Set the saving path of the clipped video files in playback mode.

### 3.5.2 Camera Setup menus

Camera Setup menus are described in “SECTION 4 Camera Setup Menus” on page 21.
SECTION 4
Camera Setup Menus

Camera Setup menus that appear when accessing Alibi cameras through a web browser present the complete set of configuration options. These options are organized in a tree of menus as shown below.

* Submenus that appear in the Camera Setup menu tree above exist only in cameras that include the applicable features.
4.1 System Setup menus

4.1.1 Device Information

The Device Information screen shows the basic information for the device, including the Device Name and Device No. (number), model, serial number, software versions, and other features. To open the Device Information screen, go to Setup tab | System | Device Information.

In the Device information screen, you can change the Device Name and Number by editing the fields, then clicking Save.

4.1.2 Time Settings

Use the Time Settings screen to set the correct time and date in the camera. Because video recordings and captures are time stamped with this information, the correct date and time is important if the files become evidence of some event. To open the Time Settings menu, go to Setup tab | System | Time Settings.
• Select the **Time Zone** from the drop-down menu. In some system applications, the monitoring system (NVR, VMS) may be in a different time zone from the camera. Select the time zone that best supports your system objectives.

**Time Sync.**

You can synchronize the clock in your camera either from an NTP server, by setting it manually, or synchronizing it with your computer.

- **NTP:** Synchronizing Time by NTP Server.
  
  a. Check the checkbox to enable the NTP function.
  
  b. Configure the following settings:

  - **Server Address:** IP address of NTP server.
  - **NTP Port:** Port of NTP server.
  - **Interval:** The time interval between the two synchronizing actions with NTP server.

  **NOTE**  
  If the camera is connected to a public network, use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP address: 210.72.145.44). If the camera is set in an isolated network, NTP software can be used to establish a NTP server for time synchronization.

- **Manual Time Sync.:** Set the camera clock manually or synchronize the clock in your PC.
  
  a. Check the checkbox to enable the NTP function.
SECTION 4: CAMERA SETUP MENUS

b. Do one of the following:
   * Enter the preferred time in the Set Time field, then click Save.
   * Check the Sync. with computer time box, then click Save.

NOTE After setting the time in the camera, open the DST tab to setup the Daylight Savings Time configuration for the camera.

4.1.3 Maintenance

The Maintenance screen includes the camera-related maintenance functions. To open the Maintenance screen, go to Setup tab | System | Maintenance.

![Maintenance Screen](image)

Reboot

Click Reboot to restart the camera. When you reboot the camera, now configuration parameters are changed.

Restore

Click Restore to reset all configuration parameters, except the IP network settings and user information, to their factory default values.

Default

Click Default to reset all configuration parameters, INCLUDING the IP network settings and user information, to their factory default values. The network IP address is reset to 192.168.1.64.
Export

Click **Export** to save the camera configuration file for Import later if necessary. You can also export the configuration and use it to quickly configure other cameras using the Import feature.

**Import Config. File**

Click **Browse** to locate a previously saved camera configuration file to import, then click **Import**. The import status is shown on the line below.

**Remote Upgrade (Firmware)**

**NOTE**  
Firmware upgrade should ONLY be performed if recommended by your Support organization.

You can upgrade in the camera either by browsing to the directory where the firmware upgrade file exists, or specifying the full path to the upgrade file. To upgrade firmware:

1. In the Remote Upgrade section of the Maintenance screen, click the drop-down list, then select either **Firmware** or **Firmware Directory**. In the example below, Firmware was selected. **NOTE**: The firmware file should be no more than two directories deep. See the example below.

2. Click **Browse**, then browse to the firmware file (for Firmware) or the directory where the firmware file exists (for Firmware Directory).
3. Click Upgrade.

4. Wait until the upgrade process completes. (1 ~ 10 minutes), then log into your camera. (You can use the camera again when the upgrade finishes.)

5. Power off the camera.

6. Power on the camera again, then open the Device Information screen. Go to Setup tab | System | Device Information.

7. Verify that the screen shows the new Firmware Version is installed.

**4.1.4 RS485**

Use the RS485 menu to configure the RS-485 communication interface to the camera (available only on cameras with an RS-485 interface). This interface is typically found on PTZ cameras and used for controlling pan - tilt - zoom camera functions through that interface.

1. Open Time RS485 interface: Go to Setup tab | System | RS485.

   ![RS485 menu](image)

   2. Use the drop-down lists to select the appropriate parameters for the RS-485 interface.

   3. Set the PTZ Address to an unused value on your PTZ network.

   4. Click Save to retain the settings.

**4.1.5 DST (Daylight Savings Time)**

Use the DST menu to configure the Daylight Savings Time mode for the camera. To setup the camera automatically adjust the clock for DST:
1. **Open Time Settings interface:** Go to **Setup tab | System | DST.**

   ![Time Settings Interface](image)

2. **Check the DST box,** then set the **Start Time** and **End Time** using the options in the drop down lists.

3. **Click Save.**

### 4.1.6 Service

Some ALIBI cameras provide a Service tab in the System Setup menu group. Depending on the camera model, other options may be present.

The Service menu allows you enable or disable the IR light. Some cameras may have additional options, such as Telnet.

**To open the Service menu,** go to **Setup tab | System | Service.**

![Service Menu](image)

In the Service menu, check or uncheck the box(es) for the item(s) you want to enable or disable, then click **Save.**
4.1.7 Fisheye Parameters (ALI-IPV5060RP camera only)

Alibi Fisheye cameras include a special setup menu called Fisheye Parameters. This menu is used to configure the camera for the mounting orientation (type - Wall, Table, or Ceiling), and Real Time Mode (Enable or Disable). These parameters affect the Live View mode options, image effect, PTZ control, Preset scene, etc. PTZ View and panoramic view cannot be performed at the same time in Live View mod. Also, when a PTZ view is displayed, no local recording is performed.

When configuring an Alibi Fisheye camera, use this menu to select the applicable Mounting Type parameter. To configure this menu:

1. Open the Fisheye Parameter menu. Go to Setup tab | System | Fisheye Parameter.

2. Open the Mount Type drop-down list and select the applicable mounting orientation of the camera: Wall, Table or Ceiling.

3. In the Real-time Mode field, select either Enable or Disable.

4. Click Save to retain your settings.

4.2 Network menus

4.2.1 TCP/IP

TCP/IP settings must be properly configured before you operate the camera over network. The camera supports both the IPv4 and IPv6. Both versions may be configured simultaneously without conflicting to each other, and at least one IP version should be configured.

Steps:

1. Open TCP/IP settings interface: Go to Setup tab | Network | TCP/IP.
2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.

NOTES

- The valid value range of MTU is 500 ~ 1500.
- Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream simultaneously by requesting a copy from the multicast group address. Before using this function, you must enable the Multicast function of your router.

3. Click Save. The camera must reboot for new settings to take effect.

4.2.2 Port

You can change the HTTP, RTSP HTTPS and Server port numbers the camera will use. To change any of these settings:

1. Open Network Port settings interface: Go to Setup tab | Network | Port.
2. Edit the HTTP, RTSP HTTPS and/or Server port numbers you want to change.

   - **HTTP Port**: The default port number is 80, and can be changed to any port range 1024 to 65535.
   - **RTSP Port**: The default port number is 554.
   - **HTTPS Port**: The default port number is 443, and can be changed to any port range 1024 to 65535.
   - **Server Port**: The default server port number is 8000.

3. Click **Save**. The camera must reboot for new settings to take effect.

### 4.2.3 DDNS

Registration on the DDNS server is required before configuring the DDNS settings of the camera.

**Steps**

1. Open Network DDNS settings interface: Go to **Setup** tab | **Network** | **DDNS**.
2. Check the **Enable DDNS** checkbox to enable this feature (see above).

