exacqVision

Digital Encoder

# E-Series User Manual

*(updated June 10, 2015)*

Information in this document is subject to change without notice.
© Copyright 2006-2015, Exacq Technologies, Inc. All rights reserved.

exacq Technologies

Exacq Technologies is a trademark of Exacq Technologies, 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. Exacq Technologies, Inc., disclaims any proprietary interest in trademarks and trade names other than its own.

Exacq Technologies makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Exacq Technologies shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Exacq Technologies, Inc.
11955 Exit Five Parkway, Bldg 3
Fishers, IN  46037  USA

exacqVision

# TABLE OF CONTENTS


1 Introduction ..... 5

2 Encoder Overview ..... 7
- E-ADE1C FRONT PANEL ..... 7
- E-ADE4C FRONT PANEL ..... 8
- E-ADE1C REAR PANEL ..... 9
- E-ADE4C REAR PANEL ..... 10
- Alarm Input Connections ..... 11
- Alarm Output Connections ..... 11

3 Network Parameters ..... 12
- Searching Online Devices ..... 12
- Modifying Network Parameters ..... 13
- Restoring Default Password ..... 13

4 Connecting to an exacqVision System ..... 14
- Initiating the Connection ..... 14
- Verifying the Connection ..... 15

5 Encoder Configuration Page ..... 16
- Installing Web Components ..... 16
- Main Page ..... 18

6 Live View ..... 19
- Starting Live View ..... 19
- Capturing a Picture ..... 20
- Operating PTZ Controls ..... 21
- Configuring Video Parameters ..... 24

7 Device Configuration ..... 25
- Local Configuration ..... 25
- Configuring Time Settings ..... 26

8 Network Settings ..... 27
- Configuring TCP/IP Settings ..... 27
- Configuring SNMP Settings ..... 28
- Configuring Port Settings ..... 30
- Configuring PPPoE Settings ..... 31
- Configuring QoS Settings ..... 32
- Configuring SOCKS Settings ..... 33
- Configuring NAT/UPnP™ Settings ..... 34
- Configuring HTTPS Settings ..... 36

Configuring Bonjour Settings ..... 38
Configuring IP Address Filter ..... 39
Configuring IEEE 802.1x Settings ..... 40
Configuring Advanced Settings ..... 41

9 Camera Settings ..... 42
Configuring Display Settings ..... 42
Configuring Video Settings ..... 44
Configuring Motion Detection ..... 45
Configuring a Video Loss Alarm ..... 49
Configuring a Privacy Mask ..... 50
Configuring Video Tampering ..... 51
Configuring Text Overlay ..... 52
Configuring Holiday Settings ..... 53

10 RS-232 and RS-485 Settings ..... 54
Configuring RS-232 ..... 54
Configuring RS-485 Settings ..... 55

11 Alarm Input/Output ..... 56
Configuring the External Alarm Input ..... 56
Configuring the External Alarm Output ..... 58

12 Exceptions ..... 59

13 User Management ..... 60
Adding a User ..... 61
Modifying a User ..... 62
Deleting a User ..... 63

14 Device Information and Maintenance ..... 64
Viewing Device Information ..... 64
Maintenance ..... 65

A Technical Support ..... 67

B Regulatory Notice ..... 68

C Warranty ..... 69

# 1 Introduction

exacqVision E-Series 1- and 4-channel encoders capture analog video and audio signals; encode the content using H.264, MJPEG, and G.711 compression technologies; and transmit the data to exacqVision video servers for recording. E-Series encoders are a cost-effective way to migrate to IP video when legacy analog CCTV equipment and infrastructure must be used.

E-Series encoders are fully compatible with exacqVision and support configuration of motion detection, image quality, streaming profiles, and digital inputs and outputs directly from exacqVision.

**Encoding**

- Supports H.264 and MJPEG formats
- Supports encoding video at up to 4CIF resolution
- Supports dual-stream encoding.
- Allows selection of compound stream encoding (with audio and video synchronization) or video stream encoding

**Network**

- One 10M/100Mbps adaptive Ethernet interface (PoE)
- Accessible by multiple web browsers, including Internet Explorer, Firefox, Chrome, and Safari
- Remote web browser access by HTTPS, ensuring high security
- Netfilter builds internet firewalls based on packet filtering
- QoS protocol enhances the data transmission performance.
- Supports SNMPv1/v2c/v3 simple network management protocol
- mDNS-based Apple's Bonjour protocol, which enables automatic discovery of devices
- Zero configuration networking (Zeroconfig), which automatically obtains the IPv4 link-local IP addresses (range: 169.254.1.0~169.254.254.255).
- Auto/manual port mapping by UPnP™
- Discoverable by exacqVision or E-Series IP Configuration Utility
- Automatically obtains IP address by DHCP protocol
- RTSP/RTP standard stream media protocol, which allows user to view live by unicast
- Transmission via RS-232 and RS-485 transparent channel (four-channel encoders only)
- Access to Internet by PPPoE method; supports Peanut Hull, DynDNS, and more
- Sets time by NTP

**PTZ Control**

- Support multiple PTZ protocols; different channels can be configured with protocol type, RS-485 address, baud rate, data bit, stop bit, even/odd parity, stream control method, and more; support for remote configuration of presets, patrols, and patterns.
- Relay input alarm can be responded to with PTZ linkage actions, such as presets, patrols, or patterns.

**Alarm**

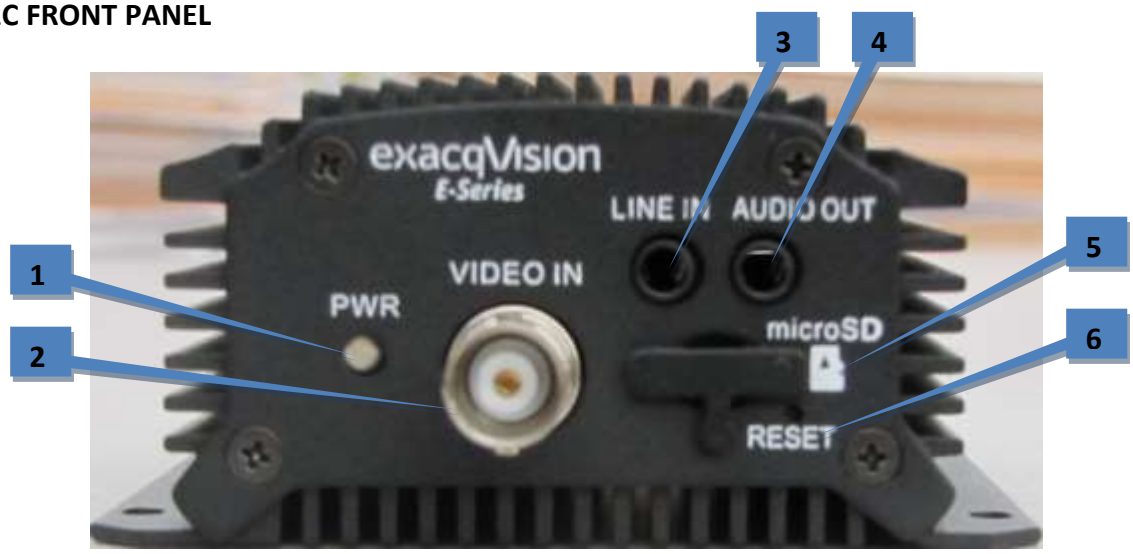
- Relay alarm input; normally open or normally closed; four configurable alarm arming periods; triggering of corresponding alarm handling methods, relay alarm output, buzzer alarm, upload to control center, PTZ linkage, presets/patrols/patterns, and more.
- Relay Alarm Output; can be connected with alarm devices for alarm handling within arming period.

**Exceptions**

- Exception alarm handling; includes network disconnect alarm, IP address conflict alarm, illegal access alarm, and more; multiple alarm handling methods supported, relay alarm output, buzzer alarm, and more.
- Exception reboot; software watchdog for inspecting important threads and system resources of device; device automatically restarted if exceptions are detected.
- Firmware watchdog for inspecting the firmware of device; device automatically restarted in case of exceptions in system task scheduling.

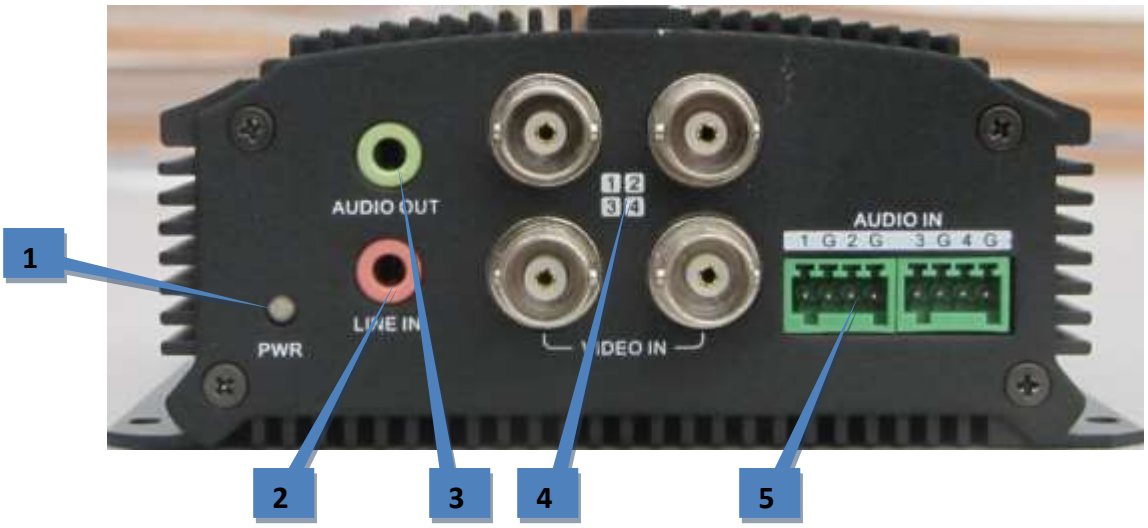
# 2 Encoder Overview

## E-ADE1C FRONT PANEL



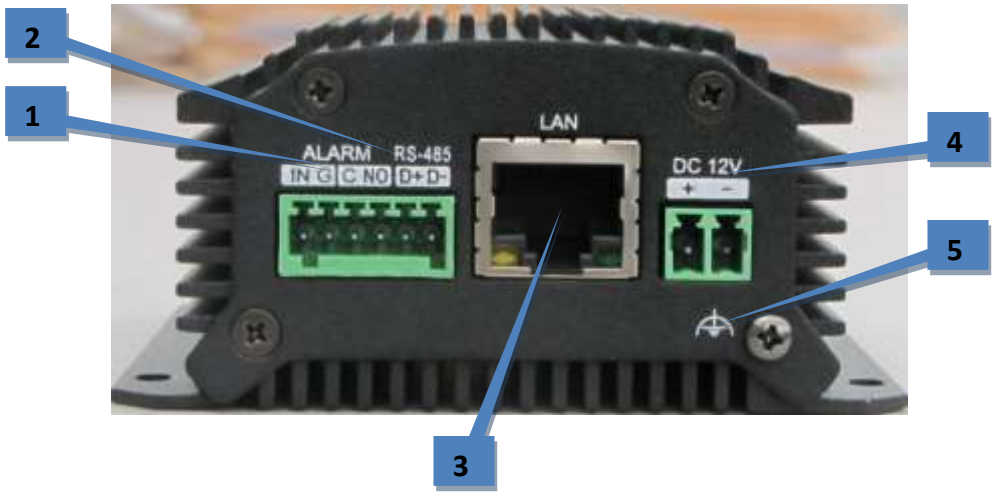

| | Item | Description |
|---|---|---|
| 1 | POWER LED Indicator | Red when the device is powered on. |
| 2 | VIDEO IN | BNC connector for video input. |
| 3 | LINE IN | 3.5mm interface for two-way audio input or audio input; connect to audio input device or active pick-up, microphone, etc. |
| 4 | AUDIO OUT | 3.5mm interface; connect to audio output device such as loudspeaker. |
| 5 | microSD | Unused (included for future expansion). |
| 6 | RESET | Hold button for more than 15 seconds after power is turned on to restore factory-default settings. |

## E-ADE4C FRONT PANEL



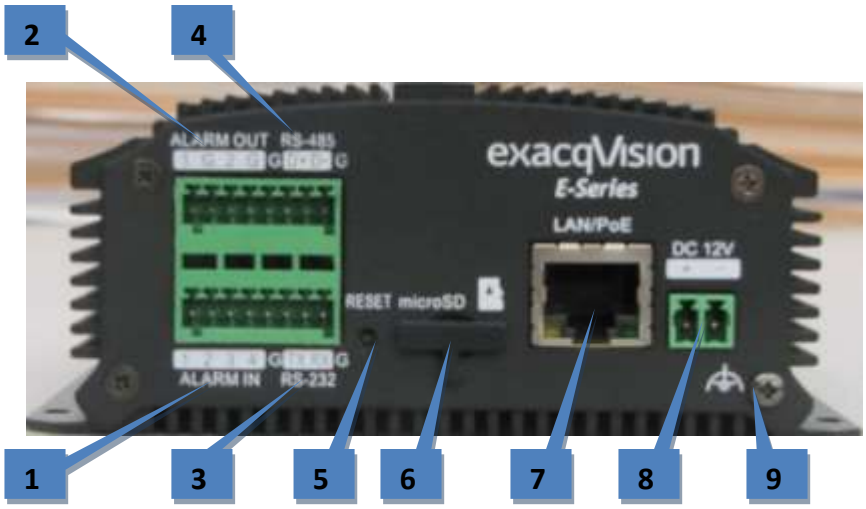

| | Item | Description |
|---|---|---|
| 1 | POWER LED Indicator | Red when the device is powered on. |
| 2 | LINE IN | 3.5mm two-way audio input interface; connect to active pick-up, microphone, etc. |
| 3 | AUDIO OUT | 3.5mm interface; connect to audio output device, such as loudspeaker. |
| 4 | VIDEO IN | BNC interface for video input. |
| 5 | AUDIO IN | Line input interface for audio input. |

## E-ADE1C REAR PANEL




| | Item | Description |
|---|---|---|
| 1 | ALARM IN /OUT | Relay alarm input/output. (JP2 pin not available on output.) |
| 2 | RS-485 | RS-485 serial interface; connect to pan/tilt unit, speed dome, etc. |
| 3 | LAN | 10M/100Mbps adaptive Ethernet interface (PoE). Right LED indicator lights in green when the network cable is connected; left LED indicator blinks in orange when data is transmitting/receiving. |
| 4 | DC12V | 12V DC power supply. |
| 5 | GND | Grounding. |

## E-ADE4C REAR PANEL

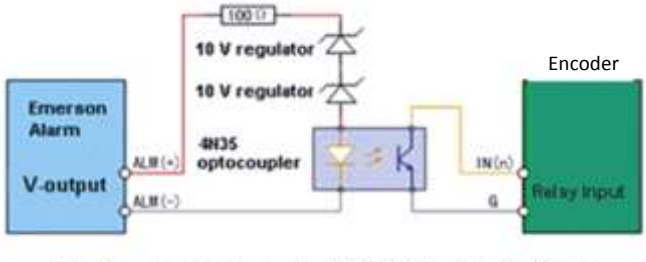



| | Item | Description |
|---|---|---|
| 1 | ALARM IN | Relay alarm input. |
| 2 | ALARM OUT | Relay alarm output. |
| 3 | RS-232 | Serial interface for configuration of device's parameters; or used as transparent channel. |
| 4 | RS-485 | RS-485 serial interface; connect to pan/tilt unit, speed dome, etc. |
| 5 | RESET | Hold button for more than 15 seconds after the device is turned on to restore factory-default settings. |
| 6 | microSD | Unused (included for future expansion). |
| 7 | LAN | 10M/100Mbps adaptive Ethernet interface (PoE). Right LED indicator lights in green when the network cable is connected; left LED indicator blinks in orange when data is transmitting/receiving. |
| 8 | DC12V | 12V DC power supply. |
| 9 | GND | Grounding. |

## Alarm Input Connections

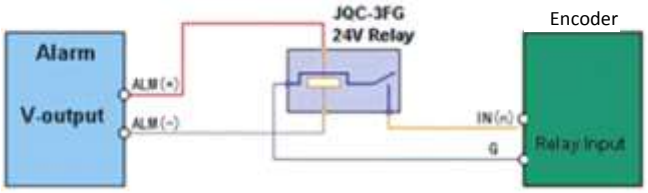
The encoder supports the open/close relay input as the alarm input mode. For the alarm input signal not in open/close relay signal mode, follow the connections shown as below:

Alarm input connections for Emerson Alarm:



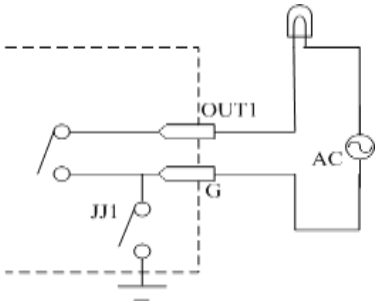

**Note: The relay input port of the Encoder should be set to NC mode.**

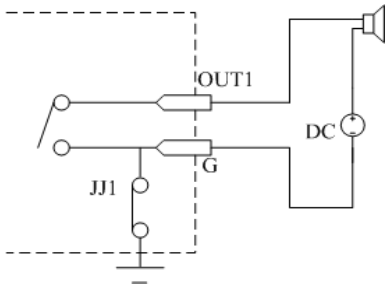
Alarm input connections for Normal Alarm:




## Alarm Output Connections

The encoder supports the open/close relay input as the alarm output mode. The alarm input can be selected to NO or NC. Different alarm output connection methods are applied to the AC or DC load:




**NOTE:** The one-input encoder does not have a JJ1 relay. Please note the different connections of JJ1 shown here. For DC load, JJ1can be safely used both in NC and NO modes, and it is recommended within the limit of 12V/1A. For external AC input, JJ1 must be open. The motherboard provides two jumpers, each corresponding to one alarm output. Both jumpers are connected by default.

# 3 Network Parameters

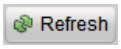
There are two ways an IP address can be assigned to the encoder:

- If a DHCP server is available, an IP address will be assigned to the encoder automatically. You can then locate the encoder in exacqVision using the Find IP Cameras feature (see section 6 of this document for more information).
- If a DHCP server is not available, the encoder will default to a link-local address.

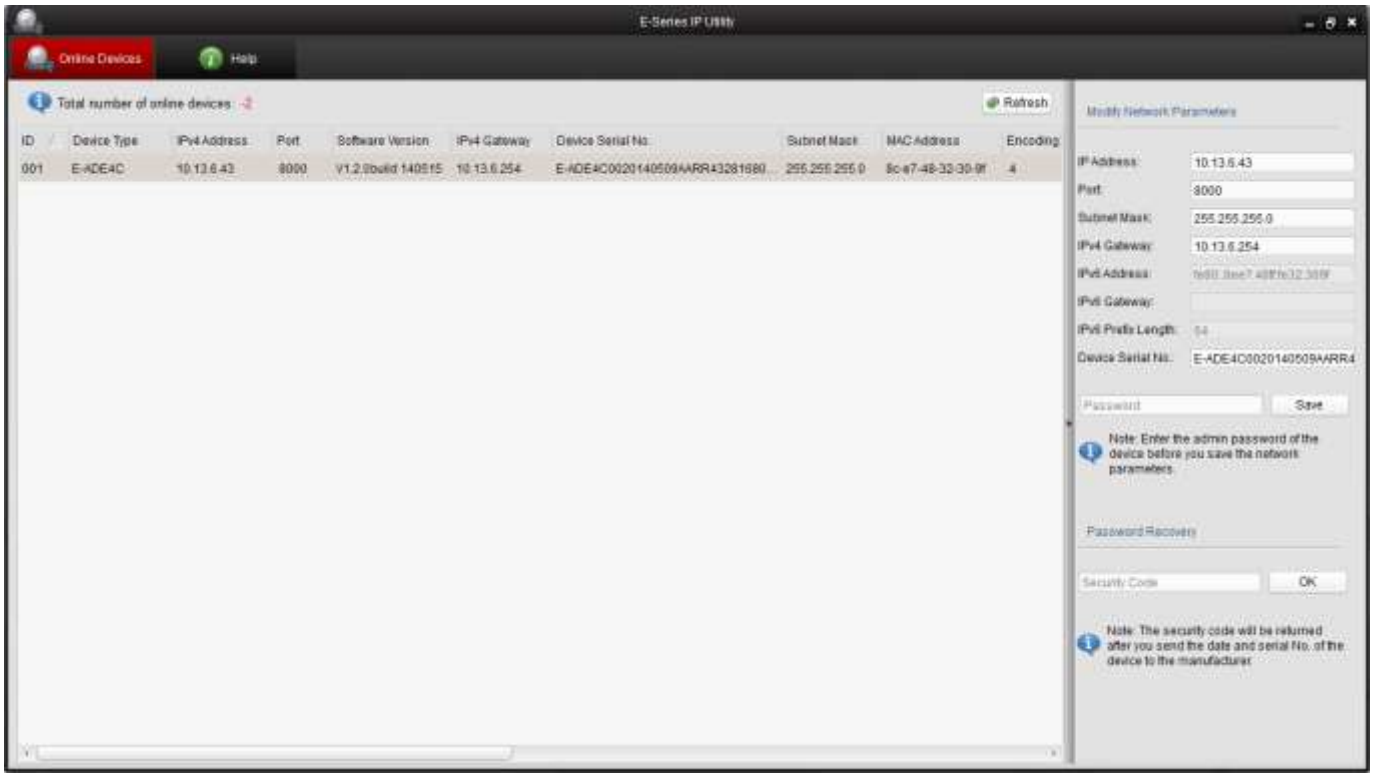
In either case, you can use the E-Series IP utility to find and configure the IP address and other network parameters.

## Searching Online Devices

Click to run the IP utility. It automatically searches online devices every 15 seconds on the computer's subnet. It displays the total number of located devices in the **Online Devices** interface. Device information such as device type, IP address, port number, and gateway are displayed.

