BC620WDR

Firmware Version 4.0

Network box camera with H.264

User Manual

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

Copyright © 2012 Siqura B.V.

Brand names

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

Liability

Siqura 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. Your feedback will help us to further improve our documentation.

More information

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

Siqura B.V.
Zuidelijk Halfrond 4
2801 DD Gouda
The Netherlands

General   : +31 182 592 333
Fax   : +31 182 592 123
E-mail   : sales.nl@tkhsecurity.com
WWW   : www.siqura.com

For a full list of TKH Security Solutions sales offices, see the last page of this manual.

Contents

Contents

1   About this manual

Document scope

This manual applies to the BC620WDR, Siqura's network box camera with H.264.
It describes in detail:

▸ How to communicate with the unit
▸ How to operate the unit
▸ How to configure the unit's settings

Instructions for camera installation and establishing connections can be found in the separate Quick Start Guide and Installation Manual provided with each BC620WDR series model.

Intended audience

This manual is aimed at technicians and operators involved in the configuration and operation of BC620WDR cameras.

Assumed skills and know-how

To work with a BC620WDR unit, a technician or operator must have adequate knowledge and skills in the fields of:

▸ Installing electronic devices
▸ Ethernet network technologies and Internet Protocol (IP)
▸ Windows environments
▸ Web browsers
▸ Video, audio, data, and contact closure transmissions
▸ Video compression methods

Specifications

The information given in this manual was current when published. Siqura reserves the right to revise and improve its products. All specifications are subject to change without notice.

Important information

Before proceeding, please read and observe all instructions and warnings in this manual. Retain this manual with the original bill of sale for future reference and, if necessary, warranty service. When unpacking your product, check for missing or damaged items. If any item is missing, or if damage is evident, do not install or operate this product. Contact your supplier for assistance.

We like to hear from you!

At Siqura, 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 by email via t.writing@tkhsecurity.com. Your feedback will help us to further improve our documentation.

Acknowledgement

Siqura units use the open-source Free Type font-rendering library.

2 Safety information

This chapter contains the BC620WDR safety instructions.

In This Chapter

2.1 Cautions

General

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.

Handle the camera carefully

Do not abuse the camera. Avoid striking, shaking, etc., as 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. Please consult technical support if a camera is suspected of malfunctioning.

Do not operate the camera beyond the specified temperature and power source ratings

Use the camera under conditions where temperature is between -30°C~+50°C (-22°F~+122°F) (continuous); +60°C (140°F) max.

Do not use strong or abrasive detergents when cleaning 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.

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.

Optical safety (BC620WDR /SFP)

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.

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). Siqura offers products that comply with the EU's RoHS Directive. The full version of the Siqura RoHS statement can be viewed at www.siqura.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.

3 Product description

This chapter provides an overview of the features of the BC620WDR.

In This Chapter

3.1 Product overview

General

The BC620WDR is a network box camera which provides superior low-light performance and wide dynamic range. It is also a highly flexible platform which can provide both embedded analytics as well as multi stream encoding. With a built-in SFP option, the BC620WDR is ready for the widest range of applications.

Multicodec and multistreaming

The BC620WDR is capable of streaming 2x H.264/MJPEG at full frame rate. It can also stream 2x MPEG-2/4 simultaneously. Each stream is optimised for its purpose: high-quality H.264 or MPEG-2 for live viewing, low-bandwidth MPEG-4 for storage, or easy-to-decode MJPEG for web applications and remote devices.

Up to twenty streams can be retrieved using RTSP. It is also possible to use the Session Announcement Protocol (SAP) to transmit MPEG-2/-4/MJPEG and H.264 streams to multicast destinations. The unit also has a Live View encoder that can convert the video input signal to MJPEG format for streaming to web applications or remote devices using the HTTP pull method.

Using the MX protocol, a total of twelve copies – three per independent MPEG-2/4 or H.264/MJPEG video stream – can be transmitted to different unicast and/or multicast destinations. The BC620WDR supports source-specific multicast (SSM).

Open Streaming Architecture (OSA) and ONVIF

The BC620WDR is designed with OSA, offering standardised streaming video and remote control based on international standards and tested with different vendors. A comprehensive HTTP API gives access to all controls and makes integration easy. The API is available at www.siqura.com. The BC620WDR also fully supports ONVIF. It has been tested to support ONVIF Profile S.

Fiber option

The BC620WDR is available with an optional pluggable SFP slot for multimode/single-mode fiber optic connections or the Siqura ECO-plug™. The ECO-plug™ offers Ethernet over Coax.

Image quality monitoring and tamper detection

The BC620WDR is fitted with video analytics to check for camera health problems. This image quality monitor analyses contrast, exposure, sharpness, and noise. Camera tamper analytics detect any changes in the position or field of view of the camera. The instant a camera is subject to failure or tampering, an alert can be raised. The BC620WDR includes SNMP support for both functions. When an image quality or tamper alarm occurs a trap is sent to an SNMP manager.

Web interface

Configuration, management, and live viewing are simplified by the access-controlled web interface. Full in-band control is available through Siqura's MX™ Configuration Tool Kit or the HTTP API. The BC620WDR is field-upgradeable.

Video Motion Detection (VMD)

The BC620WDR is fitted with a motion detector, which raises an event when a certain amount of motion is detected in a predefined area in the image. The motion detector runs real-time on the live images. The detection itself is based on 'averaged pixel change'. The region of interest (ROI) is obtained by masking the parts of the image of less or no interest, such as trees or a fountain which would otherwise trigger false events. The mask can be drawn freely over the image.

FTP Push

On the occurrence of an event, the BC620WDR can post a JPG image on a remote server. The unit pushes the image to one or two FTP servers. The event can be triggered externally, by VMD, the Image Monitor, Tamper Detect, etc., or the BC620WDR can periodically upload images to the remote server(s).

Audio and I/O channels

By combining streaming video with duplex audio and I/O contacts over IP, the BC620WDR provides all the interfaces necessary for any IP CCTV application. The balanced audio inputs/outputs are suitable for all industrial audio systems.

Analog output

With its analog output, the hybrid BC620WDR solution can provide local video for a public view monitor or local DVR.

Privacy masks

You can set up privacy masks on the BC620WDR to obscure sections of the image. This feature is often requested for such situations as city centre surveillance and point of sale (POS) keypads.

Power source choices

The BC620WDR camera can be powered by 12VDC or 24VAC (terminal block) or over the network with 802.3af-compliant PoE sources (PoE Class 3; 6.49W to 12.95W).

Reliability

Dependability and high reliability are key factors in this dome's design cycle. Siqura BC620WDR cameras are assembled with meticulous care and thorough testing at our ISO 9001-compliant factory.

3.2   Features summary

The BC620WDR offers the following features.

‣ 1/3" Pixim DPS Seawolf Imager
‣ Day/Night with IR-cut filter
‣ Super Wide Dynamic Range
‣ Back Light Compensation
‣ Alarm: 2 inputs/2 outputs
‣ Two-way audio
‣ Up to 10 privacy masks
‣ Analog output
‣ 12VDC/24VAC/802.3af Power over Ethernet
‣ Optical output option
‣ For future use: SD card slot for local recording

4 Interfaces

A variety of methods can be employed to communicate with the BC620WDR. This chapter outlines the interfaces you can use to control the unit and manage the media streams it is handling.

In This Chapter

4.1 ONVIF

The Open Network Video Interface Forum (ONVIF) is an open industry forum for the development of a global standard for the interface of IP-based physical security products. ONVIF is committed to the adoption of IP in the security market. The ONVIF specification ensures interoperability between products regardless of manufacturer. It defines a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The BC620WDR fully supports ONVIF. It has been tested to support ONVIF Profile S.

4.2 OSA

Siqura's Open Streaming Architecture (OSA) consists of a standard set of open communication protocols to govern media streaming via RTSP and equipment management via HTTP. The *Siqura Protocol for PTZ Cameras and Codecs* enables easy integration of the BC620WDR with third-party products. The protocol consists mainly of different CGI (Common Gateway Interface) program calls for listing and configuring parameters. For detailed information, refer to Siqura's *PTZ Camera and Codec Programming Interface* specification. You can download this HTTP API specification at www.siqura.com.

4.3 Web User Interface

Using the BC620WDR's web server is the most straightforward way to access the unit. The webpages enable you to configure the settings of the BC620WDR and view live video images from a standard web browser, eliminating the need for a separate application program.

4.4 MX/IP

MX/IP, a proprietary Siqura protocol, offers direct access to the settings of the BC620WDR contained in the *Management Information Base* (MIB), a list of variables stored inside the unit. The MIB can be read and/or written with special MX software. *MX Configuration Tool*, for example, offers full control of the BC620WDR through the MIB, enabling you to remotely configure device settings and manage media streams. Additionally, MX viewing and control software offers real-time monitoring of video streams (Operator Office, MX Viewer Lite) and playback of recorded images (Operator Storage). For more details on the MX/IP protocol, the MIB and Siqura's EMX network service, refer to the manuals documenting the MX Software Development Kit and the above programs.

Note: If you prefer using open standards, you can go to the Device Management page of the unit and disable the MX/IP protocol on the MX tab on this page. Be aware that doing so prevents you from upgrading the BC620WDR firmware through MX Firmware Upgrade Tool.

4.5 SNMP

The Simple Network Management Protocol (SNMP), part of the internet protocol suite, can be used to monitor network devices such as the BC620WDR for conditions or events that require administrative attention. For more information, refer to appropriate literature on SNMP.

The BC620WDR supports in-band SNMP. Via SNMP, several status variables can be read and traps can be generated on events. BC620WDR SNMP settings can be configured on the SNMP tab on the Device Management webpage of the unit.

The SNMP Agent is MIB-2 compliant and supports versions 1 and 2c of the SNMP protocol.

Note: The BC620WDR includes SNMP support for its image quality monitor and tamper detect functions. A trap is sent when bad image quality or camera tampering is detected and another one when the situation returns to normal.

Required MIB files can be downloaded at www.siqura.com.

4.6 SAP

The BC620WDR supports the Session Announcement Protocol (SAP). This is a protocol for broadcasting multicast session information. A SAP listening application can listen to the announcements advertised by the BC620WDR SAP announcer. The application can use this information to receive a video or audio stream that the BC620WDR is transmitting to the advertised multicast address. For more details, see the description of the Video webpage.

4.7 NTCIP

The National Transportation Communications for ITS Protocol (NTCIP) is a communication protocol deployed in Intelligent Transportation Systems (ITS) in the USA. It is a family of standards designed to provide definitions of common data elements and communication protocols for the interaction between traffic management centre(s) and road-side devices such as cameras, traffic signals, and highway lighting. The goal of the standards is to achieve interoperability and interchangeability between systems manufactured by different vendors in order to reduce the total cost of traffic systems, including maintenance.

The BC620WDR supports all the mandatory parts and some of the optional parts of the NTCIP CCTV specification as laid down in the NTCIP 1205:2001 v01.08 document. For details about the NTCIP configuration of the BC620WDR, see Appendix: NTCIP Configuration.

The BC620WDR supports the standard NTCIP SNMP MIB. This MIB database is used to store information, which in turn will be 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, and request access.

5 Media streaming via RTSP

The easiest way to extract a video or audio stream from the BC620WDR is to use the Real-Time Streaming Protocol (RTSP). This chapter explains the role of the BC620WDR in RTSP media sessions and describes how to open a media stream from the unit in a video player plug-in.

In This Chapter

5.1 RTSP and RTP

The BC620WDR implements an RTSP server. A hardware or software decoder (the latter within a viewing application, for example) is the RTSP client. Media sessions between client and server are established and controlled with RTSP. Media stream delivery itself is handled by the Real-Time Transport Protocol (RTP). The BC620WDR supports video and audio streaming via UDP and TCP.

Use the following URL format to get a video stream into, for example, VLC or QuickTime.

rtsp:// <IP address of encoder>:<RTSP Port>/VideoInput/<x>/<y>/<z>

where:
- **<x>** is the number of the Video Input
- **<y>** is the media type of the required encoder
- **<z>** is the encoder number

Note: The <RTSP Port> is optional. If not entered, port 554 is used by default.

Note: The encoder number index **<z>** in the URL only takes enabled encoders into account, with the encoder mode set to the indicated media type **<y>** (RTSP is a streaming protocol which takes care of stream control; it does not handle device configuration).

The stream in the following figure will be pulled from the unit with the IP address 10.1.1.2, using Video Input 1 and the first enabled MPEG-4 encoder.
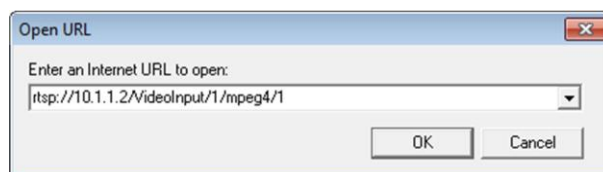
RTSP URL format
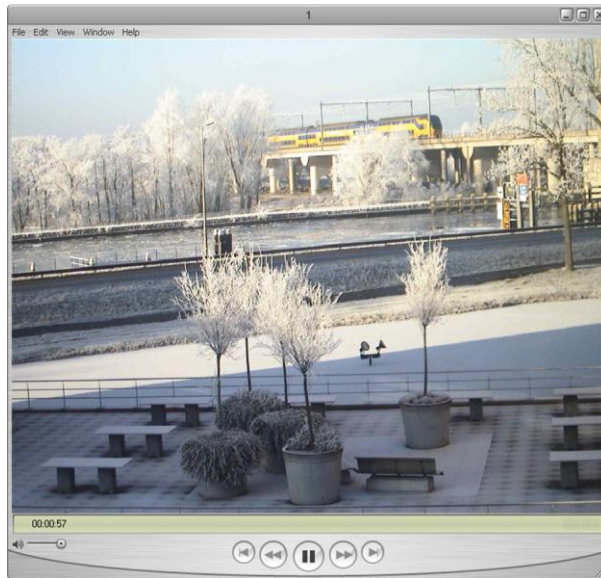
A BC620WDR video stream viewed in QuickTime

5.2   Transfer via UDP or TCP

The BC620WDR supports the following types of streaming.
▸   UDP/IP (multicast and/or unicast)
▸   TCP/IP (RTP, RTP over RTSP, RTP over RTSP over HTTP)

The BC620WDR reports to the client that it supports transfer over UDP and TCP. The choice is made on the client side. In VLC, for example, using a TCP connection can be forced (*Preferences > Inputs and Codecs > Network > RTP over RTSP (TCP)*).

For details on controlling BC620WDR media streams through HTTP and RTSP, refer to Siqura's *PTZ Camera and Codec Programming Interface* specification. You can download this HTTP API specification at www.siqura.com.

6 Webpage access

The webpages of the BC620WDR 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

6.1 System requirements

To access the webpages of the BC620WDR you need the following.
‣ A PC with a web browser installed.
‣ An IP connection between the PC and the BC620WDR.

6.2 Login

▸ **To log on to the web server of the BC620WDR**

1. Open your web browser.
2. Enter the IP address of the BC620WDR in the address bar.
   If your network configuration is correct you are directed to the login page of the unit.
   If the login page does not display correctly you may need to enable JavaScript in your web browser (see Appendix: Enabling JavaScript).
3. In the *Login* section, click **LOGIN**.
4. In the *Connect* dialog box, log in as "Admin".
   The default password is "1234".
   User name and password are case sensitive.
5. Click **OK** or press ENTER.
   On successful login, the Live Video page displays.

Enter the IP address of the BC620WDR in the address bar of the browser

BC620WDR login page

Connect dialog box

7 Webpage features

This chapter introduces the webpages and common elements found on them. It also discusses user account types and associated access levels. For an in-depth description of specific webpages and their functionalities, refer to the chapters following this chapter.

In This Chapter

7.1 Menu

Using the menu on the left of each webpage you can navigate to the other pages. Live Video, the first option on the menu, is the home page of the BC620WDR. The Logout option at the bottom logs out the current user and displays the Login box. The other menu options link to pages which allow you to view and configure user and device settings.

Live Video	Live Video	Live Video
Status	Status	Logout
Network	Network	
Video	Video	
Audio	Audio	
Data RS-422/485	Data RS-422/485	
CC Streams	CC Streams	
PTZ	PTZ	
Event Management	Event Management	
Device Management	Date and Time	
User Management	Logout	
Date and Time		
Logout		

BC620WDR menu options available to (from left to right) Admin, Operator, and Viewer accounts
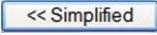
7.2 Access control

Whether a specific BC620WDR webpage appears on the navigation menu depends on the user account you logged in with. The unit has three access levels: *Admin*, *Operator*, and *Viewer*. Admins have full access to the webpages. They can create, edit, and delete user accounts on the User Management page. The Operator level gives access to the device configuration pages, but not to user management or device management. Viewer access is restricted to the home page.

7.3   Sections, buttons, tabs, and check boxes

Apart from the menu, the webpages share the following features.
- Sections showing parameter values, some of which are editable.
- Buttons (mainly *Save* and *Cancel*) for sections with editable fields.
- Tabs (on several pages) used to organise page content.
- Check boxes used to select features.

This Button	Does This	Note
Save	Writes changes to the unit.	Some sections (for example, those on the VMD tab of the Video page) do not have *Save* and *Cancel* buttons. Changes you make here are immediately written to the device.
Cancel	Undoes unsaved changes and shows values as they were before editing.	
Advanced >>	Opens the Advanced Settings section with additional settings.	**Important:** Be aware that configuring Advanced Settings requires in-depth understanding of the impact of your changes on the workings of your BC620WDR. If in doubt, do *not* change the default values.
<< Simplified	Closes the Advanced Settings section.	

8 Live Video

After a successful login, the Live Video page displays. On this page, you can view live video from the BC620WDR and - if PTZ functionality is implemented - control the camera from your web browser.

In This Chapter

8.1 Activate Live View

Live View inactive

The Live View function is inactive when you open the Live Video page.

➤ **To activate Live View**

  ▸ Click **Play LiveView>>**.

8.2   View live video
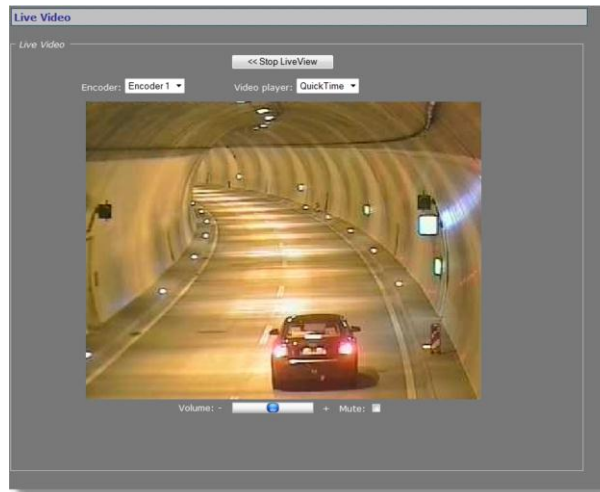
Live View activated

With Live View enabled, the Live Video section includes the following items.

Item	Description	
<<Stop Live View	Closes the preview.	
Encoder	The video encoder used to encode the images seen in the preview.	
	Encoder 1/2	H.264/MJPEG encoding.
	Encoder 3/4	MPEG-2/MPEG-4 encoding.
	Live View	Live View encoding.
Video player	*QuickTime*	The plug-in used to display the images in the previews on this page and the Video pages. Note that QuickTime does not support H.264 High Profile mode.
	VLC	
	No Player	Indicates that neither QuickTime nor VLC is detected on the host machine. For more information, see Appendix: Video Player Plug-In Installation.
Refresh rate	Available in Live View encoder mode. Indicates the current refresh rate of the webpage.	
Preview	Shows live images from the BC620WDR as encoded by the selected encoder. MPEG-2/4 and H.264 previews are streamed over RTSP. Live View encoder previews are transported to the webpage using the HTTP protocol.	
Volume	Available in Encoder # mode. Drag the sliding button to control audio volume.	
Mute	Available in Encoder # mode. Select or clear this box to mute or unmute audio, respectively.	

Enable an encoder

The preview shows images from the selected encoder, unless the specific encoder is disabled. You can enable and disable encoders on the Video page.

Enable audio

If the audio controls are not available in Encoder # mode, go to the Audio page and make sure that audio is enabled and properly configured.

Audio Disabled warning

8.3   PTZ camera control via web browser
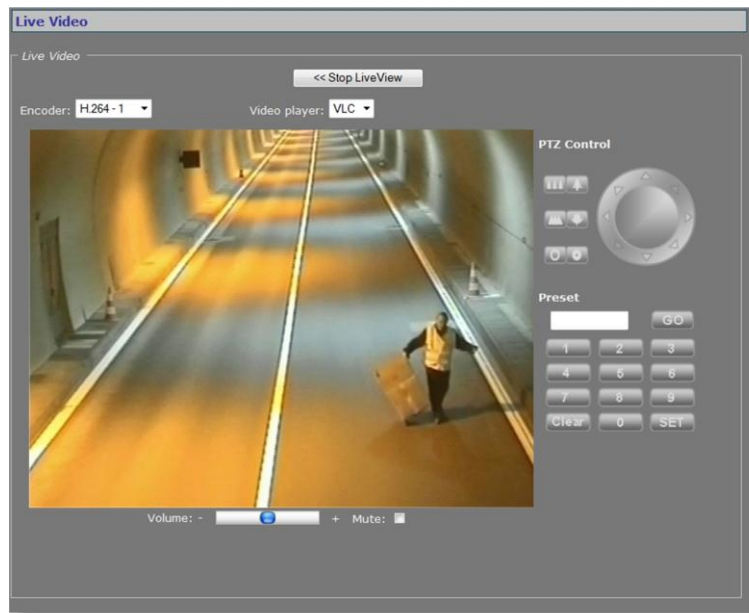
Live Video page with PTZ Control panel

Display the PTZ control panel

Although the BC620WDR itself does not have PTZ functionality, it can be mounted on a PTZ mounting bracket which can then be controlled from the BC620WDR's serial data port (RS-4xx). With a PTZ driver selected on the PTZ web page, the PTZ control panel is available on the Live Video page. If the BC620WDR supports the PTZ driver, you can use the panel to control the camera and manage the presets via the mounting bracket. PTZ drivers not included in the driver list on the PTZ page can be uploaded to the BC620WDR via PTZ Driver Management on the same page.

PTZ control

Use the upper section of the PTZ Control panel to pan, tilt, zoom, and focus the camera, and control the iris, as shown in the following figure.
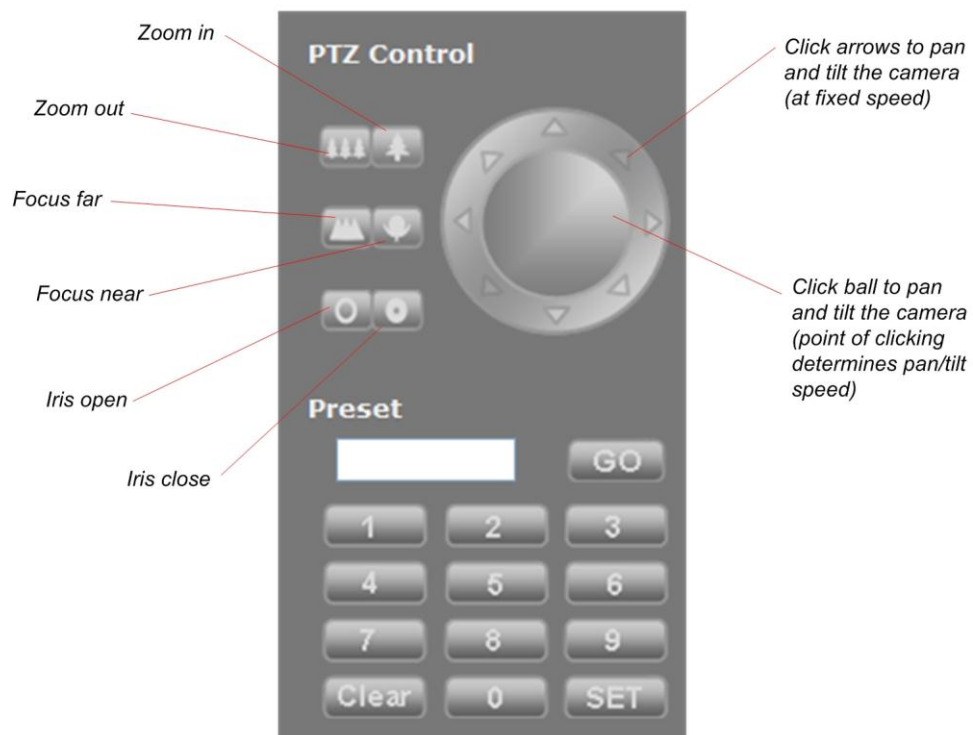
PTZ Control panel

Preset

Use the Preset section to define and recall preset camera positions.

▸ **To enter and save a preset camera position**

1. Click the appropriate number button(s) to enter the preset number.
2. Adjust the position of the camera for the desired view.
3. When satisfied with the position, click **SET**.

   Note: The SET button is not available to users with Viewer rights.

▸ **To recall a preset camera position**

1. Click the appropriate number button(s) to enter the preset number.
2. Click **GO**.

▸ **To erase a preset camera position**

1. Call the preset.
2. Press **Clear**.
3. If desired, override the preset with a new preset position.

9 Status

This chapter describes the Status page. Stream states and measurements on this page may prove helpful when troubleshooting problems.

In This Chapter

9.1 Status

Status > Status: a snapshot of the system state with automatic updating

The Status tab provides information on the stream states of video and audio streams. A stream state is reported as *Idle*, *Waiting*, or *OK*.