3. Select one of the DDNS Type. Options are SimpleDDNS, DynDNS, IPServer, and NO-IP.

   - For SimpleDDNS, you must configure the Domain name. To use this option, you must have a valid DNS server (such as 8.8.8.8 (Google)) configured in the network settings of your camera.
     
     i. In the Domain field, enter the domain name you prefer.
     
     ii. Click **Save**. If the Save occurs without error, the Domain name you entered is accepted.

   - For IPServer, you must configure the camera with a static IP address, subnet mask, gateway and preferred DNS. These values can be obtained from your Internet Service Provider (ISP).
     
     i. In the Server Address field, enter static IP address of the computer that runs the IP Server software.
     
     ii. Click **Save**.

   - For DynDNS:
i. Enter Server Address of DynDNS (e.g. members.dyndns.org).

ii. In the Domain text field, enter the domain name obtained from the DynDNS website.

iii. Enter the User Name and Password registered on the DynDNS website.

iv. Click Save.

— For NO-IP:

i. Enter Server Address field with the Server Address.

ii. In the Domain text field, enter the domain name obtained from the NO-IP website.

iii. Enter the User Name and Password registered on the NO-IP website.

iv. Click Save.
4.2.4 SNMP

You can set the SNMP function to acquire camera status, parameters and alarm information and manage the camera remotely when it is connected to the network.

Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Note: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. SNMP v3 provides encryption. When using SNMP v3, HTTPS protocol must be enabled.
IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

The 802.1X mechanism requires an authenticator (authentication device), and typically an authentication server. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authentication server must be configured to verify the credentials (user name and password) from the camera.

1. Open Network 802.1X settings interface: Go to Setup tab | Network | 802.1X

   ![Setup tab | Network | 802.1X](image)

   1. Check the Enable IEEE 802.1X box to enable the feature.
   2. Configure the 802.1X settings, including EAPOL version, user name and password. The EAPOL version must be identical with that of the router or the switch.
   3. Enter the user name and password to access the server.
   4. Click Save. A reboot is required for these settings to be in effect.

4.2.6 QoS

QoS (Quality of Service) can help solve network delay and network congestion problems by configuring the priority of sent data. To open the QoS screen, go to Setup tab | Network | QoS.
To configure QoS:

1. Edit the DSCP fields for Video/Audio DSCP, Event/Alarm DSCP and Management DSCP. The valid value range of the DSCP is 0–63. Larger DSCP values have higher priority.

   **NOTE**  
   DSCP refers to the Differentiated Service Code Point. The DSCP value is used in the IP header to indicate the priority of the data.

2. Click Save. The settings are applied when the camera is rebooted.

### 4.2.7 FTP

The FTP feature can be used to upload captured pictures to an FTP server. Picture captures can be triggered by events or a timing snapshot. To open the FTP screen, go to **Setup** tab | **Network** | **FTP**.

1. To use FTP, enter the following parameters:

   - **FTP Server Address**: Enter the IP address of the FTP server you want to use.
SECTION 4: CAMERA SETUP MENUS

- FTP server **Port** number. The default value of the FTP port is 21.
- **User Name**: User name you use to authenticate access to the server.
- **Password** and **Confirm**: Enter both fields with the password of the User Name.
- **Directory Structure**: In the Directory Structure field, select the root directory, parent directory or child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.
- **Upload Type**: To enable uploading the captured picture to the FTP server.
- **Anonymous**: Check the Anonymous box to enable the anonymous access to the FTP server. Use this option when access to the FTP Server does not require a User Name and Password. The anonymous access function must be supported by the FTP server.

2. Click **Save**.

3. Check the **Upload Picture** box, and then click **Test** to upload a picture to the server. Verify that the upload was successful. If not, correct your settings and retest.

**NOTE**

To upload the captured pictures to FTP server, you must enable continuous snapshot or event-triggered snapshot on Snapshot screen.

To upload the captured pictures to FTP server, you must select **Enable Timing Snapshot** or **Event -Triggered Snapshot** on the **Setup** (tab) | **Storage** | **Snapshot** screen.

### 4.2.8 UPnP™

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don’t need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router. To open the UPnP screen, go to **Setup** tab | **Network** | **UPnP™**.
Check the Enable UPnP™ box to use this feature, edit the Friendly Name field if necessary, then click **Save** to retain your settings.

You can verify UPnP™ functionality by opening a file browser, then looking at the items listed in the Network directory.

### 4.2.9 Email

The Email feature is used to send an email message to up to three email address when specific events occur within the camera. The Email menu is used to configure the sender's email server, user name and password, and the receiver(s) email address(es). Events that activate email alerts are configured in other menus.

The camera must be configured for Internet access to connect to your email server. Configure TCP/IP settings before configuring your email preferences.

To open the Email menu, go to **Setup tab | Network | Email**.

1. 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 (e.g., smtp.263xmail.com).
   - **SMTP Port**: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). The the SSL SMTP port is 465.
   - **Enable SSL**: Check the checkbox to enable SSL if it is required by the SMTP server.
SECTION 4: CAMERA SETUP MENUS

— **Attached Image**: Check this box if you want to send email with an image.
— **Interval**: The interval is the time between two emails sent with attached pictures.
— **Authentication** (optional): If your email server requires authentication, check this box to use authentication to connect to this server. You must specify your email User Name and Password.
— **Choose Receiver**: Select the receiver to which the email is sent. Up to 3 receivers can be configured.
— **Receiver**: The name of the user to be notified.
— **Receiver’s Address**: The email address of user to be notified.

2. Click **Save**.

4.2.10 **NAT**

The NAT menu enables you to specify the external port and IP address for HTTP, RTSP and a server port. You can enable port mapping in either **Auto** or **Manual** modes. This feature is disabled by default in Alibi cameras for corporate network security concerns.

![NAT Menu](image)

4.2.11 **HTTPS**

The HTTPS menu enables you to setup a secure connection to your camera over an insecure network. It provides bidirectional encryption of data flowing between your PC and the camera, which protects against tampering, eavesdropping, man-in-the-middle attacks and/or forging the contents. To open the HTTPS menu, go to **Setup** tab | **Network** | **HTTPS**.
1. Check the **Enable HTTPS** box to enable the feature.

2. Create either a self-signed certificate or an authorized certificate.

   — **To create a self-signed certificate:**

     **Note:** If you already have a certificate installed, the **Create Self-signed Certificate** is grayed out.

     i. Click the **Create** button below the **Create** heading.

     ii. Enter the country, host name/IP, validity and other information.

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

   — **To create the authorized certificate:**

     i. Click **Create** button to **Create Certificate Request**.
ii. Complete the fields in the certificate request form. **Note:** the Country code (example, CN (China)) and Hostname/IP entries are required.

iii. Download the certificate request and submit it to the trusted certificate authority for signature.

iv. After receiving the signed valid certificate, import the certificate to the device.

3. After a certificate is installed, information will be shown under the **Installed Certificate** heading. Click **Save** to retain your settings.

### 4.3 Video/Audio menus

#### 4.3.1 Video

The Video menu is used to setup the Main Stream video transmission settings, and Sub Stream settings for dual stream cameras. In this example, the camera has two streams: **Main Stream** (Normal) and **Sub Stream**. The configuration parameters for both are the same, but the capabilities of the two streams are much different.

To open the Video menu, go to **Setup** tab | **Video/Audio** | **Video**.
1. Select the **Stream Type** of the camera you want to configure. **Main Stream** is usually for recording and live viewing with good bandwidth, and **Sub Stream** should be used for live viewing when the bandwidth is limited.

2. Configure the following settings for your preferred performance:
   
   — **Video Type**: Select the stream type to video stream or video and audio composite stream (for cameras with audio capability). For cameras with audio, the audio signal is recorded only when the Video Type is **Video & Audio**.
   
   — **Resolution**: Select the resolution of the video output.
   
   — **Bitrate Type**: Select either **Constant** or **Variable**.
   