Click 

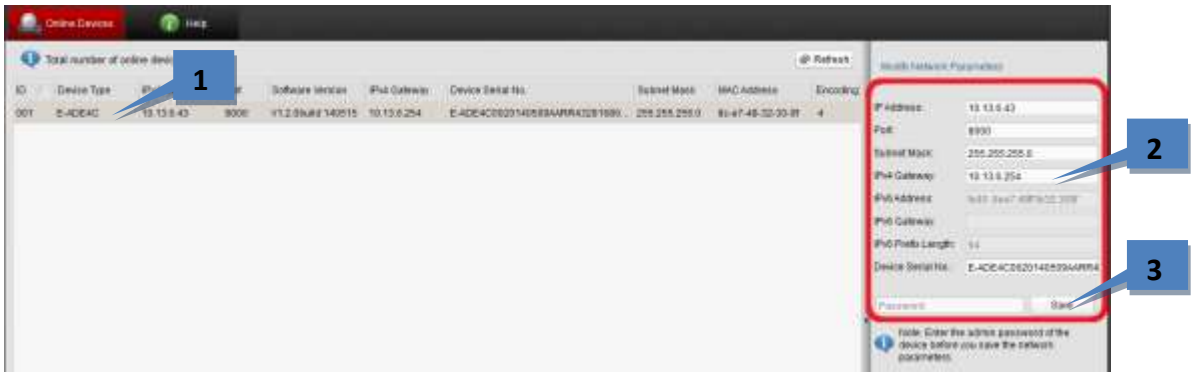
to refresh the online device list manually. Any newly searched devices are added to the list. Devices can be searched and displayed in the list within 15 seconds of connection, and they are removed from the list within 45 seconds after going offline.



## Modifying Network Parameters

1. Select the device to be modified in the device list.
2. Network parameters of the selected device are displayed in the **Modify Network Parameters** panel. Edit the modifiable network parameters as needed.
3. Enter the password of the admin account of the device in the **Password** field and click Save to save the changes.

   **NOTE:** To modify the network parameters of multiple devices simultaneously, select all the devices to be modified before editing the parameters. The IP address entered is incremented by one for the additional selected devices; that is, if you enter 10.13.6.43 for the first selected device, the next device will be assigned 10.13.6.44, and so on until each selected device is assigned an address.




## Restoring Default Password

It is recommended that you change the admin password. Default credentials for the encoder are as follows:

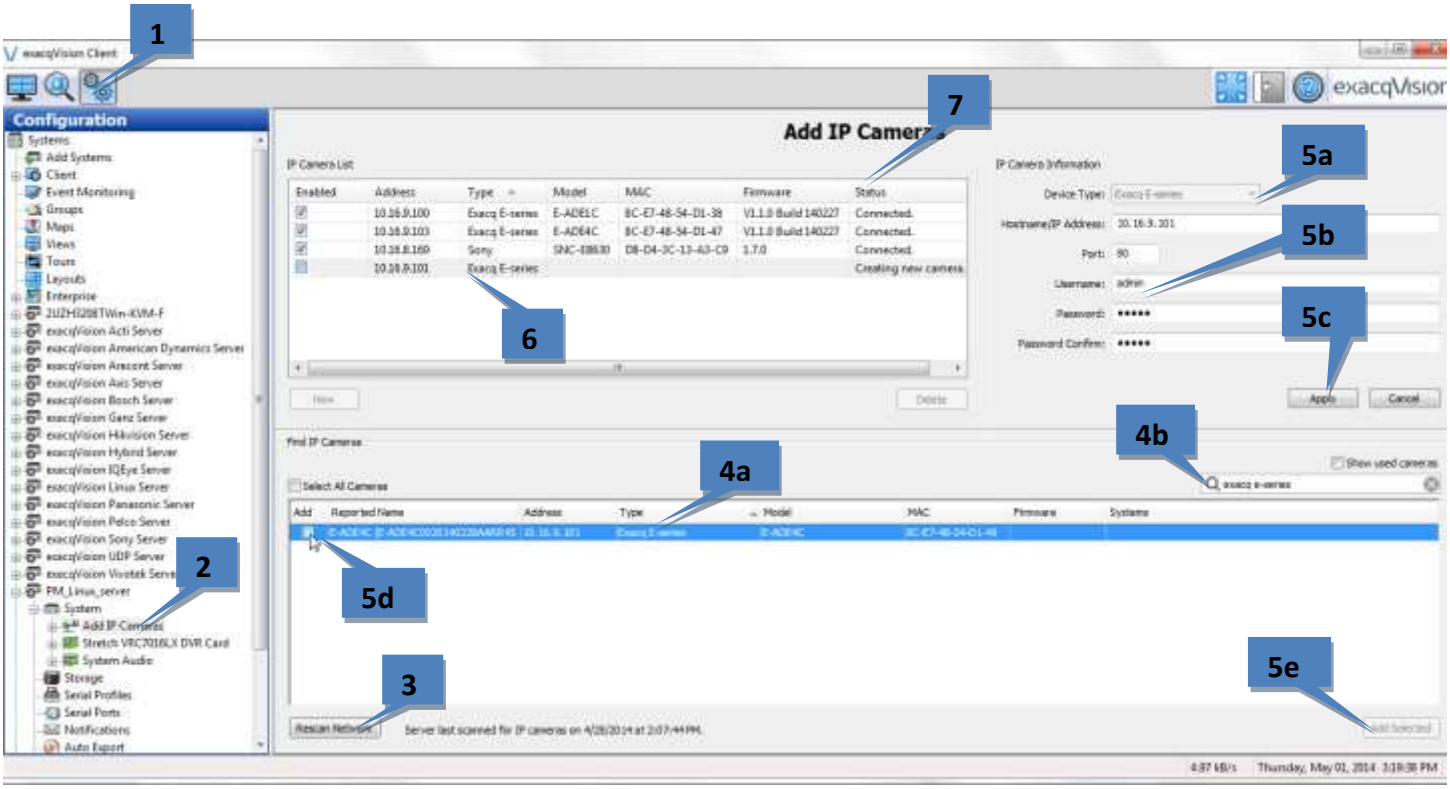
- **Username:** admin
- **Password:** admin256

# 4 Connecting to an exacqVision System

**NOTE:** The latest version of exacqVision Client can be downloaded from https://exacq.com/support/downloads.php.

## Initiating the Connection

To add the encoder to the exacqVision system using exacqVision Client, complete the following steps:




1. Open exacqVision Client and select the Config (Setup) page.
2. In the site tree, find the exacqVision server that the encoder will be associated with. Expand the server until you can select Add IP Cameras.
3. Click Rescan Network to ensure all cameras and encoders are displayed in the Find IP Cameras list.
4. Locate the encoder in the Find IP Cameras list (4a). To narrow the list, type information about the encoder, such as “E-Series” or the IP address, in the search box (4b).
5. Select the encoder entry in the list to display the encoder in the IP Camera Information section (5a). Enter the username and password (5b), and then click Apply (5c).

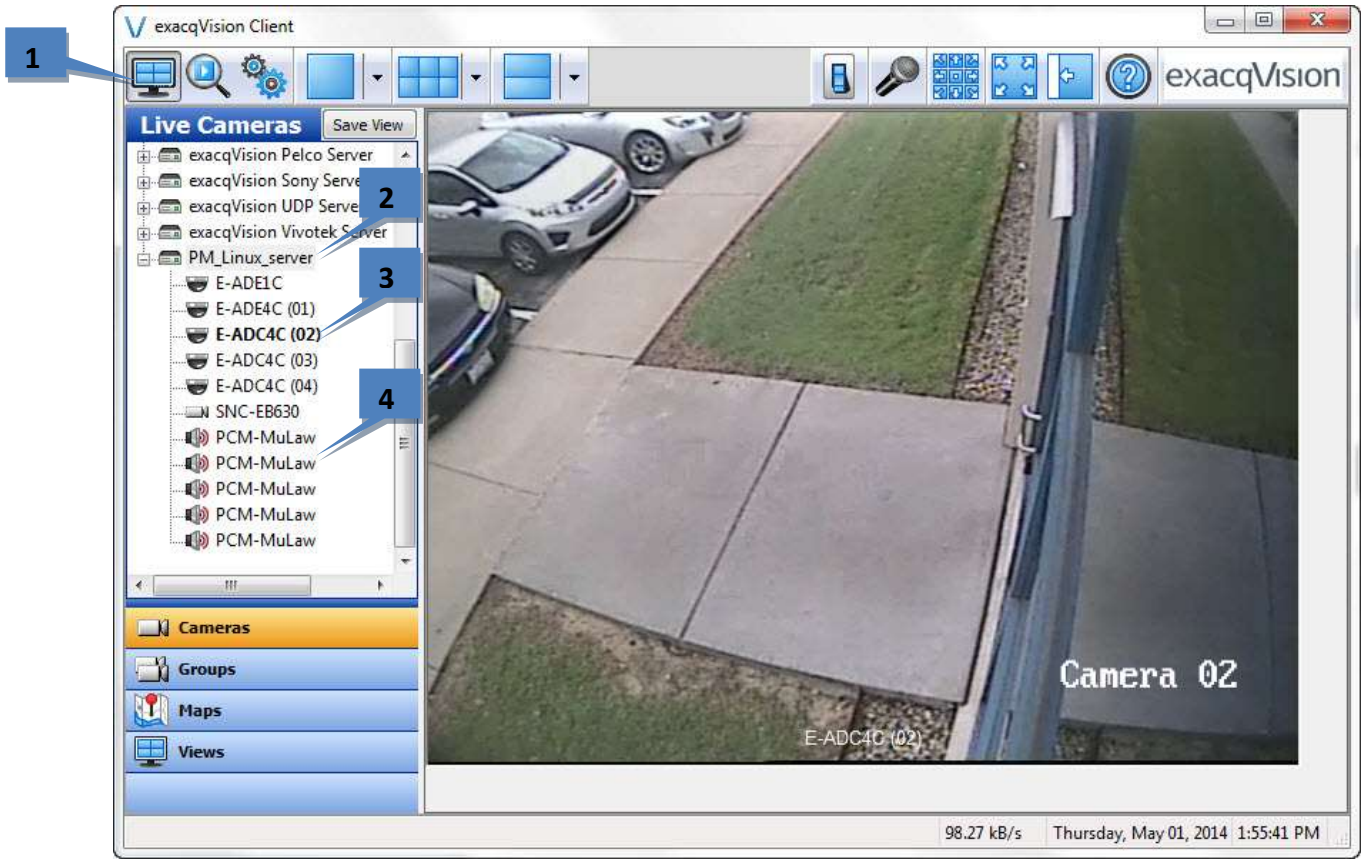
   **NOTE:** Alternatively, you can select Add (5d) next to the encoder’s entry, click Add Selected (5e), enter the username and password of the encoder in the pop-up box, and click OK.

6. Verify that the encoder has been added to the IP Camera List.
7. Look at the Status column to ensure the encoder is detected and connected.

## Verifying the Connection

To verify that the encoder is transmitting video and audio from its cameras to the exacqVision server, complete the following steps:

1. Open the exacqVision Client live page.
2. Expand the server in the site tree.
3. Select an encoder/channel combination to display video from the camera in the playback window.
4. If audio is connected, drag an audio channel into the playback window to verify the audio connection and transmission.



For complete information about exacqVision Client, click the Help button or download the user manual from https://exacq.com/support/specsheets.php?perma=exacqVision+User+Manuals.

# 5 Encoder Configuration Page

**NOTE:** Many common settings on the encoder, such as motion configuration and video settings, can be configured in exacqVision Client. The camera's web configuration page should be used primarily to configure features that cannot be changed using exacqVision Client.

The following web browsers can be used for access to the encoder's web configuration page:

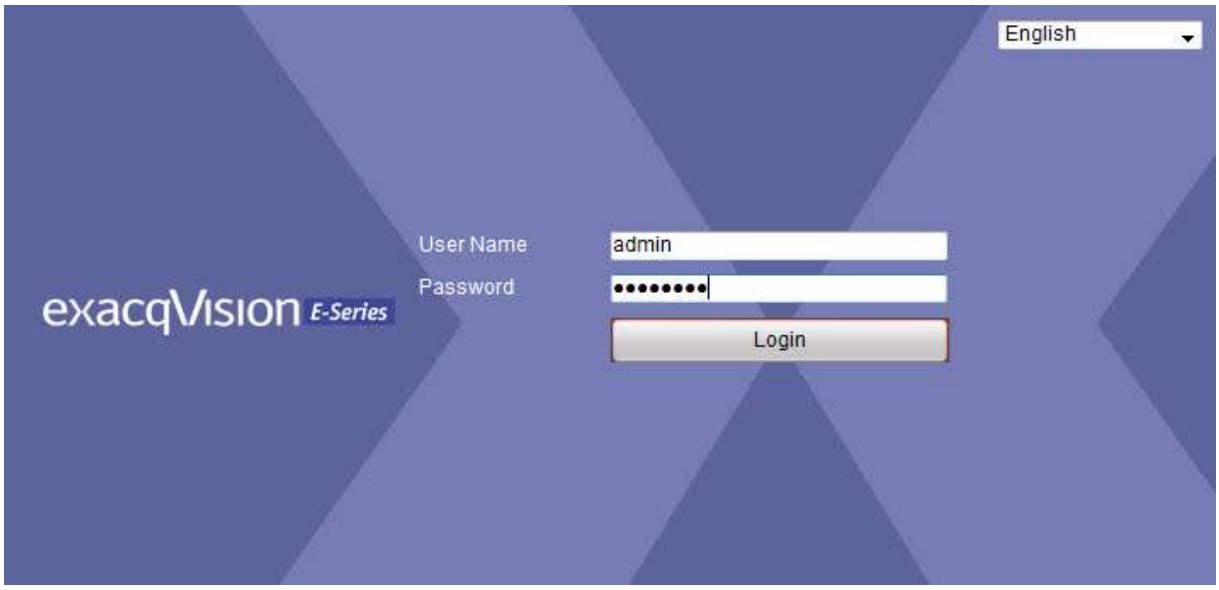
- Internet Explorer 6 and later
- Firefox 3.5 and later
- Chrome 8 and later
- Safari 5.0.2 and later
- Windows XP SP1 and later (32-bit)

You will need the following for access to the encoder's web configuration page:

- The network settings of device, as configured in the "Network Parameters" chapter of this document.
- A connection to the LAN for the encoder and a client computer.
- The username of the encoder (default: admin) and its password (default: admin256).

## Installing Web Components

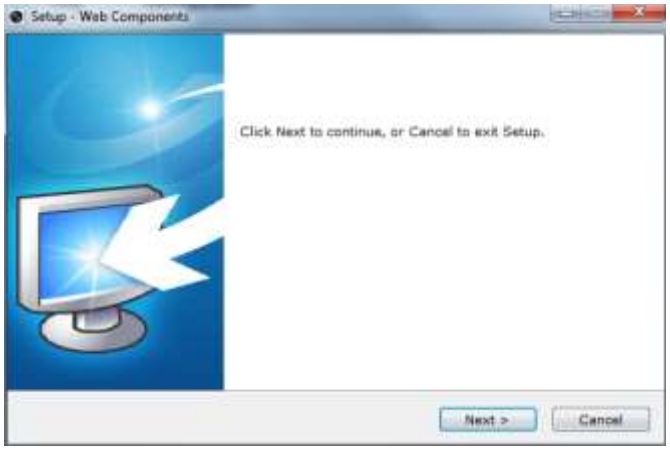
1. In the web browser, open the IP address of the encoder (such as http://192.0.0.64) and then press Enter to display the login interface.



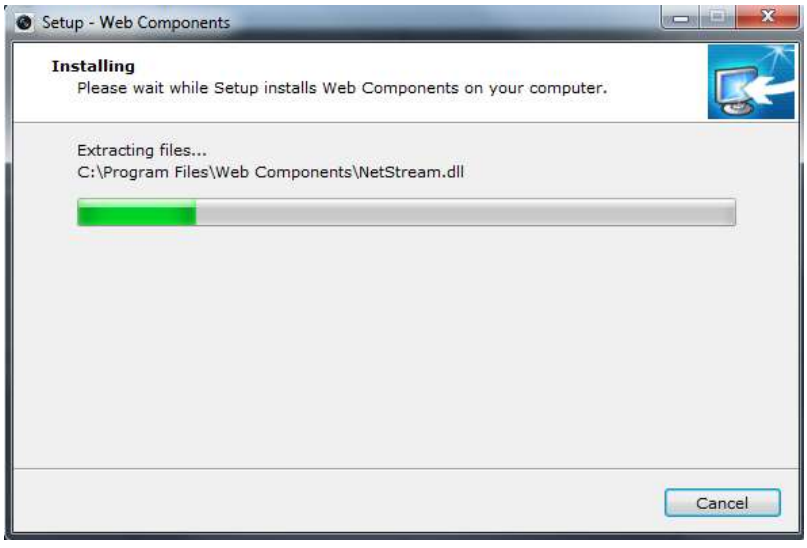

**NOTE:** When the HTTPS feature is enabled, the system will use the HTTPS login mode (https://*ipaddress*) by default. You can alternatively enter http://*ipaddress*/index.asp to use HTTP instead.

2. Enter the User Name (default: admin) and Password (default: admin256), and then click Login.
3. Download and install the plug-in if prompted.
4. Click on the live view panel by following the onscreen prompts.
5. Click Run or Save on the pop-up warning message box.

6. Click Next on the pop-up Setup dialog box.

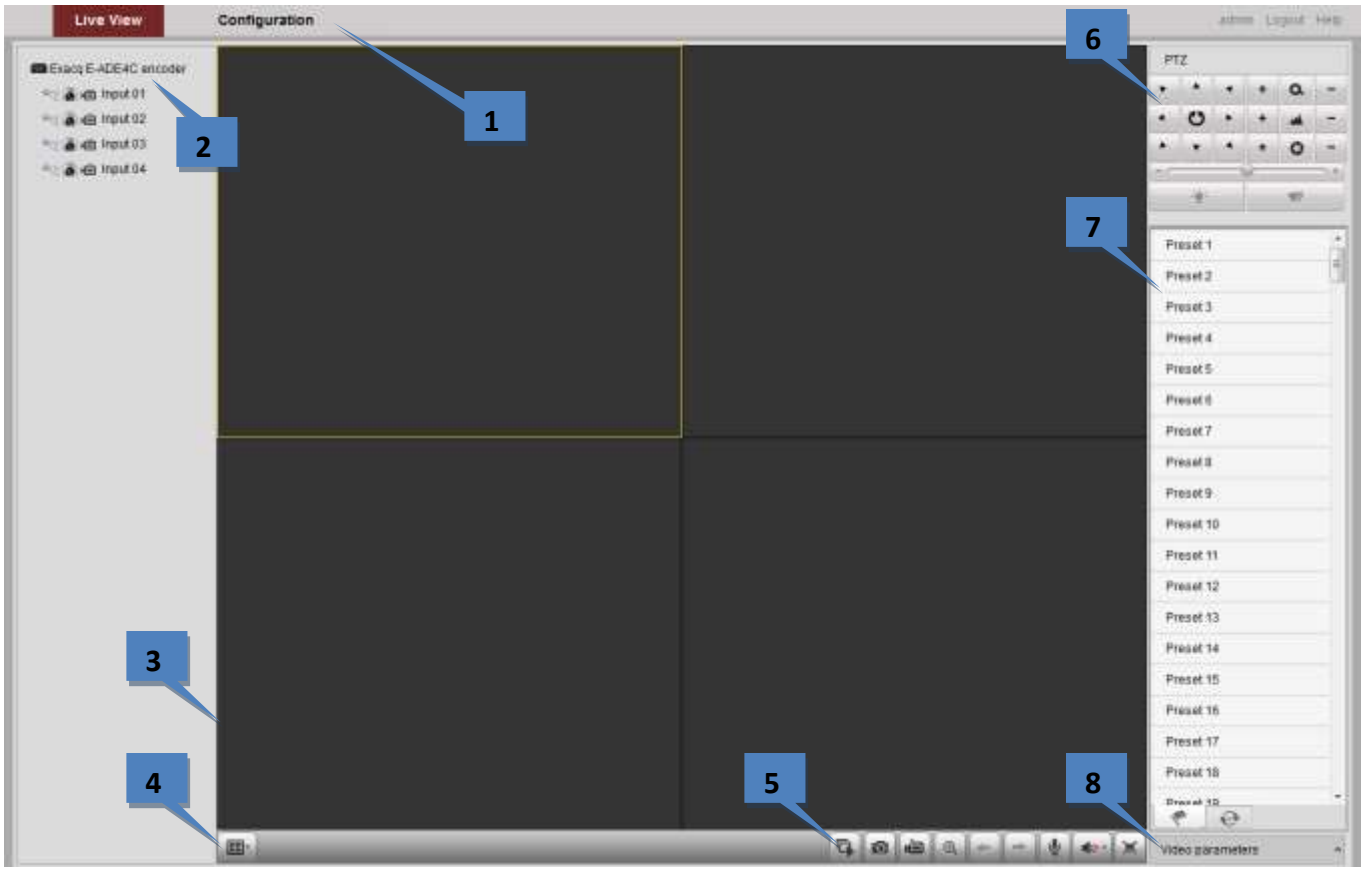



7. When the installation completes, click Finish to complete the installation of Web Components.



## Main Page

After successful login, the main page opens automatically.




The following features are available on this page:

1. **Menu Bar:** Enter the Live View and Configuration pages.
2. **Device List:** Display the connected encoder and its channels.
3. **Live Video Window:** Display the live video of the current camera.
4. **Window-division:** Choose a Live View display mode.
5. **Toolbar:** Control functions in live view mode, such as live view, audio on/off, two-way audio, and more.
6. **PTZ Control:** Control pan/tilt/zoom and the lighter and wiper controls.
7. **Preset Setting/Calling:** Set and call the preset for the camera (supports PTZ functions).
8. **Video Parameters menu:** Configure the brightness, contrast, hue, and saturation of live video. (Click the Video Parameters button to display the options.)

# 6 Live View

Live View shows you the video image transmitted from the connected camera in real time. After successful login, the system will open Live View automatically.