Stream state	Description
Ok	There is nothing wrong with the stream. If the video signal is removed from the video input on the encoder side, the Decoder rx state will still be reported as *Ok*, because the video transmitter will be sending a stream - that is, a *No Video* image - to the decoder.
Idle	The transmitter/receiver is not enabled.
Waiting	The transmitter/receiver has lost its stream connection. Possible causes: ▸ An incorrect port number. ▸ The transmitter on the encoder side is not enabled. ▸ No FloodGuard packets have been received for more than 3 seconds. For details on the FloodGuard flooding prevention mechanism, see the note on FloodGuard in the Video chapter.

9.2   Measurements

Status > Measurements

The Measurements tab shows general measurements, such as the module temperatures (current and peak) and the module uptime. You also find network specifics here, such as the MAC address, the actual IP address, the network load from this module, the load information per processor, and signal stream-specific details. You can use the FTP Push 1 section to monitor the FTP Push process.

10 Network

On the Network page, you can change the network settings of the BC620WDR. In this chapter, you will learn how to set a valid, fixed IP address and, alternatively, how to have an IP address automatically assigned by a DHCP server.

In This Chapter

10.1 Network Settings
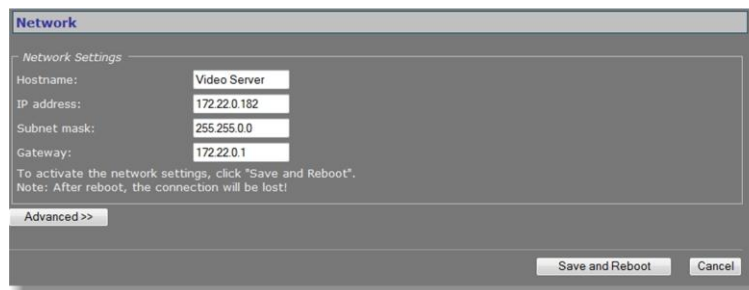
Network page

On the Network page, you can set the name of the unit, the IP address, the subnet mask, and the gateway IP address. For correct functioning of the BC620WDR, it is vital to set its network addressing to be compatible with the subnet it is hooked into.

Note: The factory-set IP address of the unit is in the 10.x.x.x range with a subnet mask of 255.0.0.0. Achieving initial communication with the unit requires that the network adapter of the browsing PC is set to the factory default subnet of the BC620WDR. Once you have made the webpages accessible in this way, you can use the Network page to change the default network settings to the desired settings.

For IP address input to be valid, the unit's IP address:
‣ must be within the 1.0.0.1 – 223.255.255.254 range
‣ cannot start with 127 (reserved for loopback on local host)

After changing IP settings, do not forget to save the new settings and reboot the unit (see chapter Device Management).

Important: It is essential to set at least the IP address and subnet mask correctly. Keep these value on record, otherwise management of the unit will require special software.

10.2 Advanced

Network > Advanced Settings

10.2.1 Services

Item	Description
RTSP server enable	Select this check box to enable the BC620WDR to act as a server in RTSP media sessions.
RTSP server port	This is the port number used to contact the RTSP server. The default transport layer port number for the RTSP protocol is 554 for both UDP and TCP transports.

10.2.2 Network

Item	Description	
DHCP enable	Allows assigning of the IP address by a DHCP server instead of using static IP addressing.	
Ethernet mode	Transmission mode and speed.	
	Auto	Autonegotiation (default).
	10 HDX	Half duplex, 10 Mbit.
	10 FDX	Full duplex, 10 Mbit.
	100 HDX	Half duplex, 100 Mbit.
	100 FDX	Full duplex, 100 Mbit.
MTU size	Set to Ethernet (1500) by default. Maximum Transmission Unit (MTU) is the maximum size (in bytes) of IP packet that can be transmitted over the network without dividing it into pieces. An MTU size that you select here must be supported on the other side of the link.	

11 Video

The Video page gives access to a variety of BC620WDR settings pertaining to camera setup, video encoding, on-screen display, video motion detection, image posting via FTP, camera health monitoring, and privacy masks. This chapter provides a detailed description of the items found on each tab.

In This Chapter

11.1 Image
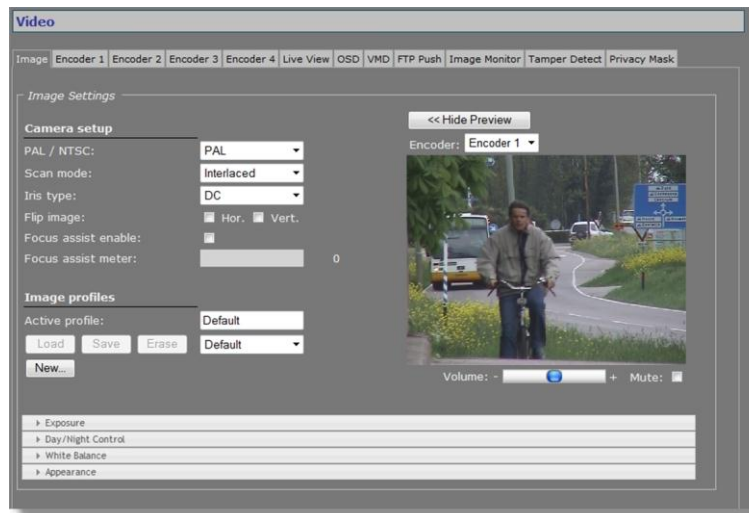
Video > Image

Tab layout

Settings on the Image tab are grouped in the following categories.
- Camera setup
- Image profiles
- Exposure
- Day/Night Control
- White Balance
- Appearance

Accordion style menus at the bottom of the Image tab are opened/closed by clicking the menu's title bar.

Preview

Click **Show Preview>>** to open the preview and see the effect of your current settings.

11.1.1 Camera setup

Item	Description	
PAL/NTSC	*PAL*	Sets the video display standard. Affects the selectable frame rates on the encoder tabs (PAL: 1-25 fps; NTSC: 1-30fps) and the maximum resolution (PAL 720x576; NTSC 720x480). Note that this setting also determines the video standard on the analog output on the back of the camera.
	NTSC	
Scan mode	*Interlaced*	Interlaced scan, originating from traditional television systems, uses two fields to create a frame, one holding the odd lines in the image, the other holding the even ones. The two fields are captured at different moments. Select this option for viewing the video on an analog monitor.
	Progressive	Progressive scan captures the entire image in one go. To be viewed on digital displays (such as PC monitors) images from progressive sources do not need deinterlacing, therefore.
Iris type	*DC*	Activates electrical iris control. The camera will automatically handle the level of light allowed to enter the lens. Select this option for DC Auto Iris lenses. Video Auto Iris lenses are not supported.
	Manual	To be selected for lenses without iris setting or manual iris setting.
Flip image	*Horizontal*	Rotates the image around a vertical axis through the centre of the image (left becomes right, and vice versa). See pictures below.
	Vertical	Rotates the image around a horizontal axis through the centre of the image (top becomes bottom, and vice versa). See pictures below.
Focus assist enable	Aactivates the Focus Assist function. Alternatively, you can also press the Focus Assist button on the back of the camera. Using Focus Assist is described below.	
Focus assist meter	With Focus Assist enabled, a blue bar indicates the focus level. A white bar with the same function appears as an overlay over the image.	

Original image

Flip horizontal
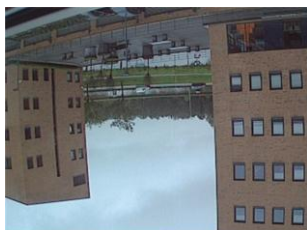
Flip vertical
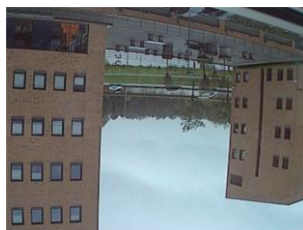
Flip horizontal and vertical (= rotate 180°)

11.1.2 Use Focus assist

BC620WDR includes Focus Assist functionality to achieve optimal image quality. Focus Assist can be used from the Video page but also from the back of the camera body. The latter may prove useful when setting the focus without a monitor.

▸ **To use Focus Assist from the web page**

1. On the **Video** page, select the **Image** tab.
2. Under *Camera setup*, select **Focus assist enable**.
    The focus level is indicated by the blue *Focus assist meter* bar. The meter is also overlaid over the image as a vertical white bar.
3. Aided by the feedback from the Focus assist meter, adjust the focus on the lens.
    The greater the detail in the scene, the higher the number on the Focus assist meter.

Focus assist meter enabled

▸ **To use Focus Assist from the camera body**

1. To activate Focus Assist, turn the focus ring of the lens all the way in one direction, and then press the white button on the back of the camera housing.
    The Focus LED - also on the back of the housing - shines orange, indicating that Focus Assist has not registered a maximum sharpness value yet.
2. Slowly turn the focus ring of the lens until the LED shines red.
3. Next, turn back the focus ring to find the point where the Focus LED shines green.
    This is the point where the camera is properly focused.

LED state	Indicates	Action
Orange	Focus Assist has not registered a maximum focus value yet.	Turn the focus ring of the lens all the way from left to right until a maximum value is seen.
Red	Focus Assist has registered a maximum focus value, but is not properly focused yet.	Slowly turn the focus ring until the Focus LED shines green.
Green	The camera is properly focused.	None

11.1.3   Image profiles

Video > Image > Image profiles

Image profiles

The accordion style menus at the bottom of the Image tab allow you to configure Exposure, Day/Night, White Balance, and Appearance settings. Combinations of these settings can be saved to and loaded from a profile. In addition to custom profiles created by the user, the profile list includes preset profiles for specific purposes. When a profile has been selected, changing one of its defined parameters sets the Profile box to '--'.

Item	Description
Active profile	The active combination of settings.
Load	Activates the selected profile.
New	Enables you to enter a name for a new profile.
Store	Saves and activates the selected profile.
Erase	Removes the selected profile.
Profile list	Available profiles.

11.1.4   Image profile management

⇒ **To create a custom image profile**

1. On the **Video** page, click the **Image** tab.
2. In the *Image profiles* section, click **New**.
3. Enter a name for the new profile, and then click **OK**.
4. Configure the required settings in the *Exposure*, *Day/Night Control*, *White Balance*, and/or *Appearance* sections.
5. Click **Save**.

⇒ **To load an image profile**

1. On the **Video** page, click the **Image** tab.
2. In the *Image profiles* section, click to open the profile list.
3. Select the profile, and then click **Load**.
   The profile displays in the Active profile box and the camera adopts the new settings.

⇒ **To erase an image profile**

1. On the **Video** page, click the **Image** tab.
2. In the *Image profiles* section, click to open the profile list.
3. Select the profile, and then click **Erase**.
   The profile is removed from the profile list.

11.1.5 Preview

Video > Image > Preview

Item	Description	
Show Preview>>	Click to view live images and see the effect of the current settings.	
<<Hide Preview	Closes the preview. This may improve webpage responsiveness.	
Encoder	The encoder handling the images seen in the preview.	
Volume	Encoder # mode	Drag the sliding button to control audio volume.
Mute	Encoder # mode	Select or clear this box to respectively mute or unmute audio.

11.1.6 Exposure

Exposure is the amount of light received by the image sensor and is determined by how wide you open the lens diaphragm (iris adjustment), by how long you keep the sensor exposed (shutter speed), and by other exposure parameters. In the Exposure section of the Image tab, you can define a variety of exposure settings.

Video > Image > Exposure

Item	Description	
Metering area	*Auto, Center, Left, Right, Top, Bottom*	Defines what zone of the image is to have most weight in measuring the exposure of the entire scene.
Gain control mode	Gain is an electronic way of increasing the video signal to control the exposure. Note that higher gain values introduce more noise in the image.	
	Auto	The camera automatically controls gain. A maximum can be set via the *Max auto gain* parameter.
	Manual	Enables gain configuration via the *Manual gain* parameter.

Item	Description	
Manual gain	Manual gain control mode only	Allows the user to set a gain value manually.
Max auto gain	Auto gain control mode only	Allows the user to set an upper limit for automatic gain control.
Auto iris threshold	Sets the target exposure system gain value (in dB) which the auto iris control will maintain. The threshold determines at what gain level the iris is activated. A lower setting activates the iris only at lighter scenes, whereas a higher setting activates the iris at darker scenes. Also note that a higher setting introduces less noise but gives less depth of field, whereas a lower setting results in more noise but also more depth of field.	
Exposure preference	*Highlights, Shadows*	Either highlight or shadow detail may be lost in a scene. Exposure preference enables you to select the proper exposure mode for the region of interest within a scene.
Transition speed	*Slow, Medium, Fast*	Controls the transition time span between subsequent exposure levels. With a slow setting, the camera takes more time to adjust to a new light situation.
Slow shutter mode	The shutter speed determines how long the image sensor is exposed to light. To see clear images in a dark environment, enable this function and select a slow shutter speed.	
	Off	Slow shutter mode disabled.
	x2	The camera averages multiple frames. With the x2 setting, for example, it averages a maximum of 2 frames to eliminate noise. The frame rate is then divided by 2. With the x32 setting, the camera averages a maximum of 32 frames to eliminate noise. The frame rate is then divided by 32 (so more than a second).
	x4	
	x8	
	x16	
	x32	
Backlight compensation	In situations where the observed object is unclear due to being under- or overlit, backlight compensation improves image exposure by using the light near the object as a reference.	
Median percentile (BLC)	TBD.	
Wide dynamic range	WDR is especially effective in solving indoor and outdoor contrast issues to enhance image quality and video display. It enables the camera to catch detailed data from the dark part of an image without any saturation from the brighter parts.	
Color roll detection	Enables the camera to correct rotating colour changes caused by the different frequencies of the shutter and a light source.	
Flicker reduction	Compensates for flickering caused by discrepancies between the frame rate (video standard) and the AC frequency of the lighting.	

11.1.7 Day/Night Control

With Day/Night Control, the camera can still catch clear images at night. In daylight, the IR cut filter blocks infrared light for clear images. At night, the IR cut filter is removed to utilise infrared light; the displayed images will be in black and white.

Video > Image > Day/Night Control

Item	Description	
Day/night mode	*Auto*	Enables day/night switching. The internal circuit automatically decides when to place/remove the IR cut filter based on the value of the lighting conditions as determined by the Transition threshold.
	Day	Activates the IR cut filter. Camera is set to colour mode.
	Night	Removes the IR cut filter. Camera is set to black and white mode.
Transition threshold	Auto mode only	Sets the threshold for the camera to place/remove the IR cut filter. With a higher threshold value, the camera switches to night mode at lower light levels (higher gain value). With a lower threshold value, the camera switches to night mode at higher light levels (lower gain value).
Transition speed	Auto mode only	Sets the delay the camera takes into account when switching from day to night mode and vice versa. Using a higher value here prevents the camera to trigger on for example headlights of a car temporary shining directly into the camera at night.
Gain boost in night mode	Auto and Night mode only	Night mode uses a low shutter speed which may cause moving objects to blur. At night and in low light conditions, Gain boost may yield a better picture.

11.1.8   White Balance

A digital camera needs to find a reference color temperature, which is a way of measuring the colour of a light source as a basis for calculating all the other colours. The unit for measuring this ratio is in degree Kelvin (K). You can select one of the white balance control modes according to the installation condition. The following table shows the colour temperature of some typical light sources.

Light source	Colour temperature in K
Cloudy sky	6,000 to 8,000
Noon sun and clear sky	6,500
Household lighting	2,500 to 3,000
75-watt bulb	2,820
Candle flame	1,200 to 1,500

Light source reference
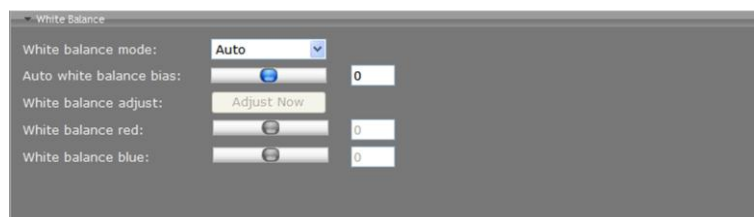
Video > Image > White Balance

Item	Description	
White balance mode	*Auto*	Continuously calculates white balance settings and dynamically adjusts for changing conditions.
	AWB	Performs a one-shot white balance calculation. The colour temperature is calculated once when enabled and not adjusted thereafter. Use the *Adjust Now* button to force recalculation.
	Manual	Enables manual setting of white balance through the *White balance red* and *White balance blue* sliders (see below).
	ATW Limit	Same as *Auto*, maximum and minimum white balance auto adjustments are limited. Extreme values are not compensated.
	ATW Desat	Same as *ATW Limit*, but gradually desaturates the image to give it a more natural look when the calculated colour temperature goes beyond the maximum and minimum white balance limits.
Auto white balance bias	Not in Manual mode	Drag the slider to make colour corrections to the selected white balance mode. Adds a bias to the calculated colour temperature.
White balance adjust	AWB mode only	Pressing *Adjust Now* sets white balance according to the current image and locks it.
White balance red White balance blue	Manual mode only	Sliders to adjust colour temperatures. Drag the sliders to increase/decrease the red/blue values in the image, while observing the preview.

11.1.9 Appearance

Video > Image > Appearance

Item	Description
Color saturation	Drag the sliding button, or enter values into the boxes, to adjust current settings, aided by the visual feedback from the preview. Settings entered here apply to all video encoders.
Contrast	
Brightness	
Sharpness	

11.2   Video encoding
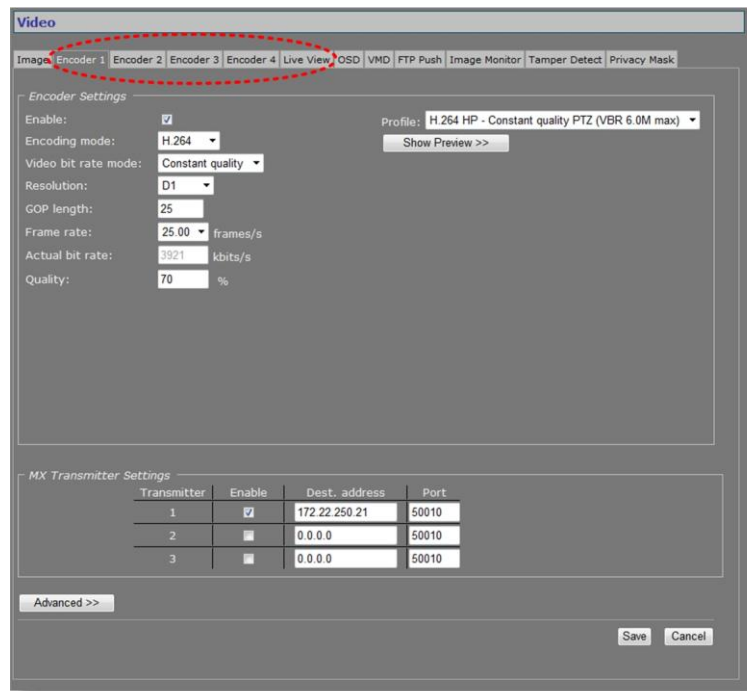
Encoder tabs on Video page

Multicodec

The BC620WDR features a built-in, multicodec video server. Four video encoders can simultaneously generate independent digital video streams with different resolutions and frame rates. Encoders 1 and 2 can each convert the video signal into H.264 or MJPEG format. Encoders 3 and 4 can both handle MPEG-2/4 encoding.

Multistreaming

Up to twenty streams can be retrieved using RTSP. A total of twelve copies – three per independent encoder – can be transmitted to different unicast and/or multicast destinations using Siqura's proprietary MX protocol. The BC620WDR supports source-specific multicast (SSM). MPEG-2/4, H.264, and audio streams can also be transmitted to multicast destinations using the Session Announcement Protocol (SAP).

(M)JPEG

BC620WDR's Live View encoder can convert the video signal to MJPEG format for streaming to web applications or remote devices using the HTTP protocol. Via FTP Push, JPEG images can also be posted on an FTP server.

11.3   Encoder 1/2
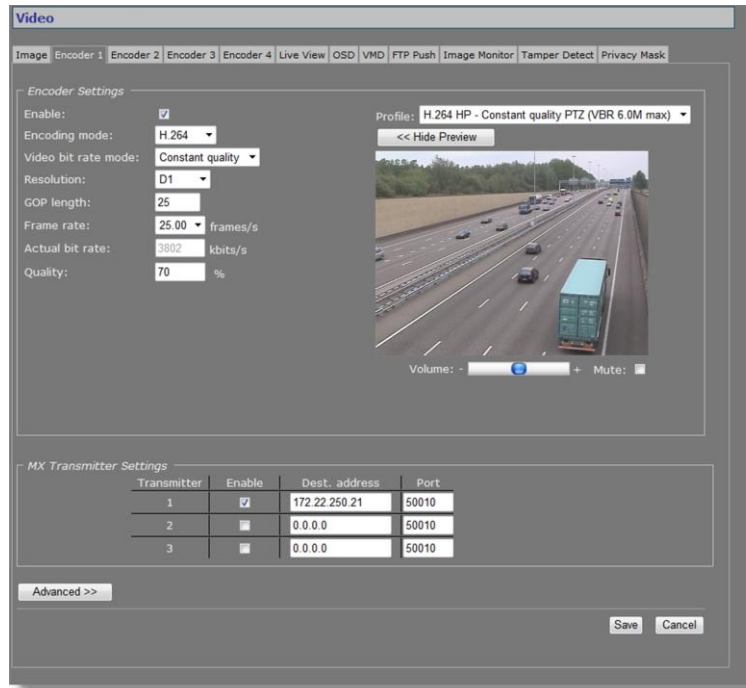
Video > Encoder 1

11.3.1   Encoder Settings

Item	Description	
Enable	All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder.	
Encoding mode	*H.264 or MJPEG*	The method used to compress the video signal.
	BC620WDR can stream (M)JPEG over UDP and HTTP. ▸ To enable and configure **UDP**/MJPEG streaming, select MJPEG from the Encoding mode list and configure settings. ▸ To transport JPEG over **HTTP** and/or use the Live View previews in the web pages, go to the Live View tab, enable the Live View encoder, and configure its settings.	
Video bit rate mode	Controls variations in bit rates.	
	Constant quality	Keeps the image quality constant, with varying network load. See *Constant Quality Mode (CQM) configuration* (below) for Siqura's recommended strategy for controlling image quality.
	Constant bit rate	Keeps network load constant at the cost of varying image quality. Frames may be skipped.
Resolution	The following resolutions are supported.	

resolution (h x v)	PAL	NTSC
D1	720x576	720x480
2/3 D1	480x576	480x480

Item	Description		
	1/2 D1	352x576	352x480
	4CIF	704x576	704x480
	2CIF	720x288	720x240
	CIF (top field only)	352x288	352x240
	QCIF	176x144	176x120
	In addition, VGA (640x480) and QVGA (320x240) are also supported.		

Note on CIF resolutions: 2CIF, CIF, QCIF use only one of the two frame fields. When CIF-encoded pictures are displayed on a monitor, the decoder simulates the second field (by extrapolation from the first field) in order to present two frame fields. CIF is mostly used for recording purposes, as a compromise between good video quality and storage capacity needed.

Note: The BC620WDR will simultaneously handle dual H.264/MJPEG encoding at full frame rate, and Live View encoding at 5 frames per second. Setting Encoders 3 and 4 to perform MPEG-2/4 encoding on D1 resolution at the same time may overtax the hardware. The total output bandwidth, including streams controlled by RTSP, and those enabled through SAP, should not exceed 25 Mb/s.

Item	Description	
GOP length	Distance in frames between two I-frames.	
Frame rate	*PAL: 1-25 fps; NTSC: 1-30 fps*. Selectable rates are determined by the video mode (PAL, NTSC) set on the Image tab.	
Bit rate	Constant bit rate mode only	The speed of the digital transmission - that is, the amount of information transferred/processed per unit of time.
Actual bit rate	Constant quality mode only	This field is dynamically updated with the current bit rate to provide feedback on the bit rate that is used on average with the current *Quality* setting.
Quality	Constant quality mode only	Reflects the amount of compression. Generally speaking: the higher the quality setting, the lower the compression ratio and the more bits are consumed. This means a trade-off has to be found between the desired quality level and available bandwidth.
Profile	Preset combinations of settings for specific purposes. When a profile has been selected, changing one of its defined parameters sets the Profile box to '--', to indicate that a custom profile has been configured. When a freely chosen parameter value combination matches a preset profile, the name of the profile shows in the Profile box.	
Show Preview>>	Click to view live images and see the effect of the current settings.	
<<Hide Preview	Closes the preview. This may improve webpage responsiveness.	
Volume	Drag the sliding button to control audio volume.	
Mute	Select or clear this box to respectively mute or unmute audio.	

11.3.1.1 Parameter value combinations

Set sensible combinations of video bit rate mode, resolution, GOP length, and frame and bit rates. When setting and saving these values, you may notice that inappropriate value combinations are 'corrected' by automatic selection of the closest suitable combination.

Important: If in doubt about the effects of specific encoder settings, you are advised to select the profile offering the closest match to your required application.

11.3.2 Constant Quality Mode configuration

Constant Quality mode (CQM) can be used in situations with intermittent increases of movement in camera images. This mode provides better pictures when quickly panning a PTZ camera, for example. Siqura recommends the following strategy for Constant Quality mode configuration.