   — **Video Quality**: When bitrate type is selected as Variable, you can select one of six levels of video quality. Higher video quality requires more network bandwidth.
   
   — **Frame Rate**: Set the frame rate to 1/16 ~ 25 fps. The frame rate is the rate at which video frames are sent to the receiving device, or the rate at which the video stream is recorded. A higher frame rate produces a smoother image with higher quality throughout, but requires more network bandwidth.
   
   — **Max. Bitrate**: Set the maximum bitrate to 32 ~ 16384 Kbps. The higher value corresponds to the higher video quality at a cost of higher network bandwidth.
   
   — **Video Encoding**: When the Stream Type of the camera is **Main Stream**, the Video Encoding standard can be set to H.264. When the Stream Type of the camera is **Sub Stream**, the Video Encoding standard can be set to H.264 or MJPEG.
   
   — **H.264 OVC**: H.264 OVC is an advanced compression coding technology. By enabling H.264 OVC, you can calculate the HDD consumption by its average bitrate, and save storage by lowering the bitrate. If you set the main stream as the stream type and H.264 as the video coding, H.264 OVC is available. You must reboot the camera when you turn on or turn off H.264 OVC.
   
   — **Profile**: The profile for this camera is **Main Profile**. No other profiles are selectable.
   
   — **I Frame Interval**: Set the I-Frame interval to 1~400. The I-frame interval represents the rate at which the entire video frame is transmitted (refreshed) when using a video compression technology such as H.264.
   
   — **Smoothening**: Refers to the smoothness of the stream. The higher value of the smoothing, the better fluency of the stream, but may lower the video quality. A lower smoothening value provides the higher stream quality that may not appear fluent.
4.3.2 Audio

Use the Audio tab to configure the audio settings for the camera microphone. Cameras without microphones may not provide this menu. Additionally, different camera models with microphones may offer settings different from those shown here.

To open the Audio menu, go to Setup tab | Video/Audio | Audio.

1. Configure the following settings.
   - **Audio Encoding**: Select either G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 or PCM. For MP2L2, the sampling rate and audio stream bitrate are configurable; for PCM, the sampling rate can be set.
   - **Audio Input**: Select either MicIn and LineIn for the connected microphone and line pickup respectively.
   - **Input Volume**: Drag the slider to select a value between 0 ~ 100
   - **Environmental Noise Filter**: Set it to OFF or ON for the best performance. When the function is enabled, extraneous noise in the environment can be reduced.

2. Click **Save**.

4.3.3 ROI

ROI (Region of Interest) encoding allows you to identify important areas of the image and apply more compression resources to improve the quality of that area instead of the lesser important background. The ROI area may appear more focused, while the background area is less focused. The ROI feature is available on only some cameras.

There are two types of ROI encoding:

- **Fixed Region**: Fixed region encoding is the ROI encoding for a manually configured area. And you can choose the Image Quality Enhancing level for ROI encoding, and you can also name the ROI area.
- **Dynamic Tracking** (not Fixed Region): Dynamic tracking refers to the ROI defined by intelligent analysis such as human face detection. You can choose the Image Quality Enhancing level for the ROI encoding.

To open the ROI menu, go to Setup tab | Video/Audio | ROI.
SECTION 4: CAMERA SETUP MENUS

To define the ROIs:

1. Click the **Draw Area** button.

2. Using your mouse, drag a rectangle over the region of interest on the image.

3. Click the **Stop Drawing** button.

4. Choose the stream type to set the ROI encoding (Main Stream or Sub Stream).

5. Choose the ROI type. Check the Fixed Region box for Fixed Region encoding. Clear the box for Dynamic Tracking.
   - If you enabled Fixed Region, you can also select the Region number (1 .. 4), the **ROI Level** (Image Quality Enhancing level) and enter a **Region Name**.
   - If Fixed Region is not enabled (i.e. Dynamic Tracking), select the **ROI Level** (Image Quality Enhancing level).

6. Click **Save**.

7. Repeat the steps above to define additional regions. You can define up to three ROI.
4.3.4 Display Info. on Stream

Check the Enable Dual-VCA box to show information about the objects in the stream. After selecting this option, configure Line Crossing, Intrusion Detection, and other VCA options as needed.

To open the Display on Stream menu, go to Setup tab | Video/Audio | Display Info. on Stream.

4.4 PTZ menus

PTZ sub-menus appear in the Settings display only when connecting to a PTZ capable camera.

4.4.1 Basic menu

Use the Basic menu to configure proportional pan, preset freezing, preset speed, and other elementary camera functions.

To open the Basic menu, go to Setup tab | PTZ | Basic.
1. Configure the following settings:

**Basic Parameters**: Enable/disable proportional pan and preset freezing, set the preset speed, keyboard control speed, and auto scan speed.

   — **Proportional Pan**: Enabling this function causes the pan/tilt speeds to change according to the amount of zoom. When using high zoom, the pan/tilt speed slows to keeping the image from moving too fast on the Live View image display.

   — **Preset Freezing**: This function enables the Live View to switch from one scene defined by a preset to another, without showing the middle areas between these two to ensure the surveillance efficiency. It can also reduce bandwidth usage.

     **Note**: Preset freezing function is not in effect when calling a pattern.

   — **Preset Speed**: You can set the speed of a defined preset from 1 to 8.

   — **Keyboard Control Speed**: Define the speed of PTZ control by a keyboard as Low, Normal or High.

   — **Auto Scan Speed**: The dome provides 5 scan modes: auto scan, tilt scan, frame scan, random scan and panorama scan. The scan speed can be set from level 1 to 40.

**PTZ OSD**: Set the on-screen PTZ status display duration.

   — **Zoom Status**: Set the OSD zooming status duration to 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.

   — **PT Status**: Set the azimuth angle display duration while panning and tilting to 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.

   — **Preset Status**: Set the preset name display duration while calling the preset as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.

**Power-off Memory**: When the camera restarts after a power off, it can resume the previous PTZ status or actions it was performing a specified time period before the power-off. You can set it to resume the status or actions it was performing 30 seconds, 60 seconds, 300 seconds or 600 seconds before power-off.
2. Click **Save** to save your settings.

### 4.4.2 Limit menu

The camera can be configured to only move only within limits of motion left, right, up, and down.

To open the Limit menu, go to **Setup** tab | **PTZ** | **Limit**.

1. Click the checkbox of **Enable Limit**, then choose the limit type as Manual Stops or Scan Stops.
   - **Manual Stops**: When manual limit stops are set, you can operate the PTZ control panel manually only in the limited surveillance area.
   - **Scan Stops**: When scan limit stops are set, the random scan, frame scan, auto scan, tilt scan, and panorama scan is performed only within the limited surveillance area.

   **NOTE** Set the Manual Stops limits before setting Scan Stops limits. When you set these two limit types at the same time, Manual Stops is valid and Scan Stops is invalid.

2. Click the PTZ control buttons to determine the left/right/up/down limit stops; you can also call the defined presets and set them as the limits of the dome.

3. Click **Set** to save the limit stops, or click **Clear** to clear the limit stops.
4.4.3 Initial Position menu

The initial position is the origin of PTZ coordinates. It can be the factory default initial position, or you can customize the initial position according to your needs. To customize the position, use the procedure below.

To open the Initial Position menu, go to Setup tab | PTZ | Initial Position.

1. Click the PTZ control buttons to point the camera at the initial target after startup. You can also call a predefined Preset position and set the Initial Position to that target.

2. Do one of the following:
   — Click Set to save the position.
   — Click Clear to set the initial position to the factory default.
   — Click Goto to point the camera at the current Initial Position.

4.4.4 Park Action menu

The Park Action feature configures the camera to start a perform a predefined park action (scan, preset, pattern, etc.) automatically after a period of inactivity (park time).

To open the Park Action menu, go to Setup tab | PTZ | Park Action.
1. Check the box to **Enable Park Action**.

