

# HSD820 Series

Full HD IP speed dome camera

## User Manual



**Note:** To ensure proper operation, please read this manual thoroughly before using the product and retain the information for future reference.

## **Copyright © 2016 Siquira B.V.**

All rights reserved.

HSD820

User Manual v4 (142703-4)

AIT55

Nothing from this publication may be copied, translated, reproduced, and/or published by means of printing, photocopying, or by any other means without the prior written permission of Siquira.

Siquira reserves the right to modify specifications stated in this manual.

## **Brand names**

Any brand names mentioned in this manual are registered trademarks of their respective owners.

## **Liability**

Siquira accepts no liability for claims from third parties arising from improper use other than that stated in this manual.

Although considerable care has been taken to ensure a correct and suitably comprehensive description of all relevant product components, this manual may nonetheless contain errors and inaccuracies. We invite you to offer your suggestions and comments by email via [t.writing@tkhsecurity.com](mailto:t.writing@tkhsecurity.com). Your feedback will help us to further improve our documentation.

## **How to contact us**

If you have any comments or queries concerning any aspect related to the product, do not hesitate to contact:

Siquira B.V.

Zuidelijk Halfroond 4

2801 DD Gouda

The Netherlands

General : +31 182 592 333

Fax : +31 182 592 123

E-mail : [sales.nl@tkhsecurity.com](mailto:sales.nl@tkhsecurity.com)

WWW : [www.siquira.com](http://www.siquira.com)

# Contents

<b>1</b>	<b>About this manual .....</b>	<b>6</b>
<b>2</b>	<b>Safety and compliance .....</b>	<b>7</b>
2.1	Safety .....	7
2.2	Cautions .....	9
2.3	Compliance .....	10
<b>3</b>	<b>Product overview .....</b>	<b>11</b>
3.1	Models .....	11
3.2	Description .....	13
<b>4</b>	<b>Access the webpages .....</b>	<b>14</b>
4.1	System requirements .....	14
4.2	Connect via web browser .....	14
4.3	Find the unit with Siqura Device Manager .....	15
4.4	Change the network settings with Siqura Device Manager .....	16
4.5	Log on to the unit .....	17
4.6	Install Siqura Viewer .....	17
4.7	The HSD820 web interface .....	18
<b>5</b>	<b>Home .....</b>	<b>19</b>
5.1	Overview .....	19
5.2	Features .....	20
5.3	PTZ Panel .....	22
<b>6</b>	<b>System settings .....</b>	<b>23</b>
6.1	System .....	24
6.1.1	Host name .....	24
6.1.2	Time zone .....	24
6.1.3	Daylight saving time .....	24
6.1.4	Time format .....	25
6.1.5	Time synchronisation .....	25
6.2	Security .....	25
6.2.1	User .....	26
6.2.1.1	Admin password .....	26
6.2.1.2	Add and manage user accounts .....	27
6.2.1.3	HTTP Authentication Setting .....	27
6.2.1.4	Streaming Authentication Setting .....	28
6.2.2	HTTPS .....	29
6.2.2.1	Create a self-signed certificate .....	29
6.2.2.2	Create and install a signed certificate .....	30
6.2.3	IP filter .....	31
6.2.4	IEEE 802.1X .....	32
6.2.4.1	CA certificate .....	32
6.2.4.2	Client certificate and private key .....	32
6.3	Network .....	33
6.3.1	Basic .....	33
6.3.1.1	Acquire an IP address automatically .....	33
6.3.1.2	Modify the fixed IP address .....	34
6.3.1.3	Use PPPoE .....	35
6.3.1.4	Advanced settings .....	35
6.3.1.5	IPv6 address configuration .....	35

6.3.2	QoS .....	36
6.3.3	SNMP .....	37
6.3.4	UPnP .....	39
6.4	DDNS .....	40
6.5	Mail .....	41
6.6	FTP .....	42
6.7	HTTP .....	43
6.8	Events .....	43
6.8.1	Application .....	44
6.8.1.1	Alarm trigger actions .....	45
6.8.1.2	Specifying file name conventions .....	47
6.8.2	Motion Detection .....	48
6.8.2.1	Motion detection area .....	50
6.8.2.2	Motion detection window .....	50
6.8.3	Network Failure Detection .....	51
6.8.4	Periodical event .....	52
6.8.5	Manual trigger .....	53
6.8.6	Audio detection .....	54
6.9	Storage management .....	55
6.9.1	SD Card .....	55
6.9.2	Network Share .....	57
6.10	Recording .....	59
6.11	Schedule .....	60
6.12	File location .....	61
6.13	View information .....	61
6.13.1	Log file .....	62
6.13.2	User Information .....	63
6.13.3	Parameters .....	64
6.14	Factory default .....	65
6.15	Software version .....	66
6.16	Software upgrade .....	66
6.17	Maintenance .....	67
<b>7</b>	<b>Video and Audio Streaming .....</b>	<b>69</b>
7.1	Video format .....	69
7.1.1	Video resolution .....	70
7.1.2	Video rotate type .....	70
7.1.3	GOV Settings .....	70
7.1.4	H.264 Profile .....	71
7.2	Video compression .....	71
7.3	Video text overlay .....	72
7.4	Video stream protocol .....	74
7.5	Video frame rate .....	75
7.6	Audio .....	75
<b>8</b>	<b>PTZ&amp;IMAGE .....</b>	<b>77</b>
8.1	Preset .....	77
8.2	Cruise .....	79
8.3	Autopan .....	80
8.4	Sequence .....	81
8.5	Home .....	83
8.6	Tilt Range .....	84
8.7	Privacy Mask .....	85
8.8	Camera - Exposure .....	86
8.9	Camera - WB .....	87
8.10	Camera - Misc 1 .....	89

8.11	Camera - Misc 2 .....	90
8.12	Camera - Profile .....	92
8.13	Camera - Default .....	93
<b>Appendix: Enable UPnP .....</b>		<b>94</b>
<b>Appendix: Delete the existing Siqua Viewer software .....</b>		<b>95</b>
<b>Appendix: Set Up Internet Security .....</b>		<b>96</b>
<b>Appendix: NTCIP Configuration .....</b>		<b>97</b>
	Supported conformance groups .....	97
	<i>Configuration</i> .....	97
	<i>CCTV configuration</i> .....	98
	<i>Motion control</i> .....	98
	SNMP MIB .....	99
<b>Index .....</b>		<b>100</b>

# 1 About this manual

---

## What's in this manual

This manual gives you the information you need to use the HSD820 camera. It tells:

- How to get access to the camera
- How to communicate with the camera
- How to operate the camera
- How to configure the settings of the camera

## Where to find more information

All product-specific manuals, such as Quick Start Guides, Installation Manuals and User Manuals, are available as PDF download at [www.siquira.com/support-files](http://www.siquira.com/support-files). We advise you to make sure that you have the latest version of this manual. For the technical specifications of the HSD820, download the HSD820 datasheet.

## Who this manual is for

These instructions are for all professionals who will configure and operate the HSD820.

## What you need to know

You will have a better understanding of how the HSD820 works if you are familiar with:

- Camera technologies
- CCTV systems and components
- Hazardous environments and ATEX/IECEX regulations (EX models)
- Ethernet network technologies and Internet Protocol (IP)
- Windows environments
- Video, audio, and contact closure transmissions
- Video compression methods

## Before you continue

Before you continue, read and obey all instructions and warnings in this manual. Keep this manual with the original bill of sale for future reference and, if necessary, warranty service. When you unpack your product, make sure there are no missing or damaged items. If any item is missing, or if you find damage, do not install or operate this product. Ask your supplier for assistance.

## Why specifications may change

At Siquira, we are committed to delivering high-quality products and services. The information given in this manual was current when published. As we continuously seek to improve our products and user experience, all features and specifications are subject to change without notice.

## We like to hear from you!

Customer satisfaction is our first priority. We welcome and value your opinion about our products and services. Should you detect errors or inaccuracies in this manual, we would be grateful if you would inform us. We invite you to offer your suggestions and comments via [t.writing@tkhsecurity.com](mailto:t.writing@tkhsecurity.com). Your feedback helps us to further improve our documentation.

## 2 Safety and compliance

This chapter provides cautions on what to do and what not to do when working with or handling your HSD820 unit. It also offers information on product compliance with environmental regulations and explains how to dispose of the product at the end of its service life.

### In This Chapter

2.1 Safety.....	7
2.2 Cautions.....	9
2.3 Compliance.....	10

### 2.1 Safety

The safety information contained in this section, and on other pages of this manual, must be observed whenever this unit is operated, serviced, or repaired. Failure to comply with any precaution, warning, or instruction noted in the manual is in violation of the standards of design, manufacture, and intended use of the module. Siqura assumes no liability for the customer's failure to comply with any of these safety requirements.

#### Trained personnel

Installation, adjustment, maintenance, and repair of this equipment are to be performed by trained personnel aware of the hazards involved. For correct and safe use of the equipment and in order to keep the equipment in a safe condition, it is essential that both operating and servicing personnel follow standard safety procedures in addition to the safety precautions and warnings specified in this manual, and that this unit be installed in locations accessible to trained service personnel only.

#### Safety requirements

The equipment described in this manual has been designed and tested according to the **UL/IEC/EN 60950-1** safety requirements. For compliance information, see the EU Declaration of Conformity which is available for download at [www.siqura.com/support-files](http://www.siqura.com/support-files).

**Warning:** If there is any doubt regarding the safety of the equipment, do not put it into operation.

This might be the case when the equipment shows physical damage or is stressed beyond tolerable limits (for example, during storage and transportation).

**Important:** Before opening the equipment, disconnect it from all power sources.

The equipment must be powered by a SELV<sup>1</sup> power supply. This is equivalent to a Limited Power source (LPS, see UL/IEC/EN 60950-1 clause 2.5) or a "NEC Class 2" power supply. When this module is operated in extremely elevated temperature conditions, it is possible for internal and external metal surfaces to become extremely hot.

1. SELV: conforming to IEC 60950-1, <60 Vdc output, output voltage galvanically isolated from mains. All power supplies or power supply cabinets available from Siqura comply with these SELV requirements.

## Power source and temperature ratings

Verify that the power source is appropriate before you plug in and operate the unit. Use the unit under conditions where the temperature remains within the range given in the Technical Specifications of this product.

## Optical safety

*The following optical safety information applies to HSD820 models with SFP interface.*

This product complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007. This optical equipment contains Class 1M lasers or LEDs and has been designed and tested to meet **IEC 60825-1:1993+A1+A2** and **IEC 60825-2:2004 safety class 1M** requirements.

**Warning:** Optical equipment presents potential hazards to testing and servicing personnel, owing to high levels of optical radiation.

When using magnifying optical instruments, avoid looking directly into the output of an operating transmitter or into the end of a fiber connected to an operating transmitter, or there will be a risk of permanent eye damage. Precautions should be taken to prevent exposure to optical radiation when the unit is removed from its enclosure or when the fiber is disconnected from the unit. The optical radiation is invisible to the eye.

*Use of controls or adjustments or procedures other than those specified herein may result in hazardous radiation exposure.*

The installer is responsible for ensuring that the label depicted below (background: yellow; border and text: black) is present in the restricted locations where this equipment is installed.



## EMC

This device has been tested and found to meet the CE regulations relating to EMC and complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. These limits are designed to provide reasonable protection against interference to radio communications in any installation. The equipment generates, uses, and can radiate radio frequency energy; improper use or special circumstances may cause interference to other equipment or a performance decrease due to interference radiated by other equipment. In such cases, the user will have to take appropriate measures to reduce such interactions between this and other equipment.

*Any interruption of the shielding inside or outside the equipment could make the equipment more prone to fail EMC requirements.*

Non-video signal lines must use appropriate shielded Cat 5 cabling (S-FTP), or at least an equivalent. Ensure that *all* electrically connected components are carefully earthed and protected against surges (high voltage transients caused by switching or lightning).

## ESD

Electrostatic discharge (ESD) can damage or destroy electronic components. *Proper precautions should be taken against ESD when opening the equipment.*

## RoHS statement



Global concerns over the health and environmental risks associated with the use of certain environmentally-sensitive materials in electronic products have led the European Union (EU) to enact the Directive on the Restriction of the use of certain Hazardous Substances (RoHS) (2002/95/EC). Siquira offers products that comply with the EU's RoHS Directive. The full version of the Siquira RoHS statement can be viewed at [www.siquira.com](http://www.siquira.com).

## Product disposal



The unit contains valuable materials which qualify for recycling. In the interest of protecting the natural environment, properly recycling the unit at the end of its service life is imperative.



When processing the printed circuit board, dismantling the lithium battery calls for special attention. This kind of battery, a button cell type, contains so little lithium, that it will never be classified as reactive hazardous waste. It is safe for normal disposal, as required for batteries by your local authority.

## 2.2 Cautions

### Handle the camera carefully

Do not abuse the camera. Avoid bumping and shaking. The camera can be damaged by improper handling or storage.

### Do not disassemble the camera

To prevent electric shock, do not remove screws or covers. There are no user serviceable parts inside. Consult technical support if a camera is suspected of malfunctioning.

### Do not block the cooling vent

This camera has a cooling fan inside. Blocking the cooling holes may lead to overheating and cause malfunction. Overheating is not covered by warranty.

### Never face the camera towards the sun

Do not aim the camera at bright objects. Whether the camera is in use or not, never aim it at the sun or other extremely bright objects, as this can damage the camera.

### Do not expose indoor models to moisture

The indoor camera model is designed for indoor use or use in locations where it is protected from rain and moisture. Turn the power off immediately if the camera is wet and ask a qualified technician for servicing. Moisture can damage the camera and also create the danger of electric shock.

### **Do not use strong or abrasive detergents to clean the camera**

Use a dry cloth to clean the camera when it is dirty. If the dirt is hard to remove, use a mild detergent and wipe gently. To clean the lens, use lens tissue or a cotton tipped applicator and ethanol. Do *not* clean the lens with strong detergents.

## **2.3 Compliance**

The EU Declaration of Conformity for this product is available for download at [www.siquira.com/support-files](http://www.siquira.com/support-files).

## 3 Product overview

This chapter introduces the HSD820 models and their features.

### In This Chapter

3.1 Models.....	11
3.2 Description.....	13

## 3.1 Models

### HSD820H2 full HD IP speed dome camera, 20x zoom



*HSD820H2-I  
(indoor model)*



*HSD820H2-E  
(outdoor model)*

- Full HD 1080p resolution
- Quad stream H.264/H.264 or H.264/MJPEG
- 20x Optical zoom / 8x Digital zoom
- Optical output / Analogue output options
- Day/Night with IR-cut filter / WDR / BLC
- 360° Continuous rotation
- 400°/s Preset targeting
- 256 Presets / 8 Programmable cruises
- Two alarm inputs / Two alarm outputs
- Two-way audio
- 16 Privacy masks
- ONVIF Profile S

### HSD820H3 full HD IP speed dome camera, 30x zoom



*HSD820H3-E  
(outdoor model)*

- Full HD 1080p resolution
- Quad stream H.264/H.264 or H.264/MJPEG
- 30x Optical zoom / 12x Digital zoom
- Optical output / Analogue output options
- Day/Night with IR-cut filter / WDR / BLC
- 360° Continuous rotation
- 400°/s Preset targeting
- 256 Presets / 8 Programmable cruises
- Two alarm inputs / Two alarm outputs
- Electronic Image Stabilisation
- Two-way audio
- 16 Privacy masks
- ONVIF Profile S
- NTCIP protocol support

#### **HSD820H3EXP Ex 316L 1080p PTZ dome camera, 30x zoom**



*HSD820H3EXP*

- Explosion-protected for use in onshore, offshore, marine, and heavy industrial applications
- Full HD 1080p resolution
- Quad stream H.264/H.264 or H.264/MJPEG
- 30x Optical zoom / 12x Digital zoom
- Day/Night with IR-cut filter / WDR / BLC
- 316L Stainless steel construction
- 360° Continuous rotation
- 400°/s Preset targeting
- 256 Presets / 8 Programmable cruises
- IP66/IP67 Ingress rating

#### **HSD820H3 SA 316L IP 1080p PTZ dome camera, 30x zoom**



*HSD820H3 SA*

- Protected for use in onshore, offshore, marine, and heavy industrial applications
- Full HD 1080p resolution
- Quad stream H.264/H.264 or H.264/MJPEG
- 30x Optical zoom / 12x Digital zoom
- Day/Night with IR-cut filter / WDR / BLC
- 316L Stainless steel construction
- 360° Continuous rotation
- 400°/s Preset targeting
- 256 Presets / 8 Programmable cruises
- IP66/IP67 Ingress rating

#### **HSD820H3PRH Pressurised IP PTZ dome camera with multistream H.264**



*HSD820H3PRH*

- Multistream support: H.264 and MJPEG
- Full HD 1080P resolution
- 30x Optical zoom / 12x Digital zoom
- Day/Night with IR-cut filter
- Back Light Compensation
- Wide Dynamic Range
- 400°/s Preset targeting
- 360° Endless panning
- 256 Presets / Eight programmable cruises
- One alarm input
- 16 Privacy masks
- Pressurised to 7 psi; able to hold pressure for up to 1 year
- Low pressure sensor, Shrader and pressure relief valves standard
- IP 67 ingress protection

## 3.2 Description

### Multistream high definition

The HSD820 series cameras have quad-stream capability for simultaneous streaming of H.264/H.264 or H.264/MJPEG. Full HD 1080p streaming with a D1 second stream or dual 720p streaming is possible. Multiple combinations of resolution and frame rate can be configured to satisfy different live viewing and recording scenarios.

### Open standards

Siquira provides multiple options to easily integrate the HSD820 series cameras with a video management system (VMS). In support of open standards, the HSD820 cameras are compliant with the ONVIF Profile S specification as well as the Siquira Open Streaming Architecture (OSA) HTTP API.

### High-speed dome

The HSD820 series cameras have a 20x (H2 model) or 30x (H3 model) auto focus zoom lens. Precision 400° per second pan and tilt drive technology offers almost instant preset positioning. Support for many presets, cruises, and sequences provides for highly flexible manual or automatic operation.

### Day/Night, Backlight Compensation, and Wide Dynamic Range

The HSD820 series cameras provide automatic day/night functionality, for use in low light situations. Backlight compensation enhances image visibility in difficult lighting conditions. Wide dynamic range solves the problem of overlit images by combining the best of two pictures with different exposure settings.

### Image stabiliser

The HSD820H3 has a built-in image stabiliser to prevent vibrations from disrupting a camera view or footage, such as those caused by wind in pole-mount installations.

### Privacy masks

Through the camera's web interface, administrators can configure privacy masks to conceal sensitive areas, such as point-of-sale keypads in retail or ATM applications as well as windows or other exposed areas appearing in city centre surveillance situations.

### Audio and I/O contacts

The HSD820 series cameras combine streaming video with duplex audio, balanced audio inputs/outputs suitable for all industrial audio systems, and I/O contacts over IP.

### Fiber option

A fiber option is available for direct connection of fiber to the camera via a flexible SFP interface. The XSNet™ range of SFP modules, with options for both single mode and multimode is available. The SFP interface is built into the camera itself so a wide range of mounting options is available.

### NEMA TS 2

The HSD820H3 has been tested and approved according to the NEMA TS 2 standard.

## 4 Access the webpages

The webpages of the HSD820 offer a user-friendly interface for configuring the settings of the unit and viewing live video images over the network. This chapter explains how to connect to the built-in web server.

### In This Chapter

4.1 System requirements.....	14
4.2 Connect via web browser.....	14
4.3 Find the unit with Siqura Device Manager.....	15
4.4 Change the network settings with Siqura Device Manager.....	16
4.5 Log on to the unit.....	17
4.6 Install Siqura Viewer.....	17
4.7 The HSD820 web interface.....	18

### 4.1 System requirements

To connect to the HSD820, access its webpages, and view live video over the network, make sure that your PC meets the following requirements.

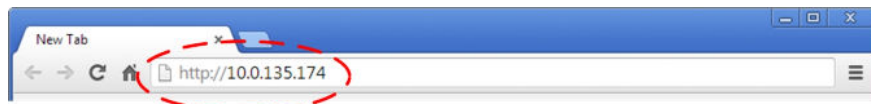
Component	Minimum requirement
Personal computer	<ul style="list-style-type: none"> <li>Intel® Pentium® IV, 3 GHz or higher, Intel® Core2 Duo, 2 GHz or higher</li> <li>1 GB RAM or more</li> <li>AGP graphics card 64 MB RAM, DirectDraw</li> </ul>
Operating system	Windows 7
Web browser	Internet Explorer 6.0 or later, Firefox, Chrome, Safari
Network card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

### 4.2 Connect via web browser

#### » To connect to the unit via your web browser

- 1 Open your web browser.
- 2 Type the IP address of the HSD820 in the address bar.
- 3 Press ENTER.  
The factory-set IP address of the HSD820 is in the 10.x.x.x range. It is printed on a sticker on the unit.  
If your network configuration is correct you are directed to the login page of the unit.

