



**Blazer Pro All-in-One Server  
Quick Start Guide**

## **Quick Start Guide**

COPYRIGHT ©2017 Hangzhou Hikvision Digital Technology Co., Ltd.

### **ALL RIGHTS RESERVED.**

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

### **About this Manual**

This Manual is applicable to Blazer Pro All-in-One Server.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only.

The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

### **Trademarks Acknowledgement**

**HIKVISION** and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

### **Legal Disclaimer**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER

ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

## Regulatory Information

### FCC Information

**FCC compliance:** 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. 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.

### EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: [www.recyclethis.info](http://www.recyclethis.info)



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: [www.recyclethis.info](http://www.recyclethis.info)

### Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.



## Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into “Warnings” and “Cautions”

**Warnings:** Serious injury or death may occur if any of the warnings are neglected.

**Cautions:** Injury or equipment damage may occur if any of the cautions are neglected.

|   |  |
|---|--|
|  |        |
| <b>Warnings</b> Follow these safeguards to prevent serious injury or death.       | <b>Cautions</b> Follow these precautions to prevent potential injury or material damage. |



### Warnings

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC, 48 VDC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

## Preventive and Cautionary Tips


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

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. 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 UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

## Symbol Conventions

The symbols that may be found in this document are defined as follows.

| Symbol  | Description   |
|---|---|
|  | Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results. |

# CONTENTS

|   |           |
|---|-----------|
| <b>1. Overview.....</b>                               | <b>3</b>  |
| <b>2. Blazer Pro Pre-Installation.....</b>            | <b>3</b>  |
| <b>3. Blazer Pro Installation .....</b>               | <b>3</b>  |
| <b>4. Front Panel.....</b>                            | <b>4</b>  |
| <b>5. Rear Panel.....</b>                             | <b>5</b>  |
| <b>6. HDD Storage Calculation Chart .....</b>         | <b>6</b>  |
| <b>7. Basic Hardware Connection and Startup .....</b> | <b>7</b>  |
| 7.1 Network Connection.....                           | 7         |
| 7.2 Output Connection .....                           | 7         |
| 7.3 Hard Disk Installation .....                      | 7         |
| 7.3.1 Installing HDD in Storage Board.....            | 7         |
| 7.3.2 Installing HDD in Server Board .....            | 9         |
| 7.4 Peripheral Connections.....                       | 10        |
| 7.4.1 Wiring of Alarm Input .....                     | 10        |
| 7.4.2 Wiring of Alarm Output.....                     | 11        |
| 7.4.3 Using of Alarm Connectors .....                 | 11        |
| 7.4.4 Controller Connection.....                      | 11        |
| 7.5 Power Connection and Startup .....                | 12        |
| <b>8. Accessing Blazer Pro Storage Board .....</b>    | <b>13</b> |
| 8.1 Activating Storage Board .....                    | 13        |
| 8.2 Using Unlock Pattern for Login .....              | 13        |
| 8.3 Setup Wizard .....                                | 14        |
| 8.4 Network Settings .....                            | 14        |
| 8.5 Adding Network Cameras .....                      | 15        |
| <b>9. Quick Start.....</b>                            | <b>16</b> |
| 9.1 Accessing Blazer Pro via Web Client .....         | 16        |
| 9.2 Resource Management .....                         | 17        |
| 9.2.1 Adding Storage Board as Encoding Device.....    | 17        |
| 9.2.2 Area Management.....                            | 19        |
| 9.3 Live View .....                                   | 20        |
| 9.3.1 Login the Control Client .....                  | 20        |
| 9.3.2 Live View.....                                  | 21        |
| 9.4 Recording Schedule Settings.....                  | 21        |
| 9.5 Playback .....                                    | 22        |
| 9.5.1 Searching Video Files for Playback.....         | 22        |
| 9.5.2 Playing Video Files.....                        | 22        |

|  |           |
|--|-----------|
| 9.6 Event and Alarm Configuration .....        | 22        |
| 9.6.1 Configuring Motion Detection Event ..... | 23        |
| 9.6.2 Configuring Motion Detection Alarm ..... | 23        |
| 9.6.3 Checking Event Logs .....                | 24        |
| <b>10. Shutting Down Blazer Pro.....</b>       | <b>25</b> |



## 1. Overview

The Blazer Pro is an all-in-one server that combines Hikvision's powerful video management system HikCentral (on Server Board) with a video storage device (Blazer Pro Storage Board). The Blazer Pro can manage up to 256 network cameras (for Blazer Pro/256/16H) or 128 network cameras (for Blazer Pro/128/16H) for recording, live view, and playback. With the power of VMS, sophisticated alarm management is possible, as well as central management, information sharing, convenient connection and multi-service cooperation. The Blazer Pro's unique design provides both powerful storage and advanced centralized video management capabilities.

**Note:** We strongly recommend that you do NOT install any other software or program on the Blazer Pro to insure its performance and reliability.

## 2. Blazer Pro Pre-Installation

The Blazer Pro is highly advanced surveillance equipment that should be installed with care. Please take into consideration the following precautionary steps before installation of the Blazer Pro.