2. Set the **Park Time**. Park Time is the length in seconds of inactivity of the camera before it begins park actions.

3. Open the **Action Type** drop down list, then click to select the action you want to perform.

4. Click **Save** to save your settings.

### 4.4.5 Privacy Mask menu

Privacy mask allow you to cover selected areas on the Live View image to prevent them from being live viewed and recorded.

To open the Privacy Mask menu, go to **Setup** tab | **PTZ** | **Privacy Mask**.

Masked area over ATM keypad
SECTION 4: CAMERA SETUP MENUS

1. Use the PTZ control buttons to display the area you want to cover with a privacy mask.

2. Click Draw Area, then click and drag the mouse across the area of the live video you want to mask. A semi-transparent box with red squares on each corner will appear on the screen.

3. Drag the red corner squares as needed to form a polygon over the area you want to cover.

4. Click Stop Drawing to complete the drawing. You can also click Clear All to clear the areas you setup without saving them.

5. Click Add to save the privacy mask. The mask will be listed in the at the bottom of the menu. In the list, you can name the mask, select a mask color, and enter an active zoom ratio.

6. Check the Enable Privacy Masks box to enable this function. The semi-transparent polygon will become opaque.

7. To change the shape or position, or delete the mask you created, click the mask entry in the list. A red border with red squares in each corner will appear in the around the mask you picked. Drag the corners to change the shape, or click Delete to remove the mask.

8. Repeat this procedure outlined above to configure additional privacy masks on the live video image. You can configure up to 24 privacy masks on the same image.

4.4.6 Scheduled Tasks menu

You can configure the camera to automatically perform certain different actions during different time periods.

To open the Scheduled Tasks menu, go to Setup tab | PTZ | Scheduled Tasks.
SECTION 4: CAMERA SETUP MENUS

1. Check the select box to **Enable Scheduled Task**.

2. Set the **Park Time**. The park time is the period of inactivity before the camera begins the scheduled task.

3. Set the schedule and task details:
   a. Click the **Edit Tasks** button to edit the task schedule.

   ![Timing Tasks](image)

   b. Click a tab at the top of the window shown above to choose the day you want to schedule a task on.

   c. Click **All Day** to set the schedule as all day, or click **Customize** and enter a Start Time and End Time for each task. If you selected **Customize**:

      i. Click the Start Time field for Period 1, then enter the start time hour and minutes when you want to start the task. Press Enter on your keyboard to set the time.

      ii. Set the End Time field for Period 1 the same way.

   d. Open the Task Type drop down list for Period 1, then select the task you want to perform during that period. If you selected Patrol, Pattern or Preset, also select the (preconfigured) Task Type ID in the right column.

   e. If you selected Customize in sub-step c above, configure additional time periods, with different tasks, if needed. The time periods you configure must not overlap.

   f. If you want to copy the schedule you created to other days of the week, check the boxes at the bottom of the window for days you want to copy the schedule to, then click **Copy**.

   g. To save the schedule you specified, click **OK**. A scheduled task is indicated in the timetable shown below.
4. To revise the schedule you created, click Edit Tasks, then follow the example outlined in step 3 to make changes.

### 4.4.7 Clear Config menu

Use this sub-menu to clear your PTZ configurations, including all presets, patrols, patterns, privacy masks, PTZ limits and scheduled tasks.

To open the Clear Config menu, go to **Setup tab | PTZ | Clear Config**.

1. In the menu above, check the boxes for the items you want to clear.

2. Click **Save** to clear the settings.
4.4.8 Smart Tracking menu

This function is used to configure the camera to automatically track the moving objects it detects. Not all the camera models support this feature.

To open the Smart Tracking menu, go to Setup tab | PTZ | Smart Tracking.

1. Check the Enable Smart Tracking box to enable this feature.

2. Click the PTZ buttons to select an object.

3. Click Set Zoom Ratio to set the current zoom ratio as the tracking zoom ratio.

4. Set the tracking duration. The camera will stop tracking when the duration ends. The duration can range from 0 to 300 seconds.

   **NOTE** Setting the duration to 0 means that there’s no duration when the camera tracks (i.e., endless).

4.4.9 Prioritize PTZ menu

In network configurations where a PTZ camera is controlled by both a Network (LAN) based controller (such as a remote login from a browser) and an RS485 joystick controller connection, this submenu is used to assign priority to either the Network connection
or the RS485 connection. An additional parameter in the menu, Delay, is used to set the time, in seconds, that the un-prioritized controller (Network or LAN) must wait before it can issue commands to the camera after the prioritized network issues a command.

To open the Prioritize PTZ menu, go to Setup tab | PTZ | Prioritize PTZ.

1. Open the Prioritize PTZ drop down list, then select the network you want to prioritize: Network or RS485.

2. In the Delay field, enter the delay, in seconds, that the un-prioritized network must wait before it can issue a command to the camera after the prioritized camera issues the command.

3. Click Save to retain your settings.

### 4.5 Image menus

#### 4.5.1 Display Settings

The Display Settings menu includes the image-related configurable parameters for the camera. It contains several sub-menus such as Image Adjustment, Exposure Settings, Day/Night Switch, etc. that can be opened or closed for compactness. Additionally, several adjustments can be seen in the Live View image on the menu.

To open the Display Settings menu, go to Setup tab | Image | Display Settings.
Configurable parameters include:

- **Switch Day and Night**: Select either **Auto-Switch** or **Scheduled-Switch**.
  - If using **Auto-Switch**, open the **Day/Night Switch** submenu to select the Sensitivity, Filtering Time, and Smart IR feature ON or OFF.
  - If using **Scheduled Switch**, set the **Start Time** and **End Time** of the switch, then open the **Day/Night Switch** submenu to select the **Smart IR** feature ON or OFF.
  
  Also, click the **Common**, **Day** and **Night** tabs to set the Saturation, Hue, Brightness, Contrast and Sharpness for Day and for Night modes.

- **Image Adjustment** submenu: Open the Image adjustment submenu to set the Saturation, Hue, Brightness, Contrast and Sharpness of the video image. Each parameter can be set to a level of 0 ~ 100 either by moving the slider or entering the value in the box on the right. The effect of the adjustment will appear in the Live View image in the menu.
• **Exposure Settings** submenu: In this submenu, set the following for the best performance:
  - **Iris Mode**: Select Auto or Manual. Some cameras may not offer both options.
  - **Exposure Time**: Value ranges from 1/3 to 1/100,000s. The nominal value is 1/150. Adjust it according to the lightening condition.
  - **Gain**: Set the gain to show the optimal brightness level.

• **Day/Night Switch** submenu: You can set the Day/Night switch to Day, Night, Auto, or Schedule. The option you select determines the submenu options.
  - **Day or Night**: These options both have one parameter: Smart IR.
  - **Auto**: If you select Auto switch, you can set the sensitivity (0..7), filtering time and Smart IR.
  - **Schedule**: Use Schedule to set that **Start Time** and **End Time** for the switch. Smart IR is also selectable.

• **Backlight Settings**: Backlight settings include BLC Area (Off, Up, Down, Left, Right, Center), the area to control, and **WDR** (Wide Dynamic Range) ON or OFF.

• **White Balance**: White Balance selection is used to correct colors in the image depending on the lighting source. You can also set the white balance manually (MWB), using Automatic White Balance (AWB1), and lock the white balance setting (Locked WB).

• **Image Enhancement**: Options in this submenu include **Digital Noise Reduction (DNR)** ON or OFF. If ON, you can also adjust the level of noise reduction.

• **Video Adjustment**: Video Adjustment includes:
  - **Mirror**: Mirror adjustment enables you to flip the image (Up/Down), flip Left/Right (reflect or Center).
  - **Rotate**: Rotate rotates the image +90 degrees. Changes the aspect ratio from 4:3 to 3:4 for displays of long corridors.
  - **Video Standard**: Select 50 Hz for PAL format, 60 Hz for NTSC format.
  - **Capture Mode**: To make a complete use of the 16:9 aspect ratio, you can enable the capture mode when you use the camera in a narrow view scene.