## Starting Live View

1. In the Live View window, select a video window.
2. Double-click a camera from the device list to start the Live View.

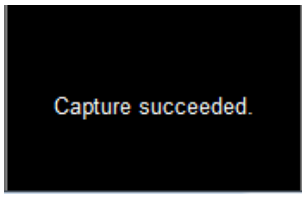
3. Click the button to start the Live View for all cameras on the device list. Additional toolbar buttons:

| Icon | Description |
|---|---|
| | Select the window-division mode. |
| / | Start/stop Live View. |
| | Capture pictures in Live View. |
| / | Manually start/stop recording. |
| | Enable e-PTZ. |
| | Previous page. |
| | Next page. |
| / | Audio on/off. |
| / | Start/stop two-way audio (Stream Type must be |

**TIP:** To display full-screen mode, double-click a live video window. To switch to the previously selected mode, double-click the live video window again.

## Capturing a Picture

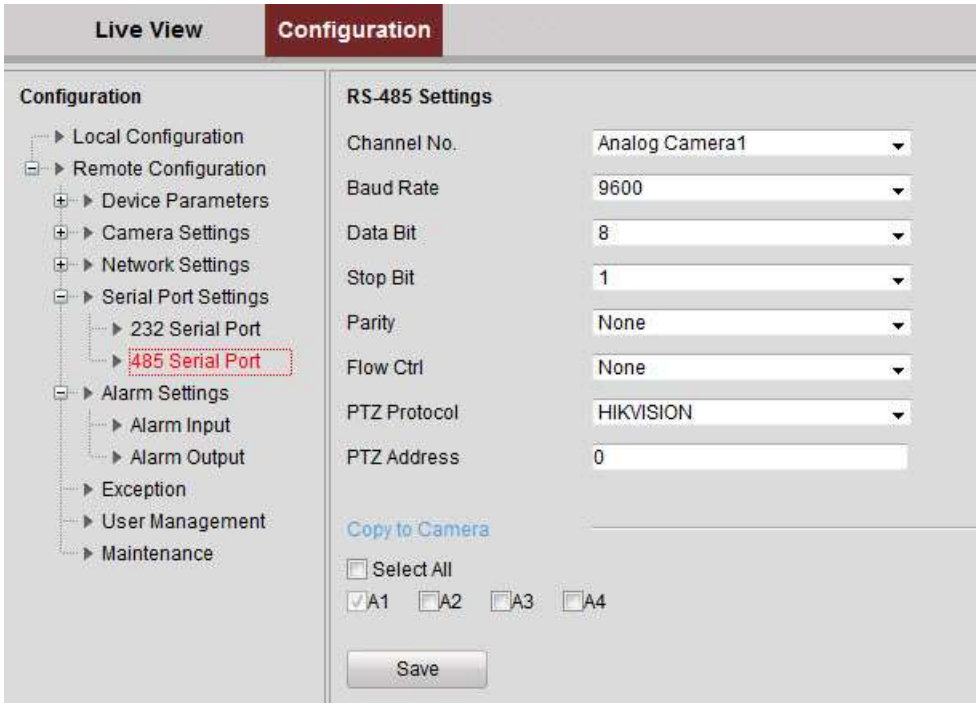
Click the button on the toolbar to capture live pictures in JPEG format. When the picture is captured, the following pop-up message box will appear at the lower right corner. The location where the picture is saved can be configured using the Local Configuration option on the Configuration page.



## Operating PTZ Controls

Before you operate PTZ controls:

1. Make sure the encoder is connected to a camera/dome that supports PTZ functions. Connect the *R+* and *R-* terminals of the device to RS-485 D+ and RS-485 D- terminals of the encoder.
2. The baud rate, PTZ control, and address are configured in the **RS-485 Settings** interface (on the **Remote Configuration menu**, select **Serial Port Settings** and then **485 Serial Port**).




The PTZ controls contain eight directional buttons (up, down, left, right, upper left, upper right, bottom left, bottom right).

The following controls are also available:

| Button | Description |
|---|---|
| | Zoom in/out |
| | Focus near/far |
| | Iris open/close |
| | Light |
| | Wiper |
| | Adjust speed of pan/tilt movement |

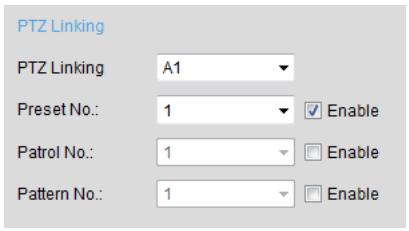
To configure presets, complete the following steps:

1. In live view mode, select a preset number from the preset list.

2. Use the PTZ control buttons to point the camera in the desired direction with the desired settings. You can use any of the following commands:
3. Click the icon to set the preset. Up to 256 presets are configurable, depending on the PTZ protocol applied.

To call a preset in Live View mode, select a predefined preset from the list and click the icon.

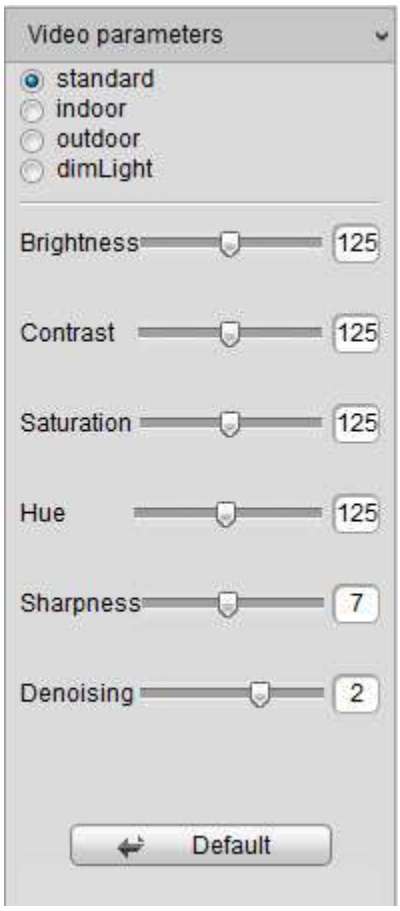
The preset can also be used to link to the alarm input when an alarm occurs.



## Configuring Video Parameters

Normally, video parameters such as brightness, contrast, saturation, and hue are controlled using exacqVision Client. However, these features can also be controlled on the web configuration page:

1. In Live View mode, click the Video parameters button at the bottom-right corner to display the Video Parameters Setting interface:




2. Select the mode according to different light conditions. Four modes are selectable:

   - **Standard:** Use for general lighting conditions (default).
   - **Indoor:** The image is relatively smoother.
   - **Outdoor:** The image is relatively clearer and sharper. The degree of contrast and saturation is high.
   - **Dim Light:** The image is smoother than the other three modes.

3. Move the slider to set the brightness, contrast, saturation and hue from 0 to 255. The default value is 128 for the brightness, contrast, and hue; the default value is 136 for the saturation.
4. Move the slider to set the sharpness from 0 to 15 and the denoising level from 0 to 3. The default value is 3 for the sharpness and 1 for the denoising level.

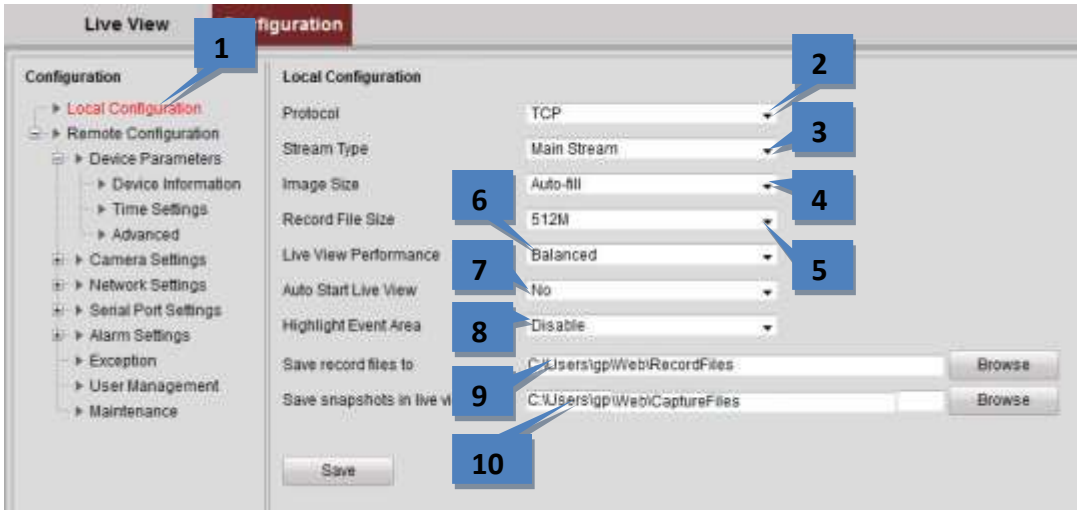
   **NOTE:** Click the Default button to restore the default settings.

# 7 Device Configuration

**NOTE:** Many common settings on the encoder, such as motion configuration and video settings, can be configured in exacqVision Client. The camera's web configuration page should be used primarily to configure features that cannot be changed using exacqVision Client.

## Local Configuration

1. Select **Local Configuration** on the **Configuration** page to open the Local Configuration interface:




The following settings can be configured on this page:

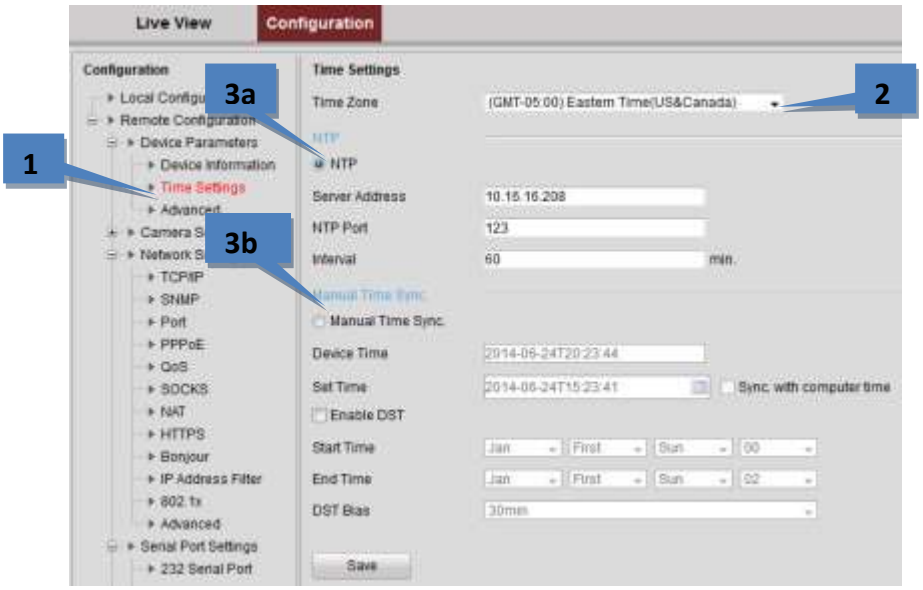
2. **Protocol Type:** Two stream transmission options are available:

   - **UDP:** provides real-time audio and video streams.
   - **TCP:** ensures complete delivery of streaming data and higher video quality, but with slightly slower transmission.

3. **Stream Type:** Select the web browser's live video stream type (Main Stream or Sub Stream). See "Configuring Video Settings" in this manual**Error! Reference source not found.** for more information.
4. **Image Size:** Select the window-division view mode (4:3, 16:9, or Auto-fill).
5. **Record File Size:** Select the size of packed video files during manual recording (256MB, 512MB, or 1GB).
6. **Live View Performance:** Set the live viewing performance to Shortest Delay, Real Time, Balanced, or Fluency.
7. **Auto Start Live View:** Select No or Yes.
8. **Highlight Event Area:** Select Enable or Disable.
9. **Save Record Files To:** Click Browse or manually enter the path for the manually recorded video files.
10. **Save Snapshots in Live View To:** Click Browse or manually enter the path for the manually captured pictures in Live View mode.

## Configuring Time Settings

1. On the **Remote Configuration menu**, select **Device Parameters**, and then **Time Settings** to open the Time Settings interface:

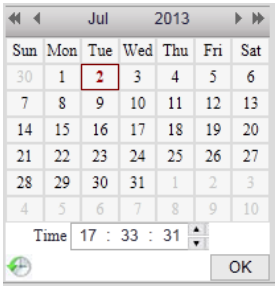



2. Select the Time Zone from the drop-down menu.
3. Select a time synchronization mode:

   - **NTP:** A Network Time Protocol (NTP) Server can be configured on your device to ensure the accuracy of system date/time. If the device is connected to a DHCP network with time server properties configured, the camera will synchronize automatically with the time server. If you select this option, enter the NTP server's IP address, port, and frequency of synchronization (from 1 to 10,080 minutes).

     **NOTE:** If the device is connected to a public network, you should 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 device is in a customized network, NTP software can be used to establish an NTP server for time sync.

   - **Manual Time Sync.:** If you select this option, click the icon to set the date from the pop-up calendar. You can click the icon to select the time.



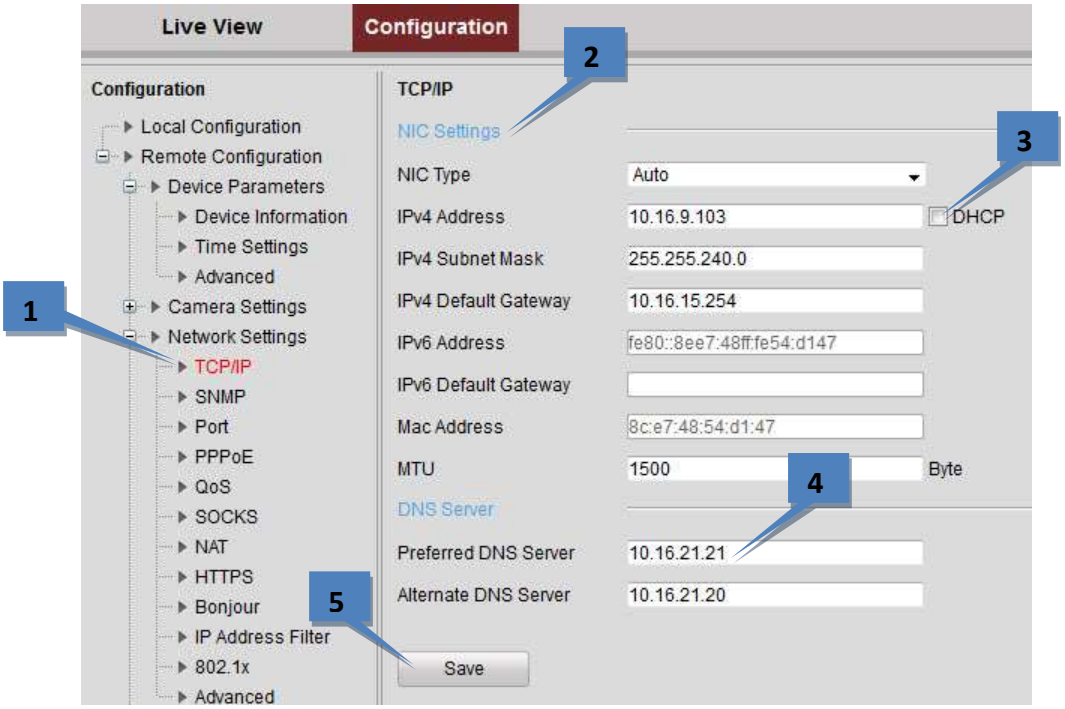

   You can also select **Sync. with Computer Time** to synchronize the time with the local computer, and enable daylight saving time (DST) and its parameters if observed in the local area.

4. Click the **Save** button to save the settings.

# 8 Network Settings

## Configuring TCP/IP Settings

1. From the **Remote Configuration menu**, select**> Network Settings** and then **TCP/IP** to open the TCP/IP Settings interface:

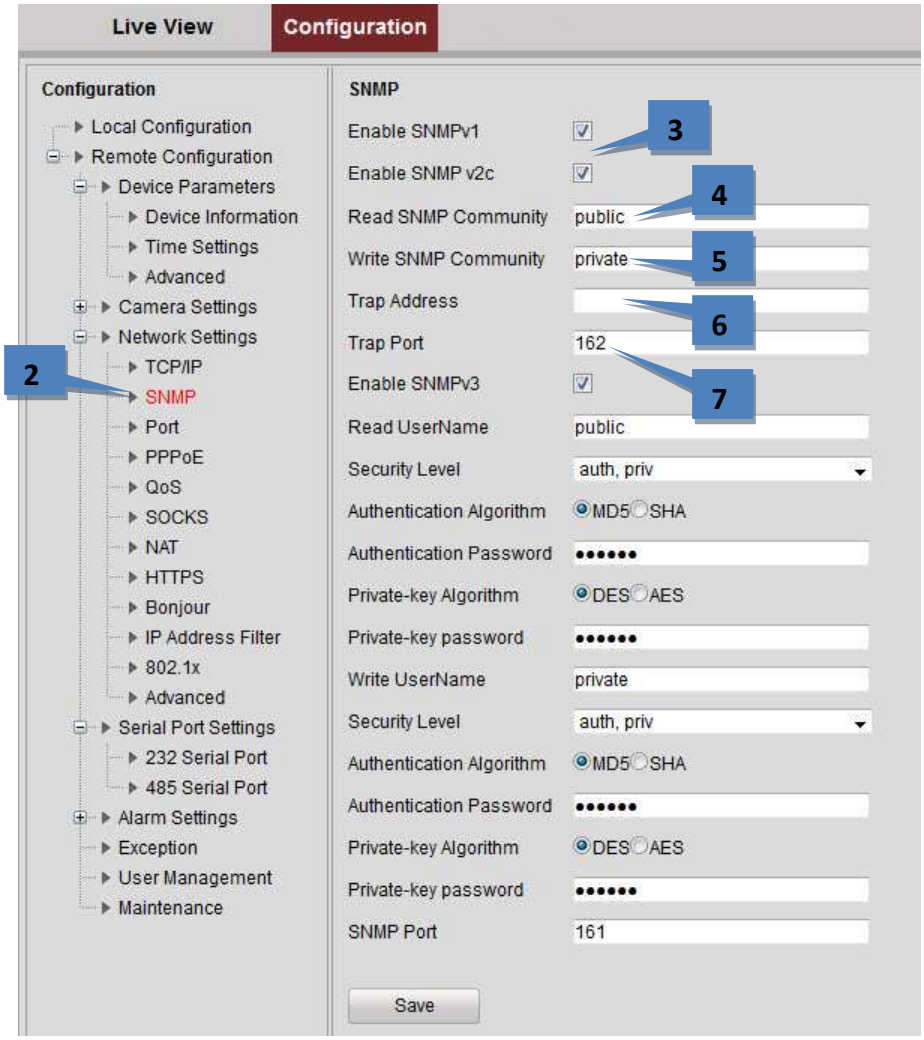



2. Configure the NIC settings, including the NIC Type, IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, and MTU settings (500 to 1500).
3. If the DHCP server is available, select DHCP to automatically obtain an IP address and other network settings from that server.
4. If the DNS server settings are required for some applications, configure the Preferred DNS Server and Alternate DNS Sever here.
5. Click the **Save** button to save the above settings.

## Configuring SNMP Settings

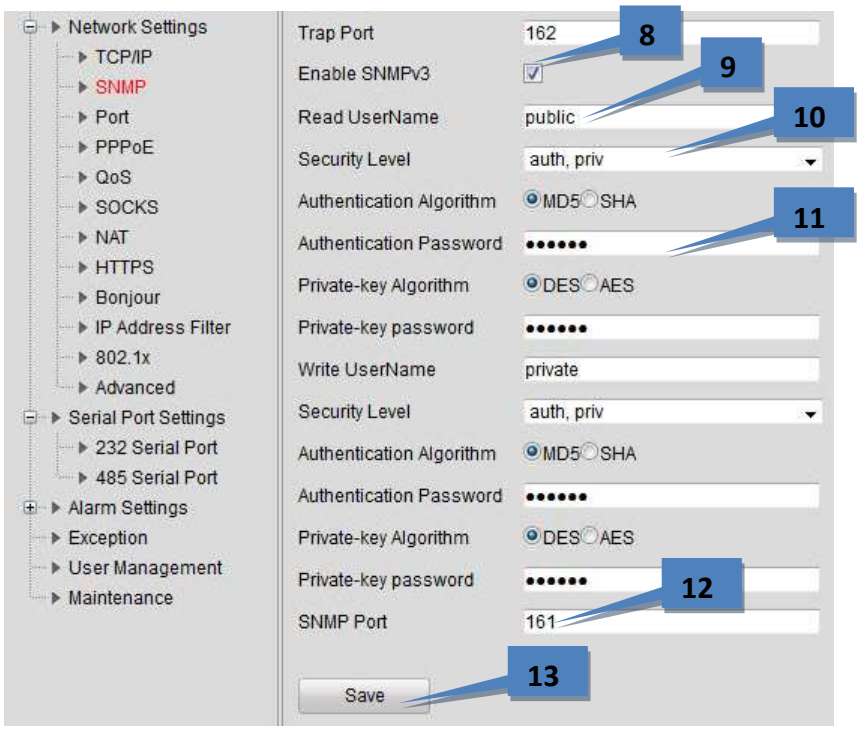
Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. If your environment uses a network management system, you can use SNMP to get camera status, parameters, and alarm-related information.

1. Before setting the SNMP, download the SNMP software. By setting the Trap Address, the device can send the alarm event and exception messages to the surveillance center.
2. From the **Remote Configuration menu**, select **Network Settings** and then **SNMP** to enter the SNMP settings interface.
3. Select SNMP v1 or SNMP v2c. You can enable both SNMP v1 and SNMP v2c.
4. Configure the Read SNMP community (default: public)
5. Configure the Write SNMP community (default: private)
6. Configure the Tap Address (default: [blank])
7. Configure the Trap Port (default: 162).