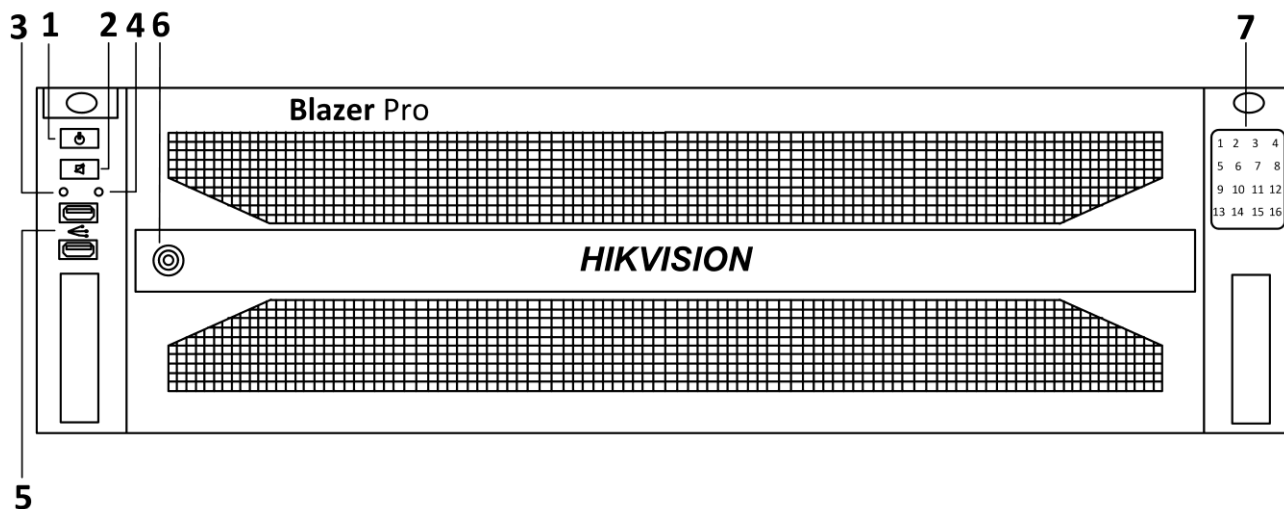
1. Keep all liquids away from the Blazer Pro.
2. Install the Blazer Pro in a well-ventilated and dust-free area.
3. Ensure environmental conditions meet factory specifications.
4. Install a manufacturer recommended HDD.

## 3. Blazer Pro Installation

During the installation of the Blazer Pro:

1. Use brackets for rack mounting.
2. Ensure there is ample room for audio and video cables.
3. When routing cables, ensure that the bend radius of the cables are no less than five times than its diameter.
4. Connect both the alarm and RS-485 cable.
5. Allow at least 2cm ( $\approx 0.75$ -inch) of space between racks mounted devices.
6. Ensure the Blazer Pro is grounded.
7. Environmental temperature should be within the range of 0 °C to +40 °C, 32 °F to 104 °F.
8. Environmental humidity should be within the range of 10% ~ 90%.

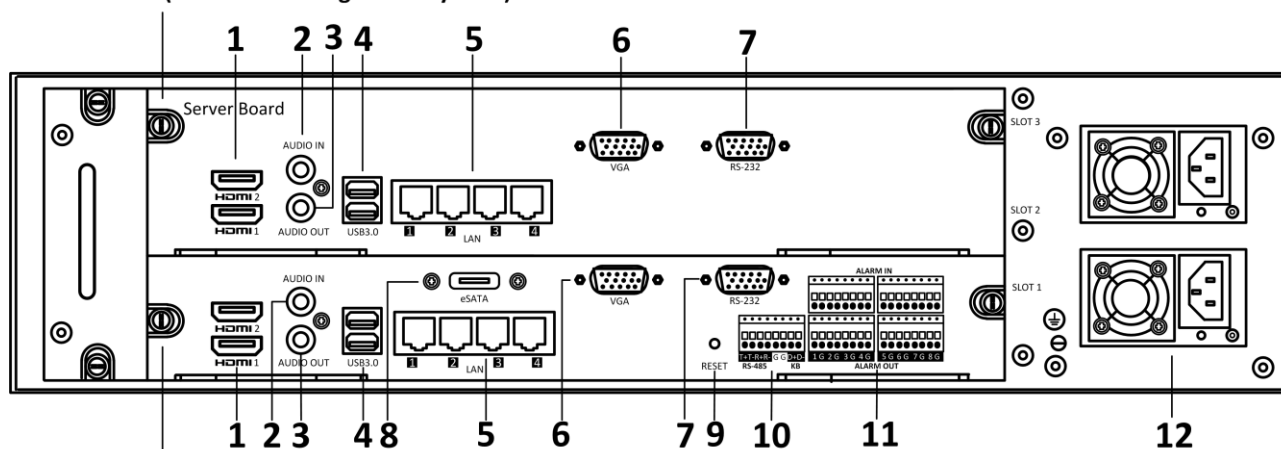
## 4. Front Panel



| No. | Name   | Function Description   |
|-----|--|--|
| 1   | <b>POWER ON/OFF</b>                          | Power on/off device.<br><ul style="list-style-type: none"> <li>● Solid blue: device is running.</li> <li>● Solid red: device is shut down.</li> </ul>                                      |
| 2   | <b>Muting Switch</b>                         | Turn on/off buzzer.<br><ul style="list-style-type: none"> <li>● Solid blue: buzzer is turned off.</li> <li>● Unlit: buzzer is turned on.</li> </ul>  |
| 3   | <b>HDD Status Indicator</b>                  | <ul style="list-style-type: none"> <li>● Solid red: at least one HDD is installed</li> <li>● Unlit: no HDD is detected.</li> <li>● Blinking red: HDD is reading/writing.</li> </ul>        |
| 4   | <b>Tx/Rx Status Indicator</b>                | Blinking blue: network communication is normal.  |
| 5   | <b>USB Interfaces<br/>(for Server Board)</b> | 2 USB 2.0 interfaces to connect additional devices such as USB mouse and USB keyboard for server board.<br><b>Note:</b> Connect USB devices like USB drive to USB interface in rear panel. |
| 6   | <b>Front Panel Lock</b>                      | You can lock or unlock the panel by the key.   |
| 7   | <b>HDD Sequence Indicator</b>                | Show the HDD installation slot.  |

## 5. Rear Panel

Server Board (for Video Management System)