**Note:** A hard reset sets the IP address of the camera to its factory-default setting.



Type the IP address of the HSD820 in the address bar of the browser

## 4.3 Find the unit with Siquira Device Manager

Siquira Device Manager is a Windows-based software tool that you can use to manage and configure Siquira IP cameras and video encoders. The tool automatically locates Siquira devices and offers you an intuitive interface to set and manage network settings, configure devices, show device status, and perform firmware upgrade.

### ► To install Siquira Device Manager

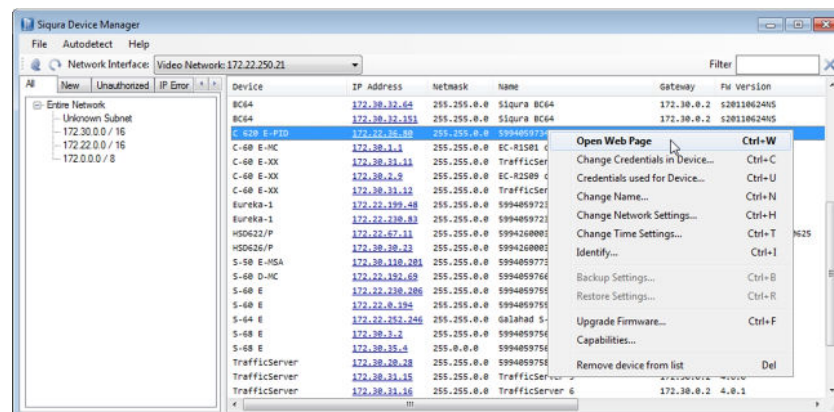
- 1 Download the latest version of Siquira Device Manager at [www.siquira.com/support-files](http://www.siquira.com/support-files).
- 2 Double-click the setup file.
- 3 Follow the installation steps to install the software.

### ► To connect to the unit via Siquira Device Manager

- 1 Start Siquira Device Manager  
The network is scanned.  
Detected devices appear in the List View pane.
- 2 If multiple network adapters exist, select the appropriate adapter to scan the network that you wish to connect to.
- 3 To perform a manual search, click the **Rescan** button.
- 4 Use the tabs in the *Tree View* pane to define the scope of your search.
- 5 Click the column headings in the *List View* pane to sort devices by type, IP address, or name.
- 6 To connect to the webpages of the HSD820, double-click its entry in the device list, - or -

Right-click the entry, and then click **Open Web Page**.

The login page of the HSD820 is opened in your web browser.



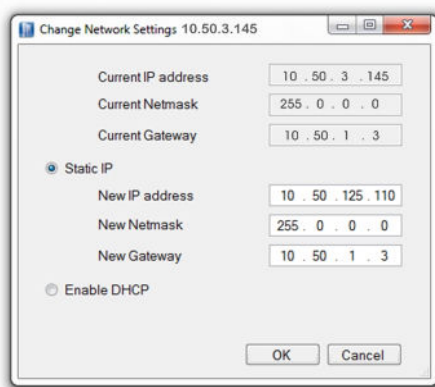
Connect to a device via Siquira Device Manager

## 4.4 Change the network settings with Siqura Device Manager

With Siqura Device Manager, you can directly change the network settings of the HSD820.

### » To assign a static IP address

- 1 Go to the list of detected devices, and then right-click the entry for the HSD820.
- 2 Click **Change Network Settings**.
- 3 In *Change Network Settings*, click **Static IP**.
- 4 Provide the camera with an appropriate IP address, netmask, and gateway address for the desired network configuration, and then click **OK**.
- 5 In the pop-up window indicating that you have successfully changed the settings, click **OK**.
- 6 Wait one minute, and then rescan the network.
- 7 To access the webpages of the HSD820, double-click its entry in the list of found devices.



*Assign a static IP address*

### » To assign a DHCP server

- 1 Record the HSD820's MAC address (see the *Serial no.* column in Siqura Device Manager) for future identification
- 2 In the list of detected devices, right-click the device with the network property that you would like to change.
- 3 Click **Change Network Settings**.
- 4 In *Change Network Settings*, click **Enable DHCP**, and then click **OK**.
- 5 In the pop-up window indicating that you have successfully changed the settings, click **OK**.
- 6 Wait one minute, and then rescan the network.  
You can identify the device by its MAC address.
- 7 To access the webpages of the HSD820, double-click its entry in the list of found devices.

**Note:** A DHCP server must be installed on the network in order to provide DHCP network support.

## 4.5 Log on to the unit

Users with a valid account for the HSD820 can log on to the unit.

### » To log on

- 1 In the *Authentication* box, log on with the account that was created for you.  
User name and password are case sensitive.  
The default user name set at the factory for the HSD820 is "Admin" with password "1234".
- 2 Click **Log In**.



**CAUTION:** MAKE SURE THAT YOU CHANGE THE DEFAULT ADMIN PASSWORD AT THE FIRST LOGIN. TO KEEP THE ACCOUNT SAFE, CREATE A STRONG, COMPLEX PASSWORD. THIS HELPS TO PREVENT UNAUTHORISED ACCESS FROM PEOPLE WHO TRY TO USE THE DEFAULT ACCOUNT.

### » To create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of the following letters, numbers, punctuation marks, and special characters: a-z, A-Z, 0-9, ! # \$ % & ' - . @ ^ \_ ~

## 4.6 Install Siqua Viewer

The first time you access the webpages of the camera, you may be prompted about the installation of Siqua Viewer. This add-on is required to view camera images in the webpages. The Siqua Viewer installation file is named `install.cab`. It does not give rise to any security risks. You can install it safely.

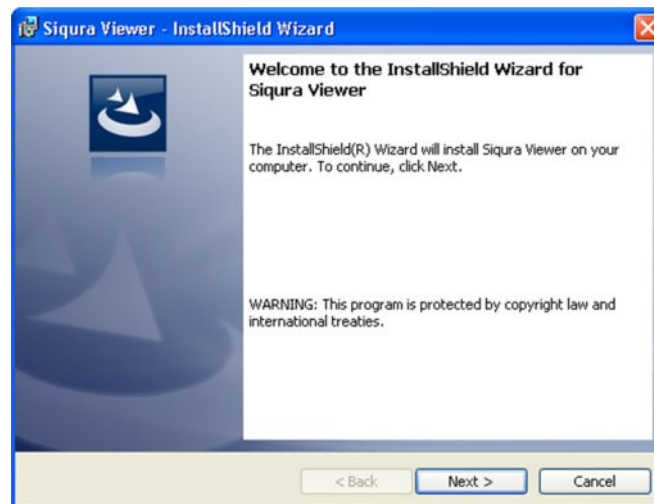


**Important:** You are strongly advised to remove a previous installation of Siqua Viewer from your computer before you initially access the camera over the network or when you encounter an "A new version is available" message. For more information, see *Appendix: Delete the existing Siqua Viewer software*.

**Note:** Make sure that the security settings of your web browser permit the use of ActiveX controls. For more information on how to modify these settings, see *Appendix: Set up Internet Security*.

### » To install the Siqua Viewer software

- 1 When prompted about the ActiveX control installation, allow the Siqua Viewer installation wizard to make changes to your computer.
- 2 In the initial screen of the installation wizard, click **Next**.  
A progress bar is displayed while the application is being installed.
- 3 When installation is complete, click **Finish**.  
The camera's web interface is displayed.



*Siquira Viewer installation wizard*

## 4.7 The HSD820 web interface

On successful login, the Home page of the HSD820 is shown. Camera settings and functions are organised on five tabs found across the top of this page: **Home**, **System**, **Streaming**, **PTZ&IMAGE**, and **Logout**.

### Home

On the Home page, users can monitor a live video stream from the camera and view stream details.

### System

Administrators can use this tab to view and configure system, security, and network related settings, and upgrade the embedded software.

### Streaming

Administrators can use this tab to set video and audio formats and compression parameters.

### PTZ&IMAGE

Administrators and users with camera control permission can use this tab to program preset points, cruise lines, autopan paths, and sequence lines, and to adjust exposure, white balance, backlight compensation and other camera-related settings.

### Logout

The Logout option logs the user off of the camera webpages and opens the Login page.

## 5 Home

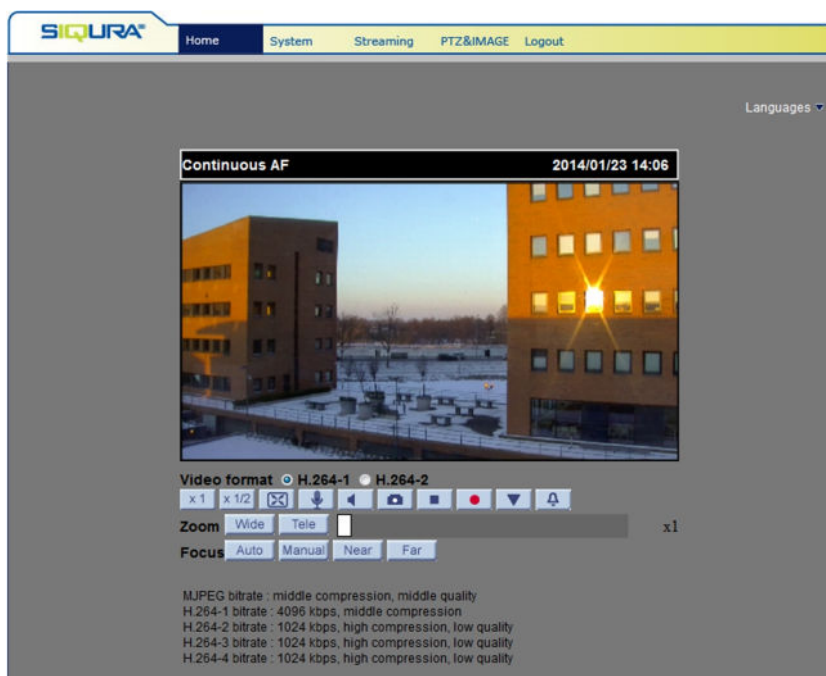
This chapter gives an overview of the actions that you can perform from the home page of the camera:

- View live video
- Control PTZ functions
- Record live view images
- Save snapshots of live view images
- Adjust the video display size
- Select the video format
- Communicate with a remote site
- See details about the current video and audio
- Select a display language for the webpages























### In This Chapter

5.1 Overview.....	19
5.2 Features.....	20
5.3 PTZ Panel.....	22

## 5.1 Overview



HSD820 home page

When you want to	Click this
Set image display to standard size	
Set image display to half size	
Set image display to full screen	
Activate/deactivate the talk function	 
Activate/mute audio	 
Save a JPEG snapshot	
Pause/Resume video streaming	 
Start/Stop Live View recording	 
Show/Hide the PTZ panel	 
Activate/Deactivate the manual trigger	 
Adjust lens angle to wide angle / tele zoom position	 
Set lens focus control to auto/manual mode	 
Adjust lens focus to near/far position while in manual mode	 

## 5.2 Features

### Languages

The HSD820 webpages can be displayed in German, English, French, Italian and Simplified Chinese. Select the desired language from the Languages list in the upper-right corner of the page.

### Video format


Use the Video format buttons to select a video stream for display in the camera view.

### Screen size

Use the image display buttons to adjust the screen size. Alternatively, you can right-click the camera view and then select Fullscreen or Normal View.

### Pan/Tilt control

You can right-click the camera view to select the screen mode for pan/tilt control.

- In *Emulated joystick* mode, you can left-click the camera view and then drag the pointer  in any direction to pan/tilt the camera. Camera rotation stops on releasing the mouse button.
- In *Center* mode, you can left-click the camera view anywhere to move the camera such that the clicked point is centred in the camera view. The amount of camera rotation is determined by the point of clicking relative to the previous centre of the camera view.

## Audio

Using the Talk and Speaker buttons, you can communicate with a remote site. The associated audio functions are available to users who have Talk and Listen privileges.

## Snapshots

Pressing the Snapshot button saves a .jpg format snapshot of the video in the camera view to the configured location (default: C:\). For information about changing the storage location, see *File location*.

**Note:** Users working with Windows 7 must log on as Administrator to implement the Snapshot function.

## Pausing/Resuming video streaming

A blank screen displays when video streaming is paused. Press the Play button to resume video streaming.

## Recording

Pressing the Recording button saves an .avi format recording of the video in the camera view to the configured location (default: C:\). For information about changing the storage location, see *File location*.

**Note:** Users working with Windows 7 must log on as Administrator to implement the Recording function.

## Manual trigger

The Manual trigger button activates the manual trigger function. You can use this to upload current video images by FTP or email. For more information, see *Manual trigger*.

## Focus

The *Auto* button activates autofocus (AF) mode. In this mode, the camera is kept focused automatically and continuously, regardless of zoom or view changes. To adjust focus manually, first press the Manual button, and then use the Near and Far buttons.

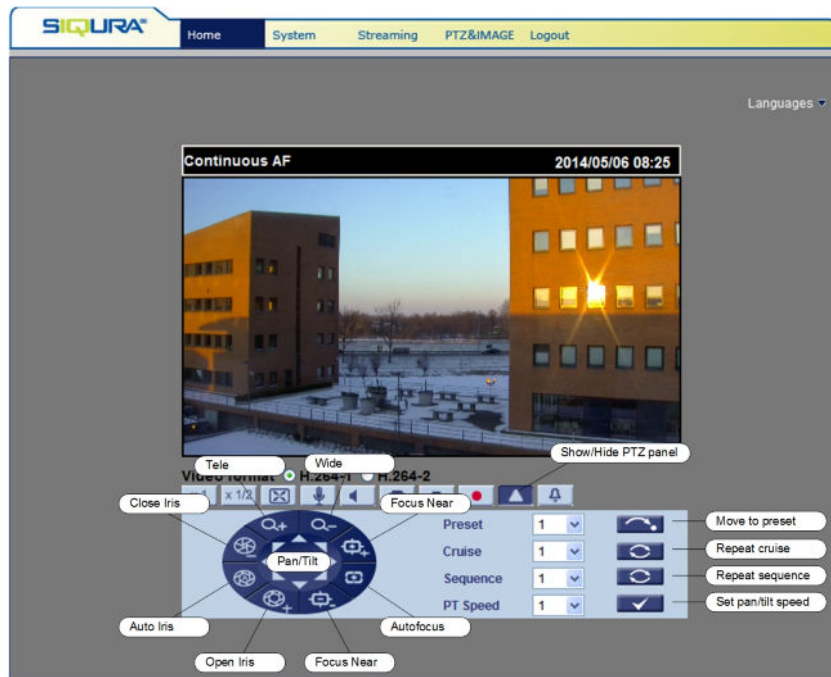
## Zoom

In Normal View and Fullscreen mode, you can use the Wide and Tele buttons or drag the Zoom slider to zoom in/out on the image. You can also click in the zoom adjustment bar at the desired zoom ratio. In Fullscreen mode, it is possible to rotate the mouse wheel for zoom adjustment.

## Info

In Normal View mode, you can double-click the camera view to display the Info box. This contains information about the current video and audio stream.

## 5.3 PTZ Panel



*HSD820 home page with PTZ panel*

The PTZ panel offers an intuitive and convenient interface for easy camera operation. You can use this panel to pan, tilt, zoom, and focus the camera, control the iris, and set the pan tilt speed. You can also move the camera to a selectable preset point, or run and repeat a cruise or sequence.

You can program presets, cruises, and sequences through the *PTZ&IMAGE* tab.

## 6 System settings

---

On the System tab, Administrators can set and modify the system parameters of the HSD820. This chapter offers a detailed description of settings, options, and values found on this tab.

### In This Chapter

6.1 System.....	24
6.2 Security.....	25
6.3 Network.....	33
6.4 DDNS.....	40
6.5 Mail.....	41
6.6 FTP.....	42
6.7 HTTP.....	43
6.8 Events.....	43
6.9 Storage management.....	55
6.10 Recording.....	59
6.11 Schedule.....	60
6.12 File location.....	61
6.13 View information.....	61
6.14 Factory default.....	65
6.15 Software version.....	66
6.16 Software upgrade.....	66
6.17 Maintenance.....	67

## 6.1 System

System > System

Clicking the System option in the left-hand panel displays the host name, time zone, and time synchronisation setting of the HSD820. Remember to press **Save** after changing any settings.

### 6.1.1 Host name

Specify a name to identify the camera on the network. If the alarm function is enabled and set to send alarm messages by mail or FTP the host name entered here is displayed in the alarm message. The maximum length of the host name is 63 characters.

### 6.1.2 Time zone

On the Time zone list, select the time zone that corresponds with the location of the camera.

### 6.1.3 Daylight saving time

#### » To enable daylight saving time

- 1 On the *System* tab, click **System** in the menu on the left.
- 2 Select **Enable daylight saving time**.
- 3 Specify the time offset.  
The format for the time offset is [hh:mm:ss]. If, for example, the time offset is 1 hour, enter 01:00:00 into the text box.
- 4 To set the daylight saving time duration, specify the **Start time** and **End time**.

## 6.1.4 Time format

### » To set a time format

- 1 On the *System* tab, click **System** in the menu on the left.
- 2 In the **Time format** list, select the desired format.  
Options: [yyyy/mm/dd], [dd/mm/yyyy]
- 3 Click **Save**.  
The date and time format shown above the live video window will be changed according to the selected format.

## 6.1.5 Time synchronisation

### » To sync the displayed date and time with those of your PC

- 1 On the *System* tab, click **System** in the menu on the left.
- 2 Click **Sync with computer time**.
- 3 Click **Save**.  
Note that the time will not be synchronised if you forget to click Save.

### » To set the displayed date and time manually

- 1 On the *System* tab, click **System** in the menu on the left.
- 2 Click **Manual**.
- 3 Enter the date and time  
Note that the entry format for date and time should match the one shown next to the entry field (yyyy/mm/dd).  
This in its turn is determined by the format that is selected on the Time format list.
- 4 Click **Save**.

### » To sync with an NTP server

- 1 On the *System* tab, click **System** in the menu on the left.
- 2 Select **Sync with NTP server**.  
The Network Time Protocol (NTP) will be used to synchronise the clock of the camera with an NTP server. For more information, refer to the website of [NTP](http://www.ntp.org) (see - <http://www.ntp.org>).
- 3 Enter the IP address or host name of the NTP server.
- 4 Select an update interval.
- 5 Click **Save**.  
Every time the camera boots up, it will be synchronised.

## 6.2 Security

From the Security pages, the administrator can perform user management, install security certificates, and enable and configure an IP address filter.

## 6.2.1 User

System > Security > User

### 6.2.1.1 Admin password

The default user name is Admin. The default password is 1234. User name and password are case sensitive.



**CAUTION:** MAKE SURE YOU CHANGE THE DEFAULT PASSWORD WHEN YOU OPEN THE WEB INTERFACE FOR THE FIRST TIME. TO KEEP THE ACCOUNT SAFE, SET A STRONG, COMPLEX PASSWORD. THIS HELPS TO PREVENT UNAUTHORISED ACCESS FROM PEOPLE WHO TRY TO USE THE DEFAULT ACCOUNT.

#### Strong password

For your privacy and to better protect your system against security risks, we strongly advise the use of strong passwords for all functions and network devices. Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user of the camera.

#### » To create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of at least two of the following categories: upper case letters, lower case letters, numbers and special characters

#### » To change the administrator password

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **User**.
- 3 Type the new password in the *Admin password* and *Confirm password* text boxes. Maximum password length is 14 characters. For security purposes, this input is displayed as dots.

**Note:** The following characters are valid: A-Z, a-z, 0-9, ! # \$ % & ' - . @ ^ \_ ~

- 4 Click **Save**.  
The web interface prompts the administrator for the new password for continued access.

**Note:** For better protection, especially in high-security systems, we advise you to change the password at regular intervals.

### 6.2.1.2 Add and manage user accounts

The camera supports a maximum of twenty user accounts. User names and passwords can be up to 16 characters. The maximum length for passwords is 14 characters. Each user can be assigned the privileges of *Camera control*, *Talk*, and *Listen*.

Privilege	Description
I/O access	Granted by default. Supports fundamental functions that enable users to view video when accessing the camera.
Camera control	Allows the user to change camera parameters on the PTZ tab.
Talk/Listen	Allow the user to communicate from the local machine with, for example, the administrator on a remote site.

#### » To add a user

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **User**.
- 3 In the *Add User* section, type the new user's name and password.
- 4 Click to select the **Camera control**, **Talk**, and **Listen** check boxes, as appropriate, to set the user's permissions.  
Permission to view the home page and operate its controls is granted, by default, to all users.
- 5 Click **Add** to add the new user.  
The new user is displayed in the User name list.

#### » To delete a user

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **User**.
- 3 In the *Manage User* section, select the name of the user you wish to delete.
- 4 Click **Delete** to remove the user.  
The application takes about 20 seconds to delete the user.

#### » To edit a user's password and privileges

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **User**.
- 3 In the *Manage User* section, select the name of the user and click **Edit**.
- 4 In the dialogue box, select/clear the user's permissions and/or change the user's password.  
Note that every user account requires a password and defined permissions.
- 5 Click **Save** to confirm settings.