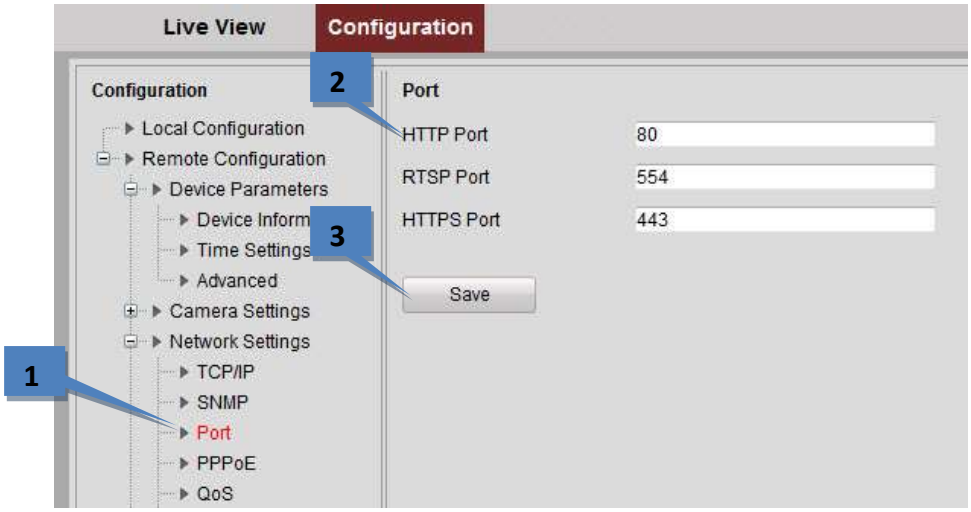

The rest of the SNMP configuration is discussed on the following page.

8. If needed, enable SNMPv3
9. Configure the read username (default: public).
10. Select the security level to “auth, priv”, “auth, no priv”, or “no auth, no priv.”
11. If the security level is set to “auth, priv”, you can configure the Authentication Algorithm and Private-key Algorithm parameters. If the security level is set to “no auth, no priv”, you cannot configure the Authentication Algorithm and Private-key Algorithm parameters.
12. Set the SNMP port (default: 161).
13. Click **Save** to save the settings.



## Configuring Port Settings

1. From the **Remote Configuration menu**, select **Network Settings** and then **Port** to open the Port Settings interface:

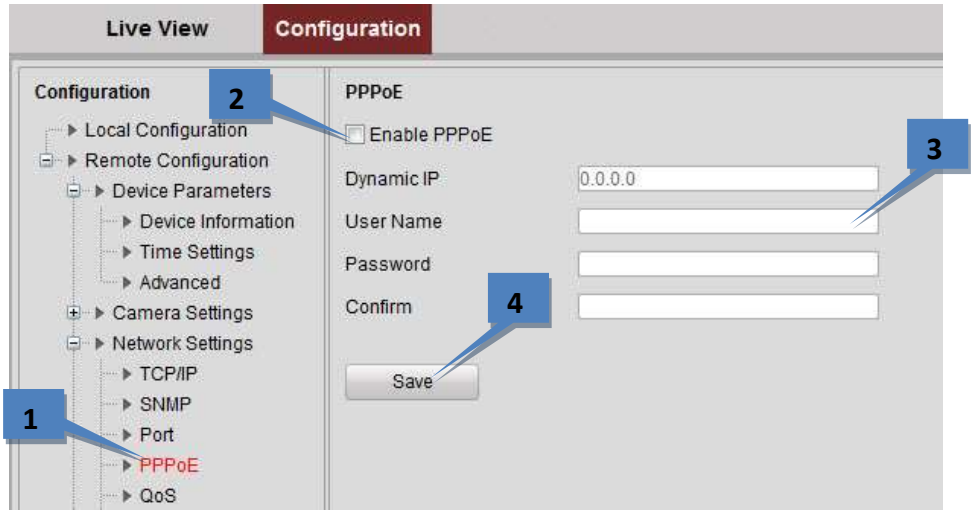



2. Set the HTTP port (default: 80), RTSP port (554), and HTTPS port (443) of the camera.
3. Click **Save** to save the settings. A system restart is required to activate changed settings.

## Configuring PPPoE Settings

Access by Point-to-Point Protocol over Ethernet (PPPoE) is also available.

1. From the **Remote Configuration menu**, select **Network Settings** and then **PPPoE Settings** to open the PPPoE settings interface:

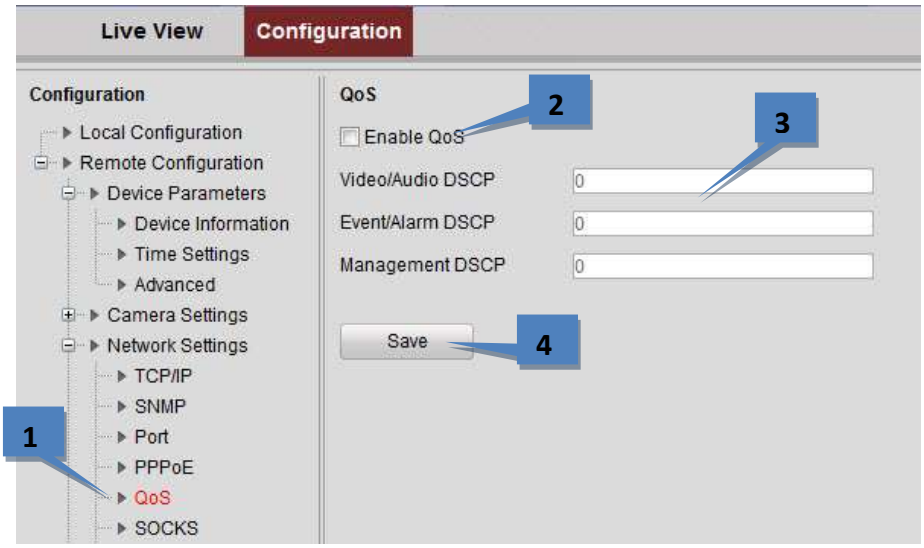



2. Select the **Enable PPPoE** checkbox.
3. Enter the **User Name**, **Password**, and **Confirm Password** for PPPoE access. These must be assigned by the ISP.
4. Click the **Save** button to save and exit.

## Configuring QoS Settings

QoS (Quality of Service) can help solve network delays and congestion by configuring the priority of data sending. The use of a QoS-aware network can prioritize traffic and thus allow critical flows to be served before flows with lesser priority. The encoder can mark the data packets for video/audio, event/alarm, and management network traffic with different DSCP values, which identify different priority levels of data sending.

1. From the **Remote Configuration menu**, select **Network Settings** and then **QoS** to open the QoS settings interface:




2. Select the **Enable QoS** checkbox.
3. Enter the DSCP (Differentiated Services Codepoint) value for the video/audio, event/alarm, and management traffic. This value is used to mark the traffic's IP header. The DSCP value defines the priority level for the specified type of traffic, such as how much bandwidth to reserve for it. The valid value range of the DSCP is 0-63. The higher DSCP value indicates a higher priority level.
4. Click **Save** to save the settings and then restart the encoder.

## Configuring SOCKS Settings

SOCKet Secure (SOCKS) is an Internet protocol that routes network packets between a client and server through a proxy server. This feature is useful if the encoder is located on a local network behind a firewall, yet alarms need to be sent to a destination outside the local network (such as the Internet). SOCKS4 and SOCKS5 are supported, and SOCKS5 additionally provides authentication so only authorized users may access a server.

1. From the **Remote Configuration menu**, select **Network Settings** and then **SOCKS** to open the SOCKS Settings interface:

2. Select the Enable SOCKS checkbox.
3. Configure the following settings:

   - **Server**: Enter the address of the SOCKS server.
   - **Server Port**: Enter the port of the SOCKS server (default: 1080).
   - **Server Type**: Select the server type ( SOCKS4 or SOCKS5). If you select SOCKS5, you can enable the user authentication on the server and then enter the login username and password.
   - **Local networks**: Define the local network segment that does not need to use SOCKS proxy server. You can enter multiple network addresses and use a semicolon (;) to separate them ("10.0.0.0/255.0.0.0; 172.16.0.0/255.240.0.0").

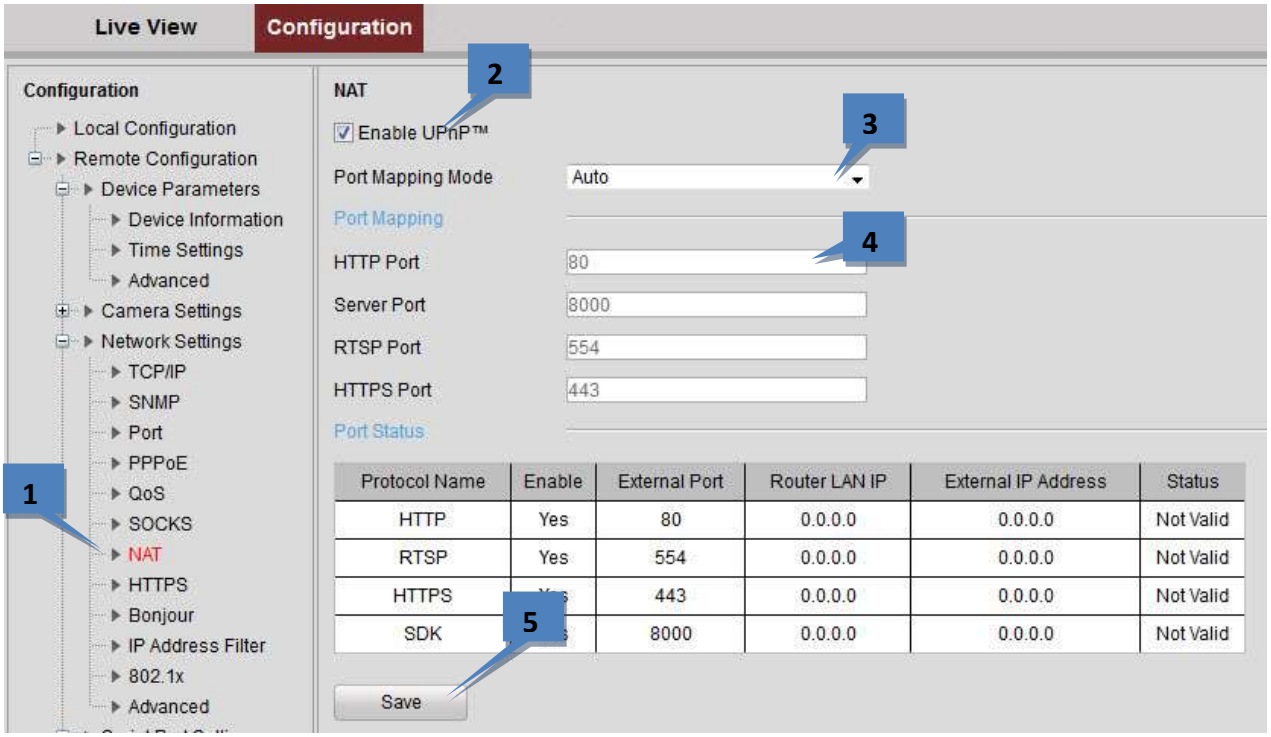
4. Click **Save** to save the settings.

## Configuring NAT/UPnP™ Settings

UPnP™ can permit the device to seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, and more. If you want to use the UPnP™ function to enable the fast connection of the device to the WAN via a router, you should configure the UPnP™ parameters of the device. **UPnP™ must be enabled for exacqVision to discover the encoder.**

If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

1. From the **Remote Configuration menu**, select **Network Settings** and then **NAT** to open the NAT settings interface.




2. Select the Enable UPnP™ checkbox.
3. Select the Port Mapping Mode:

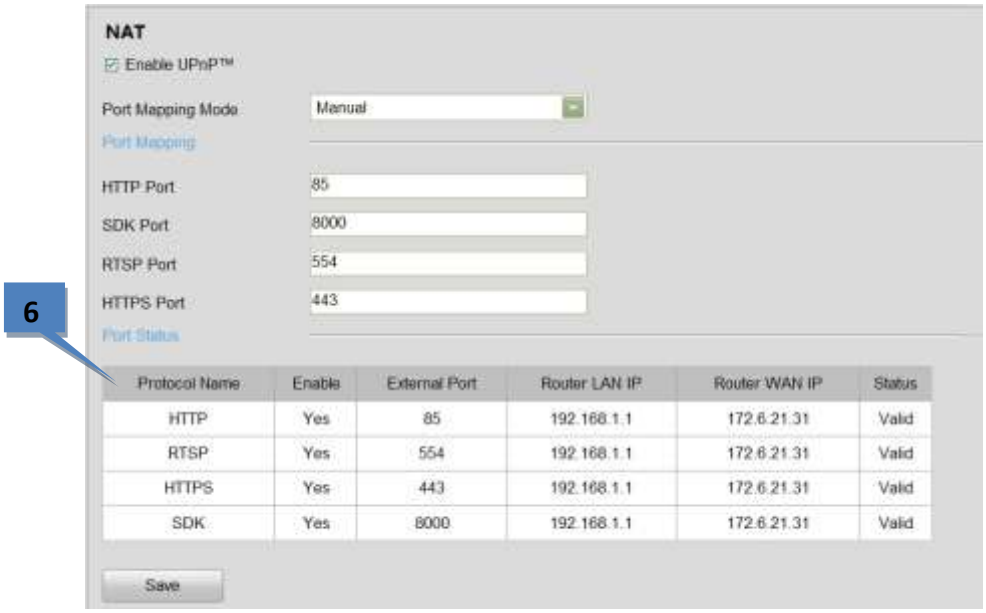
   - **Auto**: The mapping ports are automatically assigned by the router.
   - **Manual**: Continue with the following steps to edit the mapping ports.

4. Configure the HTTP Port (for access by WEB browser), SDK Port Mapping (for access by client software), RTSP Port, and HTTPS Port.

   **NOTES:** You can use the default port No., or change it according to actual requirements. The Ports indicate the port NUMBER for mapping in the router.

5. Click **Save** to save the settings.

6. You can view the status of the port mapping in the Port Status area.

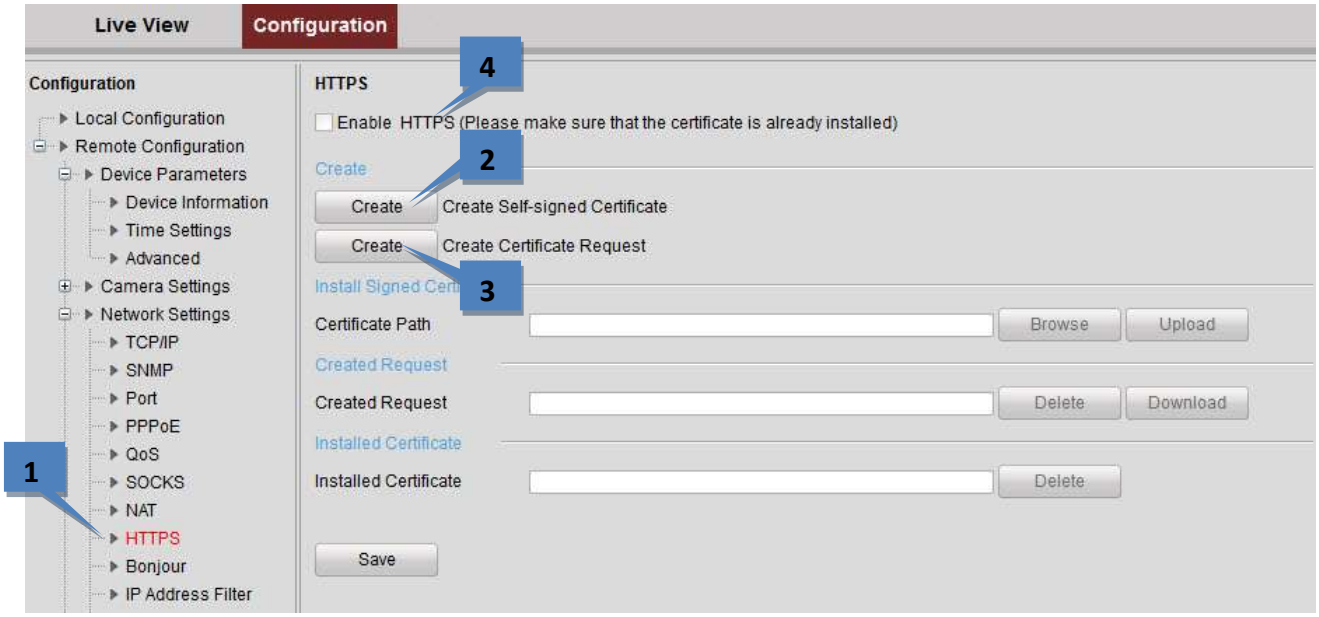


## Configuring HTTPS Settings

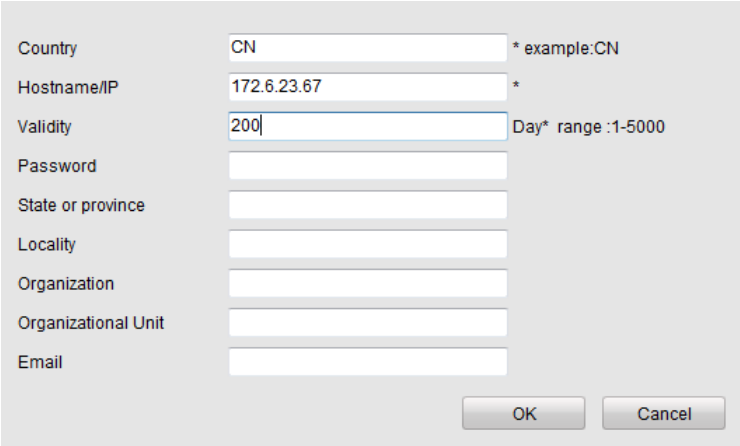
HTTPS (Hyper Text Transfer Protocol Secure) ensures the data transferred is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). HTTPS provides authentication of the web site and associated web server that one is communicating with and create a secure channel over an insecure network.

HTTPS URLs begin with "https://" and use port 443 by default.

1. From the **Remote Configuration menu**, select **Network Settings** and then **HTTPS** to open the HTTPS settings interface.




2. Click Create to create the self-signed certificate or authorized certificate. This opens the following window.




- Enter the country, host name/IP, validity, and other information.
- Click **OK** to save the settings.

3. Create the authorized certificate:

    - Click the **Create** button to create the certificate request.
    - Download the certificate request and submit it to the trusted certificate authority for signature.
    - After receiving the signed valid certificate, import the certificate to the device.

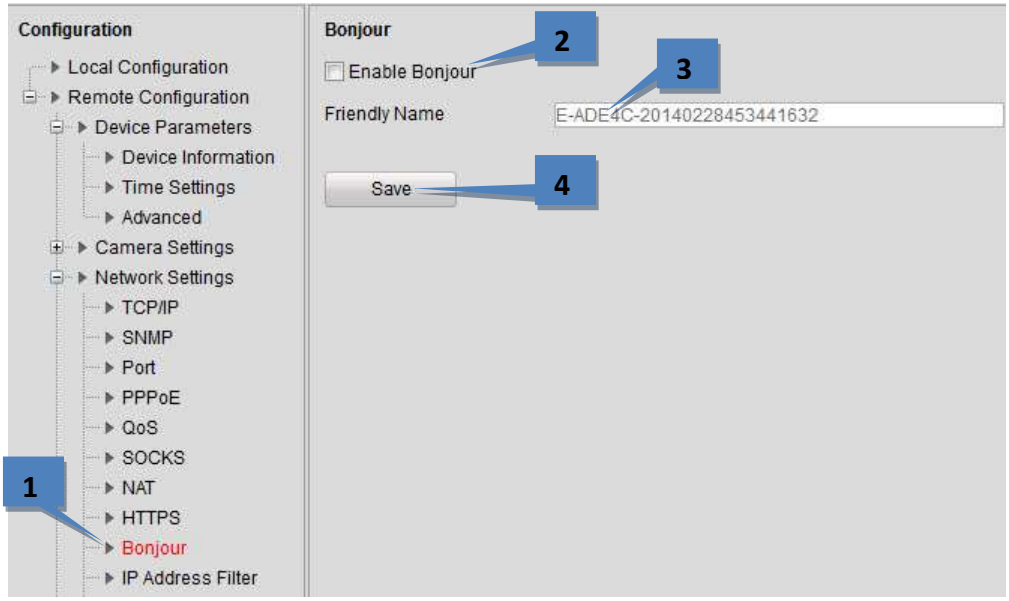
4. After you have successfully created and installed the certificate, select the Enable HTTPS checkbox.

After the HTTPS feature is enabled, the system will use the HTTPS login mode by default when you input the IP address (such as https://192.0.0.64). You can also input http://IP address/index.asp (such as http://192.0.0.64/index.asp) if you want to use HTTP mode to log in to the device.

## Configuring Bonjour Settings

Bonjour is enabled by default, and the video encoder can be automatically detected by operating systems and clients that support this protocol. Make sure you have installed the Bonjour plug-in on your PC before enabling the Bonjour function.

1. From the **Remote Configuration menu**, select **Network Settings** and then **Bonjour** to open the Bonjour settings interface.

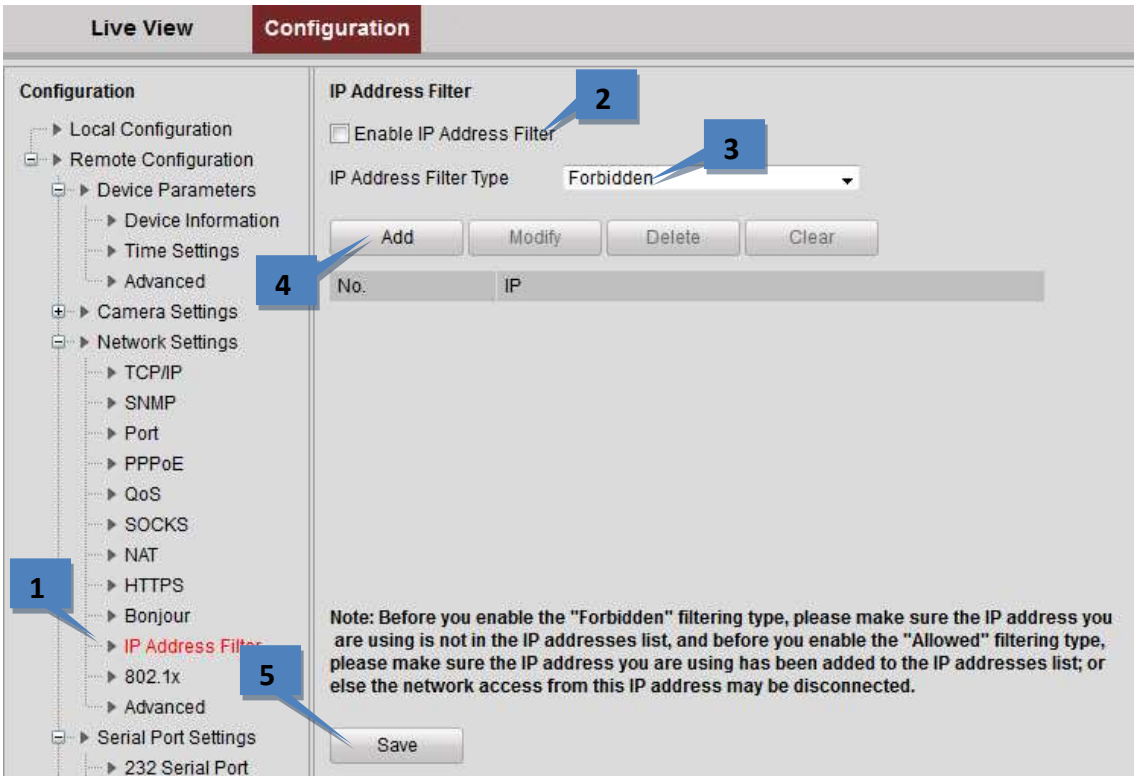



2. Select the Enable Bonjour checkbox.
3. Edit the name of device. The name is shown when the device is detected by the system. Only letters, numbers, and hyphens ("-") can be contained in the name.
4. Click **Save** to save the settings.