Storage Board (for Blazer Pro Storage Device)

| No. | Name                              | Function Description   |
|-----|-----------------------------------|--|
| 1   | <b>HDMI™ Interfaces</b>           | HDMI™ video output connector.                                  |
| 2   | <b>AUDIO OUT</b>                  | RCA connector for audio output.                                |
| 3   | <b>AUDIO IN</b>                   | RCA connector for audio input.                                 |
| 4   | <b>USB 3.0 Interfaces</b>         | USB 3.0 ports for additional devices such as USB HDD.          |
| 5   | <b>LAN Network Interfaces</b>     | LAN network interfaces.  |
| 6   | <b>VGA Interface</b>              | Connector for VGA output. Display local video output and menu. |
| 7   | <b>RS-232 Serial Interface</b>    | Connector for RS-232 devices.                                  |
| 8   | <b>eSATA Interface</b>            | eSATA interface for external HDD.                              |
| 9   | <b>Reset Button</b>               | Reset the Blazer Pro Storage Board.                            |
| 10  | <b>RS-485 Serial Interface</b>    | Connector for RS-485 devices.                                  |
| 11  | <b>ALARM IN and ALARM OUT</b>     | Connector for alarm input and alarm output.                    |
| 12  | <b>100 to 240 VAC Power Input</b> | AC 100V ~ 240V power supply.                                   |

## 6. HDD Storage Calculation Chart

The following chart shows an estimation of storage space used based on recording at one camera for an hour at a fixed bit rate.

| Bit Rate | Storage Used |
|----------|--------------|
| 96 K     | 42 MB        |
| 128K     | 56 MB        |
| 160K     | 70 MB        |
| 192K     | 84 MB        |
| 224K     | 98 MB        |
| 256K     | 112 MB       |
| 320K     | 140 MB       |
| 384K     | 168 MB       |
| 448K     | 196 MB       |
| 512K     | 225 MB       |
| 640K     | 281 MB       |
| 768K     | 337 MB       |
| 896K     | 393 MB       |
| 1024K    | 450 MB       |
| 1280K    | 562 MB       |
| 1536K    | 675 MB       |
| 1792K    | 787 MB       |
| 2048K    | 900 MB       |
| 4096K    | 1800 MB      |
| 8192K    | 3600 MB      |
| 16384K   | 7.2 GB       |

**Note:** Please note that supplied values for storage space used is just for reference. The storage values in the chart are estimated by formulas and may have some deviation from actual value.

## 7. Basic Hardware Connection and Startup

Before you can access the system via network, you need to properly power on the server and connect it to network.

### 7.1 Network Connection

**Note:** Consult your network administrator before installing the server to avoid possible network conflicts.

Use the network port on the rear panel and a network cable with RJ-45 connectors to connect the server to your system network.

The LAN interfaces of the server board (up) are used for connecting the video management system to the network, and the LAN interfaces of the storage board (down) are used for connecting the Blazer Pro Storage Board to the network.

For the LAN interface of the storage board (down), the default IP address is 192.168.1.64.

### 7.2 Output Connection

Connect a VGA cable or HDMI cable to the video out interface (VGA or HDMI) on the server.

Connect the VGA cable or HDMI cable to the display unit.

If you need to locally operate the video management system and Blazer Pro Storage Board, please connect the display units to the server board and storage board respectively.

### 7.3 Hard Disk Installation

**Before you start:**

Disconnect the power from the Blazer Pro before installing a hard disk drive (HDD). A factory recommended HDD should be used for this installation.

**Tools Required:** Screwdriver.

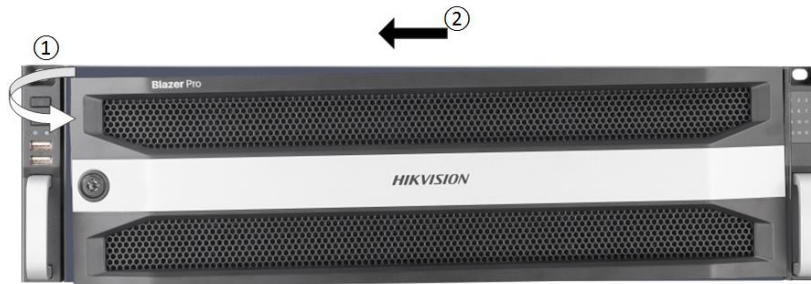
#### 7.3.1 Installing HDD in Storage Board

**Note:** The device appearance is subject to actuality.

**Steps:**

1. Unlock the bezel with the delivered key.
2. To remove the bezel from front panel, operate following steps:
  - 1) Slightly pull the bezel out of the device along the direction arrow ① and make it a little above the left mounting ear. The angle between the bezel and the front panel must be within 10°.
  - 2) Pull the bezel out of the device along the direction arrow ②.

**Note:** Handle with care to avoid damage.



3. Press the blue button to pop up the handle, hold the handle, and pull the HDD tray out of the slot.



4. Fix the HDD in the HDD tray.
  - 1) Place an HDD in the HDD tray. The SATA interface must face the HDD tray bottom.
  - 2) Adjust the HDD position. Ensure the HDD screw holes aligning with tray screw holes.
  - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.



5. Push the HDD tray back into the slot.



6. To fix the HDD tray, press the handle until you hear a click. Repeat above steps to install the rest HDD trays.



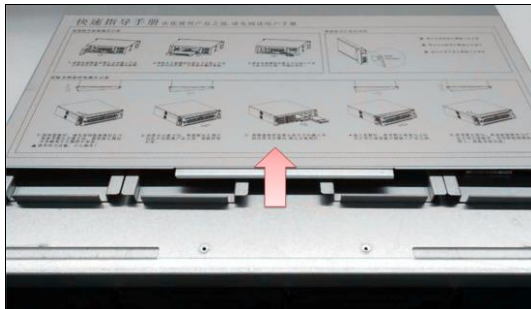
7. Install the bezel back to front panel. And lock it with key.