### 6.2.1.3 HTTP Authentication Setting

HTTP Authentication identifies whether a user is authorised to access the camera. Users are required to enter a valid user name and password before they can log on to the camera.

Two types of authentication are available.

- **Basic**

This type provides basic protection against unauthorised access. It is supported by most browsers. Note that passwords are sent over the network in clear text. If intercepted they can be reused by unauthorised users. Select this type only if you are using an SSL connection or a dedicated line.

- **Digest**

This type is a more secure option. It encrypts the password before sending it over the network.

#### 6.2.1.4 Streaming Authentication Setting

Streaming authentication prevents unauthorised users from extracting a stream from the camera via the Real Time Streaming Protocol (RTSP). If authentication is enabled, users are required to enter a user name and password before they can view a live stream.

Two types of authentication are available.

- **Basic**

This type provides basic protection against unauthorised access. It is supported by most browsers. Note that passwords are sent over the network as plain text. If intercepted they can be reused by unauthorised users. Select this type only if you are using an SSL connection or a dedicated line.

- **Digest**

This type is a more secure option. It encrypts the password before sending it over the network.

##### » To enable streaming authentication

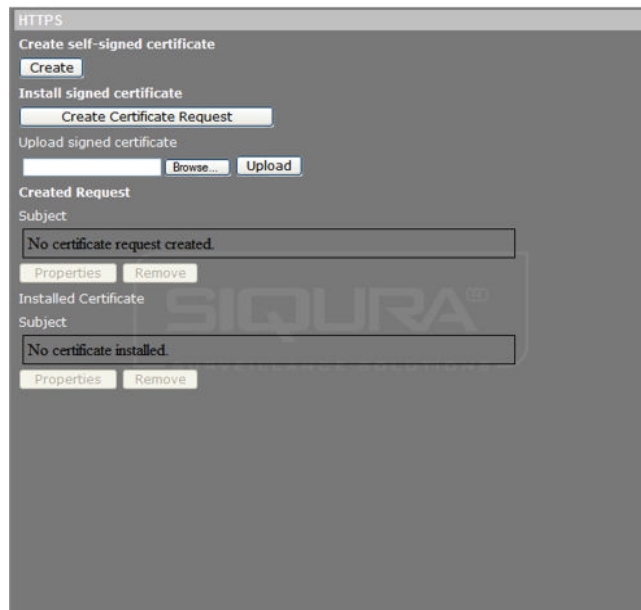
- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **User**.
- 3 In the **Type** list under *Streaming Authentication Setting*, click **basic** or **digest**, as desired.
- 4 Click **Save**.

##### » To disable streaming authentication

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **User**.
- 3 In the **Type** list under *Streaming Authentication Setting*, click **disable**.
- 4 Click **Save**.

Users will not be required to provide a name and password for authentication.

## 6.2.2 HTTPS



System > Security > HTTPS

### HTTPS, SSL, and TLS

Hypertext Transfer Protocol Secure (HTTPS) allows secure connections between the IP camera and the web browser using Secure Socket Layer (SSL) or Transport Layer Security (TLS), which protect camera settings and user name / password information from eavesdropping.

To implement and use HTTPS on the camera, an HTTPS certificate must be installed. This can be obtained by creating and sending a certificate request to a Certificate Authority (CA). Before a CA-issued certificate is obtained, users can create and install a self-signed certificate first.

**Note:** The self-signed certificate does not provide the same high level of security as when using a CA-issued certificate.

### 6.2.2.1 Create a self-signed certificate

#### » To create a self-signed certificate

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **HTTPS**.
- 3 Under *Create self-signed certificate*, click **Create**.
- 4 Enter the requested information in the *Create* dialog box, as described below.  
All fields are required.
- 5 After completing the form, click **OK** to save the certificate information.

Field	Description
Country	Enter a 2-letter combination code to indicate the country the certificate will be used in. For example, type "US" to indicate the United States.
State or province	Enter the local administrative region.
Locality	Enter other geographical information.
Organisation	Enter the name of the organisation to which the entity identified in "Common Name" belongs.
Organisational unit	Enter the name of the organisational unit to which the entity identified in "Common Name" belongs
Common name	Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
Valid days	Enter the period in days (1~9999) to indicate the valid period of certificate.

### 6.2.2.2 Create and install a signed certificate

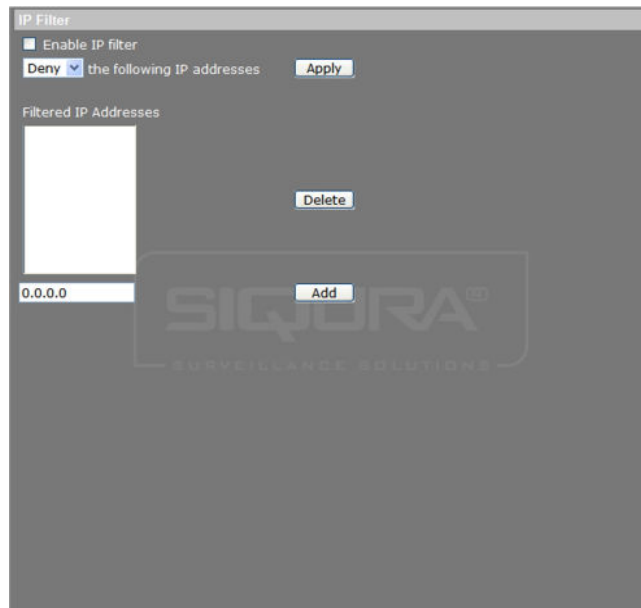
#### » To create a signed certificate request

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **HTTPS**.
- 3 To create request to obtain a signed certificate from a CA, click **Create Certificate Request**.
- 4 Enter the requested information in the *Create Certificate Request* dialog box, as described above.  
For a signed certificate from a CA, the *Valid days* field does not apply.
- 5 After completing the form, click **OK** to save the certificate information.  
The subject of the created request is shown in the Subject field.
- 6 Click **Properties**.
- 7 Copy the PEM-formatted request and send it to your selected CA.

#### » To install a signed certificate received from a CA

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **HTTPS**.
- 3 Under *Upload signed certificate*, click **Browse**.
- 4 Browse to the folder containing the signed certificate and select the file.
- 5 Click **Upload**.  
The certificate is installed and displayed under Installed Certificate.

## 6.2.3 IP filter



*System > Security > IP filter*

Using the IP filter, you can deny/allow access to the IP camera from specific IP addresses. Up to 256 IP addresses may be specified.

### » To enable the IP filter

- 1 On the *System* tab, click **Security** in the menu on the left.
- 2 In the *Security* submenu, click **IP filter**.
- 3 Select **Enable IP filter**.
- 4 To determine the IP filter behaviour, select **Deny** or **Allow** from the list.
- 5 Click **Apply**.  
IP addresses listed under Filtered IP Addresses are now allowed/denied access to the camera.

### » To add an IP address

- 1 Enter the IP address.
- 2 Click **Add**.  
The address is added to the currently configured IP addresses.  
Up to 256 IP addresses can be specified.

### » To delete an IP address

- 1 Select the IP address.
- 2 Click **Delete**.  
The IP address is removed from the list.

## 6.2.4 IEEE 802.1X

*System > Security > IEEE 802.1X*

The HSD820 is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). Users need to contact the network administrator to obtain certificates, User IDs, and passwords.

### 6.2.4.1 CA certificate

The CA certificate is created by the Certificate Authority (CA) for validation purposes. Upload the certificate to verify the server's identity.

#### » To install a CA certificate

- 1 On the *System* tab, click **Security** in the menu on the left.
  - 2 In the *Security* submenu, click **IEEE 802.1X**.
  - 3 Under *CA certificate*, click **Browse**.
  - 4 Browse to the folder containing the certificate and select the file.
  - 5 Click **Upload**.
- The certificate is installed.

### 6.2.4.2 Client certificate and private key

The Client certificate and Private key must be uploaded to authenticate the camera itself.

#### » To upload a Client certificate / Private key

- 1 On the *System* tab, click **Security** in the menu on the left.
  - 2 In the *Security* submenu, click **IEEE 802.1X**.
  - 3 Under Client certificate/Private key, click **Browse**.
  - 4 Browse to the folder containing the certificate/key and select the file.
  - 5 Click **Upload**.
- The certificate/key is installed.
- 6 In the *Identity* text box, enter the user identity associated with the certificate.

- Up to 16 characters can be used.
- 7 In the *Private key password* text box, enter the password for your user identity.  
Up to 16 characters can be used.
  - 8 To enable IEEE 802.1X, select **Enable IEEE 802.1x**.
  - 9 Click **Save**.

## 6.3 Network

From the Network pages, the administrator can configure IP address assignment and settings for Quality of Service (QoS), the Simple Network Management Protocol (SNMP), and Universal Plug and Play (UPnP).

### 6.3.1 Basic

System > Network > Basic

This page describes how to configure the camera to use a fixed IP address or acquire the address dynamically through the Dynamic Host Configuration Protocol (DHCP). You can also configure PPPoE support, Advanced network settings, and enable IPv6 support.

**Note:** When the IP address is changed, webpage communication is lost. Log on to the webpage with the new address to re-establish the connection.

#### 6.3.1.1 Acquire an IP address automatically

By default, the HSD820 cameras are configured to use a fixed IP address. Administrators can set the camera to obtain its IP address via the Dynamic Host Configuration Protocol (DHCP).

**Note:** When an IP address changes, cameras using DHCP can always be identified by their MAC address, found on the camera's label. You are advised to keep the MAC address on record for future identification.

» **To acquire the IP address via DHCP**

- 1 On the System tab, click **Network** in the menu on the left.
- 2 In the *Network* submenu, select **Basic**.
- 3 Click **Get IP address automatically**.
- 4 Click **Save** to confirm the new setting.  
The camera restarts automatically.  
To find the camera on the network, use Siquira Device Manager (available for download at [www.siquira.com](http://www.siquira.com)).

### 6.3.1.2 **Modify the fixed IP address**

The factory default IP address is in the 10.x.x.x range.

» **To modify the camera's fixed IP address**

- 1 On the System tab, click **Network** in the menu on the left.
- 2 In the *Network* submenu, select **Basic**.
- 3 Select **Use fixed IP address**.
- 4 In the *IP address* box, type the camera's IP address.
- 5 Enter the subnet mask, default gateway, and DNS server IP addresses in the appropriate boxes.  
See below for more detailed information.
- 6 Click **Save** to confirm the new settings.
- 7 Enter the new IP address in the address bar of your web browser, and then press **Enter** to re-establish communication with the camera.  
- or -  
Find the camera with Siquira Device Manager (available for download at [www.siquira.com](http://www.siquira.com))

#### **IP address**

The IP address identifies the camera on the network.

#### **Subnet mask**

The subnet mask is used to determine if the destination is on the same subnet. The default value is 255.0.0.0.

#### **Default gateway**

The default gateway is used to forward frames to destinations on other subnets. If the gateway setting is invalid, transmissions to destinations on other subnets will fail.

#### **DNS**

The primary DNS is the primary domain name server that translates host names into IP addresses. The secondary DNS is a second domain name server that is used if the primary DNS is unavailable.

### 6.3.1.3 Use PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) enables users to securely transfer data.

#### » To use PPPoE

- 1 On the System tab, click **Network** in the menu on the left.
- 2 In the *Network* submenu, select **Basic**.
- 3 Click **Use PPPoE**.
- 4 Specify the PPPoE user name and password.
- 5 Click **Save**.

### 6.3.1.4 Advanced settings

#### Web Server port

The HTTP port can be any port other than the default port, 80. If the port is changed, the user must be notified of the change for connections to be successful.

For example, if the administrator changes the HTTP port of a camera with an IP address of 192.168.0.100 from 80 to 8080, the user must type in the address `http://192.168.0.100:8080` instead of `http://192.168.0.100`.

#### RTSP port

The RTSP port can be any port other than the default port, 554. If the port is changed, the user must be notified of the change for connections to be successful. The port number may range from 1024 to 65535.

For example, if the administrator changes the RTSP port of a camera with an IP address of 192.168.0.100 from 554 to 8080, the user must type in the address `rtsp://192.168.0.100:8080` instead of `rtsp://192.168.0.100`.

#### MJPEG over HTTP port

The HTTP port that streams MJPEG can be any port other than the default port, 8008. If the port is changed, the user must be notified of the change for connections to be successful. The port number may range from 1024 to 65535.

For example, if the administrator changes the MJPEG over HTTP port of a camera with an IP address of 192.168.0.100 from 8008 to 8080, the user must type in the address `http://192.168.0.100:8080` instead of `http://192.168.0.100`.

#### HTTPS port

The HTTPS port can be any port other than the default port, 443. If the port is changed, the user must be notified of the change for connections to be successful. The port number may range from 1024 to 65535.

For example, if the administrator changes the HTTPS port of a camera with an IP address of 192.168.0.100 from 443 to 650, the user must type in the address `https://192.168.0.100:650` instead of `https://192.168.0.100`.

**Note:** To avoid network conflicts, make sure that you use a unique port number for each of the ports above.

### 6.3.1.5 IPv6 address configuration

#### » To enable IPv6 support

- 1 On the System tab, click **Network** in the menu on the left.

- 2 In the *Network* submenu, select **Basic**.
- 3 Under *IPv6 Address Configuration*, select **Enable IPv6**.
- 4 Click **Save**.  
The IPv6 IP address is displayed.

### 6.3.2 QoS



*System > Network > QoS*

#### DiffServ and QoS

Differentiated Services (DiffServ, or DS) is a method for adding Quality of Service (QoS) to IP networks. In routed networks, critical network traffic such as video and audio streams, which require a relatively uninterrupted flow of data, can get blocked due to other traffic. DiffServ can be used to classify network traffic and give precedence - that is, low-latency, guaranteed service, to high-priority traffic, while offering best-effort service to non-critical traffic such as file transfers or Web traffic.

Each stream has a DSCP (Differentiated Services Code Point) field in the IP header. Routers will identify the network service type in the DSCP field and provide the appropriate level of service. Low-latency service can be realised, for example, through priority queuing, bandwidth allocation, or by assigning dedicated routes.

#### DSCP settings

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled. The IP camera uses the following QoS Classes: Video, Audio, and Management.

#### Video DSCP

The class consists of applications such as MJPEG over HTTP, RTP/RTSP, and RTSP/HTTP.

#### Audio DSCP

This setting is available for IP cameras that support audio.

#### Management DSCP

The class consists of HTTP traffic: Web browsing.

**Note:** Before enabling this function, make sure the switches/routers in the network support QoS.

### 6.3.3 SNMP

System > Network > SNMP

With the Simple Network Management Protocol (SNMP), part of the internet protocol suite, the HSD820 can be monitored and managed remotely by a network management system.

#### SNMP v1/v2

To enable the version of SNMP to use, select the appropriate check box.

##### Read Community

Specify the community name that has read-only access to all supported SNMP objects. The default value is "public".

##### Write Community

Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is "private".

#### SNMP v3

SNMP v3 supports an enhanced security system that provides protection against unauthorised users and ensures the privacy of the messages. Users will be requested to enter a security name, authentication password and encryption password while setting the camera connections in the network management system. With SNMP v3, the messages sent between the cameras and the network management system will be encrypted to ensure privacy.

#### » To use SNMP v3

- 1 On the System tab, click **Network** in the menu on the left.
- 2 In the *Network* submenu, select **SNMP**.
- 3 Type a name in the *Security Name* box.  
Maximum length: 32 characters.

- Valid characters: A-Z, a-z, 0-9, !#\$%&'-.@^\_~
- 4 In the *Authentication Type* list, click **MD5** or **SHA**.  
SHA offers a higher security level.
  - 5 Type a password in the *Authentication Password* box.  
Length: Eight characters or more.  
For security purposes, characters/numbers are displayed as dots.  
Valid characters: A-Z, a-z, 0-9, !#\$%&'-.@^\_~
  - 6 In the *Encryption Type* list, click **DES** or **AES**.  
AES offers a higher security level.
  - 7 Type a password in the *Encryption Password* box.  
Minimum length: eight characters. Maximum length: 512 characters.  
For security purposes, characters/numbers are displayed as dots.  
Valid characters: A-Z, a-z, 0-9, !#\$%&'-.@^\_~

**Note:** The encryption password can be left blank. In that case, however, messages will not be encrypted.

- 8 Select **Enable SNMP v3**.
- 9 Click **Save**.

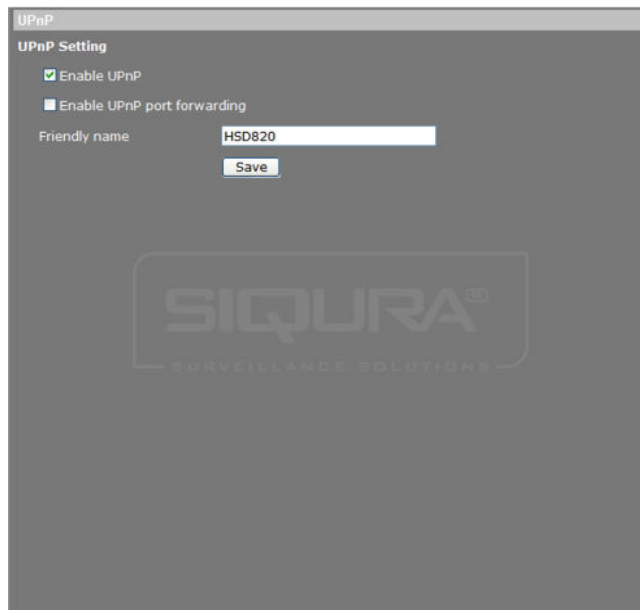
### Traps for SNMP v1/v2/v3

Traps are used by the HSD820 to send messages to a management system to report important events or status changes.

#### » To use traps

- 1 Select **Enable traps**.
- 2 In the *Trap address* box, type the IP address of the management server.
- 3 In the *Trap community* box, enter the community to use when sending a trap message to the management system.
- 4 If desired, select **Warm start**.  
A Warm Start SNMP trap signifies that the SNMP device - that is, the HSD820, reinitialises itself by performing a software reload, such that its configuration is unaltered.
- 5 Click **Save**.

### 6.3.4 UPnP



System > Network > UPnP

#### Enable UPnP

If enabled, Universal Plug and Play (UPnP) allows the HSD820 to advertise its presence and services to control points on the network. A control point can be a network device with embedded UPnP or a Video Management System (VMS). The icon of the HSD820 will appear in *My Network Places* to allow direct access.

**Note:** To access the camera from your computer through UPnP, ensure that the UPnP networking service is installed on your computer. For more information, see *Appendix: Enable UPnP*.

#### Enable UPnP port forwarding

When UPnP port forwarding is enabled, the HSD820 is allowed to open the web server port on the router automatically.

**Note:** To enable this function, ensure that your router supports UPnP and that the function is activated.

#### Friendly name

Set the name that the HSD820 will use to identify itself on the network.

## 6.4 DDNS

System > DDNS

The Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronised with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated with a static domain name so that others can connect to it by name.

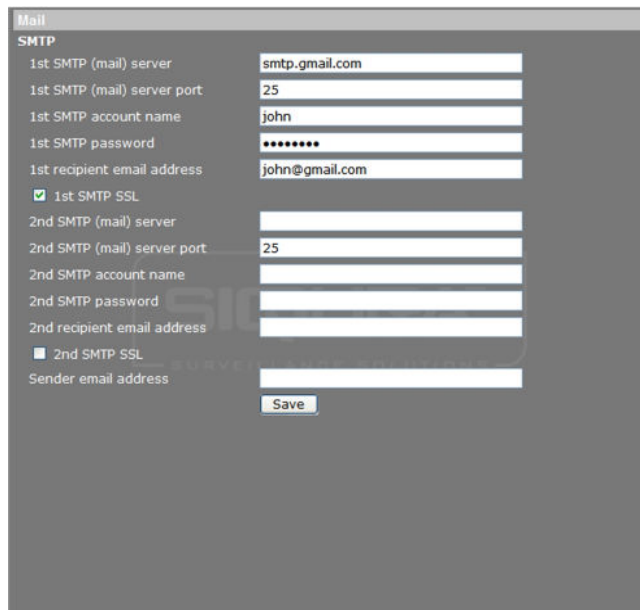
### » To use DDNS

- 1 From the Network page, set the camera to acquire its IP address via DHCP, as described in *Acquire an IP address automatically*.
- 2 On the System tab, click **DDNS** in the menu on the left.
- 3 Select **Enable DDNS**.
- 4 In the *Provider* list, select the DDNS provider .
- 5 Type the registered domain name in the *Host name* box.

**Note:** Only enter the desired third-level host name into the box. For example, if the host name is hsd820.dyndns.org, then type hsd820.

- 6 In the *User name/E-mail* box, type the user name or e-mail required by the DDNS provider for authentication.
- 7 In the *Password/Key* box, type the password or key required by the DDNS provider for authentication.
- 8 Click **Save** to confirm settings.