❧ **To configure CQM settings**

1. In *Encoder Settings*, open the **Video bit rate mode** list, and then select **Constant quality**.
2. With the video source connected and the encoder enabled, go to the *Quality* field and set the desired quality (range: [0 ... 100%]), aided by the visual feedback in the Preview.
3. Press **Save** to store your settings.
   The Actual bit rate field is dynamically updated with the current bit rate.
4. Determine if the average bit rate used with the current *Quality* setting is acceptable. If not, modify the *Quality* setting.
5. To set the upper limit for the bit rate, open the **Advanced Settings** section and use the *CQM max bit rate* field to specify the maximum bit rate.
   Generally, it is not necessary to change the default setting of 6000 kbit/s, unless there are physical limitations on the network.
6. Press **Save** to store your settings.
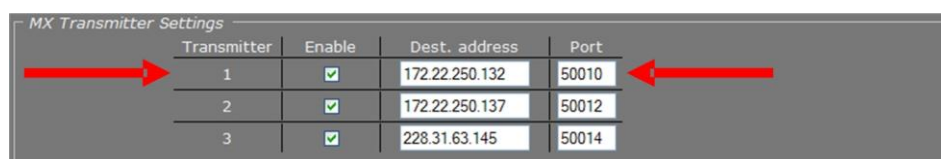
11.3.3 Make a video connection

Creating a video link between one of the BC620WDR's built-in video encoders and a decoder involves two steps:
▸ configuring the encoder's settings
▸ configuring the decoder's settings

❧ **To configure the encoder's settings**

1. Open the BC620WDR's web pages, go to the Video page, and then select the appropriate Encoder tab.
2. In the *Transmitter Settings* section, specify the destination IP address.
   This is the address of the video decoder that is to receive the video stream.
3. Enter the decoder's port number.
   For more information, see the chapter on Port Numbers.
4. Select **Enable**.
5. Press **Save**.

Transmitter	Enable	Dest. address	Port
1	☑	172.22.250.132	50010
2	☑	172.22.250.137	50012
3	☑	228.31.63.145	50014
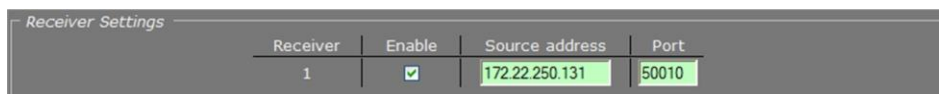
Video Transmitter Settings (encoder).
Transmitter 1 enabled, holding the decoder IP address and input port number.
An input port number must be used only once per device.

⇥ To configure the decoder's settings

1. Open the decoder's web pages, go to the Video page, and then select the Decoder tab.
2. In the *Receiver Settings* section, specify the source IP address.
   This is the address of the video encoder - that is, the BC620WDR - that will be transmitting the video stream.
3. Enter the decoder's own port number.
   For more information, see the chapter on Port Numbers.
4. Select **Enable**.
5. Press **Save**.

Receiver Settings			
Receiver	Enable	Source address	Port
1	☑	172.22.250.131	50010

Video Receiver Settings (decoder).
Receiver 1 enabled, holding the encoder IP address and the decoder input port number.
An input port number must be used only once per device.

With these settings configured correctly, the video link will be established. The decoder takes the video stream from the encoder, detects the video format, and uses the appropriate decoding algorithm to convert the stream to an analog output signal.

Note: Source and destination IP addresses can be unicast or multicast. For more information, see the chapter on Multicasting.

Highlighted fields

The source address and port number fields are highlighted in green when the enabled receiver receives a stream from the specified source. The two fields are marked in red when no stream is received with the receiver enabled and correctly configured.

11.3.4 Advanced

Important: If in doubt about these settings, do *not* change the default values.

11.3.4.1 Encoder

Depending on the selected encoding mode, specific parameter values in this section are dimmed - that is, not available for configuration.

H.264 encoding, Constant Quality Mode   MJPEG encoding, Constant Quality Mode

Video > Encoder 1/2 > Advanced Settings > Encoder

Item	Description	
Encoding profile	*Main profile*	Compatibility mode for decoders which do not support High profile.
	High profile	Improved encoding quality (as compared to Main profile).
CQM max bit rate	Available in *Constant quality* mode (CQM). Use this setting to set the maximum bit rate for a given picture quality configured in the Encoder Settings section.	
Frame rate divider	Relates to the frame rate configured in the Encoder Settings section.	
X-resolution	Variables that enable you to freely set picture resolution instead of using the resolution presets in the Encoder Settings section.	
Y-resolution		
Request I-frame	When joining a multicast stream in the middle of a long GOP, requesting an I-frame will speed up response time, i.e. image display will start sooner.	
Request I-frame hold off	Range: [0…255] frames. Requesting (too) many I-frames may add to latency. To prevent this, you can specify the distance in frames, starting after the previous I-frame, before another I-frame is sent upon request.	
Scene change detect	Enables the scene detection algorithm. If enabled, the encoder can fully restart a new GOP with an I-slice and an instantaneous decoding refresh (IDR) picture, depending on image content.	
Scene change detect period	Sets the minimum time between scene changes in milliseconds. This is a hold-off mechanism that prevents a scene change for the specified time, starting from the previous scene change.	
Force frame mode	If *Force frame mode* is enabled, the H.264 video stream is compressed and sent using entire frames (Frame mode). If disabled, the stream is compressed and sent using entire frames or the separate fields (Field mode).	
Deblocking filter	Enables the in-loop deblocking filter in the AVC encoder. H.264 encoding can handle portions of the video image in blocks of varying sizes which can be processed independently. The deblocking filter enhances image quality by smoothing block edges and reducing blocking distortion. Be aware, however, that applying the filter requires substantial processing power.	
Deblocking filter alpha coefficient	Set the alpha/beta coefficients of the deblocking filter. Entering experimental values for these coefficients may help you in achieving optimal image quality.	
Deblocking filter beta coefficient		

Item	Description	
Meta data insertion mode	Determines the method used to add meta data to the stream. For details, see the section on Meta Data Insertion.	
	Disabled	No meta data added to the stream.
	Fixed interval	Activates *Meta data insertion interval* parameter (below).
	Each I-frame	Data block is added after each I-frame. The interval is determined by the GOP length, therefore.
Meta data insertion interval	Range: [100-10000] ms. Sets the (fixed) interval at which meta data is added to the stream. Activate this parameter by setting *Meta data insertion mode* (see above) to *Fixed interval*.	

11.3.4.2 Stream Manager

Video > Encoder # > Advanced > Stream Manager

Balancing network load

Peaks in the network load vary with encoder output. Use the Stream Manager to balance network load. It can limit the output rate per stream sent to the transmitters. Be warned that setting the Stream bandwidth limit to a lower value may introduce latency because peaks in the encoder output will be buffered.

Item	Description
Stream bandwidth limit	Range: [0...100000] kbit/s. Sets the maximum bit rate per stream sent to the transmitters. This will serve to spread bursts but in its turn may give rise to latency, e.g. when handling large I-frames.
	You are advised to limit the outgoing bit rate per encoder to a maximum of 15Mbit/s. The total outgoing bit rate of all encoders (including the Live View encoder), RTSP controlled streams, and SAP streams, should not exceed 25 Mbit/s. See the value for the Total tx bit rate parameter on the Measurements tab of the Status page.
	The Stream bandwidth limit mechanism is disabled when Low latency (see below) is selected. See also the graphic in the Note on FloodGuard.
Keep-alive interval	Range: [10 … 100000] milliseconds. The frequency for sending keep-alive messages to the encoder.
Low latency	Raises the output bandwidth limit to allow for peaks in the network load. To be selected if you need to keep the delay between the input and output of images as short as possible, for improved tracking with a dome camera for example. Selecting *Low latency* disables the *Stream bandwidth limit* mechanism.

Note on Low Latency mode: This mode may cause packet loss in the network. In this mode, short bursts of 100 MB data may overflow the input buffer of an Ethernet aggregation switch. As a rule of thumb, the average load of an Ethernet port should not exceed 40% of its maximum load (i.e. 40 MB for a 100 MB port).

11.3.4.3 Transmitter

Video > Encoder # > Advanced > Transmitter 1

Item	Description	
DSCP field	Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits, up to 64 network service types can be defined. *RFC 2724 (http://www.ietf.org/rfc/rfc2474.txt*) describes the Differentiated Services (DS) field and the DiffServ Code Point. See also the note on Differentiated Services later in this chapter.	
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).	
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.	
RTP control mode	Select the transport protocol to control the stream.	
	None	No transport protocol selected.
	FloodGuard	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
	RTCP	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
Stream type	*UDP + RTP*	Default setting. Plain RTP stream over UDP.
	UDP + RTP + NKF	Adds an extended RTP header for Siqura applications requiring extra information.
RTP type	Default value: [0]. This parameter determines the RTP payload format (e.g. H.264, MPEG-2/4, or audio). To avoid an RTP type conflict, the values specified on both sides of the connection must be the same. The default value of "0" automatically sets the appropriate media type. You are advised not to change this setting.	
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.	

11.3.4.4 RTSP Transmitter

Video > Encoder # > Advanced > RTSP Transmitter

Item	Description
DSCP field	Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits, up to 64 network service types can be defined. *RFC 2724* (*http://www.ietf.org/rfc/rfc2474.txt*) describes the Differentiated Services (DS) field and the DiffServ Code Point. See also the note on Differentiated Services later in this chapter.
Enable multicast	Activates the *Default multicast IP address* text box. The RTSP transmitter itself does not require enabling.
Default multicast IP address	Select *Enable multicast* (see above) to activate this check box. The "Invalid multicast address" warning disappears upon specification of a valid multicast address.
Default multicast port	Port number for multicast sessions.

11.3.4.5 SAP Settings

Video > Encoder # > Advanced > SAP Settings

SAP announcer

The BC620WDR includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the BC620WDR is available at a specific multicast address and port.
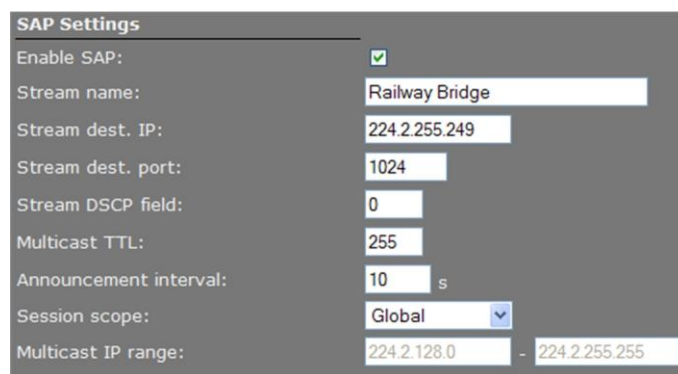
The BC620WDR can send SAP multicast streams for its H.264, MPEG-2/4, and audio encoders. The video streams include audio if audio is enabled on the Audio webpage and if the multicast IP range is the same as for video. Note that audio in itself can also be received as a separate stream. For more information about SAP, see the note later in this chapter.

Item	Description
Enable SAP	When selected, session announcements are sent at the frequency determined by the Announcement interval parameter and the media stream is transmitted to the multicast IP address specified in the Stream dest. IP address box.
Stream name	Enter a descriptive name to identify the media stream.
Stream dest. IP	Enter the multicast IP address the media stream is to be sent to. The address must be within the range defined by the Multicast IP range parameter.
Stream dest. port	The destination port number. Default: 1024.
Stream DSCP field	Range: [0…63]. See the note on DSCP.
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.
Announcement interval	Determines the frequency of announcements.
Session scope	*Global*, the default session scope, sets the *Multicast IP range* parameter to 224.2.128.0 - 224.2.255.255 (IPv4 global scope sessions). A SAP listening application will recognize the global scope and automatically listen for SAP announcements at the 224.2.127.254 multicast IP address. The *Administrative* session scope allows you to enter a custom IP range within the 239.0.0.0 - 239.255.255.255 (IPv4 administrative scope sessions) range. For an Administrative session scope, the multicast address for SAP announcements will be set to the highest address in the relevant administrative scope. For example, for a scope range of 239.16.32.0 - 239.16.33.255, the IP address 239.16.33.255 is used for SAP announcements.
Multicast IP range	See Session scope.

To configure SAP settings, do the following

1. In the SAP settings section, select **Enable SAP**.
2. Enter a stream name.
3. In the Session scope list, select **Global** or **Administrative**.
4. If you selected *Administrative* in the previous step, specify the Multicast IP range.
5. Enter the Stream Destination IP address and the port number.
   The IP address must be within the scope range displayed for the Multicast IP range parameter.
6. Enter/modify the values for Stream DSCP field, Multicast TTL, and Announcement Interval, if desired.
7. Click **Save**.
   The video stream can now be viewed in a media player, such as QuickTime or VLC.

SAP example settings

BC620WDR SAP network stream opened via VLC Playlist

11.3.5 Meta data insertion

Enabling

All BC620WDR encoders can be configured to include meta data in the video streams they generate. The insertion of meta data is enabled by setting an interval via the Advanced Settings of the encoder. A meta data message is added to the stream as a block of data with a fixed format (see examples below). The messages can contain user data, product info, and status info.

Note: This section provides a general explanation of meta data insertion as implemented in Siqura products. The unit described in this manual, may or may not feature all of the media (e.g. audio, contact closure) and encoding formats included below.

User data message

For MPEG-2 and MPEG-4, User data is preceded by the User data header (00 00 01 B2):

0x00	0x00	0x01	0xB2	User data message

For MJPEG, these (for the rest identical) messages are inserted as comment field (FF FE):

0xFF	0xFE	Size (MSB)	Size (LSB)	User data message

For H.264, these (for the rest identical) messages are inserted as SEI NAL-unit (0x06), marked as type User Data Unregistered (0x05):

0x06	0x05	Size	UUID (16 bytes)	User data message

Product info message

The Product info message (always inserted) is used to identify the source of a specific video stream. The data ID is 0x00, with the message in the following layout.

'O'	'P'	'T'	'C'	0x00	Prod. name (ASCII)	0x80	Serial nr (ASCII)	0x80	SW version (ASCII)	0x80

Status info message

This message contains all relevant status messages, related to the video stream or codec. The data ID is 0x01, with the message in the following layout.

'O'	'P'	'T'	'C'	0x01	Status1	Status2	Status3	Status4	(future expansion possible)

Status 1	Video status
Bit 0 (lsb)	Video loss on input
Bit 1	Black/white video
Bit 2	VMD alarm
Bit 3	Tampering alarm
Bit 4	Image quality alarm
Bit 5	(for future use, will be '0')
Bit 6	(for future use, will be '0')
Bit 7 (msb)	Fixed '0'

Status 2	General status
Bit 0	Temperature alarm
Bit 1	(for future use, will be '0')
Bit 2	(for future use, will be '0')
Bit 3	(for future use, will be '0')
Bit 4	(for future use, will be '0')
Bit 5	Audio present
Bit 6	Fixed '1'
Bit 7	Fixed '0'

Status 3	CC status (part 1)
Bit 0	CCin-1
Bit 1	CCin-2
Bit 2	CCin-3
Bit 3	CCin-4
Bit 4	CCin-5
Bit 5	CCin-6
Bit 6	CCin-7
Bit 7	Fixed '0'

Status 4	CC status (part 2)
Bit 0	CCin-8
Bit 1	(for future use, will be '0')
Bit 2	(for future use, will be '0')
Bit 3	(for future use, will be '0')
Bit 4	(for future use, will be '0')
Bit 5	(for future use, will be '0')
Bit 6	Fixed '1'
Bit 7	Fixed '0'

User defined text message

This message can be defined and enabled by the user, using Siqura's PTZ Cameras and Codecs API, for example. There is no maximum limit on the amount of characters. Considering that this data is part of a video stream, the maximum should be reasonable.

11.3.6   Notes

Note on Differentiated Services: Differentiated Services (DiffServ, or DS) is a method for adding QoS (Quality of Service) 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 - i.e. 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 realized, for example, through priority queuing, bandwidth allocation, or by assigning dedicated routes.

Note on RTP and RTCP: The Real-time Transport Protocol (RTP) is designed for end-to-end real-time, audio or video data flow transport. It is regarded as the primary standard for video/audio transport over multicast or unicast network services. RTP does not provide guaranteed delivery, but sequencing of the data makes it possible to detect missing packets. It allows the recipient to compensate for breaks in sequence that may occur during the transfer on an IP network. Error concealment can make the loss of packets unnoticeable.
RTP is usually used in conjunction with the Real-time Transport Control Protocol (RTCP). RTP carries the media streams. RTCP provides reception quality feedback, participant identification and synchronization between media streams.

Note on the Session Announcement Protocol (SAP): SAP, defined in *RFC 2974* (see RFC 2974 - *http://www.ietf.org/rfc/rfc2974.txt*), is a protocol for advertising multicast session information. A SAP announcer periodically broadcasts announcement packets which include the session description information of multicast sessions presented by the announcer. SAP uses the Session Description Protocol (SDP) as the format of the session descriptions. The announcement is multicast with the same scope as the session it is announcing, ensuring that the recipients of the announcement are within the scope of the session the announcement describes. SAP listening applications can listen to the announcements and use the information to construct a guide of all advertised sessions. This guide can be used to select and start a particular session. The SAP announcer is not aware of the presence or absence of SAP listeners.

Note on FloodGuard: FloodGuard is a Siqura™ proprietary stream control mechanism that can be enabled/disabled independently for each video and sampled data transmitter. FloodGuard throttles the transmitter when it no longer receives control messages from the receiver, thereby preventing the transmitter from flooding the network.

FloodGuard only works when enabled on both the transmitter and the receiver, and when the transmitter sends to a unicast address.

When a transmitter is enabled, it opens a control receive port with the port number equal to its source port number + 1. This port listens for control packets from the destination receiver. When no FloodGuard packets come in during the time set for the *FloodGuard throttle delay*, the receiver is expected to have disappeared (powered off, receiver disabled, network problem, etc.) and the stream is 'throttled'. In throttled mode the transmitter - in order to contact the intended receiver (again) - sends empty packets into the network at an interval determined by the *FloodGuard throttle interval* parameter. After reception of a valid FloodGuard packet the transmitter immediately resumes streaming.
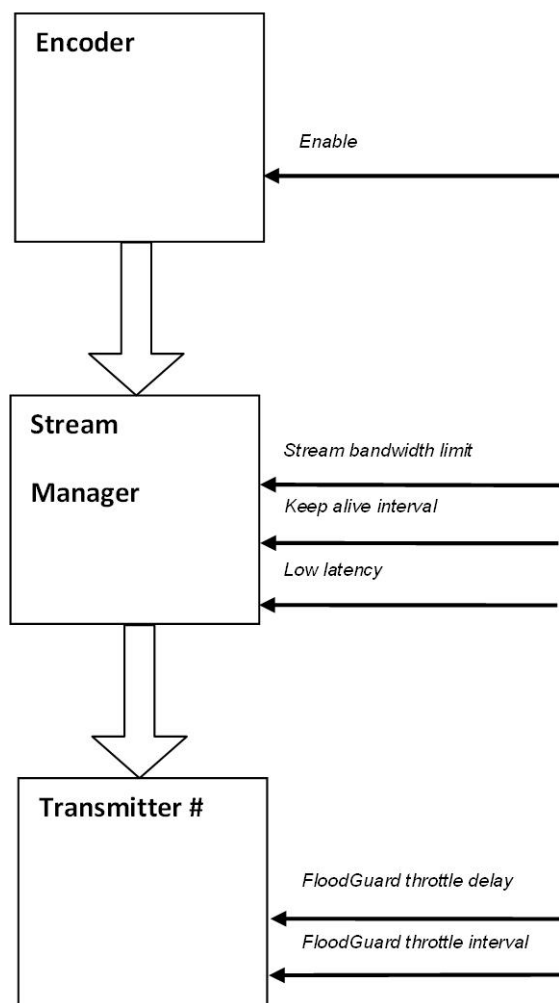
Stream Manager and FloodGuard
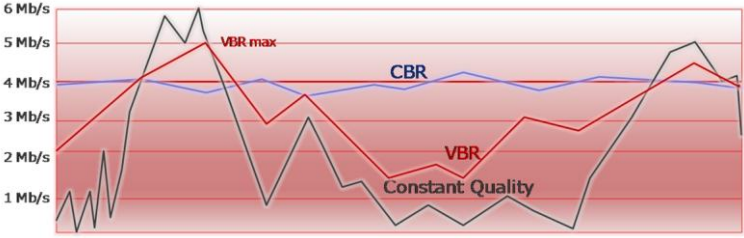
11.4   Encoder 3/4
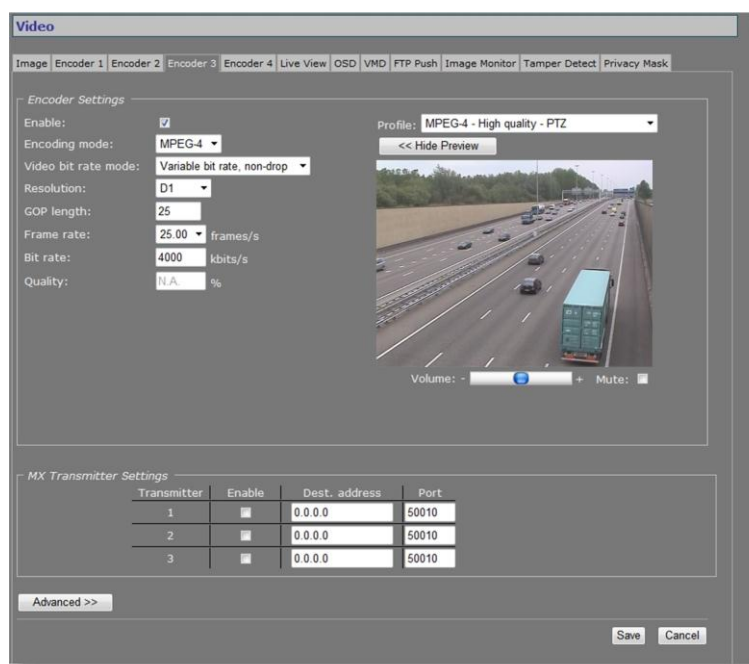
Video > Encoder 3

11.4.1   Encoder Settings

Item	Description	
Enable	All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder.	
Encoding mode	*MPEG-4 or MPEG-2*	The method used to compress the video signal.
Video bit rate mode	Controls variations in bit rates. For a concise explanation, consult the note on Encoder Settings later in this chapter..	
	MPEG-4 encoding mode supports the following bit rate modes.	
	Constant quality	Keeps the image quality constant, with varying network load (from a few kb/s to 10 Mb/s or higher). The image quality is determined by the values set for the "Q min I" and "Q min P" parameters in the Advanced Settings section.
	Variable bit rate	Variable network load, but limited to value set for the *VBR maximum bit rate* parameter in the Advanced Settings section. The frame rate will suffer when the *VBR maximum bit rate* is reached.
	Variable bit rate, non-drop	Variable network load, but limited to value set for the *VBR maximum bit rate* parameter in the Advanced Settings section. The quality will decrease when the *VBR maximum bit rate* is reached. The frame rate will be constant.
	Constant bit rate	Keeps network load constant at the cost of varying image quality. Frames may be skipped.

Item	Description
	Constant bit rate, non-drop — Keeps network load constant at the cost of varying image quality. Frames are never skipped.

MPEG-2 encoding mode supports the following bit rate mode.

Item	Description
	Constant bit rate, non-drop — Keeps network load constant at the cost of varying image quality. Frames are never skipped.
Resolution	The following resolutions are supported.

resolution (h x v)	PAL	NTSC
D1	720x576	720x480
2/3 D1	480x576	480x480
1/2 D1	352x576	352x480
4CIF	704x576	704x480
2CIF	720x288	720x240
CIF (top field only)	352x288	352x240
QCIF	176x144	176x120

In addition, VGA (640x480) and QVGA (320x240) are also supported.

For more information on CIF resolutions, see "Notes" later in this chapter.

Note: The BC620WDR will simultaneously handle dual H.264 encoding and dual MPEG-2/4 encoding at full frame rate, and Live View encoding at 5 frames per second. Setting Encoders 3 and 4 to perform MPEG-2/4 encoding in D1 resolution at the same time may overtax the hardware. The total output bandwidth, including streams controlled by RTSP, and those enabled through SAP, should not exceed 25 Mb/s.

Item	Description
GOP length	Distance in frames between two I-frames.
Frame rate	*PAL: 1-25 fps; NTSC: 1-30 fps.* Selectable rates are determined by the video mode (PAL, NTSC) set on the Image tab.
Bit rate	Range: [10…15000]. Selecting a profile (see below), automatically sets the bit rate associated with the profile.
Profile	Preset combinations of settings for specific purposes. When a profile has been selected, changing one of its defined parameters sets the Profile box to '--', to indicate that a custom profile has been configured. When a freely chosen parameter value combination matches a preset profile, the name of the profile shows in the Profile box.
Show Preview>>	Click to view live images and see the effect of the current settings.
<<Hide Preview	Closes the preview. This may improve webpage responsiveness.
Volume	Drag the sliding button to control audio volume.
Mute	Select or clear this box to respectively mute or unmute audio.

11.4.1.1 Combinations of settings

Set sensible combinations of video bit rate mode, resolution, GOP length, and frame and bit rates. When setting and saving these values, you may notice that inappropriate value combinations are 'corrected' by automatic selection of the closest suitable combination. The output bit rate set may range from 10-15000 kbps. The total output bandwidth should not exceed 25 Mb/s.

11.4.1.2 Notes

Note on CIF resolutions: 2CIF, CIF, QCIF use only one of the two frame fields. When CIF-encoded pictures are displayed on a monitor, the decoder simulates the second field (by extrapolation from the first field) in order to present two frame fields. CIF is mostly used for recording purposes, as a compromise between good video quality and storage capacity needed.

Note on Encoder Settings: Video bit rate mode can be set to be constant (i.e. the number of bits in a group of pictures) or variable. Selecting the correct mode for a given application, with emphasis on a good compromise between detail and good representation of frequent changes (motion), is generally vital.

Constant bit rate mode (CBR) is generally safest. Although the image quality may vary, the network load generated will remain fairly constant.
If constant picture quality is required and a varying network load will pose no problems, choose *Variable bit rate mode* (VBR). Video streaming is generally smoother under VBR.