### 7.3.2 Installing HDD in Server Board

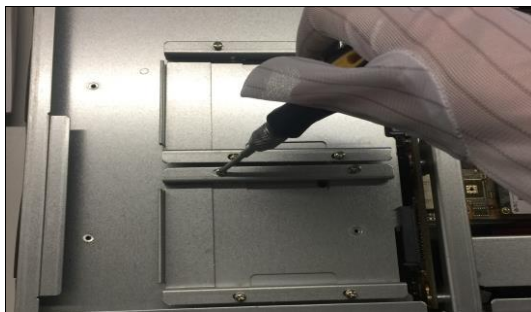
1. Unfasten the screws on the back and side of cover.



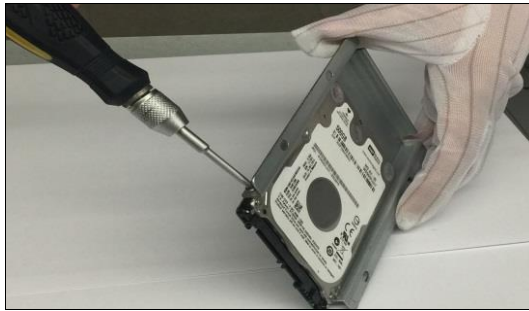
2. Push the cover along the direction shown in figure below to remove it.



3. Unfasten screws on HDD tray and take out the HDD tray.



4. Place a 2.5-inch HDD in HDD tray and fix them with four screws.



5. Place the HDD tray back and connect it with the server board.



6. Fix the HDD tray to server board with four screws.



7. Reinstall the cover to device and fasten the screws.



## 7.4 Peripheral Connections

### 7.4.1 Wiring of Alarm Input

The alarm input is an open/closed relay. To connect the alarm input to the device, use the following diagram.

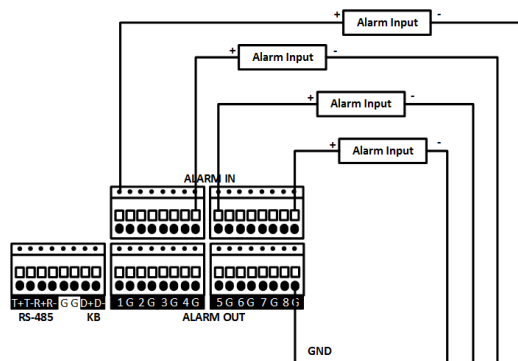
**Notes:**

- If the alarm input is not an open/close relay, please connect an external relay between the alarm



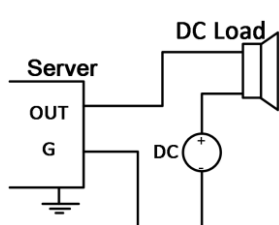
input and the device.

- The following figures only for reference, subject to the actual device.

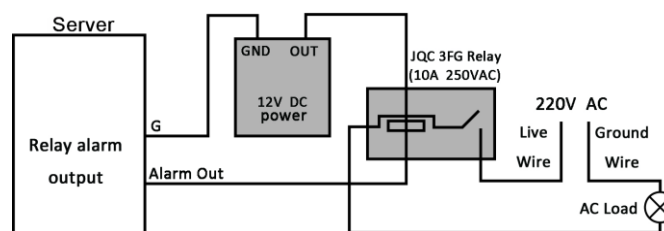


### 7.4.2 Wiring of Alarm Output

To connect to an alarm output (AC or DC load), use the following diagram:



DC Load Connection Diagram



AC Load Connection Diagram

For DC load, the jumpers can be used within the limit of 12V/1A safely.

To connect an AC load, jumpers should be left open (you must remove the jumper on the storage board in the Blazer Pro). Use an external relay for safety (as shown in the figure above).

There are 4 jumpers on the storage board, each corresponding with one alarm output. By default, jumpers are connected. To connect an AC load, jumpers should be removed.

**Example:**

If you connect an AC load to the alarm output 3 of the Blazer Pro, then you must remove the JP3.

### 7.4.3 Using of Alarm Connectors

To connect alarm devices to the Blazer Pro:

1. Disconnect pluggable block from the ALARM IN /ALARM OUT terminal block.
2. Unfasten stop screws from the *pluggable block*, insert signal cables into slots and fasten stop screws. Ensure signal cables are in tight.
3. Connect *pluggable block* back into terminal block.

### 7.4.4 Controller Connection

To connect a controller to the Blazer Pro:

1. Disconnect pluggable block from the KB terminal block of storage board.
2. Unfasten stop screws from the KB D+, D- *pluggable block*, insert signal cables into slots and fasten stop screws. Ensure signal cables are in tight.
3. Connect Ta on controller to D+ on terminal block and Tb on controller to D- on terminal block. Fasten stop screws.
4. Connect *pluggable block* back into terminal block.

**Note:** Make sure both the controller and Blazer Pro are grounded.

## 7.5 Power Connection and Startup

Plug the power supply (refer to the *Specifications*) into an electrical outlet. It is **HIGHLY** recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The server contains two sub-systems: Blazer Pro Storage Board and video management system (server board).

For the first-time access to the video management system (HikCentral), you need to connect a display unit to server board via VGA or HDMI interface. In this manual, we only introduce the basic settings for video management system.

After plugging the power supply, press the **POWER ON/OFF** switch on the front panel to start up. You are required to log in to the operating system of Blazer Pro by inputting its user name and password.

**Note:** The default user name and password of video management system's operating system are as follows:

**User Name:** *admin*

**Password:** *Abc12345*

## 8. Accessing Blazer Pro Storage Board

To operate the Blazer Pro Storage Board locally, you need to connect a display unit to storage board via VGA or HDMI interface.

### 8.1 Activating Storage Board

**Purpose:**

For the first-time access, you need to activate the storage board by setting an admin password. No operation is allowed before activation. You can also activate the device via web browser, SADP, or client software.

**Steps:**

1. Enter the same password in the text field of **Create New Password** and **Confirm New Password**.

| Activation  |              |
|---|--------------|
| User Name   | admin        |
| Create New P...   | ***** Strong |
| Confirm New P...  | *****        |
| <p>✓ Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.</p> |              |
| <p>OK Cancel</p>  |              |



*Strong Password recommended—We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*

2. Click **OK** to save the password and activate the device.

### 8.2 Using Unlock Pattern for Login

**Purpose:**

For the admin user, you can configure the unlock pattern for device login.