## 6.5 Mail

The screenshot shows a web interface for configuring mail settings. The title is 'Mail'. Under the 'SMTP' section, there are two main configurations: '1st SMTP (mail) server' and '2nd SMTP (mail) server'. The first server configuration includes fields for '1st SMTP (mail) server' (smtp.gmail.com), '1st SMTP (mail) server port' (25), '1st SMTP account name' (john), '1st SMTP password' (masked with dots), '1st recipient email address' (john@gmail.com), and a checked checkbox for '1st SMTP SSL'. The second server configuration has fields for '2nd SMTP (mail) server', '2nd SMTP (mail) server port' (25), '2nd SMTP account name', '2nd SMTP password', and '2nd recipient email address', with an unchecked checkbox for '2nd SMTP SSL'. A 'Sender email address' field is at the bottom. A 'Save' button is located at the bottom right of the form.

*System > Mail (example settings)*

On the Mail page, administrators can configure SMTP settings for sending an email via the Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. SMTP is a protocol for exchanging email messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

### » To configure SMTP settings

- 1 On the *System* tab, click **Mail** in the menu on the left.
- 2 Enter the following SMTP details:
  - 1st SMTP (mail) server (IP address or host name)
  - 1st SMTP (mail) server port (21 is the default port for FTP servers)
  - 1st SMTP account name
  - 1st SMTP password
  - 1st recipient email address (entire email address limited to 64 characters)
  - If the server requires a secure connection (SSL), select **1st SMTP SSL**
- 3 If desired, repeat step 2 for the second SMTP configuration.
- 4 Click **Save**.

### SMTP server

For SMTP server details (IP address or name), contact your network service provider or network administrator.

### Sender email address

The sender's email address will be displayed in the alarm triggered email or FTP message.

## 6.6 FTP

*System > FTP*

Administrators can configure the camera to send messages to one or two specific File Transfer Protocol (FTP) sites when an alarm is triggered. For FTP server details, contact your network administrator or network service provider, or install FTP software on a PC on the same network as the camera.


### » To configure FTP settings

- 1 On the *System* tab, click **FTP** in the menu on the left.
- 2 Enter the following FTP details:
  - Server (IP address or host name)
  - Server port (21 is the default port for FTP servers)
  - User name (from the account created on the FTP server)
  - Password
  - Remote folder

**Note:** Do not enter the complete FTP path into the remote folder field. For example, if the remote folder is C:\FTP\example\ and the FTP path is C:\FTP\, then only the word 'example' should be entered.

- 3 Enable the 1st FTP passive mode or the 2nd FTP passive mode or both, if necessary.  
In passive mode, the relevant FTP server initiates a connection with the FTP client by sending its IP address through a dynamic port. In active mode, the FTP client initiates the connection.
- 4 Press **Save** when finished.

## 6.7 HTTP



*System > HTTP*

An HTTP Notification server can listen for notification messages from IP cameras triggered by events. Alarm triggered and motion detection notifications can be sent to the specified HTTP server. See also pages such as *Application*, *Motion Detection*, and *Tampering* for HTTP Notification settings.

### » To configure HTTP settings

- 1 On the *System* tab, click **HTTP** in the menu on the left.
- 2 Enter the following HTTP details:
  - HTTP server (for example, `http://192.168.0.1/admin.php`)
  - User name
  - Password
- 3 Click **Save** when finished.

## 6.8 Events

From the Events pages, the administrator can configure settings for alarms, motion detection, network failure detection, periodical events, and manual trigger.

## 6.8.1 Application

System > Events > Application

HSD820 cameras provide two digital alarm inputs and two digital alarm outputs to be used with alarms and their specified trigger actions. For information about the alarm pin definition and connecting alarm devices, see the HSD820 Installation Manual.

On the Application page, administrators can set the active state of the digital inputs and outputs (I/O), enabling the camera to trigger an alarm when the state of the alarm connectors changes.

### » To set up alarm settings

- 1 On the **System** tab, click **Events** in the menu on the left, and then click **Application**.
- 2 Under *Alarm pin selection*, select the alarm you wish to configure, and then click **Edit**.
- 3 In the **Alarm switch** list, click **On** or **Off** to enable or disable the alarm input and the actions triggered by it.

Alternatively, you can use *By schedule* to activate the alarm function according to a schedule you have previously set on the *Schedule* page.

- 4 In the *Alarm type* list, select **Normal close** or **Normal open**, according to the application. See below for more details.
- 5 Under *Triggered action*, select the actions that are to be performed in the event of an alarm. For more information, see *Alarm trigger actions*.
- 6 If applicable, under *File name*, specify a file name for a file to be sent when an alarm occurs, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.
- 7 Click **Save**.

Note that SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions. For more information, see *Mail*, *FTP*, and/or *HTTP*.

**Important:** Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

## Alarm type

The input type drives the alarm output. *Normal close* indicates that the connectors are normally closed and a disconnection will trigger a digital output signal. *Normal open* indicates that the connectors are normally open and a connection will trigger a digital output signal. See the relevant installation manual for more information.

### 6.8.1.1 Alarm trigger actions

System > Events > Application > Triggered action

The actions detailed in this section can be set to be triggered when an alarm occurs. Make sure that the SMTP, FTP, and/or HTTP configuration is complete before you configure the triggered actions for an alarm. For more information, see *Mail*, *FTP*, and/or *HTTP*.

## Enable alarm output

The HSD820 provides two alarm outputs. They can be enabled by selecting the *Enable alarm output 1* and *Enable alarm output 2* check boxes.

**Note:** The output state is determined by any combination of the alarm inputs (digital input and motion detection). The alarm inputs can be individually enabled to drive the output, provided the alarms themselves are already enabled. The enabled alarms are combined by a logical OR to activate the output. The output type is therefore the same for all enabled alarms. An API command (from a VMS, for example) can override the current output state to inactive until the next enabled alarm is triggered, or it can also set the output state to active.

## Send message by FTP

A message is sent to the FTP site, as configured on the FTP page, when an alarm is triggered. For information on how to configure messages to be sent to an FTP site, see *FTP*.

## Upload image by FTP

When an alarm is triggered, a specified number of pre- and post-trigger buffer frames are sent to the configured FTP server. The Pre-trigger buffer function allows users to check what happened to cause the trigger.

**Note:** Normally, the range of the Pre-trigger buffer is 1-20 frames. This range will change accordingly if the MJPEG frame rate on the *Video frame rate* page is 6 or slower.

With the Post-trigger function, users can set a certain amount of images to be uploaded after the triggering of the alarm input.

**Important:** Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

### Continue image upload

If selected you can choose to upload the triggered images for a certain time or to keep uploading until the trigger is off.

- Upload for n sec  
The number of frames per second (fps) selected in the *Image Frequency* list is sent to the FTP Server for the number of seconds specified in the *Upload for n sec* box. The range is 1 to 9999 seconds.
- Upload during trigger active  
The number of frames per second (fps) selected in the *Image Frequency* list is sent to the FTP Server until the trigger is no longer active. The range is 1 to 15 frames.

### PTZ function

Assign a camera function - Preset, Sequence, Autopan, or Cruise - and specify a Preset Point/Sequence Line/Autopan Path/Cruise Line for the camera to perform at an alarm occurrence. For a description of these functions, see *PTZ&IMAGE*.

If the selected function is *Preset*, the dwell time must be specified in the *Dwell time* box. When the alarm is triggered, the camera will go to the selected Preset Point and stay there for the user-defined period of time. As for other function modes, the camera will keep executing the specified function. To stop this action, simply change the camera status.

**Note:** The dwell time can only be adjusted when *Preset* is selected as the alarm action. When the dwell time has expired, the camera will go back to its trigger position and recheck the alarm pin status.

### Record video clip

Using the options on the *Record to* list, you can have an alarm-triggered recording saved to your microSD card or NAS. The Pre-trigger buffer function allows you to check what occurrence caused the trigger. The Pre-trigger buffer time range is from 1 to 3 seconds.

You can choose from the following actions:

- Upload for n sec  
The image stream is recorded for the number of seconds (setting range from 1 to 99999 seconds) specified in the *Upload for n sec* text box with a pre-trigger buffer of the number of seconds specified in the *Pre-trigger buffer* text box.
- Upload during trigger active  
The image stream is recorded with a pre-trigger buffer of the number of seconds specified in the *Pre-trigger buffer* text box until the trigger is no longer active.

**Note:** Make sure that local recording (with the microSD card) or remote recording (with NAS) is activated (on the *Recording* page) so that this function can be implemented.

### Send message by E-mail

A message is sent by email, as configured on the Mail page, when an alarm is triggered. For more information on configuring messages to be sent via SMTP, see *Mail*.

## Upload Image by E-mail

When an alarm is triggered, a specified number of pre- and post-trigger buffer frames are sent to the configured email address.

The Pre-trigger buffer function allows users to check what happened to cause the trigger.

**Note:** Normally, the range of the Pre-trigger buffer is 1-20 frames. This range will change accordingly if the MJPEG frame rate on the Video frame rate page (see "Video frame rate" on page 75) is 6 or slower.

With the Post-trigger function, users can set a certain amount of images to be uploaded after the triggering of the alarm input.

**Important:** Make sure that the SMTP configuration has been completed. For details, see Mail ( on page 41).

## Continue image upload

If selected you can choose to upload the triggered images for a certain time or to keep uploading until the trigger is off.

- Upload for n sec  
Emails are sent for the number of seconds specified in the *Upload for n sec* box. The range is 1 to 9999 seconds. Each email contains the number of frames per second (fps) selected from the *Image Frequency* list.
- Upload during trigger active  
Emails are sent until the trigger is no longer active. Each email contains the number of frames per second (fps) selected from the *Image Frequency* list. The range is 1 to 15 frames.

## Send HTTP notification

An HTTP Notification Server can listen for notification messages from IP cameras. The HSD820 can send alarm- and motion detection-triggered notifications to the server selected in the *HTTP address* list. For information on HTTP configuration, see *HTTP*.

### » To enable the sending of HTTP notifications

- 1 Select **Send HTTP notification**.
- 2 In the **HTTP address** list, select an HTTP server.
- 3 In the *Custom parameters* box, specify the parameters for event notifications.  
If, for example, the custom parameter is set as "[action=1&group=2](#)" and the HTTP server name is "[http://192.168.0.1/admin.php](#)", the notification will be sent to the HTTP server as "[http://192.168.0.1/admin.php?action=1&group=2](#)" when an alarm is triggered.

## 6.8.1.2 Specifying file name conventions

File name

File name :

☒ Add date/time suffix

☐ Add sequence number suffix (no maximum value)

☐ Add sequence number suffix up to  and then start over

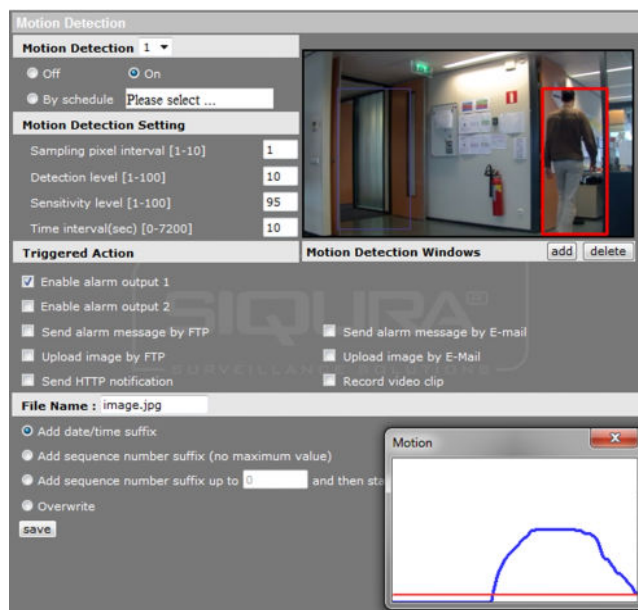
☐ Overwrite

Application > Alarm pin# status > File name

The File Name text box allows users to specify the file name conventions for captured images. The following options are available for naming image files.

- *File name*  
Enter a file name for the uploaded images. For example, image.jpg. A suffix will be added unless Overwrite is selected.
- *Add date/time suffix*  
An incremented sequence number and the date and time of when an image is captured are added to the end of the file name. The date, time, and sequence number are provided as follows:  
imageYYMMDD\_HHNNSS\_XX.jpg, where,  
- Y: Year  
- M: Month  
- D: Day  
- H: Hour  
- N: Minute  
- S: Second  
- X: Sequence Number
- *Add sequence number suffix (no maximum value)*  
An incremented sequence number is added to the end of the file name. The sequence number is unlimited.
- *Add a sequence number suffix up to n and then start over*  
An incremented sequence number is added to the end of the file name. The numbering is reset when it reaches the given maximum value, at which point images from previous numbering cycles will be overwritten.
- *Overwrite*  
The latest uploaded image file with a static file name will overwrite the previous image.

## 6.8.2 Motion Detection



System > Events > Motion detection

The Motion Detection function enables the camera to trigger an alarm when motion in a specified area reaches or exceeds a configured sensitivity threshold value.

**Note:** To prevent false alarms, Motion Detection is disabled during PTZ control and when working with presets, autopan, sequences, and cruises.

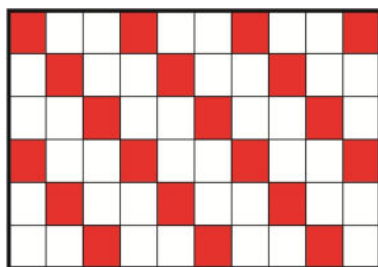
The Motion Detection function supports up to four sets of Motion Detection settings.

#### » To enable and configure a Motion Detection set

- 1 On the **System** tab, click **Events** in the menu on the left, and then click **Motion detection**.
- 2 In the **Motion Detection** list, click the Motion Detection set that you want to configure.
- 3 To enable the set, click **On**.  
The default setting is *Off*. Alternatively, you can use *By schedule* to activate this Motion Detection set according to a schedule you have previously set on the *Schedule* page.
- 4 Under *Motion Detection Setting*, enter values for the following parameters.

- Sampling pixel interval [1-10]

The default value is 1, which means the system takes one sampling pixel for every pixel. If the value is set to 3, for example, the system will take one sampling pixel for every 3 pixels per each row and each column within the detection region.



- Detection level [1-100]

The default level is 10. This parameter sets the detection level for the sampling pixels. The lower the value, the more sensitive for each sampling pixel.

- Sensitivity level [1-100]

The default level is 80, which means that if 20% or more pixels in the detection window change, the system will detect motion. The higher the value, the more sensitive it is. As the value increases, the red horizontal line in the motion indication window will lower accordingly.

- Time interval (sec) [0-7200]

The default interval is 10. This value is the duration in seconds between each detected motion.

- 5 Under *Triggered Action*, select **Enable alarm output** to activate the Alarm Output configuration.
- 6 Under *Triggered action*, select the desired trigger actions that are to be performed in the event of an alarm. For more information, see *Alarm trigger actions*.
- 7 If applicable, under *File name*, specify a file name for a file to be sent when an alarm occurs, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.
- 8 Click **Save**.  
SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions. For more information, see *Mail, FTP, and/or HTTP*.

**Important:** Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

### 6.8.2.1 Motion detection area

Per Motion Detection set, up to ten motion detection windows can be added. A red frame displays in the camera view around the selected detection area. These areas can be added removed, moved, and/or resized.



*Motion detection with two windows configured*

#### » To add a motion detection area

- Click **add**.

#### » To remove a motion detection area

- Select the area, and then click **delete**.

#### » To resize a motion detection area

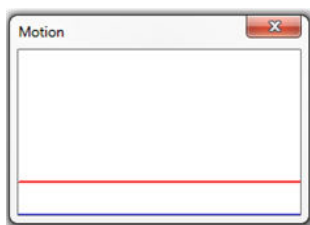
- Point to the edge of the red frame and drag the pointer to modify the size of the motion detection area.

#### » To move the motion detection frame

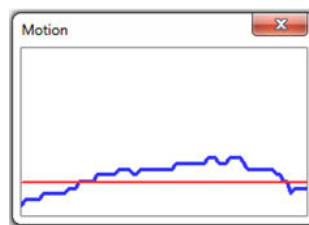
- Press and hold the mouse button in the centre of the red frame and drag the frame to the desired position.

### 6.8.2.2 Motion detection window

The Motion window appears when Motion Detection is active. It displays the configured motion detection threshold level. The amount of motion currently being detected is shown as a blue graph line relative to the motion detection threshold level.

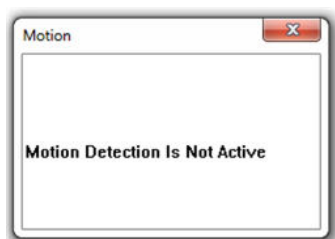


*The configured motion detection threshold level*



*Peaks rising above the set motion detection level will trigger an alarm and possibly actions as well.*

Motion Detection alarms will not trigger if the Motion Detection function is disabled or while the Motion Detection settings are saving. In these cases, the motion indication window displays the text, Motion Detection Is Not Active.



*Motion detection is disabled.*

### 6.8.3 Network Failure Detection



*System > Network failure detection*

#### Ping request

The network failure detection function enables the HSD820 to test the connection between the camera and a target host on the network (for example, an NVR, VMS, or Video Server). The camera can ping the remote machine - that is, send data packets to it, with configurable intervals to determine if it is accessible and responding. Appropriate actions can be selected to be triggered if the ping request times out without a response. Being capable of implementing local recording when network failure occurs, the camera can be a backup recording device for the surveillance system.

#### Detection Switch

Click *On* or *Off* to enable or disable the Network failure detection alarm, respectively. Alternatively, you can use *By schedule* to activate Network Failure Detection according to a schedule you have previously set on the *Schedule* page.

## Detection Type

The IP address you specify here will be pinged at the interval entered for "every  $n$  minutes". Range: 1-99 minutes.

## Triggered Action

Select the desired trigger actions which are to be performed in the event of an alarm. For more information, see *Alarm trigger actions*.

## 6.8.4 Periodical event

System > Events > Periodical event

On the Periodical event page, users can set the camera to upload images periodically to an FTP site or an email address. For example, if the time interval is set to 60 seconds, the camera will upload images to the assigned FTP site or email address every 60 seconds. The images to be uploaded are the images before and after the triggered moment. In the Triggered Action section users can define how many images are to be uploaded.

### Periodical event

The default setting for the Periodical Event function is *Off*. Enable the function by selecting *On*.

### Time interval

The default value of the time interval is 60 seconds. The setting range of the time interval is from 60 to 3600 seconds

### Triggered action

Select the desired trigger actions which are to be performed in the event of an alarm. For more information, see *Alarm trigger actions*.

### File name

The File Name text box allows users to specify the file name conventions for captured images. For more information, see *Specifying file name conventions*.

## 6.8.5 Manual trigger

**Manual Trigger**

**Manual Trigger**

☒ Off ☐ On

**Triggered Action**

<input checked="" type="checkbox"/> Enable alarm output 1	<input type="checkbox"/> Enable alarm output 2
<input type="checkbox"/> Send message by FTP	<input type="checkbox"/> Send message by E-Mail
<input type="checkbox"/> Upload image by FTP	<input type="checkbox"/> Upload image by E-Mail
<input type="checkbox"/> PTZ Function	<input type="checkbox"/> Send HTTP notification
<input type="checkbox"/> Record video clip	

**File Name**

File name :

☒ Add date/time suffix

☐ Add sequence number suffix (no maximum value)

☐ Add sequence number suffix up to  and then start over

☐ Overwrite

System > Events > Manual trigger

On the Manual trigger page, administrators can activate manual alarm triggering and define the actions to be taken when the user clicks the Manual Trigger button on the Home page.

### Manual Trigger

Click *On* or *Off* to enable or disable the Manual trigger, respectively.

### Triggered action

Select the desired trigger actions which are to be performed in the event of an alarm. For more information, see *Alarm trigger actions*.

### File name

The File Name text box allows users to specify the file name conventions for captured images. For more information, see *Specifying file name conventions*.

## 6.8.6 Audio detection

System > Events > Manual trigger

The Audio detection function allows the camera to detect audio and trigger alarms when the audio volume in the detected area reaches/exceeds the determined sensitivity threshold value.

### ► To enable Audio detection

- 1 On the *System* tab, click **Events** in the menu on the left.
- 2 Click **Audio detection**.
- 3 Under *Audio Detection*, select **On**.  
The default setting is *Off*.
- 4 Under *Audio Detection Setting*, type a *Detection Level* value.  
This value sets the detection level for each sampling volume; the smaller the value, the more sensitive it is. The default level is 10.
- 5 Under *Audio Detection Setting*, type a *Time interval* value.  
The value is the interval between each detected audio event. The default interval is 10.
- 6 Under *Triggered Action*, select the actions to be performed when audio is detected. For more information, see the *Triggered Action* section.
- 7 If applicable, under *File name*, specify a file name for a file to be sent when audio is detected, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.
- 8 Click **Save**.  
SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions.