  When installing the camera, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, then set the capture mode to the screen size option you prefer.

### 4.5.2 OSD Settings

With OSD Settings, you can label the screen for easy recognition of the view (Camera Name) and the timestamp (time and date format), a mode option (flashing or constant) and text size.

To open the OSD Settings menu, go to **Setup** tab | **Image** | **OSD Settings**.
1. Check the corresponding box to select the display of camera name, date or week if needed.

2. Edit the **Camera Name** if needed.

3. From the drop-down lists, select the preferred **Time Format**, **Date Format**, **Display Mode** and **OSD Size**.

4. Drag the text boxes to the locations on the screen that won’t obscure useful information in the image.

5. Click **Save**.

### 4.5.3 Text Overlay

The **Text Overlay** feature enables you to add useful information, other than **Camera Name** and **Date** (see “4.5.2 OSD Settings” on page 55) to the image.

To open the Text Overlay menu, go to **Setup** tab | **Image** | **Text Overlay**.
1. Check the box in front of the label entry field on the right side of the window, then enter the text you want to display. In the image above, the label is Ceiling Camera.

2. Drag the text box to the location on the image where you want it displayed.

3. Click Save.

4.5.4 Privacy Mask

The Privacy Mask feature allows you to block areas of the live video image to prevent it from being viewed or recorded.

To open the Privacy Mask menu, go to Setup tab | Image | Text Overlay.

1. Check the Enable Privacy Mask box of to enable this feature.
2. Click the **Draw Area** button.

3. Using the mouse, drag a box across the areas you want to block. In the screen above, two boxes were created. The boxes are shown as grayed-out areas. You can create up to four privacy masks. To clear any box and start again, click **Clear All**.

4. Click **Stop Drawing** to complete masking the image.

5. Click **Save**.

### 4.6 Security menus

#### 4.6.1 User

The **User** menu is used to create and delete user accounts, and change passwords. To use this menu, you must log into the camera with the **admin** user credentials.

In the User menu, you can create either of two levels of users: Operator and User. Each level has a different subset of permissions that are configurable. A third account level, Administrator, has one user name, **admin**, that cannot be deleted and has all permissions enabled. This account level is not configurable, but the admin password can be (and should be) changed from its default value, **1111**.

To open the User menu, go to **Setup** tab | **Security** | **User**.

![User Menu](image)

**Change the admin password**

1. To change the admin password, click the **User Name** admin, then click the **Modify** button. A **Modify User** window will open.
2. Enter the new admin password in the **Password** and **Confirm** fields.

3. Click **OK** to save the settings. **Record** the new password and save it in a secure location.

### To create a new user

1. In the User menu, click **Add**.

   2. In the User Name field, enter a unique user name. You can enter most keyboard characters to compose the name.

   3. In the Level drop-down list, select either **Operator** or **User**.
SECTION 4: CAMERA SETUP MENUS

4. Check and/or uncheck the boxes for the Basic and Camera permissions you want to grant or restrict the user.

5. Click **OK** to save your settings.

**To delete a user**

1. To delete a user, click the User Name in the User menu to highlight it.

2. Click the **Delete** button, then click OK in the pop-up confirmation window.

**4.6.2 (RTSP) Authentication**

RTSP Authentication can be disabled to allow anyone to access the video stream using RTSP protocol with the IP address of the camera. The default setting is **Basic** authentication (requires credentials).

To open the RTSP Authentication menu, go to **Setup tab | Security | Authentication**.

To disable RTSP authentication, open the Authentication drop-down list, then select **disable**. Click **Save** to retain this setting.

**4.6.3 Anonymous Visit**

The Anonymous Visit feature can be enabled to allow anyone to enter the camera menus without entering a User Name and Password.
To enable the Anonymous Visit feature, open the drop-down list, then select **Enable**. Click **Save** to retain this setting.

### 4.6.4 IP Address Filter

The IP Address Filter feature allows you to either restrict direct access to the camera from a browser to specific IP addresses (**Allowed**) or block specific access from specific IP addresses (**Forbidden**).

To open the IP Address Filter menu, go to **Setup** tab | **Security** | **IP Address Filter**.

To use this menu:

1. Check the **Enable IP Address Filter** box.

2. In the IP Address Filter Type field, open the drop-down list and select either:
   - **Allowed**: To enable clients at only specific at IP address to access the camera.
SECTION 4: CAMERA SETUP MENUS

Forbidden: To block clients from specific IP addresses to access the camera.

3. Click Add.

4. In the pop-up menu (see above), enter the IP address of the client computer to identify, then click OK.

5. Repeat the above two steps for each IP address that apply to the filter type you selected.

6. Click Save to retain your settings.

To delete an IP address you entered

Click (highlight) the IP address in the list that you want to delete, then click Delete. To delete all IP address you entered, click Clear.

To modify an IP address you entered

1. Click (highlight) the IP address in the list that you want to modify, then click Modify.

2. In the pop-up window, edit the IP address as needed.

3. Click OK to save the new address.
4.6.5 Security Service

To Security Service menu can be used to enable the remote login and improve the data communication security.

To open the Security Service menu, go to Setup tab | Security | Security Service.

1. Check the box of **Enable SSH** if needed. SSH improves data communication security

2. Check the box of **Enable Illegal Login Lock** if needed. This feature will lockout the IP address of the admin user who performs 7 failed user name / password attempts, or an operator user who performs 5 failed user name / password login attempts. The IP address is locked for 30 minutes.

3. Click **Save** to retain your settings.

4.7 Standard Events menus

4.7.1 Motion Detection

Normally, motion detection recording is performed by an NVR or VMS device that monitors the video stream from the camera and is configured to record when motion is sensed. However, for configurations where the camera is not monitored by an NVR or VMS, it can be configured to perform motion detection and write video segments, capture data and log data directly to an online storage device such as a NAS (Network Attached Storage). Use this menu to perform motion detection recording when the video segments and other data is saved to an online storage device.

To open the Motion Detection menu, go to Setup tab | Standard Event | Motion Detection.
To use motion detection recording:

1. Check either or both boxes for **Enable Motion Detection** or **Enable Dynamic Analysis for Motion**. **Enable Dynamic Analysis for Motion** highlights the cells where motion is detected with green rectangles in the Live View image.

2. The area of the image where motion is sensed is indicated by a red grid. For efficient utilization of the processor in the camera, select only the area of the image where motion should be sensed:
   a. Click **Clear All** to reset the motion detection area.
   b. Click **Draw Area**.
c. Using the mouse, drag a rectangle across the area of the image where you want to sense for motion. You can select multiple areas.

d. Click **Stop Drawing** when finished.

e. Move the Sensitivity slider left or right to reduce or increase the sensitivity for motion detection. (Usually, this adjustment is performed later when it is better understood how the camera responds to motion sensing.) When the camera senses motion in a grid cell, it fills the cell with red.

3. In the **Arming Schedule** section of the window, click the **Edit** button.

4. In the **Edit Schedule Time** window, you can arm the camera for eight periods of motion detection sensing for every day of the week. Click the Start and End Time for a day and period, then edit the field for that time. Note that periods cannot overlap.
In the example above, one period was setup for Monday, then copied to every other day of the week.

5. When finished setting up the schedule, click **OK**. The Arming schedule configured above is shown in the screen. Below.

![Arming Schedule](image)

For the Arming Schedule to be applied correctly:

— The clock in the camera must be set. See “4.1.2 Time Settings” on page 22 for more information.
— The **Record Schedule** of the Storage device must be configured. See “4.7.1 Record Schedule” on page 51.