After the device is activated, you can enter the following interface to configure the device unlock pattern.

**Steps:**

1. Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

**Notes:**

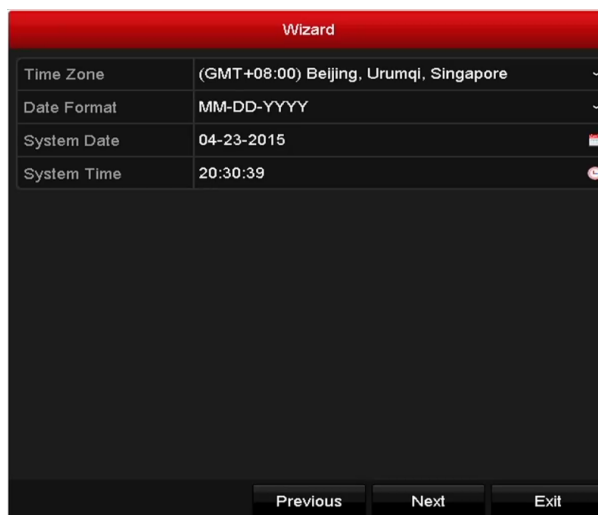
- Connect at least 4 dots to draw the pattern.
  - Each dot can be connected for once only.
2. Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully. Login and Logout

**8.3 Setup Wizard**

The Setup Wizard can walk you through some important settings of the device. By default, the Setup Wizard starts once the device has loaded.

Enable Setup Wizard when device starts. Click **Next** to continue the setup wizard.

Follow the guide of the Setup Wizard to configure the system resolution, system date/time, network settings, HDD management, record settings, etc.

**8.4 Network Settings****Purpose:**

Network settings must be properly configured before you operate device over network.

**Steps:**

1. Enter the Network Settings interface.
2. Select the **General** tab.
3. In the **General Settings** interface, configure the following settings: NIC Type, IPv4 Address,

IPv4 Gateway, MTU and DNS Server.

If the DHCP server is available, you can check the **DHCP** checkbox to automatically obtain an IP address and other network settings from that device.

4. After configuring the general settings, click **Apply** to save the settings.

## 8.5 Adding Network Cameras

### *Purpose:*

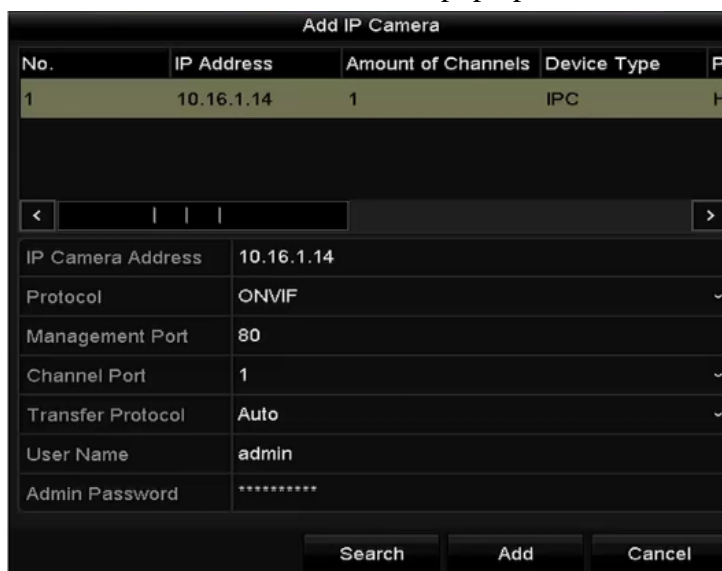
Before you can get live video or record the video files, you should add the network cameras to the connection list of the device.

### *Before you start:*

Ensure the network connection is valid and correct, and the network camera to add has already been activated. Please refer to the user manual for activating an inactive network camera.

### *Steps:*

1. Select an idle window in the live view mode.
2. Click **+** in the lower-left corner of the window to pop up the Add IP Camera interface.



The screenshot shows the 'Add IP Camera' interface. At the top, there is a table with the following data:

| No. | IP Address | Amount of Channels | Device Type | Pi |
|-----|------------|--------------------|-------------|----|
| 1   | 10.16.1.14 | 1                  | IPC         | H  |

Below the table is a form with the following fields:

- IP Camera Address: 10.16.1.14
- Protocol: ONVIF
- Management Port: 80
- Channel Port: 1
- Transfer Protocol: Auto
- User Name: admin
- Admin Password: \*\*\*\*\*

At the bottom of the form, there are three buttons: Search, Add, and Cancel.

3. Select the detected network camera and click **Add** to add it directly, and you can click **Search** to refresh the online IP camera manually.  
Or you can choose to custom add the network camera by editing the parameters in the corresponding text field and then click **Add** to add it.

## 9. Quick Start

Here we introduce the configuration for some basic features of video management system (HikCentral) Web Client and Control Client.

### 9.1 Accessing Blazer Pro via Web Client

You can access the system via Web Client which is a B/S client for management of HikCentral.

**Steps:**

1. In the address bar of the web browser, input the address of the Blazer Pro Server Board and press the **Enter** key.

A login window will pop up.

**Notes:**

- The address is in the format of `http://IP address of Blazer Pro Server Board`.

**Example:** If the IP address of Blazer Pro Server Board is `172.6.21.96`, and you should enter `http://172.6.21.96` in the address bar.

- Before you can access the system via a WAN, please configure the system's IP address in WAN Access of System Configuration. For details, refer to the *User Manual of HikCentral Web Client*.
2. On the first login via the Internet Explorer browser, allow to run the plug-in in the pop-up prompt.
  3. If it is the first time accessing the Web Client, you are required to create the *admin* password for HikCentral.

The following dialog will pop up.

Input the password and confirm password for the *admin* user and click **Save** to create the password.