Improving video picture quality and video stream quality, in terms of latency and smoothness for example, is subject to trade-offs. Many aspects of picture quality and stream quality are governed by a series of compression and signal parameters which may work favorably on one aspect while adversely affecting another.
For example, increasing the bit rate generally improves video quality, but also puts additional load on the network. But even for a given bit rate and network performance, video quality and streaming are influenced by other parameters and aspects. Please consult appropriate literature on video encoding formats, and application notes for clarification.

If in doubt about the effects of specific encoder settings, you are advised to select the profile offering the closest match to your required application.

11.4.2 Make a video connection

Creating a video link between Encoder 3/4 and a video decoder is done in the same fashion as described for Encoder 1/2 earlier in this chapter.

11.4.3   Advanced

Important: If in doubt about these settings, do *not* change the default values.

11.4.3.1 Encoder

Depending on the selected encoding mode, specific parameter values in this section are dimmed - that is, not available for configuration.

MPEG-2 mode

Video > Encoder # > Advanced > Encoder (MPEG-2 mode)

Item	Description	
Frame rate divider	Relates to the frame rate configured in the Encoder Settings section.	
X-resolution	Variables that enable you to freely set picture resolution instead of using the resolution presets in the Encoder Settings section.	
Y-resolution		
Stream type	*Transport Stream* or *Elementary Stream*.	
Quantization matrix	*MPEG Default*, *Alternative 1*, or *Alternative 2*.	
Meta data insertion mode	For details, see the section on Meta Data Insertion.	
	Disabled	No meta data added to stream.
	Fixed interval	Activates *Meta data insertion interval* parameter (below).
	Each I-frame	Data block is added after each I-frame. The interval is determined by the GOP length, therefore.
Meta data insertion interval	Activate this parameter by setting *Meta data insertion mode* (above) to *Fixed interval*.	

Note on Quantization: Quantization is a lossy compression technique used in image processing. It is based on the fact that variations in high frequency brightness, for example, are not easily distinguished by the human eye. A quantization matrix, a combination of predefined values, is used to reduce the amount of information in the high frequency components of an image, thereby making the stream more compressible. The values in a quantization matrix are often chosen such that certain frequencies are kept in the source to avoid losing image quality.

MPEG-4 mode

Video > Encoder # > Advanced > Encoder (MPEG-4 mode)

Item	Description	
VBR maximum bit rate	Range: [0...15000]. Sets a limit for variable bit rate.	
Q min I	Used to achieve consistent picture quality within a single GOP or across consecutive GOPs. Lower values produce a better picture, but will yield higher bit rates and require more processing. Default Q min I = 3; default Q min P = 2.	
Q min P		
Frame rate divider	Relates to the frame rate configured in the Encoder Settings section.	
X-resolution	Variables that enable you to freely set picture resolution instead of using the resolution presets in the Encoder Settings section.	
Y-resolution		
Request I-frame	When joining a multicast stream in the middle of a long GOP, requesting an I-frame will speed up response time, i.e. image display will start sooner.	
Request I-frame hold off	Range: [0…255] frames. Requesting (too) many I-frames may add to latency. To prevent this, you can specify the distance in frames, starting after the previous I-frame, before another I-frame is sent upon request.	
Meta data insertion mode	For details, see the section on Meta Data Insertion.	
	Disabled	No meta data added to stream.
	Fixed interval	Not supported for MPEG-4 streams. If a fixed interval is set, the nearest I-frame will be used.
	Each I-frame	Data block is added after each I-frame. The interval is determined by the GOP length, therefore.
Meta data insertion interval	Activate this parameter by setting *Meta data insertion mode* (above) to *Fixed interval*.	

11.4.3.2 Stream Manager, Transmitter #, RTSP Transmitter, and SAP settings

Configuring Stream Manager, Transmitter #, RTSP Transmitter, and SAP settings for MPEG-2/4 encoding is done in the same way as for Encoders 1/2. For details, see the description earlier in this chapter.

11.5   Live View
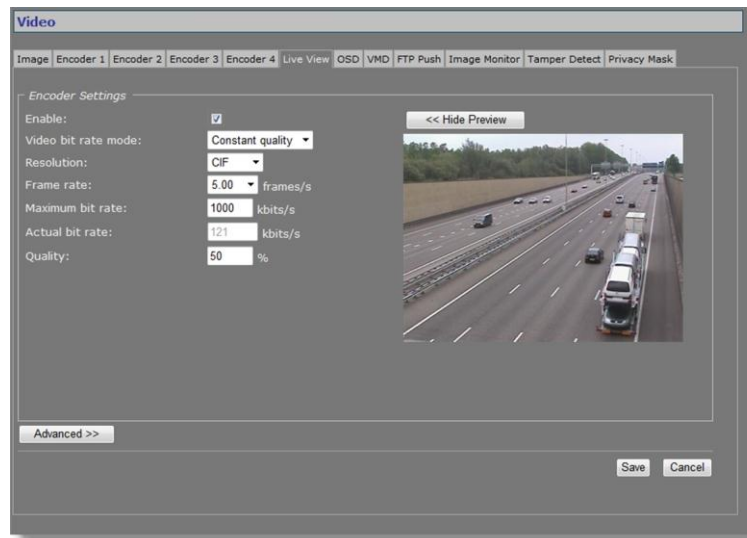
Video > Live View

11.5.1   (M)JPEG output

The BC620WDR provides multiple (M)JPEG output methods.

▸ To transport JPEG over **HTTP** and/or to use the Live View previews in the web pages, enable the Live View encoder and configure its settings.

▸ To enable and configure **UDP**/MJPEG streaming, go to the Encoder 1/2 tab, select MJPEG encoding mode and configure settings.

▸ To activate the uploading of JPEG images to an FTP server, configure the required settings on the FTP Push tab and the Event Management page.

11.5.2   Encoder Settings

Item	Description	
Enable	All encoders are enabled by default. Use this check box to disable/re-enable this specific encoder.	
Video bit rate mode	Controls variations in bit rates.	
	Constant quality	Keeps the image quality constant, with varying network load. The quality is determined by the value set for the *Quality* parameter (see below).
	Constant bit rate	Keeps network load constant at the cost of varying image quality. Frames may be skipped.
Resolution	Set sensible combinations of mode, resolution, frame rate and (maximum) bit rate. It is advised to limit MJPEG encoding to 5 fps when the BC620WDR is also handling MPEG-2/4 encoding with 1xD1 and 1xCIF or 2CIF at full frame rate.	
Frame rate		
(Maximum) bit rate		

Item	Description	
Actual bit rate	Constant Quality Mode (CQM) only	This field is dynamically updated with the current bit rate to provide feedback on the bit rate that is used on average with the current *Quality* setting.
Quality	Constant Quality Mode (CQM) only	Reflects the amount of compression. Generally speaking: the higher the quality setting, the lower the compression ratio and the more bits are consumed. This means a trade-off has to be found between the desired quality level and available bandwidth.
Show Preview>>	Click to view live images and see the effect of the current settings.	
<<Hide Preview	Closes the preview. This may improve webpage responsiveness.	

11.5.3 Advanced

Video > Live View > Advanced

Item	Description	
Frame rate divider	Relates to the frame rate configured in the Encoder Settings section.	
X-resolution	Variables that enable you to freely set picture resolution instead of using the resolution presets in the Encoder Settings section.	
Y-resolution		
Meta data insertion mode	Determines the method used to add meta data to the stream. For details, see the section on Meta Data Insertion.	
	Disabled	No meta data added to the stream.
	Fixed interval	Activates *Meta data insertion interval* parameter (below).
	Each frame	Data block is added after each frame.
Meta data insertion interval	Range: [100-10000] ms. Sets the (fixed) interval at which meta data is added to the stream. Activate this parameter by setting *Meta data insertion mode* (see above) to *Fixed interval*.	

11.6 OSD
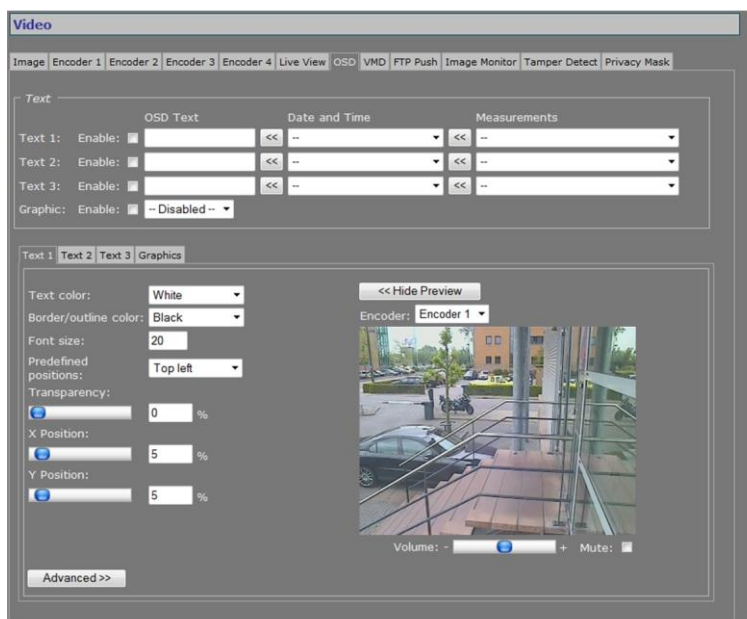
Video > OSD

11.6.1 OSD facilities

The BC620WDR features programmable on-screen display (OSD) facilities. One graphic and up to three OSD text bars can be displayed, each of which can be independently configured. Visual feedback is provided in the preview.

11.6.2 Text Settings

Item	Description
Enable	All OSD objects can be enabled and configured separately. To (temporarily) remove a bar or graphic from the screen, clear the Enable check box.
OSD text	The text to be displayed. Maximum: 255 characters. Text is displayed in a single line. The number of characters visible on screen is determined by the font size and the space offered by the screen line.
Date and Time	Select a format from the list and click the Append button to add the information to the OSD text box.
Measurements	Select a measurement from the list and click the Append button to add the information to the OSD text box.
Graphic	Graphics that have been uploaded to the module (see Graphics tab, Advanced settings) can be selected from the list and enabled.

11.6.3 Text
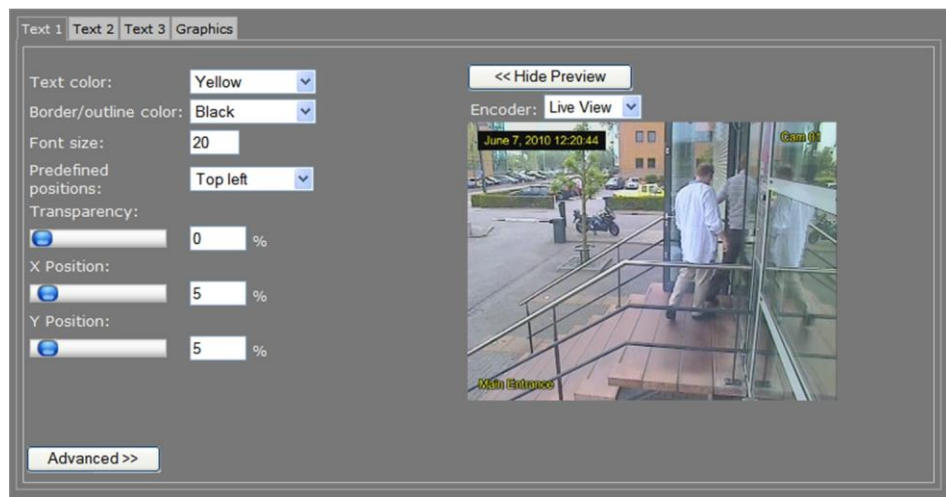
Video > OSD >Text 1, with 3 OSD bars in the preview.
Render modes: 'Border' (top left) and 'Outline' (top right & bottom left)

| Item	Description
Text color	Changes made here and in the other fields are immediately written into the device and reflected in the preview.
Border/outline color	
Font size	Range: [0...256].
Predefined positions	Presets for positioning the OSD object.
Transparency	Drag the sliding button or enter a percentage.
X Position	Variables that enable you to freely position the object, instead of using the presets. Drag the sliding buttons or enter a percentage. When a preset has been selected, changing one of its defined parameters sets the *Predefined positions* box to '--', indicating that a custom position has been configured.
Y Position	
Show Preview>>	Click to view live images and see the effect of the current settings.
<<Hide Preview	Closes the preview. This may improve webpage responsiveness.
Encoder	The encoder handling the images seen in the preview.

11.6.3.1 Advanced

Video > OSD > Text 1 > Advanced > Advanced OSD Bar 1 Settings

Item	Description
Font name	Offers a selection from default and uploaded fonts (see Font Management).
Render mode	*Outline* or *Border*.
X-Position anchor point	Variables that enable you to shift the OSD object relative to the anchor point.
Y-Position anchor point	
Rotation angle	Background size automatically adjusts to text dimensions when a bar is rotated.

Video > OSD > Text 1 > Advanced > Font Management

⇥ **To upload a font**

1. In the Font management section, click **Browse**.
   The Open dialog box displays.
2. Browse to the folder containing the font to be uploaded.
3. Select the correct file (.ttf extension), and then click **Open**.
   The file appears in the File text box on the web page.
4. To start the upload, click **Add**.
   The new font is added to the Font list and to the Font name list in the Advanced OSD Bar # Settings section.

⇥ **To remove a font**

1. In the Font management section, select the font.
2. Click the **Del** button.

11.6.4   Graphics
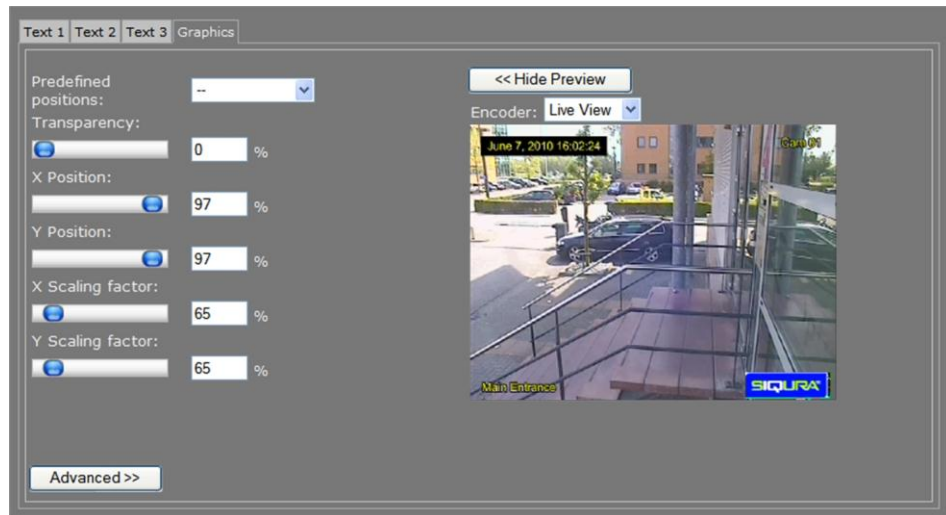
Video > OSD > Graphics, with 3 OSD bars and a graphic (bottom right) in the preview

The Graphics tab enables you to manage graphics, and scale and position a selected graphic on your screen.

Item	Description
Predefined positions	Presets for positioning the OSD object.
Transparency	Drag the sliding button or enter a percentage.
X-Position	Variables that enable you to freely position the object, instead of using the presets. Drag the sliding buttons or enter a percentage. When a preset has been selected, changing one of its defined parameters sets the *Predefined positions* box to '--', indicating that a custom position has been configured.
Y-Position	
X Scaling factor	Variables that enable you to freely configure the dimensions of the object.
Y Scaling factor	
Show Preview>>	Click to view live images and see the effect of the current settings.
<<Hide Preview	Closes the preview. This may improve webpage responsiveness.
Encoder	The encoder handling the images seen in the preview.

11.6.4.1 Advanced

Video > OSD > Graphics > Advanced > Advanced Picture Settings

Item	Description
X-Position anchor point	Variables that enable you to shift the OSD object relative to the anchor point.
Y-Position anchor point	
Animation speed scaling factor	Enables you to set the speed for an animated GIF graphic.
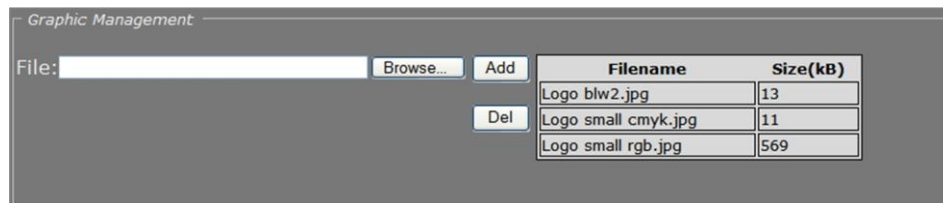
Video > OSD > Graphics > Advanced > Graphic Management

➼ **To upload a graphic**

1. In the *Graphic Management* section, click **Browse**.
   The *Open* dialog box displays.
2. Browse to the folder containing the graphic to be uploaded.
3. Select a file with the correct file extension (.bmp, .gif, .jpg, jpeg), and then click **Open**.
   The file appears in the *File* textbox.
4. To start the upload, click **Add**.
   The graphic is added to the graphics list and to the *Graphic* drop-down list in the *Text* section.

➼ **To remove a graphic**

1. In the *Graphic Management* section, select the graphic.
2. Click **Del**.

11.7 VMD
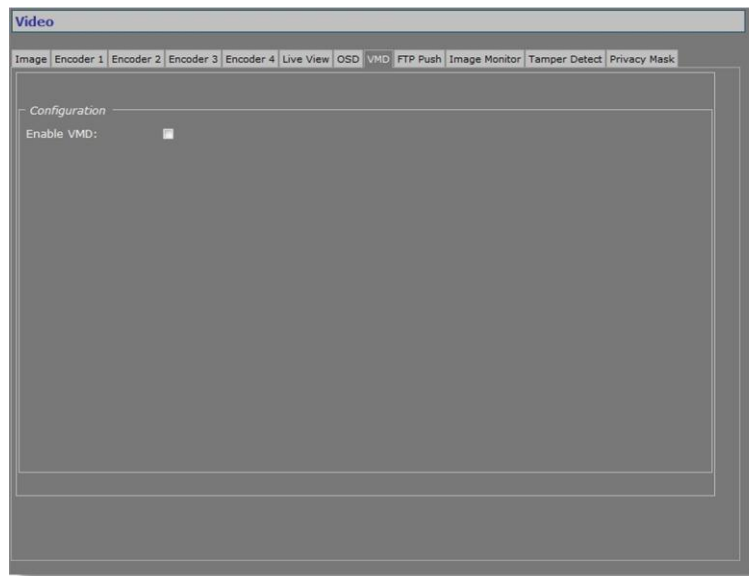
Video > VMD

Video Motion Detection (VMD) enables the user to define a portion or portions of the screen and to detect picture changes there. These changes could be caused by motion or varying lighting, for example. Regions of less interest can be masked.

11.7.1 VMD startup

⏩ **To start Video Motion Detection**
1. On the Video page, click the **VMD** tab.
2. Select **Enable VMD** to activate the detection process.
   Depending on the current VMD settings, a VMD alarm will be generated on changes in the picture.

11.7.2   Configure detection parameters
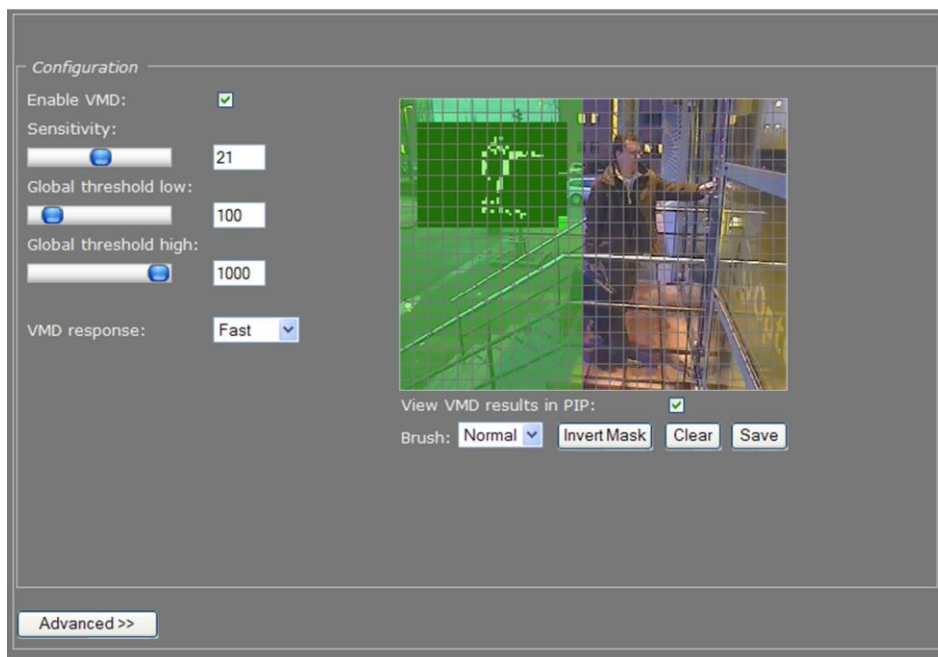
Video > VMD > Configuration

VMD enabled: Configuration section with controls, video picture, and motion detection inset, the latter with mask applied. The mask permits motion detection in the right half of the picture only, at the top of the stairs, so passers-by and cars would not be registered by the detector facility; neither will the details in the background (the trees are reflected in the window pane though, and this could be masked separately).

Item	Description
Enable VMD	Expands the Configuration section, as shown in the above figure.
Sensitivity	This setting relates to local detection levels: local change is only detected if its level exceeds a certain value. The sensitivity setting can be used to eliminate unwanted ('false') triggering (e.g. caused by background noise or constant local movement).
Global threshold low Global threshold high	These settings relate to the summed amount of change within fully or partly unmasked portion(s) of the screen; a value between the two thresholds gives rise to a corresponding VMD alarm. The level of this alarm can be set (A-N) using separate Siqura software.
VMD response	*Fast* or *Filtered*. Filtering is used to suppress a single peak as false triggering.

11.7.3   Set the mask

❱❱ **To set a mask**

‣ To edit the mask, click on the grid that is put over the image.
One or more mask elements at, and possibly around, that position, are produced.
‣ Hold the standard mouse button and drag, to 'brush' (i.e. mask) larger areas, with a 'Normal', 'Small', or 'Large' brush.
‣ Use the 'Invert Mask' button to reverse a selection.
‣ Hold the right mouse button and drag, to erase mask areas.
‣ Use the 'Save' button to store the mask in the unit.

❱❱ **To delete a mask**

‣ Press the **Clear** button.
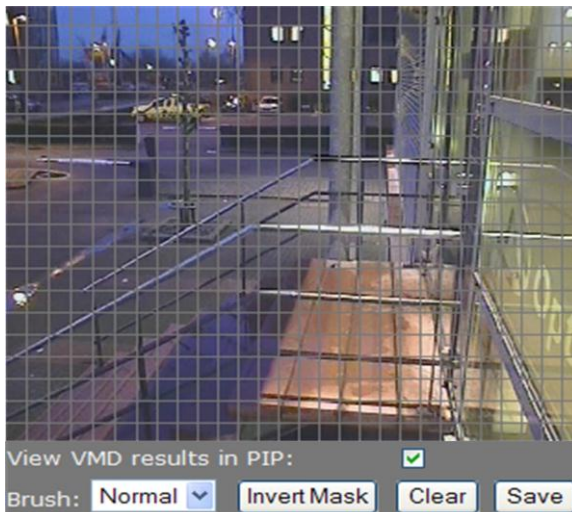
Masking grid

Item	Description	
Brush	*Normal*	Allows grid elements to be accessed in 4-element groups.
	Large	Allows grid elements to be accessed in 16-element groups.
	Small	Allows grid elements to be accessed one at a time.
Invert Mask	Enables you, for example, to start creating a mask by marking the (smaller) area(s) you *do* wish to monitor and then use this button to reverse the selection.	
View VMD results in PIP	Inserts the Video Motion Detection inset providing feedback on current VMD settings.	
Clear	Clears the mask.	
Save	Makes the current mask effective and stores it for later use.	

11.7.4   VMD detection window

The VMD detection window shows up as a small picture within the larger picture. Depending on the thresholds set, the motion detection bar on the right side of the picture shows up green or red (see figures below), the latter indicating a VMD alarm will be generated. In the pictures, the upper and lower thresholds are shown as two white markers. If the bar runs over the highest marker, it will turn green again and there will be no alarm condition.
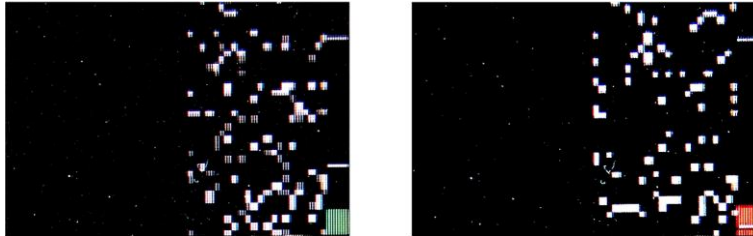
VMD detection windows, with mask applied to the left half of the window. The small white blocks indicate grid elements where change occurred above the sensitivity level. The summed change is reflected in the bars on the right, the green one (left) not reaching the lower threshold. The red one (right picture) extending past it, since this threshold is set much lower.

11.7.5   VMD alarm

If movement is detected, a module alarm (VMD) will be generated and sent out over the network using the (unsolicited) notification mechanism. Such alarms can be caught using appropriate software.

11.7.6   Advanced

Video > VMD > Advanced > VMD

Item	Description
Frame rate divider	Range: [1...100]. Used to determine the number of frames used for VMD. Only 1 divided by this value frames are evaluated.
Delay	Range: [1...10] frames. The delay in frames between the currently processed frame and the stored frame with which it is to be compared.
Event window size	Range: [1…32]. Number of frames evaluated at a time to determine if there is a VMD alarm.
Event window low mark	Range: [0…31]. Thresholds determining if there is a VMD alarm.
Event window high mark	
Feedback position	Enables you to position the detection window (not to be confused with an event window).