6. If you want to send an email or perform another linkage action when motion is detected, check the appropriate box(es) in the **Linkage Method** list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

7. Click **Save** to retain your settings.

### 4.7.2 Video Tampering

The Video Tampering feature is used to configure the camera to generate an alarm when the lens is covered. To configure video tampering, you must designate an area that is sensed for video tampering, then setup a schedule when the camera senses for that condition.

To open the Video Tampering menu, go to **Setup** tab | **Standard Event** | **Video Tampering**.
1. Check the **Enable Video Tampering** box.

2. Click **Draw Area**.

3. Using the mouse, drag a rectangle across the area of the image where you want to sense for video tampering. After drawing the rectangle, you can reposition it with the mouse.

4. Click **Stop Drawing**.
5. In the **Arming Schedule** section of the window, click the **Edit** button. The **Edit Schedule Time** window will open.

![Edit Schedule Time Window](image)

6. In the **Edit Schedule Time** window, you can arm the camera for eight periods of tamper detection sensing for every day of the week. Click the Start and End Time for a day and period, then edit the field for then time. Note that periods cannot overlap.

In the example above, one period was setup for Monday, then copied to every other day of the week.

7. When finished setting up the schedule, click **OK**. The Arming schedule configured above is shown in the screen below.
For the Arming Schedule to be applied correctly:

— The clock in the camera must be set. See “4.1.2 Time Settings” on page 22 for more information.
— The Record Schedule of the Storage device must be configured. See “4.7.1 Record Schedule” on page 51.

8. If you want to send an email or select another linkage action when tampering is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) must also be setup.

9. Click Save to retain your settings.

4.7.3 Alarm Input

The Alarm Input feature is used to configure the camera to generate an alarm when a state change is detected on the camera alarm input terminals. The alarm input terminals can be configured for Normally Open (NO) or Normally Closed (NC). The alarm is armed only when enabled in the Arming Schedule.

When an input alarm is sensed when enabled in the Arming Schedule, the camera can send an email alert or upload the alarm information to an FTP server, if selected in the menu.

To open the Alarm Input menu, go to Setup tab | Standard Event | Alarm Input.
1. In the Alarm Input menu, open the drop Alarm Input No. drop down list and select the alarm input you want to configure.

2. In the Alarm Name field, enter a descriptive name for the alarm.

3. In the Alarm Type field, select either NC (for normally closed alarm sensor) or NO (for a normally open alarm sensor).

4. Check the box(es) for the Linkage Method you prefer to use when the alarm occurs, if needed.

5. For cameras with multiple alarm inputs, you can copy the configuration you setup for this alarm input to other alarm inputs by checking the appropriate boxes in the Copy to Alarm section.

6. In the Arming Schedule section of the window, click the Edit button.
SECTION 4: CAMERA SETUP MENUS

7. In the **Edit Schedule Time** window, you can arm the camera for eight periods of motion detection sensing for every day of the week. Click the Start and End Time for a day and period, then edit the field for then time. Note that periods cannot overlap.

   In the example above, one period was setup for Monday, then copied to every other day of the week.

8. When finished setting up the schedule, click **OK**. The Arming schedule configured above is shown in the screen below.

   For the Arming Schedule to be applied correctly:
   - The clock in the camera must be set. See "4.1.2 Time Settings" on page 22 for more information.
SECTION 4: CAMERA SETUP MENUS

— The Record Schedule of the Storage device must be configured. See “4.9.1 Record Schedule” on page 80.

9. If you want to send an email or perform other actions when an alarm input is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

10. In the Copy to alarm frame, select the options you prefer. Depending on the camera, options may or may not be selectable.

11. Click **Save** to retain your settings.

4.7.4 Alarm Output

The Alarm Output feature is used to configure the camera to generate an alarm output when an alarm input occurs during its Arming Schedule.

To open the Alarm Output menu, go to **Setup tab | Standard Event | Alarm Output**.

1. In the Alarm Output menu, open the drop Alarm Output drop down list and select the alarm output you want to configure.

2. In the Alarm Name field, enter a descriptive name for the alarm.
SECTION 4: CAMERA SETUP MENUS

3. In the **Delay** field, open the drop down list and select duration of the alarm output is active. You can select either 5, 10, or 30 seconds, 1, 2, 5, or 10 minutes, or Manual.

4. For cameras with multiple alarm outputs, you can copy the configuration you setup for this alarm output to other alarm outputs by checking the appropriate boxes in the **Copy to Alarm** section.

5. In the **Arming Schedule** section of the window, click the **Edit** button.

![Edit Arming Schedule](image)

6. In the **Edit Schedule Time** window, you can arm the camera for eight periods of motion detection sensing for every day of the week. Click the Start and End Time for a day and period, then edit the field for then time. **Periods cannot overlap.**

   In the example above, one period was setup for Monday, then copied to every other day of the week.

7. When finished setting up the schedule, click **OK**. The Arming schedule configured above is shown in the screen below.
For the Arming Schedule to be applied correctly:

— The clock in the camera must be set. See “4.1.2 Time Settings” on page 22 for more information.
— The Record Schedule of the Storage device must be configured. See “4.9.1 Record Schedule” on page 80.

8. In the Copy to Alarm frame, select the options you prefer. Depending on the camera, options may or may not be selectable.

9. Click Save to retain your settings.

**4.7.5 Exception**

Exception types are certain abnormal events that are sensed by the camera. Abnormal events can include:

- HDD Full
- HDD Error
- Network Disconnected
- IP Address Conflicted
- Illegal Login

When these events occur, the camera can send an Email alert or notify the Surveillance Center indicating that some maintenance action may be required. The exception types are shown in the screen below. **NOTE:** To use this feature, the Email configuration must be setup. See “4.2.9 Email” on page 37 for more information.
To open the Exception menu, go to **Setup tab** | **Standard Event** | **Exception**.

1. In the Exception menu, open the Exception Type drop-down list and select the condition you want to be informed of.
2. Check the **Send Email** box.
3. Click **Save**.
4. Repeat the steps above for other exception types you want to be informed of.

### 4.8 VCA Event

VCA (Video Content Analytics) are software features in the camera that analyze motion in the field of view. Your Alibi camera may include one or more of the following VCA types:

- **Audio Exception Detection**: Audio exception detection determines when abnormal sounds occur in the vicinity of the camera. These abnormalities can include a sudden increase or decrease of the sound intensity. When these events occur, an alarm is generated and linkage actions can be performed.

- **Face Detection**: Face detection determines when a face appears in the field of view. When these events, an alarm is generated and linkage actions can be performed.

- **Line Crossing Detection**: An event that results when an object moves from one side of a virtual plane in the field of view to the other side.

- **Intrusion Detection**: An event that results when an object enters a virtual region of the field of view. The region may be bounded by a triangle or quadrangle region.

- **Region Entrance Detection**: Region entrance detection determines when people, vehicles or other objects enter a pre-defined virtual region in the field of view. When these events occurs, an alarm is generated and linkage actions can be performed.

- **Region Exiting Detection**: Region exiting detection determines when people, vehicles or other objects leave a pre-defined virtual region in the field of view. When these events occurs, an alarm is generated and linkage actions can be performed.
When these VCA events are configured and an event occurs, an alarm status is recorded by the camera. Some Alibi video recorders can be configured to sense these alarms to trigger video recording and perform linkage actions. Refer to the VCA features of those recorders for more information.

**4.8.1 Audio Exception Detection**

Audio exception detection determines when abnormal sounds occur in the vicinity of the camera. These abnormalities can include a sudden increase or decrease of the sound intensity. When these events occurs, an alarm is generated and linkage actions can be performed.