**Note:** The password strength should meet the system requirements. The default minimum password strength is **Medium**.



- *The password strength can be checked by the system. For your privacy, you must set the password to something of your own choosing (using a minimum of 8 characters, including*

upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. If it is not the first time login as an admin user, input the user name and password and click **Login**.

**Notes:**

- When other users (except *admin* user) first log in to HikCentral, he/she should input the initial password (*Abc123*), new password and confirm password, and click Save to create the password.
- If a failed password attempt is detected, you are required to input a verification code before you can log in.
- Any failed password attempts and verification code attempts from all sources will be accumulated. After a specified number of failed password or verification code attempts, your IP address will be locked for a defined period of time. For detailed settings of failed login attempts and locking duration, refer to the *User Manual of HikCentral Web Client*.
- The default settings for the above enforce that the account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from the current client, other client (e.g., Control Client) and other address will all be accumulated.

## 9.2 Resource Management

**Purpose:**

Before using live view, viewing playback, setting a recording schedule, or configuring events, you need to add devices to the system, and manage them by areas.

**Note:** Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturer's instructions. This initial configuration is required in order for the networked devices to link up with HikCentral.

### 9.2.1 Adding Storage Board as Encoding Device

**Purpose:**

You need to add the Blazer Pro Storage Board to the system for further management as encoding device. You can also add other encoding devices (such as DVR and network camera) to the system. In this document, we will introduce adding the Blazer Pro Storage Board by online device detection and by IP address. For other adding modes, refer to the *User Manual of HikCentral Web Client*.

#### Adding Online Storage Board

When the storage board is in the same local subnet as the Web Client, you can add it to the system by detecting the online devices automatically.

**Steps:**

1. Enter the Web Client and click **Physical View** on Home page.
2. Click **Encoding Device** tab.
3. In the Online Device panel, select the storage board to be added.
4. Click **Add to Device List**.

5. Input the required information.
  - **Alias:** Create a device name.
  - **Device Address:** The device IP address will be obtained automatically in this adding mode.
  - **Device Port:** Input the device port number. The port will be obtained automatically in this adding mode.
  - **User Name:** Input the device user name. The default user name is *admin*.
  - **Password:** Input the device password.

*Note: The password strength of the device can be checked by the system. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.*
6. (Optional) Import the encoding device's cameras to area.
  - 1) Set the **Add Camera to Area** switch to **ON**.
  - 2) Import all the cameras of the encoding device, or select specified cameras to import.
  - 3) Select an area. You can create a new area by the device name (or custom) or select an existing area.

*Note: If you do not import cameras to an area, you cannot perform the live view, playback, event settings, etc., for the cameras.*
7. After adding cameras to an area, select the **Synchronize Camera Name** checkbox to obtain the camera name from the device, and select **Get Device's Recording Settings** to get the recording schedule from the device. The device cameras will record automatically according to this schedule.
8. Click **OK** to confirm adding the device.

### Adding Storage Board by IP address

You can add the storage board to the system as encoding device by inputting its IP address and port number.

#### *Steps:*

1. Enter the Web Client and click **Physical View** on Home page.
2. Click **Encoding Device** tab.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **IP/Domain** as the adding mode.
5. Input the required information.
  - **Manufacturer:** Select the device manufacturer.
  - **Device Address:** Input the device IP address or domain name.
  - **Device Port:** Input the device port number. By default, it's *8000*.
  - **Alias:** Edit a name for the device as desired.
  - **User Name:** Input the user name of the device.
  - **Password:** Input the password of the device.

*Note: The password strength of the device can be checked by the system. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.*



6. Set the **Add Camera to Area** switch to **ON** to import the cameras of the added devices to an area. Create a new area by the device name (or custom) or select an existing area.  
**Note:** If you do not import cameras to area, you cannot perform the live view, playback, event settings, etc., for the cameras.
7. After adding cameras to an area, select the **Synchronize Camera Name** checkbox to obtain the camera name from the device. Select **Get Device's Recording Settings** to get the recording schedule from the device. The device cameras will record automatically according to this schedule.
8. Click **Add** to add the device and return to the device list page. You can also click **Add and Continue** to save the settings and continue to add other devices.

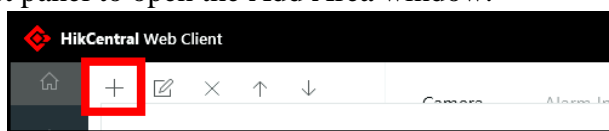
### 9.2.2 Area Management

#### **Purpose:**

The added cameras, alarm inputs, and alarm outputs should be organized into areas for convenient management. You can watch the live view, play back the video files, and perform some other device operations when you manage the devices by areas.

#### **Steps:**

1. Enter the Web Client and click **Logical View** on home page.
2. Click + on the area list panel to open the Add Area window.



3. Select the parent area in the Parent Area drop-down list.
4. Input an area name.
5. Click **Save** to add the new area.
6. Add the camera, alarm input or alarm output to the new area.
  - 1) In the area tree panel, select an area for adding elements to.
  - 2) In the element area, select an element type tab. The element types are: cameras, alarm inputs, and alarm outputs.
  - 3) Click **Add** to add the element(s) to the area.
  - 4) Select the checkbox(es) to choose the elements to be added.
  - 5) Select the area to add the element to.
  - 6) (Optional) When adding a camera to the area, select the **Synchronize Camera Name** checkbox to obtain the camera name from the device.  
(Optional) Select the **Get Device's Recording Schedule** checkbox to obtain the recording schedule configured on the local device. The cameras will record automatically according to this schedule.
  - 7) Click **Add** to add the elements to the area.

#### **Notes:**

- Up to 64 cameras can be added per area.
- A camera, alarm input, and alarm output, can only be added to an individual area.