Note on Advanced VMD Settings: Motion is detected by comparing the current frame with a reference image (e.g. a previous frame) and calculating the difference between the two. The value you enter for the *Event window size* parameter determines how many frames are evaluated for VMD purposes at a time. Not all frames from the original video stream are used for VMD. Only *1 divided by the value set for the frame rate divider* frames are evaluated.

A VMD event becomes active when, within the Event window, the number of frames with motion exceeds a configurable value, the *Event window high mark*. After this, the VMD event will remain active until the number of frames with motion drops below another configurable value, the *Event window low mark*.
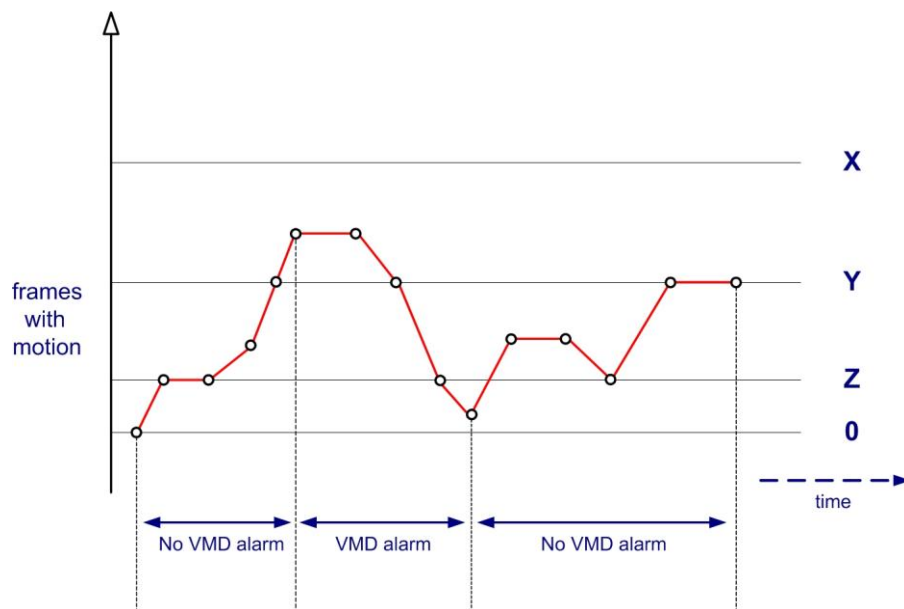
VMD Alarm: Event window high/low mark
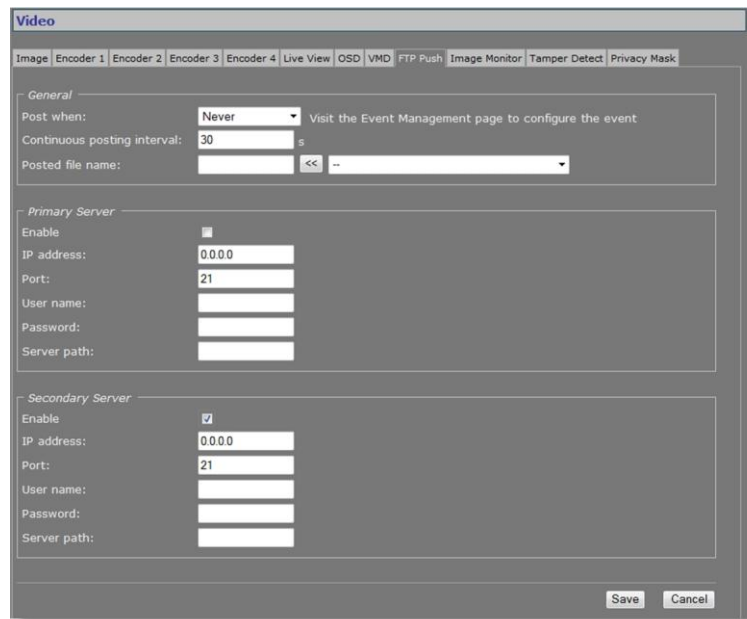
X = Event window size
Y = Event window high mark
Z = Event window low mark

VMD alarm becomes active when in at least Y out of X frames motion is detected.
VMD alarm becomes inactive when in at least Z out of X frames *no* motion is detected.

11.8   FTP Push

Video > FTP Push

11.8.1   Post JPEG images

The BC620WDR can be configured to upload images, generated by its Live View encoder, to an FTP server. Posting the files in JPEG format can be set to be continuous or event-triggered. On the Event Management page, one or more events can be associated with FTP Push.

11.8.2　General

Item	Description	
Post when	*Never*	No image posting
	Event On	Image is posted when configured event occurs.
	Event Off	Image is posted when configured event ceases.
	Event Changed	Images are posted when configured event occurs or ceases.
	Continuous	Posting not associated with any event. Images are sent continuously at the frequency set for the *Continuous posting interval* parameter.
Continuous posting interval	Range: [1-300] s. Applies to continuous posting only. Determines the frequency of image posts.	
Posted file name	Enter a descriptive name. Use the Append list and button (<<) to include extra information to identify the files. The "$", "#", and "@" symbols described below can also be typed directly after the name.	
Append list	Options to add information and file extension to the file name entered.	
	<UTC-Time/date>.jpg	Time/date. Appended as "_$.jpg".
	<SeqNr>.jpg	Sequence number. Appended as "_#.jpg".
	<SeqNr>_<UTC-Time/date>.jpg	Sequence number and time/date. Appended as "_#_$.jpg".
	<SeqNr>_<Event State>.jpg	Sequence number and event state. Appended as "_#_@.jpg". Examples of event state: T=true, F=false.
	<UTC-Time/date>_<Event State>.jpg	Time/date and event state. Appended as "_$_@.jpg".

11.8.3　FTP server

A target FTP server must hold a user account associated with the BC620WDR. You can assign a primary server and a secondary server. Images are posted simultaneously to both the primary server and secondary server.

Video > FTP Push > Primary Server, example settings

Item	Description
Enable	Select or clear to respectively enable/disable the connection with this server.
IP address	IP address of the FTP server.
Port	The FTP protocol typically uses port 21 on the FTP server to listen for clients initiating a connection. Port 21 is also where the server is listening for commands issued to it.
User name	The authorization to access the FTP server.
Password	
Server path	Folder on the FTP server assigned to the FTP client. To be used, for example, if the client is not allowed to access the server root folder.

11.8.4　Event management

Having selected *Event On*, *Event Off*, or *Event Changed* as a trigger, do not forget to go to the Event Management page to associate one or more events with the FTP push.

Event Management > FTP Push 1. Two inputs associated with FTP Push.

11.8.5 Monitor and troubleshoot FTP Push

You can monitor FTP push on the Measurements tab of the Status page. Measurements on this tab are continuously updated. In the FTP Push section, you can compare the number of incoming triggers with the number of succeeded posts.

```
FTP Push 1
Nr of incoming triggers            23
Nr of succeeded posts, server 1    22
Last post status, server 1         OK
Nr of succeeded posts, server 2    0
Last post status, server 2         N/A
```

Status > Measurements > FTP Push 1

If you need to troubleshoot the file upload process, the messages reporting the last post status will in most cases point you to possible causes of problems.

```
FTP Push 1
Nr of incoming triggers            154
Nr of succeeded posts, server 1    0
                                   ftpput:
                                   unexpected server
Last post status, server 1         response to STOR:
                                   550 Filename
                                   invalid
Nr of succeeded posts, server 2    0
Last post status, server 2         N/A
```

Last post status: example of error message

11.9   Image Monitor
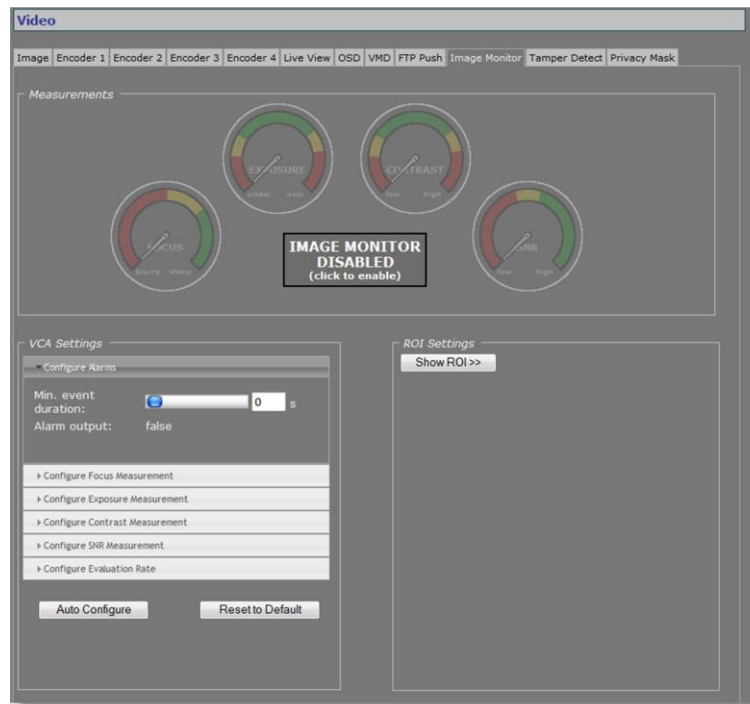
Video > Image Monitor

11.9.1   Image quality check

The Image Monitor can detect if images produced by the camera are still usable. It can give an indication of the performance of the camera and show whether or not it needs attention. A quality check is made against what is normally a good picture.

Examples of detectable occurrences:
‣ The camera is in focus during sunny days, but out of focus in low light situations.
‣ The initial daytime camera position seemed ok, but streetlights and spot lights affect the image during nighttime.
‣ The lens has got dirty.
‣ The iris control has got stuck.
‣ Camera failure.

11.9.2   Enable the Image Monitor

The Image Monitor can measure camera focus, exposure, contrast level, and SNR
(Signal-to-Noise Ratio). The four measurements are disabled by default. You can enable them
simultaneously or separately.

Note: Enabling/disabling a measurement also enables/disables the associated alarm.

▸▸ **To enable all measurements simultaneously**

▸ In the *Measurements* section, click **IMAGE MONITOR DISABLED**.
The four dials are activated, the pointers indicating the current measurements.

Image Monitor: all measurements enabled

▸▸ **To enable/disable individual measurements**

1. In the VCA Settings section, click the accordion style menu labelled with the measurement
you require.
The settings of the selected measurement display.
2. Select/Clear the **Enable** box to enable or disable the measurement, respectively.
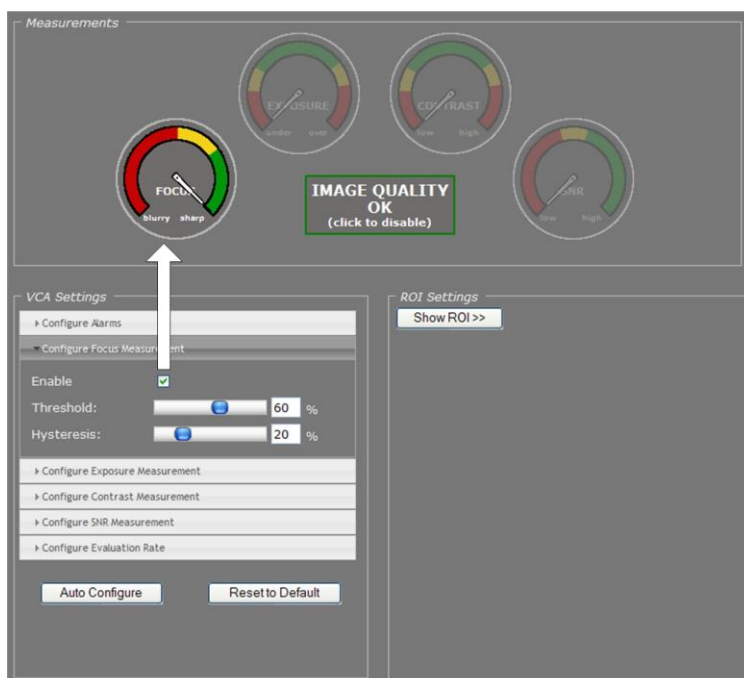
Image Monitor: FOCUS measurement enabled only

11.9.3   Dial legend

The coloured dials in the Measurements section provide a quick and easy glance at the health of the camera. You can fine-tune each measurement's alarm thresholds to your needs in the VCA Settings section.

Dial legend
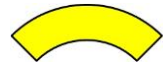
	Error state.
	Hysteresis: the area where the alarm output is either "true" or "false" depending on the preceding alarm state, as illustrated in the figure below.
	Correct camera performance.
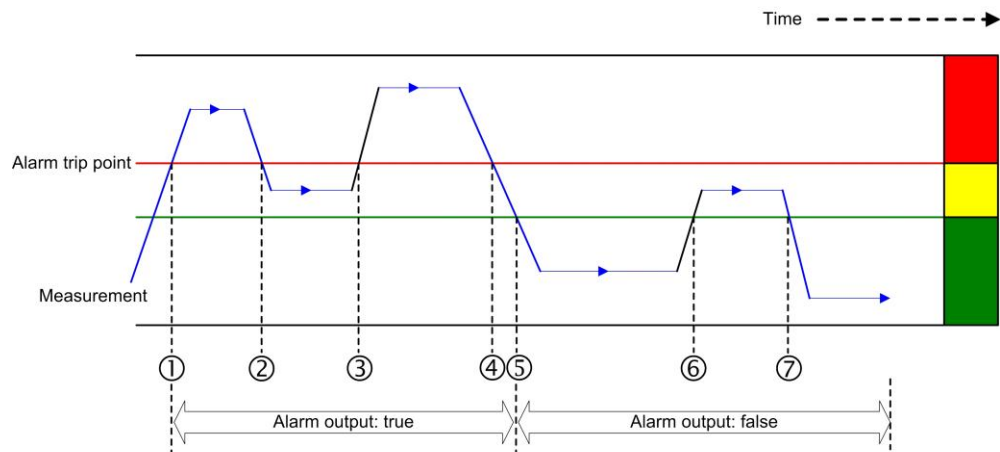
Hysteresis and alarm output

1   The Measurement rises above the trip point. After expiry of the delay set for the Min. event duration, the alarm is activated.

2   The Measurement drops into the Hysteresis area (i.e. the margin between incorrect and correct performance) but falls short of the "safe" area. The alarm is continued.

3   The Measurement re-enters the Error state area. The alarm continues.

4   The Measurements drops into the Hysteresis area. The alarm continues.

5   Camera performance is correct. The alarm is deactivated after expiry of the *Min. event duration*.

6   The Measurement rises into the Hysteresis area. The alarm trip point is not reached. Alarm output remains "false".

7   Camera performance is correct. Alarm output remains "false".
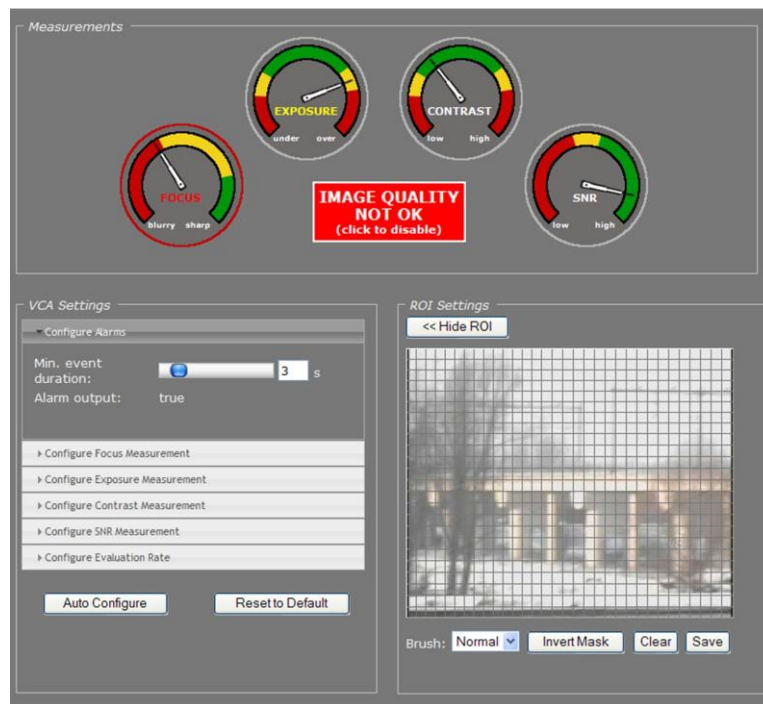
Image Quality not OK: Alarm output = true

The red circle around the Focus dial in the figure above indicates that the alarm is raised by the Focus measurement. The Exposure dial has no red circle, although the pointer is in the Hysteresis area. This shows that Exposure was correct before and that this measurement in itself is not the cause of the alarm.

Note: In addition to the visual indications on the web pages, alarms can also be read from the BC620WDR 's internal Management Information Base (MIB) using appropriate software, or through Siqura's Open Streaming Architecture (OSA) - that is, the "PTZ Camera and Codec Programming Interface" (API). The BC620WDR includes SNMP support for its image monitor and tampering detection. A trap is sent when bad image quality or camera tampering has been detected and another one when the situation returns to normal. This support requires a new SNMP MIB, the OPTC-VCA-MIB, which can be downloaded at www.siqura.com.

11.9.4　Measurements configuration
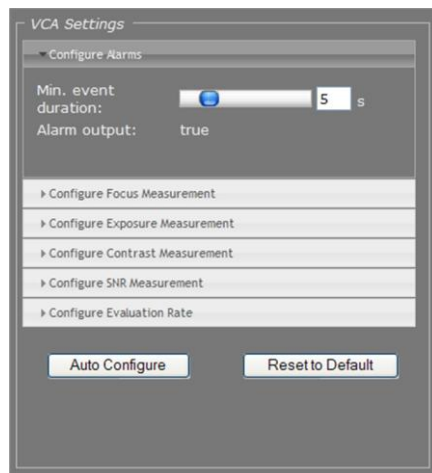
Video > Image Monitor > VCA Settings

The default Measurements values will mostly work well for you. If you do need to modify them you can do so in the VCA Settings section.

Item	Description		
Configure Alarms	*Min. event duration*		Alarm output delay time: the time span that is to elapse before a continued change in conditions actually activates/deactivates the alarm output.
	Alarm output		*True* or *False*. Indication of current status.
Configure Focus Measurement	Allow you to enable/disable each measurement separately and customise its alarm threshold and hysteresis to your requirements.		
Configure Exposure Measurement			
Configure Contrast Measurement			
Configure SNR Measurement			
Configure Evaluation Rate	The value entered here determines the speed at which the host machine processes the algorithms underlying the measurements. Higher values take up more CPU power.		
Auto Configure	Adjusts the alarm thresholds, based upon the current measurements. The green area is centred around the current pointer position.		
Reset to Default	Restores the original thresholds. Does not affect the current activity status of the measurements (i.e. being Enabled or Disabled).		

Tip: A PTZ camera moving from one preset to the next may trigger an alarm if the scene change takes too long. Setting an appropriate time for the Min. event duration parameter can delay the alarm output until the camera has adopted the new position and the alarm condition has ceased.

➠ **To configure a measurement**

1. In the *VCA Settings* section, click the button for the measurement you wish to configure.
   The measurement's settings display.
2. Select the **Enable** box, if necessary.
3. Set the alarm threshold to your requirements.
   Note that you can set two thresholds for *Exposure* (under- and overexposure) and *Contrast* (low and high contrast).
4. Set the Hysteresis.
5. Click the **Configure Alarms** button and set the *Min. event duration*, if desired.
6. Click the **Configure Evaluation Rate** button and modify this setting, if desired.

11.9.5   Region of Interest (ROI)
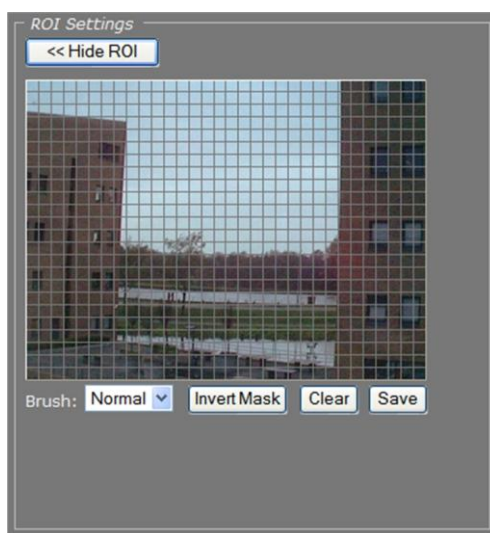
Video > Image Monitor > ROI Settings

ROI preview

Pressing Show ROI>> in the ROI Settings section opens a preview with a grid overlay. You can use it to mask portions of the image you wish to exclude from monitoring. Certain regions can disrupt the measurements or be of no importance. You may want to filter out a bright source of light, a region with low contrast, or differences in focus, for example. The part of the image that you have *not* selected on creating the mask is called the Region of Interest (ROI).

➠ **To set a mask**

▸ To edit the mask, click on the grid that is put over the image.
   One or more mask elements at, and possibly around, that position, are produced.
▸ Hold the standard mouse button and drag, to 'brush' (i.e. mask) larger areas, with a 'Normal', 'Small', or 'Large' brush.
▸ Use the 'Invert Mask' button to reverse a selection.
▸ Hold the right mouse button and drag, to erase mask areas.
▸ Use the 'Save' button to store the mask in the unit.

➠ **To delete a mask**

▸ Press the **Clear** button.

Item	Description	
Brush	*Normal*	Allows grid elements to be accessed in 4-element groups.
	Large	Allows grid elements to be accessed in 16-element groups.
	Small	Allows grid elements to be accessed one at a time.
Invert Mask	Enables you, for example, to start creating a mask by marking the (smaller) area(s) you *do* wish to monitor and then use this button to reverse the selection.	
Clear	Clears the mask.	
Save	Makes the current mask effective and stores it for later use.	

11.10 Tamper Detect
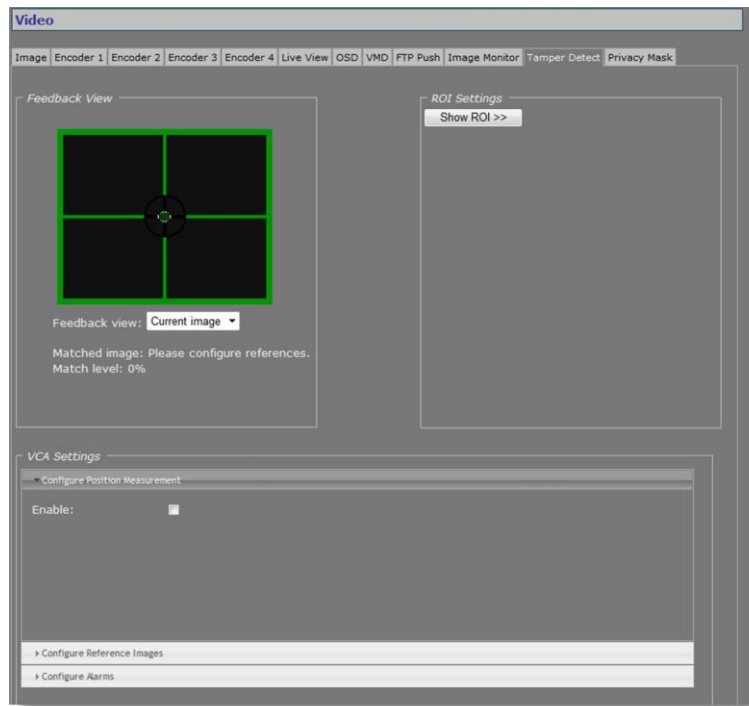
Video > Tamper Detect

11.10.1 Camera movement and scene changes

As a result of tampering, or more accidentally, after cleaning, a camera may no longer cover the area designated for monitoring. The Tamper Detect function can detect camera position changes and scene changes such as a blocked camera view, for example. It does so by comparing the current image to one or more reference images that were captured and stored earlier.

11.10.2 Enable Tamper Detect

Tamper Detect is disabled by default.

▸ **To enable Tamper Detect**

  ▸ In the *VCA Settings* section, select **Enable**.
    The Position Measurement settings are opened.

Important: If no reference images have been stored yet, a BLOCKED OR CHANGED SCENE alarm displays in the Feedback View. Tamper Detect cannot find a match with the current image. You will need to create one or more reference images first.
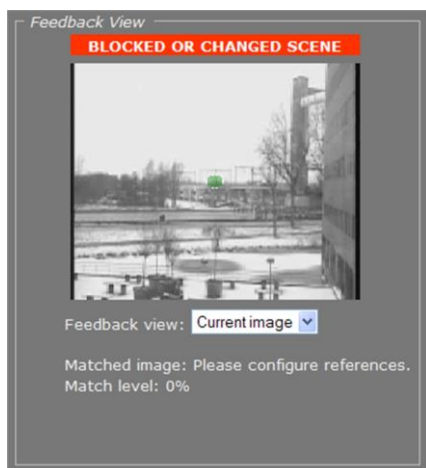
Tamper Detect enabled: No reference images found

11.10.3 Reference images

You can create up to 16 reference images. This enables you to store images captured in different day/night situations and/or from multiple PTZ preset positions. When the camera moves to a different preset Tamper Detect tries to match the new scene to the available reference images.