**Important:** Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

## 6.9 Storage management

Recorded video can be stored on a microSD card inserted into the camera or on a network share.

### 6.9.1 SD Card

The screenshot shows the 'Storage Management' interface. It is divided into several sections:

- Device information:**
  - Device type: SD card
  - Free space: 1235748KB
  - Total size: 1921952KB
  - Status: Yes
  - Full: No
- Device setting:**
  - Format device:
- Disk cleanup setting:**
  - ☒ Enable automatic disk cleanup
  - Remove recordings older than: 1 day(s)
  - Remove oldest recordings when disk is: 85 % full
  -
- Recording list:**
  - From: 2014-05-08 to: 2014-05-10
  - Date (yyyy-mm-dd) Date (yyyy-mm-dd)
  - 

FileName	Size
M0_20140509_160625.avi	8218KB
M0_20140509_160649.avi	2195KB
N_20140509_160353.avi	13090KB
N_20140509_163058.avi	47554KB

  -

System > Storage management > SD Card

You can implement local recording using a microSD/SDHC card up to 64 GB. On the Storage Management page, administrators can view capacity information of the microSD/SDHC card and a recording list with all the recording files that are saved on the memory card. Administrators can also format the SD card and implement automatic recording cleanup.

**Note:** Format the microSD/SDHC card when using it for the first time. Formatting is also required when a memory card already used on one camera is transferred to another camera with a different software platform.

#### » To implement and activate recording to the SD card

- On the *Storage Management* page, format the card, if necessary, and configure disk cleanup settings.
- On the *Recording* page, set a recording schedule.  
- and/or -
- Under *Triggered action* on the *Application*, *Motion detection*, *Network failure detection*, *Tampering*, *Manual trigger*, or *Audio detection* webpage, select **Record video clip**.  
When the recording mode is set to *Always* (consecutive recording) and microSD/SDHC card recording is also allowed to be triggered by events, the system will immediately start recording to the memory card once events occur. The camera will return to the regular recording mode when event recording stops.

## Device information

The Device information section of the Storage Management page shows:

- The type of storage card
- The amount of free space available on the card
- The total amount of storage on the card
- Status - whether or not there is a card in the microSD slot of the camera
- Full - whether or not the card has any available memory

## Device setting

Under Device setting, the administrator can format or reformat an inserted SD card.



**Warning:** Formatting the SD card erases *all* information on the card. Be sure to download any information on the card you want to save before reformatting. See *Recording list* below for more information.

## Disk cleanup setting

Use this section to remove old recordings automatically. You can set it to remove recordings older than the specified number of days or weeks and/or to remove recordings starting with the oldest on the card when a specified percentage of the card is full.

## Recording list

Each video file on the microSD/SDHC card is listed in the Recording list. The maximum file size is 60 MB per file. When the recording mode is set to "Always" (consecutive recording) and the microSD/SDHC card recording is also allowed to be triggered by events, the system will immediately start event recording to the memory card when an event occurs. The camera returns to the regular recording mode after event recording stops.

Using the *From/To* time boxes, users can search the recorded files in a specified time range. Two file formats - that is, \*.avi (video format) and \*.jpeg (image format), are available for selection. The following capital letters are used to indicate the recording type:

- A: Alarm
- M: Motion detection
- N: Network failure
- R: Regular (scheduled recording)
- T: Tampering
- U: Audio detection
- V: Manual trigger

Files can be removed, sorted, and downloaded.

### » To remove a file

- 1 Click on the selected file.
- 2 Press the **Remove** button.  
The file is deleted from the card.

### » To sort the files by name and date

- Click **Sort**.

### » To save or view a recording file

- 1 In the Recording list, select a file.
- 2 Click **Download**.

A window appears with a link to the file.

- 3 Click on the link to save the file locally or to play it in your default viewing software.

## 6.9.2 Network Share

System > Storage management > Network Share

The HSD820 supports recording video to a network share. On the Network Share page, administrators can view capacity information of the network share and a recording list with all the recording files that are saved on the network share. Administrators can also format the network share and implement automatic recording cleanup.

### » To implement and activate recording to the network share

- 1 On the *Network Share* page, use the *Host* and *Share* boxes in the *Storage Settings* section to specify the path to the network share.
- 2 In the *User name* and *Password* boxes, provide the credentials required to access the network share.
- 3 Click **Save**.  
The network share status information appears in the Device information section.
- 4 Format the network share, if necessary, and configure disk cleanup settings.

**Warning:** Formatting the network share erases *all* information on the share. Be sure to save a copy of any information on the share you need to keep before reformatting. See *Recording list* below for more information.

- 5 On the *Recording* page, set a recording schedule.  
- and/or -

Under *Triggered action* on the *Application*, *Motion detection*, *Network failure detection*, *Tampering*, *Manual trigger*, or *Audio detection* webpage, select **Record video clip**.

When the recording mode is set to *Always* (consecutive recording) and recording is also allowed to be triggered by events, the system will immediately start recording to the network share once events occur. The camera will return to the regular recording mode when event recording stops.

## Device information

The Device information section of the Network Share page shows:

- The type of storage device
- The amount of free space available on the device
- The total amount of storage on the device
- Status - whether the device is offline or online
- Full - whether or not there is storage space available

## Storage Settings

Use this section to provide details regarding the protocol to be used, the path to the network share, and the user's identity. If you cannot access the network share, verify that the network settings are correctly configured and that you have the required share and user permissions.

## Format device

Clicking *Format* erases all information on the network share.

## Disk cleanup setting

Use this section to remove old recordings automatically. You can set it to remove recordings older than the specified number of days or weeks and/or to remove recordings starting with the oldest on the disk when a specified percentage of the disk is full.

## Recording list

Each video file on the network storage card is listed in the Recording list. The maximum file size is 60 MB per file. When the recording mode is set to "Always" (consecutive recording) and recording to network storage is also allowed to be triggered by events, the system will immediately start event recording to the network storage when an event occurs. The camera returns to the regular recording mode after event recording stops.

Using the *From/To* time boxes, users can search the recorded files in a specified time range. Two file formats - that is, \*.avi (video format) and \*.jpeg (image format), are available for selection. The following capital letters are used to indicate the recording type:

- A: Alarm
- M: Motion detection
- N: Network failure
- R: Regular (scheduled recording)
- T: Tampering
- U: Audio detection
- V: Manual trigger

Files can be removed, sorted, and downloaded.

### » To remove a file

- 1 Click on the selected file.
- 2 Press the **Remove** button.  
The file is deleted from the network storage.

### » To sort the files by name and date

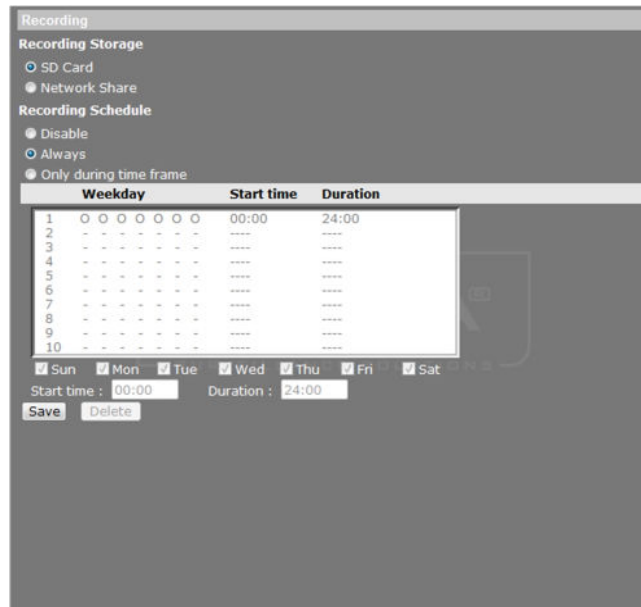
- Click **Sort**.

### » To save or view a recording file

- 1 In the Recording list, select a file.

- 2 Click **Download**.  
A window appears with a link to the file.
- 3 Click on the link to save the file locally or to play it in your default viewing software.

## 6.10 Recording



System > Recording

### Recording schedules

Administrators can configure up to 10 recording schedules that meet the surveillance requirements. Recordings are stored on the microSD/SDHC card or on a network share.

- Select **Disable** to terminate the recording function - that is, if no scheduled recording is desired.
- Select **Always** for continuous recording.

#### » To configure a recording schedule for a specific time frame

- 1 On the *System* tab, click **Recording** in the menu on the left.
- 2 Under *Recording Storage*, click **SD Card** or **Network Share**.
- 3 Select **Only during time frame**.
- 4 On the schedule overview, click on the row (1-10) representing the schedule you wish to configure.
- 5 To add days to the schedule, select the appropriate check boxes.
- 6 Specify the start time and duration of the recording.  
Duration range: 0 to 168 hours.
- 7 Click **Save**.

#### » To delete a recording schedule

- 1 On the schedule overview, select the schedule that you want to delete.
- 2 Click **Delete**.

## 6.11 Schedule

	Weekday	Start time	Duration
1	- - - - -	----	----
2	- - - - -	----	----
3	- - - - -	----	----
4	- - - - -	----	----
5	- - - - -	----	----
6	- - - - -	----	----
7	- - - - -	----	----
8	- - - - -	----	----
9	- - - - -	----	----
10	- - - - -	----	----

☐ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat

☒ Day  
☐ Night  
☒ Time

Start time : 00:00    Duration : 24:00

*System > Schedule*

On the Schedule page, Administrators can create up to ten time schedules that meet the surveillance requirements for functions, such as Motion detection, Application, and Network failure detection.

### » To create a schedule

- 1 On the *System* tab, click **Schedule** in the menu on the left.
- 2 On the schedule overview, click on the row (1-10) representing the schedule that you wish to configure.
- 3 To add days to the schedule, select the appropriate check boxes.
- 4 To specify the start time and duration of the schedule, click either **Day** or **Night**, or click **Time**, and then set the start time and duration.  
Duration range: 00:00 to 168:59
- 5 Click **Save**.

### » To delete a schedule

- 1 On the schedule overview, select the schedule that you want to delete.
- 2 Click **Delete**.

**Note:** You need to select **By Schedule** on pages such as Motion detection and Network failure detection to enable the Schedule function.

## 6.12 File location



System > File location

The HSD820 offers JPEG snapshot and MJPEG recording functionality. Users can specify a storage location for the snapshots and live video recordings. The default storage location is C:\.

**Note:** To implement the Snapshot and Recording functions, users working with Windows 7 must run Internet Explorer as administrator (right-click the IE browser icon and select "Run as Administrator").

### » To change the storage location:

- 1 Enter the new location in the *All files stored at:* box.

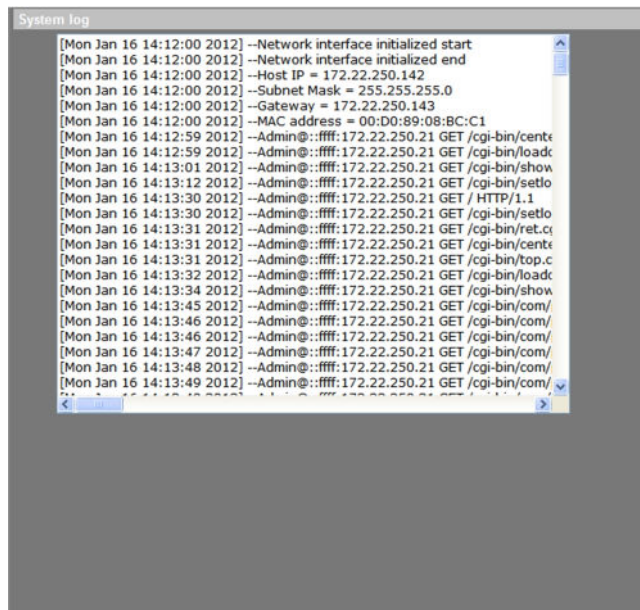
**Note:** Make sure the selected file path contains only valid characters such as letters and numbers.

- 2 Alternatively, click **Select** to browse for a location.
- 3 Once you have chosen a new location, click **Save**.  
All new snapshots and recorded video will be saved to the designated location.

## 6.13 View information

Via the *View information* option in the left-hand pane, administrators can access the camera log file, display user information, and get an overview of the camera parameters and their current values.

### 6.13.1 Log file



*System > View information > Log file*

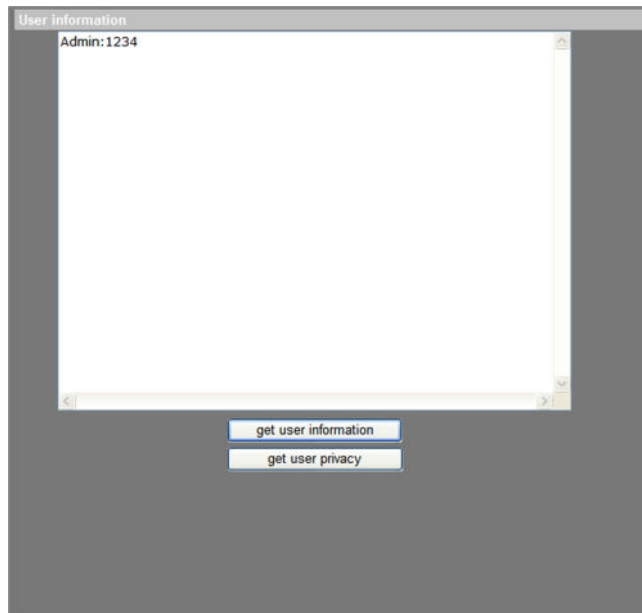
The system log provides useful information about the configuration and connections after system launch.

#### » To view the system log

- On the **System** tab, click **View information** in the menu on the left, and then click **Log file**.

The system log is displayed.

## 6.13.2 User Information



*System > View information > User information*

The Administrator can view each added user's login information and privileges. See also *User*.

### » To view the list of user accounts

- On the *System* tab, click **View information** in the menu on the left, and then click **User information**.

A list of users and their passwords displays.

"Viewer: 4321" indicates that the login name is "Viewer", and the password is "4321".

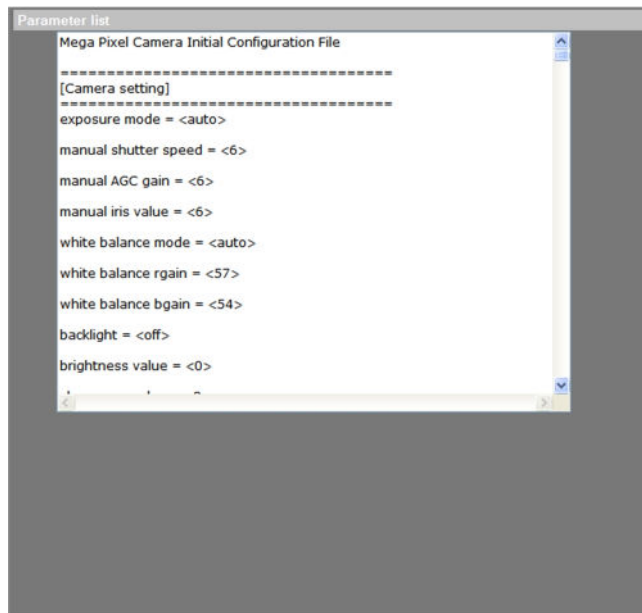
### » To view the user permissions

- 1 On the *System* tab, click **View information** in the menu on the left, and then click **User information**.
- 2 Click **Get User Privacy**.

A list of users and their privileges displays.

Each of the four numbers after every user name corresponds to one of the four permissions in the following order: I/O access, Camera control, Talk, and Listen. The number 1 indicates that a privilege is granted; the number 0 indicates that a privilege is denied. For more information, see *User*.

### 6.13.3 Parameters



*System > > View information > View parameters*

The HSD820 camera's parameters are stored in its configuration file.

» **To view the system parameters**

- On the System tab, click **View information** in the menu on the left, and then click **Parameters**.

The parameters are displayed in the browser.

**Note:** Refresh the webpage to view the most current parameter values.

## 6.14 Factory default



*System > Factory default*

The Factory default page enables administrators to reset the camera to the default factory settings.

### » To perform a full restore to the default factory settings

- 1 On the *System* tab, click **Factory default** in the menu on the left.
- 2 Click **Full Restore**.  
The system will restart in 30 seconds.

**Note:** The camera's IP address will be restored to the factory default IP address - that is, 10.x.x.x.

### » To perform a partial restore (excluding the network settings)

- 1 On the *System* tab, click **Factory default** in the menu on the left.
- 2 Click **Partial Restore**.  
The system will restart in 30 seconds.

**Note:** The camera's current network settings will not be affected by the restore.

### » To restart the system without changing its settings

- 1 Click **Reboot**.
- 2 Refresh the webpage after the system has restarted.

## 6.15 Software version

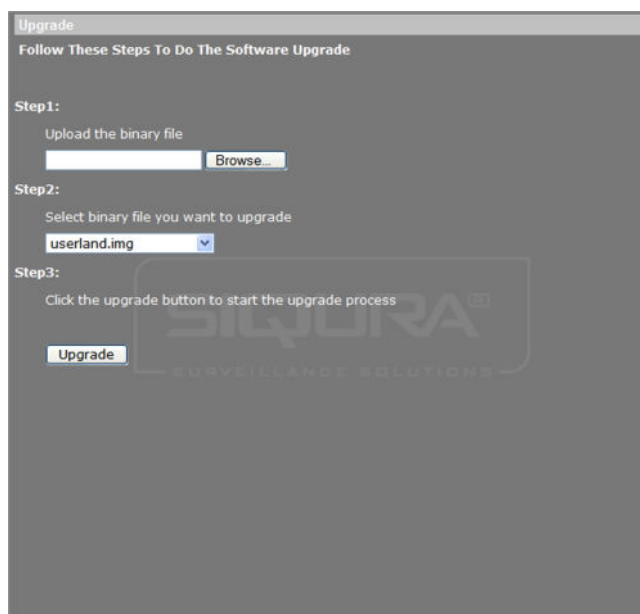


System > Software version

### » To display software version of the camera

- On the **System** tab, click **Software version** in the menu on the left.  
Version information is shown in the web browser. Note that version numbers appearing in your webpage may differ from the numbers shown in the example above.

## 6.16 Software upgrade



System > Software upgrade

Administrators can upgrade the software of the HSD820 on the Software upgrade page.

**Important:** Upgrading the software also resets the factory default settings, including the IP address. Make sure to note all settings before proceeding.

#### » To upgrade the software of your camera

- 1 Make sure that the upgrade software file is available before attempting to upgrade software.
- 2 On the *System* tab, click **Software upgrade** in the menu on the left.
- 3 Click **Browse** and select the location and binary file to be uploaded, such as `userland.img`, for example.

**Note:** Software upgrade file names must be `userland.img`. Other file upgrades should only be performed by qualified technicians. Do not change the upgrade file name, or the system will fail to find the file.

- 4 Select the file to be upgraded from the *Select binary file you want to upgrade* list.
- 5 Click **Upgrade**.  
The upgrade process starts. Progress is shown by an upgrade status bar.  
When the upgrade process is complete, the web browser returns to the home page and operation can continue.
- 6 Close your web browser.
- 7 On the Windows **Start Menu**, click **Control Panel**, and then click **Programs and Features**.
- 8 In the programs list, select **Siquira Viewer**, and then click **Remove** to uninstall the existing Siquira Viewer.
- 9 Reopen your web browser, log on to the HSD820, and then allow the automatic download and installation of Siquira Viewer.

## 6.17 Maintenance



System > Maintenance

Administrators can use this page to export configuration files (.bin) to a specified location for future use.

### » To export the configuration file

- 1 On the *System* tab, click **Maintenance** in the menu on the left.
- 2 Press **Export**.
- 3 In the *File Download* dialogue box, select **Open** or **Save**.
- 4 If saving the file, choose the local directory where it should be saved.

It is also possible to upload an existing configuration file to the camera.

### » To upload a configuration file

- 1 On the *System* tab, click **Maintenance** in the left column.
- 2 To locate the required file, click **Browse**.
- 3 When you have selected the desired file, click **Upload**.

# 7 Video and Audio Streaming

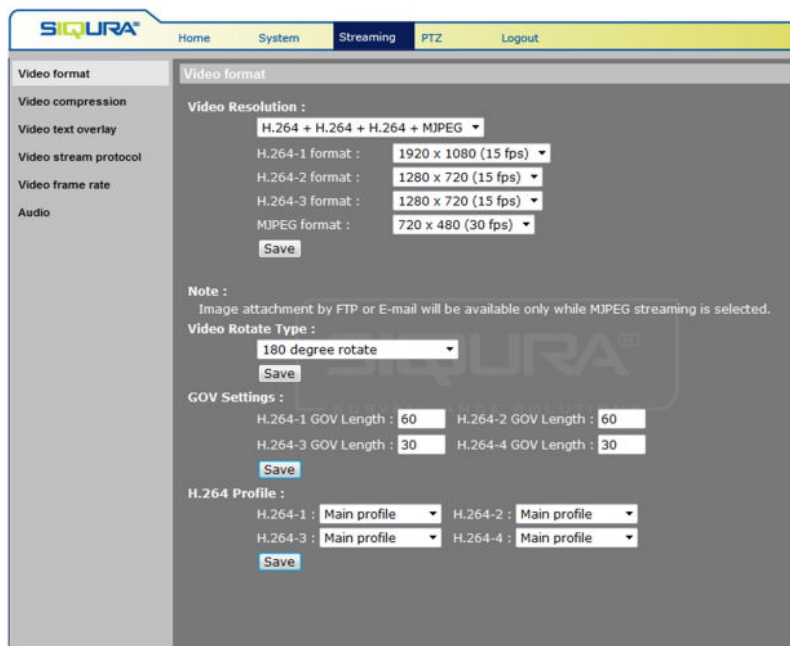
This chapter describes the Streaming tab which can be used to view and modify settings related to video format, video compression, video text overlay, video stream protocol, frame rate, and audio transmission mode.