## Configuring IP Address Filter

You can allow or forbid access by specified IP addresses to the encoder by enabling IP Address Filter**.** Up to 256 IP address can be added to the list (allowed/forbidden) by Web Browser.

1. From the **Remote Configuration menu**, select **Network Settings** and then **IP Address Filter** to open the IP address filter settings interface.



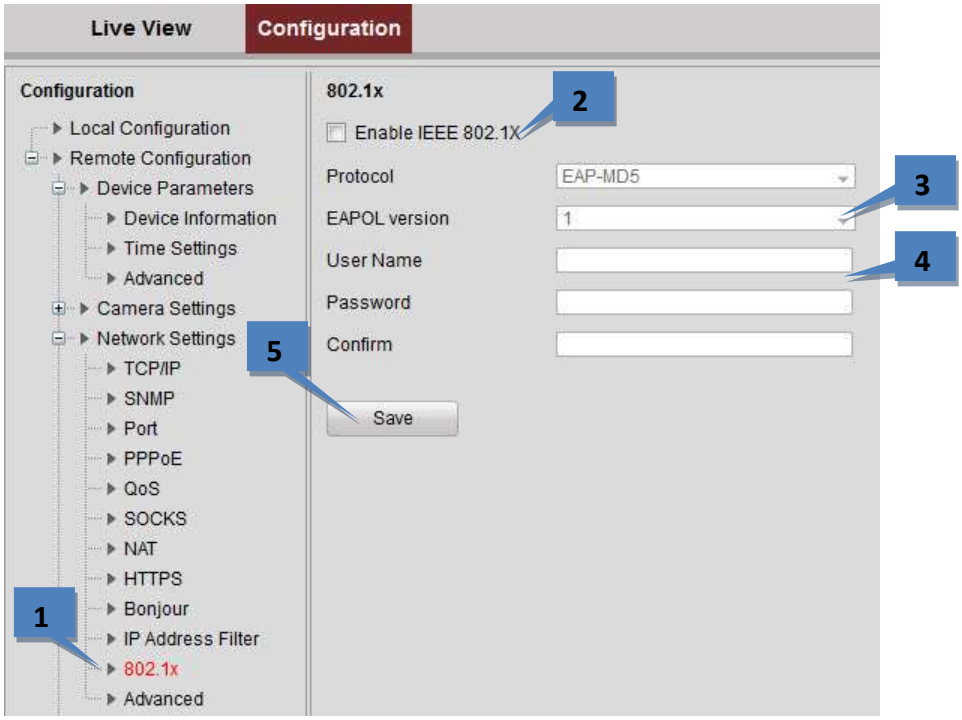

2. Select the **Enable IP Address Filter** checkbox.
3. Select the filter type of IP address (**Allowed** or **Forbidden)**.
4. Click the **Add** button to add the IP address to the selected filter type list.

5. Click **Save** to save the settings.

## Configuring IEEE 802.1x Settings

You can use IEEE 802.1x as an authentication mechanism if using a LAN or WLAN.

1. From the **Remote Configuration menu**, select **Network Settings** and then **802.1x** to open the IP address filter settings interface.

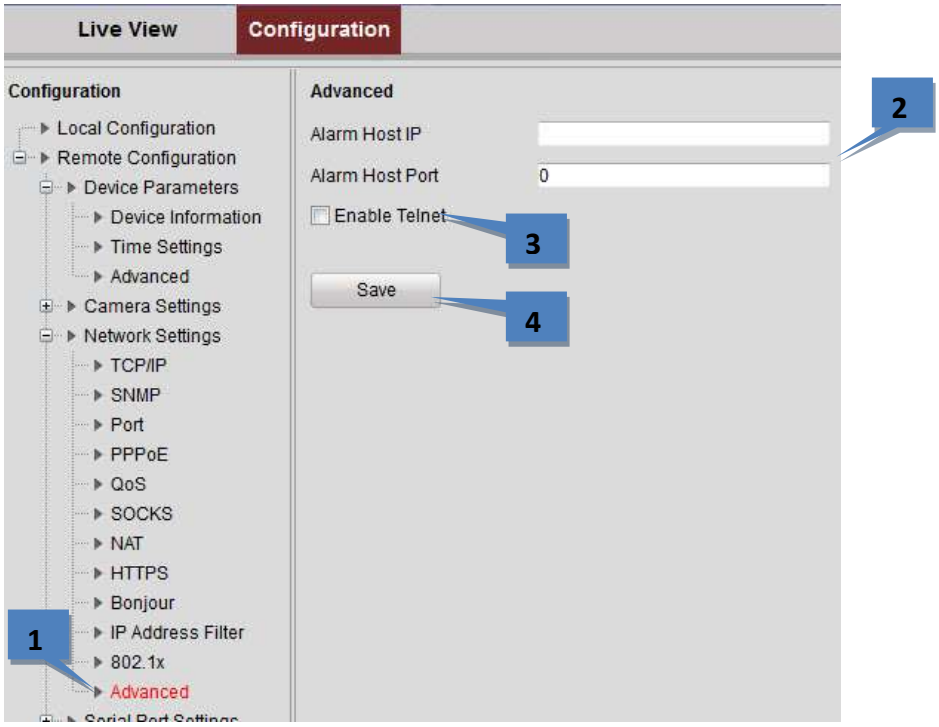



2. Select the **Enable IEEE 802.1X** checkbox.
3. The **Protocol** is automatically selected. Select **EAPOL Version** 1 or 2.
4. Enter the login credentials.
5. Click **Save** to save the settings.

## Configuring Advanced Settings

The Advanced page allows you to configure an alarm host.

1. From the **Remote Configuration menu**, select **Network Settings** and then **Advanced** to enter the Advanced interface.




2. Enter the IP address and port of the alarm host.
3. Select **Enable Telnet** if required.
4. Click **Save** to save the settings.

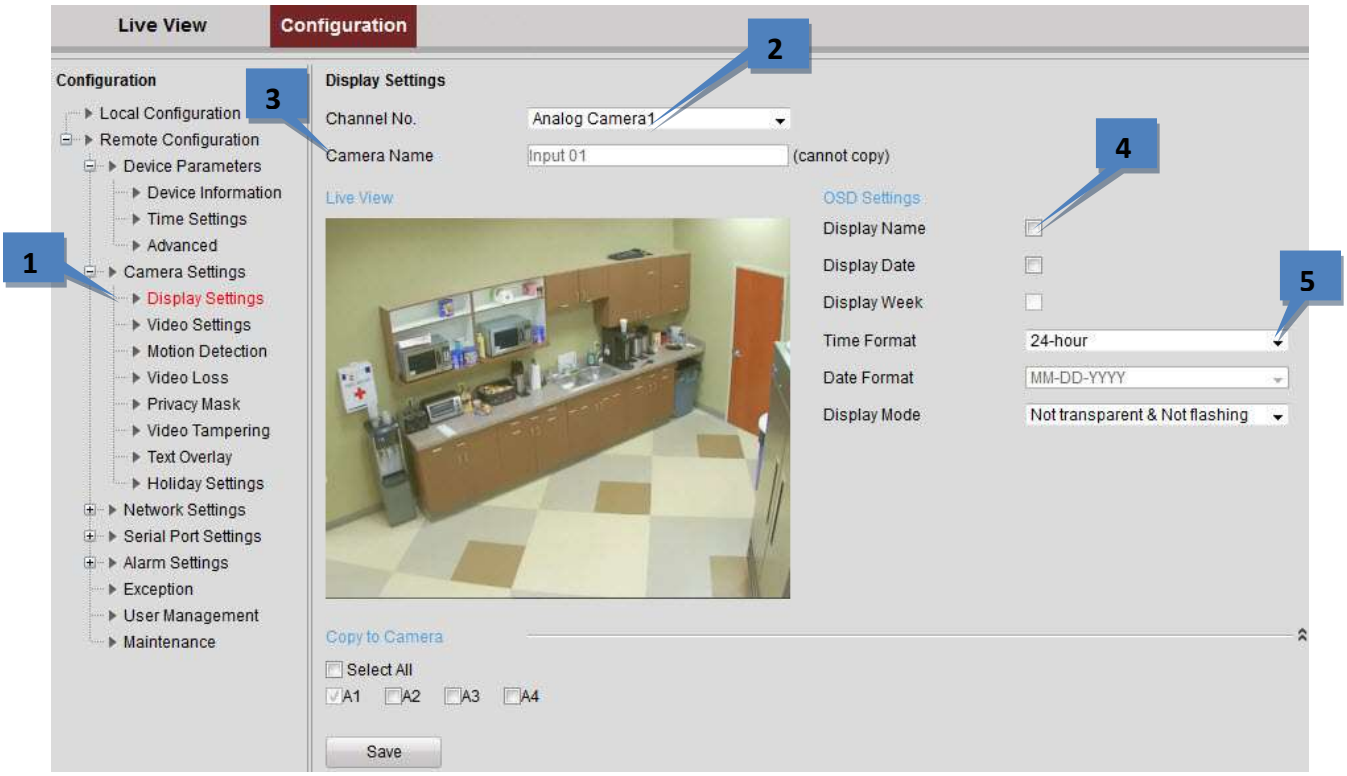
# 9 Camera Settings

**NOTE:** Many common settings on the encoder, such as motion configuration and video settings, can be configured in exacqVision Client. The camera's web configuration page should be used primarily to configure features that cannot be changed using exacqVision Client.

## Configuring Display Settings

To configure onscreen display, complete the following steps:

1. On the **Remote Configuration menu**, select **Camera Settings** and then **Display Settings** to open the Display Settings interface:




2. Select the camera from the **Channel No.** drop-down list.
3. Edit the camera name in the **Camera Name** field.
4. Select the display of camera name, date, or week by selecting the checkboxes (if required).
5. Set the **Time Format**, **Date Format**, and **Display Mode** by selecting them from the drop-down lists.

6. In the preview image, you can adjust the OSD location on the screen by moving the text frame.

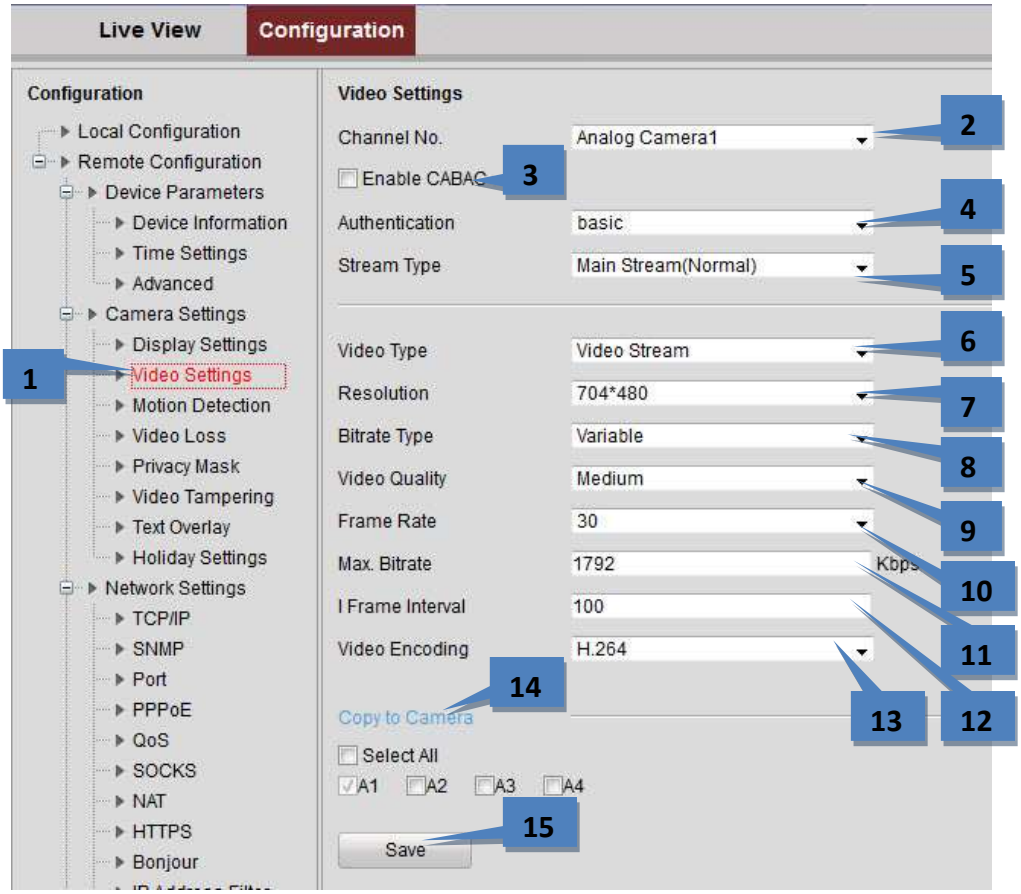
7. To copy the display settings of the current camera to other cameras, expand the **Copy to Camera** panel and select the cameras, or click **Select All** to select all cameras.

8. Click **Save** to activate the settings.

## Configuring Video Settings

To configure video settings, complete the following steps:

1. From the **Remote Configuration menu**, select **Camera Settings** and then **Video Settings** to open the Video Settings interface:



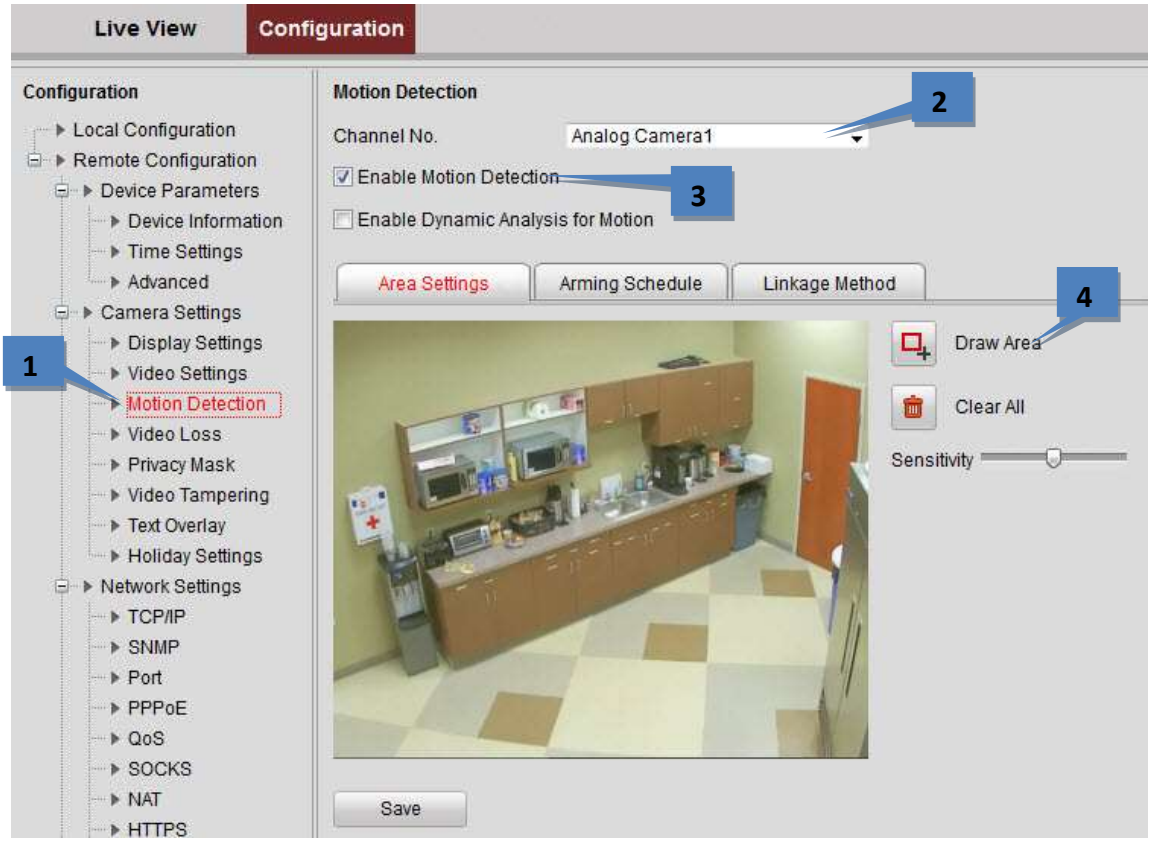

2. Select the **Channel** from the drop-down list.
3. Select the **Enable CABAC** checkbox if applicable.
4. Select Enable or Basic from the **Authentication** drop-down list.
5. Select the **Stream Type** of the camera: Main Stream (Normal), Main Stream (Event), or Sub Stream. The main stream is usually for recording and live viewing with good bandwidth, and the sub stream can be used for live viewing when the bandwidth is low.
6. Select the video type (Video Stream or Video&Audio). The audio signal will be recorded only when the **Video Type** is **Video&Audio**.
7. Select the **Resolution** of the video input.
8. Select the **Bitrate Type** (**Constant** or **Variable**).
9. If the bitrate is **Variable**, select the **Video Quality**. Up to six levels of video quality can be configured.
10. Set the **Frame Rate** from 1 to 30 fps (or 1 to 15 fps if Video Encoding is set to MJPEG).
11. Set the **Max. Bitrate** from 32 to 8192 Kbps. This is not configurable if Video Encoding is set to MJPEG.
12. Set the **I Frame Interval** from 1 to 400. A higher value results in lower video quality.
13. Set the **Video Encoding** standard to H.264 or MJPEG.
14. To copy the display settings of the current camera to other cameras, expand the **Copy to Camera** panel and select the cameras, or click **Select All** to select all cameras.
15. Click **Save** to activate the settings.

## Configuring Motion Detection

Motion detection can trigger an alarm and record video when motion is observed in the camera view. To configure motion detection, complete the following steps:

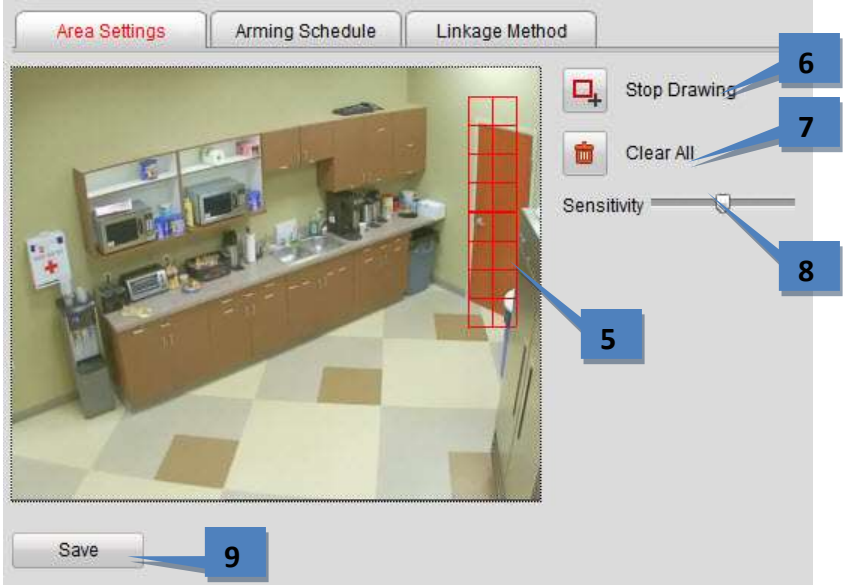
### Set the Motion Detection Area

1. From the **Remote Configuration menu**, select **Camera Settings** and then **Motion Detection** to open the Motion Detection settings interface.




2. Select the **Channel** from the drop-down list.
3. Select the **Enable Motion Detection** checkbox.
4. Click the **Draw Area** button.

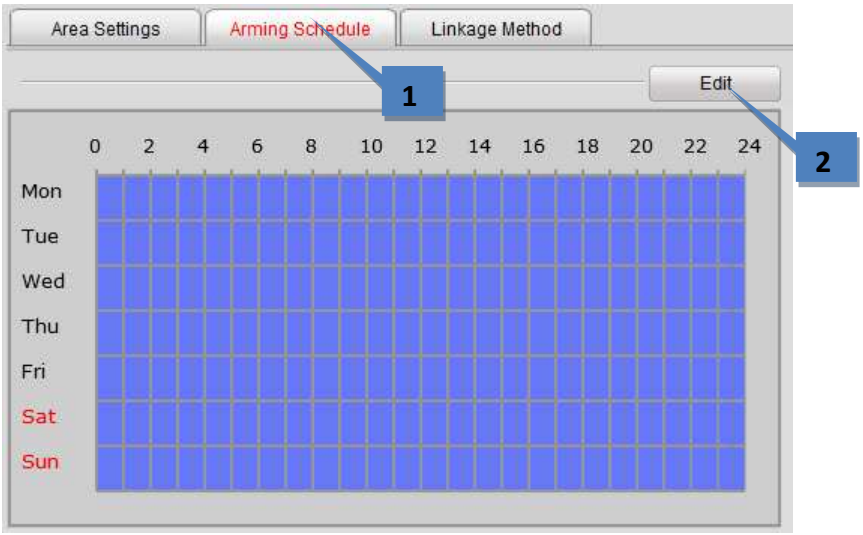
5. Draw the motion detection area by clicking and dragging the mouse in the live video image. Up to eight motion detection areas can be drawn in the same image.