11.10.3.1 Create a reference image

▸ **To create a reference image**

1. In the *VCA Settings* section, click **Configure Reference Images**.
2. Open the **Reference image** list, and then select the image you want to create.
3. Enter a descriptive name in the *Label* box.
4. Enter a value (in seconds) for the *Sampling duration*.
   This parameter enables you to capture the background of a scene only and have specific elements such as moving objects filtered out of the image. With a longer time span for the sampling duration, persons passing in front of the camera, for example, or cars driving on a highway can be smoothed out to prevent them from triggering a changed scene alarm.
5. Click the **Sample reference** button.
   The current image is sampled.
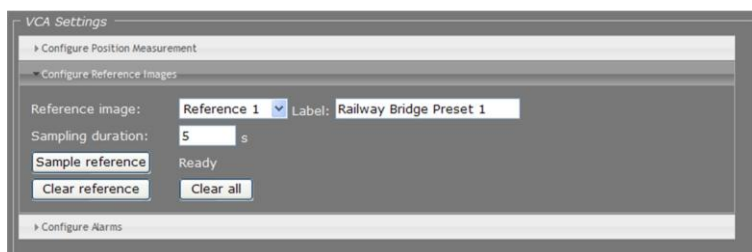
Reference image 1 created

11.10.3.2 Mask the ROI

You can use the ROI settings section to exclude portions of the image from monitoring, as explained earlier in the Region of Interest section.

Region of less interest masked

11.10.3.3 Image comparison

Tamper Detect compares the current scene with all available reference images. If a match is found a green crosshair is superimposed on the image in the Feedback view. Information about the matched image and the match level is displayed under the Feedback view.

The small green circle in the middle of the image indicates the amount of camera movement that is allowed. A position alarm is raised when the green circle is outside the crosshair centre. For information about adjusting the amount of allowed camera movement, see Position Measurement.

If no match is found a BLOCKED OR CHANGED SCENE alarm is raised.
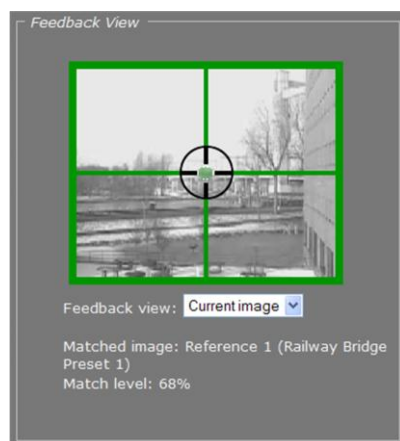
Current image matches Reference 1
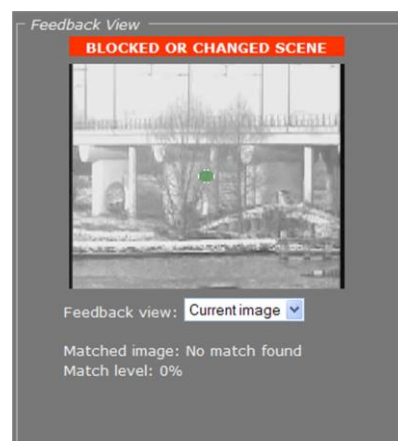
Reference image(s) available. No match found with current image, though.

The drop-down list in the Feedback View section can be used to display the current image, the best matching reference image, or a specific reference image.
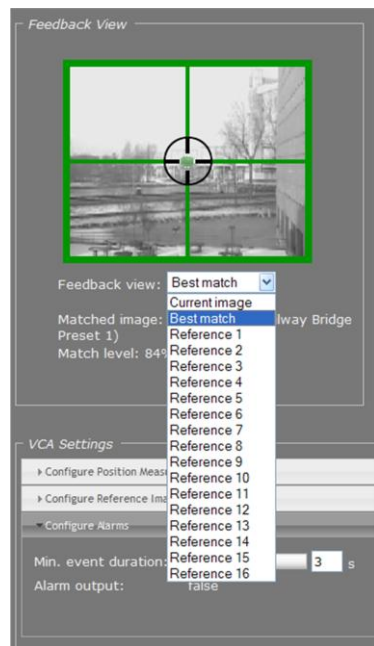
Feedback view list

11.10.3.4 Delete a reference image

▸ **To delete a reference image**

1. In the *VCA Settings* section, open the **Reference image** list.
2. Select the image you wish to delete.
3. Press **Clear reference**.
   Note that the *Clear all* button deletes *all* available references.

11.10.4   Position measurement

Video > Tamper Detect > Position Measurement

After creating one or more reference images you can configure the Position Measurement settings to define thresholds for allowed camera movement and image matching.

Item	Description
Enable	Enables Tamper Detect functionality.
Match threshold	The current image and the reference image it is compared with are considered a match upon reaching the degree of similarity specified here. The lower the percentage entered for this parameter, the fuzzier the match.
Match hysteresis	This is the margin area where there is either a match or no match, depending on the preceding match level. If your alarm output frequently alternates between "true" and "false" you can use this parameter to fine-tune your settings. For more information on hysteresis, see also Dial legend.
Position threshold	Determines the amount of camera movement that is allowed before a position alarm is raised. Raising this value allows more camera movement. This is indicated by the increased size of the green circle in the center of the image.
Evaluation rate	The value entered here determines the speed at which the host machine processes the algorithms underlying the measurements. Higher values take up more CPU power.
Defaults	Restores the original settings. Does not affect the current activity status of Tamper Detect - that is, being Enabled or Disabled.

11.10.5 Alarms

Video > Tamper Detect > Configure Alarms

The Configure Alarms section enables you to view the current status of the alarm output and to set a delay for the activation/deactivation of alarm outputs.

Note: In addition to the status indication in this section, alarms can also be read from the BC620WDR 's internal Management Information Base (MIB) using appropriate software, or through Siqura's Open Streaming Architecture (OSA) - that is, the "PTZ Camera and Codec Programming Interface" (API). The BC620WDR includes SNMP support for its image monitor and tamper detect functions. A trap is sent when bad image quality or camera tampering has been detected and another one when the situation returns to normal. This support requires a new SNMP MIB, the OPTC-VCA-MIB, which can be downloaded at www.siqura.com.

Item	Description
Min. event duration	Alarm output delay time: the time span that is to elapse before a continued change in conditions actually activates/deactivates the alarm output.
Alarm output	*True* or *False*. Indication of current status.

Tip: A PTZ camera moving from one preset to the next may trigger an alarm if the scene change takes too long. Setting an appropriate time for the Min. event duration parameter can delay the alarm output until the camera has adopted the new position and the alarm condition has ceased.

11.10.5.1 Alarm examples
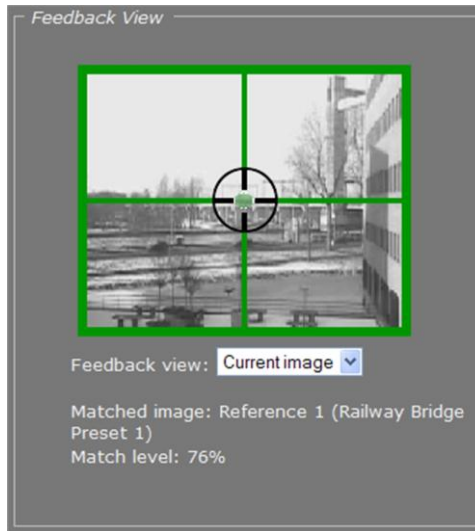
Original camera position
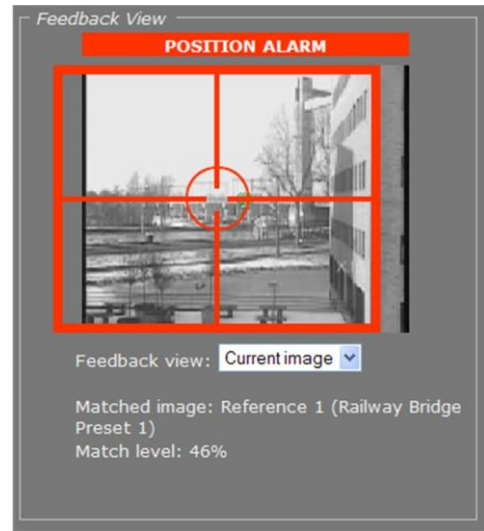
Camera has moved to the right. Although the current image still matches Reference 1, the changed camera position results in a position alarm.
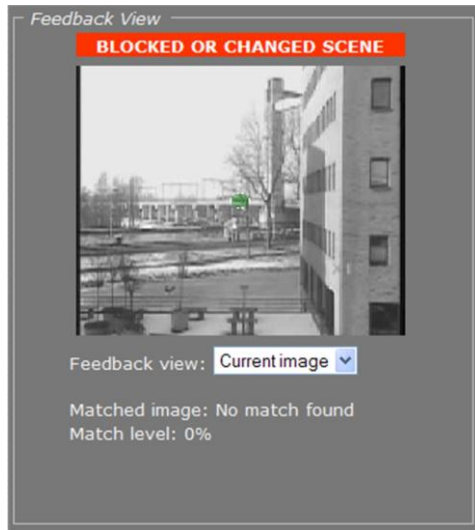
Camera has moved further to the right. Current image no longer matches any reference image, resulting in a changed scene alarm.
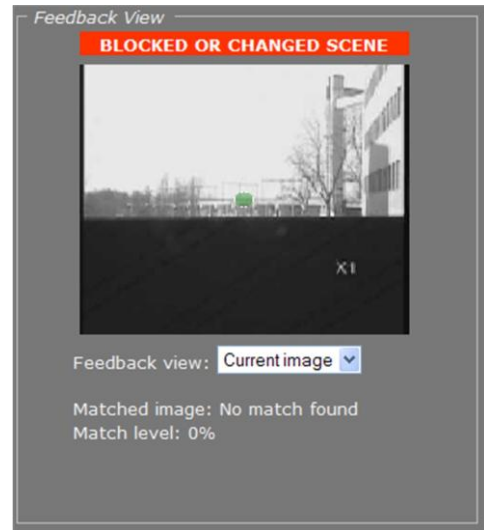
Blocked scene alarm

11.11 Privacy Mask
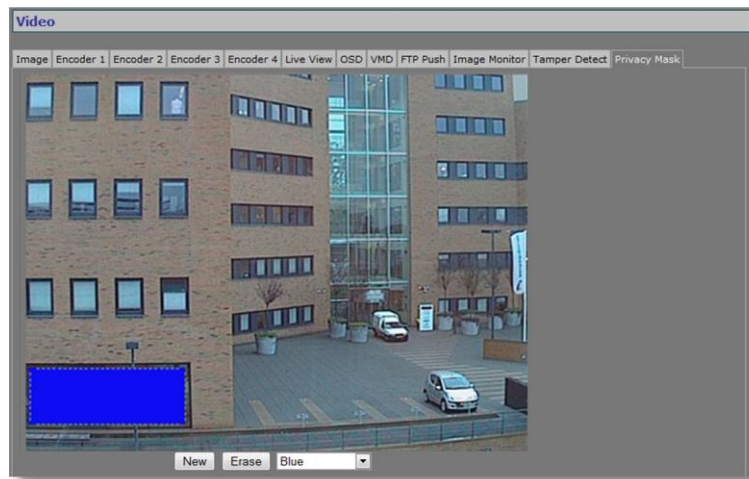
Video > Privacy Mask

The privacy mask function aims to avoid intrusive monitoring. The BC620WDR supports up to 10 masks.

▸ **To create a privacy mask**

1. On the *Video* page, click the **Privacy Mask** tab.
2. Under the preview, click **New**.
    A square mask appears as an overlay in the centre of the preview.
3. Use the pointer to position and size the mask.
    If desired, click to select the mask, and then select a mask colour from the list under the preview.

▸ **To delete a mask**

1. On the *Video* page, click the **Privacy Mask** tab.
2. Using the pointer, select the mask in the preview.
3. Click **Erase**.

12 Audio

This chapter describes the functionality and settings found on the Audio page of the BC620WDR.

In This Chapter

12.1 Enable audio
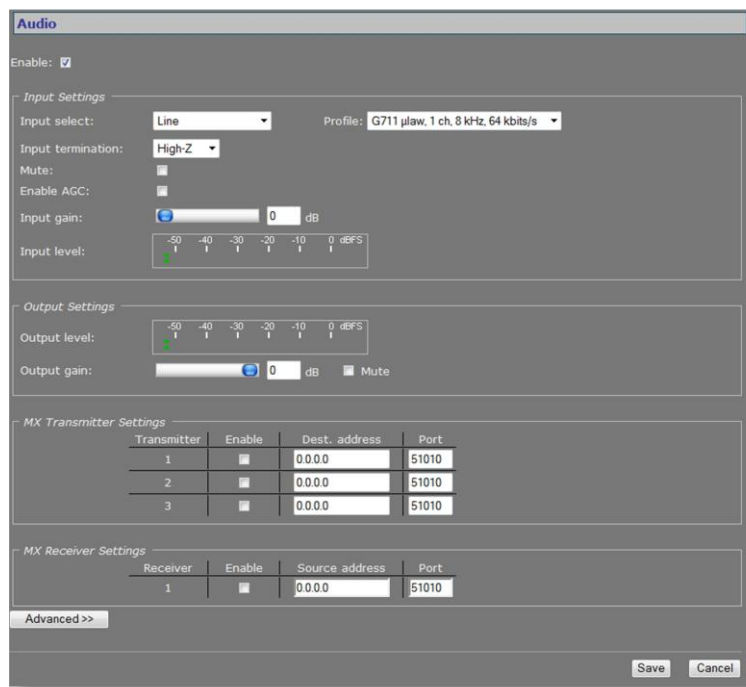
Audio page

Using the *Enable* check box at the top of the Audio page, you can enable/disable the entire audio functionality (the latter, for example, to prevent unwanted eavesdropping). Remember to *Save* the configuration to make it effective.

12.1.1 Input Settings

Item	Description
Input select	*Line*, *Microphone*, or *Microphone + bias*.
Input termination	Can be set to High-Z or 600 ohms, to match audio source. Single-ended.
Mute	Audio on/off.
Enable AGC	To adjust the gain to an appropriate level, Automatic Gain Control reduces the volume if the signal is strong and raises it when it is weaker.
Input gain	Range: [0…30] dB. Is disabled when AGC is enabled. Drag the sliding button or type a value. Gain control reacts directly, without the need to press *Save*.
Input level	VU meter to display audio input level.
Profile	Preset combinations of settings. A non-standard setting configured through the Advanced Settings gives '--' in the Profile selector.
	G711 A-law. 1 ch. 8 kHz 64 kbit/s ▸ default setting ▸ mainly used in Europe ▸ mono, low quality ▸ used for QuickTime
	G711 µ-law. 1 ch. 8kHz. 64 kbit/s ▸ mainly used in USA ▸ mono, low quality ▸ used for Genetec's Omnicast
	Legacy PCM ▸ 2 channels (stereo) ▸ high quality, 15.7 kHz ▸ compatible with all Siqura products (including C-20, C-40, S-40)

12.1.2 Output Settings

Item	Description
Output level	VU meter to display audio output level.
Output gain	Range: [-80…0] dB.
Mute	Select or clear this box to respectively mute or unmute audio.

12.2 Make audio connections

Audio > MX Transmitter and MX Receiver Settings, two-way audio

Audio streams

The BC620WDR provides bidirectional audio. The BC620WDR can send three audio streams to different destinations, multicast or unicast, to an A-80, or any C-/S-series codec with an audio interface. It can also receive one audio stream from an A-80 or any C-/S-series codec that features audio.

Highlighted fields

The source address and port number fields are highlighted in green when the enabled receiver receives a stream from the specified source. The two fields are marked in red when no stream is received with the receiver enabled and correctly configured.

Two-way audio

The figure above shows the setup for two-way audio on the side of the BC620WDR. The device on the other side of the connection (with the IP address 172.22.250.131) would need similar settings, that is - it must hold the IP address of the BC620WDR as the destination and source. Transmitters and receivers must be enabled in order for streaming to start. Remember to *Save* a configuration to make it effective.

12.2.1 MX Transmitter Settings

Item	Description
Enable	Select/Clear to enable/disable the stream transmission, respectively.
Dest. address	IP address of the codec that will receive the stream.
Port	The local port number of the codec that will receive the stream.

12.2.2 MX Receiver Settings

Item	Description
Enable	Select/Clear to enable/disable the stream reception, respectively.
Source address	IP address of the codec that will transmit the stream.
Port	The local port number of the BC620WDR.

12.3   Advanced

Important: If in doubt about these settings, do *not* change the default values.

12.3.1   Audio Input

Audio Input		
Channels:	1	
Sample rate:	8000	samples/s
Audio detect threshold channel 1:	-10	dB
Audio detect threshold channel 2:	-10	dB

Audio > Advanced > Audio Input

Item	Description
Channels	Range: [1…2]. When selecting 1 channel, only the signal on the 'A1' input is used (either line or microphone).
Sample rate	Range: [7850…48000]. Allows you to enter custom settings (other than those included in the Profile list in the Input Settings section), e.g., for communication with a C-20 codec. Examples: ▸ 7850 Hz A-law ▸ 15710 Hz A-law ▸ 15710 Hz PCM ▸ 43200 Hz PCM
Auto detect threshold channel 1 Auto detect threshold channel 2	Range: [-60…0] dB. The audio level is measured. When the audio level reaches the threshold set here, the audio detect flag is set. This flag can be used to generate a 'silence' alarm or a 'too much noise' alarm.

12.3.2   Audio Output

Audio Output		
Bass:	0	dB
Treble:	0	dB

Audio > Advanced > Audio Output

Item	Description
Bass	Range: [0…18] dB.
Treble	Range: [0…6] dB.

12.3.3   Audio Encoder

Audio > Advanced > Audio Encoder

Item	Description
Audio format	*PCM 16bit, A-law 8bit, µ-law 8bit.*

12.3.4   Audio Decoder

Audio > Advanced > Audio Decoder

Generally speaking, Audio Decoder settings follow the settings of the source - that is, the encoder on the other side of the connection. The settings shown in the figure above are defaults, used when receiving a stream of which the format cannot be determined, for example.

Item	Description
Channels	Range: [1-2]. Default: 1. When selecting 1 channel, the incoming audio stream is sent to both the 'A1' and 'A2' outputs.
Sample rate	Range: [7850…48000]. Examples (for 1 and 2 channels): ▸ *7850 Hz* A-law ▸ *15710 Hz* A-law ▸ *15710 Hz* PCM ▸ *43200 Hz* PCM
Audio format	*PCM 16bit, A-law 8bit, µ-law 8bit.*

12.3.5   Transmitter

Audio > Advanced > Transmitter #

Item	Description	
DSCP field	Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits, up to 64 network service types can be defined. *RFC 2724* (*http://www.ietf.org/rfc/rfc2474.txt*) describes the Differentiated Services (DS) field and the DiffServ Code Point. See also the note on Differentiated Services later in this chapter.	
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).	
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.	
RTP control mode	Select the transport protocol to control the stream.	
	None	No transport protocol selected.
	FloodGuard	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.
	RTCP	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.
Stream type	*UDP + RTP*	Default setting. Plain RTP stream over UDP.
	UDP + RTP + NKF	Adds an extended RTP header for Siqura applications requiring extra information.
RTP type (0 = auto)	Default value: [0]. This parameter determines the RTP payload format (e.g. H.264, MPEG-2/4, or audio). To avoid an RTP type conflict, the values specified on both sides of the connection must be the same. The default value of "0" automatically sets the appropriate media type. You are advised not to change this setting.	
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.	

12.3.6   Receiver 1

Audio > Advanced > Receiver 1

Item	Description		
Filter on source port	Can be used to filter incoming signals. With multiple signals sent to the same IP address and destination port number, *Filter on source port* can be used to filter the input, i.e. to accept only signals from the transmitting port specified here. The filter will not be active if set to 0 (the default and recommended setting).		
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).		
Reorder buffer size	Used to reorder incoming packets.		
Stream fail delay	Range: [0...10000] ms. Default: 300 ms. Timeout in ms before going to NoStream state.		
RTP control mode	Select the transport protocol to control the stream.		
	None	No transport protocol selected.	
	FloodGuard	Flooding prevention mechanism. For more information, see the note on FloodGuard later in this chapter.	
	RTCP	Real-Time Control Protocol, a network control protocol for use in communications systems to control streaming media servers.	
RTP type (0 = auto)	Default value: [0]. This parameter determines the RTP payload format (e.g. H.264, MPEG-2/4, or audio). To avoid an RTP type conflict, the values specified on both sides of the connection must be the same. The default value of "0" automatically sets the appropriate media type. You are advised not to change this setting.		
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.		

12.3.7   RTSP Transmitter

RTSP Transmitter

DSCP field:	0
Default multicast IP address:	0.0.0.0
Default multicast port:	50000

Audio > Advanced > RTSP Transmitter

Item	Description
DSCP field	Range: [0...63]. DSCP (Differentiated Services Code Point) uses the first 6 bits of the ToS (Type of Service) field in the header of IP packets for packet classification purposes. The bit pattern in the field indicates the type of service and forwarding behavior at the next node. With 26 bits, up to 64 network service types can be defined. *RFC 2724* (*http://www.ietf.org/rfc/rfc2474.txt*) describes the Differentiated Services (DS) field and the DiffServ Code Point. See also the note on Differentiated Services later in this chapter.
Default multicast IP address	Destination IP address for multicast sessions.
Default multicast IP port	Port number for multicast sessions.

Note on Differentiated Services: Differentiated Services (DiffServ, or DS) is a method for adding QoS (Quality of Service) 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 - i.e. 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 realized, for example, through priority queuing, bandwidth allocation, or by assigning dedicated routes.

Note on RTP and RTCP: The Real-time Transport Protocol (RTP) is designed for end-to-end real-time, audio or video data flow transport. It is regarded as the primary standard for video/audio transport over multicast or unicast network services. RTP does not provide guaranteed delivery, but sequencing of the data makes it possible to detect missing packets. It allows the recipient to compensate for breaks in sequence that may occur during the transfer on an IP network. Error concealment can make the loss of packets unnoticeable.
RTP is usually used in conjunction with the Real-time Transport Control Protocol (RTCP). RTP carries the media streams. RTCP provides reception quality feedback, participant identification and synchronization between media streams.

12.3.8   SAP Settings

Audio > Advanced > SAP Settings

The BC620WDR includes a SAP announcer. The Session Announcement Protocol is used to advertise that a media stream generated by the BC620WDR is available at a specific multicast address and port. For more information about SAP, see the note below.

Item	Description
Enable SAP	When selected, session announcements are sent at the frequency determined by the Announcement interval parameter and the media stream is transmitted to the multicast IP address specified in the Stream dest. IP address box.
Stream name	Enter a descriptive name to identify the media stream.
Stream dest. IP	Enter the multicast IP address the media stream is to be sent to. The address must be within the range defined by the Multicast IP range parameter.
Stream dest. port	The destination port number. Default: 1024.
Stream DSCP field	Range: [0…63]. See the note on DSCP.
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.
Announcement interval	Determines the frequency of announcements.
Session scope	*Global*, the default session scope, sets the *Multicast IP range* parameter to 224.2.128.0 - 224.2.255.255 (IPv4 global scope sessions). A SAP listening application will recognize the global scope and automatically listen for SAP announcements at the 224.2.127.254 multicast IP address. The *Administrative* session scope allows you to enter a custom IP range within the 239.0.0.0 - 239.255.255.255 (IPv4 administrative scope sessions) range. For an Administrative session scope, the multicast address for SAP announcements will be set to the highest address in the relevant administrative scope. For example, for a scope range of 239.16.32.0 - 239.16.33.255, the IP address 239.16.33.255 is used for SAP announcements.
Multicast IP range	See Session scope.

Note on the Session Announcement Protocol (SAP): SAP, defined in *RFC 2974* (see RFC 2974 - *http://www.ietf.org/rfc/rfc2974.txt*), is a protocol for advertising multicast session information. A SAP announcer periodically broadcasts announcement packets which include the session description information of multicast sessions presented by the announcer. SAP uses the Session Description Protocol (SDP) as the format of the session descriptions. The announcement is multicast with the same scope as the session it is announcing, ensuring that the recipients of the announcement are within the scope of the session the announcement describes. SAP listening applications can listen to the announcements and use the information to construct a guide of all advertised sessions. This guide can be used to select and start a particular session. The SAP announcer is not aware of the presence or absence of SAP listeners.

13 Data RS-422/485

This chapter describes the Data RS-422/485 page of the BC620WDR.

In This Chapter

13.1 General Settings

Data RS-422/485 page

Item	Description	
Wire mode	*RS-422*	The RX-4xx interface type is set in software. Select the appropriate type from this list.
	RS-485 (2-wire)	
	RS-485 (4-wire)	

13.2 UART Settings

The BC620WDR uses a Universal Asynchronous Transmitter/Receiver (UART) for data transmission. The UART recognises and reproduces the words in the data stream. This is only possible if the UART is programmed to understand the serial data format.

Item	Description	
Bit rate	*1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bit/s.*	The speed of the digital transmission - that is, the amount of information transferred/processed per unit of time.
Word length (excluding parity)	*5, 6, 7, 8.*	Determines the number of bits that is transferred in a single operation.
Stop bits	*1, 2.*	Indicate the end of a data character to enable the receiver to resynchronise with the stream.
Parity mode	*None, Even, Odd, Mark , Space.*	Enables sending of an extra bit with each data character for error detection purposes.

13.3 Make data connections

Data RS-422/485 > MX Transmitter/Receiver Settings

After selecting a data mode (see General Settings) and configuring the interface (see UART Settings), data link configuration is done in the same fashion as described for video links.

⇥ **To configure a data link**

1. In the *Transmitter Settings* section, set at least one destination IP address.
2. Set a port number or leave it at the default.
3. Enable the stream.
4. Click **SAVE** to write the new configuration to the device.

The data interface is bidirectional in the sense that apart from a streams transmitter, a receiver is available on the same unit. However, the data transmitter and receiver are independent of one another, except for the data interface settings.

Do not forget to enable both the transmitter and the receiver, and to configure the UART correctly (see Advanced Settings).

When using multicasting, it is possible for a group of codecs to both send and listen to the same multicast address.