**Note:** The Streaming tab can be accessed by administrators only.

## In This Chapter

7.1 Video format.....	69
7.2 Video compression.....	71
7.3 Video text overlay.....	72
7.4 Video stream protocol.....	74
7.5 Video frame rate.....	75
7.6 Audio.....	75

## 7.1 Video format



The screenshot shows the SIQURA web interface with the 'Streaming' tab selected. The 'Video format' sub-tab is active, displaying the following configuration options:

- Video format:** A dropdown menu showing 'H.264 + H.264 + H.264 + MJPEG'.
- Video Resolution:** Four dropdown menus for different H.264 formats:
  - H.264-1 format: 1920 x 1080 (15 fps)
  - H.264-2 format: 1280 x 720 (15 fps)
  - H.264-3 format: 1280 x 720 (15 fps)
  - MJPEG format: 720 x 480 (30 fps)
- Save:** A button to save the resolution settings.
- Note:** A text box stating 'Image attachment by FTP or E-mail will be available only while MJPEG streaming is selected.'
- Video Rotate Type:** A dropdown menu showing '180 degree rotate'.
- Save:** A button to save the rotate type settings.
- GOV Settings:** Four input fields for GOV Length:
  - H.264-1 GOV Length: 60
  - H.264-2 GOV Length: 60
  - H.264-3 GOV Length: 30
  - H.264-4 GOV Length: 30
- Save:** A button to save the GOV settings.
- H.264 Profile:** Four dropdown menus for H.264 profiles:
  - H.264-1: Main profile
  - H.264-2: Main profile
  - H.264-3: Main profile
  - H.264-4: Main profile
- Save:** A button to save the profile settings.

Streaming > Video format

On the Video format page, users can select the video resolution settings, and configure image orientation, GOV, and H.264 profile settings.

### 7.1.1 Video resolution

The HSD820 series cameras have quad-stream capability for simultaneous streaming of H.264/H.264 or H.264/MJPEG. Full HD 1080p streaming with a D1 second stream or dual 720p streaming is possible.

#### » To set up the video resolution for the HSD820

- 1 On the *Streaming* tab, click **Video format** in the menu on the left.
- 2 On the **Video Resolution** list, select a streaming format combination.
- 3 In the video format list(s), select the preferred resolution setting(s).
- 4 Click **Save** to confirm the setting.

**Note:** Image attachment by FTP or e-mail is available only when MJPEG streaming is selected.

### 7.1.2 Video rotate type

A camera can be oriented in a variety of ways for different applications.

#### » To select a video rotation type

- 1 On the *Streaming* tab, click **Video format** in the menu on the left.
- 2 Choose one of the following video rotation types:
  - **Normal video.** The camera's orientation is not modified.
  - **Flip video.** The image rotates across the horizontal axis.
  - **Mirror video.** The image rotates across the vertical axis.
  - **90 degree clockwise.** The image rotates 90° clockwise.
  - **180 degree rotate.** The image rotates 180°.
  - **90 degree counterclockwise.** The image rotates 90° counterclockwise.
- 3 Click **Save** to confirm settings.

### 7.1.3 GOV Settings

To save bandwidth, users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream. Less bandwidth is needed if the GOV length is set to a high value. However, the shorter the GOV length the better the video quality is.

#### » To configure the GOV settings

- 1 On the *Streaming* tab, click **Video format** in the menu on the left.
- 2 In the *GOV Settings* section, type the values in the GOV Length boxes.

Range: 2 to 64.

The default value for H.264-1 / H.264-2 / H.264-3 / H.264-4 is 60 / 60 / 30 / 30 (NTSC) or 50 / 50 / 25 / 25 (PAL).
- 3 Click **Save** to confirm the GOV setting.

### 7.1.4 H.264 Profile

Users can set each H.264 profile to Baseline Profile, Main Profile, or High Profile according to the compression needs. The default setting is Main Profile.

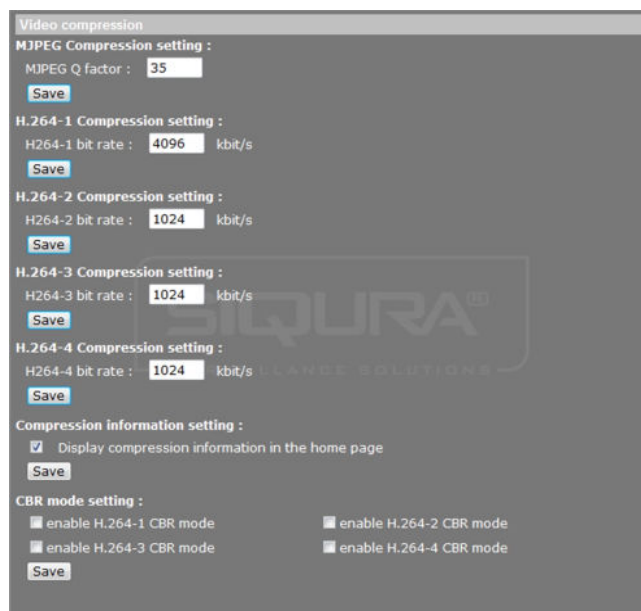
#### » To set an H.264 profile

- 1 On the *Streaming* tab, click **Video format** in the menu on the left.
- 2 In the **H.264-x** list, select the desired profile.

**Note:** Make sure that the profile you select is supported by the system.

- 3 Click **Save**.

## 7.2 Video compression



*Streaming > Video compression*

Administrators can select the appropriate video compression mode for an application on the Video compression page.

#### » To change MJPEG compression settings

- 1 On the *Streaming* tab, click **Video compression** in the menu on the left.
- 2 Set a value for the *MPEG Q factor* parameter.  
Range: [1...70]. Default setting: 35. Higher values give higher image quality. They require higher bit rates, though, and therefore consume more bandwidth.
- 3 Click **Save** to confirm settings.

#### » To change H.264 compression settings

- 1 On the *Streaming* tab, click **Video compression** in the menu on the left.
- 2 Set values for the bit rates for each H.264 video stream.  
Range H.264-1: [64...8192] kbps. Default: 4096 kbps.

Range H.264-2: [64...2048] kbps. Default: 1024 kbps.

Range H.264-3: [64...2048] kbps. Default: 1024 kbps.

Range H.264-4: [64...2048] kbps. Default: 1024 kbps.

- 3 Click **Save** to confirm settings.

#### » To display compression information on the home page

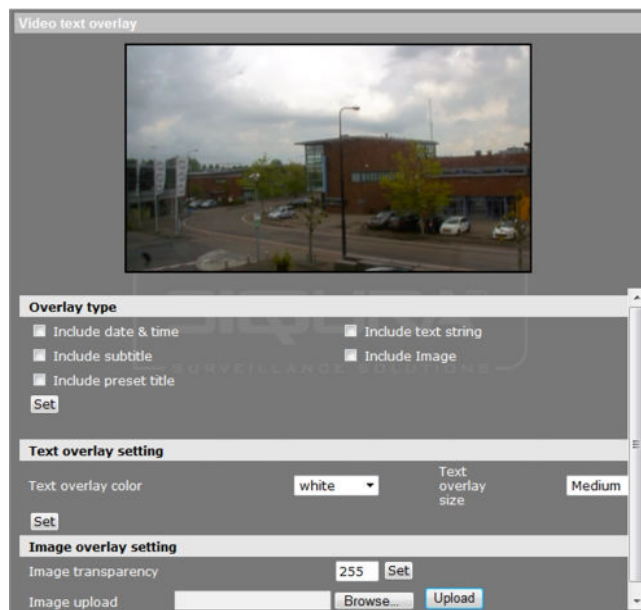
- 1 On the *Streaming* tab, click **Video compression** in the menu on the left.
- 2 Select the **Display compression information in the home page** check box.
- 3 Click **Save** to confirm settings.

#### » To enable constant bit rate (CBR) mode

Constant bit rate (CBR) mode may be preferred if the available bandwidth is limited. It is important to take the image quality into account when choosing a CBR mode.

- 1 On the *Streaming* tab, click **Video Compression** in the menu on the left.
- 2 Click to select CBR mode for the applicable H.264 video stream(s).
- 3 Click **Save**.

## 7.3 Video text overlay



*Streaming > Video text overlay*

The HSD820 features programmable on-screen display (OSD) facilities. Date and time information, a subtitle, the name of the current preset, a text string, and an image (such as a logo) can be displayed as overlays over the camera images.

#### » To add a text overlay

- 1 On the *Streaming* tab, click **Video text overlay** in the menu on the left.
- 2 Click to select the overlay type(s) you wish to add.  
*Include date & time:* available options are 'date', 'time', or 'date & time'.  
*Include subtitle:* up to three text boxes can be used.

*Include preset title:* adds the name of the current camera preset.

*Include text string:* type the text you wish to add.

- 3 Align the text(s) as necessary and drag the text box(es) to the desired position on the preview.
- 4 Click **Set**.
- 5 In the **Text overlay color** list, select a font colour.
- 6 In the **Text overlay size** list, set the text size to small, medium or large.
- 7 Click **Set**.

#### » To add an image overlay

- 1 On the *Streaming* tab, click **Video text overlay** in the menu on the left.
- 2 In the *Overlay type* section, click **Include Image**.
- 3 Drag the image box to the desired position on the preview.
- 4 Under *Image overlay setting*, click **Browse**.
- 5 Locate and select an image that meets the following requirements:
  - Format: 8-bit .bmp
  - Width: a multiple of 32 pixels
  - Height: a multiple of 4 pixels
- 6 Click **Upload**.
- 7 Type a value in the *Image transparency* box.  
Range: 0 - 255.
- 8 Click **Set**.



Camera view with three overlays: Image overlay (top left), Date & time (bottom left), and Preset title (bottom right)

## 7.4 Video stream protocol

*Streaming > Video stream protocol*

On the Video Stream Protocol page, users can select a protocol for streaming media over the network to the webpages via the Siqura Viewer application.

**Note:** The protocols on this page only apply to streams going to a Siqura Viewer.

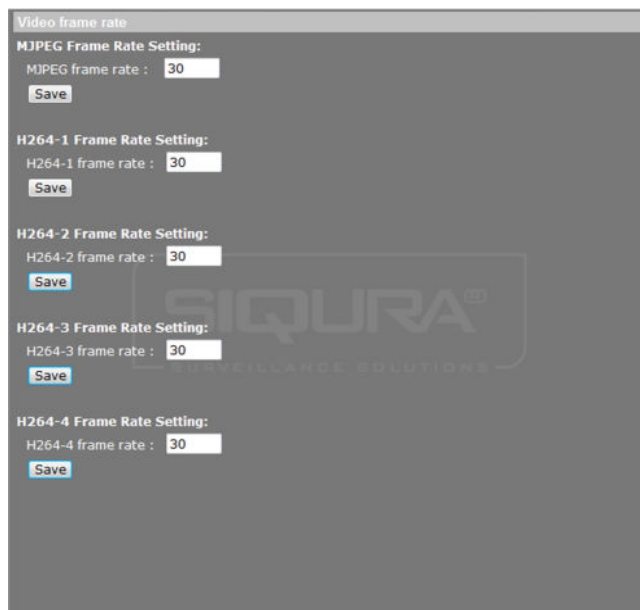
Protocol	Description
RTP over UDP	Real-Time Transport Protocol, using UDP transport, lessens network delay and is required for two-way audio streams.
RTP over RTSP (TCP)	Real-Time Transport Protocol, using TCP transport, guarantees that data is delivered and that no packets are dropped, but some network delay may occur.
RTSP over HTTP	A standard solution to help RTSP work through firewalls and Web proxies, so that viewers behind a firewall can access RTSP streams.
MJPEG over HTTP	Consecutive JPEG images are sent individually over HTTP.
Multicast mode	Multicast streaming reduces bandwidth usage for streams being transmitted to multiple clients.

### » To set a video stream protocol

- 1 On the *Streaming* tab, click **Video stream protocol** in the menu on the left.
- 2 Select a streaming protocol.  
To use Multicast mode, you must also supply the Multicast IP address and the appropriate video and audio ports. In the Multicast TTL text box, specify the number of routers (hops) that multicast traffic is permitted to pass before expiring on the network
- 3 Click **Save**.

**Note:** Only RTP over UDP supports two-way audio.

## 7.5 Video frame rate

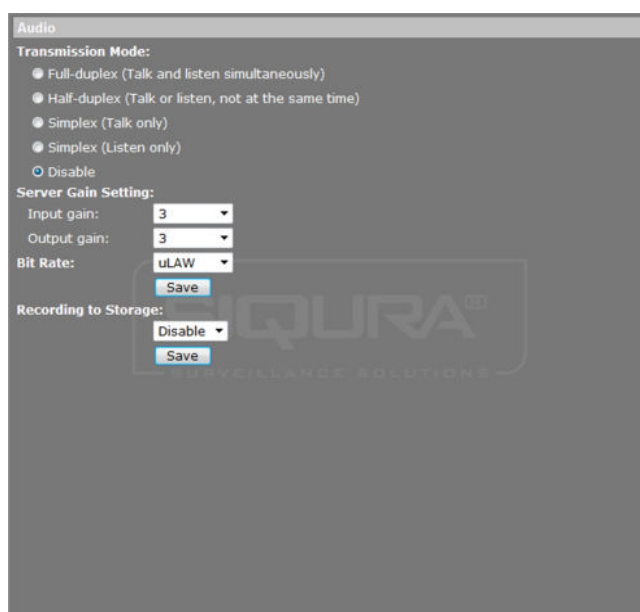


*Streaming > Video frame rate*

On the Video frame rate page, the administrator can set the MJPEG, H.264-1, H.264-2, H.264-3, and H.264-4 frame rate - that is, the number of frames per second. The default frame rate is 30 fps. The setting range is from 1 to 30 fps. After setting a value, click **Save** to confirm your setting.

**Note:** Lower frame rates will decrease video smoothness.

## 7.6 Audio



*Streaming > Audio*

On the Audio page, administrators can select the transmission mode and bit rate for audio streams.

#### » To configure audio settings

- 1 On the *Streaming* tab, click **Audio** in the menu on the left.
- 2 Under *Transmission Mode*, click to select one of the following options:
  - **Full-duplex** – Audio can be transmitted and received at the same time, so local and remote sites can communicate with each other simultaneously.
  - **Half-duplex** – Audio can be either transmitted or received, so one site can talk or listen to the other site in turn.
  - **Simplex (Talk only)** – Audio can be transmitted, so one site can speak to the other site.
  - **Simplex (Listen only)** – Audio can be received, so one site can listen to the other site.
  - **Disable** – The audio transmission function is turned off.
- 3 Under *Server Gain Setting*, select audio input/output gain levels for sound amplification. The audio input gain value is adjustable from 1 to 10. The audio output gain value is adjustable from 1 to 6. Set the audio gain to **Mute** to turn off the sound.
- 4 On the *Bit Rate* list, select the audio transmission bit rate. Audio transmission bit rates include the following options:
  - 16 kbps (G.726)
  - 24 kbps (G.726)
  - 32 kbps (G.726)
  - 40 kbps (G.726)
  - $\mu$ -LAW (64 kbps) (G.711)
  - A-LAW (64 kbps) (G.711)Both  $\mu$ -LAW and A-LAW use 64 kbps. However,  $\mu$ -LAW and A-LAW use different compression formats. While higher bit rates allow for better audio quality, they also require more bandwidth.
- 5 Click **Save**.

#### » To enable audio recording

- 1 On the *Streaming* tab, click **Audio** in the menu on the left.
- 2 Click to open the list under *Recording to Storage*, and then click **Enable**.
- 3 Click **Save**.

**Note:** If the chosen bit rate is not compatible with the player, there will only be noise instead of audio during playback.

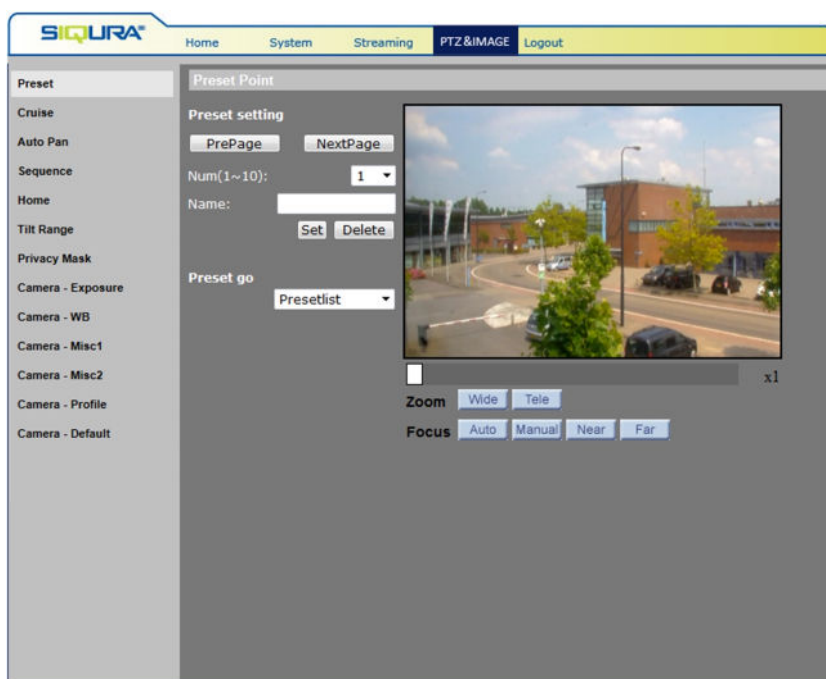
## 8 PTZ&IMAGE

From the PTZ&IMAGE tab, users can view a live video stream, control the PTZ functions, and configure camera parameters.

### In This Chapter

8.1 Preset.....	77
8.2 Cruise.....	79
8.3 Autopan.....	80
8.4 Sequence.....	81
8.5 Home.....	83
8.6 Tilt Range.....	84
8.7 Privacy Mask.....	85
8.8 Camera - Exposure.....	86
8.9 Camera - WB.....	87
8.10 Camera - Misc 1.....	89
8.11 Camera - Misc 2.....	90
8.12 Camera - Profile.....	92
8.13 Camera - Default.....	93

## 8.1 Preset



PTZ > Preset

HSD820 cameras support 256 preset points.

» **To set a preset point**

- 1 On the *PTZ&IMAGE* tab, click **Preset** in the menu on the left.
- 2 Position the pointer on the live view pane.
- 3 Keeping the left mouse button pressed, move the camera to the desired view by dragging the (red) pointer.
- 4 Using the buttons under the live view pane, adjust the fine zoom/focus ratio.
- 5 Click to open the **Num** list, and then assign a number to the current camera position. Numbers 1-256 are accessed with the PrePage and NextPage buttons.
- 6 In the *Name* text box, enter a descriptive name.
- 7 To save these settings, click **Set**.

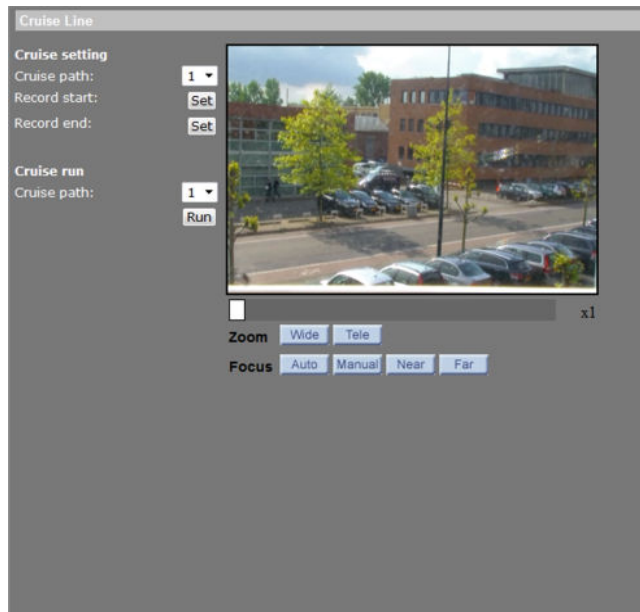
» **To move the camera to a specified preset point**

- 1 On the *PTZ&IMAGE* tab, click **Preset** in the menu on the left.
- 2 Under *Preset go*, click to open the **Presetlist**. Numbers 1-256 are accessed with the PrePage and NextPage buttons.
- 3 Select the desired preset point. The camera moves to the target position.