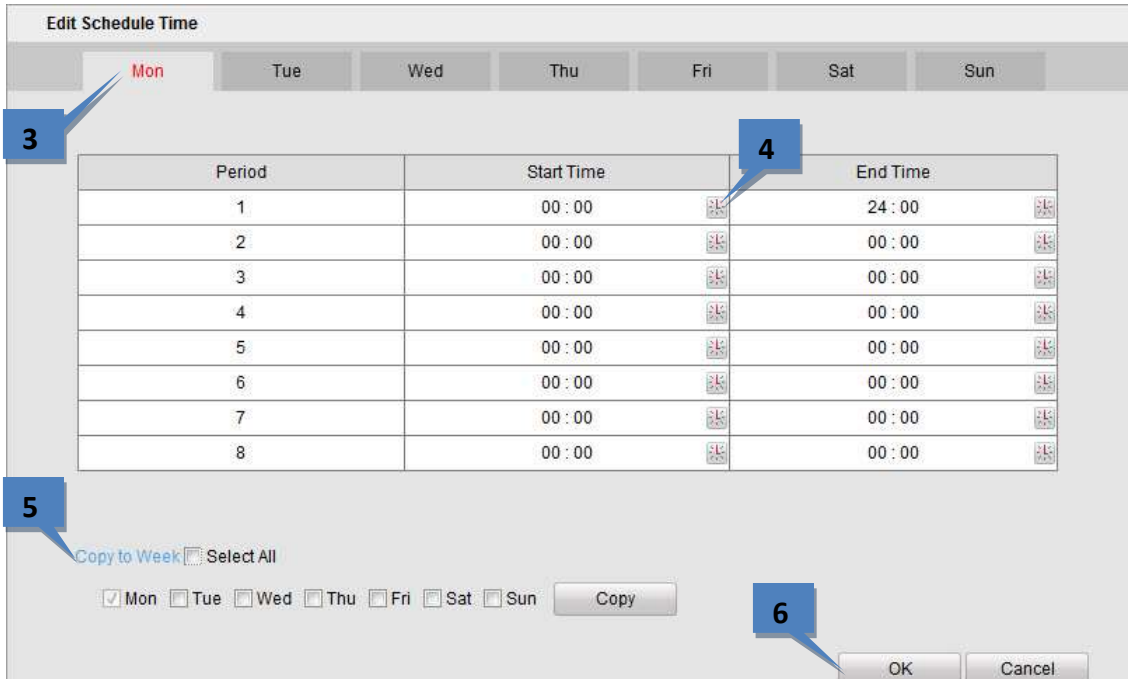

6. Click the **Stop Drawing** button to finish drawing.
7. Click the **Clear All** button if you want to clear all areas.
8. Move the **Sensitivity** slider bar to set the sensitivity of the camera.
9. Click the **Save** button to save the settings.

**Set the Arming Schedule for Motion Detection**

1. Select the **Arming Schedule** tab.




2. Click the **Edit** button to open the **Edit Schedule Time** window.




**NOTE:** The time of each segment cannot be overlapped. Up to eight segments can be configured for each day. The **Holiday** option is available in the Schedule drop-down list after you have enabled a holiday schedule in **Holiday** settings.

3. Choose the day you for which want to set the arming schedule.
4. Click the clock buttons to set the time period for the arming schedule.
5. Copy the schedule to other days, if desired.
6. Click the **OK** button to save the settings.

**Set the Alarm Actions Taken for Motion Detection**

1. To specify the alarm type when an event is triggered, select the **Linkage Method** tab.

2. Select the alarming linkage methods:

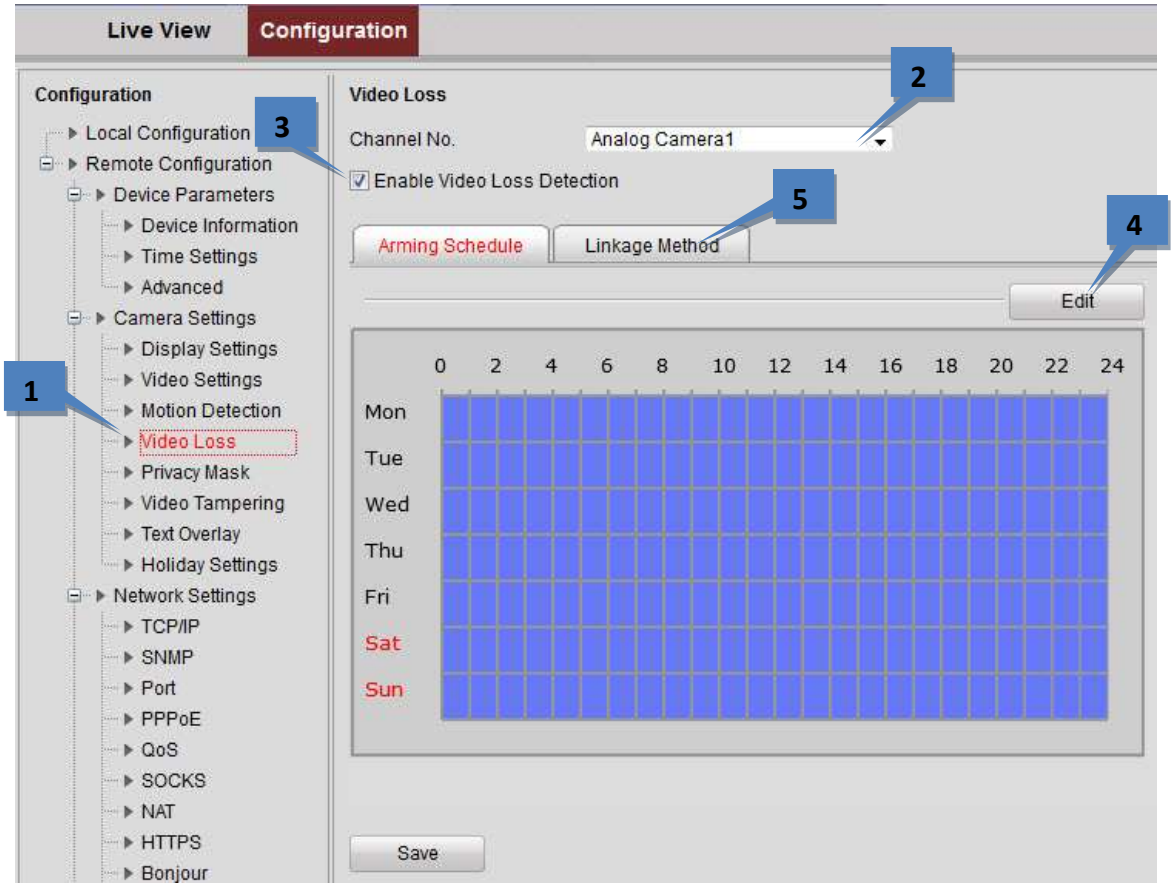
   - **Full Screen Monitoring**
   - **Audible Warning**
   - **Notify Surveillance Center**

3. Select the **Alarm Output** to trigger.
4. Select the **Trigger Channel**.

## Configuring a Video Loss Alarm

To configure the video loss alarm, complete the following steps:

1. From the **Remote Configuration menu**, select **Camera Settings** and then **Video Loss** to open the video loss alarm setting interface.

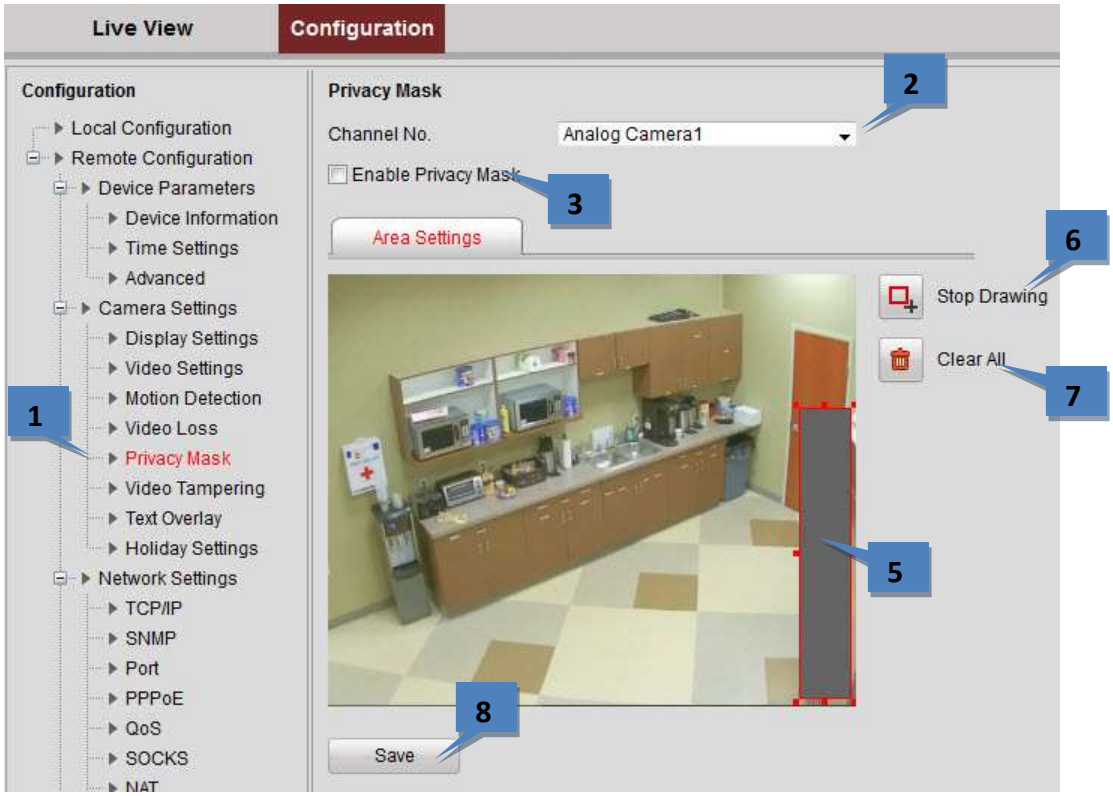



2. Select the **Channel** for which to configure the video loss alarm.
3. Select Enable Video Loss Detection checkbox.
4. Click **Edit** to edit the arming schedule for video loss detection. The arming schedule configuration is the same as setting of the Arming Schedule for Motion Detection.
5. Click the **Linkage Method** tab to set the actions taken for the video loss alarm.

## Configuring a Privacy Mask

A Privacy Mask enables you to cover certain areas on the video of the channel to from live viewing and recording. To configure the privacy mask, complete the following steps:

1. From the **Remote Configuration menu**, select **Camera Settings** and then **Privacy Mask** to open the Privacy Mask settings interface.

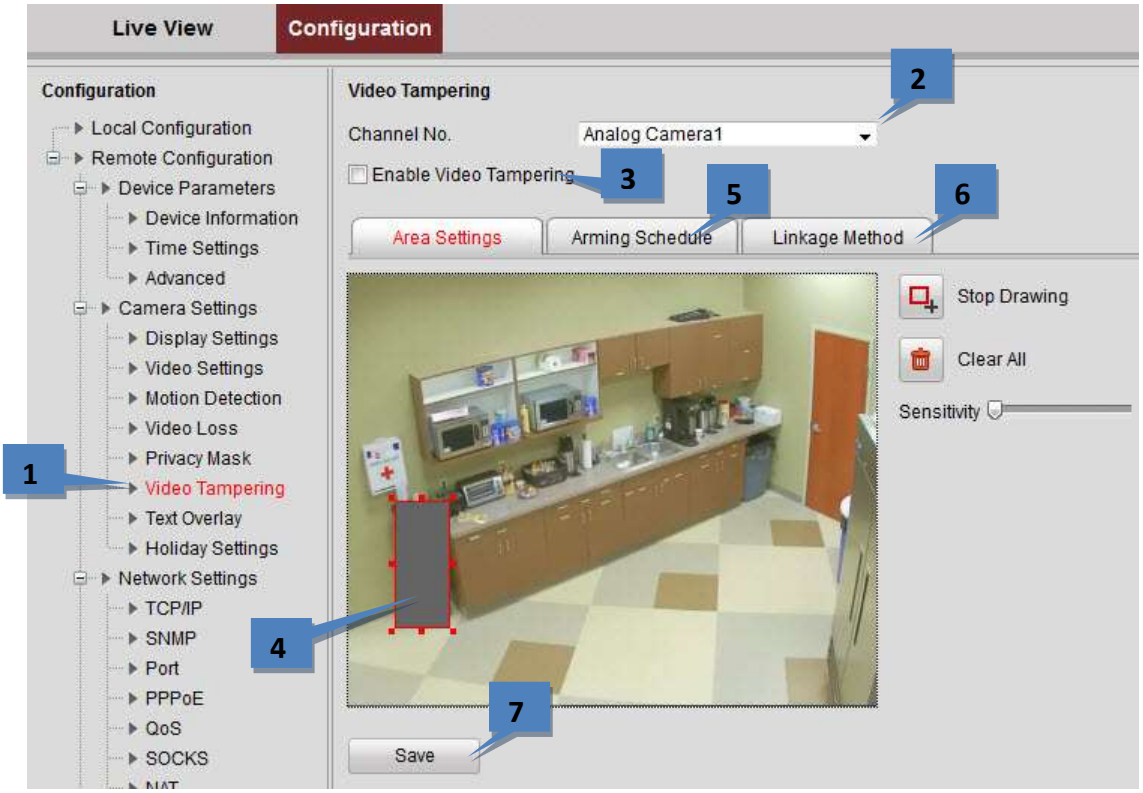



2. Select the **Channel** for which to configure the privacy mask.
3. Select the **Enable Privacy Mask** checkbox.
4. Click the **Draw Area** button (not shown).
5. Draw the mask area by clicking and dragging the mouse in the live video image. Up to four privacy mask areas can be configured.
6. Click the **Stop Drawing** button to finish drawing.
7. You can click the **Clear All** button to clear all of the areas without saving it.
8. Click **Save** to save the settings.

## Configuring Video Tampering

To configure video tampering, complete the following steps:

1. From the **Remote Configuration menu**, select **Camera Settings** and then **Video Tampering** to open the Video Tampering interface.
2. Select the **Channel** for which to configure the tamper-proof detection alarm.




3. Select the **Enable Video Tampering** checkbox.
4. Draw the tampering area.
5. On the Arming Schedule tab, Click **Edit** to edit the arming schedule for tampering. The arming schedule configuration is the same as for the Arming Schedule for Motion Detection.
6. Select the **Linkage Method** tab to set the actions taken for the tampering alarm.
7. Click **Save** to save the settings.

## Configuring Text Overlay

To configure the text overlay, complete the following steps:

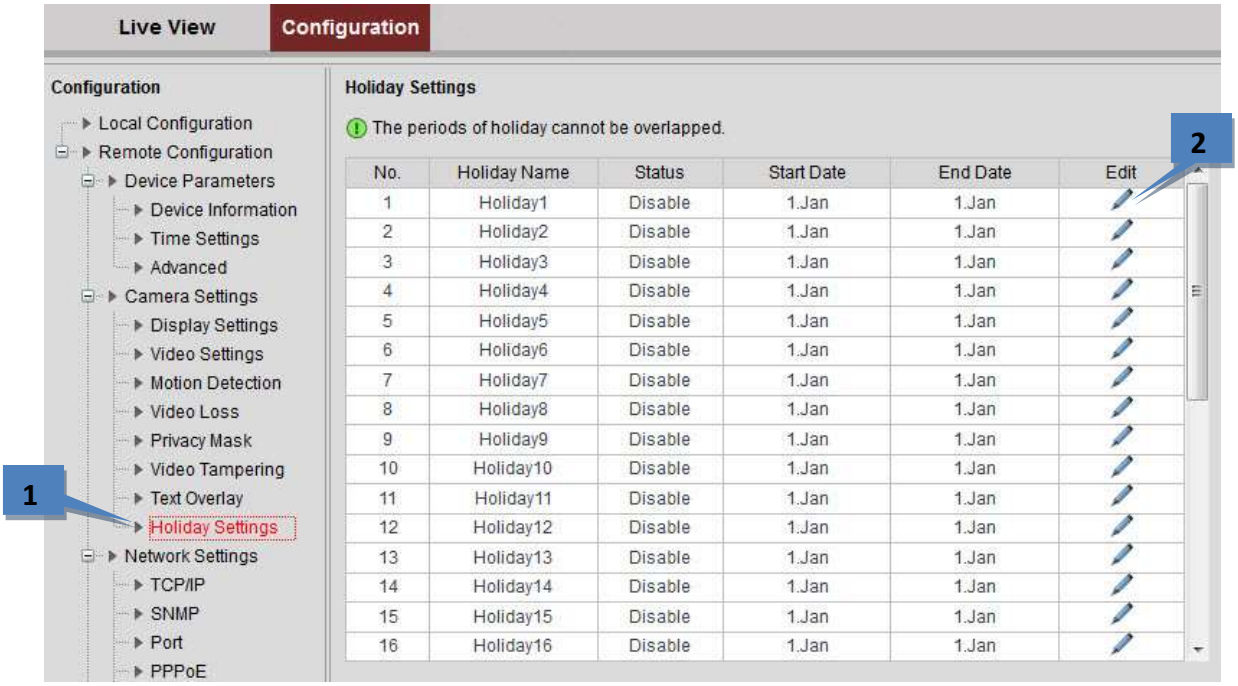
1. From the **Remote Configuration menu**, select **Camera Settings** and then **Text Overlay Settings** to open the Text Overlay Settings interface.

2. Select the **Channel** from the drop-down list.
3. Edit the user-defined text content.
4. Select the checkbox to display the text in the overlay.
5. In the preview image, you can adjust the text location on the screen by moving the text frame.
6. To copy the text overlay settings of the current camera to other cameras, expand the **Copy to Camera** panel and select the cameras, or click **Select All** to select all cameras.
7. Click **Save** to activate the settings.

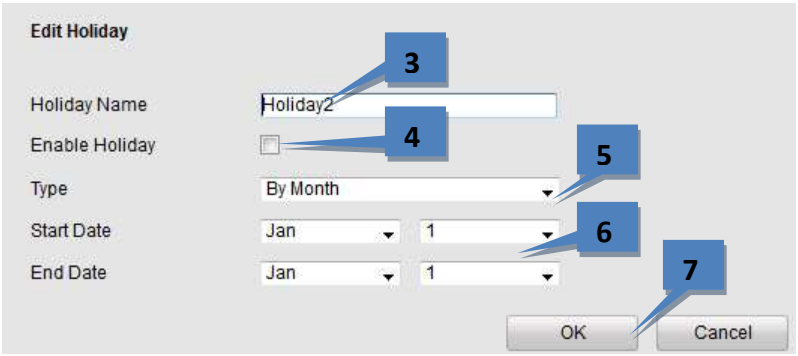
## Configuring Holiday Settings

If you want a  separate recording schedule on holidays, complete the following steps:

1. From the **Remote Configuration menu**, select **Camera Settings** and then **Holiday Settings** to open the Holiday Settings interface.




2. Select an item from the list and click the pencil button to edit the holiday.
3. Edit the holiday name.
4. Select the checkbox to enable the holiday's schedule.
5. Select the time interval (**By Date**, **By Week**, or **By Month**).
6. Set the **Start Date** and **End Date**.
7. Click **OK** to save the settings and go back to the Holiday Settings interface.




8. Verify the finished holiday settings on the list.
9. Repeat the same steps to configure up to 32 holiday settings.

**NOTE:** The **Holiday** option is available in the Schedule drop-down list when you have enabled holiday schedule in **Holiday settings**.

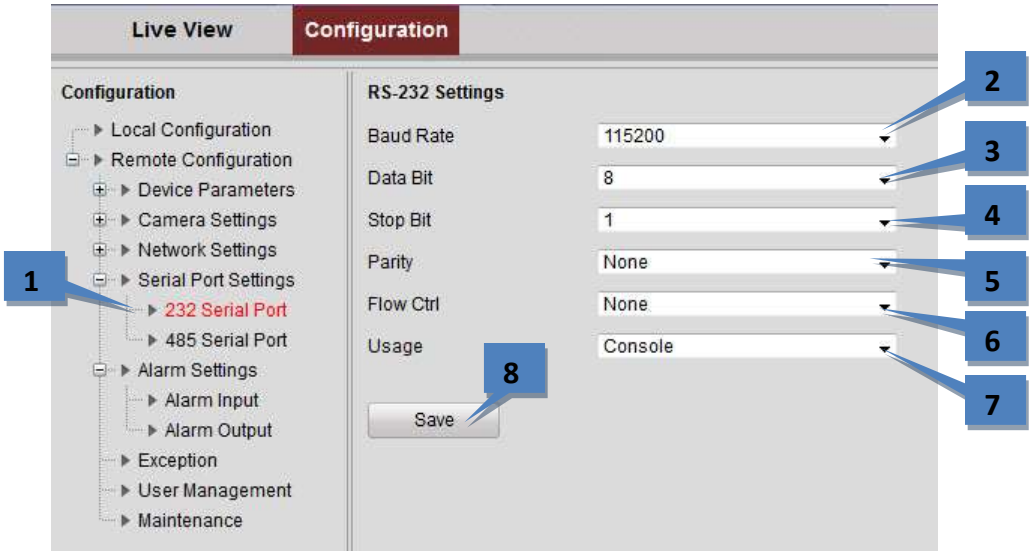
# 10 RS-232 and RS-485 Settings

**NOTE:** RS-232 is not available on one-channel encoders.

## Configuring RS-232

To configure RS-232, complete the following steps:

1. From the **Remote Configuration menu**, select **Serial Port Settings** and then **232 Serial Port** to enter the RS-232 port setting interface:



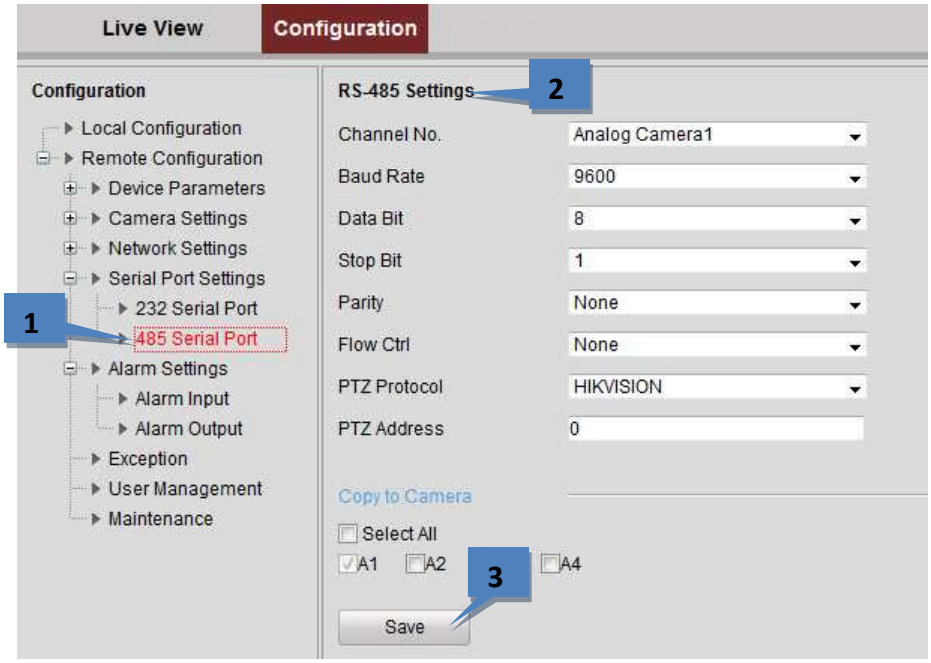

**NOTE:** If you want to connect the encoder by the RS-232 port, the parameters of the RS-232 should be exactly the same as the parameters you configured here.