Highlighted fields

The source address and port number fields are highlighted in green when the enabled receiver receives a stream from the specified source. The two fields are marked in red when no stream is received with the receiver enabled and correctly configured.

13.4　TCP Server Settings

Data RS-422/485 > TCP Server Settings

TCP connections are always bidirectional, so no separate transmitter and receiver settings are needed.

Item	Description
Server enable	Enables streaming of UART data over TCP using a client/server connection. The server accepts requests from a specific client, or any host if not specified.
Server port	Range: [0...65535].

13.5　Advanced

Important: If in doubt about these settings, do *not* change the default values.

13.5.1　RS-4xx Settings

RS-422/485 > Advanced > RS-4xx Settings

For details about 'data words' and data transfer optimisation, see the note below.

Item	Description
Bit rate	Range: [300...115200]. The speed of the digital transmission, that is - the amount of information transferred/processed per unit of time. Enables you to set a bit rate other than the presets in the UART settings section.
UART gap timeout	Range: [0...255] data words. Will have the next packet sent when the line has remained idle for longer than the timeout.
UART max. latency	Range: [0...255] data words. The maximum latency of the data channel is controlled by forcing a packet to be sent when the first data word of the packet was received longer ago than the number of word times set here.
Line termination enable	Normally, the devices at the two extremes of a bus are terminated, while intermediate devices are not. Therefore: RS-422, always enable (being point-to-point); RS-485, enable only for the first and last module connected to the bus configuration.
Line biasing enable	If biasing is needed (RS-485), it should be enabled on at least 1 module on the bus. RS-422 does not require biasing.

Note on Data Transfer Optimisation: A 'word time' is the transmit time for one data word. The amount of time one data word takes to travel on the line is determined by bit rate and word length. Using the *UART gap timeout* and *UART max. latency* variables you can tailor the data channel for your specific protocol. A delay < 5 milliseconds is possible with minimal settings. One or more data words are bundled in packets. The packaging process influences the performance of the UART mode. At high bit rates, say 115 kbit/s, it may be desirable to adjust some of the low-level UART settings to prevent high CPU loads. At such speeds, a large number of small network packets might increase CPU load by 15%.

The process can be optimised using the RS-4xx settings in the Advanced Settings section. Packets can be sent depending on the configuration of the *UART gap timeout* and *UART max. latency* variables. These can be set such that fewer but larger packets are sent, making the stream simpler to handle, at a considerably lower CPU load. Configuring these settings is often a trade-off between latency (due to packaging) and payload efficiency. In other words, many network packets with a small payload (low latency) versus fewer packets with a large payload (higher latency).

At lower bit rates, a need for smoother PTZ may also require modification of these low-level settings. Note that this depends on the application. For example, PTZ commands must be sent frequently, but require few words. Latency can be minimised by proper fine-tuning of the *UART gap timeout* and *UART max. latency* variables.

13.5.2   Transmitter

Data RS-422/485 > Advanced > Transmitter 1

Item	Description
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.
FloodGuard enable	Should be on when sending to a unicast IP address, so that an alarm can be generated if no control messages from the receiver have come in for the time set by the FloodGuard throttle delay variable.
FloodGuard throttle delay	Amount of time after which the transmitter will enter throttled mode.
FloodGuard throttle interval	Sets the frequency of empty packets being sent into the network while the transmitter is in throttled mode.
Stream type	The UDP + NKF option will add an extended RTP header for Siqura applications requiring extra information.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

13.5.3   Receiver 1

Data RS-422/485 > Advanced > Receiver 1

Item	Description
Source port filter	Can be used to filter incoming data traffic. With multiple signals sent to the same IP address and destination port number, Source port filter can be used to filter the input, that is - to accept only data from the transmitting port specified here. The filter will not be active if set to 0 (the default and recommended setting).
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).
Reorder buffer size	Used to reorder incoming packets.
Stream fail delay	Range: [0...10000] ms. Default: 300 ms. Timeout in ms before going to NoStream state.
FloodGuard enable	Should be on, to enable the sending of control messages.
FloodGuard tx interval	Interval at which the receiver sends control messages to the transmitter (see the section on FloodGuard).
Stream type	The UDP + NKF option will add an extended RTP header for Siqura applications requiring extra information.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.
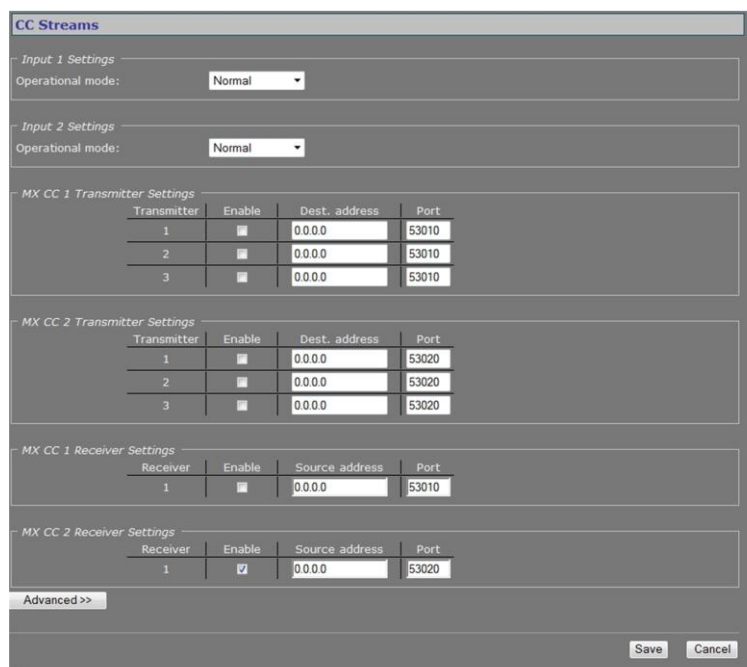
14 CC Streams

This chapter provides information about the BC620WDR's contact closure (CC) channels, CC status, and alarms.

In This Chapter

14.1 CC channels, CC status, and alarms

CC Streams page

CC channels

The contact closure channels of the BC620WDR, each capable of transmitting three copies per signal, are independent and their transmitters and receivers can also be used separately. It is possible to send a CC-signal from a CC 1 interface to a CC 2 and vice versa.

CC status

The receiver relays are normally open (fail-safe). Each CC input is sampled 100 times per second. Changes are transmitted directly, so overall latency of the contact closure signals is <20 ms. To confirm, the actual contact closure status is transmitted every 100 ms; there is no further forward error correction on these signals.

Alarms

If a contact closure signal is to be transmitted to a PC, the software requesting it can open a contact closure stream from the BC620WDR, which will carry the CC information. At the opposite end of the link (a PC running the software), the contact closures may be regarded as, and even named alarms, but those 'alarms' are not necessarily related to module alarms.

In the module, closing a physical CC input will change the payload of the existing stream, as described above, and additionally cause a module alarm saying the input status is 'closed'. A notification about the latter module alarm is also sent out over the network and can be caught separately by application software. Alternatively, application software can poll the BC620WDR and check for the module alarm. Stream alarms (link alarms in the modules, at both link ends) become active if the link fails.

14.2   Input # Settings

CC Streams > Input 1 Settings

Item	Description	
Operational mode	*Normal*	Direction.
	Invert	
	Force active	Always on (e.g. for testing purposes).
	Force inactive	Always off.

14.3   Make contact closure connections

Making CC links is similar to making video/data/audio links, but without additional interface configuration.
  ‣   To make a contact closure connection
  ‣   On the Transmitter side, fill in a destination IP address and port number for each codec you want a CC stream to go to, and then enable the stream.
  ‣   On the other side of the link (i.e. the codec you want to receive the CC stream), fill in the source IP address, the local port number (the same as specified for the transmitter), and then enable the receiver.

Note: Clearing an Enable check box disables the transmission or reception of the stream, not the contact input or output itself. If the stream is disabled, the contact can still be controlled and read using MX software or the HTTP API.

14.4   Advanced

Important: If in doubt about these settings, do *not* change the default values.

14.4.1   Transmitter

CC Streams > Advanced   > Transmitter 1

Item	Description
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).
Multicast TTL	Range: [0...127]. Specify the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

14.4.2   Receiver 1

CC Streams > Advanced > Receiver 1

Item	Description
Source port filter	Can be used to filter incoming data traffic. With multiple signals sent to the same IP address and destination port number, Source port filter can be used to filter the input, that is - to accept only data from the transmitting port specified here. The filter will not be active if set to 0 (the default and recommended setting).
Connection priority	Parameter intended for use with MX Software Development Kit (MX SDK).
Reorder buffer size	Used to reorder incoming packets.
Stream fail delay	Range: [0...10000] ms. Default: 300 ms. Timeout in ms before going to NoStream state.
Link loss alarm timeout	Range: [1...1000] s. Default: 10 s. Time in seconds before alarm sent.

15 PTZ

The BC620WDR itself does not have PTZ functionality, but it can be mounted on a PTZ mounting bracket which can then be controlled from the BC620WDR's serial data port (RS-4xx). With a PTZ driver selected on the PTZ web page, the PTZ control panel is available on the Live Video page. This chapter explains how to enable PTZ control, upload and remove PTZ drivers, and configure data settings.

In This Chapter

15.1 Enable PTZ control
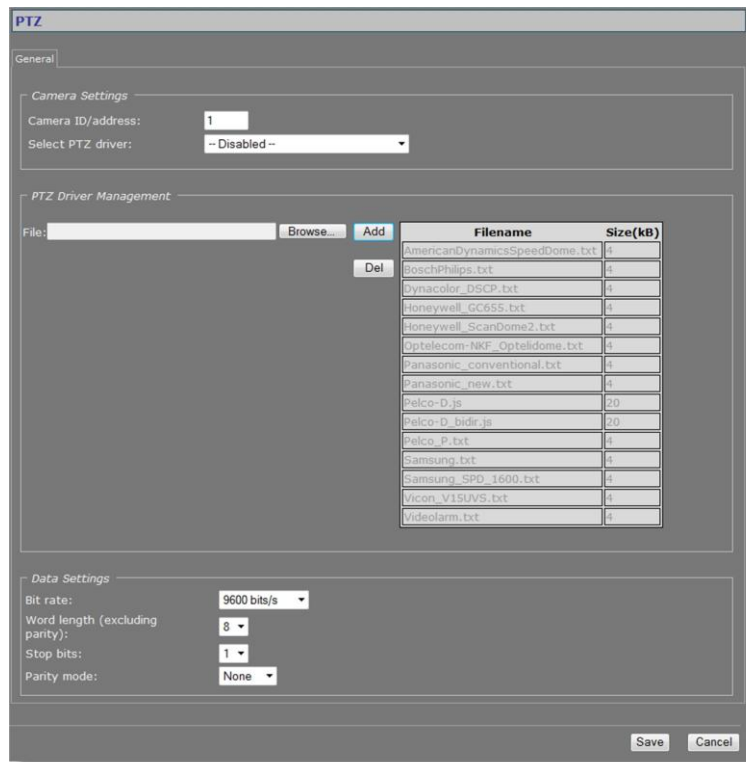
PTZ page

PTZ camera control is enabled by selecting a driver that is supported by the camera. If the required driver is not included in the PTZ driver list, you can upload it to the BC620WDR (see below).

⇥ **To enable PTZ control**

1. In the *Camera Settings* section, specify the Camera ID/address.
2. From the *PTZ driver* list, select the protocol supported by the PTZ device you wish to control.
3. Click **Save**.
   You can now control the camera with the control panel on the Live Video page.

15.2 Upload/Remove PTZ drivers

⇥ **To upload a PTZ driver**

1. In the *PTZ Driver Management* section, click **Browse**.
2. In the *File to Upload* dialog box, browse to the folder containing the driver.
3. Select the appropriate file (`.txt` or `.js` extension), and then click **Open**.
   The driver displays in the *File* text box.
4. Click the **Add** button.
   The driver is added to the list of available drivers in the *PTZ Driver Management* and *Camera Settings* sections.

⇥ **To remove a PTZ driver**

1. In the *PTZ Driver Management* section, select the driver you wish to remove.
2. Click the **Del** button.

15.3 Data Settings

PTZ > Data Settings

Item	Description	
Bit rate	*1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bit/s.*	The speed of the digital transmission - that is, the amount of information transferred/processed per unit of time.
Word length (excluding parity)	*5, 6, 7, 8.*	Determines the number of bits that is transferred in a single operation.
Stop bits	*1, 2.*	Indicate the end of a data character to enable the receiver to resynchronise with the stream.
Parity mode	*None, Even, Odd, Mark , Space*	Enables sending of an extra bit with each data character for error detection purposes.

Note: Changes you make in the Data Settings section are copied to the RS-422/485 page.

16 Event Management

This chapter describes the Event Management page.

In This Chapter

16.1 Associate events with output facilities
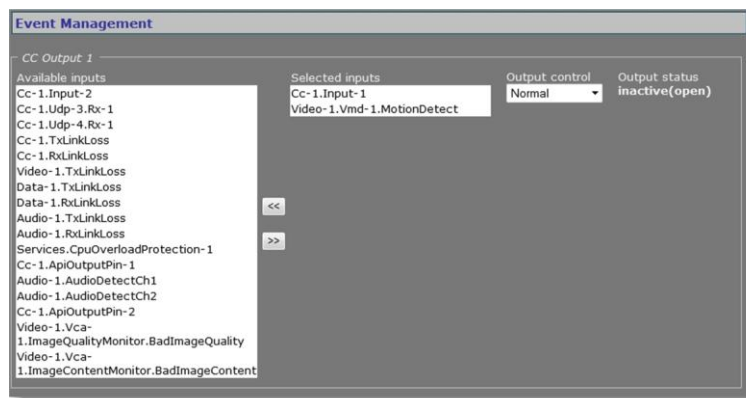
Event Management

On the Event Management page, you can configure how the BC620WDR is to handle incoming events/alarms. The event sources listed under Available inputs can be routed to a CC output, CC stream, or FTP push.

16.1.1 CC Output

Item	Description	
Available inputs	List of sources that can be selected as inputs for each of the two contact closure outputs.	
Selected inputs	Selected inputs are connected with a logical OR so that any one will cause a remote contact to close.	
Output control	*Normal*	Direction.
	Invert	
	Force active	Always on (for testing purposes, for example).
	Force inactive	Always off.
Output status	*Inactive (open)* or *active (closed).* Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.	

16.1.2 CC Stream

Event Management > CC Stream 1

Item	Description
Available inputs	List of sources that can be selected as inputs for each of the two contact closure streams.
Selected inputs	Selected inputs are connected with a logical OR so that any one will cause a remote contact to close when the corresponding transmitter is set up correctly from the CC Streams page.
Stream status	*Inactive (open)* or *active (closed).* Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.

16.1.3   FTP Push

If FTP push is configured to be event-triggered (see the FTP Push tab of the Video page), you need to select one or more sources from the Available inputs list that will activate an image upload to the FTP server(s).

Event Management > FTP Push 1. Two inputs associated with FTP Push.

Item	Description
Available inputs	List of sources that can be selected as triggers for an FTP push.
Selected inputs	On selection of multiple inputs, the inputs are connected with a logical OR. Any one will cause an image upload to the FTP server.
FTP push status	*Inactive (open)* or *active (closed).* Active: one or more of the selected inputs is true. Inactive: none of the selected inputs is true.

17 Device Management

This chapter describes the Device Management page of the BC620WDR. On this page, you can view identification information and assign device labels. You can also prepare the unit for SNMP management, enable support for Siqura's MX protocol, enable Auto Discovery, enable ONVIF, upgrade/downgrade the embedded firmware, and reboot the BC620WDR.

In This Chapter

17.1 General
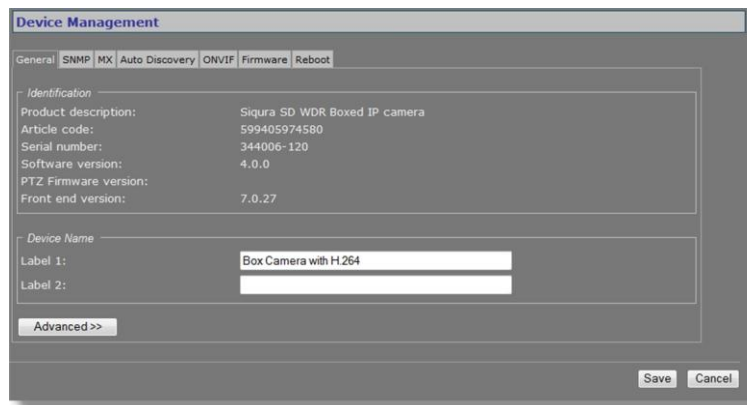
Device Management > General

17.1.1 Identification

This section offers administrative module information.

17.1.2　Device Name

Item	Description
Label 1	The Device name section contains label settings, which can be edited and saved.
Label 2	Values entered for the Label 1 and Label 2 variables are stored in the Management Information Base (MIB) of the module. The labels jointly constitute the device label, a user-friendly name for the physical device, which will serve to identify and address the module on the network when working with the MX network service and MX applications. The current value for Label 1 is displayed in the upper pane of the web pages.

Title pane with Label 1 value

17.1.3　Advanced

Device Management > General > Advanced

17.1.3.1　Alarm Settings

Item	Description
Board temperature alarm	A notification is issued on the network when the temperature value set here is exceeded. Module alarms can be read and processed using additional Siqura software (which will also enable you to configure alarm levels and destinations).

17.1.3.2　Identify

Item	Description
Flashing DC LED	Range: [0 …1000]. To identify a BC620WDR among other units, enter a value and click **Save**. The PWR LED on the back of this particular unit will blink for the number of seconds you set.

17.2   SNMP

Device Management > SNMP

17.2.1   SNMP System Information

The SNMP System Information section shows the network/device data specifically made available to the SNMP manager for making the device, its location and service manager(s) traceable.

17.2.2   SNMP Communities

The community strings (names which can be regarded as passwords) in the SNMP Communities section must conform to those configured in the SNMP manager. Often, these are 'public', mainly used for the read and trap communities, and 'private' or 'netman', for read-write operations. The manager program may offer additional choices.

17.2.3   SNMP Agent

The module has an SNMP Agent running which listens for information requests from the SNMP manager on port 161 by default.

17.2.4 SNMP Traps

A BC620WDR alarm status change generates a trap which can be caught by any SNMP manager. The BC620WDR can, for example, send traps on the occurrence of Image Quality and Camera Tampering events. Variables, which can be read from the BC620WDR's MIB through an SNMP manager, indicate why the alarm occurred. The OPTC-VCA-MIB required for this can be downloaded, together with the other BC620WDR MIBs, at www.siqura.com.

Note that *Version* and *Destination IP : port* are required fields.

Item	Description
Version	The SNMP version used.
Destination IP : port	The IP address associated with the manager program, and the destination port (162 is the default port).
Alternative destination IP : port	If desired, an alternative destination IP address and port can be added.
Enable authentication trap	It is possible to add an authentication trap to be able to catch attempts at access using the wrong community string.

17.2.5 Polling

Depending on facilities offered by the SNMP manager, a number of variables can be read out and in a few cases be edited and set. The Ethernet port variables are contained in the 'system' and 'interfaces' sections of RFC 1213-MIB.

17.3   MX

Device Management > MX

17.3.1   MX/IP

MX/IP is a UDP protocol used to communicate with Siqura equipment over a network connection. The Siqura Software Suite applications use the MX/IP protocol to access, configure, and control Siqura network devices.

Item	Description
Enable MX	In addition to the proprietary MX/IP protocol, a BC620WDR can be accessed, configured and managed using a variety of open standards. Therefore, you can disable the MX protocol. Be aware that doing so will prevent you from upgrading the BC620WDR firmware through the MX Firmware Upgrade Tool application.

17.3.2   MX Notifications

Item	Description
IP address	With 255.255.255.255 as the IP address for the manager, the MX notifications would be broadcast over the subnet.
Port	Generally, the MX notifications port must not be modified.
Unsolicited notifications interval	Sends the module status as MX notification at the specified interval to be picked up by a management program.
Retransmission count	If desired, notifications can be retransmitted. With a retransmission count value of 2, the actual number of transmissions equals 3 (including the original transmission).
Retransmission interval	Sets the frequency of retransmissions.

17.4   Auto Discovery
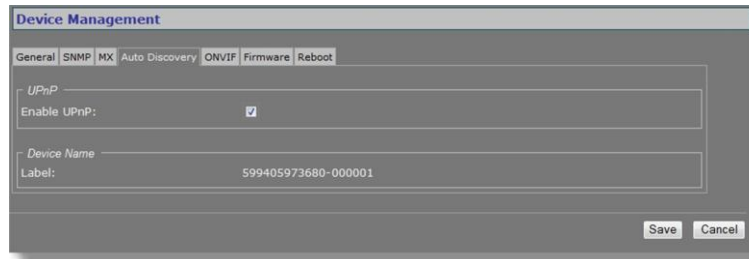
Device Management > Auto Discovery

17.4.1   Advertise the BC620WDR

On the Auto Discovery tab, you can enable UPnP (Universal Plug and Play). If enabled, UPnP allows the BC620WDR to advertise its presence and services to control points on the network. A control point can be a network device with embedded UPnP, a VMS application or a spy software tool, such as Device Spy.

17.4.1.1   Note

Note on UPnP: The goal of Universal Plug and Play (UPnP), a set of computer network protocols, is to enable peer-to-peer simple and robust connectivity among stand-alone devices and PCs from different vendors. UPnP networking involves (some or all of) the following steps.

Step 1: *Discovery*. Devices advertise their presence and services to a control point on the network. Control points can search for devices on the network. A discovery message is exchanged, containing a few essential specifics about the devices, e.g. its type, identifier and a pointer to more detailed information.

Step 2: *Description*. The control point can request the device's description from the URL provided in the discovery message. The device description is expressed in XML and includes vendor-specific information, such as the model name, serial number, manufacturer name, URLs to vendor-specific web sites.

Step 3: *Control*. The control point can send actions to a device's service.

Step 4: *Event*. The control point listens to state changes in the devices.

Step 5: *Presentation*. If a device has a URL for presentation, the control point can display a page in a web browser, and – if the page offers these capabilities - allow the user to control the device and/or view the device status.

The BC620WDR supports the following Universal Plug and Play (UPnP) functionality: *Discovery*, *Description* (partly supported), and *Presentation*.

17.4.2   Test UPnP

After enabling UPnP, you can use a tool, such as Device Spy (included in the 'Developer Tools for UPnP Technologies'), to check if the BC620WDR correctly advertises its presence and device description on the network.

» **To view the BC620WDR device description in Device Spy**

1. Start Device Spy.
   The network is scanned.
   A list of detected UPnP devices displays in the left-hand panel.
2. Select your BC620WDR in the left-hand-panel.
   The device description is shown in the right-hand panel.
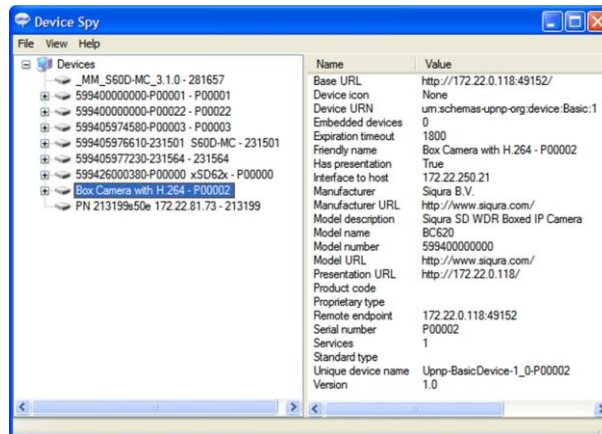
BC620WDR device description in Device Spy

» **To view the BC620WDR device description in XML (using Device Spy)**

1. Start Device Spy.
2. In the left-hand panel, right-click the BC620WDR entry.
3. Select **Get Device XML**.
   The XML device description opens in your web browser.
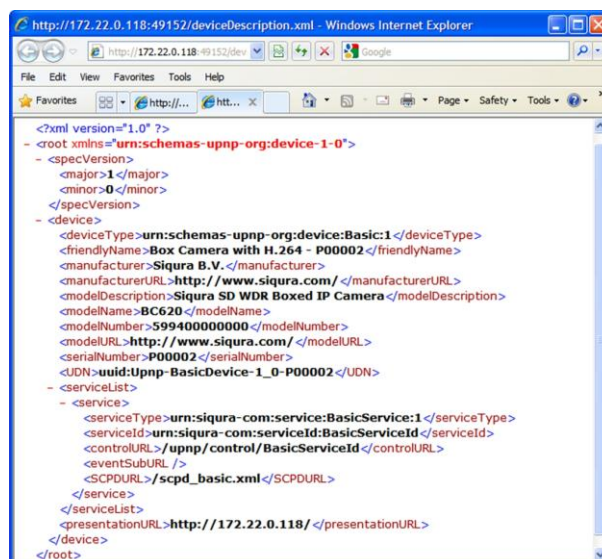
BC620WDR XML device description

⇥ **To access the BC620WDR's web pages via Device Spy**

1. Start Device Spy.
2. In the right-hand panel, double-click the **Presentation URL** entry.
   -or-
   In the left-hand panel, right-click the BC620WDR entry, and then select **Display Presentation Page**.
   The login page of the BC620WDR displays in your browser.

Note: Do not double-click the Base URL entry in the Details pane. The connection will not be made, due to an incorrect port number. Use the Presentation URL instead.

17.5   ONVIF

Device Management > ONVIF

The BC620WDR supports the ONVIF standard. On the ONVIF tab, you can enable ONVIF compatibility and ONVIF discovery.

Item	Description
Enable ONVIF	Enables the ONVIF interface on the BC620WDR.
Enable ONVIF Discovery	Makes the BC620WDR discoverable for ONVIF clients. Clear this check box if you prefer to disable discovery. In that case, the BC620WDR can still be controlled from ONVIF clients that "know" of its existence.