» **To delete a preset point**

- 1 On the *PTZ&IMAGE* tab, click **Preset** in the menu on the left.
- 2 Under *Preset setting*, click to open the **Num** list. Numbers 1-256 are accessed with the PrePage and NextPage buttons.
- 3 Select the preset point you wish to delete.
- 4 Click **Delete**.

## 8.2 Cruise



PTZ > Cruise

A cruise is a route formed with manual operation (through adjusting the pan and tilt position), which can be stored and recalled to execute repeatedly. The HSD820 series cameras support up to eight programmable cruise paths.

### » To record a cruise path

- 1 On the *PTZ&IMAGE* tab, click **Cruise** in the menu on the left.
- 2 Under *Cruise setting*, select a path number on the **Cruise path** list.

**Note:** An existing recording stored under the selected path number will be overwritten with the new recording.

- 3 Position the pointer on the live view pane.
- 4 Keeping the left mouse button pressed, drag the (red) pointer across the live view to move the camera to the starting point of the cruise path.
- 5 Click the **Set** button of *Record start*.
- 6 Pan, tilt, and zoom the camera to program the cruise path.
- 7 When finished, click the **Set** button of *Record end*.

### » To execute a defined cruise

- 1 On the *PTZ&IMAGE* tab, click **Cruise** in the menu on the left.
- 2 Under *Cruise run*, select the desired cruise from the **Cruise path** list.
- 3 Press **Run**.

The camera starts panning/tilting/zooming as recorded.

To view the cruise in full-screen mode, right-click the live view pane, and then select **fullscreen**.

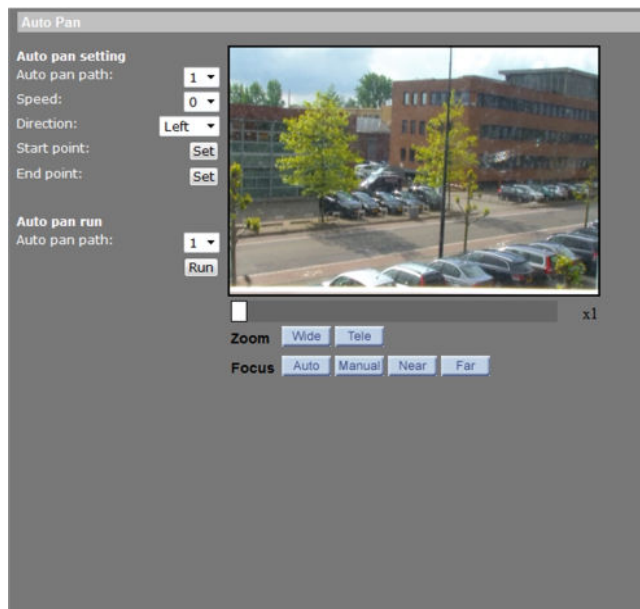
The cruise is repeated at ten-second intervals.

### » To stop running a cruise

- Drag the (red) mouse pointer across the live view pane in any direction.

The current cruise stops and is no longer repeated.

## 8.3 Autopan



*PTZ > Autopan*

Autopan is the motion of scanning an area horizontally so the dome camera captures a horizontal view. The HSD820 series cameras support up to four programmable autopan paths.

### » To record an autopan path

- 1 On the *PTZ&IMAGE* tab, click **Autopan** in the menu on the left.
- 2 Under *Autopan setting*, select a path number on the **Autopan path** list.

**Note:** An existing recording stored under the selected path number will be overwritten with the new recording.

- 3 Select a pan speed from the **Speed** list.
- 4 From the *Direction* list, select a direction for the autopan. For more information, see below.
- 5 Position the pointer on the live view pane.
- 6 Keeping the left mouse button pressed, drag the (red) pointer across the live view to move the camera to the starting point of the autopan path.
- 7 Click the **Set** button of *Start point*.

**Note:** The zoom ratio of an autopan start point will persist throughout the entire path.

- 8 Move the camera to the desired end point of the autopan.
- 9 Click the **Set** button of *End point*.

### » To execute a defined autopan path

- 1 On the *PTZ&IMAGE* tab, click **Autopan** in the menu on the left.
- 2 Under *Autopan run*, select the desired autopan path from the **Autopan path** list.
- 3 Press **Run**.

The camera starts moving horizontally as recorded.

To view the autopan path in full-screen mode, right-click the live view pane, and then select **fullscreen**.

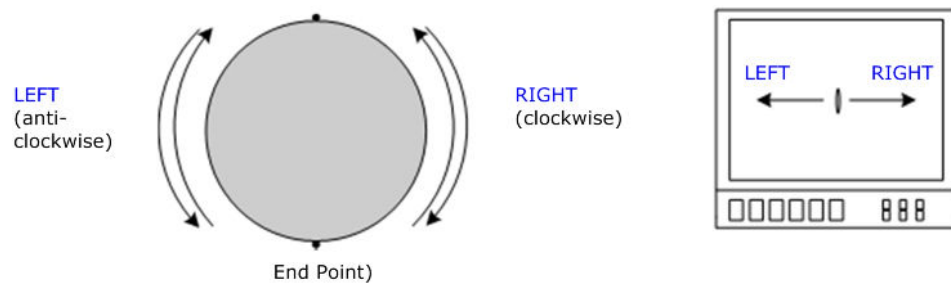
The autopan path is repeated at ten-second intervals.

#### » To stop running an autopan path

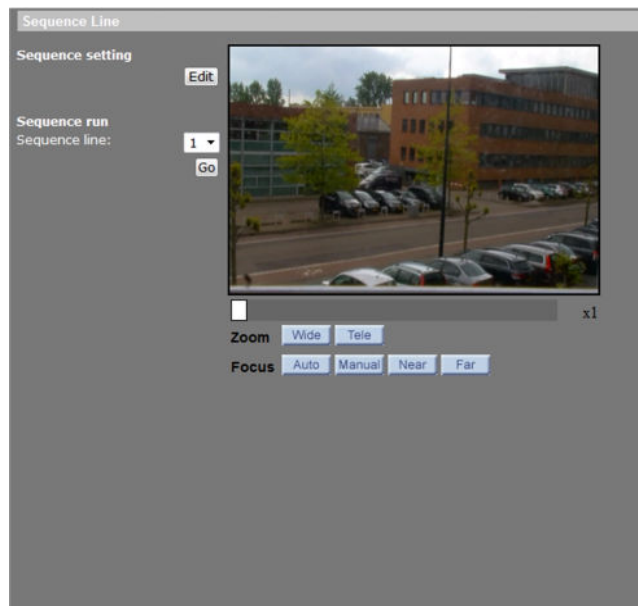
- Drag the (red) mouse pointer across the live view pane in any direction.  
The current autopan path stops and is no longer repeated.

#### Direction

Use this item to set the autopan direction of the dome camera. The dome will start to pan clockwise from the start point to the end point if your selection is RIGHT, and then return to the start point. The dome will start to pan counterclockwise from the start point to the end point if your selection is LEFT, as shown below.



## 8.4 Sequence



PTZ > Sequence

The sequence function executes prepositioning of the pan, tilt, zoom, and focus features in a certain sequence for a camera. The HSD820 series cameras support up to eight sequence lines. Up to 64 points can be specified for each sequence line.

**Note:** Before setting this function, users must set at least two preset points.

» **To program a sequence line**

- 1 On the *PTZ&IMAGE* tab, click **Sequence** in the menu on the left.
- 2 Under *Sequence setting*, click **Edit**.
- 3 Click to open the **Sequence line** list on the *Sequence Set* page, and then select the number of the line (1-8) you wish to program.
- 4 Set up each sequence point in the desired order by assigning a preset from the *Name* list, and specifying a dwell time (0-255) and speed (0-14) in the corresponding text boxes.  
For more information on dwell times, see below.  
Sequence points 1-64 can be accessed through the Pre page and Next page buttons.
- 5 Click **Save**.

» **To execute a defined sequence**

- 1 On the *PTZ&IMAGE* tab, click **Sequence** in the menu on the left.
- 2 Under *Sequence run*, select the number of the sequence line to be run from the **Sequence line** list.
- 3 Press **Go**.  
The camera starts moving from preset to preset sequentially as programmed.  
To view the cruise in full-screen mode, right-click the live view pane, and then select **fullscreen**.  
The sequence is continuously repeated.

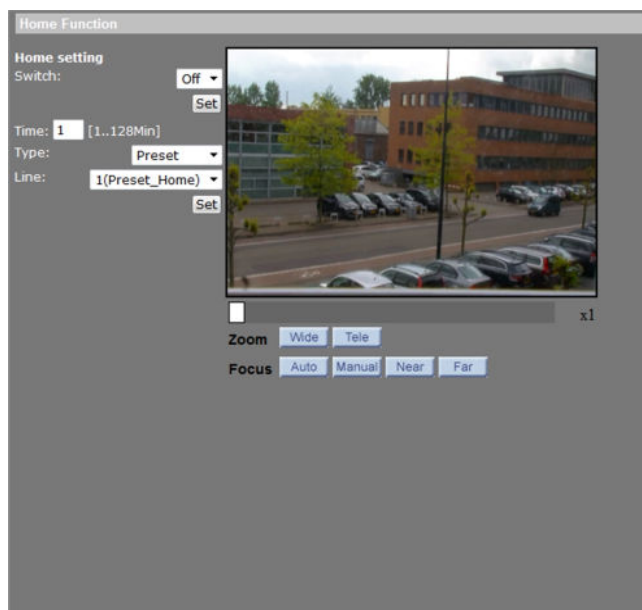
» **To stop running a sequence**

- Drag the (red) mouse pointer across the live view pane in any direction.  
The current sequence stops and is no longer repeated.

**Dwell time**

The dwell time is the duration time the dome remains at a sequence point. The range is from 0 to 255 seconds. The dome will go to the next sequence point when the dwell time expires.

## 8.5 Home



PTZ > Home

Users are able to set an operation mode to ensure constant monitoring; if the dome idles for a period of time, the preset function is activated automatically; this is the HOME function. The HOME function allows constant and accurate monitoring to avoid the dome stopping or missing events.

### » To activate/deactivate the Home function

- 1 On the *PTZ&IMAGE* tab, click **Home** in the menu on the left.
- 2 Under *Home setting*, click to open the **Switch** list, and then select **On** or **Off** to activate/deactivate the HOME function, respectively.

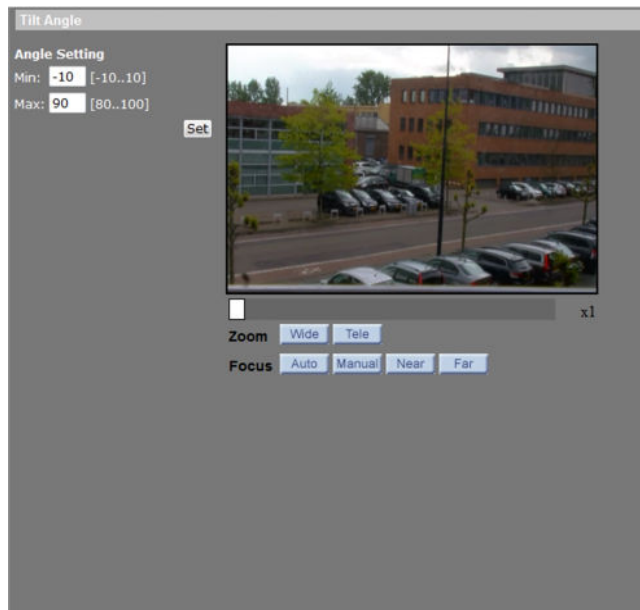
### » To configure the Home function

- 1 On the *PTZ&IMAGE* tab, click **Home** in the menu on the left.
- 2 In the *Time* box, enter the camera idle time (see below); range [1-128] minutes.
- 3 From the *Type* and *Line* lists, select the function and line number to be executed when camera idle time expires.
- 4 Click **Set**.

### Time

The time entered in the *Time* box represents the duration of camera idle time (1-128 minutes) that you want to elapse before running a Preset point, Sequence line, Autopan path, or Cruise line. With the Home function activated, the camera starts to count down when it idles, and then executes the predefined action when the time expires.

## 8.6 Tilt Range



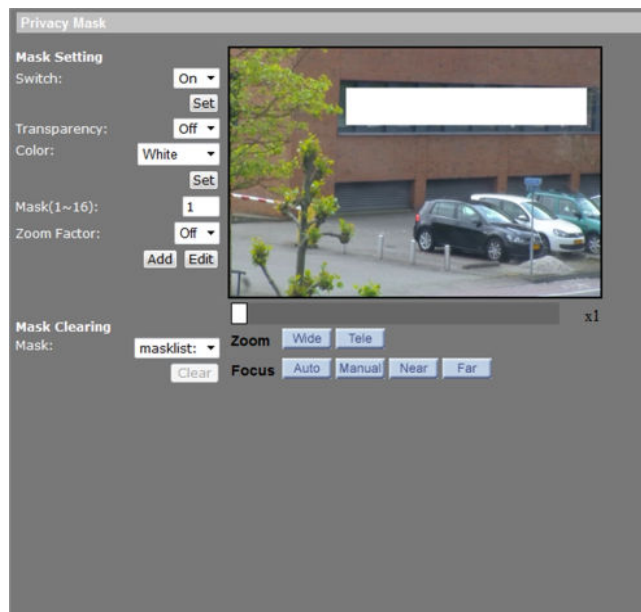
*PTZ > Tilt Range*

The tilt range of the HSD820 cameras is adjustable from minimum  $-10^{\circ}$  to maximum  $100^{\circ}$ .

### » To adjust the angle setting

- 1 On the *PTZ&IMAGE* tab, click **Tilt Range** in the menu on the left.
- 2 Enter the desired minimum and maximum tilt angle in the corresponding text boxes.
- 3 Click **Set**.

## 8.7 Privacy Mask



PTZ > Privacy Mask

The Privacy Mask function aims to avoid any intrusive monitoring. The HSD820 supports up to 16 privacy masks.

### » To set a privacy mask

- 1 On the *PTZ&IMAGE* tab, click **Privacy Mask** in the menu on the left.
- 2 Under *Mask Setting*, click to open the **Switch** list, select **On**, and then click **Set**.
- 3 Set the *Transparency* of the mask to **On** or **Off**, as desired.
- 4 Select the colour of the mask from the *Color* list, and then click **Set**.
- 5 In the *Mask (1~16)* text box, assign a number to the mask.
- 6 Set the *Zoom Factor* to **On** or **Off**, as desired.  
If you select *On* the mask is not displayed when the zoom factor is smaller than the current zoom factor.
- 7 Click **Add**.
- 8 Drag the red box to position the mask on the camera view as desired.
- 9 Drag the borders of the box to resize the mask as desired.  
It is recommended to set the mask to twice the size of the object to be masked.
- 10 Click **Set**.

### » To edit a privacy mask

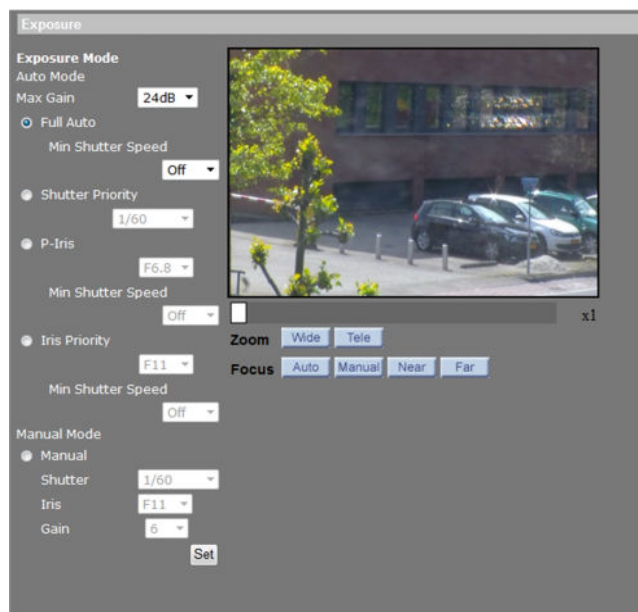
- 1 On the *PTZ* tab, click **Privacy Mask** in the menu on the left.
- 2 In the *Mask (1-16)* text box, enter the number of the mask you wish to edit, and then click **Edit**.  
The camera adopts the position and angle used when the mask was set initially.

- 3 Make the required changes as described above.
- 4 Click **Set**.

#### » To remove a mask

- 1 On the *PTZ* tab, click **Privacy Mask** in the menu on the left.
- 2 Under *Mask Clearing*, click to open the **Mask** list.
- 3 Select the number of the mask to be removed.
- 4 Click **Clear**.

## 8.8 Camera - Exposure



PTZ > Camera - Exposure

Exposure is the amount of light received by the image sensor. It is determined by the width of the lens diaphragm opening, the shutter speed and other exposure parameters. On the Exposure page, users can select one of the exposure modes for optimised video output in accordance with the operating environment.

### Max Gain

Here, you can select an appropriate, maximum level for automatic gain control (AGC) or set this to 'off'.

### Full Auto

In this mode, the camera's shutter speed, iris, and gain control circuits work together to provide consistent video output.

### Shutter Priority

In this mode, it is the shutter speed that takes main control of exposure.

### P-Iris

In this mode, users can manually adjust the iris size and minimum shutter speed.

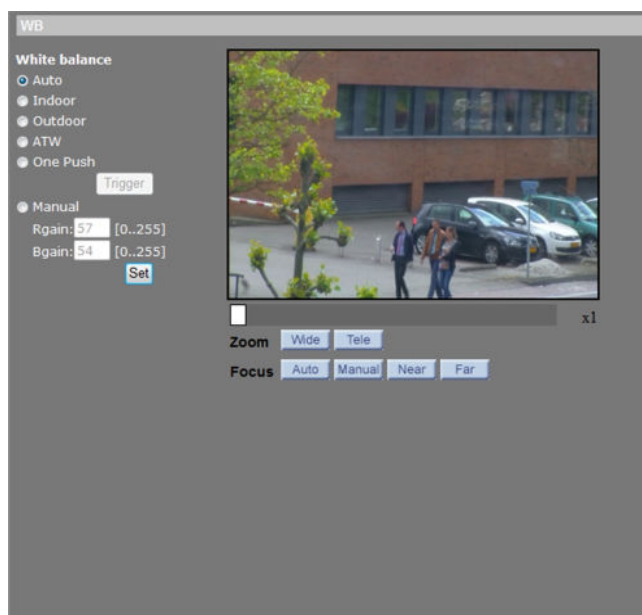
## Iris Priority

In this mode, the iris opening has the highest priority in exposure control. The lower the number, the more light is let into the lens.

## Manual

In this mode, the shutter speed, iris opening, and gain settings can be specified manually.

## 8.9 Camera - WB



PTZ > Camera - WB

## Colour temperature

A camera needs to measure the quality of a light source and create a reference colour temperature in order to calculate all the other colours. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance control modes, according to the operating environment. The table below gives the colour temperatures of some light sources as a general reference.

Light source	Colour temperature in °K
Cloudy sky	6000 to 8000
Noon sun and clear sky	6500
Household lighting	2500 to 3000
75 W bulb	2820
Candle flame	1200 to 1500

## Auto

The camera detects a colour temperature range and calculates an optimal white balance. The Auto White Balance mode is suitable for light sources with colour temperature ranges from 2700 to 7800 K.

## Indoor/Outdoor

The white balance is adjusted to a colour temperature range for either indoor or outdoor lighting conditions.

### ATW

In Auto Tracing White Balance (ATW) mode, the camera takes out the signals in a screen in the range from 2500 K to 10000 K. It continuously adjusts the camera colour balance to changes in the colour temperature which may occur, for example, when moving from an indoor scene to an outdoor scene.

### One Push

With the One Push function, white balance is adjusted and fixed according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. The function is suitable for light sources with any kind of colour temperature.

#### » To set the white balance using One Push

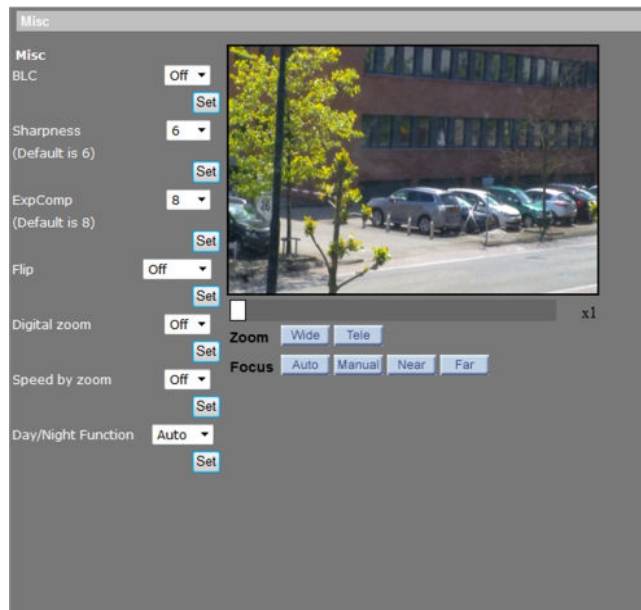
- 1 Point the camera at the area to be monitored.
- 2 Under *White balance*, click **One Push**.
- 3 Click **Set**.
- 4 Click **Trigger** to adjust the white balance.