2. Select the **Baud Rate**.
3. Select the **Data Bit**.
4. Select the **Stop Bit**.
5. Select the **Parity**.
6. Select the **Flow Ctrl**.
7. Select the **Usage**.
8. Click **Save** to save the settings.

## Configuring RS-485 Settings

The RS-485 serial port is used to control the PTZ of the camera. To configure RS-485, complete the following steps:

1. From the **Remote Configuration menu**, select **Serial Port Settings** and then **485 Serial Port** to open the RS-485 port setting interface:



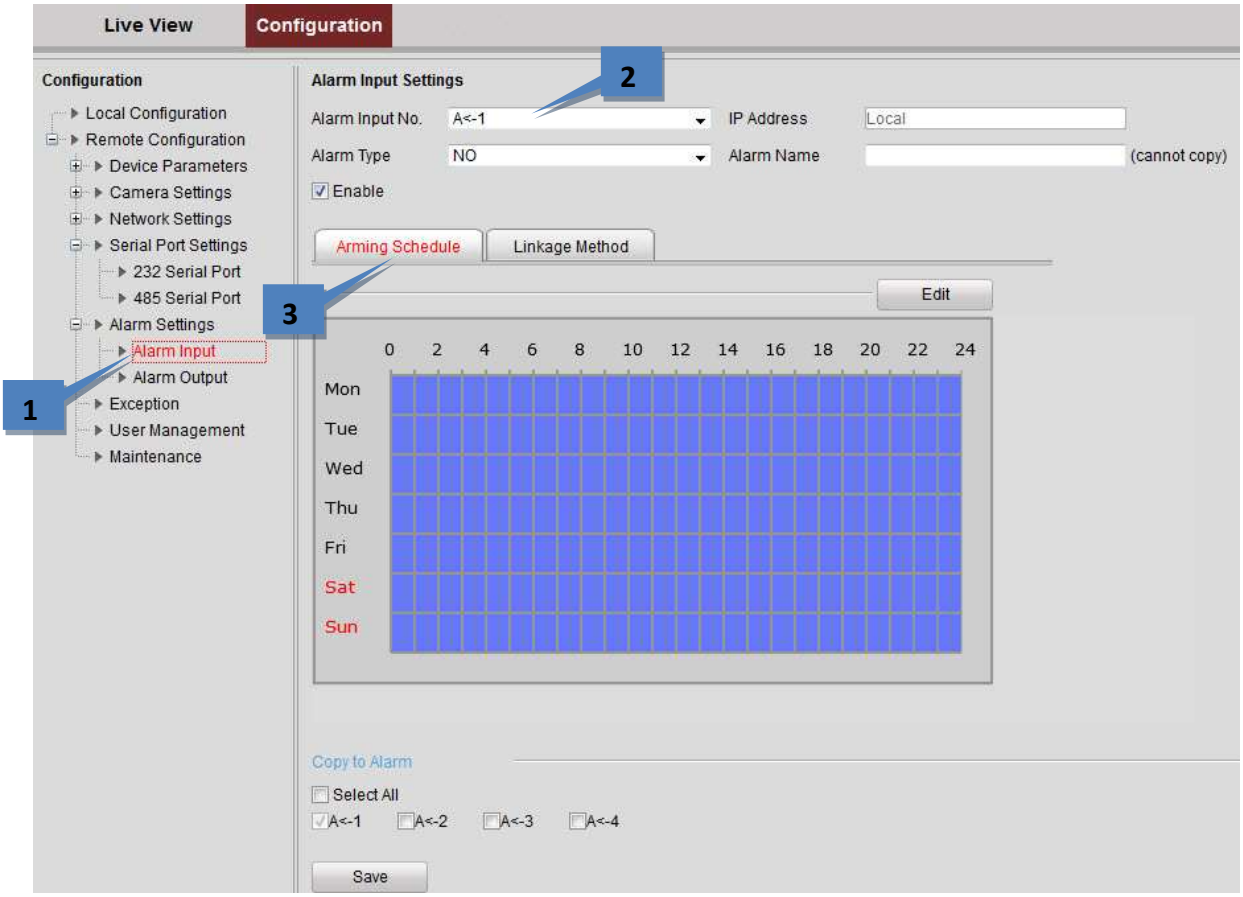

2. Set the RS-485 parameters. By default, the **Baud Rate** is set as 9600, the **Data Bit** as 8, the **Stop Bit** as 1, and the **Parity** and **Flow Ctrl** as None. The **Baud Rate**, **PTZ Protocol**, and **PTZ Address** parameters should be exactly the same as the parameters of the connected PTZ camera.
3. Click **Save** to activate the settings.

# 11 Alarm Input/Output

## Configuring the External Alarm Input

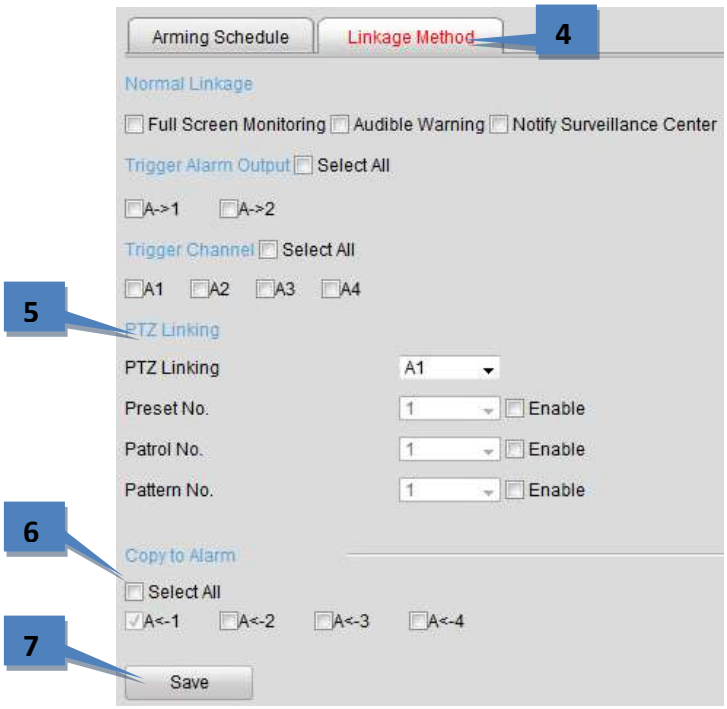
To configure the external alarm input, complete the following steps:

1. From the **Remote Configuration menu**, select **Alarm Settings** and then **Alarm Input** to open the Alarm Settings interface.




2. Choose the **Alarm Input No.** and the **Alarm Type**: NO (Normally Open) or NC (Normally Closed).
3. Set the **Arming Schedule** for the alarm input.

4. Select the **Linkage Method** tab to set the actions taken for the alarm input. Select any or all of **Full Screen Monitoring**, **Audible Warning**, and **Notify Surveillance Center**.

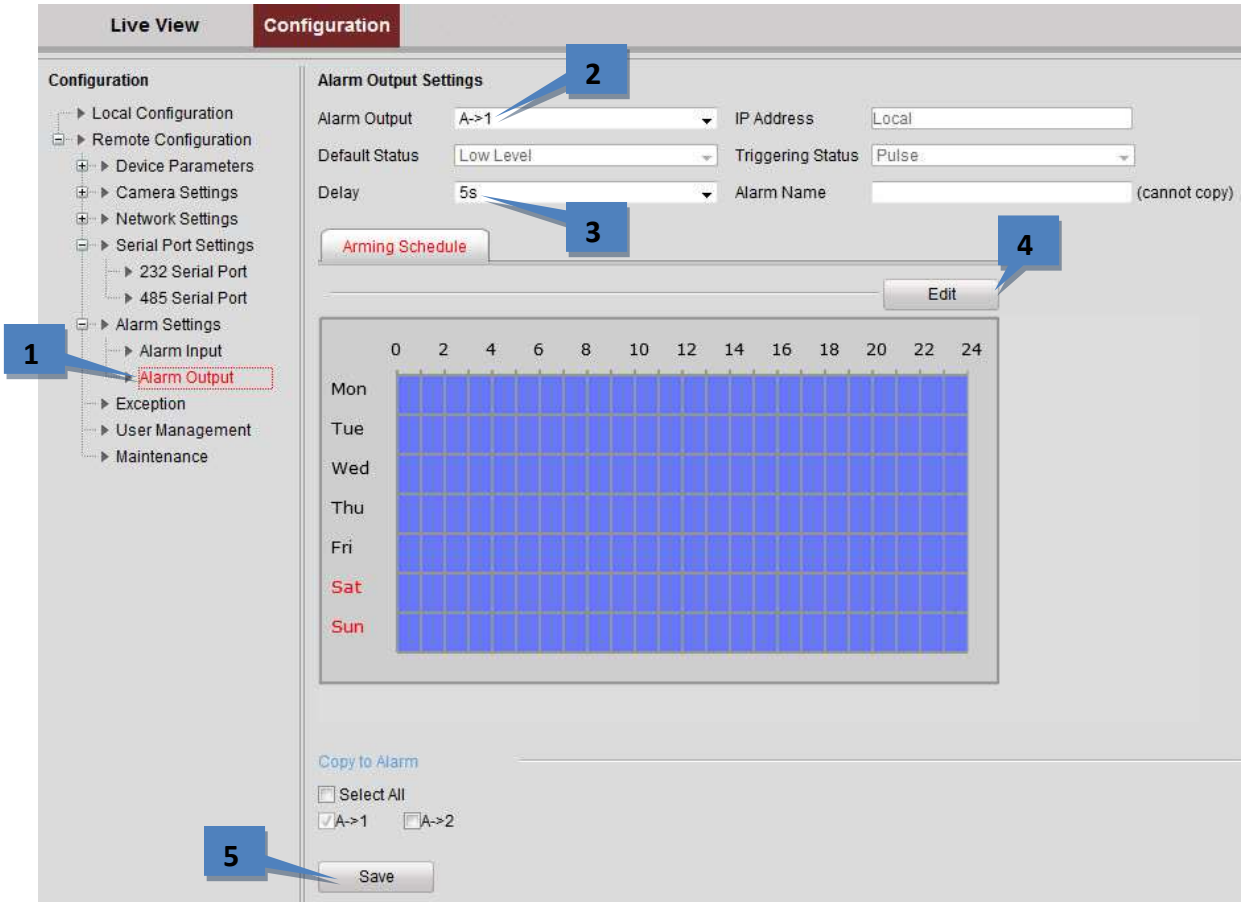



5. You can also choose the PTZ linking for the alarm input if your camera is installed with a pan/tilt unit. Choose the PTZ Linking channel, and then select the Enable checkbox next to Preset Calling, Patrol Calling, or Pattern Calling.
6. You can copy your settings to other alarm inputs.
7. Click **Save** to activate the settings.

## Configuring the External Alarm Output

To trigger an external alarm output when an event occurs, open the Alarm Output Settings interface to set the related parameters:

1. From the **Remote Configuration menu**, select **Alarm Settings** and then **Alarm Output** to open the Alarm Output Settings interface.



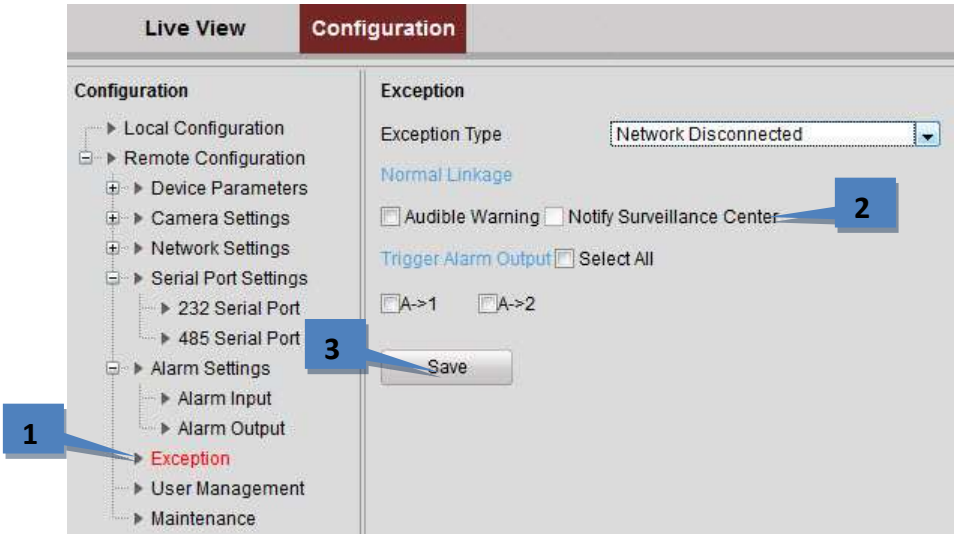

2. Select one alarm output channel in the **Alarm Output** drop-down list.
3. Set the **Delay** time to **5sec**, **10sec**, **30sec**, **1min**, **2min**, **5min, 10min**, or **Manual**. The **Delay** refers to the time duration that the alarm output remains in effect after alarm occurs. (If you choose **Manual**, you need to manually disable the alarm output.)
4. Click **Edit** to enter the **Edit Schedule Time** interface. The time schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection.
5. Return to the Alarm Output Settings interface and click **Save** to save the settings.

# 12 Exceptions

The exception type can be network disconnected, IP address conflict, illegal access, video standard mismatch, video signal exception, record/capture exception, and video resolution mismatch. When the selected resolution under **Configuration > Camera Settings >Video Settings** and the actual video input resolution are mismatched, the exception alarm will occur.

To configure exceptions, complete the following steps:

1. From the **Remote Configuration menu**, select **Exceptions** to open the Exception settings interface.
2. Select the checkbox to set the action or actions (**Audible Warning** or **Notify Surveillance Center**) to be taken for the Exception alarm.

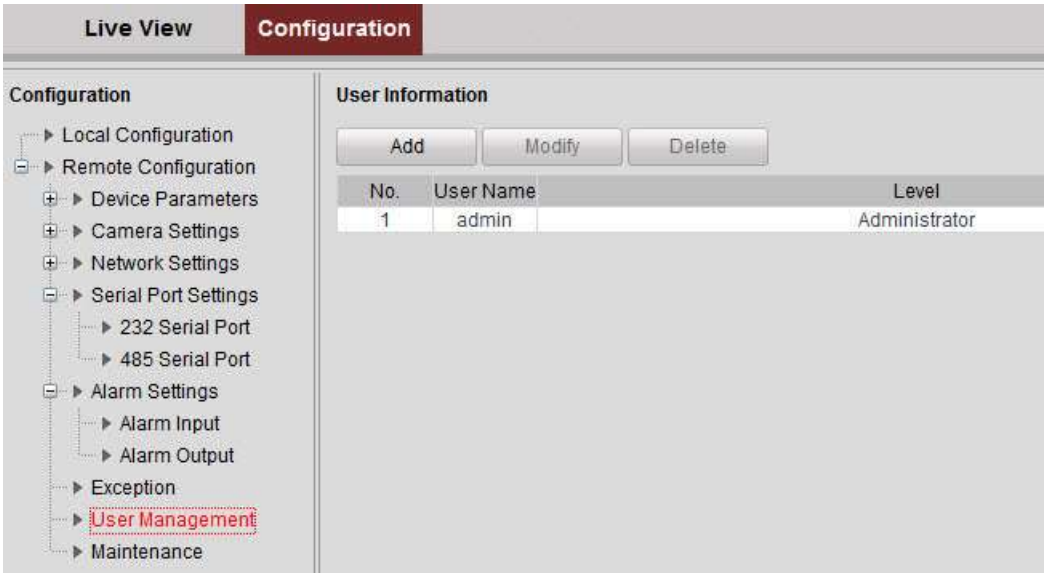



3. Click **Save** to activate the settings.

# 13 User Management

The admin user can create up to 31 users.

From the **Remote Configuration menu**, select **User Management** to open the User Information interface:



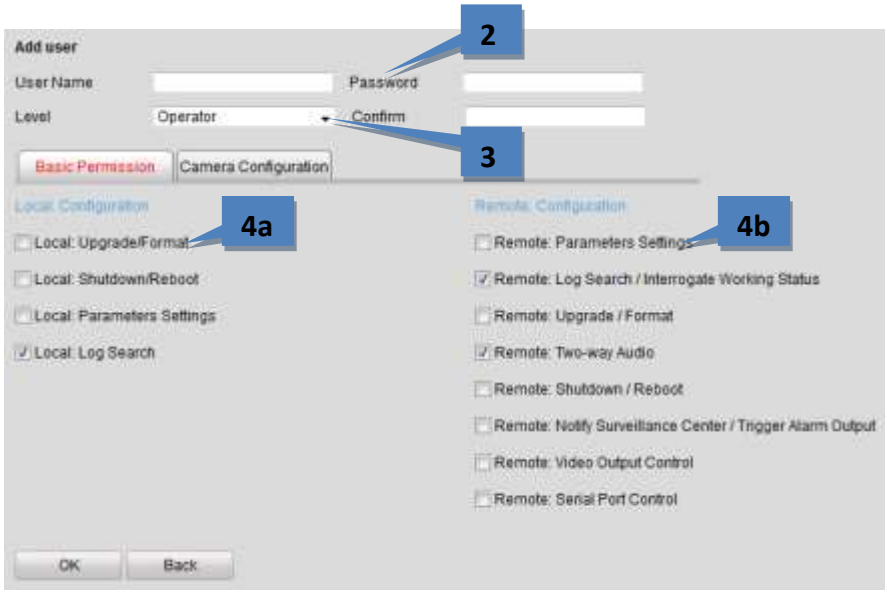
## Adding a User

To add a user, complete the following steps:

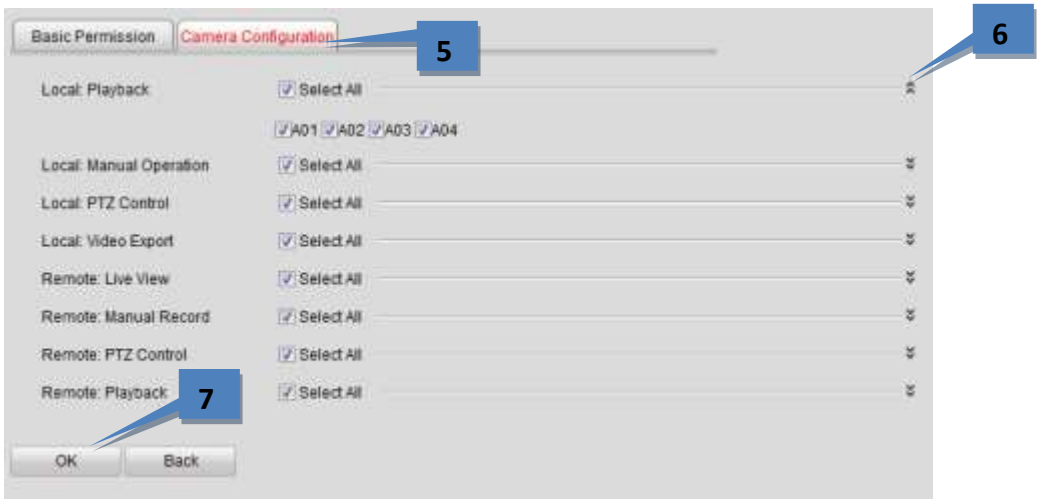
1. Click **Add** (not shown) to enter the Add User interface.
2. Input the **User Name** and **Password**, and confirm the password.
3. Select the **Level** (**Operator** or **User**).

   - **Operator:** Two-way Audio in Configuration and all operating permission in Camera Configuration.
   - **User:** Only the local/remote playback in the Camera Configuration.

4. On the **Basic Permission** tab, select **Local Configuration** and **Remote Configuration** permissions for the user.




5. On the **Camera Configuration** tab, select channels for which the user has permission to use each feature.
6. Use the arrows to display or hide the channel numbers.