17.5.1   Note

Note on ONVIF: The Open Network Video Interface Forum (ONVIF) is a global and open CCTV/security industry forum which aims to increase interoperability of cameras, codecs, and VMS and similar systems of different brands and manufacturers by standardising the discovery, management, control and other interfaces between them. The ONVIF architecture is largely built on top of web services. Web services typically use the HTTP protocol to exchange XML messages according to the Simple Object Access Protocol (SOAP) standard. A standardised API is defined between server and client devices. ONVIF defines an NVT (Network Video Transmitter) to model the server side (that is, codecs and cameras) and an NVC (Network Video Controller) to model the client side (that is, VMS systems and the like). The communication between NVC and NVT is standardised by the ONVIF core specification document and the API is formally defined by making use of WSDL (Web Service Description Language) files.

17.6   Firmware
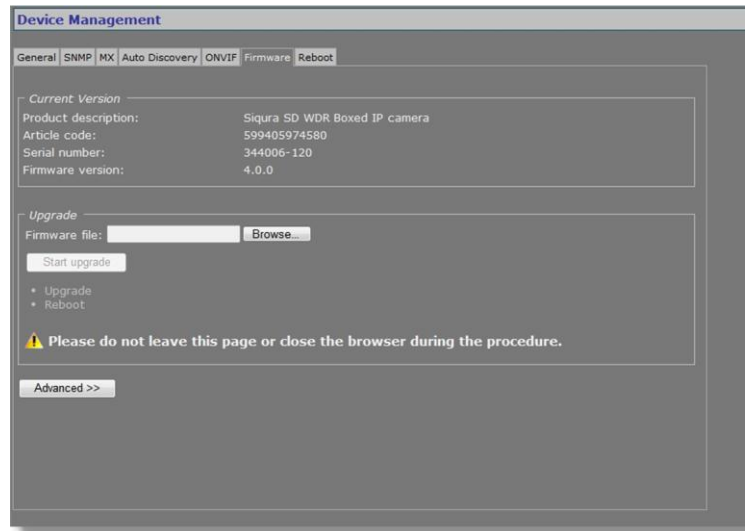
Device Management > Firmware

17.6.1   Firmware images

The BC620WDR has two firmware storage areas: a *fixed image* area and an *upgrade image* area. The fixed image area contains the original factory version of the firmware. This cannot be erased. The upgrade image area is usually empty upon factory release.

If the existing firmware in the BC620WDR is to be replaced, a new version can be written to the upgrade image area. There, the new image resides in erasable (flash) memory.

An upgrade image can replace an existing upgrade image written to the device at an earlier upgrade. It is essential that the upgrade image is compatible with the BC620WDR.

17.6.2   Current Version

This section offers information on the currently active firmware version.

17.6.3   Upgrade

This section of the webpage enables you to upgrade the firmware residing in the upgrade image area.

Important: On upgrading a BC620WDR to firmware version 4.0 and higher, all existing users are deleted. After a successful upgrade, you can access the webpages with the default Admin account (user name = Admin; password = 1234).

Note: It is possible to use the upgrade section to downgrade a unit to an earlier version of the firmware. As a result, a unit may have version 4.0.1 in its fixed image area and version 3.12 in its upgrade image area, for example. After the downgrade, the unit can only be accessed by user "root" with a "1234" password. With these credentials, you can log on and then perform a reset to factory settings. This restores the default version 3.12 users - that is, "root" and "admin", both with an empty password.

↦ **To upgrade the BC620WDR firmware**

1. On the *Device Management* page, open the **Firmware** tab.
2. In the *Upgrade* section, click **Browse**.
3. In the *Choose File to Upload* dialog box, browse to the folder containing the firmware image.
4. Select the firmware file (`.sqrfw` extension), and then click **Open**.

   Note: Files with an `.nkffw` extension cannot be used to upgrade the BC620WDR via the web page. You can use them to upgrade the unit through MX Firmware Upgrade Wizard. This software is embedded in Siqura's MX Configuration Tool and is also available as a stand-alone tool.

5. Click **Start upgrade**.
   Progress of the upgrade is shown under the *Start upgrade* button.

   Important: Do not leave the Firmware tab or close your browser during the upgrade procedure.

   A "Successfully upgraded to version ..." message indicates a successful upgrade.
6. Click **refresh now** to refresh the web page immediately, or wait for it to refresh automatically after 30 seconds.
   The new software version displays in the Current Version section of the Firmware tab.

17.6.4 Troubleshoot upgrade issues

Successful upgrades are reported as "Successfully upgraded to version ..." In the event of an unsuccessful upgrade, the following error messages may help you pinpoint the cause of the problem.

▸ *Upgrade procedure already in progress*
   The unit received multiple upgrade requests at approximately the same time. However, only one request can be handled at a time. The later request receives this error message.

▸ *Invalid firmware file*
   The unit performs a number of checks to determine the validity of the file. If it finds problems with the file, such as the file not being a firmware file with a `.sqrfw` extension, it displays this error message.

▸ *Device hardware is incompatible*
   If the image identifier of the hardware does not match the image identifier of the firmware file, this error message indicates that the selected firmware file is not intended for the unit. In that case, the upgrade procedure is terminated. The fixed image and the upgrade image stay in the memory of the unit. After a reboot, the unit runs the **same image** as before the reboot.

▸ *Firmware file is corrupt*
   The firmware file contains a CRC error. When this error occurs, the unit reboots automatically and restarts with the **fixed image**.

▸ *Rule validation failed*
   The rules embedded in the firmware file and the result of checking these rules indicate that the firmware should not be installed on this unit.

▸ *Failed to write firmware to flash*
   The firmware file is streamed directly into flash. Various errors may occur while writing the firmware to flash. There may be connection loss, for example, or a reboot during the upgrade procedure. If any such error occurs, the unit reboots automatically and restarts with the **fixed image**.

▸ *Failed to revert back to the factory firmware.*
   This message displays in the unlikely case that something goes wrong reverting back to the factory-installed firmware.

17.6.5 Advanced

For various reasons you may want to downgrade the BC620WDR firmware to the original factory-installed image kept in the fixed image area. This can be done in the Advanced Settings section of the Firmware tab.

▸ **To revert to the BC620WDR's fixed image**

1. On the *Device Management* page, open the **Firmware** tab.
2. Click **Advanced >>**.
3. Click **Revert to factory version**.
4. To confirm the removal of the upgraded firmware, press **Continue**.
   Progress of the downgrade process is shown under the *Revert to factory version* button.

   Important: Do not leave the Firmware tab or close your browser during the downgrade procedure.

   A "Successfully reverted to version ..." message indicates a successful downgrade.
5. Click **refresh now** to refresh the web page immediately, or wait for it to refresh automatically after 30 seconds.
6. Log on to the unit again.
   On reopening the Firmware tab, the Current Version section has the version number of the factory-installed image.

17.7 Reboot
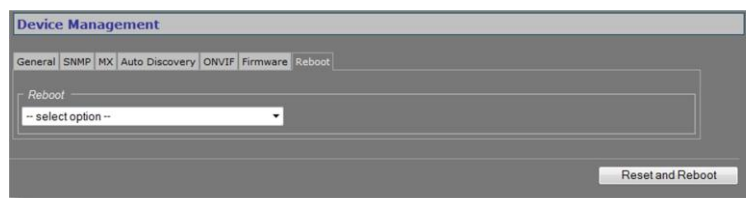
Device Management > Reboot

Item	Description
Reboot	Reboots the unit without resetting variables.
Reset to factory settings: keep network settings	Reset option for all variables that can be set by the user, with the exception of the network settings.
Reset to factory settings; incl. network settings	A complete reset which will restore the unit's settings, including the IP address/subnet mask, to their original, default values. This could make the unit unreachable for in-band communications, in which case the internal web pages are accessible only by (temporarily) moving a PC to the same subnet as the BC620WDR.

18   User Management

The User Management page is accessible to users with an Admin account. On this page, Administrators can manage user accounts and set the Linux root password.

In This Chapter
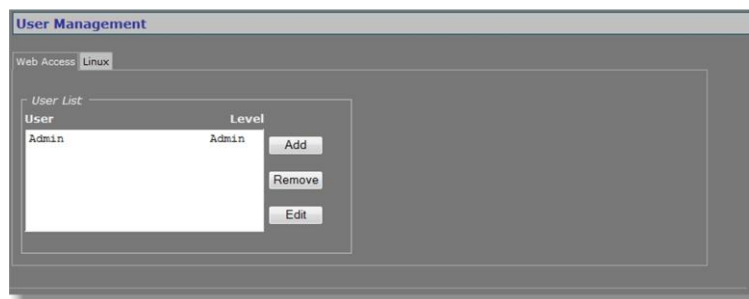
18.1   Web Access

User Management > Web Access

18.1.1   Access control
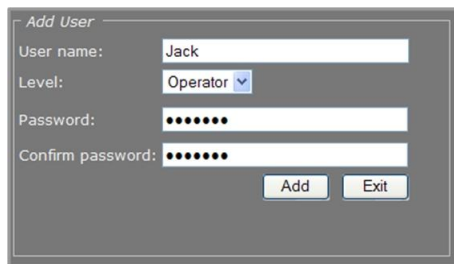
The BC620WDR has three levels of access to the internal web pages. User groups are: *Administrators*, *Operators*, and *Viewers*. Do *not* use the name of one of these groups as a user name. Out of the box, the unit has no user accounts configured. The BC620WDR supports up to 20 users at a time.

Important: On upgrading a BC620WDR to firmware version 4.0 and higher, all existing users are deleted. After a successful upgrade, you can access the webpages with the default Admin account (user name = Admin; password = 1234).

18.1.2   Manage user accounts

❯❯ **To add a user**

1. On the *User Management* page, open the **Web Access** tab.
2. In the *User List* section, click **Add**.
   The Add User section displays.
3. Enter the new user name (alphanumeric and underscore only) and password. Confirm the password to prevent errors.
4. Select the appropriate access level.
5. To write the settings into the unit, click **Add**.
   The user is added to the User List.
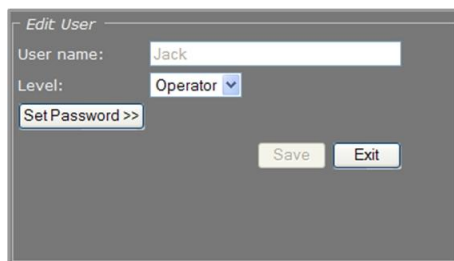
Adding a user

❯❯ **To edit a user**

1. On the *User Management* page, open the **Web Access** tab.
2. Select the user name from the *User List*, and then click **Edit**.
   The Edit User section displays.
3. Modify the user name, permission level, and/or password.
4. To write the settings into the module, click **Save**.

Editing a user

❯❯ **To delete a user**

1. On the *User Management* page, open the **Web Access** tab.
2. Select the user name from the *User List*, and then click **Remove**.
3. To confirm the deletion, press **OK**.

18.2 Linux
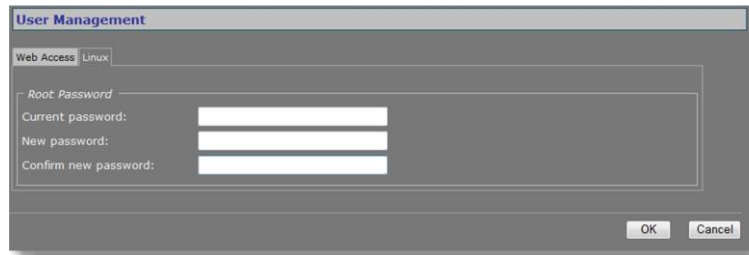
User Management > Linux

The root account is a special account that can be used for system administration. The account is always present and should be password protected at all times. The root password, which is required when logging on to Linux with root authority, is "1234" by default. Using the Linux tab an Admin can set or change the root password. Should you have forgotten the password to your Admin account and be locked out of the system, you can regain access by logging in as root with a valid root password. Through the root account you can then reset the Admin password.

19 Date and Time

The BC620WDR has a battery-supported real-time clock. This chapter explains how to adjust the date and time either manually or automatically.

In This Chapter

19.1 Date and Time

Date and Time

In the Date and Time section, you can set the date and time manually (as shown in the figure above). After entering changes, press Save to make them permanent.

The date and/or time are displayed on screen if enabled on the OSD tab of the Video page. The on-screen position and colour of the text are governed by the relevant OSD settings.

The BC620WDR adds 1 hour to the local time when Daylight Savings Time is enabled. The unit does *not* automatically change between summer and winter time. The user has to set the proper state in the Date and Time section of the web page (or use an MX/IP command).

19.2 SNTP Settings

The date and time can be adjusted automatically with the aid of a Simple Network Time Protocol (SNTP) server. If enabled, the SNTP server is queried automatically by the internal clocks, with a configurable time interval.

⇥ **To set up the BC620WDR for use with an SNTP server**

1. In the *SNTP Settings* section, clear the **Enable time service** check box, and then click **Save**.
2. On the *Time zone* list, select your local zone.
3. Select **Enable Daylight Savings Time**, if required.
4. Click **Save**, and then wait for 2 seconds.
5. Set the **Date** and **Local time** values.
   A maximum error of 5 minutes is allowed for these settings.
6. Click **Save**.
7. In the *SNTP Settings* section, select the **Enable time service** check box.
8. Select the **IP address from DHCP** check box or specify the IP address of the time server.
   Assigning the IP address via DHCP requires that DHCP is enabled in section Advanced of the Network page.
9. Adjust the **Time service query interval** (if necessary), and then click **Save**.
   The unit will now synchronise (within the interval set in the SNTP Settings section) to the time server and remain synchronised, also after reboots.

Notes for advanced users

‣ Far off (more than a few minutes) or jumping time server values may be rejected by the unit.
‣ You should *never* test the tracking to the time server by changing the time in the NTP server. You can only test it by leaving Time Service mode, changing "Local Time" slightly (max 5 minutes), and then enabling Time Service mode again.
‣ After detecting a negative time jump (between 0 … -1 hour), when connecting to the NTP server, for example, the next NTP client update cycle will be delayed for that time plus the normal polling interval. You may disable, and then enable NTP mode to immediately synchronise.
‣ Changing the local time may sometimes trigger a reboot of the unit. The time will be correct after the reboot.

19.3 Advanced

Date and Time > Advanced

Item	Description
User defined time zone	Enables you to enter a custom time zone. The Time zone list in the Date and Time section indicates "User defined" on entering and saving a custom value.

20 Multicast, multi-unicast, and port numbers

The BC620WDR can be used in a multicast setting. This chapter outlines IP multicast and one of its methods in particular: source-specific multicast. It then describes the concept of multi-unicast. You also learn about assigning valid port numbers.

In This Chapter

20.1 Multicast

IP multicast

The BC620WDR supports IP multicast. This is a method for 'one-to-many' real-time communication over an IP network. The technique can be used to send BC620WDR media streams to a group of interested receivers in a single transmission. The intermediary network switches and routers replicate the data packets to reach the multiple receivers on the network. The switches and other network devices used must be carefully configured for, and capable of handling multicasting and its associated protocols (most notably IGMP). Packets should be sent over each link in the network only once. If not, broadcasting will occur, which can put a very heavy load on the network. This is a phenomenon inherent to multicasting and the facilities of network devices, not of the BC620WDR itself, although it is compounded by the density of the UDP streams used.

Multicast group

A multicast group is used by the source, that is - the BC620WDR, and the receivers to send and receive multicast messages. To define a multicast group, the source unit should be assigned a valid multicasting ('destination') TX stream address and the destination units should get this same address as source. IPv4 uses the address range 224.0.0.0 through 239.255.255.255 for multicast applications. The source unit has no knowledge of how many receivers there are. The group vanishes when the source is disabled, but the source will *not* automatically be disabled when the last remaining destination is cancelled and will keep transmitting at least towards the nearest switch. Additionally, it is possible to have the multicast group units send unsolicited membership reports, keeping it alive even if only one - any - unit of the group is still active.

Source-specific multicast

The BC620WDR also supports source-specific multicast (SSM). This technique allows a receiver to specify a specific source sending to the multicast group and receive traffic originating from that source only. Singling out the source in this way can considerably reduce the network load. Note that SSM must be supported by the last-hop router and the receiver's operating system, and that the receiver requires IGMPv3 to be able to specify the specific source.

SSM is implemented on the encoder side, by having the unit transmit a multicast stream to the 232.x.x.x group (the range assigned to SSM) via RTSP. The Session Description Protocol (SDP) file generated by the RTSP server includes additional information containing the source IP (S) and the multicast group (G). The RTSP client in the decoder can then issue an IGMP join message containing S and G. The intermediary routers can use this information to determine the shortest path between encoder and decoder to route the multicast stream. On the decoder side, the user requests a stream from the encoder, using an SSM aware RTSP client (such as VLC, for example).

For more information on source-specific multicast, refer to the following.

rfc4607 http://tools.ietf.org/pdf/rfc4607.pdf
rfc4570 http://tools.ietf.org/pdf/rfc4570.pdf
rfc3569 ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc3569.txt.pdf
rfc5760 http://www.rfc-editor.org/rfc/pdfrfc/rfc5760.txt.pdf

20.2 Multi-unicast

As an alternative to multicasting, the BC620WDR features 'multi-unicasting', that is - sending out up to 4x3 independent copies of video, and 3 of audio, data and contact closure streams. If the bit rates selected are moderate, it may be more convenient to use this mechanism instead of multicasting, even though the network gets more signal to carry from the encoder.

When such a destination is removed, the source also stops sending the corresponding stream. If the input channel of a destination is disabled without disabling the source, source transmission will be throttled, but not disabled (this behaviour is selectable through the FloodGuard settings). The source downsizes the stream by sending empty UDP packets until a wake-up call is received. The empty packets, of course, carry the relevant IP/port information.

20.3 Port numbers

A valid UDP port number in a Siqura A-, C-, S-, and V-series system is an unsigned 16-bit integer between 1024 and 65536. Generally, you do not need to select other than the default receiver port numbers as given in the MIB (Management Information Base). If you want to change these receiver port numbers for some reason, use even numbers. A given receiver port number N is associated with the port number N+1, through which control information is returned to the source.

Eligible port numbers in general are within the range indicated above, with some exceptions. Those within the 3000-10000 range are reserved and/or hard-coded, or may become reserved, so only 10000-65535 are generally safe. Default port numbers (used by receivers) are shown in the following table.

| **General**		**Example**	
Video	50xxx	Video	50010
Audio	51xxx	Audio	51010
Data	52xxx	Data 1	52010 (RS-4xx)
		Data 2	52020 (RS-232)
CC	53xxx	CC 1	53010
		CC 2	53020

Default port numbers

Siqura MX applications using automatic port number allocation may use 55000 and up.

Appendix: Enabling Javascript

To have the BC620WDR webpages displayed correctly, JavaScript must be enabled in your web browser.

➠ **To enable JavaScript in Internet Explorer**

1. On the *Tools* menu in Internet Explorer, click **Internet Options**.
2. On the *Security* tab, click the Internet globe icon, and then click **Custom level**.
3. On the *Settings* list, search for *Active scripting*, and then click **Enable**.
4. Click **OK**, and then close *Internet Options*.
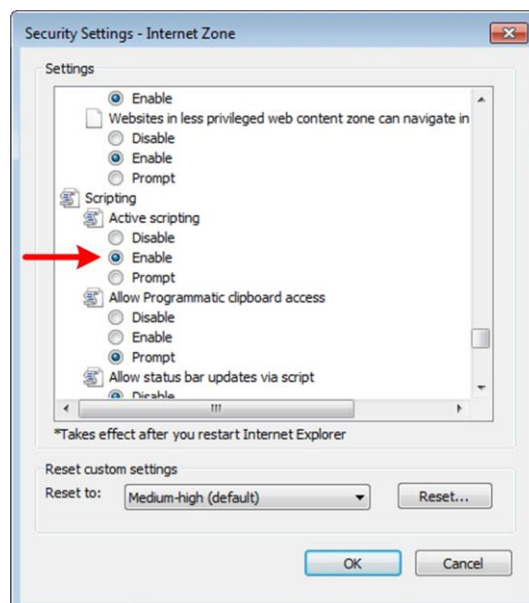
Active scripting enabled
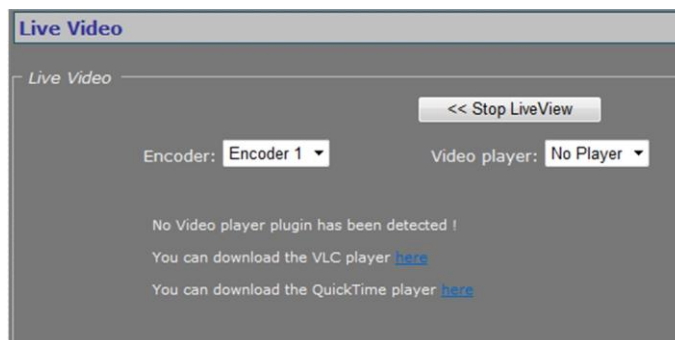
Appendix: Video player installation

Viewing video streams on the webpages of the BC620WDR requires a video player installation on the machine running the web browser. This appendix provides instructions for installing QuickTime and VLC, the video plug-ins supported by the BC620WDR.

In This Chapter

Download video player software

The BC620WDR supports QuickTime and VLC. If neither is detected when you attempt to open a video stream in the webpages, the Video player list indicates "No Player". You can use the hyperlinks on the webpage (see below) to download the required software.
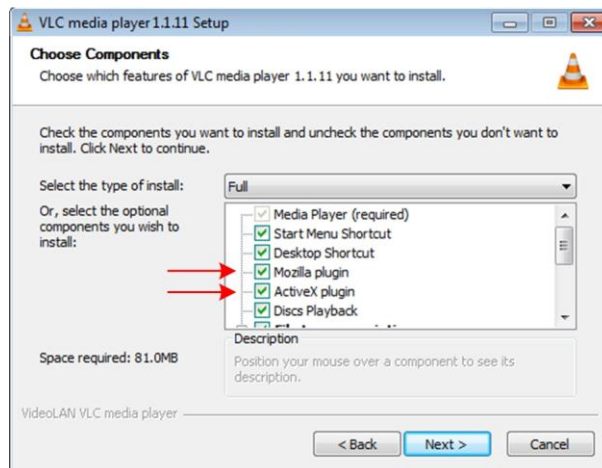

Live Video page with video player download links

QuickTime

QuickTime installation is straightforward and self-explanatory.

VLC

VLC installation requires special attention. When installing this software, make sure you select the Mozilla plug-in and ActiveX plug-in components in the VLC Setup wizard.

Required components: Mozilla and ActiveX plug-ins

Note: The support of VLC, an open source community, may differ between releases. The BC620WDR has been successfully tested with VLC v1.1.11.

VLC and Windows Vista/Windows 7

❯❯ **To configure VLC media player settings when running this plug-in on a Windows Vista or Windows 7 PC.**

1. Open the VLC media player.
2. On the *Tools* menu, click **Preferences**.
3. In the *Show settings* section (lower left corner), click **All**.
4. Expand the **Video** list, and then click **Output Modules**.
5. In the *Video output module* list, click either DirectX video output, OpenGL video output, or Windows GDI video output.
6. Expand **Output Modules**, and then click **DirectX**.
7. Clear the **Use hardware YUV > RGB conversions** check box.
8. Click **Save**.

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 BC620WDR.

In This Chapter

Supported conformance groups

The BC620WDR 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 Siqura 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, and request access.

TKH Security Sales Offices

China

Tel. +86 755 863 392 09
sales.cn@tkhsecurity.com

Czech Republic

Gemini B, Na Pankráci 129/1724, 140 00, Praha 4
Tel. +420 225 992 275
sales.cz@tkhsecurity.com

Denmark

Industriparken 16 DK-2750 Ballerup
Tel. +45 702 036 63
th@tkhsecurity.dk

France

Air Park de Paris - Bât. le Cormoran 3, rue Jeanne
Garnerin, 91320 Wissous
Tel. +33 1 64 54 15 90
Fax +33 1 64 48 68 15
sales.fr@tkhsecurity.com

Germany

Heinrich-Hertz-Str. 40, D--40699 Erkrath
Tel. +49 211 21 02 33-50
Fax +49 211 21 02 33-80
sales.de@tkhsecurity.com

Italy

Tel. +39 0331 268202
sales.it@tkhsecurity.com

The Netherlands

Zuidelijk Halfrond 4, 2801 DD, Gouda
Tel. +31 20 462 07 00
Fax +31 20 462 07 99
sales.nl@tkhsecurity.com

Poland

ul. 17 Stycznia 119, 121, 64-100 Lezno
Tel. +48 65 525 55 55
Fax +48 65 525 56 66

Singapore

25 International Business Park, #04-112 German
Centre, Singapore 609916
Tel. +65 6264 7501
Fax +65 6264 7503
sales.sg@tkhsecurity.com

Spain

Avda. de Bruselas, 5 - 1a Planta, 28108 Alcobendas,
Madrid
Tel. +34 91 676 8164
Fax +34 91 676 8614
sales.es@tkhsecurity.com

Sweden

Finlandsgatan 12, SE-164 74 Kista
Tel. +46 152 33 34 00
Fax +46 152 33 34 01
info@tkhsecurity.se

United Arab Emirates

Office No. D610, DSOA Head Quarter Building, Dubai
Silicon Oasis, Dubai
Tel. +971 4 5015741
Fax +971 4 5015742
sales.ae@tkhsecurity.com

United Kingdom

Century Business Centre, Manvers Way, Manvers,
Rotherham S63 5DA
Tel. +44 8451 172 500
Fax +44 1709 300 046
sales.uk@tkhsecurity.com

USA

12920 Cloverleaf Center Drive, Germantown,
Maryland 20874
Tel. +1 301 444 2200
Fax +1 301 444 2299
sales.us@tkhsecurity.com