## 9.3 Live View

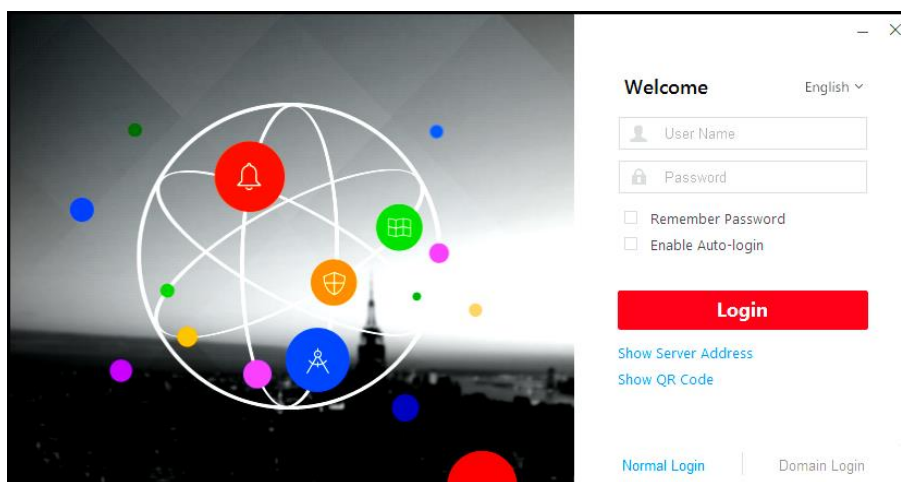
After adding the devices to your managed area, you can use the live view of the camera via the Control Client which provides multiple operating functionalities.

### 9.3.1 Login the Control Client

Two kinds of user (normal user and domain user) are supported for accessing the system via Control Client. Here we only introduce the normal user login in this document. Please refer to the *User Manual of HikCentral Control Client* for the domain user login and refer to *User Manual of HikCentral Web Client* for the Active Directory setup.

**Steps:**

1. Double-click  on the desktop to run the Control Client.






2. Select **Normal Login** tab on the bottom.
3. Click **Show Server Address** and input the parameters.
  - **Server Address:** Input the address (IP address or domain name) of the Blazer Pro Server Board that you want to connect to. To access the local Blazer Pro, you can input *localhost*.
  - **Port:** Input the port number. By default, it's 80.
4. Input the user name and password of the Blazer Pro Server Board.
5. Click **Login** to enter the Control Client.

**Notes:**

- If failed login attempt is detected, you are required to input the verification code before you can login successfully.
- The failed password attempt and verification code attempt from current client, other client (e.g., Web Client) and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts. For detailed settings of failed login attempts and locking duration, refer to *User Manual of HikCentral Web Client*.
- The account will be frozen for 10 minutes after 5 failed password attempts.

### 9.3.2 Live View

#### Steps:

1. After logging into the Control Client, click  to enter the Live View interface.
2. Click  on the left to enter the area mode.
3. (Optional) Click  and select the window division mode for live view.
4. Drag the camera to the display window,  
or double-click the camera name after selecting the display window to start the live view.

**Note:** For detailed operations about live view, refer to *User Manual of HikCentral Control Client*.

## 9.4 Recording Schedule Settings

#### Purpose:

In order to view the camera's video files via the Control Client, you should set the schedule recordings via the Web Client.

HikCentral provides three storage methods: 1) storing on the encoding devices, 2) storing on the Central Video Recorder, 3) storing on the Cloud Storage Server for storing the video files of the cameras according to the configured recording schedule. You can also store the video files of the remote site's cameras in the central system's Recording Server.

#### Notes:

- In this document, we only cover the method of storing video files of current site's cameras on the encoding devices. For the configuration of storing the video files on other location, refer to the User Manual of HikCentral Web Client.
- If the recording schedule was imported from the device upon adding it to HikCentral, this section should be skipped.

#### Steps:

1. On the HikCentral Web Client Home page, click **Recording** to open the recording settings page.
2. Click **Add** to configure camera recording settings.
3. Select the camera(s) to configure the recording settings for.
4. Set the **Main Storage** switch to **ON** to set the main storage location.
5. Input the required information.
  - **Storage Location:** Store the video files on the Encoding Device.
  - **Recording Schedule Template:** Select the recording type as all-day time-based template, all-day event-based template, or customized template. Click **View** to view the template. For setting the custom recording, refer to *User Manual of HikCentral Web Client*.  
**All-Day Time-Based Template:** Record video all-day continuously.  
**All-Day Event-Based Template:** Record video when event occurs.
  - **Stream Type:** Select the recording stream type.
  - **Pre-record:** Time to record video preceding detected events. The value of the pre-record period is not editable. This field is available for cameras that are configured with event-based recording.
  - **Post-record:** Time to record video following detected events. This field is available for cameras that are configured with event-based recording.
  - **Video Files Storage:** Select the storage mode for the recorded videos.

**Overwrite:** Overwrite the oldest videos when disk or allocated quota is full.

**Expired Time:** When this option is selected, HikCentral will automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period for keeping videos. The actual retention period for the videos depends on the allocated storage.

- **Enable ANR:** Turn the automatic network replenishment on to temporarily store the video in the device when network fails and transport the video to storage board when network recovers.
6. Optional, you can switch the **Auxiliary Storage** as **ON** to enable the auxiliary storage and set the parameters.
  7. Click **Add** to save the recording settings and back to the recording list page. You can also click **Add and Continue** to save the settings and continue to add other recording settings.

## 9.5 Playback



### *Purpose:*

After configuring the recording settings for the camera via the Web Client, the video files can be searched and played back remotely.

**Note:** Here we only introduce the playback of continuous video files. For other operations about playback, refer to the *User Manual of HikCentral Control Client*.

### 9.5.1 Searching Video Files for Playback

#### *Steps:*



1. After login the Control Client, click  on the control panel to enter the Playback page.
2. Drag the camera/area to the display window, or double-click the camera/area to begin playback.
3. You can click the calendar  on the toolbar to select the date and time to search the video file for playback.