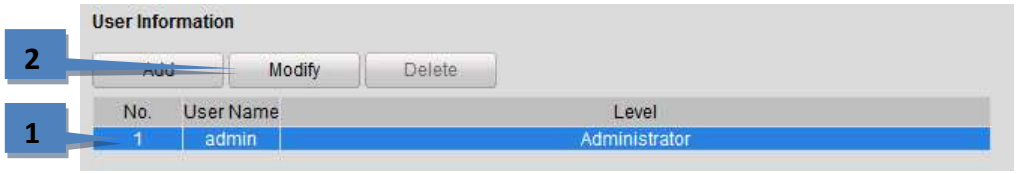



7. Click **OK** to finish the user addition.

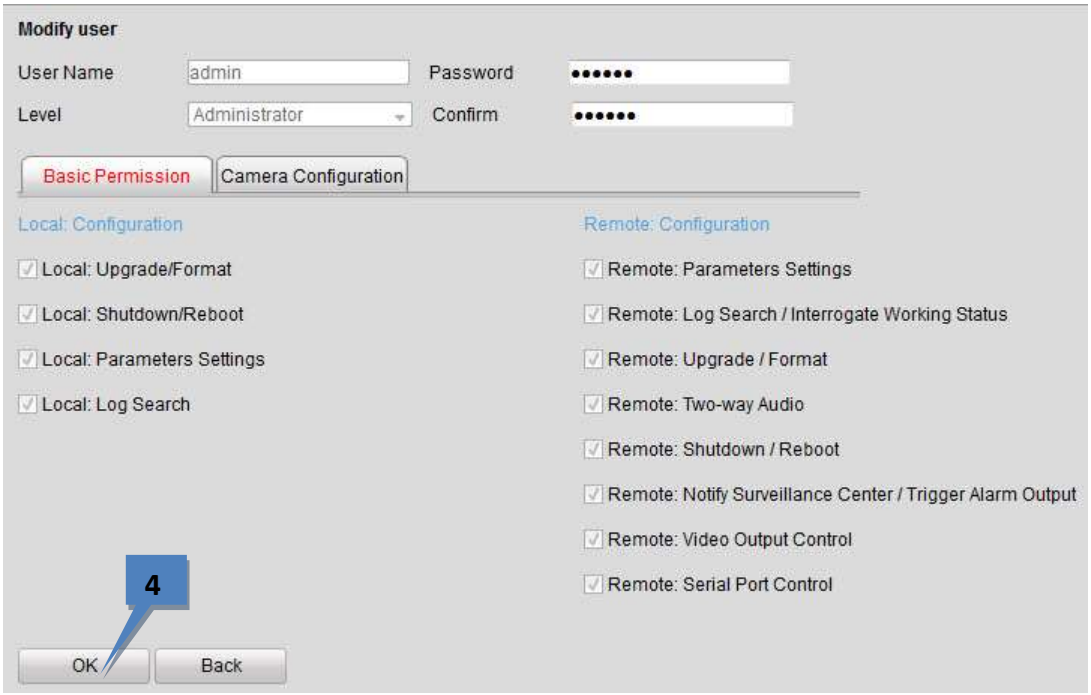
## Modifying a User

To modify a user account, an admin must complete the following steps:

1. Select the user account from the list on the User Information interface:




2. Click **Modify** to enter the setting interface.

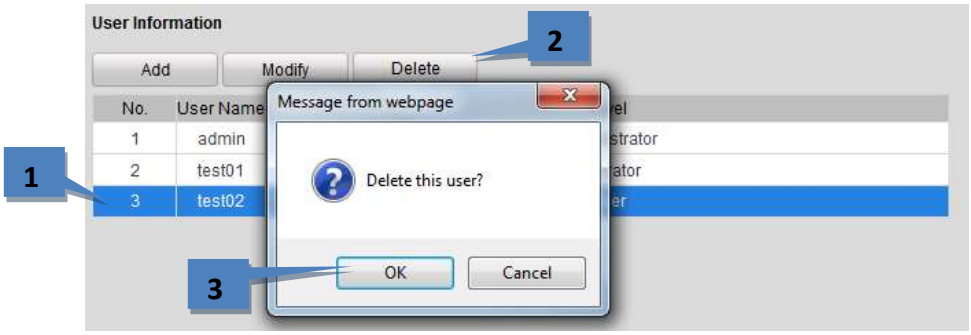



3. Modify the information as needed.
4. Click **OK** to finish the user modification.

## Deleting a User

To delete a user account, complete the following steps:

1. Select the user account from the list in the User Information interface.
2. Click **Delete** to display a confirmation message.

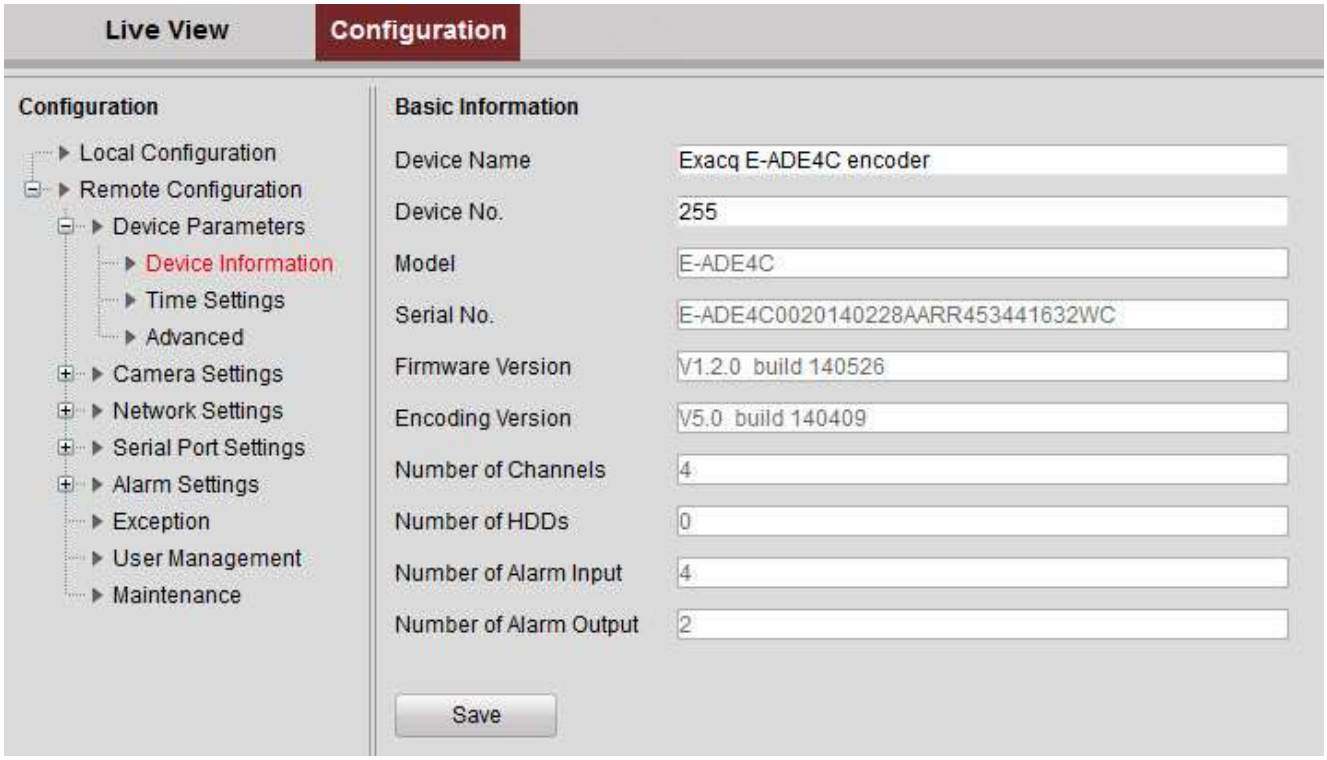



3. Click **OK** to delete the selected user account.

# 14 Device Information and Maintenance

## Viewing Device Information

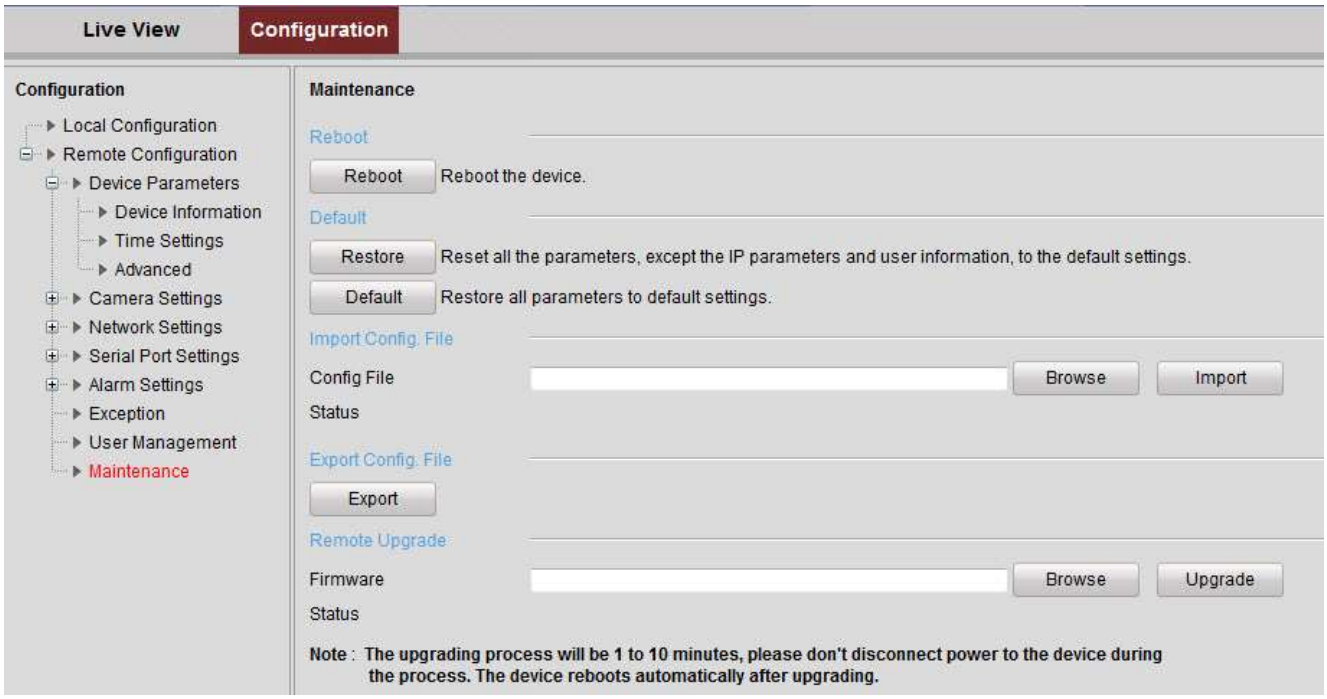
From the **Remote Configuration menu**, select **Device Parameters** and then **Device Information** to open the Device Information interface:




You can edit the **Device Name** and **Device No.**, and view the device information, including **Model**, **Serial No.**, **Firmware Version**, **Encoding Version**, **Number of Channels**, **Number of HDDs**, **Number of Alarm Input**, and **Number of Alarm Output**.

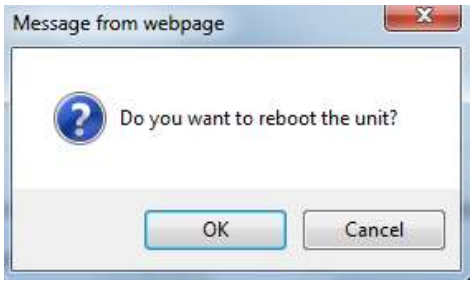
## Maintenance

From the **Remote Configuration menu**, select **Maintenance** to open the Maintenance interface:



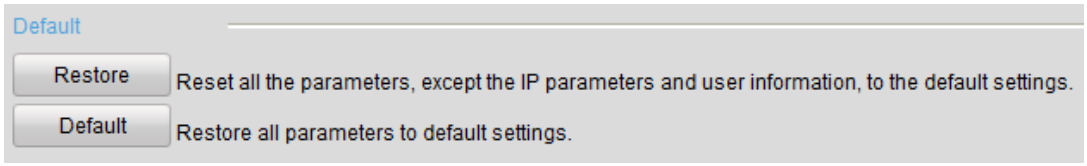

### Restarting the Device

On the Maintenance page, select **Reboot.** Confirm the message to reboot the encoder.

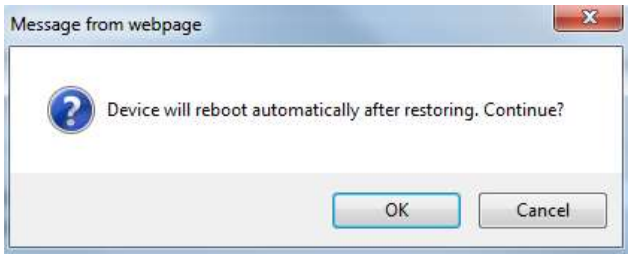


**Restoring Default Settings**

On the Maintenance page, select **Restore** to restore the default settings for all parameters except the IP address, subnet mask, gateway, and port. Select **Default** to restore the default settings for all parameters.




Click **OK** to restore and reboot the device to validate the settings.




**Importing/Exporting Configuration Files**

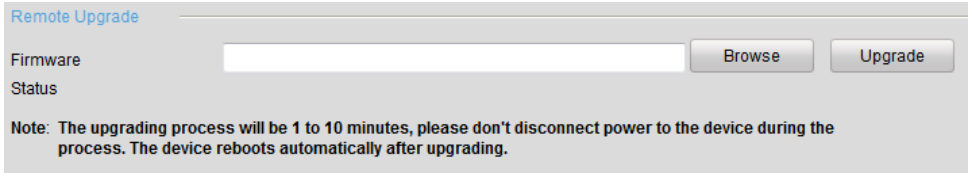
The configuration files of the device can be exported to a local device for backup, and the configuration files of one device can be imported to multiple device devices if they are to be configured with the same parameters.

On the **Maintenance** page, click **Browse** to select the file from the selected backup device and then click the **Import** button to import a configuration file. After the import, the device will reboot automatically.

On the **Maintenance** page, click the **Export** button to export configuration files to the selected local backup device.

**Upgrading the System**

On the **Maintenance** page, click **Browse** to select the local update file and then click **Upgrade** to start remote upgrade.



# A Technical Support

Exacq Technologies is committed to providing exceptional technical and engineering support. When you need help with your exacqVision product, please be ready with a complete description of the problem, including any error messages or instructions on re-creating the error.

Technical support can be contacted as follows:

**Exacq Technologies, Inc.**
11955 Exit Five Parkway, Bldg 3
Fishers, IN 46037 USA
Phone: +1-317-845-5710
Fax: +1-317-845-5720
Web: https://exacq.com/support/techsupport/
https://exacq.com/support/emailform/

# B Regulatory Notice

## Federal Communications Commission (FCC)
## Radio Frequency Interference Statement

The Exacq Product contains incidental radio frequency-generating circuitry and, if not installed and used properly, may cause interference to radio and television reception. This equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of the Federal Communications Commission (FCC) Rules. These limits are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area may cause interference to radio and television reception, in which case users will be required to correct the interference at their own expense. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by one or more of the following measures: Reorient the television or radio receiving antenna, and/or relocate the Exacq product and the radio or TV with respect to each other. If necessary, users should consult the manufacturer or an experienced radio/television technician for additional suggestions. Users may find helpful the following booklet prepared by the Federal Communications Commission: “How to Identify and Resolve Radio-TV Interference Problems,” which is available from the Government Printing Office, Washington DC, 20402 (stock #004-000-00345-4).

## CE Notice

Marking by the CE symbol indicates compliance of this device to the EMC directive of the European Community. Such marking is indicative that this device meets or exceeds the following technical standards:

- EN55022: Conducted Emissions
- EN55022: Radiated Emissions
- 61000-4-2 Electrostatic Discharge
- 61000-4-3 Radiated Immunity
- 61000-4-4 Electrical Fast Transients
- 61000-4-5 Surge Immunity
- 61000-4-6 Conducted Immunity

Electromagnetic compatibility (EMC) requires the use of shielded cable and ferrite cores for all wiring added by the user. Good shielding techniques should be applied in the user’s system.

# C Warranty

## LIMITED WARRANTY AND LIMITATION OF LIABILITY

LIMITED WARRANTY. Exacq hardware products are warranted against defects in materials and workmanship for three (3) years from the date Exacq ships the products to the Customer. All software products are licensed to the Customer under the terms of the appropriate Exacq Technologies license. For a period of ninety (90) days from the Delivery Date, Exacq software products (when properly installed on Exacq hardware products) (a) will perform substantially in accordance with the accompanying written materials, and (b) the medium on which the software product is recorded will be free from defects in materials and workmanship under normal use and service. Any replacement of a licensed software product will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Customer must obtain a Return Material Authorization number from Exacq before returning any products under warranty to Exacq. Customer shall pay expenses for shipment of repaired or replacement products to and from Exacq. After examining and testing a returned product, if Exacq concludes that a returned product is not defective, Customer will be notified, the product returned at Customer's expense, and a charge made for examination and testing. This Limited Warranty is void if products or parts are damaged by (a) improper handling, normal wear and tear, accidents, theft, vandalism, fire, water or other peril; (b) conditions outside the specifications for operation of the products, including but not limited to, electrical power, temperature humidity, dust or lightning; (c) Customer supplied third party software not intended for use with the applicable Exacq software; (d) utilization of an improper hardware or software key; (e) or improper use, negligence, repair, alteration or maintenance of the product not performed by Exacq Technologies, Inc. or its authorized service centers or authorized technicians.

CUSTOMER REMEDIES. Exacq's sole obligation (and Customer's sole remedy) with respect to the foregoing Limited Warranty shall be to, at its option, return the fees paid or repair/replace any defective products, provided that Exacq receives written notice of such defects during the applicable warranty period. Customer may not bring an action to enforce its remedies under the foregoing Limited Warranty more than one (1) year after the accrual of such cause of action.

RETURN/CANCELLATION POLICY. Customer may return unwanted products within thirty (30) days of the Delivery Date. Customer shall pay a twenty percent (20%) restocking charge on any unwanted products returned to Exacq. No returns will be accepted after the thirty (30) day period has expired. Where special equipment or services are involved, Customer shall be responsible for all related work in progress; however, Exacq shall take responsible steps to mitigate damages immediately upon receipt of a written cancellation notice from Customer. A Return Material Authorization number must be obtained from Exacq for return of any products. Exacq may terminate any order if any representations made by Customer to EXACQ are false or misleading.

NO OTHER WARRANTIES. EXCEPT AS EXPRESSLY SET FORTH ABOVE, THE PRODUCTS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, AND NO OTHER WARRANTIES, EITHER EXPRESSED OR IMPLIED ARE MADE WITH RESPECT TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT OR ANY OTHER WARRANTIES THAT MAY ARISE FROM USAGE OF TRADE OR COURSE OF DEALING. EXACQ DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF OR THE RESULTS OF THE USE OF THE PRODUCTS IN TERMS OF CORRECTNESS ACCURACY RELIABILITY OR OTHERWISE AND DOES NOT WARRANT THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE. EXACQ EXPRESSLY DISCLAIMS ANY WARRANTIES NOT STATED HEREIN.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. The entire liability of Exacq and its licensors, distributors and suppliers (including its and their directors, officers, employees and agents) is set forth above. To the maximum extent permitted by applicable law, in no event shall Exacq and its licensors, distributors and suppliers (including its and their directors, officers, employees and agents) be liable for any damages including but not limited to any special, direct, indirect, incidental, exemplary, or consequential damages, expenses, lost profits, lost savings, business interruption, lost business information, or any other damages arising out of the use or inability to use the products, even if Exacq or its licensors, distributors, and suppliers has been advised of the possibility of such damages. Customer acknowledges that the applicable purchase price or license fee for the products reflects this allocation of risk. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply. If the foregoing limitation of liability is not enforceable because an Exacq product sold or licensed to Customer is determined by a court of competent jurisdiction in a final non appeal able judgment to be defective and to have directly caused bodily injury death or property damage in no event shall Exacq's liability for property damage exceed the greater of $50,000 or fees paid for the specific product that caused such damage

WARNING: IN ANY APPLICATION THE RELIABILITY OF OPERATION OF THE PRODUCTS CAN BE IMPAIRED BY ADVERSE FACTORS, INCLUDING BUT NOT LIMITED TO FLUCTUATIONS IN ELECTRICAL POWER SUPPLY, COMPUTER HARDWARE MALFUNCTIONS, COMPUTER OPERATING SYSTEM SOFTWARE FITNESS, FITNESS OF COMPILERS AND DEVELOPMENT SOFTWARE USED TO DEVELOP AN APPLICATION, INSTALLATION ERRORS, SOFTWARE AND HARDWARE COMPATIBILITY PROBLEMS, MALFUNCTIONS OR FAILURES OF ELECTRONIC MONITORING OR CONTROL DEVICES, TRANSIENT FAILURES OF ELECTRONIC SYSTEMS (HARDWARE AND/OR SOFTWARE), UNANTICIPATED USES OR MISUSES, OR ERRORS ON THE PART OF THE USER OR APPLICATIONS DESIGNER (ADVERSE FACTORS SUCH AS THESE ARE HEREAFTER COLLECTIVELY TERMED "SYSTEM FAILURES"). ANY APPLICATION WHERE A SYSTEM FAILURE WOULD CREATE A RISK OF HARM TO PROPERTY OR PERSONS (INCLUDING THE RISK OF BODILY INJURY AND DEATH) SHOULD NOT BE RELIANT SOLELY UPON ONE FORM OF ELECTRONIC SYSTEM DUE TO THE RISK OF SYSTEM FAILURE. TO AVOID DAMAGE, INJURY, OR DEATH, THE USER OR APPLICATION DESIGNER MUST TAKE REASONABLY PRUDENT STEPS TO PROTECT AGAINST SYSTEM FAILURES, INCLUDING BUT NOT LIMITED TO BACK-UP OR SHUT DOWN MECHANISMS. BECAUSE EACH END-USER SYSTEM IS CUSTOMIZED AND DIFFERS FROM EXACQ'S TESTING PLATFORMS AND BECAUSE A USER OR APPLICATION DESIGNER MAY USE EXACQ PRODUCTS IN COMBINATION WITH OTHER PRODUCTS IN A MANNER NOT EVALUATED OR CONTEMPLATED BY EXACQ THE USER OR APPLICATION DESIGNER IS ULTIMATELY RESPONSIBLE FOR VERIFYING AND VALIDATING THE SUITABILITY OF EXACQ PRODUCTS WHENEVER EXACQ PRODUCTS ARE INCORPORATED IN A SYSTEM OR APPLICATION, INCLUDING, WITHOUT LIMITATION, THE APPROPRIATE DESIGN, PROCESS AND SAFETY LEVEL OF SUCH SYSTEM OR APPLICATION.