1. Open the Audio Exception Detection menu. Go to Setup | VCA Events | Audio Exception Detection.

2. Check the Audio Loss Exception box to detect a loss of audio from the camera.
3. Check the **Sudden Increase of Sound Intensity Detection** box to detect a steep rise in the sound level near the camera microphone. You can set the detection sensitivity and threshold for the steep sound rise. Use the **Real-time Volume** display to view the relative sound level from the microphone.

   a. If you selected this option, set the drag the **Sensitivity** slider to produce the best result as follows: The smaller the sensitivity value, the more severe the change should be to trigger the detection. Sensitivity can range from 1 .. 100.

   b. If you selected this option, **Sound Intensity Threshold** slider to produce the best result as follows: The adjustment is used to filter the sound in the environment. The louder the sound in the environment, the higher the value should be. Sound intensity threshold can range from 1 .. 100.

4. Check **Sudden Decrease of Sound Intensity Detection** box to detect the steep drop in the sound level near the camera microphone. You can set the detection sensitivity and threshold for the steep sound drop. Use the **Real-time Volume** display to view the relative sound level from the microphone.

   a. If you selected this option, set the drag the **Sensitivity** slider to produce the best result as follows: The smaller the sensitivity value, the more severe the change should be to trigger the detection.

5. By default, Audio Exception Detection when enabled is continuously armed. To change the arming schedule, click the **Edit** button above the schedule graphic. In the **Edit Schedule Time** window, click on a field or tab to change the value. You can select up to 8 armed periods for each weekday. **Periods cannot overlap.**

   ![Edit Schedule Time](image)

   In the example above, one period was setup for Monday, and then copied to every other day of the week.

6. When finished setting up the schedule, click **OK**. The new Arming schedule will be shown in the menu.

7. If you want to send an email, or perform other actions when an Audio Exception is detected, check the appropriate box(es) in the **Linkage Method** list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.
8. Click **Save** to retain your settings.

### 4.8.2 Face Detection

Face detection determines when a face appears in the field of view. When these events, an alarm is generated and linkage actions can be performed.

1. Open the Audio Exception Detection menu. Go to **Setup | VCA Events | Face Detection**.

2. Check the **Enable Face Detection** box to enable this function.

3. Check the **Enable Dynamic Analysis for Face Detection** box to mark faces detected on live video with a green rectangle.
   a. If you selected this feature, also enable the **Rules** option on the **Local Configuration | Local Setup | Live View Parameters** menu.

4. Click-and-drag the slider **Sensitivity** bar to set the detection sensitivity. The higher the value is, the more easily the face can be detected. Sensitivity can range from 1 .. 5.
5. By default, Face Detection when enabled is continuously armed. To change the arming schedule, click the Edit button above the schedule graphic. In the Edit Schedule Time window, click on a field or tab to change the value. You can select up to 8 armed periods for each weekday. Periods cannot overlap.

![Edit Schedule Time](image)

In the example above, one period was setup for Monday, and then copied to every other day of the week.

6. When finished setting up the schedule, click OK. The new Arming schedule will be shown in the menu.

7. If you want to send an email, or perform other actions when a face is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

8. Click Save to retain your settings.

### 4.8.3 Line Crossing Detection

The Line Crossing Detection enables you to configure a virtual plane in the camera and detect objects that move through the plane. The plane is identified with an A side and a B side. You can configure the feature to report an event when objects move through the plane from A to B (A → B), from B to A (B → A), or from either A to B or B to A (A ↔ B). Also, you can set the sensitivity of the detection, and the weekly time period during which these events are sensed. Traverse Virtual Plane events are reported in the camera log, and can be used to trigger event recording. You can configure up to four virtual planes the camera.

To use the Line Crossing Detection feature:

1. Open the Line Crossing Detection menu. Go to Setup | VCA Events | Line Crossing Detection.
2. Check the **Enable Line Crossing Detection** box.

3. Open the drop down list on the Line entry, and select a number for the virtual plane you want to create. You can form up to 4 virtual planes on one video image.

4. Click on the yellow line in the image. “Handles” will appear at both ends of the line. Drag the handles to where the plane should begin and end in the image.
5. Click the **Direction** drop down list and select either A → B, B → A, or A↔B.

6. Set the **Sensitivity** slider as needed. To do that, move some objects through the plane, then monitor the log to verify they were detected. If they weren’t, increase the sensitivity, and try again.

7. To add up to four line crossing virtual planes to the image. Open the **Line** drop down list, select a unused plane number, and then repeat steps 3 through 6 above to configure an additional plane.

8. By default, virtual plane when enabled is continuously armed. To change the arming schedule, click the **Edit** button above the schedule graphic. In the **Edit Schedule Time** window, click on a field or tab to change the value. You can select up to 8 armed periods for each weekday. **Periods cannot overlap.**
In the example above, one period was setup for Monday, then copied to every other day of the week.

9. When finished setting up the schedule, click OK. The new Arming schedule will be shown in the menu.

10. If you want to send an email or perform other actions when a line crossing event is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

11. Click Save to retain your settings.

### 4.8.4 Intrusion Detection

The Intrusion Detection feature enables you to define a region of the image where objects intruding into that space are sensed and reported as events. You can configure up to four intrusion detection regions in the camera. Also, you can set the threshold, sensitivity, and percentage of the region to trigger detection, and configure an arming schedule for detection of these events.

To use the Intrusion Detection feature:

1. Open the Intrusion Detection menu. Go to Setup | VCA Events | Intrusion Detection.
2. Check the **Enable Intrusion Detection** box.

3. Click the **Draw Area** button.

4. Click a spot in the image where a corner of the detection area should exists, then click the on three other corners in a circular fashion to form a yellow three- or four-sided bounding box. Right click anywhere else to close the bounding box to a three- or four-sided region.
5. Set the **Threshold**, **Sensitivity**, and **Percentage** as needed to detect an intrusion. To check your settings, move some object into the intrusion area, and then monitor the log to verify that it was detected. If it wasn’t, adjust the parameters as needed and try again.

6. To add an additional (up to four) **Intrusion Detection** region to the image, open the **Region** drop down list, select a unused plane number, and then repeat steps 3 through 5 above to configure an additional region. If not, continue with the next step.

7. By default, Intrusion Detection when enabled is continuously armed. To change the arming schedule, click the **Edit** button above the schedule graphic. In the **Edit Schedule Time** window, click on a field or tab to change the value. You can select up to 8 armed periods for each weekday. **Periods cannot overlap.**
In the example above, one period was setup for Monday, and then copied to every other day of the week.

8. When finished setting up the schedule, click OK. The new Arming schedule will be shown in the menu.

9. If you want to send an email or perform other actions when an intrusion is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

10. Click Save to retain your settings.

### 4.8.5 Region Entrance Detection

Region entrance detection determines when people, vehicles or other objects enter a pre-defined virtual region in the field of view. When these events occurs, an alarm is generated and linkage actions can be performed.

1. Open the Region Entrance Detection menu. Go to Setup | VCA Events | Region Entrance Detection.
2. Check the **Enable Region Entrance Detection** box of to enable the function.

3. On the **Region** line, select a region number from the drop-down.

4. Click the **Draw Area** button to start the region drawing.

5. Click a spot in the image where a corner of the detection area should exists, then click the on three other corners in a circular fashion to form a yellow four-sided bounding box. Right click anywhere else to close the bounding box to a four-sided region.

6. Open the **Detection Tar...** dropdown list, and then select either All, Human or Vehicle to set the detection sensitivity.
7. Repeat the above steps to configure other regions. You can create up to four regions. Use the Clear button to clear pre-defined regions.

8. By default, Region Entrance Detection when enabled is continuously armed. To change the arming schedule, click the Edit button above the schedule graphic. In the Edit Schedule Time window, click on a field or tab to change the value. You can select up to 8 armed periods for each weekday. Periods cannot overlap.

![Edit Schedule Time](image)

In the example above, one period was setup for Monday, and then copied to every other day of the week.