**Note:** In this mode, the value of white balance will not change as the scene or the light source varies. Therefore, users may have to re-adjust the white balance by pushing the Trigger button again when needed.

### Manual

In this mode, users can change the white balance value manually by adjusting the Rgain and Bgain. Rgain/Bgain values range from 0 to 255.

## 8.10 Camera - Misc 1



PTZ > Cam - Misc1

On the Camera - Miscellaneous Setups Menu 1 (Misc1) page, users can set various camera parameters including Backlight Compensation, Sharpness, Exposure Compensation, Image Flip, Digital Zoom, Speed by Zoom, and Day/Night.

### BLC

Backlight Compensation (BLC) enhances the visibility of objects in the foreground of an image when there is a bright light in the background.

### Sharpness

The sharpness value describes the clarity of detail perceived in an image. A higher sharpness value implies a clearer image. A lower sharpness value implies a more obscure image. The sharpness value is adjustable from 1 to 15.

### ExpComp

Exposure Compensation (ExpComp) allows the user to adjust the exposure to compensate for unusual or problematic lighting conditions that could result in less-than-optimal images. The function can also be used to create intentional underexposure or overexposure. ExpComp values range from 1 to 15.

### Flip

Users can track an object continuously as it passes under the dome camera by setting Flip to Mechanical (M.E.) mode.

**Note:** Flip setting is controlled manually only. If a Preset Position or a point for an other function such as Sequence, is set to a position that can only be reached through FLIP motion, that position cannot be reached anymore when the Flip function is turned off.

M.E. mode is a standard mechanical operation. As the dome camera tilts to the maximum angle, it will pan 180°, and then continue tilting to keep tracking objects.

**Note:** To make the dome camera tilt between a specific range, such as  $-10^{\circ}$  to  $+100^{\circ}$  or  $-10^{\circ} \sim +190^{\circ}$ , go to the *Tilt Range* page to set the tilt angle range. Otherwise, the dome camera will tilt  $90^{\circ}$  as the default setting.

### Digital zoom

With digital zoom set to *On*, it is possible to zoom in further on the video when the lens is fully zoomed in using optical zoom.

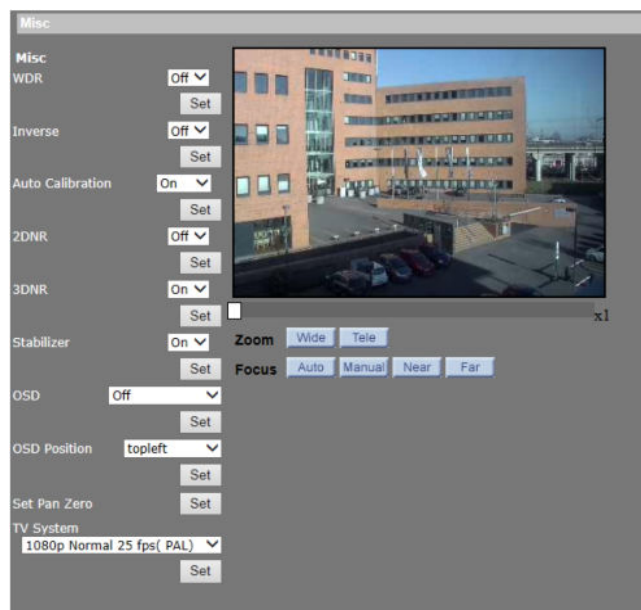
### Speed by zoom

When enabled, the pan/tilt speed is adjusted by an internal algorithm when zooming automatically. The larger the zoom ratio, the lower the rotation speed.

### Day/Night function

When the Day/Night function is set to *Night*, the camera removes the IR-cut filter and switches to monochrome for clearer images in low-light conditions. When set to *Day*, the filter is returned and the image is in colour. In *Auto* mode, the camera detects the lighting conditions and switches the filter accordingly.

## 8.11 Camera - Misc 2



PTZ > Camera - Misc2

On the Camera - Miscellaneous Setups Menu 2 (Misc2) page, users can set various camera parameters.

### WDR

To enhance video display, the wide dynamic range (WDR) function solves high contrast or changing light issues by taking the best of two pictures with different exposure settings. WDR is especially effective in solving indoor and outdoor contrast issues. The user can enable or disable the WDR function, according to the application.

### Inverse

With the Inverse function, the video in the camera preview can be rotated  $180^{\circ}$ .

## Autocalibration

There is one horizontal and one vertical infrared ray check point in each dome. When the dome camera's position is moved during installation or maintenance, the relative distance between the original set point and the check point may change. When enabled, the autocalibration function automatically detects this change and resets the point back to the original position.

## 2DNR

With the 2D Noise Reduction function, the processor analyses pixel by pixel and frame by frame to eliminate environmental noise signal so that a high quality image can be produced even in low light conditions.

## 3DNR

In addition to 2D Noise Reduction, the HSD820H3 also includes 3DNR which generates enhanced noise reduction.

## Stabilizer

The HSD820H3 has a built-in image stabiliser to prevent vibrations from disrupting a camera view or footage, such as those caused by wind in pole-mount installations. Enable this function to provide stable pictures even at the highest zoom ratio.

## OSD and Set Pan Zero

The camera's direction, azimuth, and elevation can be displayed on screen. To use this feature, you must first align the camera to the north and assign the pan zero position to the camera.

### » To set pan zero

- 1 Using a compass and PTZ camera control, pan the camera until it faces straight north.
- 2 To activate Set Pan Zero, click **Set**.

### » To display the current camera position on screen

- 1 Click to open the OSD list.
- 2 Click **On**.
- 3 Click **Set**.

The camera position is displayed as "N 000/##". The measurement after the slash indicates the elevation. The OSD is continuously updated as you move the camera.

Selecting the *Compass Only* option displays the camera direction and hides the azimuth and elevation.

### » To position the OSD overlay on your screen

- 1 Click to open the OSD Position list.
- 2 Click the required position.

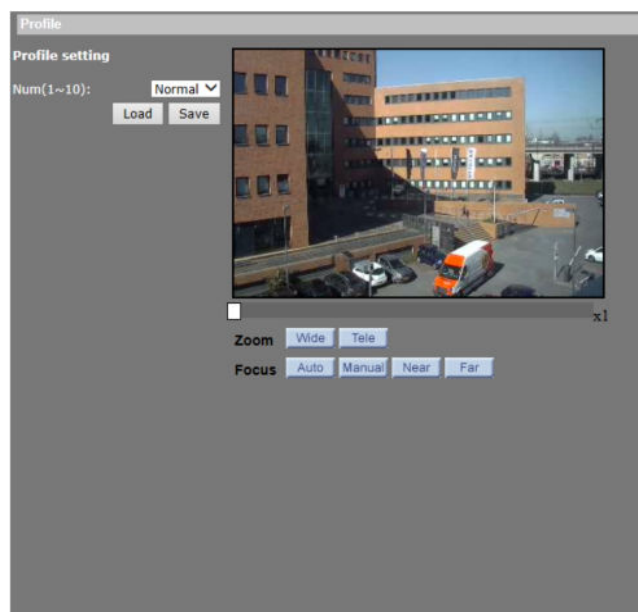
## TV System

Select the video format that matches the TV system (either NTSC or PAL) associated with the camera.

### » To select the camera's TV system

- 1 For systems using the National Television System Committee standard, select one of the NTSC options. For those using the Phase Alternate Line system, select a PAL option.
- 2 Click **SET** to confirm the new setting.

## 8.12 Camera - Profile



PTZ > Camera - Profile

Combinations of camera settings, such as those made on the Exposure, WB, Misc1, and Misc2 pages, can be stored as profiles which can be used for specific scenarios with different time schedules. You can set up and store up to 10 sets of camera parameter configurations. Schedules to be used must be set up in advance on the Schedule page.

### » To create a profile

- 1 Configure the various camera settings as needed.
- 2 Open the **Profile** section.
- 3 Click the **Num** list, and then select a number for the profile.
- 4 Type the profile name in the *Name* box.
- 5 Click **Save**.
- 6 To link the profile to a schedule you have configured on the *Schedule* page, select **By schedule**.
- 7 Click the **Schedule** box, and then select a schedule.

Multiple schedules can be selected.

- 8 Click **Save**.

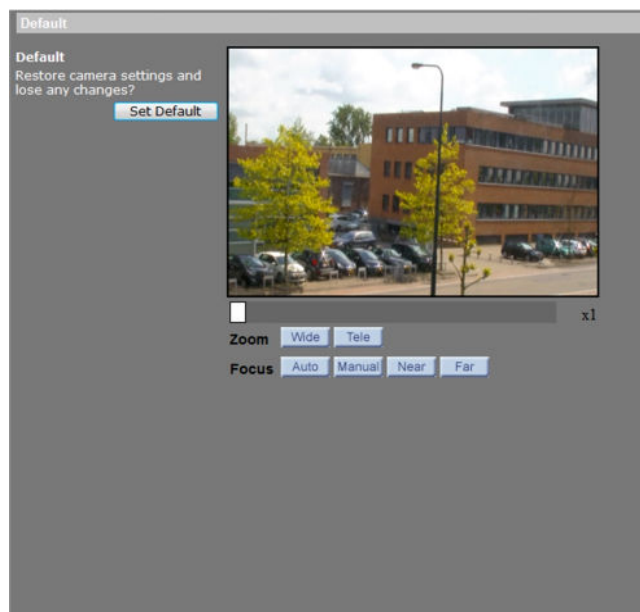
#### » To activate a profile

- 1 On the *Camera - Profile* page, click to open the **Num** list.
- 2 Select the required profile number.  
The profile name is displayed in the Name box.
- 3 Click **Load**.  
The profile takes a while to load.  
The camera adopts the settings associated with the profile.

#### » To delete a profile

- 1 On the *Camera - Profile* page, click to open the **Num** list.
- 2 In the **Num** list, select the profile to be deleted.
- 3 Click in the **Name** box, and then click the **Close** button (x) which pops up.
- 4 Click **Save**.

## 8.13 Camera - Default



PTZ > Camera - Default

The Default option is used to restore some camera settings such as backlight compensation, exposure mode, exposure compensation, autocalibration, and white balance control to their factory defaults.

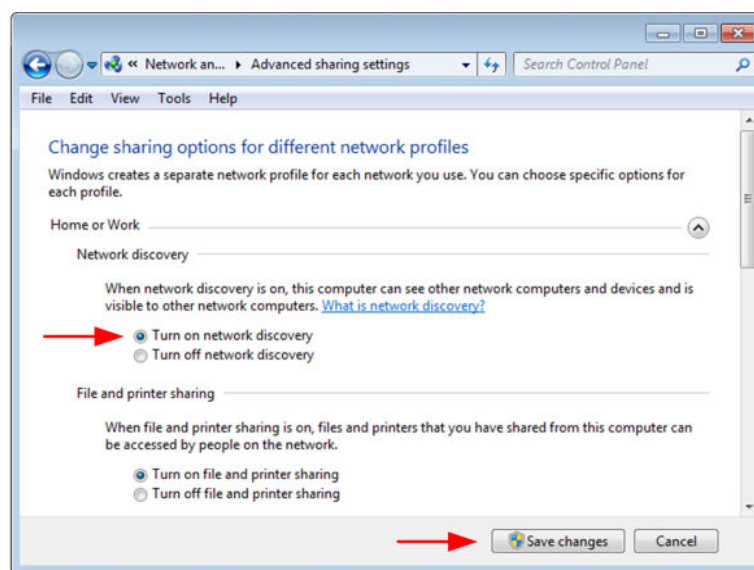
# Appendix: Enable UPnP

With UPnP enabled in Windows, it is possible to see Siqura devices in Windows Explorer. You can double-click a device to open its webpages.

## » To enable UPnP in Windows 7

- 1 In *Control Panel*, click **Network and Sharing Center**.
- 2 In the left pane, click **Change advanced sharing settings**.
- 3 Under the relevant network profile, click **Turn on network discovery**.
- 4 Click **Save changes**

UPnP will now automatically start when you turn on your computer.



*Enable network discovery*

# Appendix: Delete the existing Siqua Viewer software

---

Viewing camera images in the HSD820 webpages requires Siqua Viewer software. You are strongly advised to remove a previous installation of Siqua Viewer from your computer before initial access to the camera over the network or when you encounter an "A new version is available" message.

## » To uninstall Siqua Viewer

- 1 On the Windows **Start Menu**, click **Control Panel**.
- 2 Click **Programs and Features**.
- 3 On the programs list, select **Siqua Viewer**.
- 4 Click **Uninstall**.

Deleting Temporary Internet files may improve your web browser performance.

## » To delete the Temporary Internet files

- 1 Open your web browser.
- 2 On the **Tools** menu, select **Internet options**.
- 3 In the *Browsing history* section of the *General* tab, click **Delete**.
- 4 Select **Temporary Internet files**, and then click **Delete**.

# Appendix: Set Up Internet Security

---

If ActiveX control (Siqua Viewer) installation is blocked, set the Internet security level to default or change the ActiveX controls and plug-ins settings.

## » To set the Internet Security level to default

- 1 Start Internet Explorer (IE).
- 2 On the **Tools** menu, select **Internet options**.
- 3 Click the **Security** tab, and then select the (logo of the) **Internet** zone.
- 4 Under *Security level for this zone*, click the **Default Level** button.
- 5 Click **OK** to confirm the setting.
- 6 Close the browser window, and start a new session later to access the HSD820.

## » To modify ActiveX Controls and Plug-ins settings

- 1 Start Internet Explorer (IE).
- 2 On the **Tools** menu, select **Internet Options**.
- 3 Click the **Security** tab, and then select the (logo of the) **Internet** zone.
- 4 Under *Security level for this zone*, click the **Custom Level** button.  
The Security Settings - Internet Zone dialog box displays.
- 5 Under *ActiveX controls and plug-ins*, set all items listed below to **Enable** or **Prompt**.  
Note that items may vary from one IE version to another.
  - Allow previously unused ActiveX controls to run without prompt.
  - Allow Scriptlets.
  - Automatic prompting for ActiveX controls.
  - Binary and script behaviors.
  - Display video and animation on a webpage that does not use external media player.
  - Download signed ActiveX controls.
  - Download unsigned ActiveX controls.
  - Initialize and script ActiveX controls not marked as safe for scripting.
  - Run ActiveX controls and plug-ins.
  - Script ActiveX controls marked safe for scripting.
- 6 Click **OK** to accept the settings and close the *Security Settings* dialog box.
- 7 Click **OK** to close the Internet Options dialog box.
- 8 Close the browser window, and start a new session later to access the HSD820.

# Appendix: NTCIP Configuration

The National Transportation Communications for ITS Protocol (NTCIP) provides a communications standard that ensures the interoperability and interchangeability of traffic control and Intelligent Transportation Systems (ITS) devices. This appendix provides information about the conformance groups which are supported by the HSD820.

## In This Chapter

Supported conformance groups.....	97
SNMP MIB.....	99

## Supported conformance groups

The HSD820 firmware supports all the mandatory parts and some of the optional parts (see table below) of the NTCIP CCTV specification as laid down in the NTCIP 1205:2001 v01.08 document. This means that - in terms of section 4 of this document - the following conformance groups are supported.

Conformance group	Reference	Conformance requirement
Configuration	NTCIP 1201:1996	mandatory
CCTV Configuration	NTCIP 1205	mandatory
Motion Control	NTCIP 1205	optional

*Conformance statement table*

## Configuration

Most of the Configuration conformance group objects listed below contain static device information.

- Global Set ID parameter
- Maximum modules parameter
- Module table
- Module number
- Module device node
- Module make
- Module model
- Model version
- Module type
- Base standards parameter

## CCTV configuration

The CCTV Configuration conformance group consist of objects that specify the configuration parameters of a CCTV. For details, refer to NTCIP 1205. Conformance requirement within the group is mandatory.

- rangeMaximumPreset
- rangePanLeftLimit
- rangePanRightLimit
- rangePanHomePosition
- trueNorthOffset
- rangeTiltUpLimit
- rangeTiltDownLimit
- rangeZoomLimit
- rangeFocusLimit
- rangeIrisLimit
- rangeMinimumPanStepAngle
- rangeMinimumTiltStepAngle
- timeoutPan
- timeoutTilt
- timeoutZoom
- timeoutFocus
- timeoutIris
- labelTable
  - labelEntry
  - labelIndex
  - labelText
  - labelFontType
  - labelHeight
  - labelColor
  - labelStartRow
  - labelStartColumn
  - labelStatus
  - labelLocationLabel
  - labelEnableTextDisplay

## Motion control

The Motion Control group defines the variables that provide PTZ control. For details, refer to NTCIP 1205. Conformance requirement within the group is mandatory.

- presetGotoPosition
- presetStorePosition
- positionPan
- positionTilt
- positionZoomLens
- positionFocusLens
- positionIrisLens

**Note:** Camera control through NTCIP on Siquira multichannel products is limited to video channel 1.

## SNMP MIB

NTCIP has its own SNMP MIB. This database is used to store information, which is used to control cameras and other devices in the transportation management system. An electronic version of the MIB is available from a NEMA FTP site. To get access to the FTP site, send your name, organisation name, and email address to [ntcip@nema.org](mailto:ntcip@nema.org), and request access.

# Index

## A

About this manual.....	6
Access the webpages.....	14
Acquire an IP address automatically.....	33
Add and manage user accounts.....	27
Admin password.....	26
Advanced settings.....	35
Alarm trigger actions.....	45
Appendix: Delete the existing Siqua Viewer software.....	95
Appendix: Enable UPnP.....	94
Appendix: NTCIP Configuration.....	97
Appendix: Set Up Internet Security.....	96
Application.....	44
Audio.....	75
Audio detection.....	54
Autopan.....	80

## B

Basic.....	33
------------	----

## C

CA certificate.....	32
Camera - Default.....	93
Camera - Exposure.....	86
Camera - Misc 1.....	89
Camera - Misc 2.....	90
Camera - Profile.....	92
Camera - WB.....	87
Cautions.....	9
CCTV configuration.....	98
Change the network settings with Siqua Device Manager.....	16
Client certificate and private key.....	32
Compliance.....	10
Configuration.....	97
Connect via web browser.....	14
Create a self-signed certificate.....	29
Create and install a signed certificate.....	30
Cruise.....	79

## D

Daylight saving time.....	24
DDNS.....	40
Description.....	13

## E

Events.....	43
-------------	----

## F

Factory default.....	65
Features.....	20
File location.....	61
Find the unit with Siqua Device Manager...	15
FTP.....	42

## G

GOV Settings.....	70
-------------------	----

## H

H.264 Profile.....	71
Home.....	19
Home.....	83
Host name.....	24
HTTP.....	43
HTTP Authentication Setting.....	27
HTTPS.....	29

## I

IEEE 802.1X.....	32
Install Siqua Viewer.....	17
IP filter.....	31
IPv6 address configuration.....	35

## L

Log file.....	62
Log on to the unit.....	17

## M

Mail.....	41
Maintenance.....	67
Manual trigger.....	53
Models.....	11
Modify the fixed IP address.....	34
Motion control.....	98
Motion Detection.....	48
Motion detection area.....	50
Motion detection window.....	50

## N

Network.....	33
Network Failure Detection.....	51
Network Share.....	57

## O

Overview.....	19
---------------	----

**P**

Parameters.....	64
Periodical event.....	52
Preset.....	77
Privacy Mask.....	85
Product overview.....	11
PTZ Panel.....	22
PTZ&IMAGE.....	77

Video resolution.....	70
Video rotate type.....	70
Video stream protocol.....	74
Video text overlay.....	72
View information.....	61

**Q**

QoS.....	36
----------	----

**R**

Recording.....	59
----------------	----

**S**

Safety.....	7
Safety and compliance.....	7
Schedule.....	60
SD Card.....	55
Security.....	25
Sequence.....	81
SNMP.....	37
SNMP MIB.....	99
Software upgrade.....	66
Software version.....	66
Specifying file name conventions.....	47
Storage management.....	55
Streaming Authentication Setting.....	28
Supported conformance groups.....	97
System.....	24
System requirements.....	14
System settings.....	23

**T**

The HSD820 web interface.....	18
Tilt Range.....	84
Time format.....	25
Time synchronisation.....	25
Time zone.....	24

**U**

UPnP.....	39
Use PPPoE.....	35
User.....	26
User Information.....	63

**V**

Video and Audio Streaming.....	69
Video compression.....	71
Video format.....	69
Video frame rate.....	75