### 9.5.2 Playing Video Files

After searching the video files for the normal playback, you can control the video playback in the following ways:

- **Timeline**

The timeline indicates the video files duration, and video files of different types are color coded.

Click  or  to zoom in or out the timeline bar. You can also use the mouse wheel to zoom in or out on the timeline.

- **Thumbnails**

Hover the cursor over the timeline to view the video thumbnails. Click the thumbnail (if supported) to play back the video of the specific time.

- **Locking Files**

Move the mouse to the playback window. Click  icon and set the locking duration to protect the video file from being overwritten when the HDD is full or from being “manually” deleted.

## 9.6 Event and Alarm Configuration

### *Purpose:*

In the HikCentral Web Client, you can set the linkage actions for the detected events and alarms. Status of the events and alarms can be received by the Control Client from the devices.

In this document, we will introduce setting camera alarm as an example. For the settings of other event types (e.g., alarm input, encoding device exception, server alarm), please refer to the *User Manual of HikCentral Web Client*.

### 9.6.1 Configuring Motion Detection Event

The camera exception types vary according to the connected device. In the following example, we will introduce the motion detection settings. For the settings of other camera exception types (e.g., video loss, video tampering), please refer to the user manual of the connected devices.

#### **Purpose:**

A motion detection alarm is triggered when the camera detects motion within its defined area.

#### **Steps:**

1. Click **Event & Alarm** and click **System-Related Event** tab to enter the Event Management interface.
2. Click **Add** to enter the Add Event page.
3. Select the source type as *Camera* and select the triggering event as *Motion Detection*.
4. Select the specific camera in the Source panel.
5. Click **Add** to add the event and return to the event list page. You can also click **Add and Continue** to save the event settings and continue to add event.

### 9.6.2 Configuring Motion Detection Alarm

#### **Purpose:**

After configuring the event, you can configure the alarm (here we still take the motion detection alarm as an example) for trigger actions for notification.

**Example:** HikCentral can send notification email to designated recipient when motion is detected.

#### **Steps:**

1. Click **Event & Alarm** and click **Alarm** tab to enter the alarm settings page.
2. Click **Add** to enter the adding alarm page.
3. Set the required parameters.
  - **Triggered by:** Select the source type as *Camera*, source –a specific camera, and the triggering event as *Motion Detection* for triggering the alarm.
  - **Alarm Name:** Create an alarm name.
  - **Description:** Optionally, input alarm handling instructions and remarks.
  - **Arming Schedule Template:** Create an arming schedule, and define when the alarm will be triggered.
  - **Alarm Priority:** Define the alarm priority, and filter alarms that will be displayed in the Control Client.
  - **Recipient:** Select the user that will receive alarm information, as well as the user that will receive alarm information when they log into HikCentral via Control Client or Mobile Client.

#### **Additional Settings:**


- **Related Cameras:** Select the cameras for viewing the live video and playback when the alarm occurs in the Control Client's Alarm Center.

- **Lock Video Files for:** Set the time duration for protecting the video file from being deleted.
  - **Related Map:** Select the map to show the alarm information and you should add the camera to the map as a hot spot.
  - **Trigger Pop-up Window:** Pop up the alarm window on Control Client to display all the alarm related cameras' live videos and playback when alarm occurs.
  - **Actions:** Trigger linkage actions when alarm occurs.
    - **Trigger actions when:** Trigger linkage actions immediately after alarm occurs, or trigger actions after the alarm is not handle within a certain time duration (customized).
    - **Trigger Audible Warning:** Set the voice text for playing on the PC when alarm is triggered.
    - **Link Alarm Output:** Select the alarm output (if available) of an external device to be activated when alarm is triggered.
    - **Trigger PTZ:** Trigger selected camera preset, patrol or pattern of the selected camera(s) when alarm is triggered.
    - **Display on Smart Wall:** Display the alarm video of the related camera on the smart wall. You can select the added smart wall and select which window to display the alarm.
    - **Create Tag:** Add tag to the video that is triggered by the alarm when you select cameras in the **Related Cameras** field. You can search for and check the video in the Control Client.
    - **Send Email:** Select an email template to join the alarm information to, according to the defined email settings.
4. Click **Add** to add the alarm and return to the Alarm page. You can also click **Add and Continue** to save the settings and continue to add other alarm.


### 9.6.3 Checking Event Logs

If the camera detects motion, the event logs can be checked in the Control Client.

#### *Steps:*

1. Log into the HikCentral via the Control Client.
2. Click  on the control panel to enter the Alarm Center page, and click the **Search** tab.
3. Select the event source, triggering event type, and time range.
4. Select the **Event** radio button to select the log type.
5. Click **Search**.

The matched log files will display in the list. You can check the detailed event information.


6. Click the **Alarm Name** field of the searched alarm to view the detailed information, as well as the linked picture, video, and map.
7. Click  to save the information to your PC.

## 10. Shutting Down Blazer Pro

Press the following steps to shut down the boards separately.

- **For server board:**

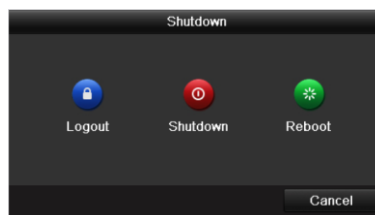
*Steps:*

1. Connect a display unit to the server board via VGA or HDMI interface.
2. In the video management system, click  in the lower left corner of the desktop.
3. Click  button and the server board will shut down.

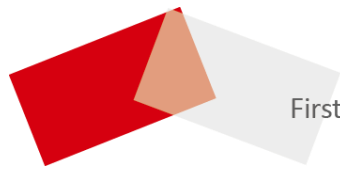
- **For storage board:**

*Steps:*

1. Connect a display unit to the storage board via VGA or HDMI interface.
2. In the storage board operating system, enter **Menu > Shutdown**.



3. Select **Shutdown**.
4. Click **Yes** and the storage board will shut down.



First Choice for Security Professionals