9. When finished setting up the schedule, click OK. The new Arming schedule will be shown in the menu.

10. If you want to send an email, or perform other actions when an region entrance is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

11. Click Save to retain your settings.

### 4.8.6 Region Exiting Detection

Region exiting detection determines when people, vehicles or other objects leave a pre-defined virtual region in the field of view. When these events occurs, an alarm is generated and linkage actions can be performed.

1. Open the Region Exiting Detection menu. Go to Setup | VCA Events | Region Exiting Detection.
2. Check the **Enable Region Exiting Detection** box of to enable the function.

3. On the **Region** line, select a region number from the drop-down.

4. Click the **Draw Area** button to start the region drawing.

5. Click a spot in the image where a corner of the detection area should exists, then click the on three other corners in a circular fashion to form a yellow four-sided bounding box. Right click anywhere else to close the bounding box to a four-sided region.

6. Open the **Detection Tar... (-get)** drop down list, and then select either All, Human or Vehicle to set the detection sensitivity.
7. Repeat the above steps to configure other regions. You can create up to four regions. Use the Clear button to clear all pre-defined regions.

8. By default, Region Exiting Detection when enabled is continuously armed. To change the arming schedule, click the Edit button above the schedule graphic. In the Edit Schedule Time window, click on a field or tab to change the value. You can select up to 8 armed periods for each weekday. Periods cannot overlap.

![Edit Schedule Time](image)

In the example above, one period was setup for Monday, and then copied to every other day of the week.

9. When finished setting up the schedule, click OK. The new Arming schedule will be shown in the menu.

10. If you want to send an email, or perform other actions when an region exit is detected, check the appropriate box(es) in the Linkage Method list. Note that the Email configuration (see “4.2.9 Email” on page 37) and FTP server configuration (see “4.2.7 FTP” on page 35) must also be setup.

11. Click Save to retain your settings.

### 4.9 Storage menus

#### 4.9.1 Record Schedule

The Recording Schedule feature configures the camera to record video either continuously, when motion detection occurs, when an alarm occurs, or when motion detection and/or an alarm occurs. Also, the camera can be configured to the time before and/or the time after any recording event is scheduled.

To open the Record Schedule menu, go to Setup tab | Storage | Record Schedule
12. In the record schedule menu:
   
a. Open the **Pre-record** drop-down list and select your preferred pre-record time. Pre-record time is the time you set to start recording before the scheduled time or 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 at 9:59:55.

b. Open the **Post-record** drop-down list and select your preferred post-record time. Post-record time is the time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

c. Open the **Overwrite** drop-down list and select **Yes** or **No**. Overwrite is the action taken when the storage device is full. If you select Yes, the oldest files on the disk are overwritten with the newest data.

13. Check the **Enable Record Schedule** box.

14. Click **Edit** to open the **Edit Schedule** window will open. In the Edit Schedule window, you can select up to 8 periods for each weekday when different kinds of recording will occur. The periods you select cannot overlap.
15. To edit the record schedule:
   
a. Click the tab for the day of the week you want to schedule.

b. Select the bullet for All Day or Customize.

   i. If you selected All Day, open the drop-down list and select the kind of recording you want to perform.

   ii. If you selected Customize, click the Start Time field for Period 1, then enter the start time hours and minutes. Repeat for the End Time field, then in the Record Type column, open the drop-down list and select the recording type for this period. Repeat this step for other periods for the day, if needed.

   **NOTE**
   
   When configuring Storage for Motion or Events, you must also select (click) Trigger Channel under the specific Event you are using. For instance, if using Motion (as shown), you must also go to Motion Detection and click Trigger Channel to ensure event triggers are recognized for recording to the microSD or NAS device. If you set the schedule and don’t select Trigger Channel, the camera will not record due to events to the mapped storage.

   c. If you want to copy the schedule of the day you configured to other days, check the boxes for the days you want to copy the schedule to, then click Copy.

   d. Repeat steps a through c above, if needed.

   e. Click OK to save the schedule you established.
In the schedule shown above, the Record Schedule was setup by clicking All Day, Motion Detection (from the drop-down list), Copy to Week checkbox, Copy button, OK button.

16. In the Record Schedule window, click Save.

4.9.2 Storage Management

In the Storage Management menu, you can prepare external storage for use (Format), and set the percentages of Pictures (Captures) and Video recordings across the storage device. This menu is only useful after you configured an external storage device (NAS NFS or SMB/CIFS) to save video data and captures.

To open the Storage Management menu, go to Setup tab | Storage | Storage Management.
SECTION 4: CAMERA SETUP MENUS

1. Check the box for the HDD you want to configure.

   **NOTE** If the Status of the HDD is **Offline**, the HDD is not recognized. Check the settings on the NAS menu. See “4.9.3 NAS” on page 93.

2. In the HDD Device List, if the **Status** external storage device (HDD) you added shows an **Uninitialized** status:
   
   a. Click the **Format** button to format the HDD. Format performs a full format of the HDD (erases all data from the disk).

   b. Wait until Format completes before continuing. When Format completes, the HDD status will change to **Normal**.

3. Edit the percentages of the HDD allocated for **Picture** and **Record** data as needed.

4. Click **Save**.

4.9.3 NAS

Use the NAS (Network Attached Storage) menu to identify network storage devices the camera or recorder will use to save video and capture data. One of two different NAS menu screens may appear, depending on the model of the IP camera or recorder. One type (most common) allows you to add a regular NAS device from the network (see “A” below); the other type allows you to add a NAS as a NFS (Network File Server) or a SMB/CIFS (Server Message Block / Common Internet File System) device (see “B” below). SMB/CIFS requires user authentication. With either type of NAS, the device must be properly initialized (formatted) by the Alibi software before it can be used (see “4.9.2 Storage Management” on page 92 on page 68 for more information).
To open the NAS menu, go to Setup tab | Storage | NAS.

1. To add a NAS device using the screen shown above:
   a. Click an unused HDD No. in the list (see below).

   ![Image of NAS menu setup screen]

   b. Enter the Server Address (IP address of the server), the File Path in the entry fields.
   c. In the Mounting Type drop-down list, select either NFS or SMB/CIFS (for the device type you want to add).
   d. If you select SMB/CIFS in the type field, enter the User Name and Password for the device. See below.

   ![Image of NAS menu setup screen]

   e. Click Test to verify the settings.

2. Click Save.
4.9.4 Snapshot

Use the Snapshot menu to configure periodic and event-triggered screen captures of video from the camera. Screen captures are saved to the storage device configured in the Storage Management menu (see “4.9.2 Storage Management” on page 92). Snapshots can be downloaded using the camera Remote Access Playback features (see “3.3 Playback screen” on page 15).

To open the Snapshot menu, go to Setup tab | Storage | Snapshot.

1. To enable a Timing snapshot (snapshots are taken after every interval of time and saved):
   a. Check the Enable Timing Snapshot box.
   b. Open the Quality drop-down list and select either Low, Medium or High.
   c. Select the Interval (time between snapshots). The Interval can be in milliseconds (default), seconds, minutes, or days.
   d. Click Save.

2. To enable an Event-Triggered snapshot (snapshots are when an event, such as Motion Detection occurs):
SECTION 4: CAMERA SETUP MENUS

a. Check the Enable Event-Triggered Snapshot box.

b. Open the Quality drop-down list and select either Low, Medium or High.

c. Select the Interval (time between snapshots). The Interval range can be 1000 ms ~ 65535 ms.

3. Click Edit to open the Edit Schedule window will open. In the Edit Schedule window, you can select up to 8 periods for each weekday when snapshots will occur. The periods you select cannot overlap.

![Edit Schedule Window]

a. Click the Start and End Time for a day and period, then edit the field for the time. Periods cannot overlap.

b. Use the Copy feature to copy the schedule to other days of the week. In the example above, one period was setup for Monday, then copied to every other day of the week.

4. When finished setting up the schedule, click OK. The Arming schedule configured above is shown in the screen below.
5. Click **Save**.